УТВЕРЖДЕН
11443195.4012-053 92 2012 ЛУ

СПЕЦИАЛЬНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

«АККОРД-РАУ»

Руководство Администратора ИБ СЗИ НСД

(АИБ технологического участка)

Листов 156

Москва

2020

АННОТАЦИЯ

Специальное программное обеспечение (СПО) средств защиты информации от несанкционированного доступа «Аккорд-РАУ» (далее – «Аккорд-РАУ», РАУ) предназначено для централизованного мониторинга событий ИБ и управления средствами защиты информации от несанкционированного доступа (СЗИ НСД) «Аккорд».

Данный документ описывает действия Администратора информационной безопасности технологического участка РАУ (далее – Администратор ИБ ТУ, АИБ ТУ), связанные с непосредственной эксплуатацией системы информационной безопасности (далее – система) в штатном режиме функционирования.

СОДЕРЖАНИЕ

1 Введение 4

1.1 Область применения 4

1.2 Функции Администратора ИБ ТУ 4

1.3 Комплект поставки 4

2 Назначение и условия применения 5

2.1 Назначение 5

2.2 Условия применения 5

3 Планирование работы и эксплуатация «Аккорд-РАУ» 6

4 Работа с сервером централизованного управления 7

4.1 Общие принципы управления 7

4.2 Вкладка «Роли» 7

4.3 Вкладка «Идентификаторы» 25

4.4 Вкладка «Компьютеры системы» 30

4.5 Вкладка «Учётные записи» 52

4.6 Создание пользователя технологического участка 67

4.7 Работа с журналами 69

4.7.1 Общие сведения 69

4.7.2 Оперативный журнал 69

4.7.3 Журнал ASM 79

4.7.4 Журнал АРМ АБИ 81

5 Перечень оповещающих сообщений 84

6 Перечень сообщений ASM 89

7 Перечень событий ПАК «Аккорд» на подконтрольных объектах 141

8 Перечень событий АРМ АБИ 145

9 Перечень принятых сокращений 154

1 Введение

1.1 Область применения

Деятельность Администратора ИБ ТУ.

1.2 Функции Администратора ИБ ТУ

Администратор ИБ ТУ в рамках полномочий, делегированных ему Администратором ИБ, выполняет следующие функции:

- осуществляет следующие настройки РАУ:
  - настройка политики безопасности;
  - настройка контроля доступа;
  - настройка разрешенных коммуникационных портов;
- проводит контроль управляющего воздействия на компоненты РАУ в части:
  - изменения настроек (включая настройки мониторинга);
  - применения шаблонов настроек;
- участвует в разборе и устранении нештатных ситуаций, связанных как с работой РАУ, так и с работой СЗИ от НСД «Аккорд».

1.3 Комплект поставки

В комплект поставки РАУ входят следующие компоненты:

- сервер централизованного управления (СЦУ) с предустановленными СЗИ от НСД и ПО сервера централизованного управления;
- клиентские компоненты (сетевые агенты), устанавливаемые на подконтрольных объектах (ПКО);
- лицензии на подключение подконтрольных объектов к РАУ на touch memory (далее – ТМ) типа DS 1996;
- комплект рабочей документации на компакт-диске (CD).

2 Назначение и условия применения

2.1 Назначение

РАУ обеспечивает:

- централизованный сбор и хранение информации о зарегистрированных событиях доступа к подконтрольным объектам;
- возможность централизованного управления СЗИ от НСД «Аккорд» на подконтрольных объектах;
- единую точку контроля доступа к периферийным устройствам и контроля использования отчуждаемых машинных носителей.

2.2 Условия применения

Условия применения компонентов РАУ приведены в документе «11443195.4012-053 90. СПО СЗИ НСД «Аккорд-РАУ». Руководство Администратора».

3 Планирование работы и эксплуатация «Аккорд-РАУ»

Для более эффективного применения «Аккорд-РАУ» и поддержания уровня защищенности Администратор ИБ ТУ выполняет следующие задачи:

- поддерживает средства защиты в работоспособном состоянии и периодически контролирует корректность их работы;
- проводит изменения настроек средств защиты в соответствии с корректировками плана защиты, вызванными изменением состава пользователей, перечня решаемых задач и соответствующими изменениями функциональных обязанностей сотрудников.

В случае возникновения ситуации, когда связь между работающим по централизованной схеме ПКО и СЦУ временно невозможна (например, поломка сети, перенос оборудования на новое место, где сетевое оборудование не настроено и т.д.), а пользователю необходимо выполнять свою работу, Администратор ИБ переводит ПКО в автономный режим работы. Для этого необходимо на ПКО в ACSETWS.EXE установить флаг «Станция не управляется по сети» (или в AcWs32.ini установить параметр NoNetManaged=Yes) и перезапустить службу или перезагрузить ПКО.

4 Работа с сервером централизованного управления

4.1 Общие принципы управления

Пользовательский интерфейс ПО сервера централизованного управления подчиняется следующим правилам:

- кнопка <Добавить> предназначена для добавления той или иной сущности;
- кнопка <Удалить> предназначена для удаления той или иной сущности;
- кнопка <Импорт> предназначена для осуществления импортирования настроек с компьютеров системы в ASM;
- кнопка <Экспорт> предназначена для осуществления экспортирования настроек из ASM на компьютеры системы.

Максимальный размер имен пользователей, названий ролей, технологических участков, компьютеров, учетных записей пользователей и поля «Описание» во вкладках ASM составляет сто символов.

Все выводимые на экран окна сообщений (MessageBox) автоматически закрываются через пять секунд с эмуляцией нажатия выбранной по умолчанию кнопки.

В подразделах 4.2 – 4.5 описывается пользовательский интерфейс СЦУ, доступный администратору ИБ для выполнения его обязанностей.

4.2 Вкладка «Роли»

Права доступа (ПРД) для учетной записи определяются ролью, которая зависит от уровня субъекта доступа в иерархии (Все компьютеры-ТУ-СВТ).

В РАУ предусмотрены следующие встроенные роли[1]:

- **Admins_NSHR** – используется для первоначальной настройки системы и НШР и имеет полный доступ в ASM, под этой ролью работает Администратор нештатного режима (Администратор НШР) РАУ;
- **Admins_SCM** – под этой ролью работает Администратор РАУ;

[1] Назначение роли возможно только на ПКО под управлением ОС Windows

- **Admins** – соответствует группе «Администраторы» в «Аккорде»;
- **Admins_XXX** (где **XXX** соответствует номеру участка) – автоматически создается при создании нового технологического участка и уничтожается только при удалении данного участка; соответствует группе «Администраторы» в «Аккорде»;
- **Everyone** – соответствует группе «Обычные» в «Аккорде»;
- **Everyone_XXX** (где XXX соответствует номеру участка) – автоматически создается при создании нового технологического участка и уничтожается только при удалении данного участка; соответствует группе «Обычные» в «Аккорде»;
- **AIBs_SCM** – администратор информационной безопасности РАУ;
- **AIB_TU: имя роли** – роль, под которой работает Администратор ИБ технологического участка, создается после добавления технологического участка Администратором ИБ участка;
- **OIBs_SCM** – под этой ролью работает Оператор информационной безопасности РАУ;
- **AUDITORs_SCM** – роль, под которой работает Контролер РАУ.

В РАУ существуют два типа ролей:

- базовые роли;
- подчинённые роли.

Каждая подчинённая роль зависит от одной базовой роли. У базовой роли могут быть несколько подчинённых ролей.

В столбце «Зависит от роли» вкладки «Управление > Роли системы» СЦУ, приведённой на рисунке 1, указано, является ли данная роль базовой или подчинённой. Если роль является базовой, то данный столбец не заполняется. Если роль является подчинённой, то в данном столбце приводится информация, от какой базовой роли унаследована данная роль.

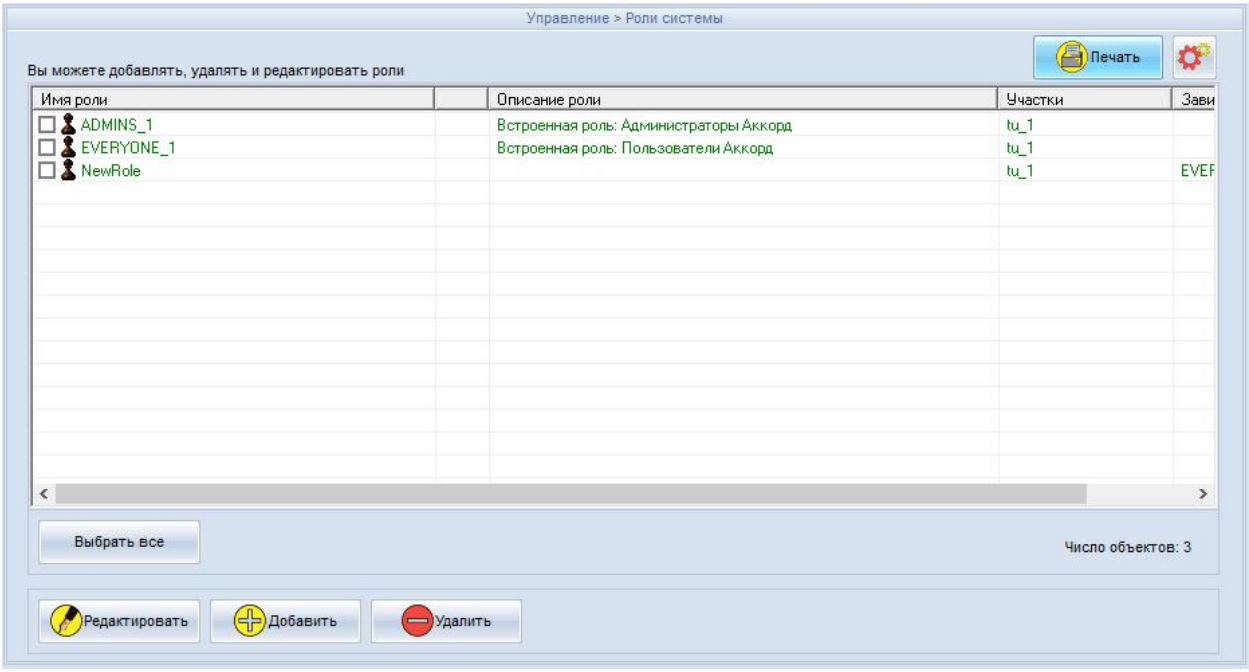

Рисунок 1 - Вкладка «Управление > Роли системы»

Выбор типа роли (подчинённая или базовая) осуществляется при её создании. При нажатии кнопки <Добавить> во вкладке «Управление > Роли системы», приведённой на рисунке 1, появляется окно добавления роли, приведённое на рисунке 2.

Если в данном окне снять флажок «Подчинённая роль. Зависит от базовой роли», то будет создана базовая роль.

При создании базовой роли необходимо задать её параметры в редакторе ПРД.

Если установить флажок «Подчинённая роль. Зависит от базовой роли» и в раскрывающемся списке указать базовую роль, то будет создана подчинённая роль.

При создании подчинённой роли все её параметры, кроме имени и описания, наследуются от базовой роли.

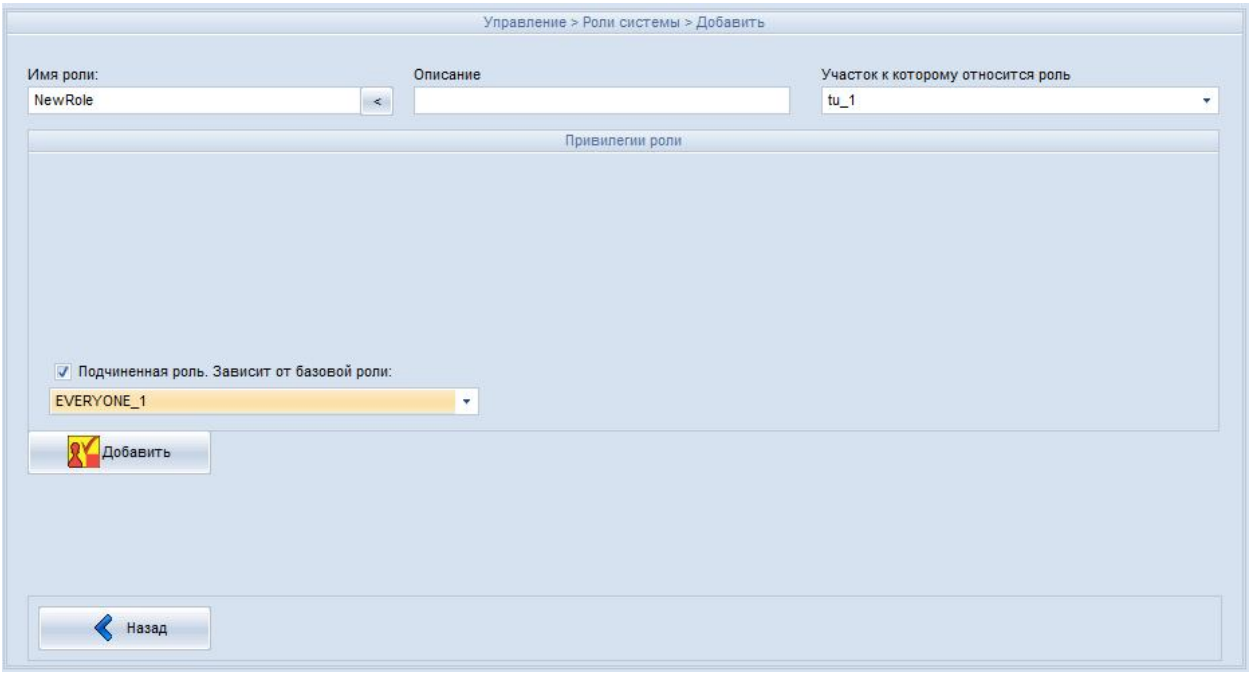

Рисунок 2 - Добавление роли

При создании роли по шаблону необходимо в окне добавления роли, приведённом на рисунке 4, левой кнопкой мыши выбрать раскрывающийся список в поле «Имя роли». Появится окно, приведённое на рисунке 3, в котором необходимо выбрать роль и нажать кнопку <Ok>.

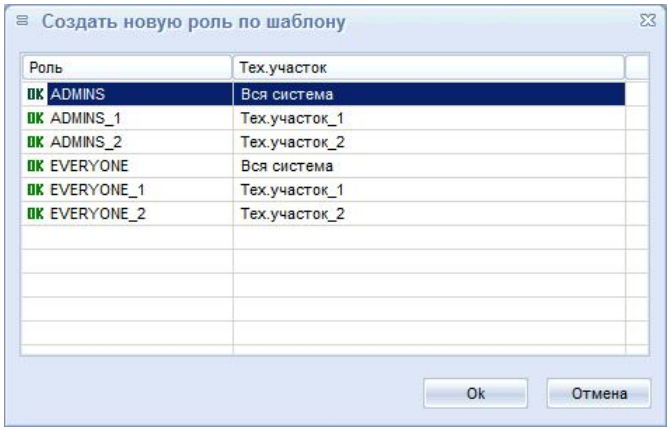

Рисунок 3 - Создание роли по шаблону

При редактировании базовой роли выводится окно, приведённое на рисунке 4. Изменяются синхронизируемые параметры зависящих от базовой подчинённых ролей. Список подчинённых ролей базовой роли выводится в области «Подчиненные роли» окна, приведённого на рисунке 4. Индикатор в виде лампочки слева от имени роли указывает, что данная подчинённая роль по одной или нескольким группам параметров рассинхронизирована с базовой ролью.

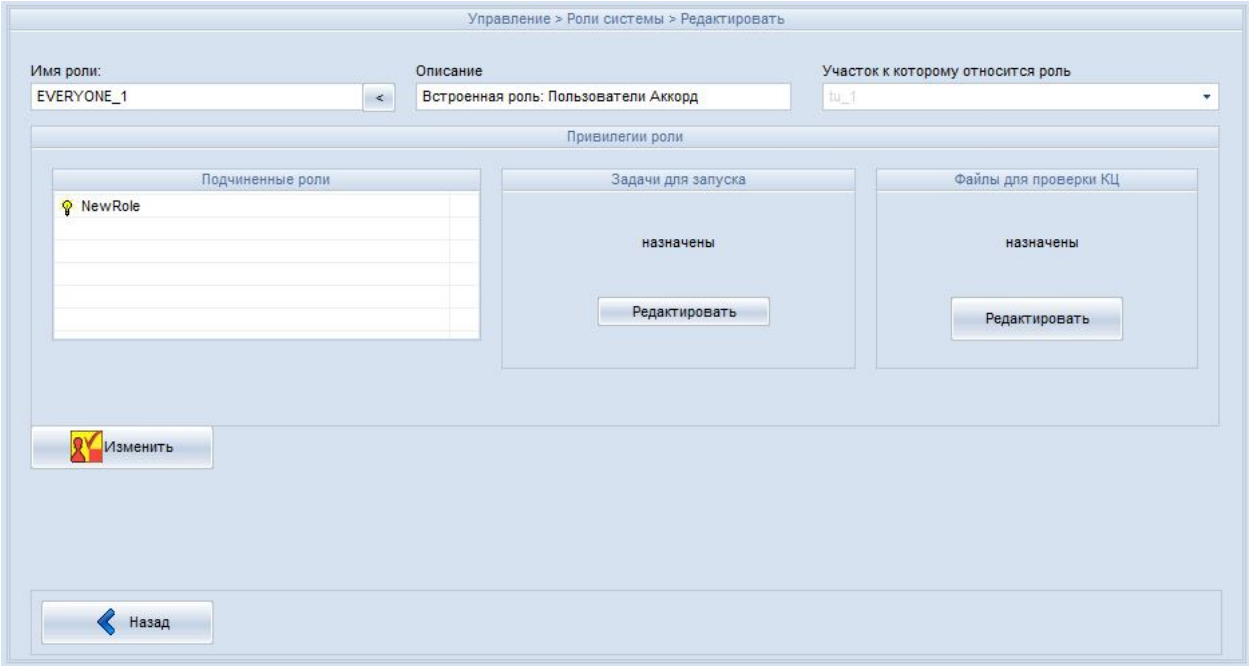

Рисунок 4 - Редактирование базовой роли

Если дважды щёлкнуть мышью по имени роли в списке подчинённых ролей, то будет выведено окно синхронизации, приведённое на рисунке 5.

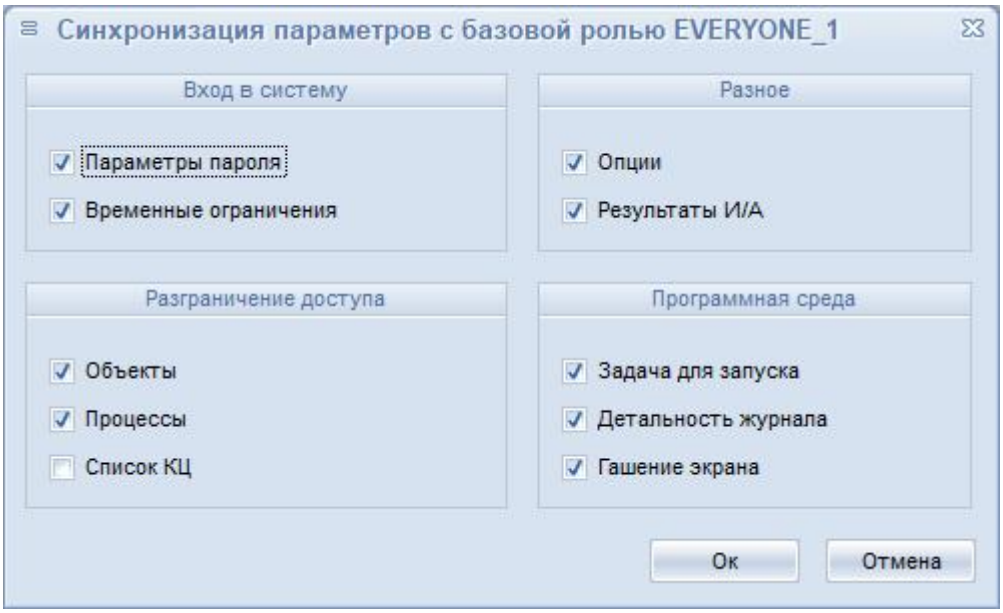

Рисунок 5 - Синхронизация групп параметров

Данное окно позволяет просмотреть и задать группы параметров настройки синхронизации подчинённой и базовой ролей.

Отсутствие флажка у какой-либо группы означает, что значения одного или нескольких параметров подчинённой роли, входящих в данную группу, отличаются от значений аналогичных параметров базовой роли. При редактировании дан-

ной группы параметров у базовой роли аналогичные параметры подчинённой роли изменены не будут.

Наличие флажка у какой-либо группы означает, что значения параметров подчинённой роли, входящих в данную группу, совпадают со значениями аналогичных параметров базовой роли. При редактировании данной группы параметров базовой роли будут изменены аналогичные параметры у подчинённой роли.

Если установить отсутствующий флажок и нажать <Ok>, то параметры данной группы подчинённой и базовой роли будут синхронизированы.

Если выделить роль в списке подчинённых ролей и нажать на клавиатуре клавишу «Delete», то выбранная роль перестанет быть подчинённой, станет базовой и исчезнет из списка.

При редактировании подчинённой роли выводится окно, приведённое на рисунке 6.

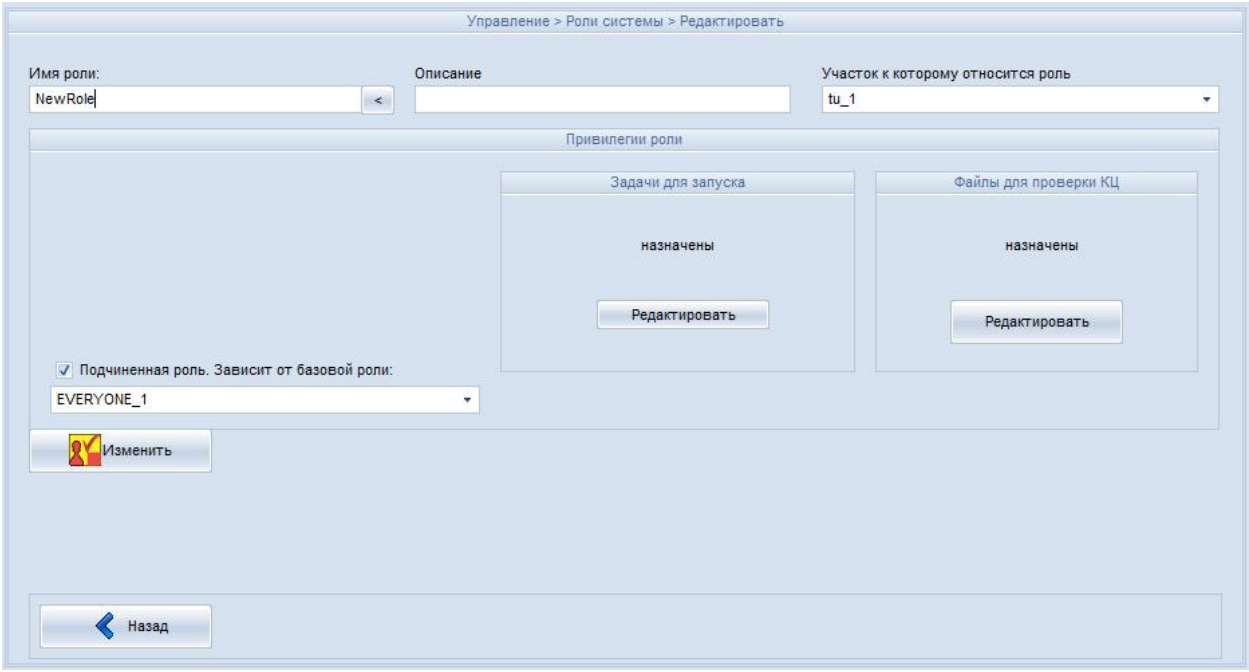

Рисунок 6 - Редактирование подчинённой роли

Если снять флажок «Подчинённая роль. Зависит от базовой роли», то роль перестанет быть подчинённой и станет базовой.

Допускается индивидуальное редактирование подчинённых ролей. При этом подчинённая роль по редактируемым параметрам рассинхронизируется с базовой ролью. В этом случае во вкладке редактирования ролей появляется кнопка <Синхронизировать> и индикатор в виде лампочки, как показано на рисунке 7.

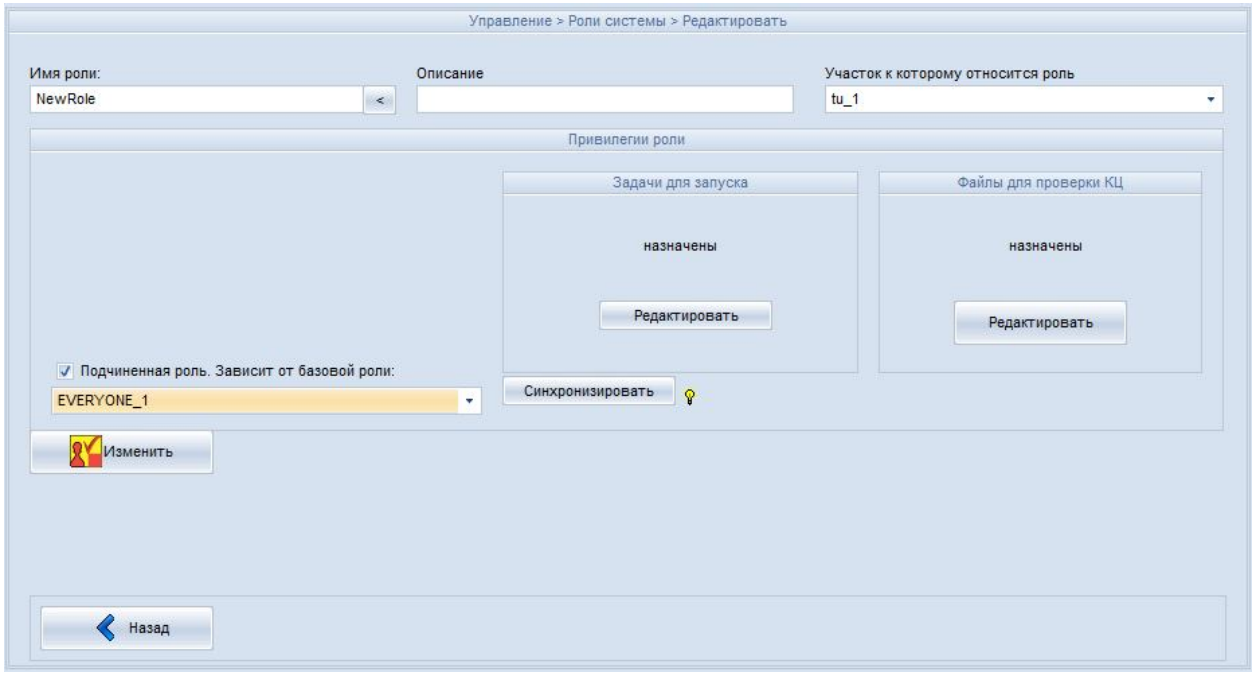

Рисунок 7 - Редактирование подчинённой роли. Рассинхронизация

При нажатии кнопки <Синхронизация> выводится окно, приведённое на рисунке 5.

Все встроенные роли СЦУ (Admins_NSHR, Admins_SCM, Admins, Admins_XXX, Everyone, Everyone_XXX, AIBs_SCM, AIB_TU: имя роли, OIBs_SCM и AUDITORs_SCM) являются базовыми.

Чтобы задать или редактировать задачи для запуска роли, необходимо нажать кнопку <Редактировать> в области «Задачи для запуска». После этого появится окно, приведённое на рисунке 8, в котором следует задать необходимые задачи для запуска и нажать кнопку <Сохранить> (длина строки окна редактирования списка задач составляет 120 символов).

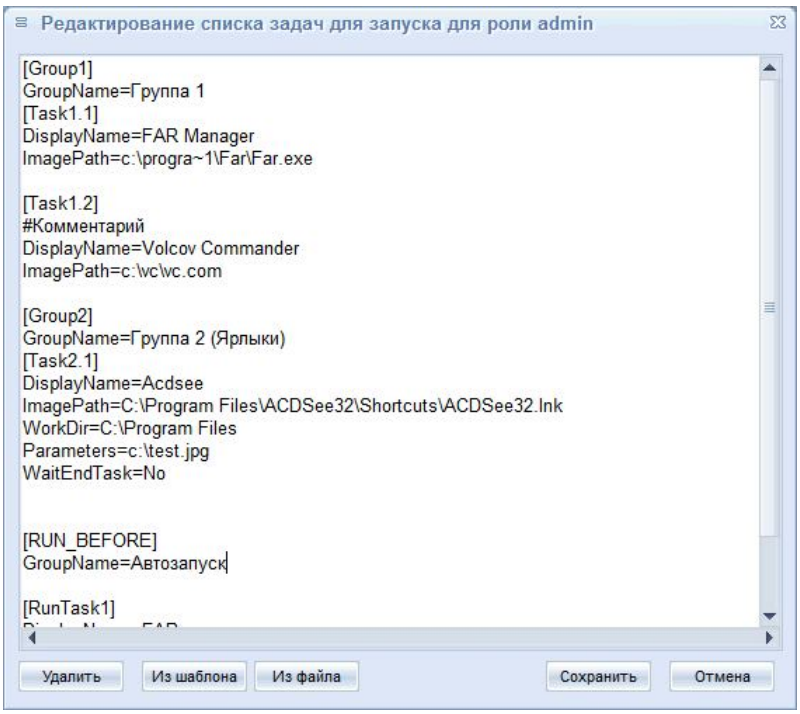

Рисунок 8 – Редактирование списка задач для запуска

При создании списка задач для запуска по шаблону необходимо в окне, приведённом на рисунке 8, нажать кнопку <Из шаблона>. Появится окно, приведённое на рисунке 9.

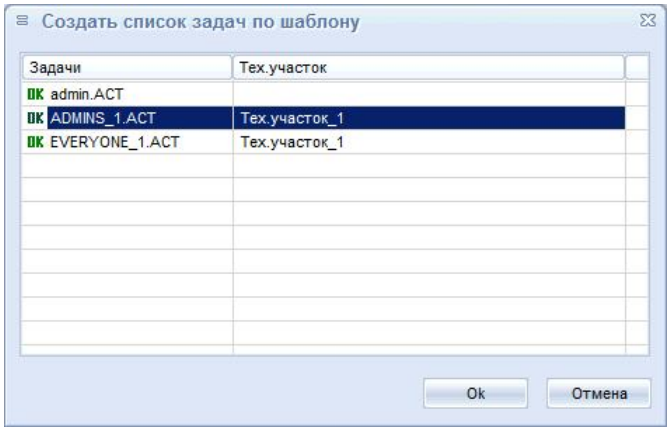

Рисунок 9 – Создание списка задач по шаблону

Нужно выбрать необходимый шаблон с именем роли, задачи которой планируется назначить редактируемой роли, и нажать кнопку <Ok>.

При создании списка задач для запуска из файла нажать кнопку <Из файла>. После выполнения описанной процедуры появляется окно выбора файла. В этом окне выбрать нужный файл и нажать кнопку <Открыть>.

После внесения изменений нажать кнопку <Сохранить> (рисунок 8), для отмены операции – кнопку <Отмена> (рисунок 8).

РАУ позволяет осуществлять контроль целостности файлов и системного реестра на ПКО. Для ПКО под управлением ОС Windows список контролируемых файлов может формироваться как локально – на самом ПКО, так и удалённо – на СЦУ, для ПКО под управлением ОС Linux список формируется только локально, посредством СЦУ происходит только его перерасчёт. Информация о контроле целостности файлов на ПКО под управлением ОС Linux приведена в разделе 4.4.

При удалённом формировании списка контролируемых файлов на ПКО под управлением ОС Windows необходимо выполнить следующие действия:

- создание на СЦУ задания для контроля целостности и передача его на ПКО;
- расчёт на ПКО эталонных контрольных сумм по полученному заданию и передача их на СЦУ;
- формирование на СЦУ базы с новым списком контролируемых файлов и передача её на ПКО.

Для создания или редактирования задания для контроля целостности нужно нажать кнопку <Редактировать> в области «Файлы для проверки КЦ» вкладки «Управление > Роли системы > Редактировать», приведённой на рисунках 4 и 6.

Появится окно, примерный вид которого приведён на рисунке 10.

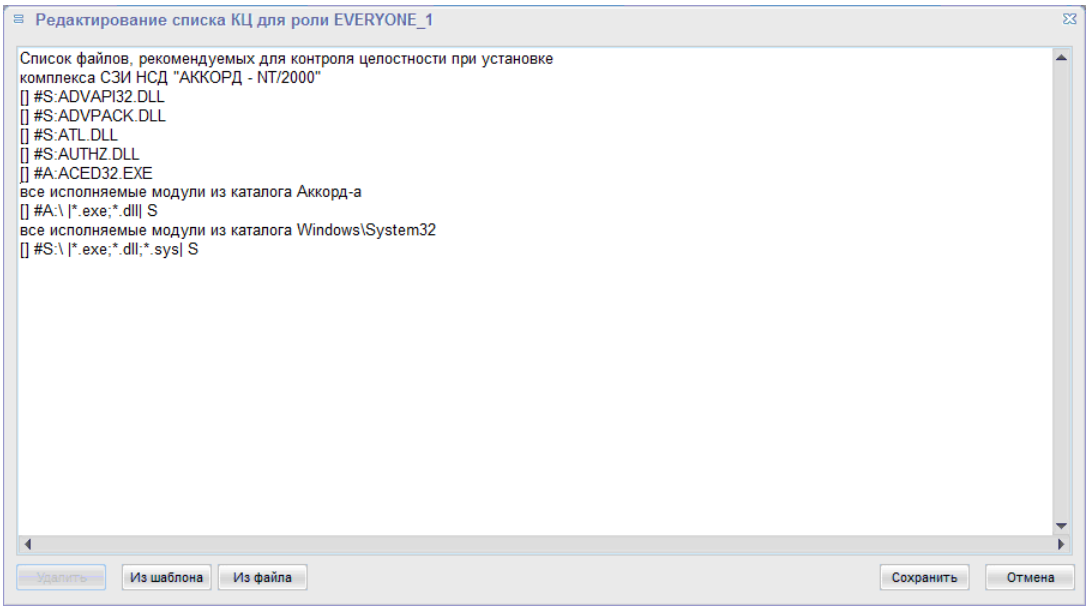

Рисунок 10 - Редактирование списка контролируемых файлов

В данном окне указываются файлы, целостность которых нужно контролировать. При этом следует соблюдать следующие правила.

1 В одной строке допускается указывать только одно имя файла или папки.

2 Каждая строка, задающая файлы, целостность которых нужно контролировать, должна начинаться с пустых квадратных скобок []. В противном случае строка рассматривается как комментарий.

3 После пустых квадратных скобок должен следовать пробел.

4 После пробела должно следовать полное (с путём) имя файла либо полное имя папки.

5 Полное имя папки должно заканчиваться символом «\».

6 При задании полных имён папок и файлов допускается использовать следующие сокращения:

- #W: – папка Windows на системном диске;
- #S: – папка Windows\System32 на системном диске;
- #D: – папка Windows\System32\Drivers на системном диске;
- #P: – папка Program Files на системном диске;
- #A: – папка установки ПАК СЗИ от НСД «Аккорд-Win32/64».

7 После полного имени папки через пробел необходимо указать фильтр, определяющей правила выбора файлов, целостность которых нужно контролировать. Фильтр должен представлять собой одну или несколько разделённых точкой с запятой (;) символьных масок (шаблонов), заключённых между вертикальными линиями «|».

8 В символьных масках допускается использование следующих символов подстановки:

* – для замены любой строки символов;

? – для замены одиночного символа.

9 Если после фильтра через пробел указать символ «S», то выбор файлов, целостность которых нужно контролировать, будет выполняться и во всех дочерних каталогах данной папки. Если не указывать, то только в указанной папке.

10 Если все буквы в имени файла приведены в верхнем регистре (заглавные), то контроль целостности данного файла будет осуществляться в статическом режиме. В противном случае целостность данного файла будет контролироваться в динамическом режиме. Информация о статическом и динамическом режимах контроля файлов приведена в документах 11443195.4012-036 97 «ПАК Аккорд-Win32 (версия 4.0). Установка правил разграничения доступа. Программа

ACED32» и 11443195.4012-036 97 «ПАК Аккорд-Win64 (версия 5.0). Установка правил разграничения доступа. Программа ACED32».

11 Каждая строка, задающая исключения из списка файлов, целостность которых нужно контролировать, должна начинаться с символа «-» за которым должна следовать строка, удовлетворяющая правилам 1 - 10.

Примеры строк, задающих файлы, целостность которых нужно контролировать, приведены в таблице 1.

Таблица 1 - Примеры строк, задающих файлы, целостность которых нужно контролировать

Строка	Описание
[] c:\ |*.*| S	Выбор всех файлов на диске c:
[] #A:\ |*.*| S	Выбор всех файлов в папке c:\Accord.NT\ (c:\Accord.x64\)
[] #A:Identifiers\ |*.dll| S	Выбор всех библиотек dll в папке c:\Accord.NT\Identifiers\ (c:\Accord.x64\ Identifiers\) и всех дочерних папках
[] #S:\ |a*.exe; file?.dll; *.lo?| S	Выбор исполняемых файлов, имя которых начинается на букву «a», библиотек dll, имя которых состоит из пяти символов, начинается на «file» и заканчивается произвольным символом, например, file1.dll, file5.dll и files.dll, и файлов, расширение которых состоит из трёх символов и начинается с букв «lo», например, 20160826155445.low и Aced32.log, в папке Windows\System32 и всех дочерних папках
[] C:\FOLDER\ |*.exe;*.dll|	Выбор всех исполняемых файлов и библиотек dll в папке C:\FOLDER\. Файлы в дочерних паках не выбираются
[] #S:ATL.DLL	Выбор файла «ATL.DLL» в папке Windows\System32
[] c:\Accord.x64\Aced32.exe	Выбор файла «Aced32.exe» в папке c:\Accord.x64\
-[] c:\Accord.x64\Aced32.exe	Исключение файла «Aced32.exe» из папки c:\Accord.x64\

Строка	Описание
-[] #S:\ |a*.exe; file?.dll; *.lo?| S	Исключение исполняемых файлов, имя которых начинается на букву «a», библиотек dll, имя которых состоит из пяти символов, начинается на «file» и заканчивается произвольным символом и файлов, расширение которых состоит из трёх символов и начинается с букв «lo» из папки Windows\System32 и всех дочерних папок

При необходимости установить на контроль целостности системный реестр надо добавить в список файлов следующую строку:

[] HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\ACRUNNT:>IMAGEPATH

Существует возможность создавать задания для контроля целостности на основе файла и на основе шаблона. Данные процедуры описаны в документах 11443195.4012-036 97 «ПАК Аккорд-Win32 (версия 4.0). Установка правил разграничения доступа. Программа ACED32» и 11443195.4012-036 97 «ПАК Аккорд-Win64 (версия 5.0). Установка правил разграничения доступа. Программа ACED32».

При нажатии в окне, приведённом на рисунке 10, кнопки <Сохранить> появится сообщение, приведённое на рисунке 11.

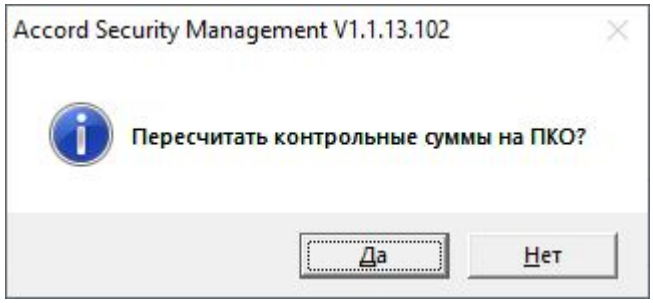

Рисунок 11 - Запрос пересчёта эталонных контрольных сумм

Для передачи задания для контроля целостности на подконтрольные объекты нажать кнопку <Да>. После этого будет выведено окно, содержащее список ПКО, на которых существует роль, в рамках редактирования которой создаётся данное задание для контроля целостности. Пример такого окна приведён на рисунке 12.

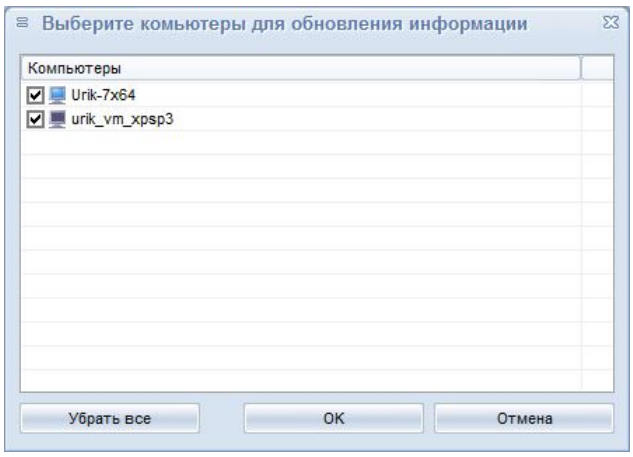

Рисунок 12 - Выбор ПКО для передачи задания для контроля целостности

После выбора нужных ПКО и нажатия <OK> на СЦУ будут созданы текстовые файлы с именем …\Asm\AcConNet\Out\CompName\RoleName.HSH_TASK, где:

- … – каталог установки СЦУ;
- CompName – имя компьютера (ПКО), выбранного для передачи задания для контроля целостности;
- RoleName – роль, в рамках редактирования которой создаётся данное задание для контроля целостности.

Созданные файлы содержат задания для контроля целостности. Данные файлы СЦУ передаёт на выбранные ПКО.

Примечание. Файл с заданием для контроля целостности для всех подчинённых ролей будет создан и отправлен на СЦУ при создании или изменении задания для контроля целостности базовой роли либо при установке для подчинённой роли флажка «Список КЦ» в окне синхронизации групп параметров, приведённом на рисунке 5.

Получив файл с заданием для контроля целостности, ПО ПКО выполняет расчёт эталонных контрольных сумм. Расчёт выполняется незаметно для пользователя ПКО. Если во время расчёта произойдёт перезагрузка ПКО или его выключение, то после загрузки расчёт будет продолжен.

После завершения расчёта файл с эталонными контрольными суммами будет передан на СЦУ. Файл соответствует заданию для контроля целостности и имеет следующие отличия. Квадратные скобки здесь не пустые, а содержат значение эталонной контрольной суммы, вычисленной на данном ПКО для указанного файла, например, [091E05CC5357E5A0FABAA8579894947342]. Вместо сокращений и символьных масок здесь присутствуют полные имена файлов. Строки задания для контроля целостности, содержащие символьные маски, заменяются

несколькими строками, по количеству выбранных по данной маске файлов. Строки дополнены атрибутами файлов.

Если файла, указанного в задании для контроля целостности, не окажется на ПКО, то вместо эталонной контрольной суммы квадратные скобки будут содержать запись «NOT FOUND». В дальнейшем данный файл не будет включён в базу со списком контролируемых файлов Accord.Amz.

При получении файл с эталонными контрольными суммами сохраняется на СЦУ с именем …\Asm\AcConNet\In\CompName\RoleName.CRC, где:

- … – каталог установки СЦУ;
- CompName – имя компьютера (ПКО), от которого получен файл;
- RoleName – роль, в рамках редактирования которой формируется список контроля целостности файлов.

После получения файла становится возможным формирование и передача на ПКО базы с новым списком контролируемых файлов Accord.Amz. Для передачи базы на ПКО необходимо во вкладке «Компьютеры системы» выбрать нужный ПКО и нажать кнопку <Передача баз>.

Если операция формирования списка контролируемых файлов прошла успешно, то в столбце «ПКО» вкладок «Компьютеры системы», «Роли системы» и «Учётные записи» будет находиться литера «К».

Примечание. Для отображения во вкладках столбца «ПКО» следует нажать кнопку <Настройка отображения информации> и в появившемся окне установить флаг «Настроен контроль целостности (К)».

Если при формировании списка контролируемых файлов возникли ошибки, то база сформирована не будет. При попытке передачи баз будет выведено сообщение об ошибке.

Примечания:

1 Для обеспечения возможности передачи баз на ПКО до разрешения ошибок, возникающих при формировании списка контролируемых файлов, следует в настройках СЦУ установить флаг «Не передавать базы, если нет актуального списка КЦ» (по умолчанию он снят). В этом случае при формировании и передаче баз процесс сборки остановлен не будет, список файлов для контроля целостности и их эталонные контрольные суммы будут взяты из файла …\Asm\AcConNet\In\CompName\CompName.amz, а в журнал ASM запишется предупреждающая информация.

2 Если СЦУ функционирует в режиме «Классический РАУ», то контроль целостности файлов ПКО осуществляется согласно процедуре, описанной в подразделе 4.4.

Вся информация об ошибках сохраняется в журнале ASM.

В случае возникновения ошибок при формировании списка контролируемых файлов во вкладках «Компьютеры системы», «Роли системы» и «Учётные записи» ПКО, на которых не удалось сформировать список контролируемых файлов, роли и учётные записи для которых не удалось сформировать список контролируемых файлов, маркируются восклицательным знаком красного цвета.

Если нажать кнопку <Изменить> в окне, приведённом на рисунке 6 или рисунке 7, то будет выведено окно редактора прав доступа ACED32, приведённое на рисунке 13. С помощью данного редактора можно изменять параметры роли, включая установку уровня доступа пользователя при использовании на ПКО механизма мандатного разграничения доступа, а также осуществить предварительный просмотр базы пользователей (без возможности модификации и сохранения), полученной от подконтрольного объекта. Для этого нужно выбрать команду Файл -> Импорт базы, после выполнения которой загрузится файл базы пользователей ПКО (при выходе из редактора изменения в базе не сохраняются).

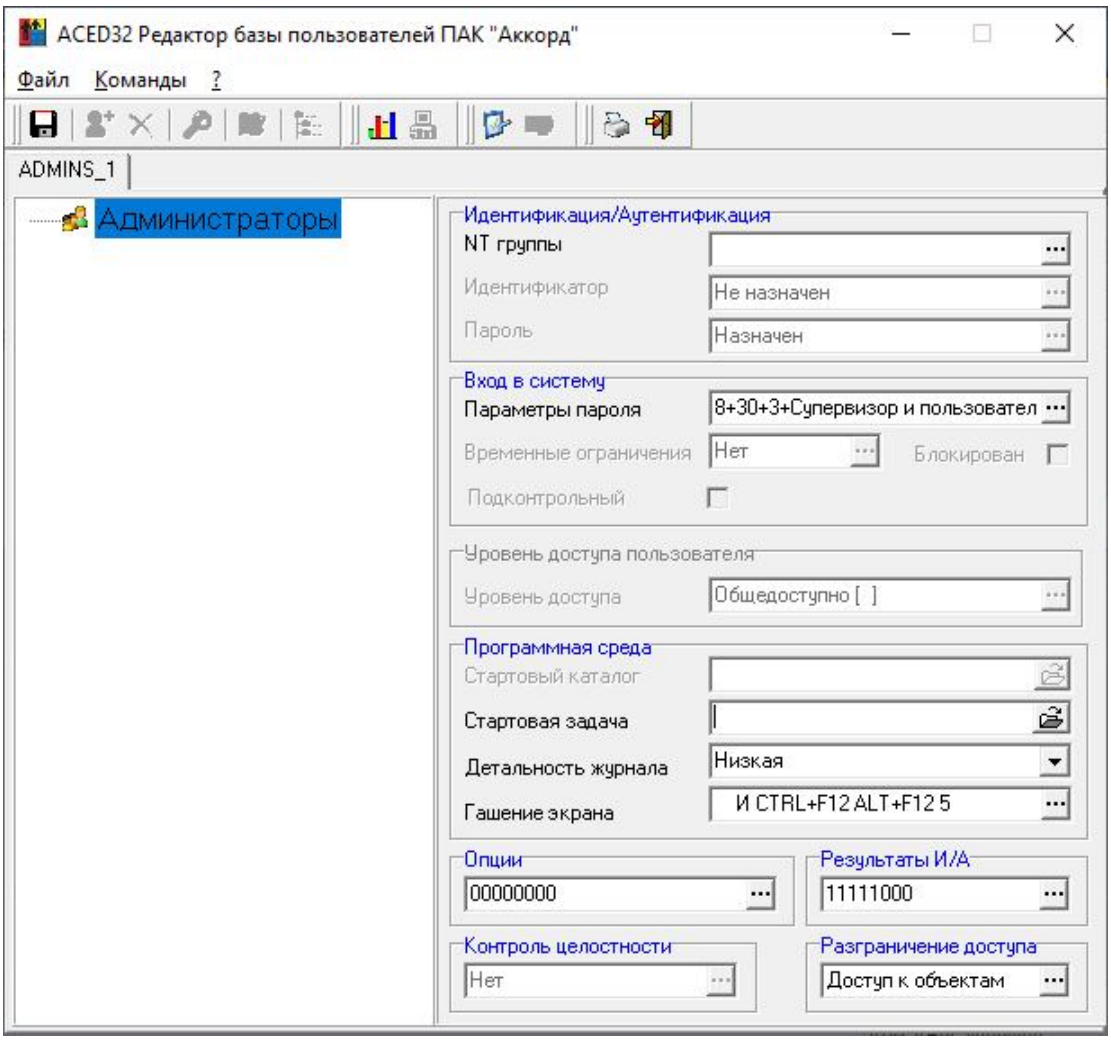

Рисунок 13 – Редактирование базы пользователей «Аккорд»

Чтобы установить доступ к коммутационным портам и периферийным устройствам, необходимо левой кнопкой мыши выбрать раскрывающийся список в поле «Разграничение доступа». Далее на экране появляется окно редактирования списка объектов, в котором можно выбрать необходимый объект и определить для него права доступа.

На рисунке 14 показан список объектов (устройства, файловая система, реестр), для которых могут быть заданы правила разграничения доступа. О задании правил разграничения доступа подробно описано в документах 11443195.4012-036 97 «ПАК Аккорд-Win32 (версия 4.0). Установка правил разграничения доступа. Программа ACED32» и 11443195.4012-036 97 «ПАК Аккорд-Win64 (версия 5.0). Установка правил разграничения доступа. Программа ACED32».

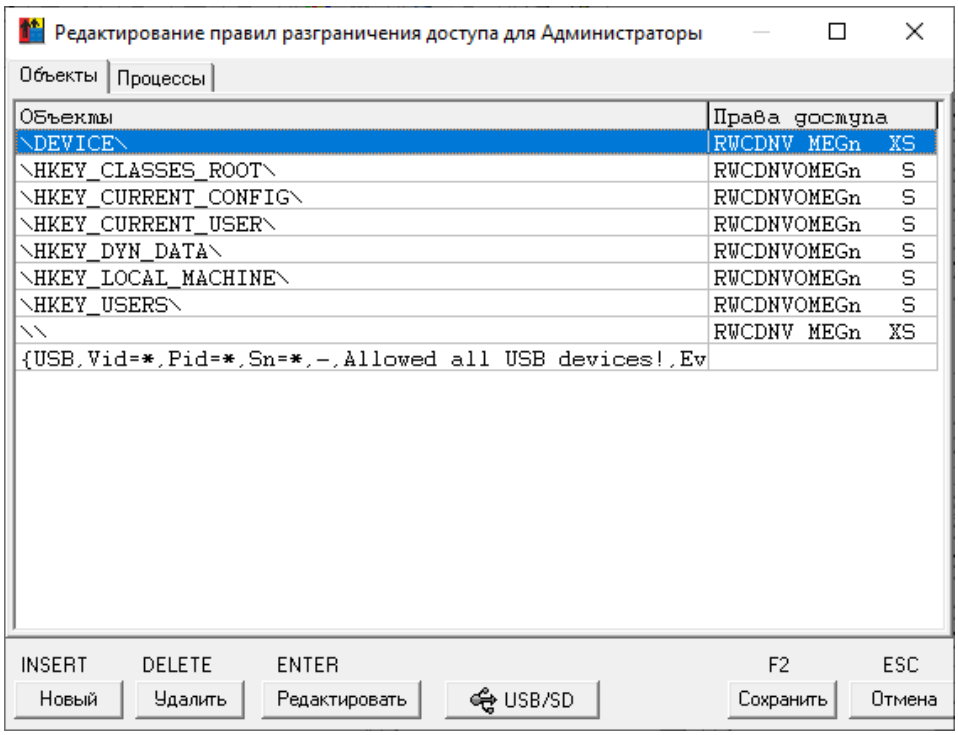

Рисунок 14 – Перечень объектов для установки прав доступа

Уровень детальности журнала ПАК «Аккорд» на ПКО должен быть установлен в значение не ниже уровня «Низкий», как показано на рисунке 13.

ВНИМАНИЕ! Если роль назначена некоторому технологическому участку, её могут редактировать только Администраторы ИБ технологических участков!

Для удаления роли необходимо во вкладке «Управление > Роли», приведённой на рисунке 1, выбрать роль и нажать кнопку <Удалить>. Появится сообщение о подтверждении действия, приведённое на рисунке 15.

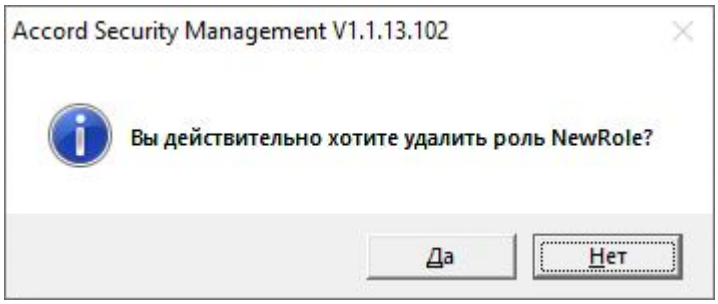

Рисунок 15 – Удаление роли

В РАУ предусмотрена возможность автоматического редактирования параметров учётной записи пользователя системы (п. 4.5) при выполнении процедуры удаления роли, назначенной данной учётной записи. При этом содержимое поля «Роль:» для текущей учётной записи аннулируется.

Следует помнить, что пользователь Системы, которому принадлежит учётная запись с аннулированным параметром «Роль:», не сможет получить доступ к консоли AsmT.exe.

Для отображения в списке ролей вкладки «Управление > Роли системы», приведённой на рисунке 1, информации о наличии списков файлов контроля целостности, списков задач и стартовых задачах следует нажать кнопку <Настройка отображения информации>. Появляется окно, приведённое на рисунке 16, в котором устанавливаются флаги напротив той информации о настройках ПКО, которую следует отобразить.

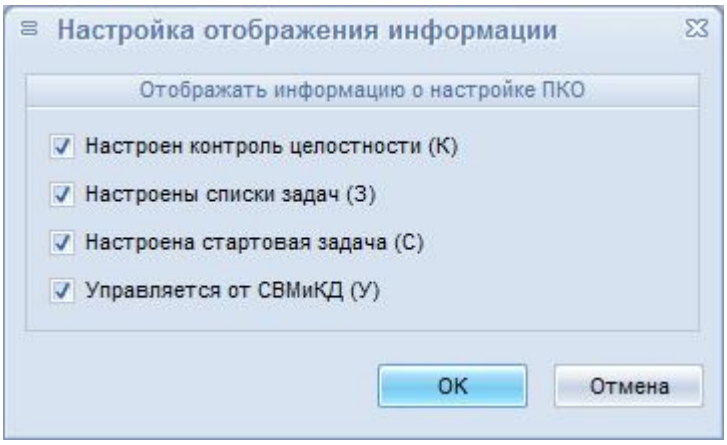

Рисунок 16 – Настройка отображения информации о ПКО

После добавления отображаемой информации в таблице ролей появляется столбец с названием «ПКО» (рисунок 17). Наличие литеры «К» в данном столбце означает, что для данной роли определен список файлов для контроля целостности, наличие литеры «З» – определен список задач, литеры «С» – определен список стартовых задач, литеры «У» – данный компьютер управляется от СВМиКД.

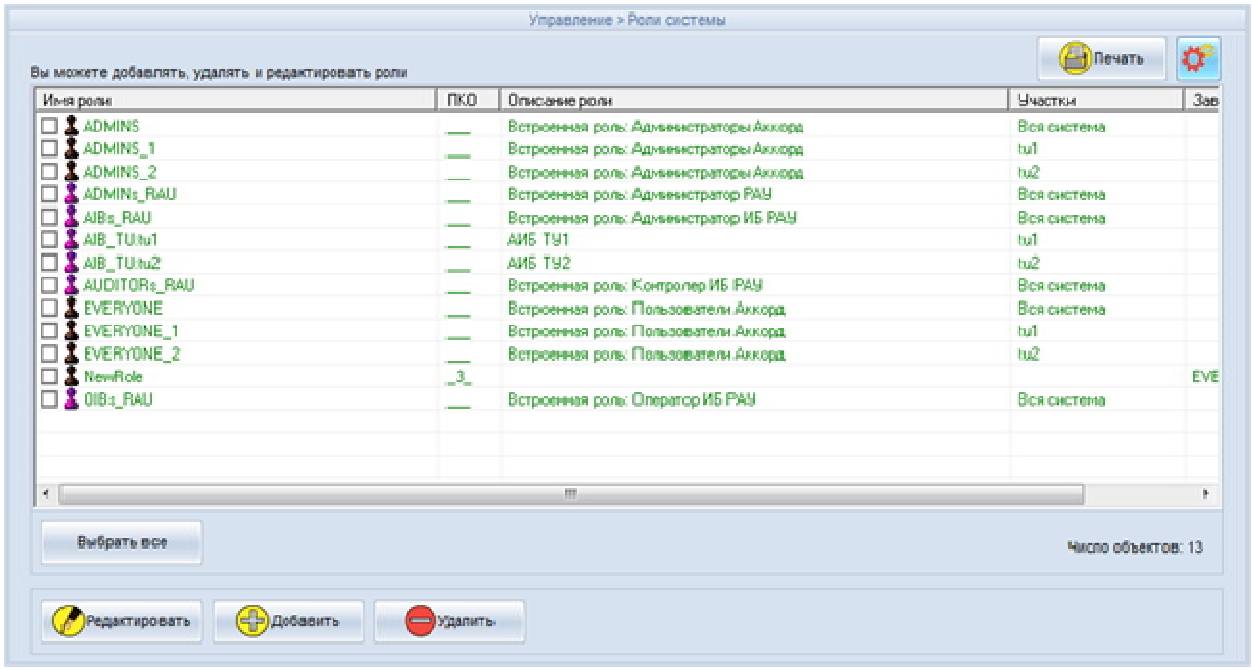

Рисунок 17 – Роли системы. Отображение информации о ПКО

4.3 Вкладка «Идентификаторы»

Вкладка «Управление > Идентификаторы» позволяет осуществлять добавление, удаление и импорт идентификаторов, используемых на ПКО, в базу СЦУ. Вкладка приведена на рисунке 18.

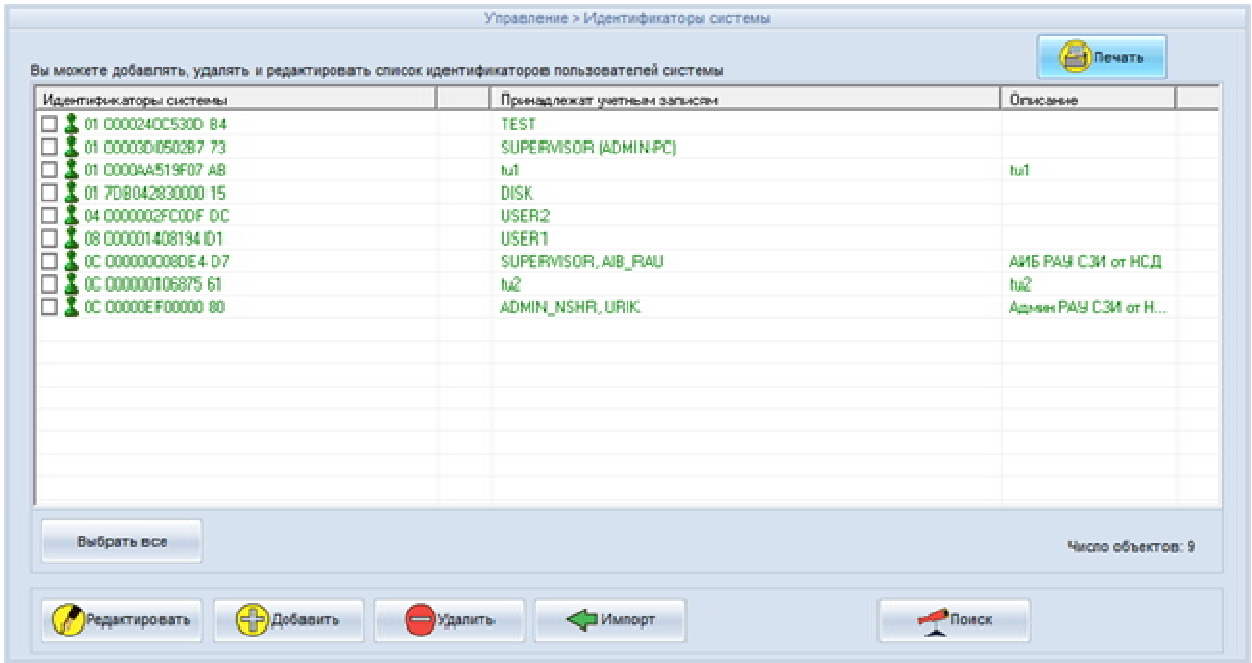

Рисунок 18 – Идентификаторы системы

Кнопка <Печать> позволяет распечатать выбранную информацию на принтере, а также сохранить в файл (с указанным разделителем). При ее нажатии по-

является окно, приведённое на рисунке 19, в котором следует выбрать способ печати: в файл или на принтер, тип выводимой информации (серийный номер идентификатора, принадлежность учетным записям и описание); при печати в файл следует также указать разделитель.

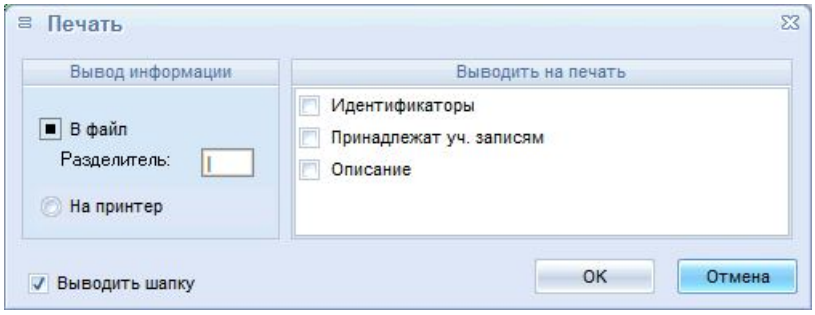

Рисунок 19 – Печать информации об идентификаторе

При добавлении или изменении идентификатора надо выбрать опцию «уже записан» или «сгенерировать» – в последнем случае в идентификаторе генерируется новый секретный ключ взамен старого. Далее необходимо нажать кнопку <Прочитать> и предъявить идентификатор (рисунок 20). Для добавления идентификатора в базу нажать кнопку <Добавить>.

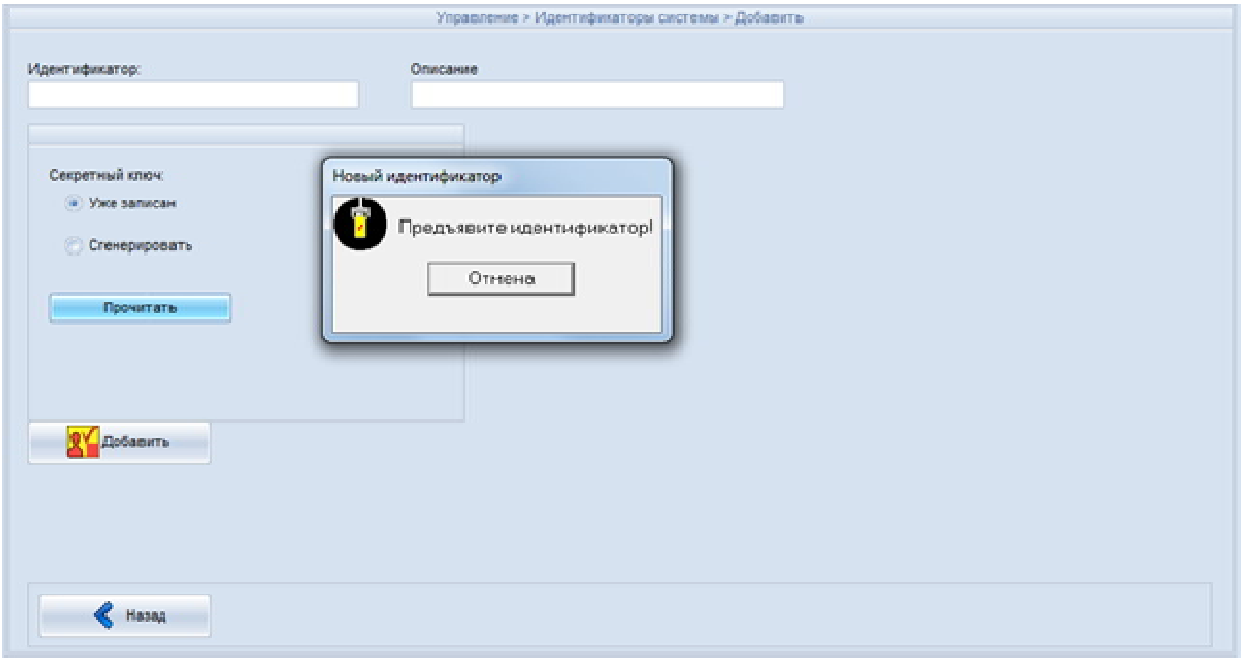

Рисунок 20 – Требование предъявить идентификатор

Для удаления идентификатора следует во вкладке «Идентификаторы» (рисунок 18) выбрать нужный идентификатор и нажать кнопку <Удалить>. При ее нажатии появляется окно подтверждения действия, приведённое на рисунке 21.

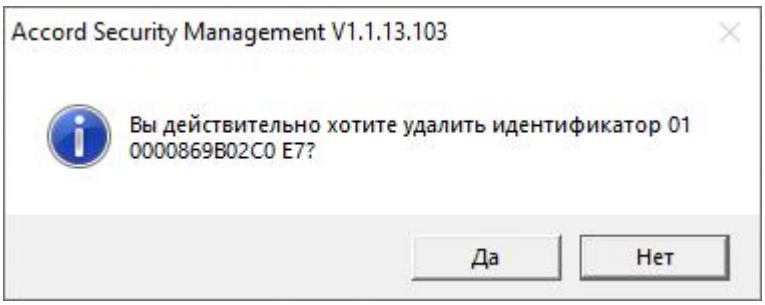

Рисунок 21 – Удаление идентификатора

Идентификаторы можно импортировать из базы СЗИ от НСД «Аккорд» (например C:\Accord.NT\ACCORD.AMZ). Для этого во вкладке «Идентификаторы» (рисунок 18) необходимо нажать кнопку <Импорт>. Появляется окно (рисунок 22), в котором нужно нажать кнопку <Импортировать>.

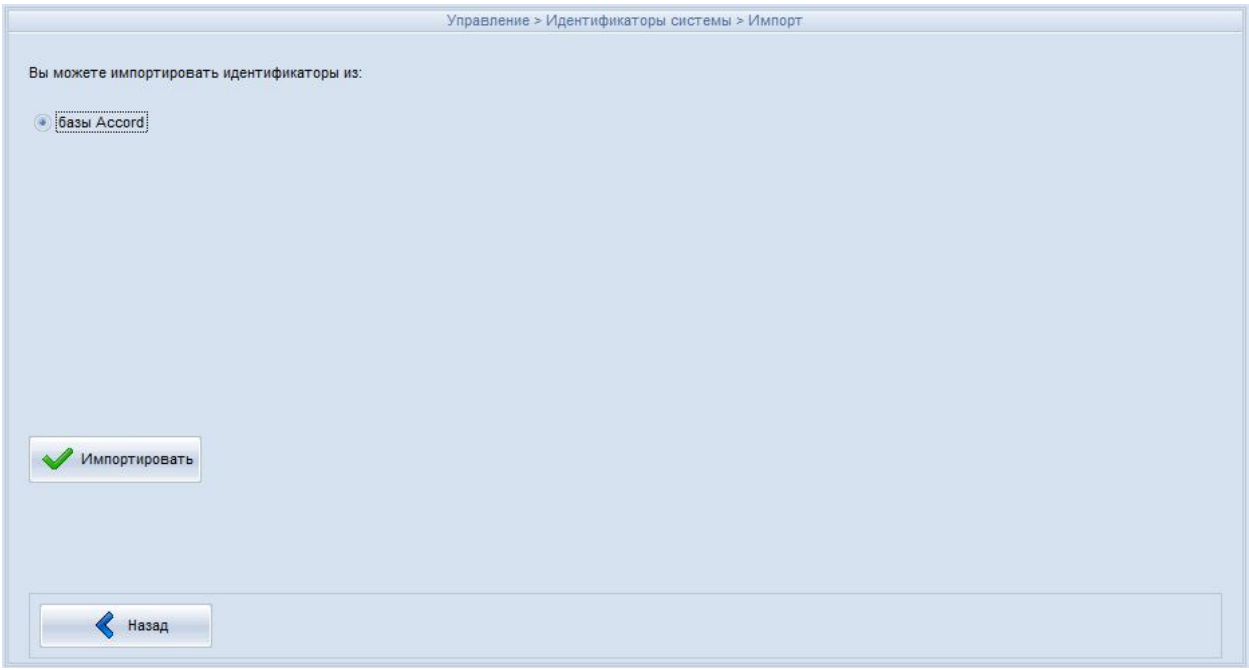

Рисунок 22 – Импорт идентификатора

При нажатии кнопки <Импортировать> (рисунок 22) появляется окно выбора каталога (рисунок 23), в котором следует выбрать необходимый файл.

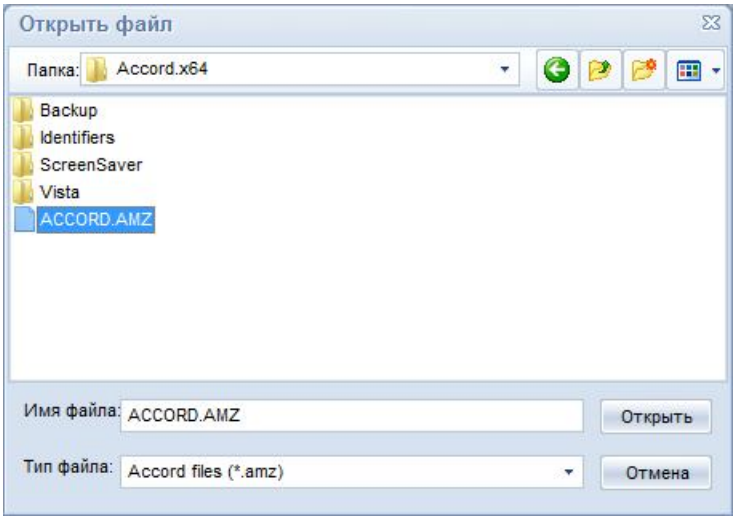

Рисунок 23 – Окно выбора каталога

После этого в правой части окна появятся импортированные идентификаторы, из которых следует выбрать необходимые для добавления в базу (для выбора всех идентификаторов нужно нажать кнопку <Выбрать все>) и нажать кнопку <Добавить> (рисунок 24).

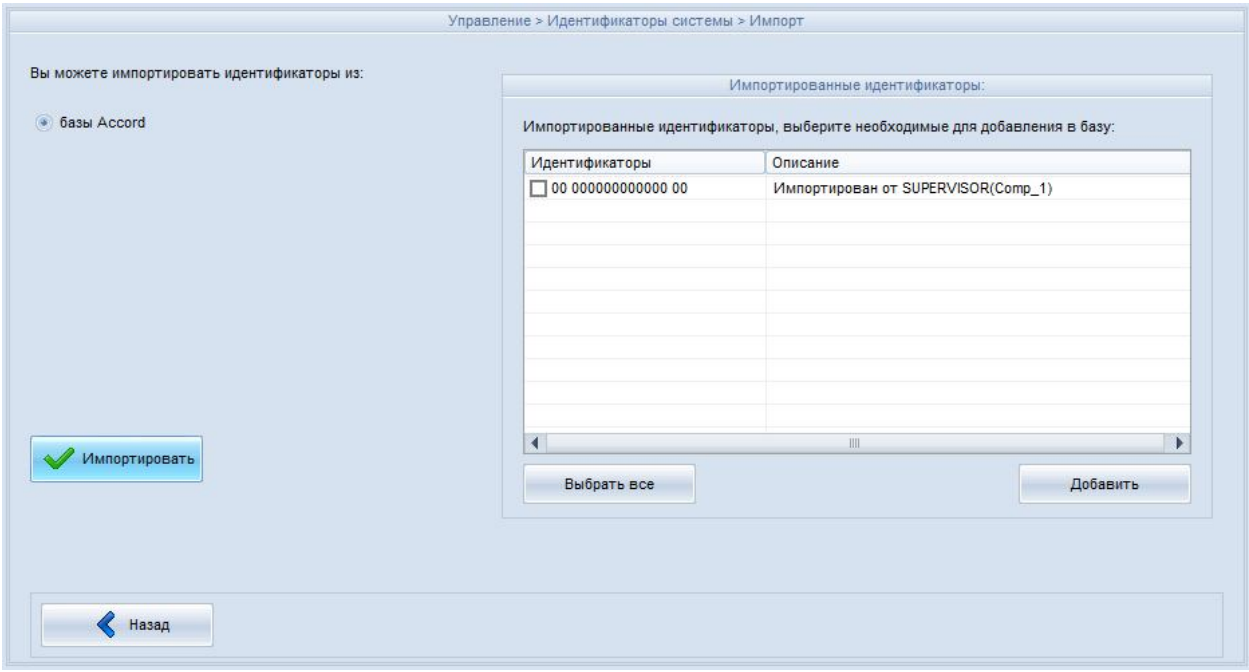

Рисунок 24 - Выбор импортированных идентификаторов (импорт из базы «Аккорда»)

Если необходимо определить, помещён ли данный идентификатор в базу СЦУ, следует нажать кнопку <Поиск> на вкладке «Идентификаторы» (рисунок 18), при этом появится окно с сообщением «Предъявите идентификатор» (рисунок 25).

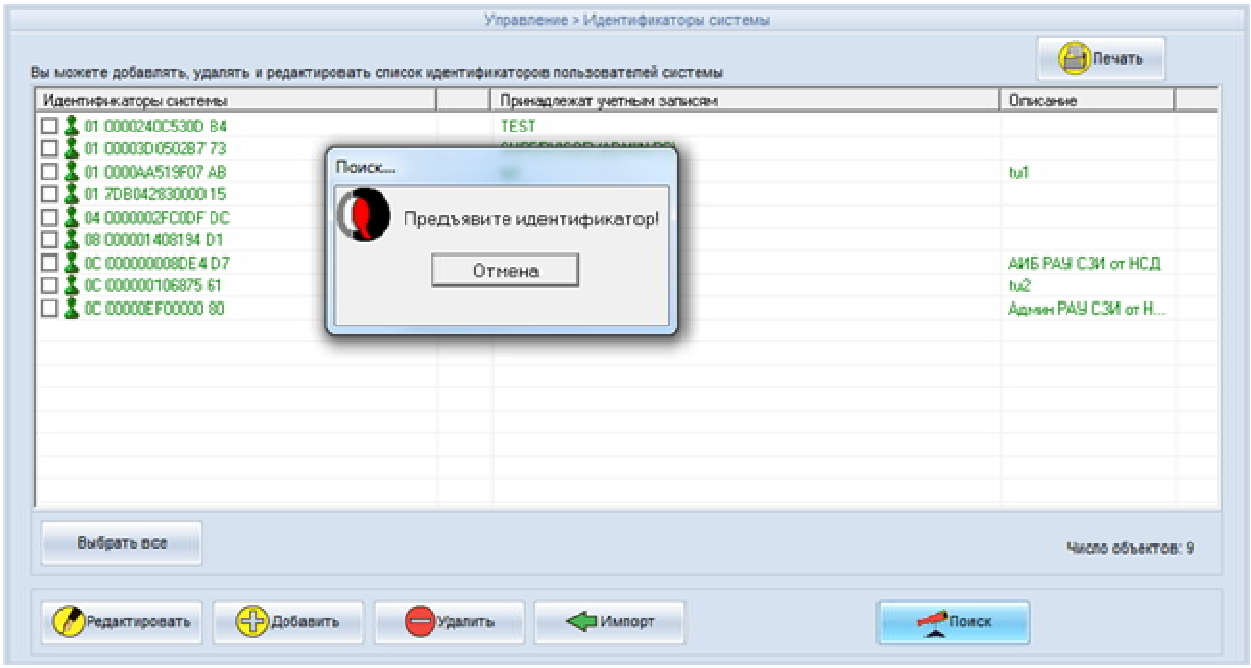

Рисунок 25 - Сообщение «Предъявите идентификатор»

Необходимо приложить идентификатор к считывателю. Если данный идентификатор есть в базе СЦУ, соответствующая запись будет выделена, как показано на рисунке 26.

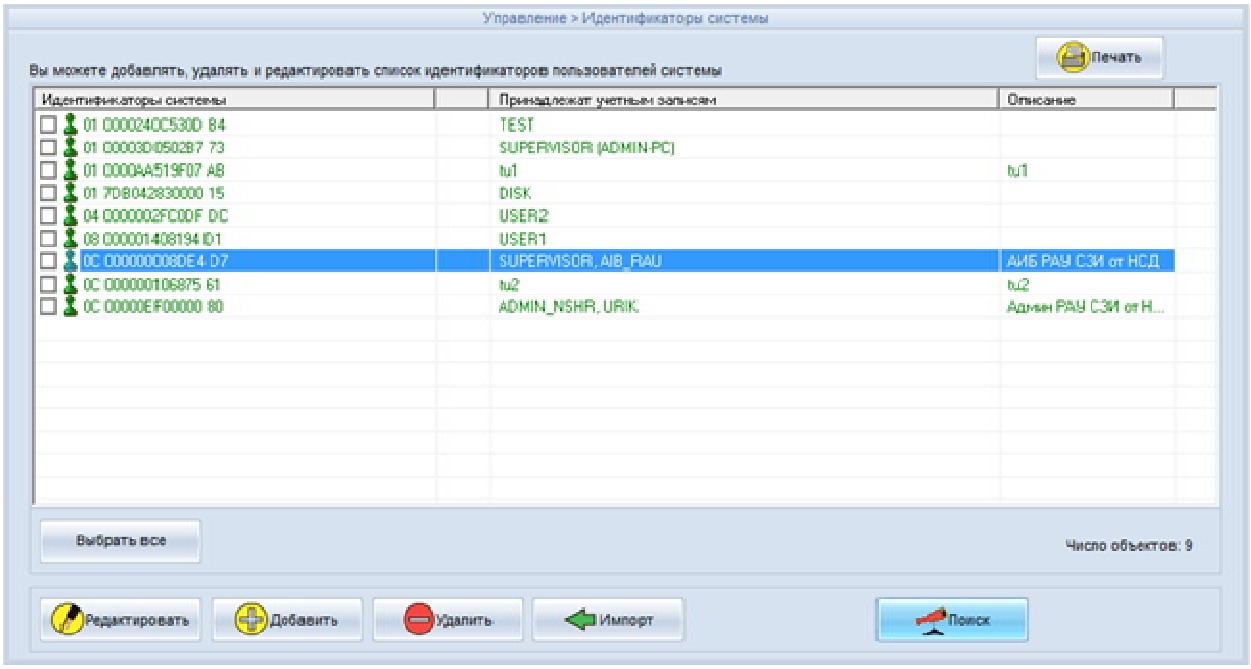

Рисунок 26 - Найдена учетная запись, которой назначен идентификатор

Если идентификатор отсутствует в базе СЦУ, в нижней части окна появится сообщение «Идентификатор не зарегистрирован!», как показано на рисунке 27.

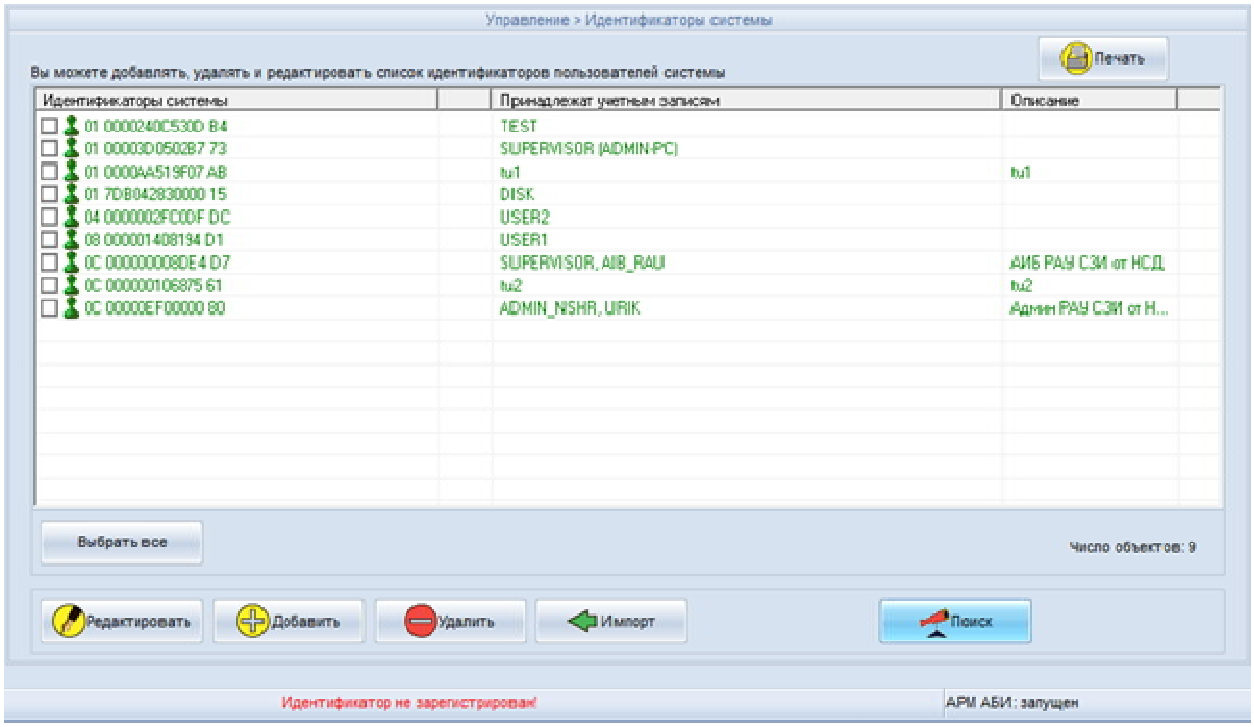

Рисунок 27 - Сообщение о том, что идентификатор не зарегистрирован

4.4 Вкладка «Компьютеры системы»

Вкладка «Управление > Компьютеры системы» позволяет добавлять, удалять и импортировать ПКО в базу СЦУ, передавать базы СЦУ на ПКО, выполнять настройку СЗИ «Аккорд» ПКО, включая формирование дискреционных и мандатных правил разграничения доступа и списка привилегированных процессов. Вкладка «Управление > Компьютеры системы» приведена на рисунке 28.

Примечание. При работе в режиме «Классический РАУ» вид вкладки «Управление > Компьютеры системы» приведён на рисунке 60.

В данной вкладке красным цветом отображаются ПКО, на которых не активированы СЗИ от НСД «Аккорд».

Кнопка <КС на ПКО> предназначена для получения доступа к спискам контроля целостности для ПКО под управлением ОС Linux. При нажатии на неё появляется окно со списком файлов, поставленных на контроль, и с результатом сравнения контрольных сумм файлов с эталонным значением (рисунок 29).

Совпадающие значения контрольных сумм (эталонной и вычисленной) помечаются знаком ОК.

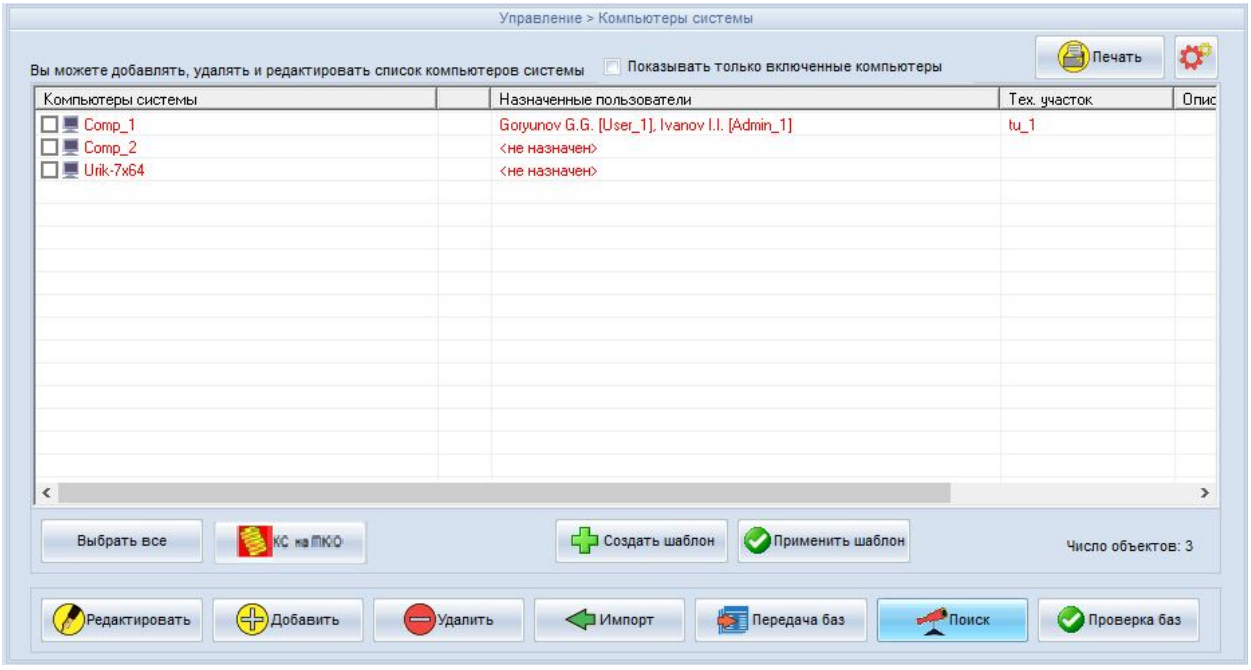

Рисунок 28 – Компьютеры системы

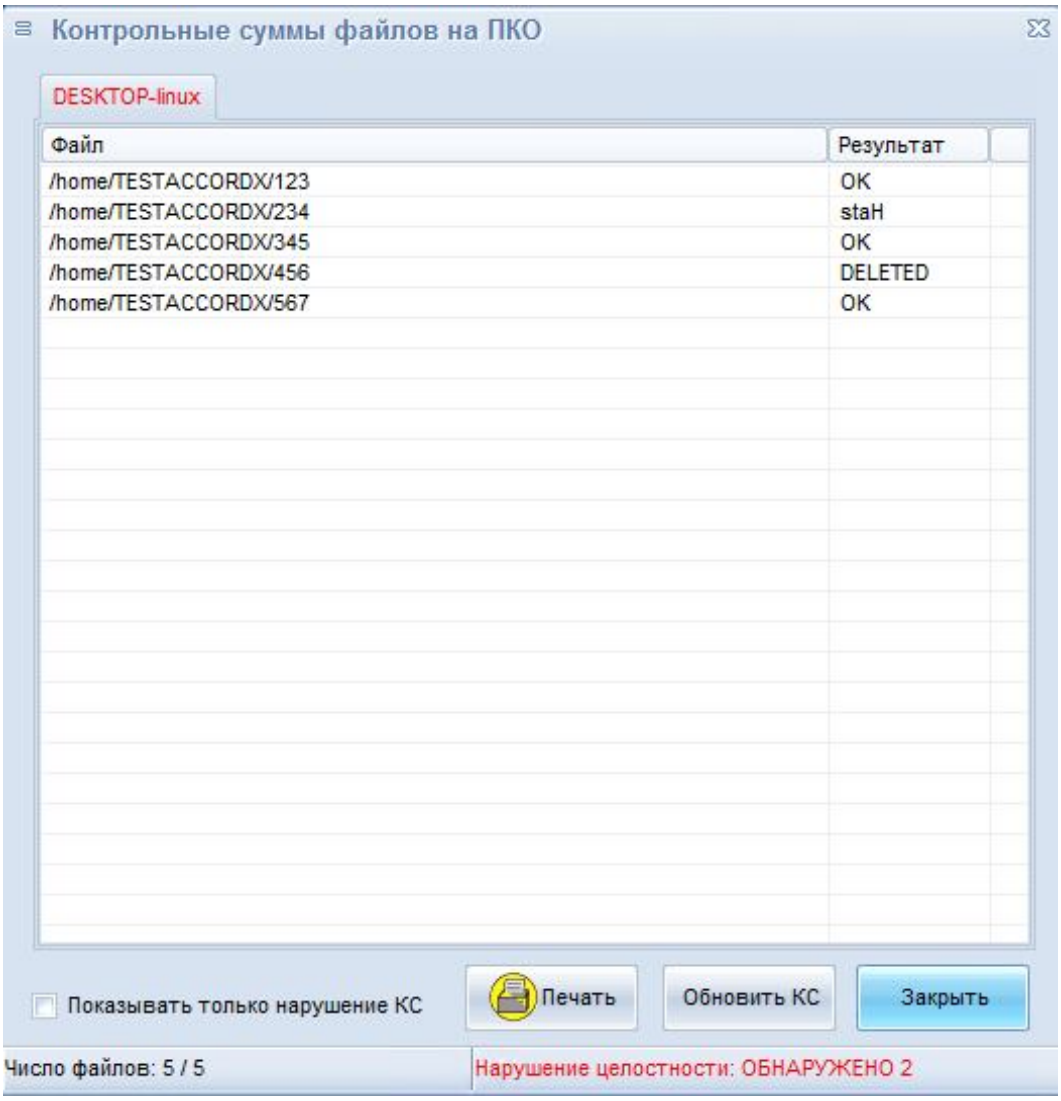

Рисунок 29 - Окно со списком контролируемых файлов для ПКО под управлением ОС Linux

В поле «Нарушение целостности:» отображается количество файлов с изменёнными контрольными суммами. В случае необходимости (если несовпадение контрольных сумм не является инцидентом информационной безопасности) Администратор ИБ ТУ имеет возможность пересчитать контрольные суммы на выбранном ПКО с последующей записью новых эталонных контрольных сумм. Для этого необходимо нажать кнопку <Обновить КС>.

Кнопка <Печать> позволяет распечатать выбранную информацию на принтере, а также сохранить в файл (с указанным разделителем). При ее нажатии появляется окно, приведённое на рисунке 30. В данном окне можно выбрать способ печати: в файл или на принтер, тип выводимой информации (имя компьютера, описание компьютера, тех. участок и т. д.); при печати в файл следует также указать разделитель.

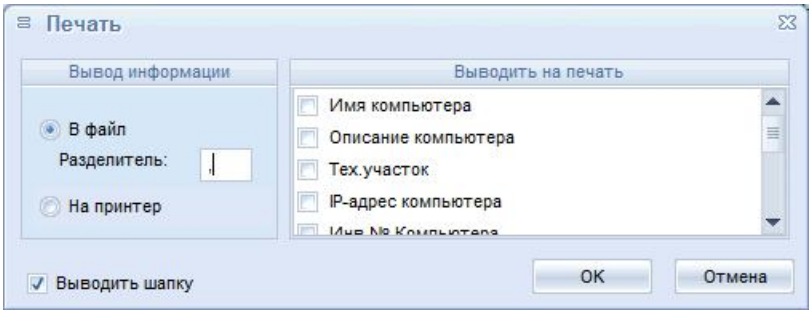

Рисунок 30 - Печать информации о подконтрольном объекте

Для отображения в списке компьютеров информации о наличии на них списков файлов контроля целостности, списков задач и стартовых задачах следует в окне, приведенном на рисунке 28, нажать кнопку <Настройка отображения информации>. При ее нажатии появляется окно, приведённое на рисунке 16, в котором устанавливаются флаги напротив той информации о настройках ПКО, которую следует отобразить. После добавления отображаемой информации в таблице компьютеров появляется столбец под названием «ПКО», как показано на рисунке 31.

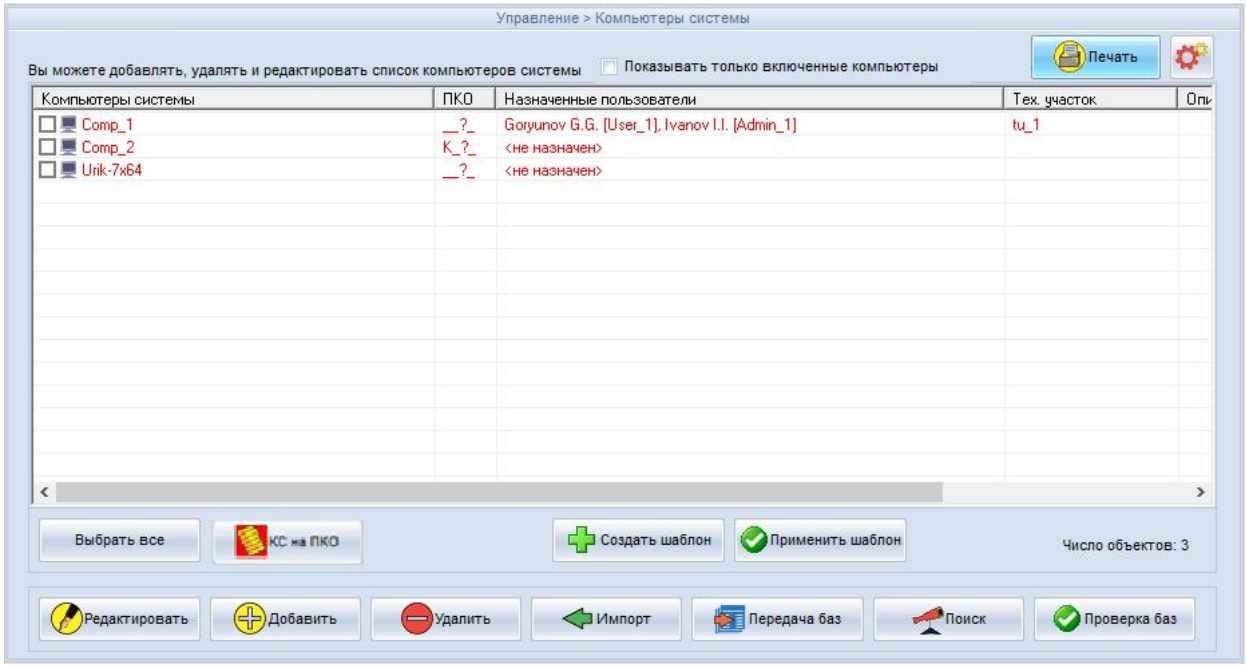

Рисунок 31 – Компьютеры системы. Настройка отображения информации о ПКО

Наличие литеры «К» в данном столбце означает, что для данной учётной записи определён список файлов для контроля целостности, наличие литеры «З» – определён список задач, литеры «С» – определён список стартовых задач, литеры «У» – данный компьютер управляется от СВМиКД.

Для добавления компьютера необходимо нажать кнопку <Добавить> (рисунок 28). В появившемся окне (рисунок 32) задать имя компьютера. Также можно задать описание компьютера и назначить его технологическому участку.

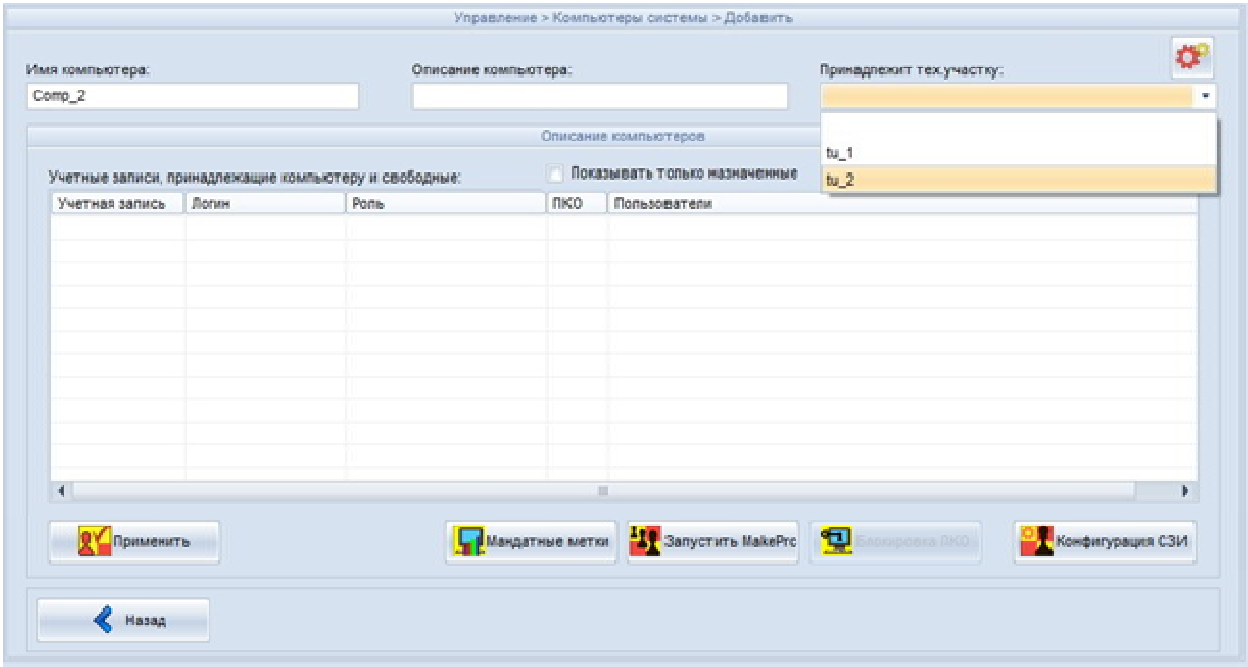

Рисунок 32 – Добавление компьютера

Для редактирования компьютера нажать кнопку <Редактировать> (рисунок 28). В появившемся окне можно изменить имя компьютера, его описание, а также принадлежность к технологическому участку (рисунок 33).

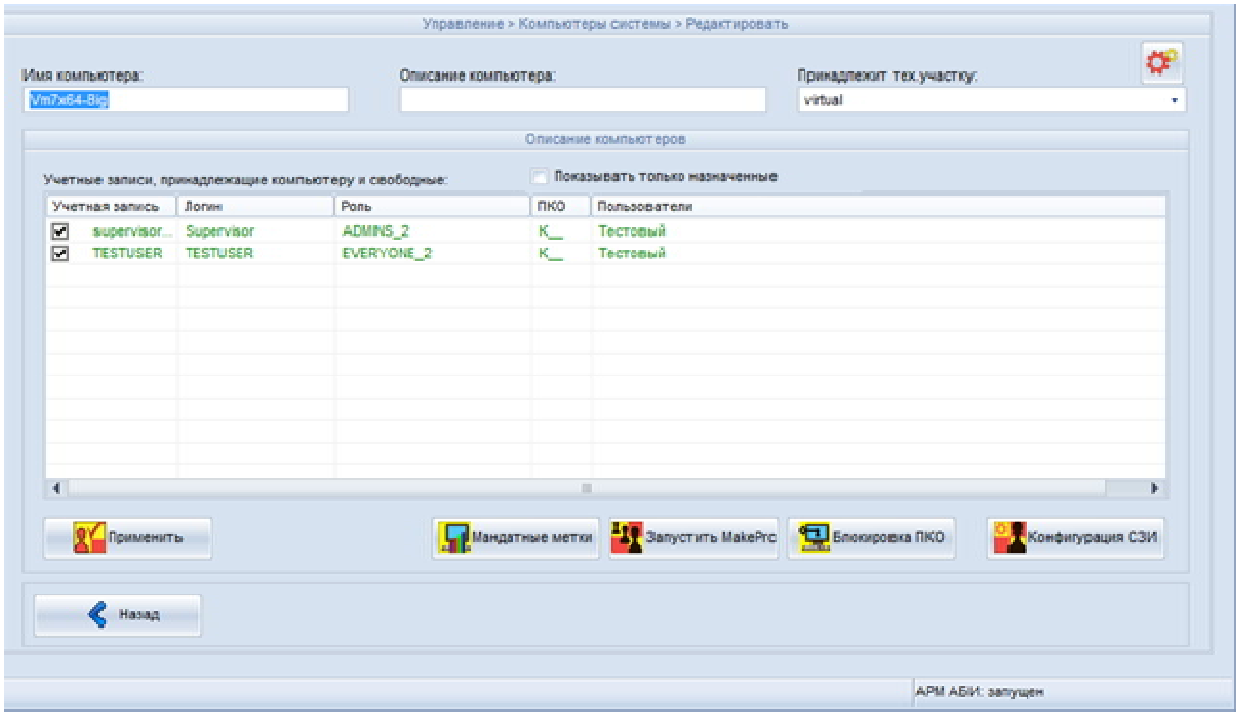

Рисунок 33 – Редактирование списка подконтрольных объектов

Нажатие кнопки <Блокировка ПКО> делает возможным выполнение следующих функций: блокировка/разблокировка ПКО, завершение сеанса работы пользователя, перезагрузка ПКО, выключение ПКО (рисунок 34).

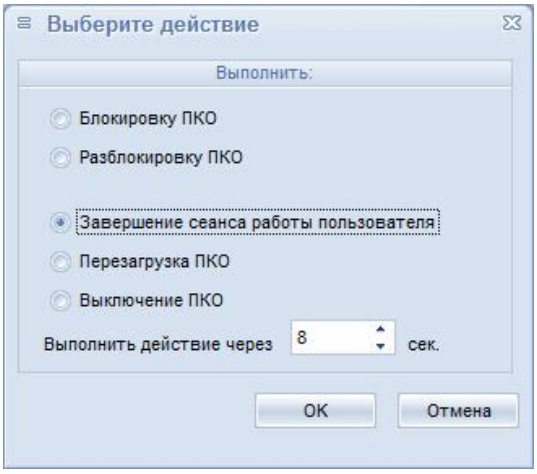

Рисунок 34 - Окно при нажатии кнопки <Блокировка ПКО>

При установке таймера на выполнение выбранного действия и нажатии кнопки <ОК> на экране ПКО появится соответствующее сообщение (рисунок 35).

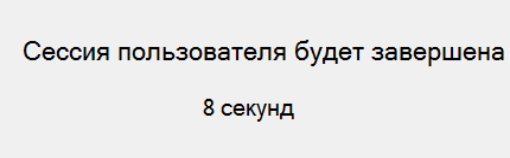

Рисунок 35 - Сообщение на ПКО о принудительном завершении сеанса пользователя по истечении установленного времени

Кнопка <Мандатные метки> предназначена для установки меток мандатного доступа к объектам ПКО (в случае использования на ПКО мандатного механизма разграничения доступа).

При нажатии кнопки <Мандатные метки>[1] появляется главное окно программы ACED32.EXE, в котором следует выбрать функцию установки меток мандатного допуска (Команды\Метки мандатного допуска, рисунок 36).

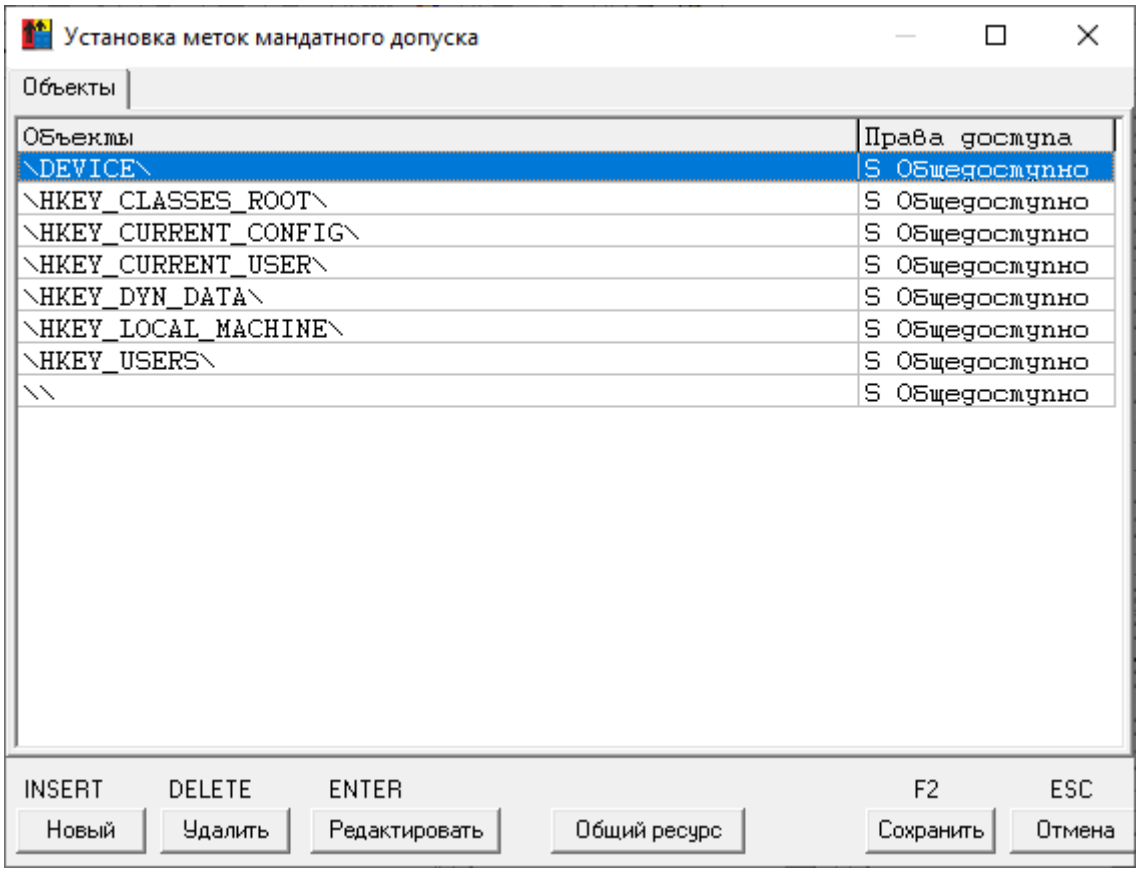

Рисунок 36 – Установка меток мандатного допуска

При редактировании списка общих ресурсов ПКО на СЦУ на ПКО необходимо выполнить процедуру обновления списка общих ресурсов: запустить ACED32.EXE, затем выбрать функцию Команды\Метки мандатного допуска\Общий ресурс\Обновить ресурсы на диске.

[1] Только для ПКО под управлением ОС Windows

При нажатии кнопки <Конфигурация СЗИ> появляется окно, в котором отображаются настройки СЗИ от НСД «Аккорд», версия его программного обеспечения и IP-адрес, серийный номер контроллера, а также инвентарный номер ПКО (заполняется вручную, рисунки 37/38).

Рисунок 37 – Конфигурация СЗИ на ПКО под управлением ОС Windows

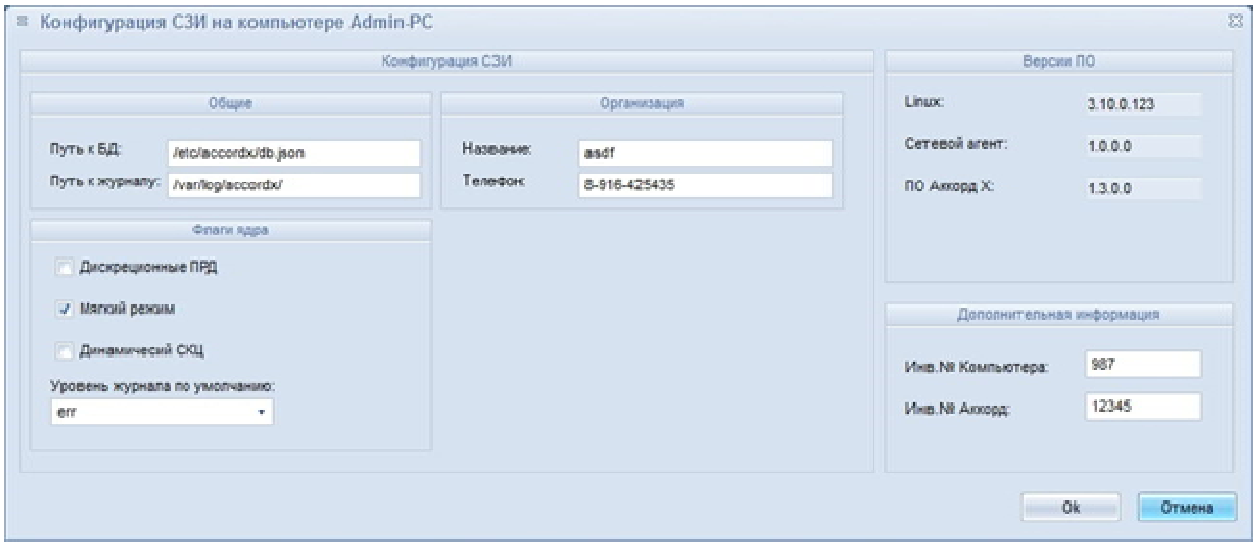

Рисунок 38 - Конфигурация СЗИ на подконтрольном объекте под управлением ОС Linux

При необходимости изменения настроек СЗИ от НСД «Аккорд» на выбранном ПКО следует установить нужные настройки в поле «Конфигурация СЗИ». Для сохранения изменений нажать кнопку <Ok>.

В случае успешного сохранения настроек на экране появляется сообщение, приведённое на рисунке 39.

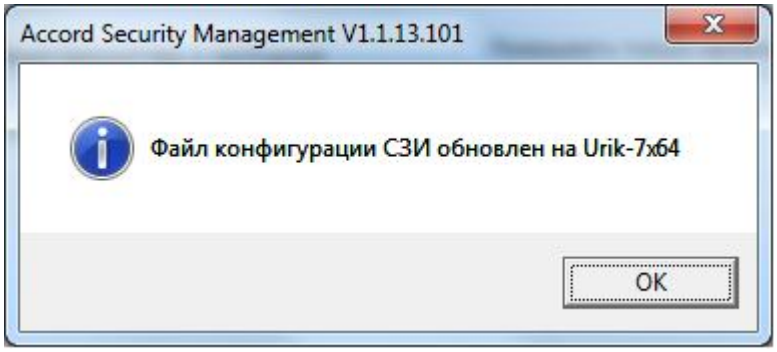

Рисунок 39 – Сообщение об успешном изменении настроек СЗИ от НСД «Аккорд»

Существует возможность редактирования списка привилегированных процессов с последующей его передачей на ПКО. Для этого нужно нажать кнопку <Запустить MakePrc>[1] (рисунок 33).

Если необходимо определить, зарегистрирован ли компьютер в системе, следует нажать кнопку <Поиск> во вкладке «Компьютеры» (рисунок 28). При ее нажатии появляется окно (рисунок 40), в котором необходимо указать IP-адрес компьютера или его имя.

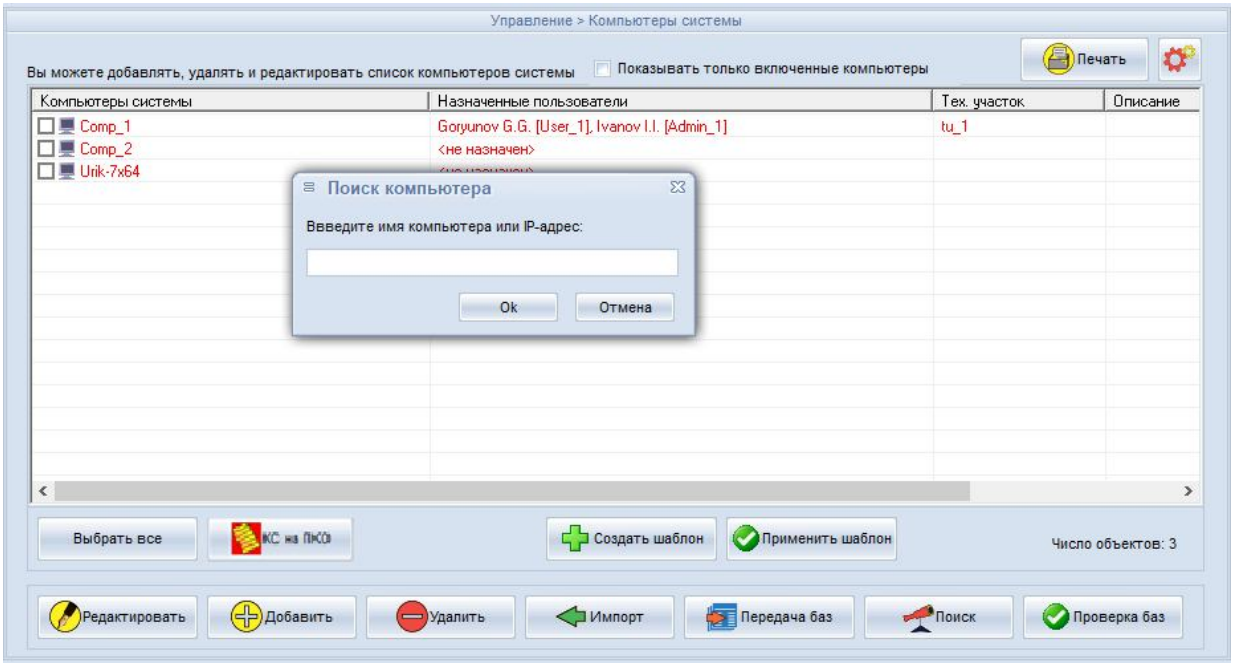

Рисунок 40 – Поиск компьютера по имени или IP-адресу

[1] Только для ПКО под управлением ОС Windows

Если данный компьютер зарегистрирован в системе, то будет выделена строка, соответствующая данному компьютеру, как показано на рисунке 41.

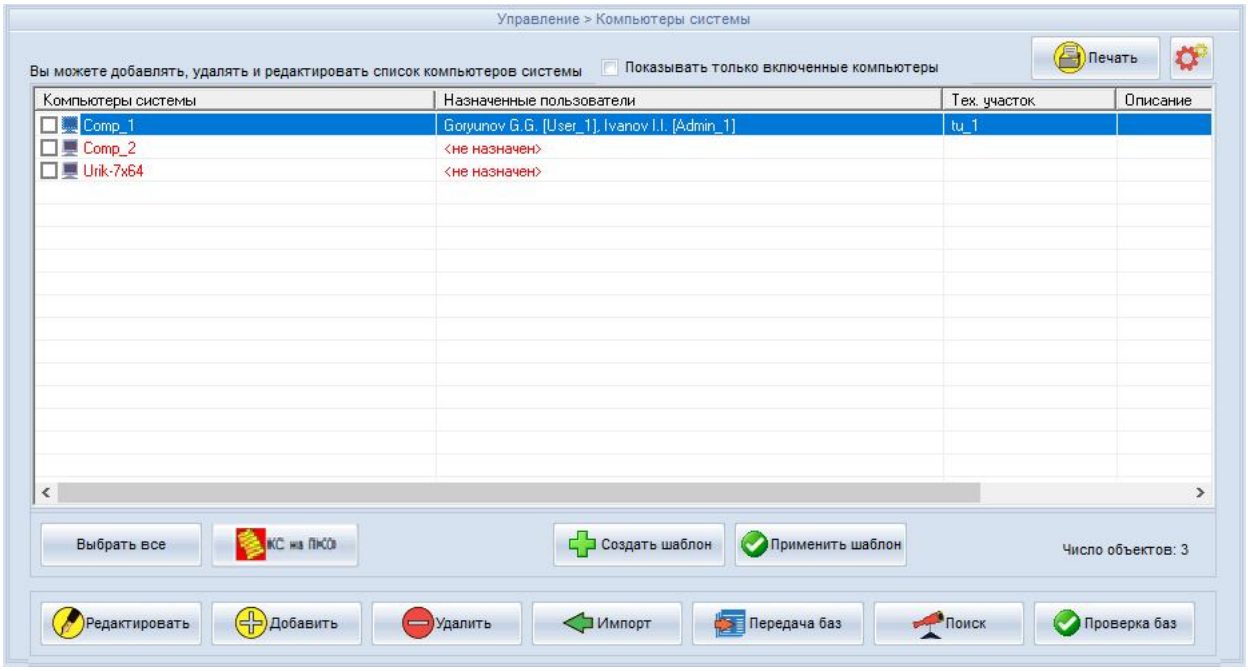

Рисунок 41 – Найден компьютер

Если компьютер не зарегистрирован в системе, в нижней части окна появится сообщение «Компьютер не найден!», как показано на рисунке 42.

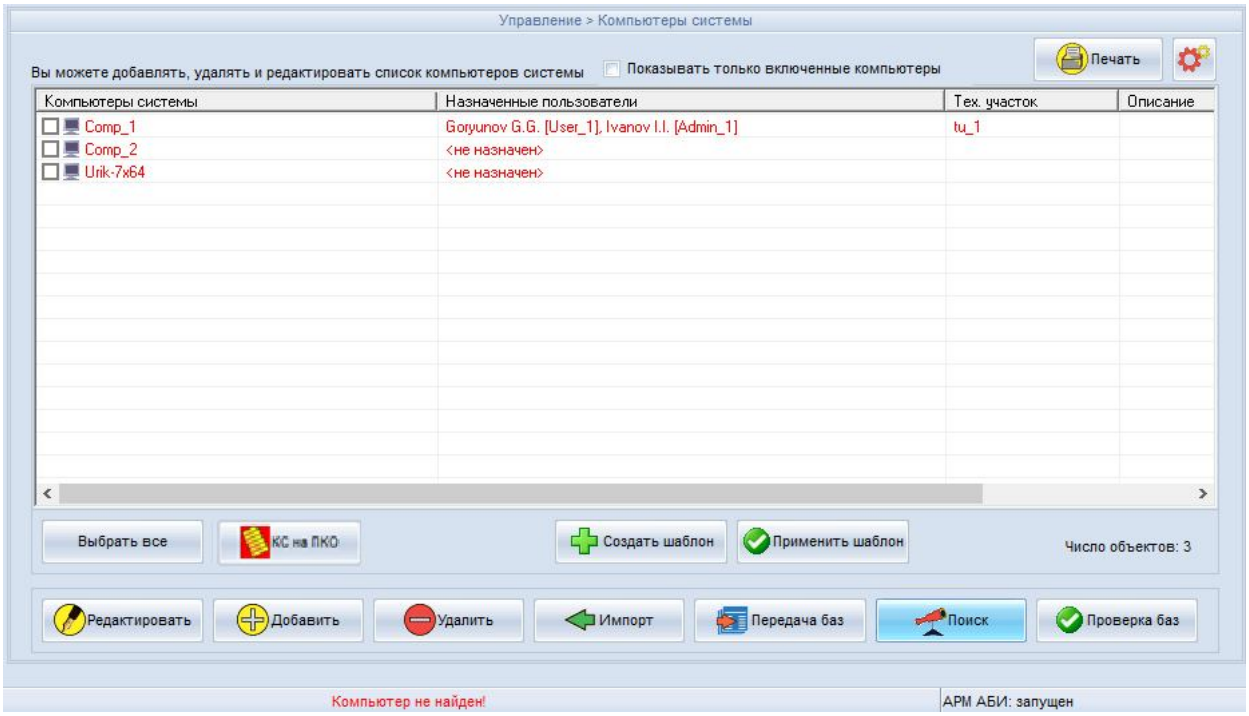

Рисунок 42 – Сообщение о том, что компьютер не найден

Для удаления компьютера из системы необходимо во вкладке «Управление > Компьютеры системы» (рисунок 28) выделить его и нажать кнопку <Удалить>. Появится окно подтверждения этого действия (рисунок 43).

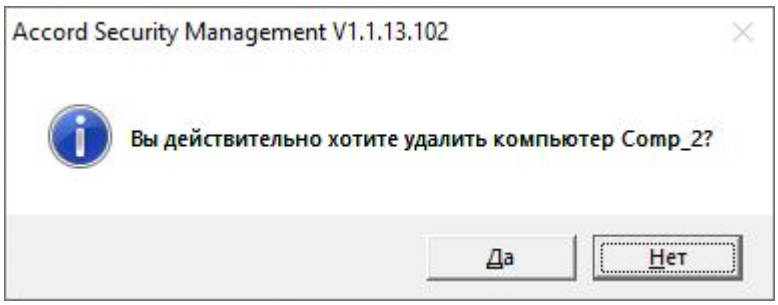

Рисунок 43 – Окно подтверждения удаления компьютера

При нажатии <Да> происходит очистка каталогов, содержащих файлы ПКО (каталоги \Asm\ACCONNET\OUT\CompName\), а также каталогов \Asm\OutBases_Temp и \Asm\ACCONNET\IN.

Кнопка <Проверка баз> обеспечивает автоматическое применение изменений ролей и баз пользователей, выполненных на ПКО.

ВНИМАНИЕ! Синхронизировать базы пользователей могут только Администраторы ИБ соответствующих технологических участков!

Кнопка <Импорт> во вкладке «Управление > Компьютеры системы» (рисунок 28) необходима для регистрации ПКО. При нажатии данной кнопки появляется окно импорта компьютеров (рисунок 44). Чтобы импортировать компьютеры из базы «Аккорд-РАУ», необходимо установить соответствующий флаг («Вы можете импортировать компьютеры из:» - «базы Accord -РАУ») в окне, показанном на рисунок 44, и нажать кнопку <Импортировать>.

Рисунок 44 - Импорт компьютеров

При ее нажатии появляется окно выбора файла, в котором следует указать файл, из которого необходимо импортировать компьютеры. Импорт компьютеров осуществляется из файла «AcNode.lst».

После этого в правой части окна появятся импортированные компьютеры. Следует выбрать из них необходимые для добавления в базу (для выбора всех учетных записей нужно нажать кнопку <Выбрать все>) и нажать кнопку <Добавить> (рисунок 45).

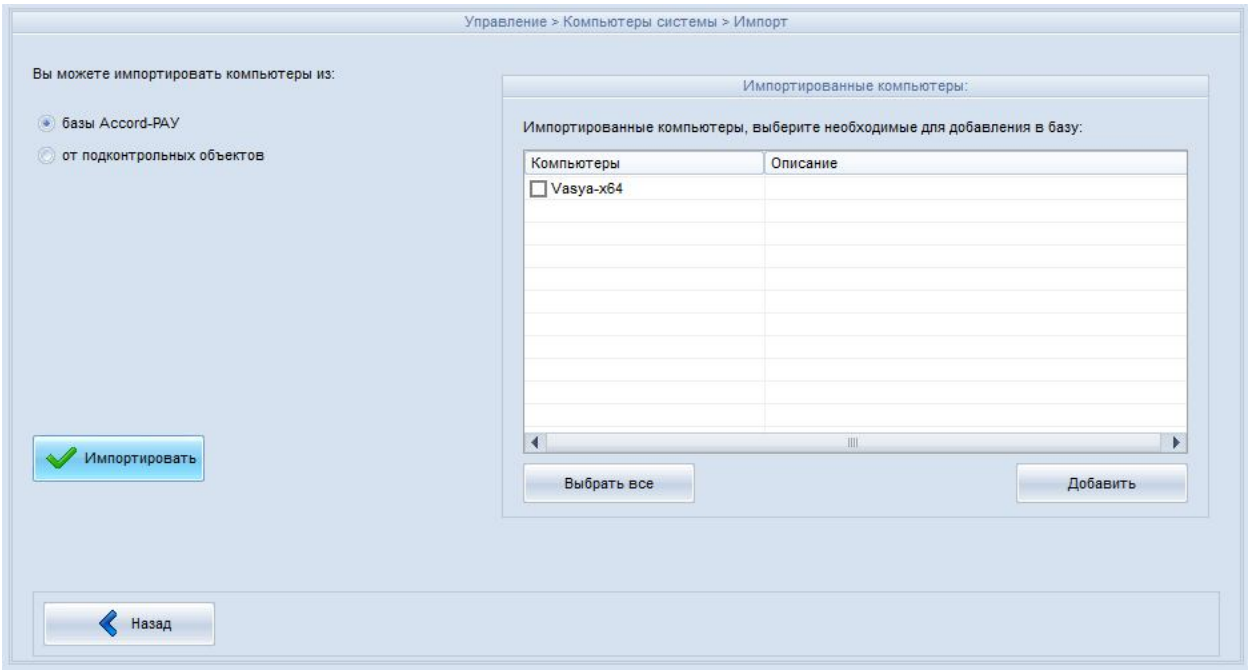

Рисунок 45 - Выбор импортированных компьютеров (импорт из базы «Аккорд-РАУ»)

Чтобы импортировать компьютеры от подконтрольных объектов, необходимо установить соответствующий флаг («Вы можете импортировать компьютеры из:» - «от подконтрольных объектов») в окне, показанном на рисунок 46, и нажать кнопку <Импортировать>.

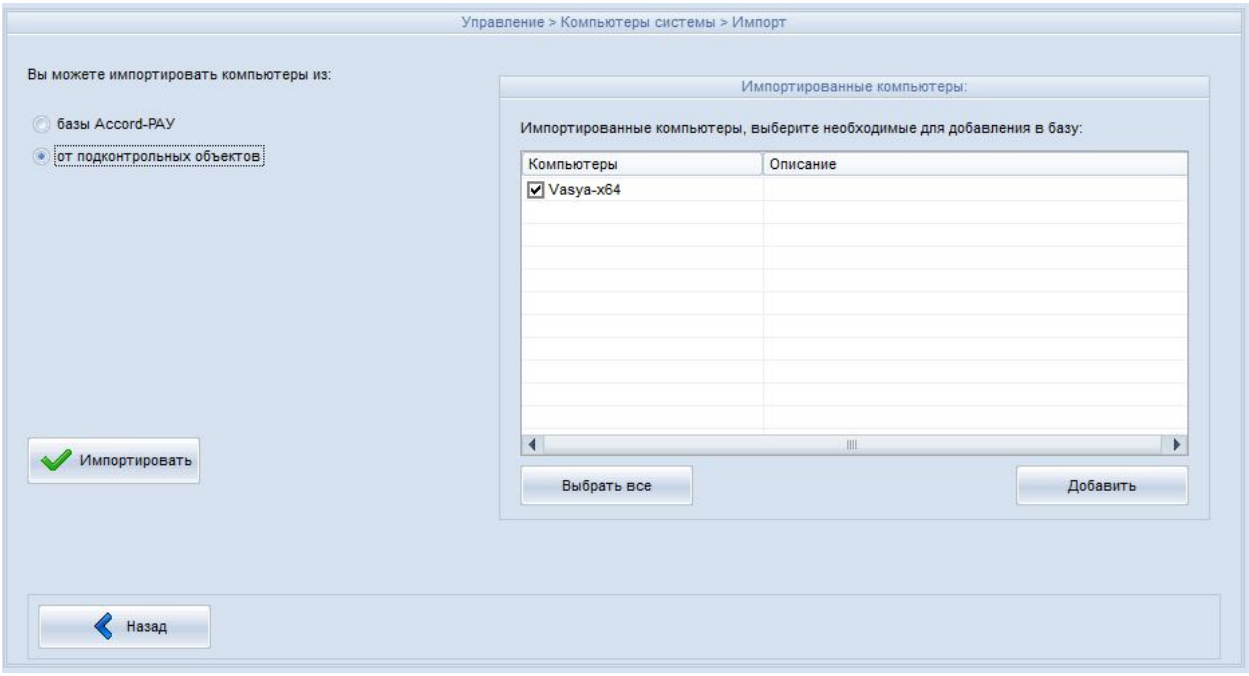

Рисунок 46 - Выбор импортированных компьютеров (импорт от ПКО)

После этого в правой части окна появятся импортированные компьютеры, следует выбрать из них необходимые для добавления в базу (для выбора всех учетных записей нужно нажать кнопку <Выбрать все>) и нажать кнопку <Добавить> (рисунок 46).

В РАУ в целях обеспечения возможности одновременной работы нескольких пользователей ASM предусмотрено выполнение динамического обновления баз пользователей: если в рамках работы одного пользователя РАУ другой пользователь выполнил процедуру редактирования баз данных, то появляется сообщение «Базы модифицированы другим администратором. Обновлены».

В РАУ также имеется возможность динамического сохранения баз данных непосредственно в рамках редактирования баз данных персоналом РАУ. Эта процедура выполняется автоматически при изменении баз пользователей.

Передача баз пользователей на ПКО в рамках централизованной схемы осуществляется кнопкой <Передача баз> (предварительно выбрать компьютеры (рисунок 28), на которые планируется передать базы). При ее нажатии появляется окно передачи баз пользователей на ПКО, приведённое на рисунке 47.

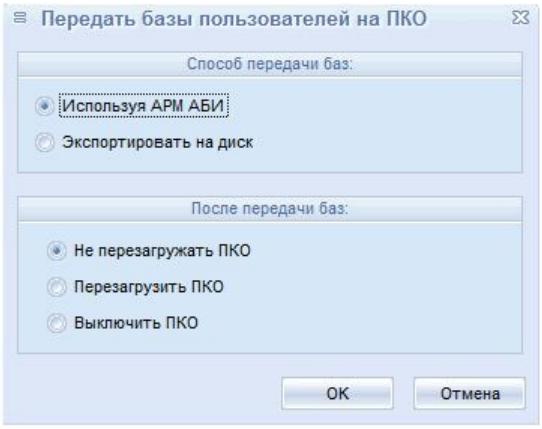

Рисунок 47 - Передача баз пользователей по централизованной схеме

Выбрать пункт «Используя АРМ АБИ» (рисунок 47) и нажать кнопку <OK>.

Если база пользователей успешно передана на ПКО, то появляется сообщение, приведённое на рисунке 48.

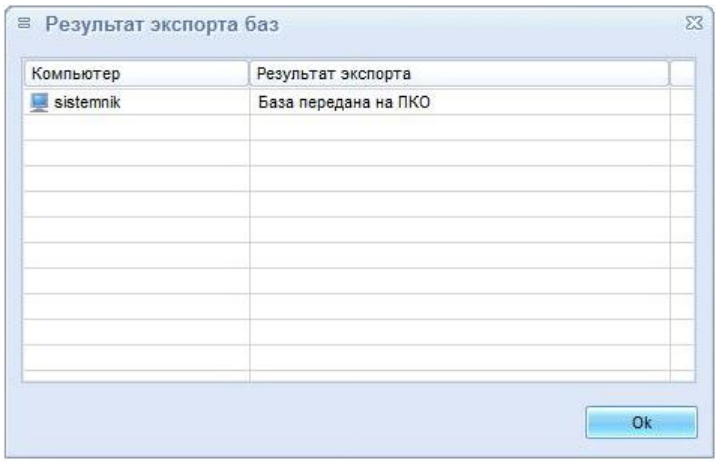

Рисунок 48 – Сообщение об успешной передаче базы пользователей на ПКО

Если во время выполнения процедуры передачи базы пользователей служба AcConNet загружена, появляется сообщение о постановке в очередь (рисунок 49).

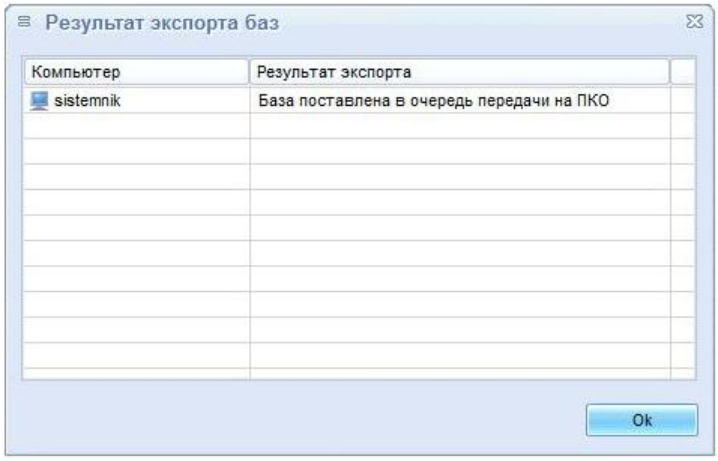

Рисунок 49 – Сообщение о том, что база пользователей поставлена в очередь передачи на ПКО

По истечении некоторого времени база пользователей автоматически передается на ПКО, и на экране появляется сообщение, показанное на рисунке 48.

Если во время выполнения процедуры передачи базы пользователей ПКО выключен, то на экране появляется сообщение о готовности к передаче, приведённое на рисунке 50.

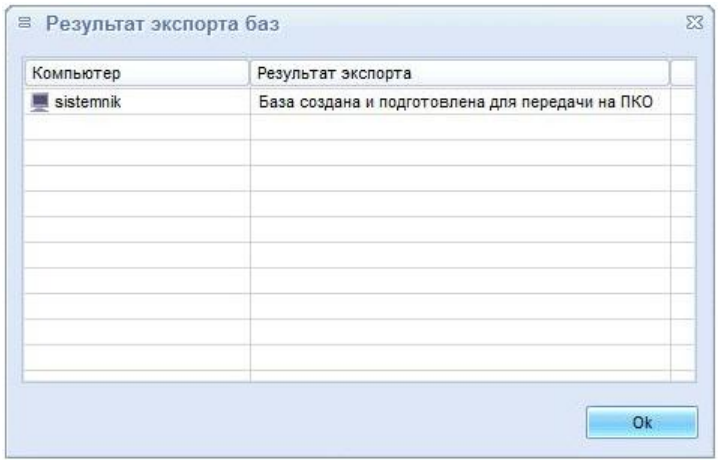

Рисунок 50 – Сообщение о том, что база пользователей создана и подготовлена для передачи на ПКО

База пользователей автоматически будет передана при следующем включении ПКО, и на экран будет выведено сообщение, приведённое на рисунке 51.

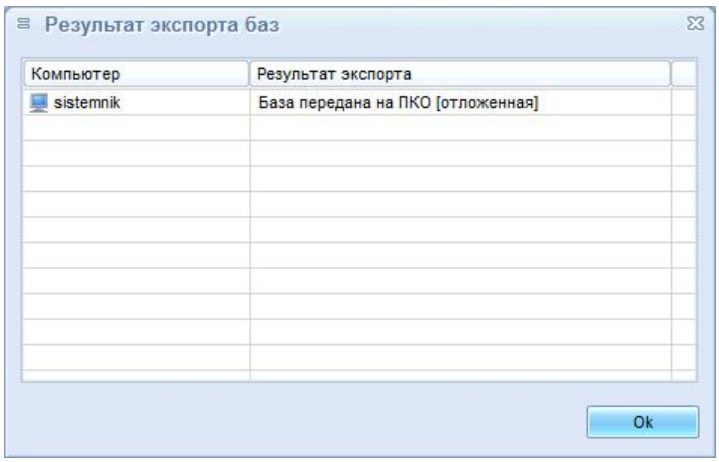

Рисунок 51 - Сообщение о том, что отложенная база передана на ПКО

Если процедура передачи базы пользователей выполняется на ПКО, на котором не активирована система защиты ПАК «Аккорд», на экране появляется сообщение с пометкой «[Аккорд не активирован]», приведённое на рисунке 52.

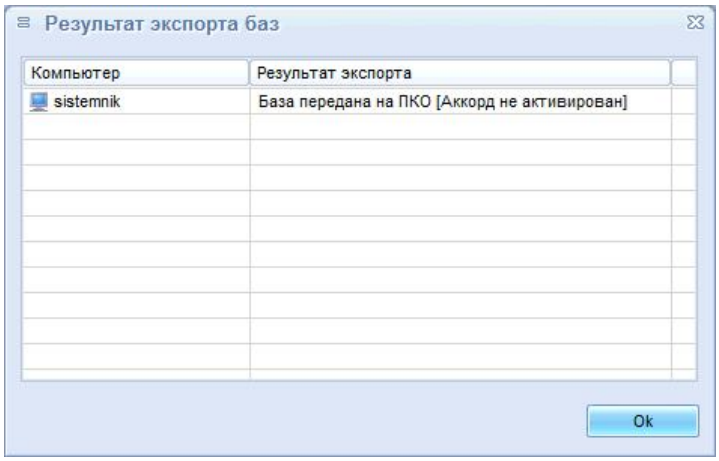

Рисунок 52 – Сообщение о передаче базы пользователей на ПКО, на котором не активирована система защиты ПАК «Аккорд»

Значение таймаута для передачи баз пользователей на ПКО составляет две минуты. При необходимости время таймаута можно изменить. Для этого в файле AcCon32.ini необходимо изменить значение параметра TcpAckTimeout.

Передача баз пользователей на ПКО технологического участка в рамках децентрализованной схемы осуществляется кнопкой <Передача баз> (предварительно выбрать компьютеры (рисунок 28), на которые планируется передать базы). При этом производится копирование перечня учетных записей на внешний носитель. Если в качестве внешнего носителя используется USB-накопитель, то перед тем, как выполнить процедуру передачи баз пользователей на ПКО в рамках децентрализованной схемы, необходимо добавить его в единую базу USB-носителей. Процедура выполняется Администратором в соответствии с докумен-

том 11443195.4012-053 90 «СПО СЗИ НСД «Аккорд-РАУ». Руководство Администратора».

При нажатии кнопки <Передача баз> появляется окно, приведённое на рисунке 53. В данном окне выбрать пункт «Экспортировать на диск» и нажать кнопку <OK>.

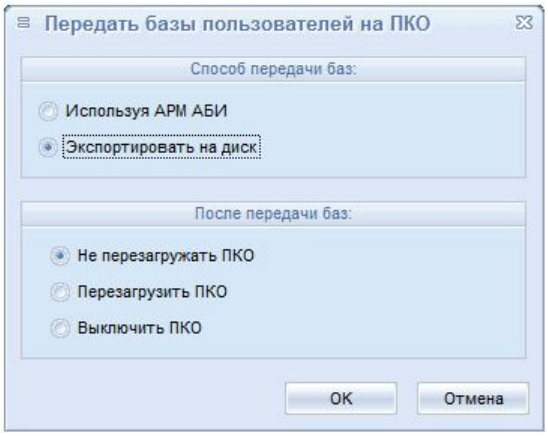

Рисунок 53 - Передача баз пользователей по децентрализованной схеме

Далее появляется окно выбора каталога, в котором нужно выбрать любой каталог на внешнем носителе и нажать кнопку <Применить>.

Если процедура экспорта баз пользователей выполнена успешно, на экране появляется сообщение, приведённое на рисунке 54.

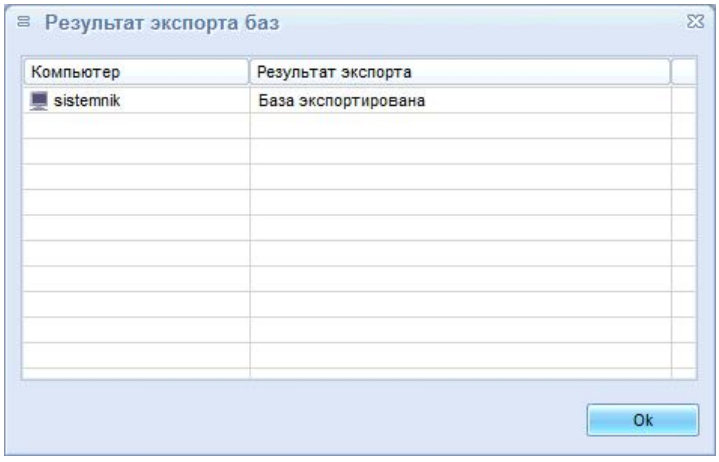

Рисунок 54 – Сообщение о том, что база пользователей экспортирована на диск

Базы пользователей экспортируются в файл <выбранный_каталог>\Out\xxx\xxx.AMZ, где <выбранный_каталог> – каталог на внешнем носителе, xxx – имя ПКО, xxx.AMZ – файл, в котором находится список баз пользователей. Далее список на внешнем носителе должен быть доставлен на ПКО.

Для этого на ПКО необходимо выполнить следующие действия (чтобы функция импорта базы пользователей стала доступной, на ПКО в файле «AcWs32.ini» необходимо установить параметр NoNetManaged=Yes или в главном окне программы регистрации рабочей станции (ACSETWS.EXE) установить флаг «Станция не управляется по сети»):

- в трее выбрать правой кнопкой мыши сетевой клиент ПАК «Аккорд», приведённый на рисунке 55;

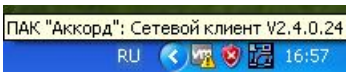

Рисунок 55 – Значок сетевого клиента ПАК «Аккорд» в трее

- появится меню, приведённое на рисунке 56;

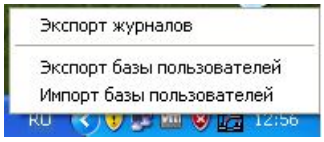

Рисунок 56 – Контекстное меню сетевого клиента ПАК «Аккорд» в трее

- в этом меню выбрать пункт «Импорт базы пользователей». Появляется сообщение «Предъявите идентификатор». Предъявить идентификатор Администратора «Аккорд» ПКО. Появится окно ввода пароля, приведённое на рисунке 57;

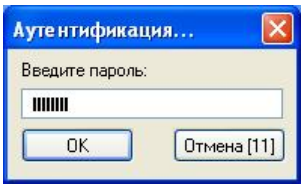

Рисунок 57 – Окно ввода пароля

- ввести пароль и нажать <OK>. Появится окно выбора каталога для импорта базы пользователей, приведённое на рисунке 58;

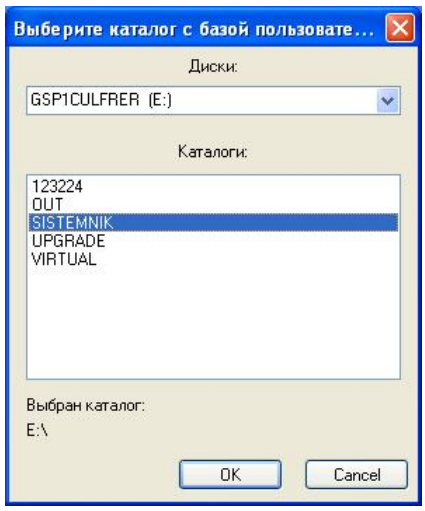

Рисунок 58 – Выбор каталога для импорта базы пользователей

- выбрать нужный каталог и нажать <OK>.

Если импорт базы пользователей выполнен успешно, на экране появится сообщение, приведённое на рисунке 59.

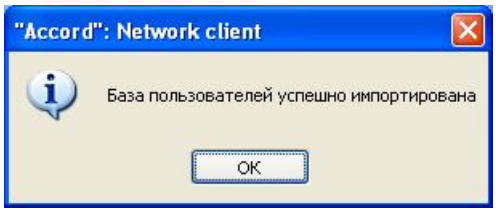

Рисунок 59 – Оповещение об успешном выполнении процедуры импорта базы пользователей

При первом выполнении процедуры создания файлов базы пользователей на СЦУ создаётся каталог C:\Asm\OutBases\CompName (где «CompName» – имя ПКО). В нем хранятся файлы базы пользователей, которые создаются в ASM при нажатии кнопки <Передача баз>.

Далее при выполнении процедуры передачи баз пользователей на ПКО на СЦУ создаётся каталог C:\Asm\ACCONET\OUT\CompName (где «CompName» – имя ПКО), в котором хранятся копии файлов базы пользователей, эквивалентные переданным на ПКО.

Если файлы в каталоге C:\Asm\OutBases\CompName эквивалентны файлам в каталоге C:\Asm\ACCONET\OUT\CompName, процедура передачи файлов базы пользователей на ПКО не производится. Если различия имеются, файлы из каталога C:\Asm\OutBases\CompName переписываются в каталог C:\Asm\ACCONET\OUT\CompName и передаются на ПКО.

РАУ позволяет осуществлять контроль целостности файлов на ПКО. Для этого необходимо перейти в режим «Классический РАУ»: во вкладке «Настройки > Основные настройки» выбрать флаг «Использовать классический режим РАУ» и нажать кнопку <Применить>. Далее перейти во вкладку «Управление > Компьютеры системы», приведённую на рисунке 60, установить флаги напротив тех ПКО, для которых создаётся задание для контроля целостности, и нажать кнопку <Создать шаблон>.

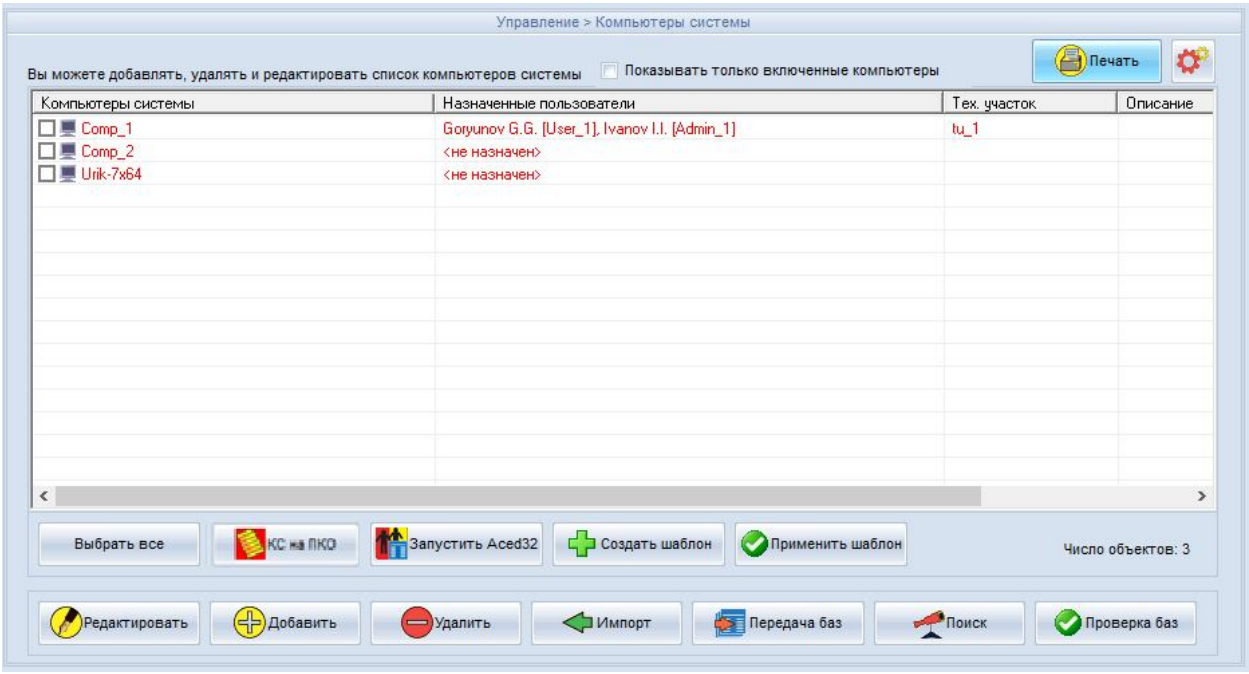

Рисунок 60 - Вкладка «Компьютеры системы» при работе в режиме «Классический РАУ»

При ее нажатии появляется окно, приведённое на рисунке 61.

Рисунок 61 - Вкладка Компьютеры системы > Создать шаблон

В данном окне следует установить переключатель в положение «Задания расчета КЦ» и нажать <Создать>. Появится стандартное диалоговое окно Windows создания файла. В данном окне следует указать имя файла задания. Файлу присваивается расширение *.HSH_TASK.

После указания имени файла задания выводится окно, примерный вид которого приведён на рисунке 10. В данном окне указываются файлы, целостность которых нужно контролировать. При указании файлов должны соблюдаться правила, приведённые в подразделе 4.2. Примеры строк, задающих файлы, целостность которых нужно контролировать, приведены в таблице 1.

Существует возможность создавать задания для контроля целостности на основе файла и на основе шаблона. Данные процедуры описаны в документах 11443195.4012-036 97 «ПАК Аккорд-Win32 (версия 4.0). Установка правил разграничения доступа. Программа ACED32» и 11443195.4012-036 97 «ПАК Аккорд-Win64 (версия 5.0). Установка правил разграничения доступа. Программа ACED32».

После создания или изменения задания для контроля целостности в окне, приведённом на рисунке 10, нажать кнопку <Сохранить>.

ВНИМАНИЕ! Для осуществления процедуры удаленного контроля целостности файлов на ПКО кнопками <Создать шаблон> и <Применить шаблон> необходимо установить флаг «Использовать удаленный расчет КЦ» во вкладке

«Настройка > Основные настройки». Если данный флаг не установлен, файлы с заданием КЦ не будут переданы на ПКО.

Если в окне, приведённом на рисунке 60, были установлены флаги напротив некоторых ПКО, то сформированное задание сразу будет передано на выбранные ПКО.

Если ПКО выбраны не были, то в окне, приведённом на рисунке 60, нужно установить флаги напротив тех ПКО, на которых нужно контролировать целостность файлов, указанных в задании, и нажать кнопку <Применить шаблон>. В появившейся вкладке выбора шаблона следует установить переключатель в положение «Задания расчета КЦ» и в стандартном диалоговом окне Windows открытия файла указать созданный файл задания для контроля целостности. Сформированное задание будет передано на выбранные ПКО.

Получив файл с заданием для контроля целостности, ПО ПКО выполняет расчёт эталонных контрольных сумм. Расчёт выполняется незаметно для пользователя ПКО. Если во время расчёта произойдёт перезагрузка ПКО или его выключение, то после загрузки расчёт будет продолжен.

После завершения расчёта файл с эталонными контрольными суммами будет передан на СЦУ. Файл соответствует заданию для контроля целостности и содержит значения эталонных контрольных сумм, вычисленных на ПКО для указанного файла. Вместо сокращений и символьных масок здесь присутствуют полные имена файлов. Строки задания для контроля целостности, содержащие символьные маски, заменяются несколькими строками, по количеству выбранных по данной маске файлов. Строки дополнены атрибутами файлов.

Если файла, указанного в задании для контроля целостности, не окажется на ПКО, то вместо эталонной контрольной суммы квадратные скобки будут содержать запись «NOT FOUND».

При получении файл сохраняется на СЦУ с именем, совпадающим с именем файла задания, и расширением *.CRC.

Чтобы применить созданное задание для контроля целостности к некоторой группе пользователей ПАК СЗИ от НСД «Аккорд» на некоторых ПКО, следует во вкладке «Управление > Компьютеры системы», приведённой на рисунке 60, выбрать данные ПКО и нажать кнопку <Запустить Aced32>. Появится главное окно редактора базы пользователей ПАК СЗИ от НСД «Аккорд» – AcEd32, приведённое на рисунке 62.

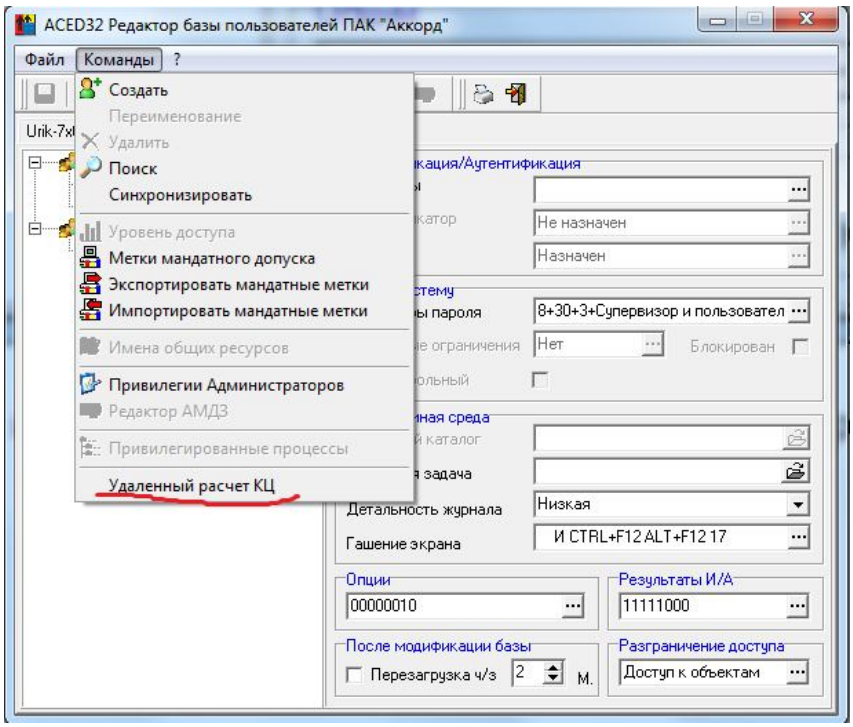

Рисунок 62 - Главное окно редактора базы пользователей ПАК СЗИ от НСД «Аккорд»

В главном меню данного окна или контекстном меню, появляющемся при нажатии правой кнопки мыши на группе пользователей, выбрать пункт «Удаленный расчет КЦ». Появится окно контроля целостности файлов, приведённое на рисунке 63. Данное окно содержит список фалов, целостность которых контролируется на ПКО.

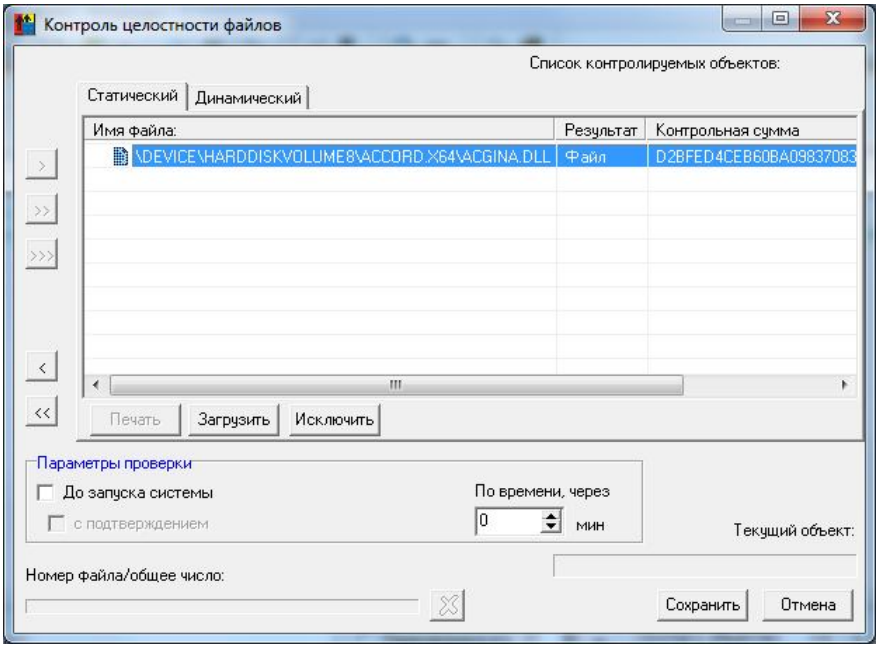

Рисунок 63 - Окно контроля целостности файлов

Следует нажать кнопку <Загрузить> и в появившемся стандартном диалоговом окне Windows открытия файла указать файл с эталонными контрольными суммами *.CRC. Примерный вид окна контроля целостности файлов со списком файлов, целостность которых контролируется на ПКО, приведён на рисунке 64.

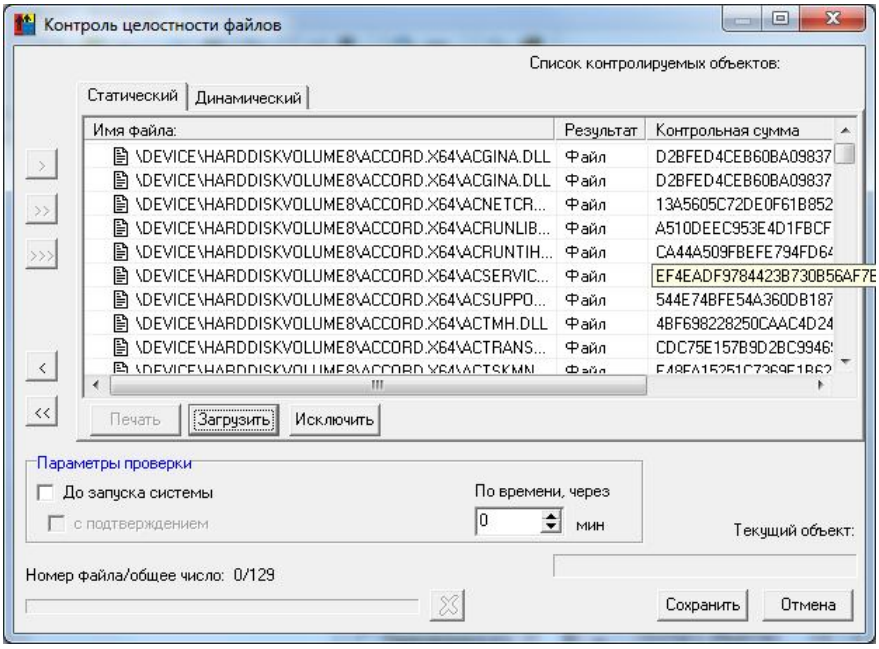

Рисунок 64 - Список файлов, целостность которых контролируется на ПКО

В этом окне нажать кнопку <Сохранить> и затем выйти из редактора базы пользователей ПАК СЗИ от НСД «Аккорд».

База для контроля целостности файлов передаётся на выбранные ПКО. На ПКО появляется новый файл «Accord.amz», содержащий актуальную информацию для контроля целостности файлов.

4.5 Вкладка «Учётные записи»

Вкладка «Управление > Учётные записи» позволяет формировать единую базу учётных записей персонала и пользователей ПКО: добавлять, удалять, редактировать и импортировать учётные записи. Вкладка «Управление> Учётные записи» приведена на рисунке 65.

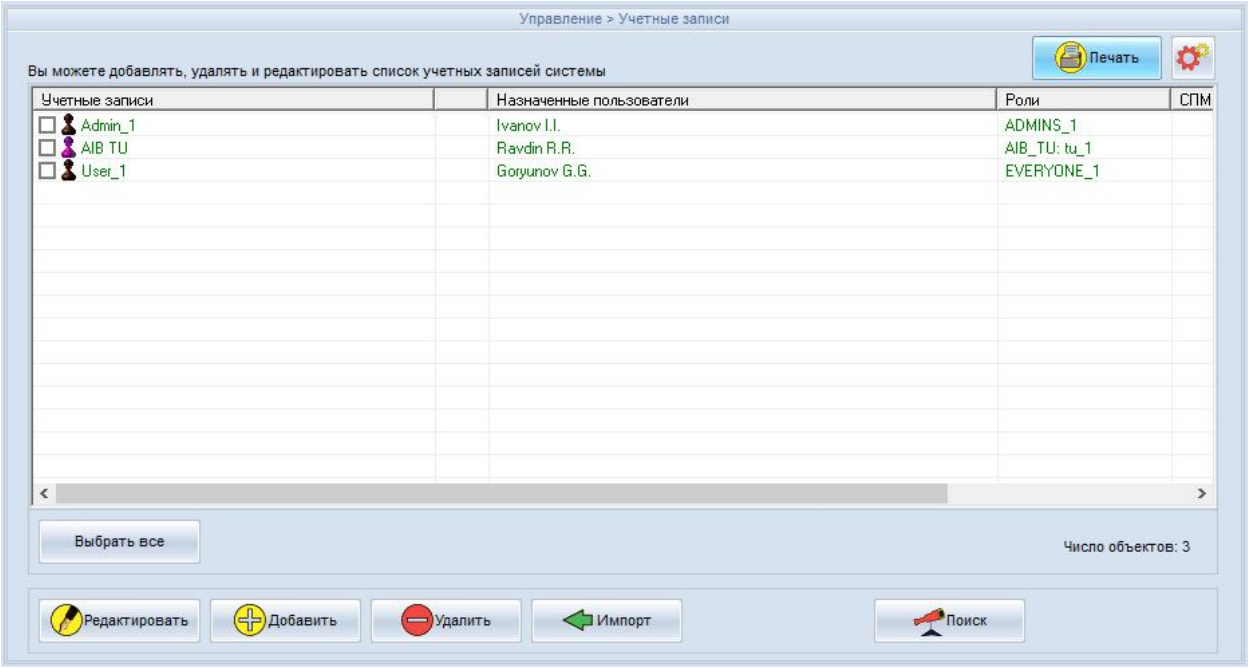

Рисунок 65 - Учетные записи системы

Для отображения в таблице учётных записей информации о наличии списков файлов контроля целостности, списков задач, стартовых задачах следует нажать кнопку <Настройка отображения информации>. При ее нажатии появляется окно, приведённое на рисунке 16, в котором устанавливаются флаги напротив той информации о настройках ПКО, которую следует отобразить. После добавления отображаемой информации в таблице учётных записей появляется столбец под названием «ПКО», как показано на рисунке 66.

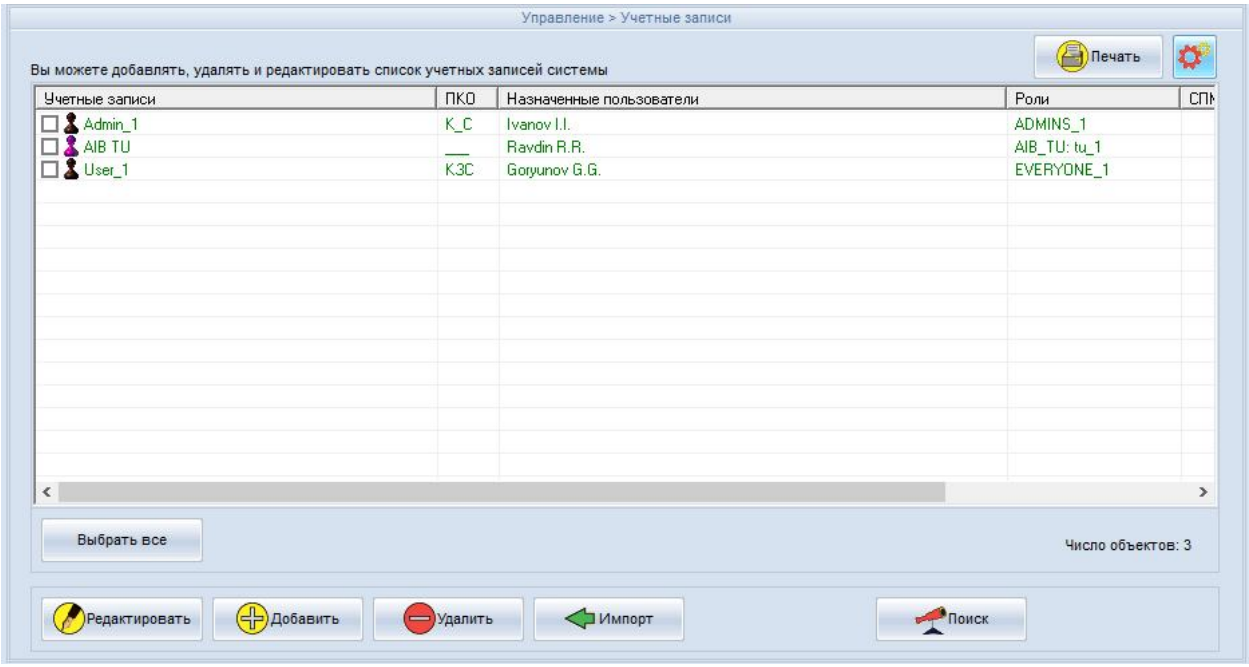

Рисунок 66 – Учётные записи. Отображение информации о ПКО

Наличие литеры «К» в данном столбце означает, что для данной учётной записи определён список файлов для контроля целостности, наличие литеры «З» – определён список задач, литеры «С» – определён список стартовых задач, литеры «У» – данный компьютер управляется от СВМиКД.

Кнопка <Печать> позволяет распечатать выбранную информацию на принтере, а также сохранить в файл (с указанным разделителем). При ее нажатии появляется окно, приведённое на рисунке 67. В данном окне можно выбрать способ печати: в файл или на принтер, тип выводимой информации (имя учётной записи, имя назначенного ей пользователя, имя роли); при печати в файл следует также указать разделитель.

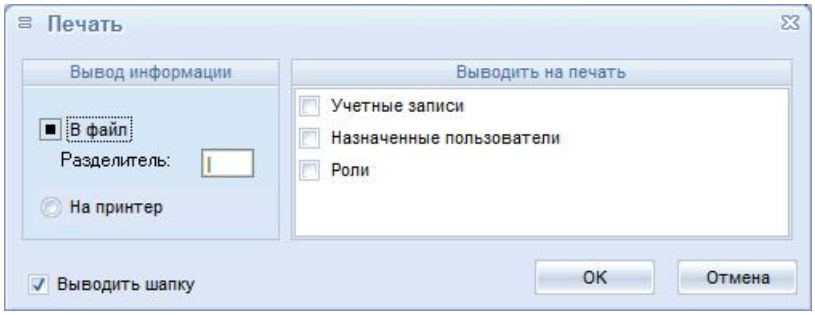

Рисунок 67 - Печать информации об учетной записи

Для добавления новой учетной записи нажать кнопку <Добавить>.

В появившемся окне, приведённом на рисунке 68, ввести имя учётной записи, указать роль, назначить пользователя (сотрудника как физического лица)[1], которому соответствует данная учетная запись, имя пользователя[2], ввести пароль и подтвердить его ввод, назначить пользователю идентификатор, полное имя пользователя[3] и выбрать компьютеры, на которых будет создана данная учётная запись. После ввода этих параметров нажать кнопку <Применить>.

[1] Действительные имя, фамилия и отчество соответствующего сотрудника регистрируются Администратором РАУ во время выполнения процедуры добавления нового пользователя в соответствии с документом 11443195.4012-053 90 «Руководство Администратора РАУ».

[2] Логин в базе пользователей АМДЗ.

[3] Имя пользователя в домене.

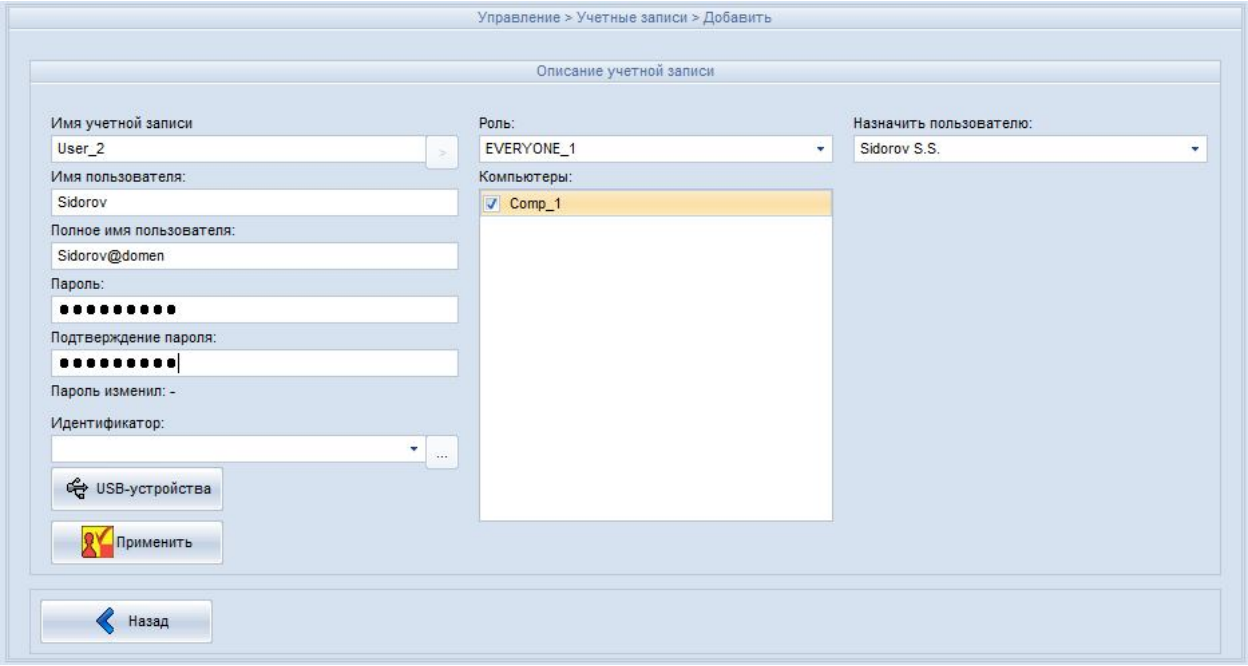

Рисунок 68 - Добавление новой учетной записи

При регистрации ПКО система создаёт «свою» учетную запись «ASM_ACCOUNT» в группе «Администраторы», с помощью которой становится возможным выполнение следующих операций: добавление, удаление пользователей, смена пароля пользователя и т. д. Данный механизм никак не связан с информацией, которая устанавливается в разделе «Результаты И/А» программы ACED32. Информация, установленная в разделе «Результаты И/А» определяет, какая информация о пользователе, полученная в результате процесса идентификации или аутентификации, передается из контроллера в программную подсистему разграничения доступа. Т.е. для успешного выполнения процедуры «Автологин» (процедуры, при которой пользователь авторизуется на аппаратном уровне, а программная часть автоматически подгружает его профиль доступа) необходимо включить первые пять флагов в разделе «Результатов И/А» (подробнее смотри документ 11443195.4012-036 97 «Установка правил разграничения доступа. Программа ACED32»).

Чтобы отредактировать настройки учетной записи, нужно выделить её и нажать кнопку <Редактировать> на вкладке «Учётные записи» (рисунок 65). В появившемся окне, приведённом на рисунке 69, следует изменить параметры учётной записи.

Примечание. Во вкладке «Учётные записи > Редактировать» при выборе роли для редактируемой учётной записи отображаются только те компьютеры, которые принадлежат такому же технологическому участку, как и выбранная роль.

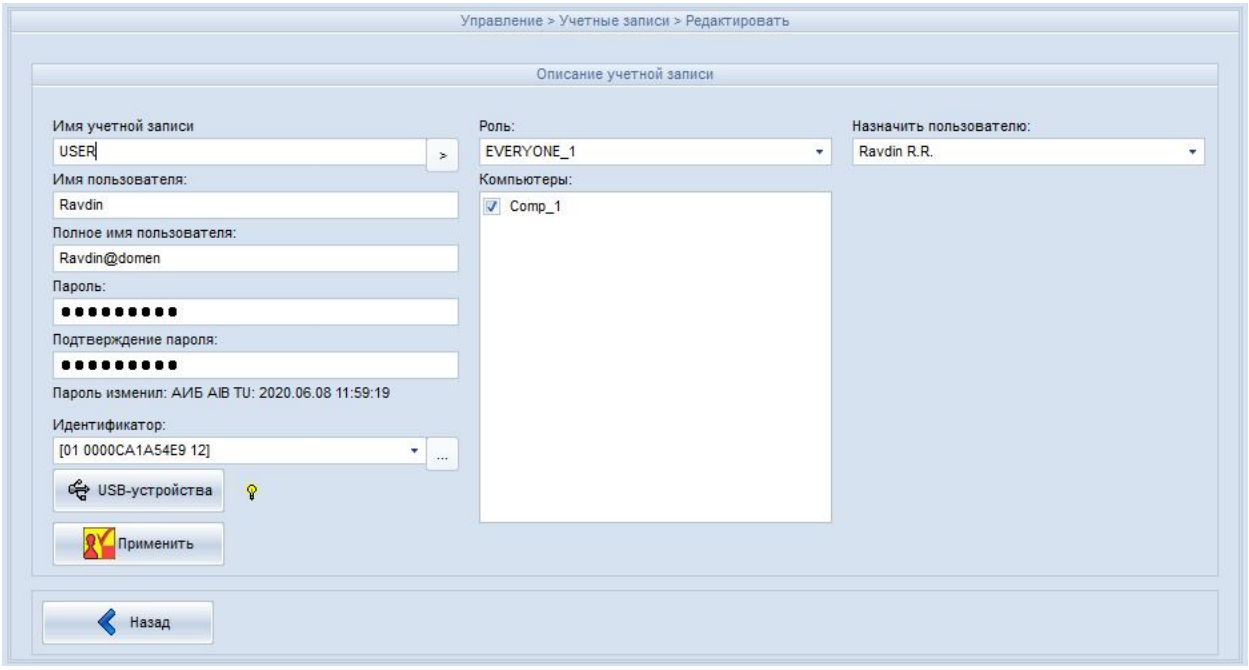

Рисунок 69 – Редактирование учётной записи

При нажатии кнопки <USB-устройства> будет выведено окно, приведённое на рисунке 70.

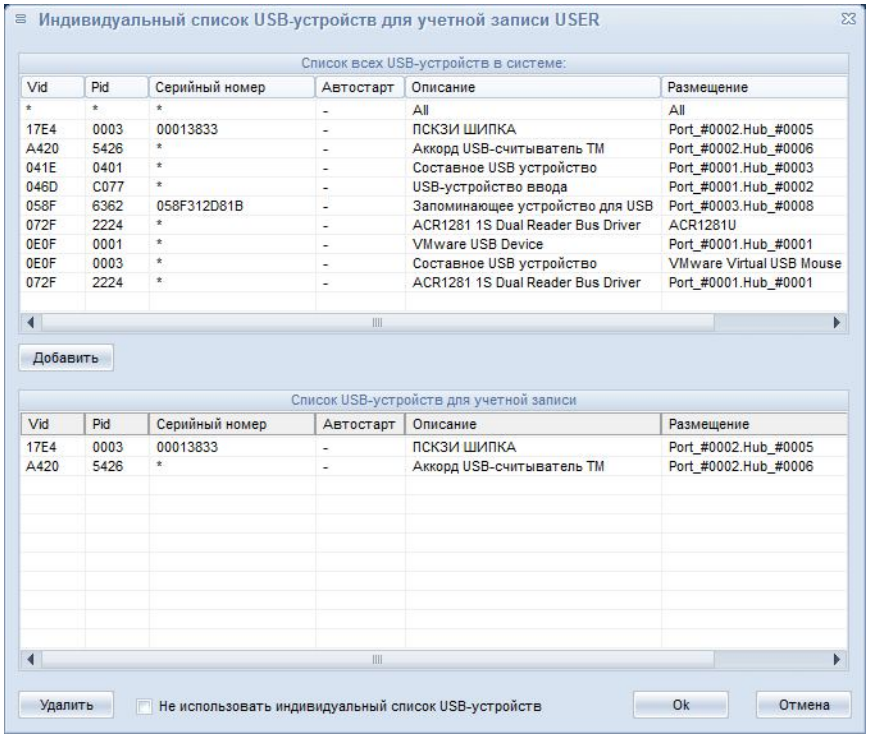

Рисунок 70 - Настройка списка разрешённых USB-устройств для учётной записи

В верхней части окна приведён список всех USB-устройств в РАУ. В нижней части окна – список разрешённых USB-устройств учётной записи.

Для добавления USB-устройства в список разрешённых USB-устройств выделить его в верхнем списке и нажать кнопку <Добавить>.

Для удаления USB-устройства из списка разрешённых учётной записи USB-устройств выделить его в нижнем списке и нажать кнопку <Удалить>.

Установка флажка «Не использовать индивидуальный список USB-устройств» активирует режим управления доступом к USB-устройствам на уровне учётных записей. При этом «загорается» индикатор – лампочка (рисунок 69).

Снятие флажка «Не использовать индивидуальный список USB-устройств» активирует режим управления доступом к USB-устройствам на уровне ролей. Индикатор - лампочка в окне, приведённом на рисунке 69, при этом «гаснет».

После завершения редактирования необходимо нажать кнопку <Применить>.

В РАУ предусмотрена возможность автоматического редактирования параметров учётной записи пользователя системы при выполнении процедуры удаления пользователя (выполняет Администратор РАУ согласно документу «11443195.4012-053 90. Руководство Администратора РАУ»). При выполнении процедуры удаления пользователя системы в параметрах учётных записей, назначенных данным пользователям, содержимое поля «Назначить пользователю» аннулируется.

ВНИМАНИЕ! Имеется возможность автоматической коррекции базы пользователей РАУ (файлы *.acc) в части редактирования параметров учётных записей. Для этого в командной строке следует выполнить AsmT.exe /fix (рисунок 71).

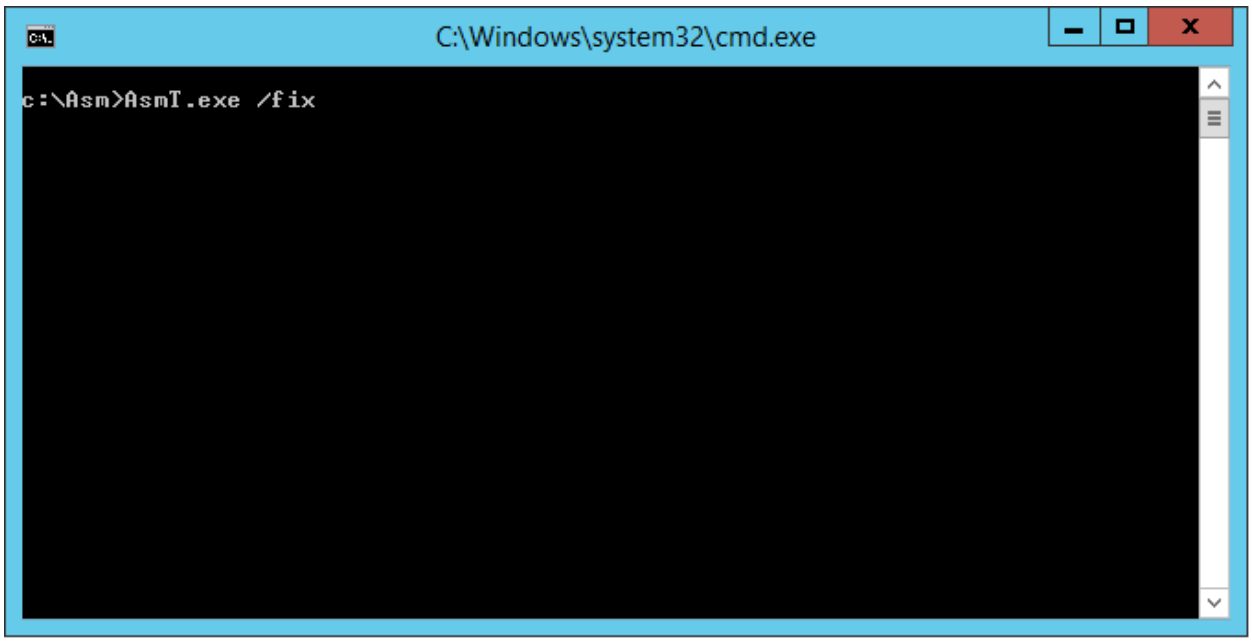

Рисунок 71 – Запуск утилиты AsmT.exe с параметром /fix

По выполнении данной команды происходит автоматическая проверка наличия файлов ролей у учётных записей РАУ. Если соответствующие файлы у каких-либо учётных записей отсутствуют, содержимое поля «Роль» в параметрах соответствующих записей аннулируется, при этом появляется сообщение:

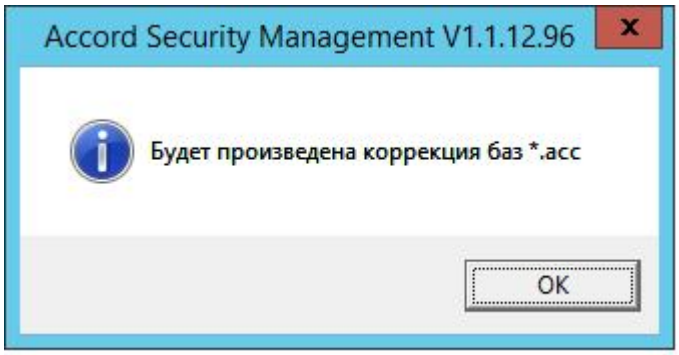

Рисунок 72 – Сообщение о начале выполнения процедуры коррекции базы пользователей РАУ

При нажатии кнопки <OK> выполняется процедура коррекции базы пользователей РАУ, по завершении которой появляется сообщение:

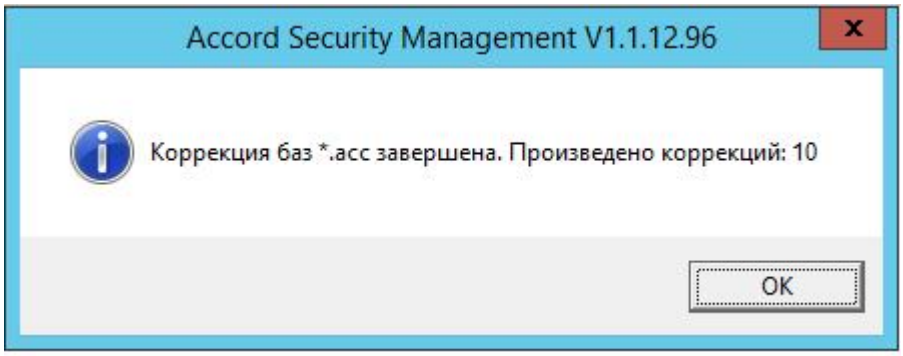

Рисунок 73 – Сообщение о завершении процедуры коррекции базы пользователей РАУ

ВНИМАНИЕ! В ASM реализована функция централизованной смены паролей учетных записей пользователей ПКО. Для этого во вкладке «Учётные записи > Редактировать» следует изменить пароль учётной записи пользователя ПКО, затем выполнить процедуру передачи базы пользователей на ПКО (подробнее смотри подраздел 4.4). При изменении пароля пользователя, если редактируется существующая учетная запись или если для редактируемой учетной записи назначены два и более ПКО, выводится сообщение о необходимости передачи обновленных баз пользователей на ПКО, приведенное на рисунке 74.

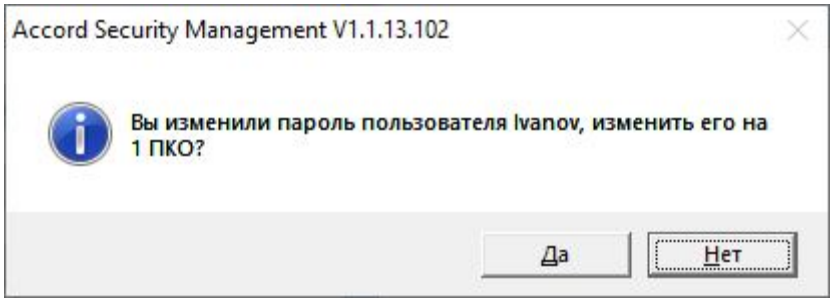

Рисунок 74 – Сообщение о необходимости передачи обновленных баз пользователей на ПКО

При нажатии кнопки <Да> выполняется процедура передачи базы пользователей (с новым паролем) на те ПКО, на которых зарегистрирован пользователь.

Во вкладке «Учётные записи > Редактировать» отображается информация о дате, времени и имени учётной записи (персонала РАУ либо пользователя), выполнившего процедуру смены пароля. Данная информация отображается в поле «Пароль изменен».

Базы учётных записей пользователей ПКО хранятся на СЦУ в каталоге C:\ASM\TEMPLATE\. При удалении или обновлении ПО сервера базы учётных записей не удаляются.

Администратор ИБ технологического участка может изменить свой пароль. Для этого во вкладке «Учётные записи» следует выбрать учётную запись Администратора ИБ технологического участка и нажать кнопку <Редактировать>. Затем в появившемся окне изменить пароль.

При выходе из ASM для Администратора ИБ технологического участка появляется сообщение, приведённое на рисунке 75.

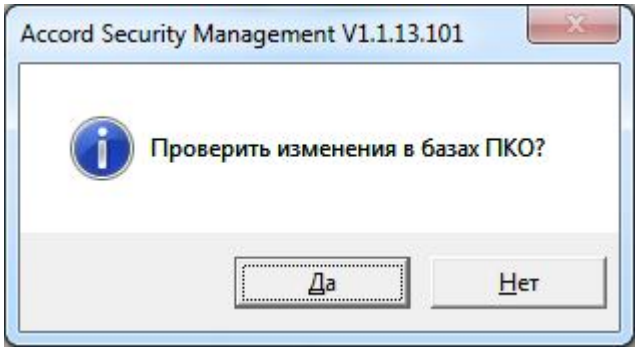

Рисунок 75 – Предложение о проведении проверки на наличие изменений баз пользователей ПКО

При нажатии в этом сообщении кнопки <Да> выполняется проверка наличия изменений в базе ASM. Если Администратор ИБ технологического участка изменил базы пользователей и не передал эти изменения на ПКО, при выходе из ASM появляется соответствующее оповещение. При этом в строке состояния отображается счетчик ПКО, для которых осуществляется проверка изменений баз пользователей.

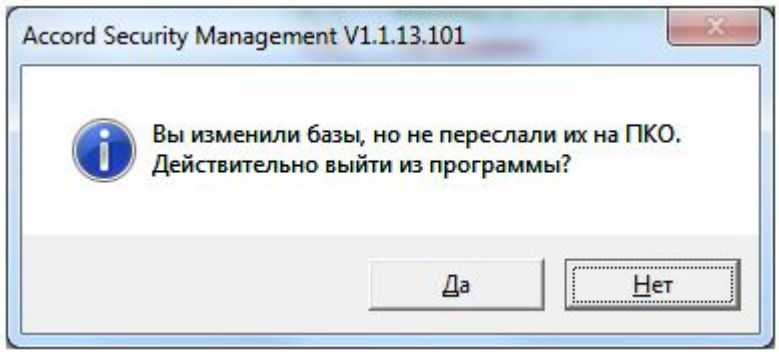

Рисунок 76 –Оповещение о необходимости передачи обновленных баз пользователей на ПКО

При нажатии кнопки <Нет> появляется окно для пересылки баз пользователей на ПКО (рисунок 47).

Чтобы удалить учётную запись, следует её выделить и нажать кнопку <Удалить> (вкладка «Учётные записи») (рисунок 65). Появится окно подтверждения этого действия (рисунок 77).

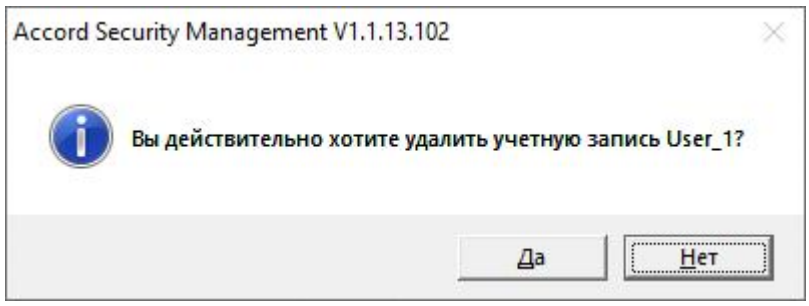

Рисунок 77 - Окно подтверждения удаления учетной записи

В РАУ при выполнении процедуры удаления учётной записи пользователя системы автоматически выполняется процедура редактирования параметров пользователя, которому принадлежала данная учётная запись. При этом содержимое поля «Учётная запись» для текущего пользователя аннулируется (п. 4.2).

Также в РАУ имеется возможность автоматического редактирования параметров компьютера при выполнении процедур удаления учётной записи пользователя и самого пользователя системы (последнее выполняет Администратор РАУ согласно документу «11443195.4012-053.90. Руководство Администратора РАУ»). При этом в параметрах учётных записей, назначенных компьютеру (п. 4.4) содержимое полей «Учётная запись», «Пользователи» аннулируется.

Если необходимо определить, какой учетной записи принадлежит данный идентификатор, следует нажать кнопку <Поиск> на вкладке «Учетные записи» (рисунок 65). Появится окно с сообщением «Предъявите идентификатор» (рисунок 78).

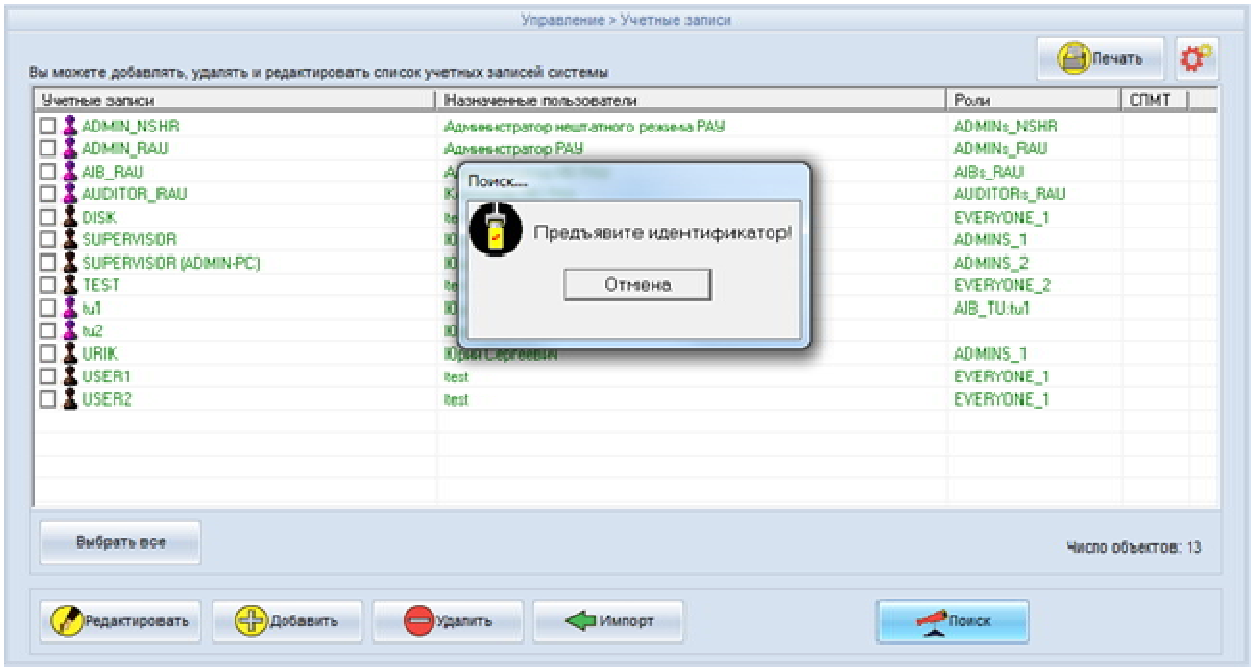

Рисунок 78 - Окно с сообщением «Предъявите идентификатор»

Если данный идентификатор назначен какой-либо учетной записи, эта учетная запись будет выделена (рисунок 79), в ином случае в нижней части окна появится сообщение «Идентификатор не зарегистрирован!» (рисунок 80).

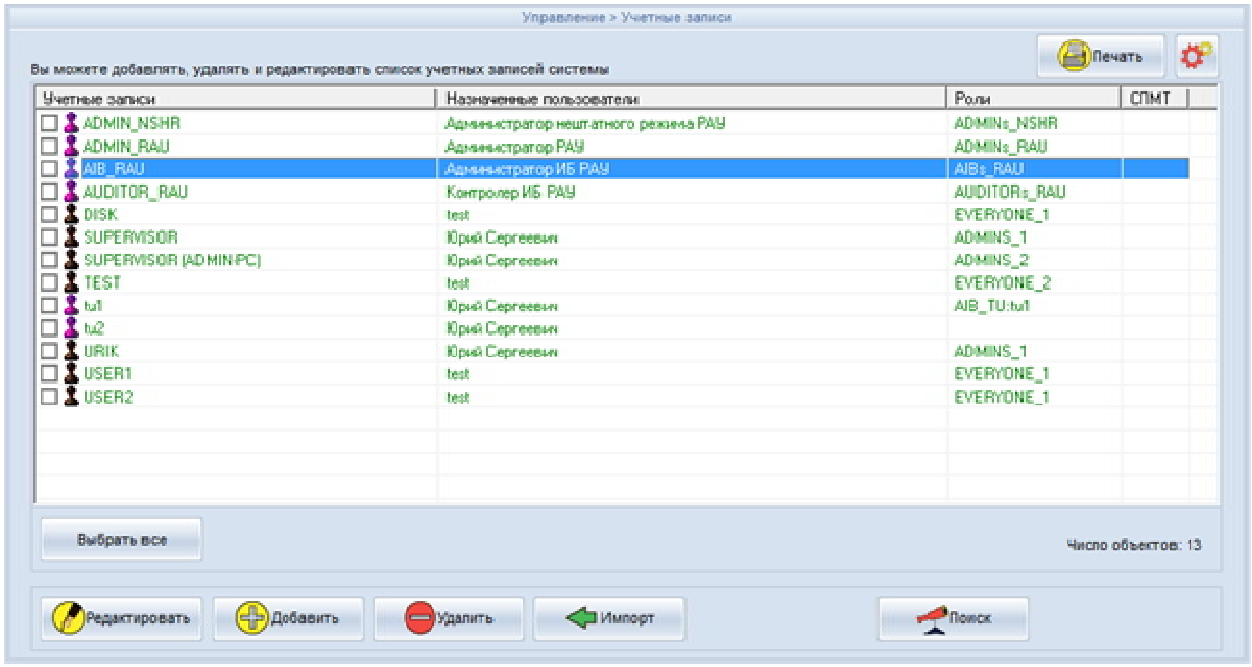

Рисунок 79 - Учётная запись, которой назначен идентификатор

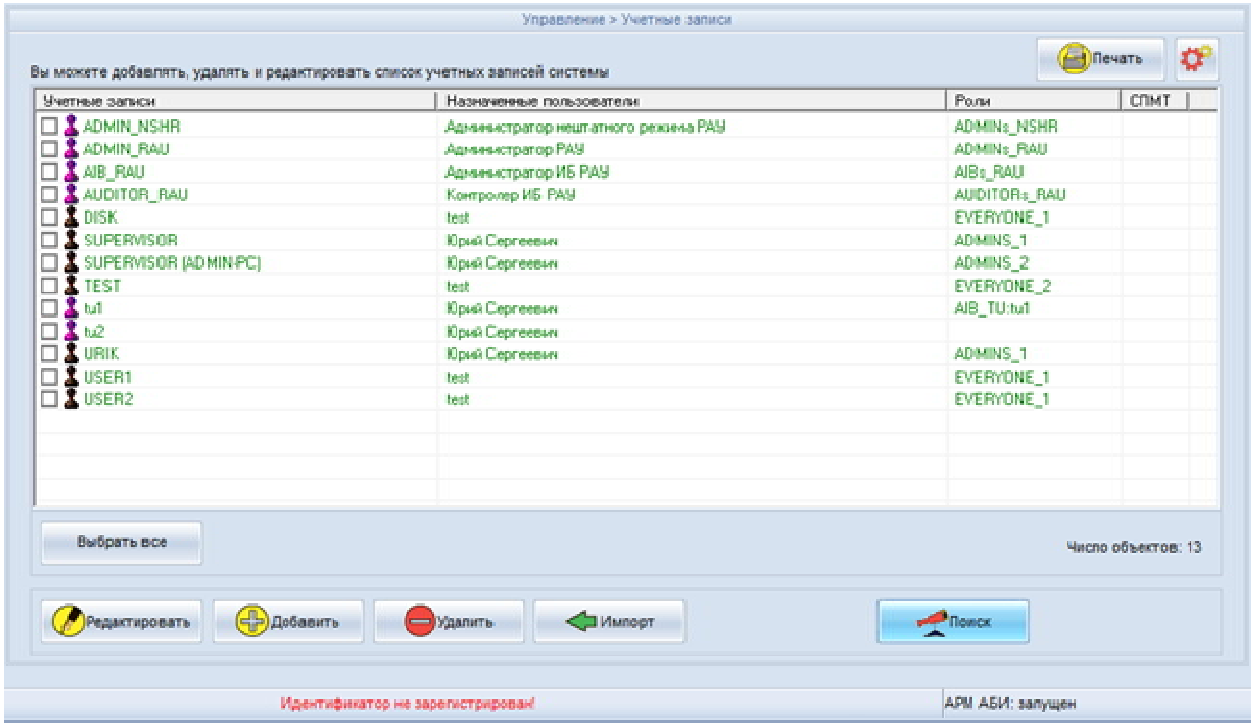

Рисунок 80 - Сообщение о том, что идентификатор не зарегистрирован

Для получения данных об учётных записях пользователей ПКО в рамках централизованной схемы необходимо во вкладке «Учетные записи» нажать кнопку <Импорт> (рисунок 65). Далее в появившемся окне (рисунок 81) выбрать флаг «Вы можете импортировать учетные записи из:» - «базы пользователей NT».

В этом окне следует ввести IP-адрес или имя сервера, из базы пользователей которого будут импортированы учётные записи, а также имя и пароль Администратора данного сервера.

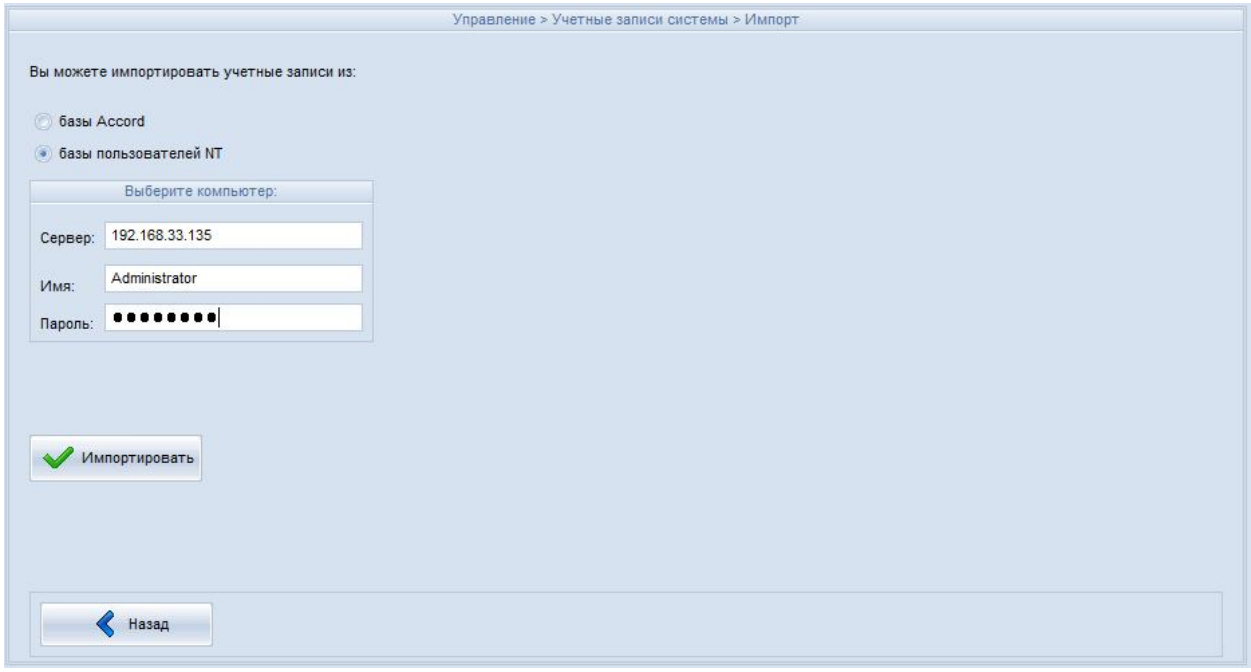

Рисунок 81 - Ввод данных о сервере, из базы пользователей которого будут импортированы учетные записи

После этого в правой части окна появятся импортированные учетные записи, из которых следует выбрать необходимые для добавления в базу (для выбора всех учетных записей нужно нажать кнопку <Выбрать все>), и нажать кнопку <Добавить> (рисунок 82).

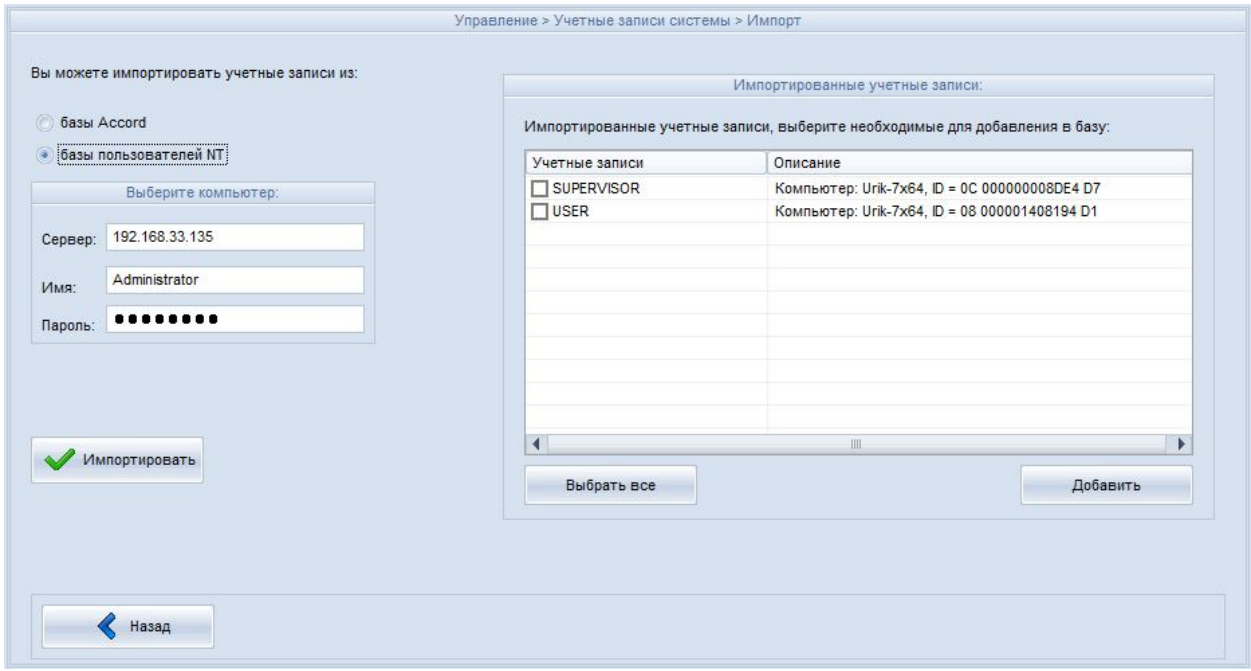

Рисунок 82 - Выбор импортированных учетных записей (импорт из базы пользователей NT)

Для получения данных об учетных записях пользователей ПКО технологического участка в рамках децентрализованной схемы используется функция экс-

порта списка пользователей СЗИ ПКО (чтобы функция экспорта стала доступной, на ПКО в файле «AcWs32.ini» необходимо установить параметр NoNetManaged=Yes или в главном окне программы регистрации рабочей станции (ACSETWS.EXE) установить флаг «Станция не управляется по сети»). При этом производится копирование перечня учетных записей на внешний носитель, в качестве которого может использоваться USB флэш-накопитель или флоппи-диск. Если в качестве внешнего носителя используется USB флеш-накопитель, то перед тем, как выполнить процедуру получения баз пользователей ПКО в рамках децентрализованной схемы, необходимо добавить флеш-накопитель в единую базу USB-носителей. Данная процедура выполняется Администратором РАУ в соответствии с документом 11443195.4012-053 90 «Руководство Администратора РАУ».

Чтобы передать базы пользователей, необходимо на ПКО в трее выбрать правой кнопкой мыши сетевой клиент ПАК «Аккорд» (рисунок 55), после чего появляется контекстное меню (рисунок 56).

Далее выбрать команду «Экспорт базы пользователей» (рисунок 56), после чего появляется сообщение «Предъявите идентификатор». Предъявить идентификатор Администратора «Аккорд» подконтрольного объекта.

После этого появится окно ввода пароля. Ввести пароль и нажать кнопку <OK> (рисунок 57).

После выполнения операции ввода пароля появляется окно выбора каталога для сохранения базы пользователей, приведённое на рисунке 83. В этом окне выбрать нужный каталог и нажать кнопку <OK>.

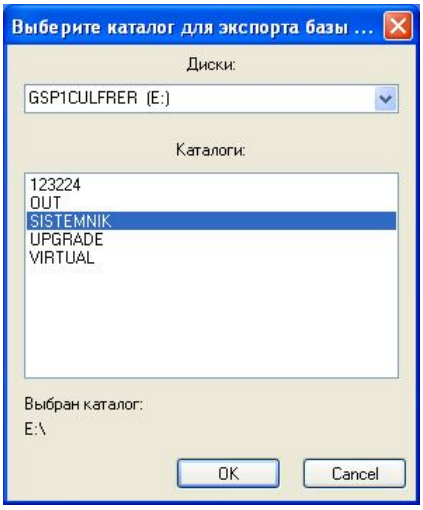

Рисунок 83 – Выбор каталога для сохранения базы пользователей

При импорте базы пользователей она сохраняется в каталог E:\IN\xxx\, где E – имя внешнего носителя, xxx – имя ПКО. В каталоге xxx сохраняются следующие файлы: xxx.AMZ – файл, содержащий базу пользователей ПКО; xxx.ini – файл, содержащий параметры конфигурации ПКО; www.act – файлы, содержащие списки задач, разрешенных для запуска пользователю, www – имя пользователя, для которого назначен список задач.

Примечание. Количество данных файлов зависит от количества пользователей ПКО, для которых назначен список задач для запуска.

Если описанная процедура выполнена успешно, появляется сообщение, приведённое на рисунке 84.

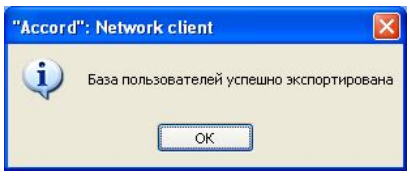

Рисунок 84 - Сообщение об успешном экспорте базы пользователей

Далее базы пользователей на внешнем носителе должны быть доставлены на СЦУ.

Если в окне, приведённом на рисунке 81, установить переключатель «Вы можете импортировать учётные записи из:» в положение «базы Accord», то при нажатии кнопки <Импортировать> будет выведено окно, приведённое на рисунке 85.

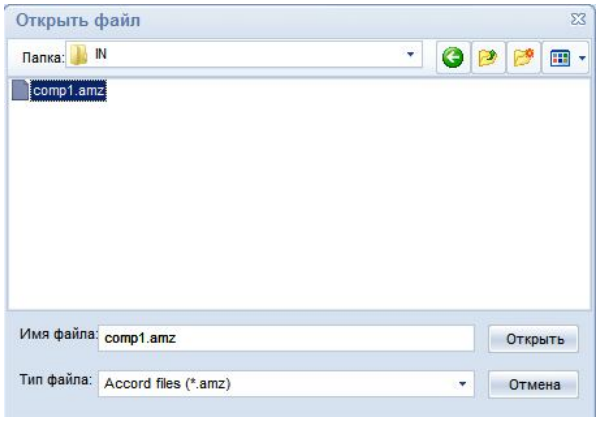

Рисунок 85 - Выбор файла *.amz, из которого необходимо импортировать учетные записи

В этом окне следует указать файл с именем ПКО, из которого необходимо импортировать учётные записи. По умолчанию предлагается открыть файл xxx.AMZ, где xxx – имя ПКО, из каталога E\IN\xxx\, где E – внешний носитель, xxx –

имя ПКО. После этого в правой части вкладки импорта учётных записей будет выведен список импортированных учётных записей, как показано на рисунке 86.

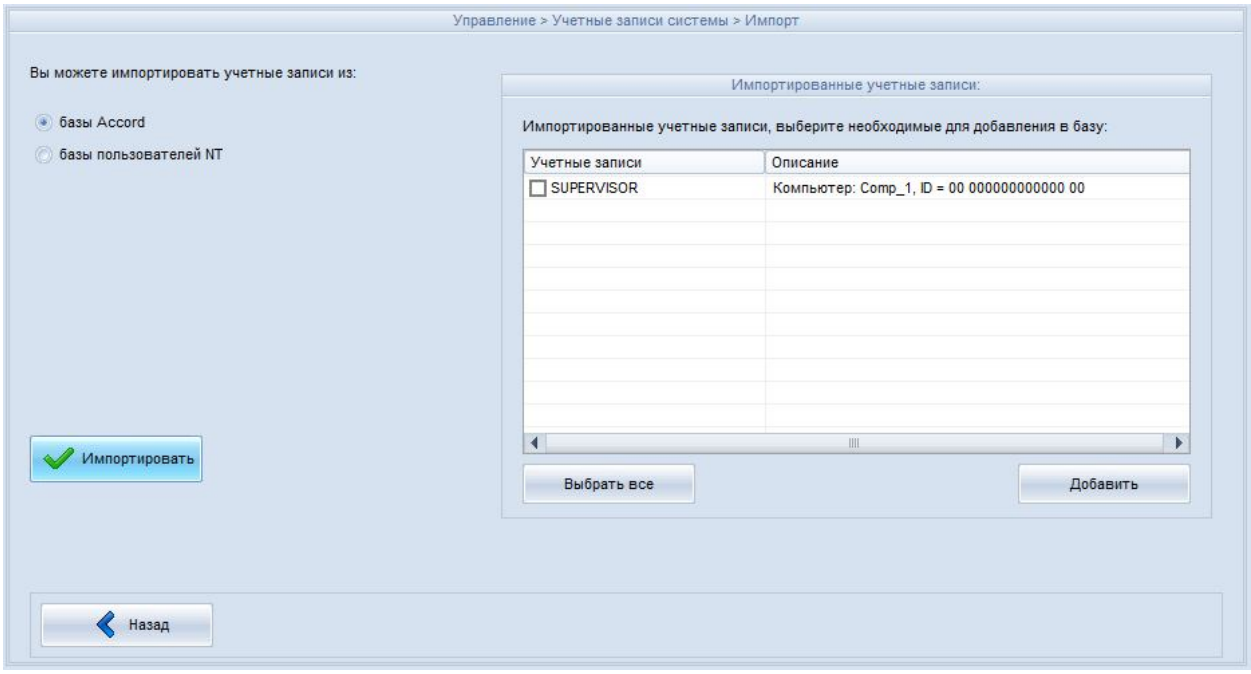

Рисунок 86 - Выбор импортированных учетных записей (импорт из базы «Аккорда»)

Из данных учётных записей следует выбрать те, которые нужно добавить в базу (для выбора всех учетных записей нужно нажать кнопку <Выбрать все>) и нажать кнопку <Добавить>.

При первом выполнении процедуры получения базы пользователей ПКО на СЦУ создается каталог C:\Asm\ACCONET\IN\CompName (где «CompName» – имя ПКО), в котором хранятся файлы базы пользователей ПКО. СЦУ принимает файлы базы пользователей ПКО (состоящие из файлов CompName.amz, CompName.ini, CompName.ver, *.act) только при наличии изменений в базе пользователей ПКО: если различие между файлами, хранящимися на ПКО, и файлами в каталоге C:\Asm\ACCONET\IN\CompName отсутствует, то файлы не принимаются.

4.6 Создание пользователя технологического участка

До выполнения процедуры создания пользователя технологического участка должны быть выполнены следующие действия:

- создание пользователя. Выполняется Администратором РАУ в соответствии с документом 11443195.4012-053 90 «Руководство Администратора»;

- создание технологического участка. Выполняется Администратором ИБ в соответствии с документом 11443195.4012-053 91 «Руководство Администратора ИБ»;

- создание Администратора ИБ технологического участка. Выполняется Администратором ИБ в соответствии с документом 11443195.4012-053 91 «Руководство Администратора ИБ».

Администратор ИБ технологического участка должен выполнить следующие действия:

- добавить идентификатор для пользователя технологического участка. Данная операция выполняется в соответствии с подразделом 4.3 настоящего документа;

- добавить компьютер для пользователя технологического участка. Данная операция выполняется в соответствии с подразделом 4.4 настоящего документа;

- создать учетную запись пользователя технологического участка, указав имя пользователя и назначив ему роль, компьютер и идентификатор. Данная операция выполняется в соответствии с подразделом 4.5 настоящего документа.

Чтобы создать пользователя технологического участка, необходимо выполнить следующие действия:

- на подконтрольном объекте создать пользователя «Гл.Администратор» и других пользователей (выполняет Администратор ИБ ПКО);

- на СЦУ создать пользователей. Данную операцию выполняет Администратор РАУ в соответствии с документом 11443195.4012-053 90 «Руководство Администратора»;

- создать технологический участок. Данную операцию выполняет Администратор ИБ в соответствии с документом 11443195.4012-053 91 «Руководство Администратора ИБ»;

- во вкладке «Учётные записи» импортировать учётные записи пользователей ПКО кнопкой <Импорт>. Данную операцию выполняет Администратор ИБ технологического участка в соответствии с подразделом 4.5 настоящего документа;

- выполнить операцию редактирования учётных записей пользователей ПКО, в рамках которой необходимо назначить созданного Администратором РАУ пользователя редактируемой учётной записи. Данную операцию выполняет

Администратор ИБ технологического участка в соответствии с подразделом 4.5 настоящего документа;

- сохранить изменения. Данную операцию выполняет Администратор ИБ технологического участка в соответствии с подразделом 4.5 настоящего документа;
- передать базу пользователей на ПКО Данную операцию выполняет Администратор ИБ технологического участка в соответствии с подразделом 4.5 настоящего документа.

4.7 Работа с журналами

4.7.1 Общие сведения

В РАУ существуют журналы трех типов:

- оперативный журнал;
- журнал ASM;
- журнал АРМ АБИ.

4.7.2 Оперативный журнал

4.7.2.1 Общие сведения

В оперативном журнале содержатся следующие сведения о действиях пользователей на рабочих местах:

- вход / выход пользователя ПКО;
- статус ПКО;
- настройки ПАК «Аккорд» на ПКО;
- сообщения о подключении / отключении USB-устройств;
- информация о выполняемых файловых операциях;
- информация о выполняемых операциях с реестром.

Каждая запись оперативного журнала содержит следующие поля:

- имя подконтрольной рабочей станции, на которой произошло событие;
- дата и время, когда произошло событие;
- имя процесса, выполнившего операцию;

- имя пользователя, совершившего действие, вызвавшее генерацию события;
- сообщение о событии, генерируемое ПАК СЗИ от НСД «Аккорд» подконтрольной рабочей станции. Перечень возможных сообщений приведен в разделе 7;
- тип события. Информация о возможных типах сообщений приведена в разделе 7;
- описание (комментарий) к событию.

Информация оперативных журналов находится на СЦУ в следующих файлах:

- «AcSetup_YYY.log», где YYY – дата и время формирования файла. Файлы хранятся в каталоге ASM/ACCONNET/Client.Log/XXX/<дата>, где XXX – имя каталога, соответствующего имени ПКО, <дата> - дата создания файла журнала. В файлах хранится информация об активации и снятии защиты ПАК СЗИ от НСД «Аккорд» на рабочей станции
- «**********.LOW», где «**********» – дата и время формирования файла с точностью до секунды, например, 18_01_2013/20131005172617.LOW. Файлы хранятся в каталоге ASM/ACCONNET/Client.Log/XXX/YYY/, где XXX – имя каталога, соответствующего имени ПКО, YYY – имя каталога, соответствующего дате в формате дата – месяц- год. В файлах хранится вся информация оперативного журнала, не записываемая в файл «AcSetup_YYY.log».

При передаче оперативных событий на СЦУ автоматически выполняется удаление переданных файлов оперативных журналов AcSetup_YYY.log с ПКО с последующим их перемещением (архивированием) в каталог \Accord.NT\Client.arc (или \Accord.x64\Client.arc в 64-битных ОС), расположенный на ПКО.

ВНИМАНИЕ! Чтобы по выполнении передачи оперативных событий с ПКО на СЦУ автоматически выполнялась процедура архивирования переданных файлов оперативных журналов AcSetup_YYY.log, необходимо параметру RenameLow в файле конфигурации \Asm\LogConfig.ini присвоить значение «Yes», а параметру DeleteLow в файле конфигурации \Asm\LogConfig.ini присвоить значение «No».

Оперативный журнал обновляется в режиме реального времени.

Сбор оперативных журналов происходит в автоматическом режиме.

ВНИМАНИЕ! Для сбора журналов ПКО и их передачи в ядро СОИБ ASM должен быть запущен!

Окно, отображающее оперативный журнал, приведено на рисунке 87.

Администратор ИБ технологического участка выполняет следующие функции:

- просмотр сообщений оперативного журнала на СЦУ. Данная функция описана в пункте 4.7.2.2;
- конвертирование оперативного журнала. Данная функция описана в пункте 4.7.2.3;
- экспортирование оперативного журнала. Данная функция описана в пункте 4.7.2.4;
- импортирование оперативного журнала. Данная функция описана в пункте 4.7.2.5;
- настройка индивидуального почтового адреса и фильтра событий для передачи в оперативный журнал. Данная функция описана в пункте 4.7.2.6.

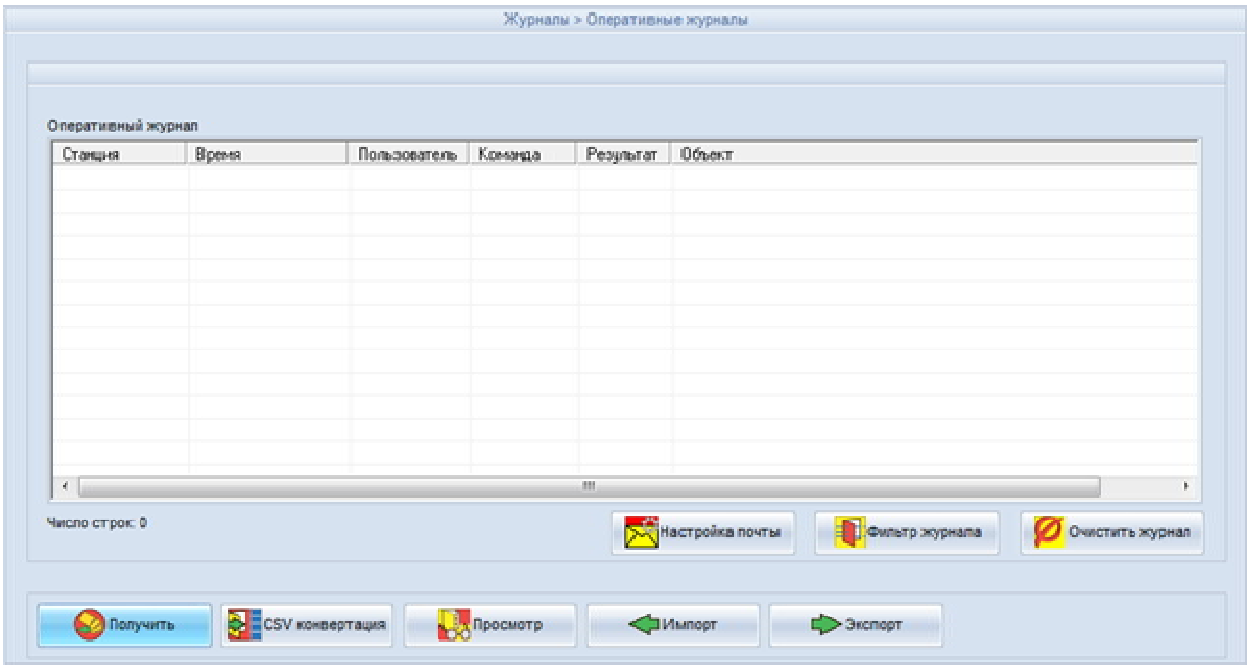

Рисунок 87 - Оперативные журналы

4.7.2.2 Просмотр сообщений оперативного журнала

Администратор ИБ технологического участка может просматривать оперативные журналы только тех ПКО, которые входят в состав его технологического участка.

Для просмотра оперативного журнала на СЦУ необходимо в окне, приведённом на рисунке 87, нажать кнопку <Просмотр>. Появляется окно выбора журналов, приведённое на рисунке 88.

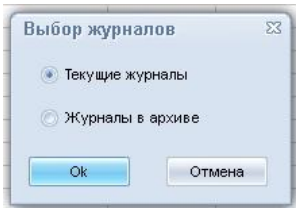

Рисунок 88 - Выбор журналов для просмотра

В данном окне осуществляется выбор журналов для просмотра: «Текущие журналы» позволяет выбрать файлы журналов в каталоге \Asm\AcConNet\Client.Log, «Журналы в архиве» – файлы журналов в каталоге \Asm\AcConNet\Client.Arc. При нажатии кнопки <Ok> будет выведено окно просмотрщика журналов событий с окном указания конкретного файла журнала. Примерный вид данных окон приведён на рисунке 89.

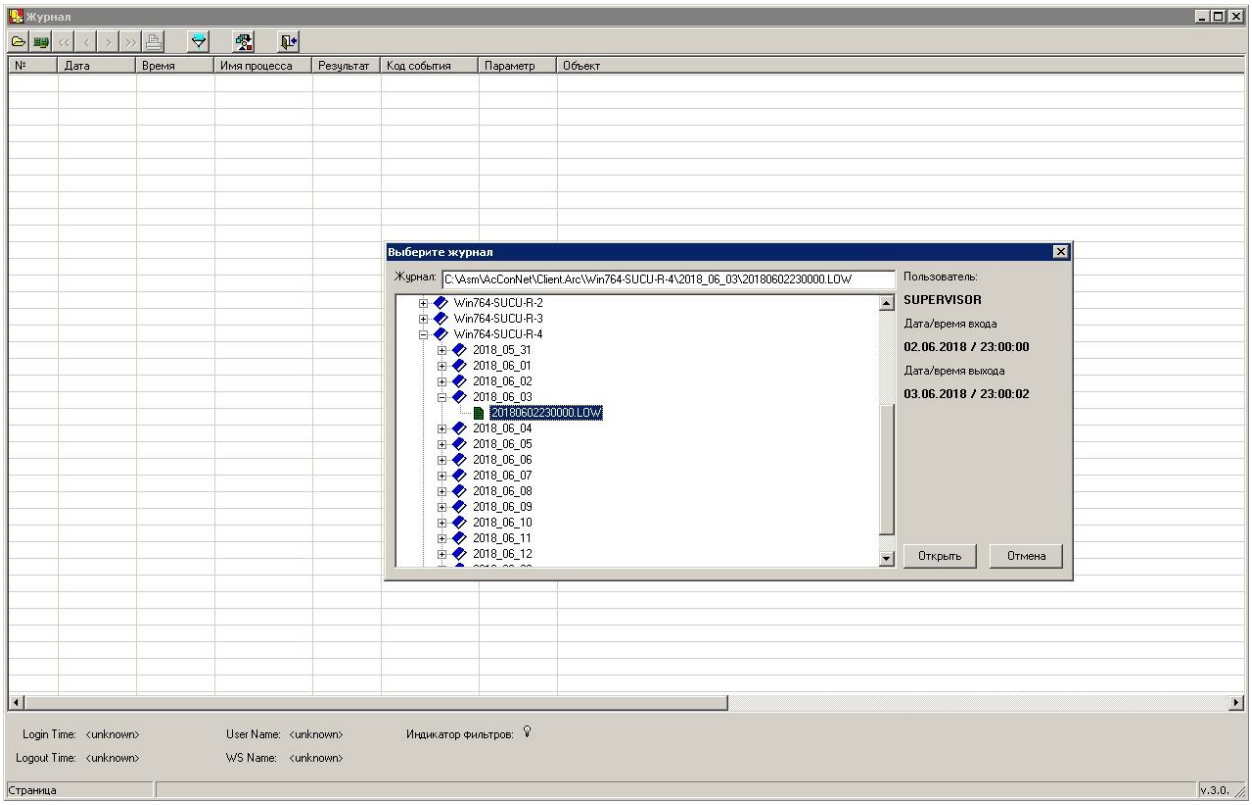

Рисунок 89 - Окно просмотрщика журналов событий

4.7.2.3 Конвертирование оперативного журнала

Администратору ИБ технологического участка предоставляется возможность конвертирования оперативного журнала в файл формата *.CSV или *.XML.

Формат, в который будет конвертироваться журнал, выбирается в настройках фильтров подсистемы управления событиями информационной безопасности. Для конвертирования оперативного журнала необходимо в окне, приведенном на рисунке 87, нажать кнопку <CSV конвертация> или <XML конвертация> (в зависимости от выбранного формата файла экспорта). После этого в каталоге, указанном в поле «CSV файл для конвертации журналов:» или в поле «XML файл для конвертации журналов», будет создан файл выбранного формата, содержащий данные оперативного журнала. В данный файл помещаются все события из оперативных журналов. В зависимости от настроек параметров экспорта журналов после конвертации всё содержимое журналов может перемещаться в архив – каталог Asm\AcConNet\Client.Arc.

По завершении процедуры преобразования оперативного журнала в общепринятые форматы на экране появляется соответствующее сообщение:

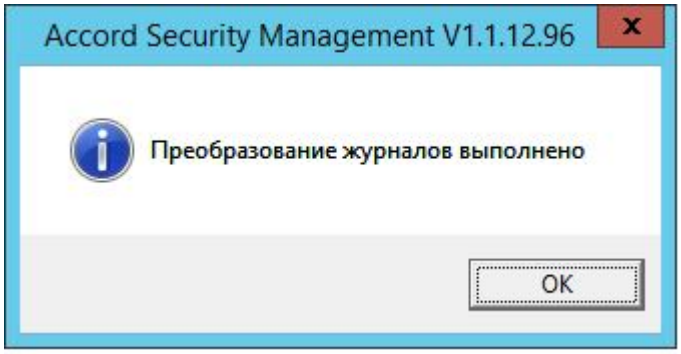

Рисунок 90 – Сообщение о выполненной процедуре конвертации оперативного журнала в общепринятые форматы

При выполнении этой процедуры кнопками <CSV конвертация> или <XML конвертация> в консоли AsmT.exe информация о выполненной процедуре (дата и время запуска и окончания процедуры конвертации, список конвертированных файлов оперативного журнала) записывается в журнал Low2XmlCsv.log (рисунок 91).

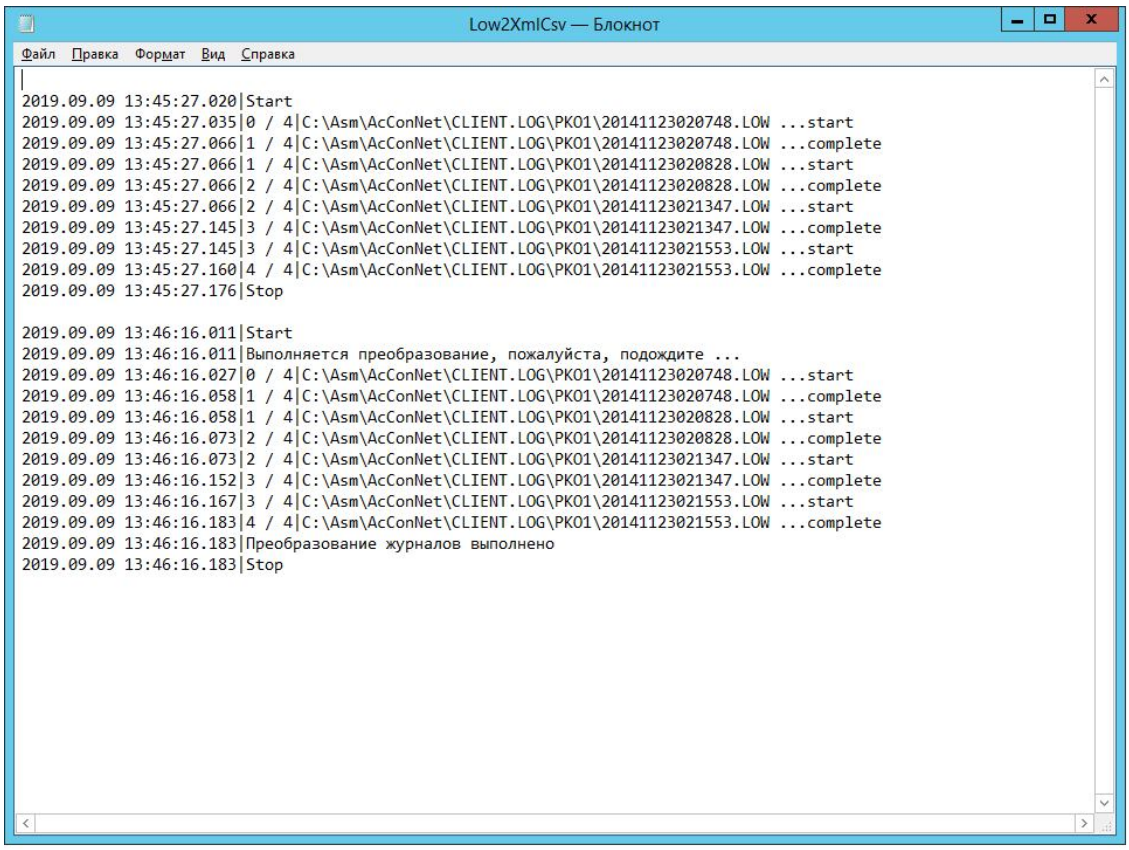

Рисунок 91 – Журнал Low2XmlCsv.log после выполнения процедуры конвертации кнопками <CSV конвертация> или <XML конвертация> в консоли AsmT.exe

Процедуру конвертации оперативного журнала также можно выполнить с помощью утилиты Low2XmlCsv.exe[1]. Информация о выполненной процедуре также записывается в журнал Low2XmlCsv.log[2] (однако при этом в журнале не отображаются сообщения о начале и окончании выполнения преобразования журналов, рисунок 92).

[1] Утилита находится в каталоге C:\Asm.

[2] После каждой последующей конвертации оперативного журнала информация о процедуре добавляется в файл журнала Low2XmlCsv.log.

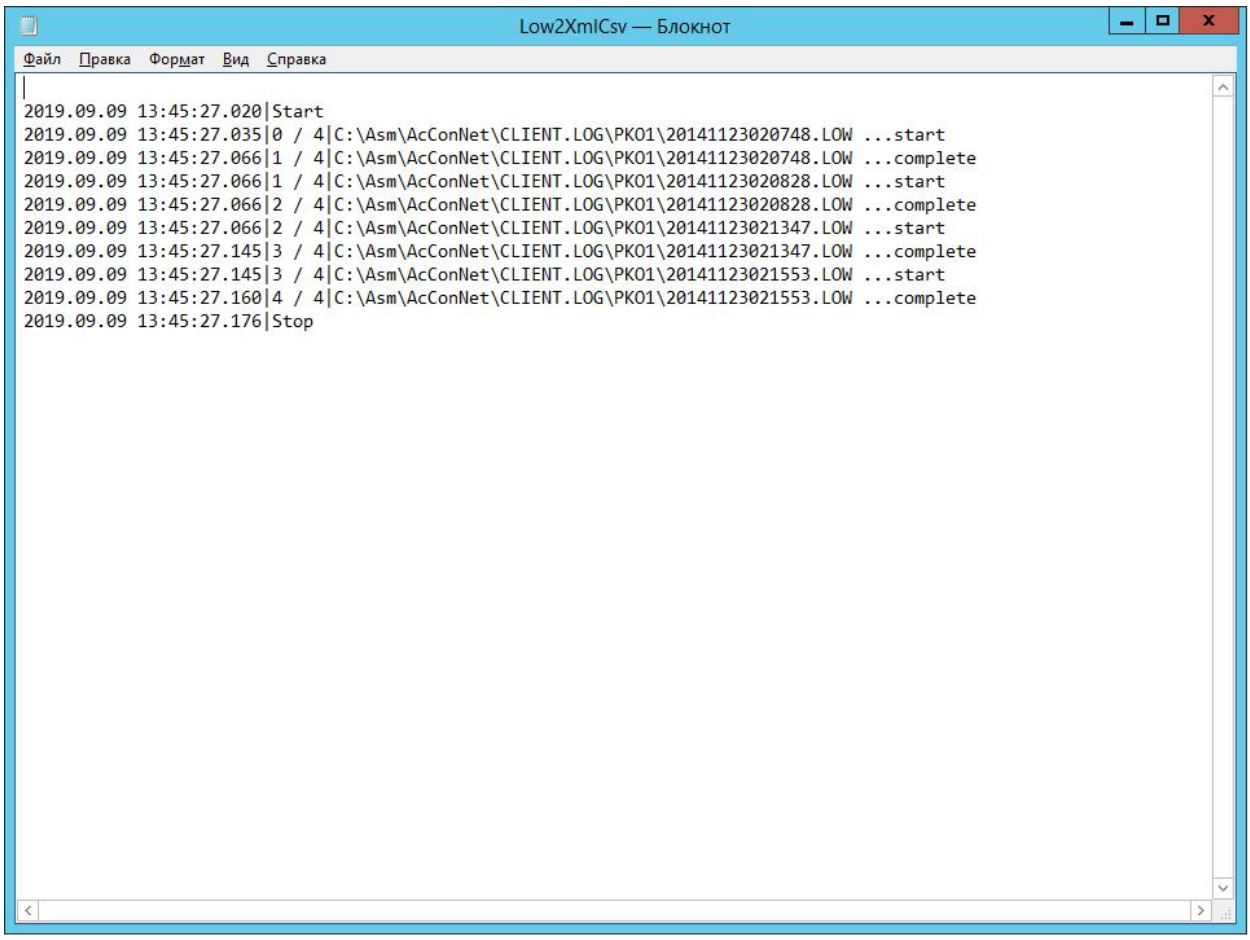

Рисунок 92 - Журнал Low2XmlCsv.log после выполнения процедуры конвертации с помощью утилиты LowToCsvXml.exe

В РАУ отсутствует возможность одновременного выполнения процедуры конвертации оперативного журнала и кнопкой <CSV конвертация> (или <XML конвертация>) консоли AsmT.exe, и с помощью утилиты Low2XmlCsv.exe.

ВНИМАНИЕ! В РАУ при попытке запуска процедуры конвертации оперативного журнала во время выполнения текущего процесса конвертации появляется следующее сообщение:

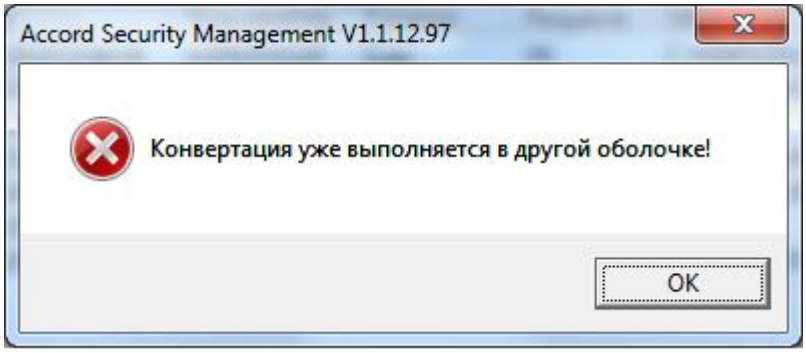

Рисунок 93 – Сообщение о невозможности запуска консоли при выполнении процедуры конвертации

ВНИМАНИЕ! Файл *.csv по умолчанию имеет разделители в виде символа «=». Чтобы изменить данный символ разделителя на любой другой, следует в файле asm.ini в секции «TCIM» изменить значение параметра «Separator».

4.7.2.4 Экспортирование оперативного журнала

Чтобы экспортировать оперативный журнал (например, для дальнейшего анализа в системах мониторинга), необходимо в окне, приведённом на рисунке 87, нажать <Экспорт>. Появляется окно выбора каталога. Выбрав каталог для экспорта журнала, следует нажать <Применить>.

4.7.2.5 Импортирование оперативного журнала

Для сбора журналов ПКО в децентрализованном режиме используется функция экспорта журналов СЗИ от НСД ПКО. При этом осуществляется копирование журналов на отчуждаемый носитель, например, USB-носитель, в каталог <выбранный_каталог>:\IN\<имя_станции>\, где <выбранный_каталог> – каталог на внешнем носителе, <имя_станции> – имя станции с которой экспортируется данный журнал.

Содержащий экспортируемые журналы отчуждаемый носитель доставляется на СЦУ. Администратор ИБ, получив данный носитель, выполняет следующие действия:

- подключает полученный отчуждаемый носитель к СЦУ. При использовании в качестве отчуждаемого USB-носитель необходимо добавить его в единую базу USB-носителей. Данная процедура выполняется Администратором РАУ в соответствии с документом «11443195.4012-053 90. СПО СЗИ НСД «Аккорд-РАУ». Руководство Администратора».
- копирует журналы с отчуждаемого носителя на СЦУ;
- в окне «Оперативные журналы», приведённом на рисунке 87, нажимает <Импорт>;
- в появившемся окне выбирает необходимый каталог и нажимает <Применить>.

4.7.2.6 Настройка индивидуального почтового адреса и фильтра событий для передачи в оперативный журнал

Для настройки индивидуального механизма передачи информации о событиях НСД необходимо на вкладке «Настройка > Оперативный журнал» нажать кнопку <Настройка> в поле «При возникновении НСД» (рисунок 94).

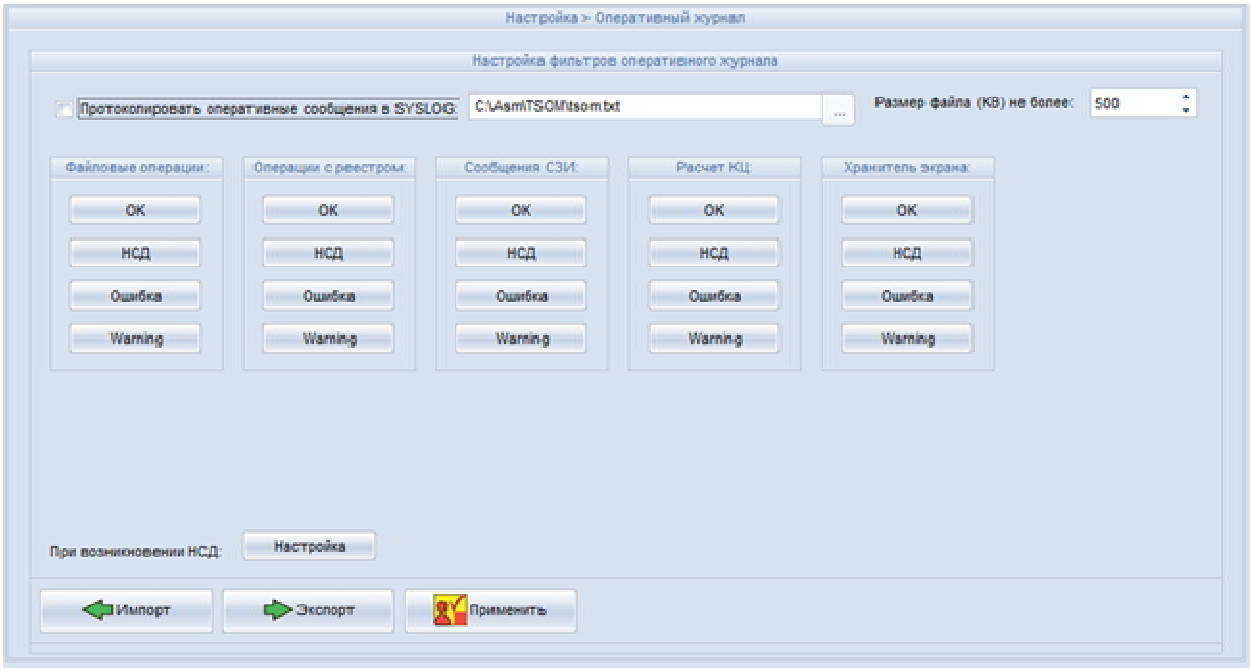

Рисунок 94 - Вкладка Настройка > Оперативный журнал

В появившемся окне настройки реакции на НСД (рисунок 95) следует выставить галочку в поле «Отправлять на почту».

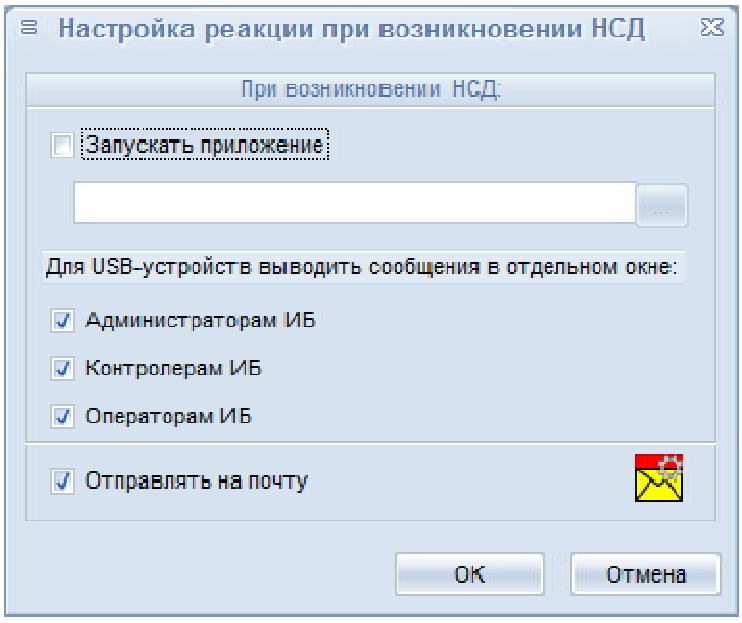

Рисунок 95 - Настройка реакции при возникновении НСД

Далее на вкладке Журналы > Оперативные журналы (рисунок 87) нажать кнопку <Настройка почты>. При ее нажатии появится окно настройки индивидуальной почты (рисунок 96).

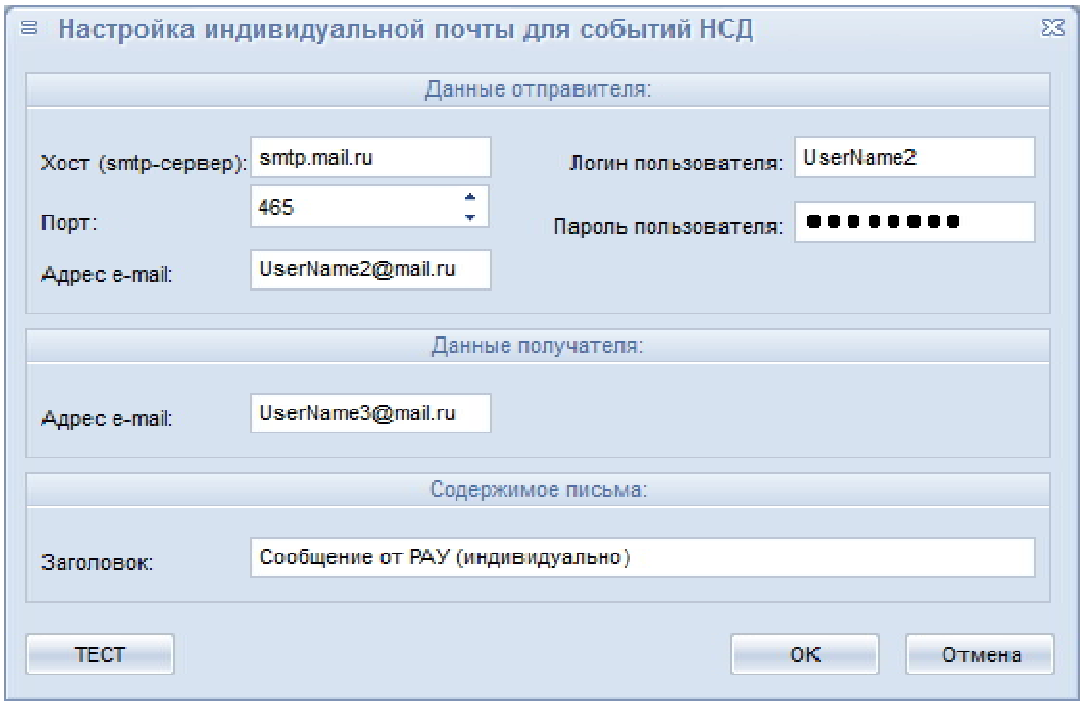

Рисунок 96 - Окно настройки индивидуальной почты для передачи событий НСД

Если в этом окне поле «Хост (smtp-сервер)» не заполнено, то указанный почтовый адрес считается отключенным и не будет использоваться для передачи сообщений. Если это поле заполнено, то на указанный почтовый адрес будут передаваться сообщения о событиях НСД от отдельного ПКО, принадлежащего указанному тех.участку.

При нажатии на вкладке Журналы > Оперативные журналы кнопки <Фильтр журнала> (рисунок 87) появится окно настройки фильтров, в котором можно выбрать типы передаваемых событий (рисунок 97).

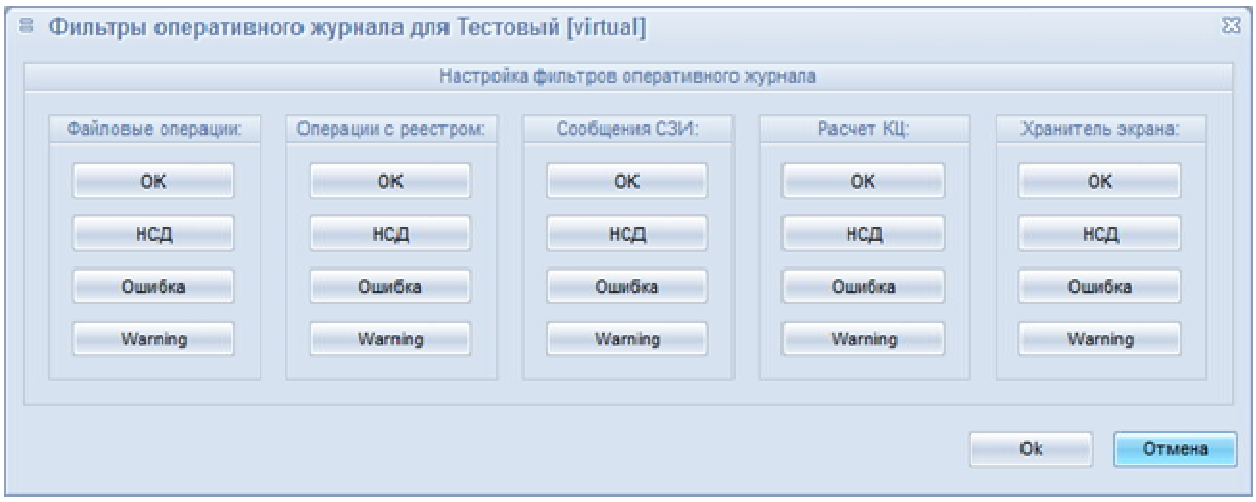

Рисунок 97 - Окно настройки фильтров оперативного журнала для индивидуальной почты

В данном окне выбираются типы событий, информацию о которых следует передавать в оперативный журнал для текущей учетной записи. Настройки фильтра хранятся в каталоге ASM\AccountName_FilterParam.ini, где параметр «AccountName» – это имя учетной записи.

4.7.3 Журнал ASM

В журнал ASM помещается информация о событиях, возникающих при функционировании утилиты ASM, включая:

- информацию о добавлении, удалении, изменении, импортировании пользователей, идентификаторов пользователей, ПКО, учётных записей, USB-устройств и ролей в базу ASM;
- информацию о приёме / передаче базы;
- информацию об экспорте / импорте настроек;
- информацию об изменении параметров конфигурации ASM. Записи журнала, содержащие данную информацию, имеют префикс CFG и отображаются в окне журнала зеленым цветом;
- информацию об изменении параметров ПАК «Аккорд» на ПКО. Записи журнала, содержащие данную информацию, имеют префикс INI и отображаются в окне журнала пурпурным цветом;
- сообщения о НСД.

Окно, отображающее журнал ASM, приведено на рисунке 98.

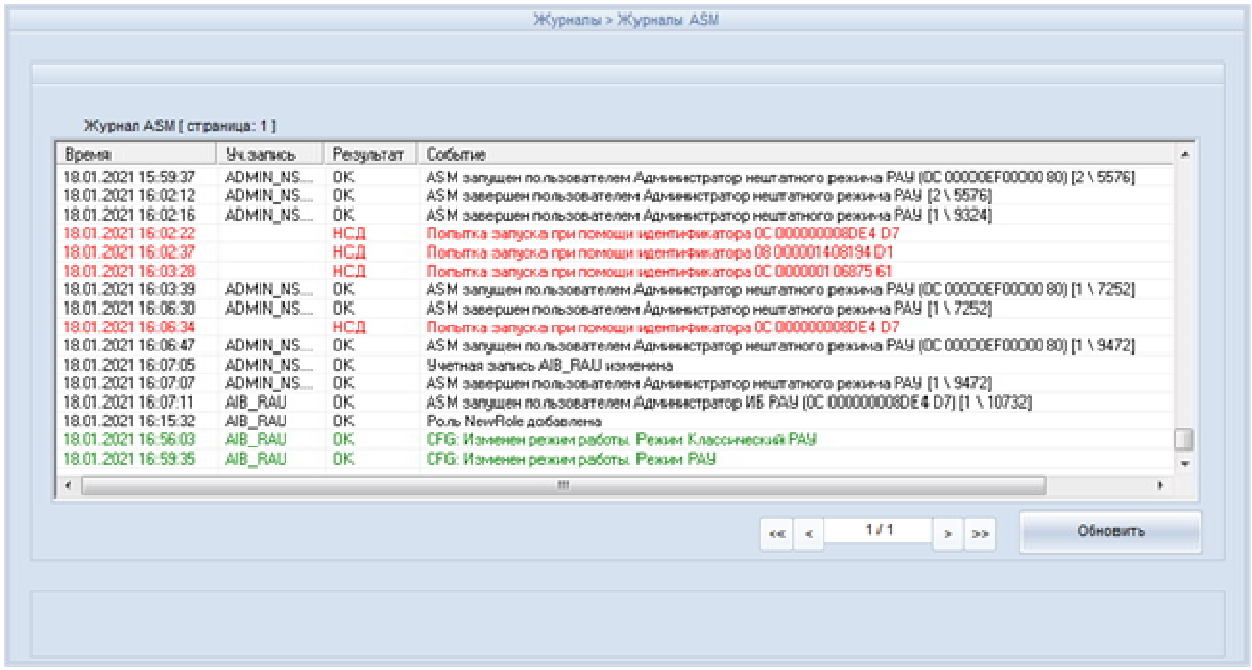

Рисунок 98 - Журнал ASM

Каждая запись журнала ASM содержит следующие поля:

- дата и время, когда произошло событие;
- имя учётной записи Администратора ИБ, инициировавшего выполнение действия, которое вызвало генерацию события. Если событием является передача администратором ИБ базы на ПКО, то данное поле будет содержать имя учётной записи Администратора ИБ. Если событием является изменение пароля пользователя на ПКО, то данное поле будет содержать имя «SYSTEM». Если в поле «Сообщение о событии» записывается значение «НСД. Попытка запуска при помощи идентификатора IDNAME», то в данное поле ничего не записывается;
- тип сообщения. В журнале ASM все сообщения подразделяются на четыре типа:
  - информационные сообщения;
  - предупреждающие сообщения;
  - сообщения об ошибке;
  - сообщения о НСД;
- сообщение о событии. Перечень возможных сообщений приведен в разделе 5.

Журнал ASM хранится на СЦУ в текстовом файле asm.log. Информация хранится в виде строк, заканчивающихся специальными символами «перевод

строки» (код 0x0D) и «возврат каретки» (код 0x0A). Каждая строка содержит информацию об одном событии и имеет следующую структуру:

- дата события;
- символ пробела;
- время события;
- символ пробела;
- сообщение о событии. Перечень возможных сообщений приведен в разделе 5;
- символ «|»;
- имя учётной записи.

4.7.4 Журнал АРМ АБИ

В журнал АРМ АБИ помещается информация о командах, исполняемых агентами ПКО по запросу СЦУ. Данная информация фиксируется на ПКО в текстовых файлах AcWs32.log, а также передается на СЦУ. На СЦУ журнал АРМ АБИ хранится в текстовом файле AcWs32.log.

Уровень детализации журналов АРМ АБИ может изменяться путём задания значения параметра ServiceLogLevel в конфигурационном файле AcCon32.ini на СЦУ.

Параметр ServiceLogLevel может принимать одно из следующих значений:

0 – Error – в журнал АРМ АБИ помещаются только сообщения об ошибках;

1 – Info – в журнал АРМ АБИ помещаются сообщения об ошибках и информационные сообщения;

2 – Debug – в журнал АРМ АБИ помещаются сообщения об ошибках, информационные и отладочные сообщения.

Каждая запись журнала АРМ АБИ содержит следующие поля:

- имя ПКО, с которым связано данное событие;
- дата и время, когда произошло событие;
- сообщение о событии. Перечень возможных сообщений приведен в разделе 8;
- тип сообщения. В журнале АРМ АБИ все сообщения подразделяются на следующие типы:

- базовые сообщения;
- информационные сообщения;
- сообщения об ошибке;
- отладочные сообщения;

• примечание. Данное поле заполняется только для строк, содержащих базовые сообщения, сигнализирующие о произошедших ошибках. В поле приводится информация, детализирующая возникшие ошибки. Все возможные значения поля «Примечание» приведены в разделе 8.

Окно, отображающее журнал АРМ АБИ, приведено на рисунке 99.

Базовые сообщения журнала АРМ АБИ сигнализируют о результате выполнения операции следующим образом:

• если операция выполнена успешно, то поле «Результат» журнала содержит значение «ОК», и соответствующее сообщение отображается в журнале АРМ АБИ черным цветом;

• если вследствие программного сбоя или по иной причине операция выполнена с ошибками, некорректно, то поле «Результат» журнала содержит значение «ОШИБКА», и соответствующее сообщение отображается в журнале АРМ АБИ красным цветом.

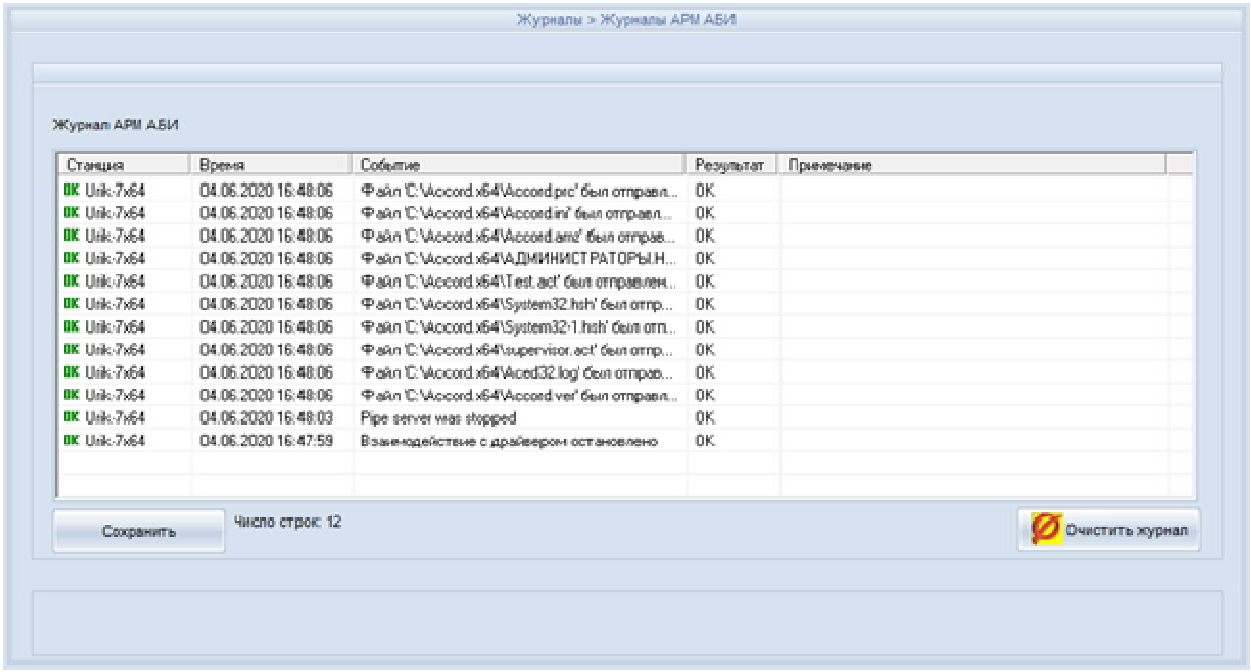

Рисунок 99 – Журнал АРМ АБИ

Журнал АРМ АБИ можно сохранить в текстовый файл. Для этого необходимо в окне, приведённом на рисунке 99, нажать кнопку <Сохранить>. В появившемся окне сохранения файла нужно задать имя файла, в который будет сохранён журнал АРМ АБИ, и нажать кнопку <Сохранить>.

5 Перечень оповещающих сообщений

Оповещающие сообщения выводятся только на экран и не фиксируются ни в каких журналах. Перечень оповещающих сообщений, действия, при которых генерируются данные сообщения, а также действия, которые необходимо предпринять при появлении данных сообщений, приведены в таблице 2.

Таблица 2 – Перечень оповещающих сообщений

Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
«Ошибка чтения ТМ…» (на красном фоне)	В ответ на запрос ТМ-идентификатор был неправильно прислонен к съемнику информации	Снова приложите ТМ-идентификатор к съемнику информации после появления нового запроса
«Это не сетевой ТМ»	В ответ на запрос был прислонен ТМ-идентификатор, не содержащий необходимой информации	Прислонить сетевой ТМ-идентификатор
«В данное время вход в систему запрещен»	Попытка войти в систему в то время, когда работа запрещена настройкой временных ограничений	Необходимо обратиться к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка) и уточнить разрешенное время работы и в случае возможности и необходимости скорректировать временные ограничения. Процедура установки временных ограничений описана в документации ПАК СЗИ от НСД «Аккорд»
«Ваш пароль просрочен. Обратитесь к администратору для смены» (на красном фоне)	Попытка войти в систему, используя просроченный пароль или закончились все попытки смены пароля	Необходимо обратиться к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка) для смены пароля

Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
«Доступ не разрешен!» (на красном фоне)	Использован недопустимый идентификатор пользователя или введен неправильный пароль при попытке входа в систему	Повторить попытку процедуры идентификации / аутентификации, если не поможет обратиться к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка)
«Требуется Администратор» (на красном фоне) «Разберитесь с ошибками» (на оранжевом фоне)	Попытка пользователя войти в систему	Несовпадение контрольных и текущих параметров аппаратной и программной частей системы. Необходимо обратиться к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка) для выявления и устранения причины изменения параметров
«Такую комбинацию символов недопустимо использовать в качестве пароля»	Попытка пользователя сменить пароль	Пользователь пытается задать в качестве нового пароля комбинацию символов, которую легко подобрать, например, qwerty. Необходимо ввести более сложную комбинацию символов. Желательно, чтобы пароль содержал цифры, буквы верхнего и нижнего регистра, а его длинна была не менее восьми символов
«Отсутствует разрешение на смену пароля»	Попытка пользователя сменить пароль	У пользователя нет прав на смену пароля. Необходимо обратиться к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка)

Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
В идентификаторе нет свободных страниц для записи»	Попытка регистрации 32-ой рабочей станции без сохранения списка на АРМ АИБ и очистки памяти ТМ	Объем идентификатора DS1996 позволяет хранить данные о 31 рабочей станции и их открытые ключи. Если в сети остались незарегистрированные станции, то следует добавить список на АРМ АИБ и после очистки памяти ТМ провести регистрацию остальных рабочих станций
«ВНИМАНИЕ! Станция имеет адрес 127.0.0.1. Скорее всего она не подключена к сети. Вы желаете продолжить регистрацию станции?»	Попытка регистрации рабочей станции с IP-адресом 127.0.0.1	Необходимо нажать кнопку <Нет> в появившемся сообщении. Выполнить процедуру регистрации, убедившись, что между ПКО и ASM существует сетевое соединение
Доступ запрещен	Попытка исполнения функции без соответствующих прав при работе по централизованной схеме	Если нет необходимости в доступе к данному ресурсу, и попытка доступа была предпринята по ошибке, то никаких действий предпринимать не нужно. Если же необходим доступ к данному ресурсу, то следует обратиться к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка)
Заполните все необходимые поля	Не заполнен пароль при попытке авторизации в автономном режиме	Введите пароль

Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
Ошибка получения XID	При попытке авторизации не были получены XID – данные учетной записи ASM, необходимые для записи базы в плату на ПКО. Причинами данной ошибки могут являться проблемы со связью (сетью) на момент запроса XID или отсутствие на сервере централизованного управления учётной записи ASM	1 Проверьте наличие связи межу сервером централизованного управления и ПКО. При отсутствии связи, восстановите ее. 2 Обратитесь к Администратору ИБ для проверки существования на сервере централизованного управления учётной записи ASM, под которой произошла данная ошибка
Ошибка чтения ТМ-идентификатора	При работе в автономном режиме в ответ на запрос ТМ-идентификатор был неправильно прислонен к съемнику информации	Снова приложите ТМ-идентификатор к съемнику информации после появления нового запроса
Отправлена база пользователей	При работе в автономном режиме отправлена база пользователей	Данное сообщение информирует об успешной отправке базы пользователей в автономном режиме. Никаких действий при его появлении выполнять не нужно
Файлы баз были экспортированы	При работе в автономном режиме выполнен экспорт файлов	Данное сообщение информирует об успешном экспортировании файлов баз в автономном режиме. Никаких действий при его появлении выполнять не нужно
Файлы баз были импортированы	При работе в автономном режиме выполнен импорт файлов	Данное сообщение информирует об успешном импортировании файлов баз в автономном режиме. Никаких действий при его появлении выполнять не нужно

Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
База пользователей не применена, откат к предыдущей версии	Попытка обновления базы пользователей	Повторите попытку обновления базы пользователей, если и повторная попытка окажется неудачной, получите новую базу пользователей и повторите попытку обновления, если и это не поможет, обратитесь к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка)
Файлы журналов были экспортированы	При работе в автономном режиме выполнен экспорт файлов журналов	Данное сообщение информирует об успешном экспортировании файлов журналов в автономном режиме. Никаких действий при его появлении выполнять не нужно
Отсутствует файл учетной записи ASM. Выполните настройку и запустите службу AcConNet!	После установки сервера централизованного управления РАУ при первом его запуске не была сразу же выполнена предварительная настройка сетевого идентификатора	Выполнить предварительную настройку сетевого идентификатора и запустить службу AcConNet

6 Перечень сообщений ASM

Перечень сообщений ASM, действия, при которых генерируются данные сообщения, а также действия, которые необходимо предпринять при появлении данных сообщений, приведены в таблице 4. В таблице 4 используются следующие условные обозначения:

USERNAME – имя пользователя;

IDNAME – уникальный идентификационный номер (UID) идентификатора;

WSNAME – имя компьютера;

FRAMENAME – название тех. участка;

ACCOUNTNAME – имя учетной записи пользователя;

ROLENAME – имя роли;

USBNAME – наименование USB-устройства (VID ,PID), серийный номер устройства, описание и размещение;

NT_GROUPNAME – имя группы пользователей NT;

TASKNAME – стартовая задача;

FILENAME – полное имя файла (включая путь);

LOG_DETAIL – детальность (уровень детализации) журнала;

NUMBER – в зависимости от контекста – минимальная длина пароля, срок действия пароля в днях, количество попыток смены пароля, интервал времени (в минутах) через который включается хранитель экрана;

ACCESS_LEVEL – уровень доступа пользователя;

ADMIN_ATTR_SET – набор атрибутов администратора, подвергшихся изменению. Полный набор включает следующие атрибуты: Редактирование пользователей, Редактирование контроля, Управление журналом, Редактирование настроек, Контролер, Оператор НШР;

OBJECTNAME – имя объекта. В качестве объектов здесь выступают логические диски, каталоги, файлы, реестр, сетевые ресурсы, съемные диски (USB-флэш, Zip, floppy, сменные HDD), принтеры и другие устройства;

SERVERNAME – имя сервера, на котором хранится база пользователей;

FLAG_SET – набор опций, подвергшихся изменению. Полный набор опций включает: Не контролировать UNC имена, Удаление файлов с очисткой, Марки-

ровка печати, Блокировка клипборда, Может изменять дату/время, Запрет доступа к общим ресурсам, Полный доступ для сервера централизованного управления, Проверять доступ к реестру;

PASS_ALPHABET – набор подмножеств символов, подвергшихся изменению, из которых должен состоять пароль пользователя. Полный набор подмножеств символов включает: Заглавные латинские буквы, строчные латинские буквы, цифры, подмножество символов [!@#$%^&*()];

IA_RESULT_SET – набор параметров идентификации и аутентификации, подвергшихся изменению. Полный набор параметров включает: Идентификатор, Секретный ключ станции, Ключ пользователя, Имя пользователя, Пароль, Флаги ОС, Номер пользователя, Уровень доступа пользователя;

SS_PARAM_SET – набор настроек Screen Saver, подвергшихся изменению. Полный набор включает: Используется, Световая индикация, Звуковая индикация, Не выключать монитор, Защита паролем;

PASS_OPT – дополнительные параметры пароля, подвергшиеся изменению. Данные параметры включают: Не менять пароль в АМДЗ;

ACCESS_CONTROL – набор параметров, определяющих права доступа к объекту. Полный набор включает следующие параметры: S, 0, 1, R, W, C, D, N, V, O, M, E, G, n, r, w, X;

PM_NUMBER – параметр, принимающий значение 1, если флаг, о котором говорится в сообщении, установлен, и значение 0, если флаг снят (не установлен);

PM_NUM – параметр, принимающий значение 0, если в поле «Результат выполнения» установлено значение «Все состояния», значение 1, если в поле «Результат выполнения» установлено значение «НСД», значение 2, если в поле «Результат выполнения» установлено значение «Ошибка»;

REGISTRY_NUMBER – параметр, принимающий значение 1, если флаг, о котором говорится в сообщении, установлен, и значение 0, если флаг снят (не установлен);

REGISTRY_NUM – параметр, принимающий значение 0, если в поле «Результат выполнения» установлено значение «Все состояния», значение 1, если в поле «Результат выполнения» установлено значение «НСД», значение 2, если в поле «Результат выполнения» установлено значение «Ошибка»;

SZI_NUM – параметр, принимающий значение 0, если в поле «Результат выполнения» установлено значение «Все состояния», значение 1, если в поле «Результат выполнения» установлено значение «НСД»;

Hash_NUM – параметр, принимающий значение 0, если в поле «Результат выполнения» установлено значение «Все состояния», значение 1, если в поле «Результат выполнения» установлено значение «НСД»;

Amdz_NUM – параметр, принимающий значение 0, если в поле «Результат выполнения» установлено значение «Все состояния», значение 1, если в поле «Результат выполнения» установлено значение «НСД»;

Screen-Saver_NUM – параметр, принимающий значение 0, если в поле «Результат выполнения» установлено значение «Все состояния», значение 1, если в поле «Результат выполнения» установлено значение «НСД»;

ScreenSaver_NUMBER – параметр, принимающий значение 1, если флаг, о котором говорится в сообщении, установлен, и значение 0, если флаг снят (не установлен).

ERRORCODE – код ошибки. Возможные значения кода ошибки приведены в таблице 3.

Таблица 3 - Возможные значения кода ошибки

Код ошибки	Описание
0	Невозможно осуществить запись в указанное место
2	Файл не найден
23	Отсутствуют права для выполнения операции
169	на ПКО отсутствует ASM_ACCOUNT
3003	Ошибка доступа
3008	Произошла ошибка конфигурации
10060	Попытка установить соединение была безуспешной, т. к. от другого компьютера за требуемое время не получен нужный отклик, или было разорвано уже установленное соединение из-за неверного отклика уже подключенного компьютера

ВНИМАНИЕ! В столбце «Сообщение» таблицы 4 приводятся тексты в таком содержании, в котором они отображаются в окне журнала ASM, приведённом на

рисунке 98. В файле журнала сообщения фиксируются в структуре, описанной в пункте 4.7.2.

Таблица 4 – Перечень событий ASM

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
Информационные сообщения. Сообщения данного типа фиксируются в журнале ASM	Пользователи успешно добавлены в базу	Процедура импорта пользователей ПКО в базу ASM выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Идентификаторы успешно обновлены в базе	Процедура обновления идентификаторов в базе ASM выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Идентификаторы успешно добавлены в базу	Процедура импорта идентификаторов, используемых на ПКО, в базу ASM выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Новые идентификаторы не обнаружены	При выполнении процедуры импорта идентификаторов от ПКО обнаруживается, что новые идентификаторы в базе отсутствуют	Повторите процедуру импорта идентификаторов от ПКО
	Компьютеры успешно добавлены в базу	Процедура импорта компьютеров (ПКО) в базу ASM выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	Компьютеры WSNAME успешно добавлены в базу	Процедура импорта ПКО WSNAME в базу ASM выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Учетные записи успешно добавлены в базу	Процедура импорта учетных записей пользователей ПКО в базу ASM выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	USB-устройства успешно добавлены в базу	Процедура импорта USB-носителей ПКО в базу ASM выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	ASM запущен пользователем USERNAME [FRAMENAME]	Выполнен запуск ASM	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	ASM завершен пользователем USERNAME [FRAMENAME]	Выполнено завершение работы ASM	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	Пользователь USERNAME удален	Процедура удаления пользователя USERNAME выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Идентификатор IDNAME удален	Процедура удаления идентификатора IDNAME выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Идентификатор IDNAME уже есть в базе, обновлен!	В ходе выполнения добавления идентификаторов в базу оказалось, что один из идентификаторов уже есть в базе. Идентификатор в базе переписан на новый	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Компьютер WSNAME удален	Процедура удаления компьютера выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Тех. участок FRAMENAME удален	Процедура удаления тех. участка выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	Учетная запись ACCOUNTNAME удалена	Процедура удаления учетной записи выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Роль ROLENAME удалена	Процедура удаления роли ROLENAME выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	USB USBNAME удален	Процедура удаления USB-устройства USBNAME выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Идентификатор IDNAME успешно добавлен в базу	Процедура добавления идентификатора в базу ASM выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	USB-устройство успешно добавлено в базу	Процедура добавления USB-устройства в базу ASM выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	USB-устройство уже есть в базе, обновлено!	В ходе выполнения добавления USB-устройств в базу оказалось, что одно USB-устройство уже есть в базе. USB-устройство в базе переписано на новое	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Роль ROLENAME изменена	Процедура редактирования роли выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Роль ROLENAME изменена. Список объектов изменен	Процедура редактирования списка объектов роли ROLENAME выполнена успешно. За данным сообщением обязательно следуют одно или несколько следующих сообщений: «Добавлен объект OBJECTNAME [ACCESS_CONTROL]», «Удален объект OBJECTNAME [ACCESS_CONTROL]», «Изменен объект OBJECTNAME [ACCESS_CONTROL]», детализирующих проделанные изменения	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	Роль ROLENAME изменена. Флаги были [FLAG_SET1] стали [FLAG_SET2]	Процедура редактирования флагов роли выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Роль ROLENAME изменена. Алфавит был [PASS_ALPHABET1] стал [PASS_ALPHABET2]	Процедура редактирования настроек алфавита пароля пользователя выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Роль ROLENAME изменена. Стартовая задача была TASKNAME1 стала TASKNAME2	Процедура редактирования стартовой задачи выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Роль ROLENAME изменена. NT группы были NT_GROUPNAME1 стали NT_GROUPNAME2	Процедура редактирования принадлежности роли к группе NT выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Роль ROLENAME изменена. Результаты ИА были [IA_RESULT_SET1] стали [IA_RESULT_SET2]	Процедура редактирования параметров идентификации и аутентификации выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	Роль ROLENAME изменена. Детальность журнала была LOG_DETAIL1 стала LOG_DETAIL2	Процедура редактирования уровня детализации журнала выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Роль ROLENAME изменена. Хранитель экрана (флаги) были [SS_PARAM_SET1] стали [SS_PARAM_SET2]	Процедура редактирования параметров хранителя экрана выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Роль ROLENAME изменена. Хранитель экрана (время) был0 NUMBER1 стало NUMBER2	Процедура редактирования параметров хранителя экрана выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Роль ROLENAME изменена. Мин. длина пароля была NUMBER1 стала NUMBER2	Процедура редактирования минимальной длины пароля выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Роль ROLENAME изменена. Дни действия пароля были NUMBER1 стали NUMBER2	Процедура редактирования срока действия пароля выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	Роль ROLENAME изменена. Попыток смены пароля было NUMBER1 стало NUMBER2	Процедура редактирования количества попыток для смены пароля выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Роль ROLENAME изменена. Доп. параметры пароля были [PASS_OPT1] стали [PASS_OPT2]	Процедура редактирования дополнительного параметра пароля выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Роль ROLENAME изменена. Уровень пользователя был ACCESS_LEVEL1 стал ACCESS_LEVEL2	Процедура редактирования уровня доступа пользователя выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Роль ROLENAME изменена. Атрибуты администратора были [ADMIN_ATTR_SET1] стали [ADMIN_ATTR_SET2]	Процедура редактирования атрибутов администратора выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Роль ROLENAME добавлена	Процедура добавления роли в базу ASM выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	Учетная запись ACCOUNTNAME добавлена	Процедура добавления учетной записи в базу ASM выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Учетная запись ACCOUNTNAME изменена	Процедура редактирования учетной записи выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Пользователь USERNAME изменен	Процедура редактирования пользователя (полное имя, описание, логин, роль, компьютеры) выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Пользователь USERNAME добавлен	Процедура добавления пользователя в базу ASM выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Компьютер WSNAME изменен	Процедура редактирования компьютера выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	Компьютер WSNAME изменен, новый ТУ FRAMENAME	Процедура переназначения компьютера к другому технологическому участку выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Компьютер WSNAME добавлен	Процедура добавления компьютера в базу ASM выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Участок FRAMENAME изменен	Процедура редактирования тех. участка выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Участок FRAMENAME добавлен	Процедура добавления тех. участка в базу ASM выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	Созданы базы: WSNAME	Процедура создания баз *.amz выполнена успешно. В результате выполнения данной процедуры на компьютере WSNAME созданы пользователи в группах Admins и Everyone, назначен пользователь Гл.Администратор, и всем пользователям компьютера присвоены соответствующие учетные записи	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Ключ идентификации успешно записан в сетевой идентификатор	Процедура создания сетевого идентификатора выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Новый ключ идентификации успешно создан	Процедура повторного создания сетевого идентификатора с генерацией нового ключа идентификации выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	WSNAME журналы получены	Процедура получения журналов с компьютера WSNAME выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	WSNAME база AMZ получена	Процедура получения базы пользователей выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	WSNAME база USB получена	Процедура получения базы USB-устройств от включенных ПКО выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	WSNAME Изменен пароль пользователя USERNAME. Успешно	Процедура смены пароля пользователя USERNAME ПКО WSNAME выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	WSNAME Изменен пароль пользователя USERNAME [Аккорд не активирован]. Успешно	Процедура смены пароля пользователя USERNAME ПКО WSNAME выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Файл конфигурации СЗИ подготовлен для отправки на WSNAME	Процедура подготовки файла конфигурации выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	Файл конфигурации СЗИ обновлен на WSNAME	Передача обновленного файла конфигурации на ПКО выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Файл списка привилегированных процессов подготовлен для отправки на WSNAME	Процедура подготовки (создания) файла привилегированных процессов выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Файл списка привилегированных процессов обновлен на WSNAME	Передача обновленного файла привилегированных процессов на ПКО выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Изменены мандатные метки для ПКО WSNAME. Список объектов изменен	Процедура редактирования меток мандатного доступа для пользователей ПКО WSNAME выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Учетная запись ACCOUNTNAME1 переименована в ACCOUNTNAME2	Процедура редактирования параметров учетной записи выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Добавлен объект OBJECTNAME [ACCESS_CONTROL]	Процедура добавления, удаления или изменения объекта	Данное сообщение информирует об успешном выполнении операции.

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	Удален объект OBJECTNAME [ACCESS_CONTROL]	OBJECTNAME выполнена успешно. Данным сообщениям обязательно предшествует сообщение «Роль ROLENAME изменена. Список объектов изменен», в котором указывается для какой роли добавлен, удален или изменен объект	Никаких действий при его появлении выполнять не нужно
	Изменен объект OBJECTNAME [ACCESS_CONTROL]		
	WSNAME Пользователь USERNAME изменил пароль	Процедура смены пароля пользователя ПКО (посредством команды Ctrl-Alt-Del -> «Сменить пароль») выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	WSNAME Отправлена база пользователей. Успешно	Процедура отправки базы пользователей выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	WSNAME Отправлена база пользователей [Аккорд не активирован]. Успешно	Процедура отправки базы пользователей выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	WSNAME Отправлена база пользователей [отложенная]. Успешно	Процедура отправки базы пользователей после включения ПКО выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	WSNAME Отправлена база пользователей [отложенная] *.amz *.ini *.act *.prc. Успешно	Процедура отправки базы пользователей после включения ПКО выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Базы модифицированы другим администратором. Обновлены	Динамическое обновление баз пользователей выполнено успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Базы актуальны	Выполнено динамическое обновление баз пользователей. Модификаций баз со стороны других учетных записей управляющего персонала не выявлено	Данное сообщение информирует о том, что базы пользователей находятся в актуальном состоянии. Никаких действий при его появлении выполнять не нужно
	Пользователи успешно импортированы из базы NT [SERVERNAME]	Процедура импорта пользователей из базы NT выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Пользователи успешно импортированы из базы Accord-a [WSNAME.amz]	Процедура импорта пользователей из базы ПАК «Аккорд» выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	Идентификаторы успешно импортированы из базы Accord-a [WSNAME.amz]	Процедура импорта идентификаторов из базы Accord-a выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Компьютеры успешно импортированы из базы [ACNODE.LST]	Процедура импорта компьютеров из базы [ACNODE.LST] выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Компьютеры успешно импортированы от подконтрольных объектов	Процедура импорта компьютеров от подконтрольных объектов (из выбранного каталога) выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Учетные записи успешно импортированы из базы NT [SERVERNAME]	Процедура импорта учетных записей из базы NT выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Учетные записи успешно импортированы из базы Accord-a [WSNAME.amz]	Процедура импорта учетных записей из базы ПАК «Аккорд» выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	Роли успешно импортированы из базы NT [SERVERNAME]	Процедура импорта ролей из базы NT выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	USB-устройства успешно импортированы из баз ПКО	Процедура импорта USB-устройств от включенных ПКО выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	USB-устройства успешно импортированы из базы Accorda [WSNAME.amz]	Процедура импорта USB-устройств из базы ПАК «Аккорд» выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Роли успешно добавлены в базу	Процедура импорта ролей, используемых на ПКО, в базу ASM выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Процесс ACCONNET.EXE перезапущен	Выполнен автоматический перезапуск ACCONNET.EXE после его сбоя	При частом появлении данного сообщения (более пяти раз за сутки) необходимо обратиться в службу технической поддержки ЗАО «ОКБ САПР»

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	WSNAME Передача базы. База поставлена в очередь передачи на ПКО	Во время выполнения процедуры передачи баз пользователей на ПКО WSNAME служба AcConNet была загружена. По истечении некоторого времени база пользователей автоматически передается на ПКО	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	WSNAME Передача базы. База создана и подготовлена для передачи на ПКО	Во время выполнения процедуры передачи базы пользователей ПКО WSNAME выключен. База пользователей автоматически передастся при включении ПКО	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	WSNAME Передача базы. База передана на ПКО	Процедура передачи базы пользователей на ПКО WSNAME выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	WSNAME Передача базы. База на ПКО актуальна	Процедура передачи базы пользователей на ПКО WSNAME выполнена успешно. Полученная база идентична уже имеющейся на ПКО	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	WSNAME Передача базы. База на ПКО актуальна [Аккорд не активирован]	Процедура передачи базы пользователей на ПКО, на котором не активирована система защиты ПАК «Аккорд», выполнена успешно. Полученная база идентична уже имеющейся на ПКО	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	WSNAME Передача базы. База передана на ПКО [отложенная]	Процедура передачи отложенной базы пользователей выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	WSNAME Передача базы. База передана на ПКО [Аккорд не активирован]	Процедура передачи базы пользователей на ПКО WSNAME, на котором не активирована система защиты ПАК «Аккорд», выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Экспорт успешно завершен	Процедура экспорта журналов событий выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Импорт успешно завершен	Процедура импорта журналов событий выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	Экспорт настроек успешно завершен	Процедура формирования шаблонов настроек выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Импорт настроек успешно завершен	Процедура применения (импорта) шаблонов настроек выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
Сообщения об изменении параметров конфигурации ASM (сообщения с префиксом CFG). Сообщения данного типа фиксируются в журнале ASM	CFG: Включена синхронизация учетных записей РАУ с пользователями Аккорд	Установлен флаг «Синхронизация учетных записей РАУ с пользователями Аккорд»	Никаких действий выполнять не нужно
	CFG: Ключ идентификации успешно записан в сетевой идентификатор	Выполнена настройка сетевого идентификатора	Никаких действий выполнять не нужно
	CFG: Новый ключ идентификации успешно создан	Выполнена генерация нового секретного ключа для сетевого идентификатора	Никаких действий выполнять не нужно
	CFG: Включена. При запуске программы использовать уч.запись пользователя Аккорд	Установлен флаг «При запуске программы использовать уч.запись пользователя Аккорд»	Никаких действий выполнять не нужно
	CFG: Выключена. При запуске программы использовать уч.запись пользователя Аккорд	Снят флаг «При запуске программы использовать уч.запись пользователя Аккорд»	Никаких действий выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	CFG: Изменен путь к АРМ АБИ =	Выполнена корректировка пути к АРМ АБИ	Никаких действий выполнять не нужно
	CFG: Изменен таймаут отклика АРМ АБИ =	Выполнена настройка таймаута отклика АРМ АБИ	Никаких действий выполнять не нужно
	CFG: Изменено время перезагрузки WS =	Выполнена настройка времени перезагрузки ПКО после обновления баз пользователей	Никаких действий выполнять не нужно
	CFG: Изменен период сборки баз =	Выполнена настройка периода автоматического создания баз пользователей	Никаких действий выполнять не нужно
	CFG: Изменена автоматическая сборка баз пользователя = Выключена	Снят флаг «Автоматическая сборка баз пользователей»	Никаких действий выполнять не нужно
	CFG: Изменена автоматическая сборка баз пользователя = Включена	Установлен флаг «Автоматическая сборка баз пользователей»	Никаких действий выполнять не нужно
	CFG: Изменена сборка баз пользователя перед выходом = Включена	Установлен флаг «Сборка баз пользователей перед выходом»	Никаких действий выполнять не нужно
	CFG: Изменена сборка баз пользователя перед выходом = Выключена	Снят флаг «Сборка баз пользователей перед выходом»	Никаких действий выполнять не нужно
	CFG: Изменено максимальное число строк в журнале АРМ АБИ =	Скорректировано максимальное количество строк в журнале АРМ АБИ	Никаких действий выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	CFG: Изменено максимальное число строк в журнале ASM =	Скорректировано максимальное количество строк в журнале ASM	Никаких действий выполнять не нужно
	CFG: Изменено максимальное число строк в журнале TSOM =	Скорректировано количество строк в оперативном журнале	Никаких действий выполнять не нужно
	CFG: Выключена синхронизация учетных записей РАУ с пользователями Аккорд	Снят флаг «Синхронизация учетных записей РАУ с пользователями Аккорд»	Никаких действий выполнять не нужно
	CFG: Включено протоколирование оперативных сообщений в SYSLOG	Установлен флаг «Протоколировать оперативные сообщения в SYSLOG»	Никаких действий выполнять не нужно
	CFG: Выключено протоколирование оперативных сообщений в SYSLOG	Снят флаг «Протоколировать оперативные сообщения в SYSLOG»	Никаких действий выполнять не нужно
	CFG: Изменен путь к файлу с оперативными сообщениями TSOM =	Выполнена корректировка пути к файлу с оперативными сообщениями TSOM	Никаких действий выполнять не нужно
	CFG: TSOM Изменен фильтр PM Создать каталог = PM_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «Создать каталог»	Никаких действий выполнять не нужно
	CFG: TSOM Изменен фильтр PM Удалить каталог = PM_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «Удалить каталог»	Никаких действий выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	CFG: TSOM Изменен фильтр PM Изменить текущий каталог = PM_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «Изменить текущий каталог»	Никаких действий выполнять не нужно
	CFG: TSOM Изменен фильтр PM Переименовать каталог = PM_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «Переименовать каталог»	Никаких действий выполнять не нужно
	CFG: TSOM Изменен фильтр PM Создать файл = PM_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «Создать файл»	Никаких действий выполнять не нужно
	CFG: TSOM Изменен фильтр PM Открыть файл = PM_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «Открыть файл»	Никаких действий выполнять не нужно
	CFG: TSOM Изменен фильтр PM Закрыть файл = PM_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «Закрыть файл»	Никаких действий выполнять не нужно
	CFG: TSOM Изменен фильтр PM Удалить файл = PM_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «Удалить файл»	Никаких действий выполнять не нужно
	CFG: TSOM Изменен фильтр PM Аттрибуты файла = PM_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «Атрибуты файла»	Никаких действий выполнять не нужно
	CFG: TSOM Изменен фильтр PM Запуск программы = PM_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «Запуск программы»	Никаких действий выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	CFG: TSOM Изменен фильтр PM Выход из программы = PM_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «Выход из программы»	Никаких действий выполнять не нужно
	CFG: TSOM Изменен фильтр PM Найти первый файл = PM_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «Найти первый файл»	Никаких действий выполнять не нужно
	CFG: TSOM Изменен фильтр PM Найти следующий файл = PM_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «Найти следующий файл»	Никаких действий выполнять не нужно
	CFG: TSOM Изменен фильтр PM Переименовать файл = PM_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «Переименовать файл»	Никаких действий выполнять не нужно
	CFG: TSOM Изменен фильтр PM Проверка существования пути = PM_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «Проверка существования пути»	Никаких действий выполнять не нужно
	CFG: TSOM Изменен фильтр PM Result = PM_NUM	Выполнена корректировка настроек TSOM: изменен параметр «Результат выполнения»	Никаких действий выполнять не нужно
	CFG: TSOM Изменен фильтр PM Прекращение работы программы = PM_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «Прекращение работы программы»	Никаких действий выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	CFG: TSOM Изменен фильтр PM Установить дату = PM_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «Установить дату»	Никаких действий выполнять не нужно
	CFG: TSOM Изменен фильтр PM Установить время = PM_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «Установить время»	Никаких действий выполнять не нужно
	CFG: TSOM Изменен фильтр REGISTRY Открыть ключ реестра = REGISTRY_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «Открыть ключ реестра»	Никаких действий выполнять не нужно
	CFG: TSOM Изменен фильтр REGISTRY Закрыть ключ реестра = REGISTRY_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «Закрыть ключ реестра»	Никаких действий выполнять не нужно
	CFG: TSOM Изменен фильтр REGISTRY Создать ключ реестра = REGISTRY_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «Создать ключ реестра»	Никаких действий выполнять не нужно
	CFG: TSOM Изменен фильтр REGISTRY Удалить ключ реестра = REGISTRY_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «Удалить ключ реестра»	Никаких действий выполнять не нужно
	CFG: TSOM Изменен фильтр REGISTRY Перечисление ключей реестра = REGISTRY_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «Перечисление ключей реестра»	Никаких действий выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	CFG: TSOM Изменен фильтр REGISTRY Установить значение параметра ключа = REGISTRY_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «Установить значение параметра ключа»	Никаких действий выполнять не нужно
	CFG: TSOM Изменен фильтр REGISTRY Прочитать значение параметра ключа = REGISTRY_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «Прочитать значение параметра ключа»	Никаких действий выполнять не нужно
	CFG: TSOM Изменен фильтр REGISTRY Удалить параметр ключа = REGISTRY_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «Удалить параметр ключа»	Никаких действий выполнять не нужно
	CFG: TSOM Изменен фильтр REGISTRY Создать параметр ключа = REGISTRY_NUMBER	Выполнена корректировка настроек TSOM в части операций с реестром: установлен (или снят) флаг «Создать параметр ключа»	Никаких действий выполнять не нужно
	CFG: TSOM Изменен фильтр REGISTRY Перечисление параметров ключа = REGISTRY_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «Перечисление параметров ключа»	Никаких действий выполнять не нужно
	CFG: TSOM Изменен фильтр REGISTRY Result = REGISTRY_NUM	Выполнена корректировка настроек TSOM в части результата выполнения операций с реестром: изменен параметр «Результат выполнения»	Никаких действий выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	CFG: TSOM Изменен фильтр SZI Result = SZI_NUM	Выполнена корректировка настроек TSOM в части результата выполнения сообщений СЗИ: изменен параметр «Результат выполнения»	Никаких действий выполнять не нужно
	CFG: TSOM Изменен фильтр Hash Result = Hash_NUM	Выполнена корректировка настроек TSOM в части результата выполнения расчета КЦ: изменен параметр «Результат выполнения»	Никаких действий выполнять не нужно
	CFG: TSOM Изменен фильтр ScreenSaver Result = ScreenSaver_NUM	Выполнена корректировка настроек TSOM в части результата выполнения операций с Хранителем экрана: изменен параметр «Результат выполнения»	Никаких действий выполнять не нужно
	CFG: TSOM Изменен фильтр ScreenSaver ScreenSaver включен по времени = ScreenSaver_NUMBER	Выполнена корректировка настроек TSOM: установлен (или снят) флаг «ScreenSaver включен по времени»	Никаких действий выполнять не нужно
	CFG: TSOM Изменен фильтр ScreenSaver ScreenSaver включен используя горячие клавиши = ScreenSaver_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «ScreenSaver включен используя горячие клавиши»	Никаких действий выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	CFG: TSOM Изменен фильтр ScreenSaver ScreenSaver включен с АРМ АБИ = ScreenSaver_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «ScreenSaver включен с АРМ АБИ»	Никаких действий выполнять не нужно
	CFG: TSOM Изменен фильтр ScreenSaver ScreenSaver выключен с помощью ТМ = ScreenSaver_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «ScreenSaver выключен с помощью ТМ»	Никаких действий выполнять не нужно
	CFG: TSOM Изменен фильтр ScreenSaver ScreenSaver выключен с АРМ АБИ = ScreenSaver_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «ScreenSaver выключен с АРМ АБИ»	Никаких действий выполнять не нужно
	CFG: TSOM Изменен фильтр ScreenSaver ScreenSaver выключен с помощью ТМ АБИ = ScreenSaver_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «ScreenSaver выключен с помощью ТМ АБИ»	Никаких действий выполнять не нужно
	CFG: TSOM Изменен фильтр ScreenSaver Выключен временной контроль ScreenSaver-а = ScreenSaver_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «Выключен временной контроль ScreenSaver-а»	Никаких действий выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	CFG: TSOM Изменен фильтр ScreenSaver Включен временной контроль ScreenSaver-a = ScreenSav-er_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «Включен временной контроль ScreenSaver-a»	Никаких действий выполнять не нужно
	CFG: TSOM Изменен фильтр ScreenSaver Попытка разблокировать чужим ТМ = ScreenSav-er_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «Попытка разблокировать чужим ТМ»	Никаких действий выполнять не нужно
	CFG: Изменена внешняя программа обрабатывающая НСД =	Установлено приложение, которое запускается в случае возникновения НСД	Никаких действий выполнять не нужно
	CFG: Отключена внешняя программа обрабатывающая НСД	Удалено приложение, которое запускается в случае возникновения НСД	Никаких действий выполнять не нужно
	CFG: Изменен метод конвертации журналов TSIEM = XML	Установлен метод конвертации журналов XML	Никаких действий выполнять не нужно
	CFG: Изменен метод конвертации журналов TSIEM = CSV	Установлен метод конвертации журналов CSV	Никаких действий выполнять не нужно
	CFG: изменен путь к файлу для конвертации журналов TSIEM =	Корректировка пути к файлу для конвертации журналов выполнена успешно	Никаких действий выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	CFG: Включено перемещение файлов в архив после конвертации	Флаг «Перемещать журналы в архив после конвертации» установлен успешно	Никаких действий выполнять не нужно
	CFG: Выключено перемещение файлов в архив после конвертации	Флаг «Перемещать журналы в архив после конвертации» снят успешно	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр PM Прекращение работы программы = PM_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «Прекращение работы программы»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр PM Установить дату = PM_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «Установить дату»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр PM Установить время = PM_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «Установить время»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр PM Создать каталог = PM_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «Создать каталог»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр PM Удалить каталог = PM_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «Удалить каталог»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр PM Изменить текущий каталог = PM_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «Изменить текущий каталог»	Никаких действий выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	CFG: TSIEM Изменен фильтр PM Переименовать каталог = PM_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «Переименовать каталог»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр PM Создать файл = PM_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «Создать файл»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр PM Открыть файл = PM_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «Открыть файл»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр PM Закрыть файл = PM_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «Закрыть файл»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр PM Удалить файл = PM_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «Удалить файл»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр PM Аттрибуты файла = PM_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «Атрибуты файла»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр PM Запуск программы = PM_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «Запуск программы»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр PM Выход из программы = PM_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «Выход из программы»	Никаких действий выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	CFG: TSIEM Изменен фильтр PM Найти первый файл = PM_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «Найти первый файл»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр PM Переименовать файл = PM_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «Переименовать файл»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр PM Проверка существования пути = PM_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «Проверка существования пути»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр PM Result = PM_NUM	Выполнена корректировка настроек TSIEM изменен параметр «Результат выполнения»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр REGISTRY Открыть ключ реестра = REGISTRY_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «Открыть ключ реестра»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр REGISTRY Закрыть ключ реестра = REGISTRY_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «Закрыть ключ реестра»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр REGISTRY Создать ключ реестра = REGISTRY_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «Создать ключ реестра»	Никаких действий выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	CFG: TSIEM Изменен фильтр REGISTRY Удалить ключ реестра = REGISTRY_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «Удалить ключ реестра»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр REGISTRY Перечисление ключей реестра = REGISTRY_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «Перечисление ключей реестра»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр REGISTRY Установить значение параметра ключа = REGISTRY_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «Установить значение параметра ключа»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр REGISTRY Прочитать значение параметра ключа = REGISTRY_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «Прочитать значение параметра ключа»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр REGISTRY Удалить параметр ключа = REGISTRY_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «Удалить параметр ключа»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр REGISTRY Создать параметр ключа = REGISTRY_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «Создать параметр ключа»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр REGISTRY Перечисление параметров ключа = REGISTRY_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «Перечисление параметров ключа»	Никаких действий выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	CFG: TSIEM Изменен фильтр REGISTRY Result = REGISTRY_NUM	Выполнена корректировка настроек TSIEM в части результата выполнения операций с реестром: изменен параметр «Результат выполнения»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр SZI Result = SZI_NUM	Выполнена корректировка настроек TSIEM в части результата выполнения сообщений СЗИ: изменен параметр «Результат выполнения»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр Hash Result = Hash_NUM	Выполнена корректировка настроек TSIEM в части результата выполнения расчета КЦ: изменен параметр «Результат выполнения»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр Amdz Result = Amdz_NUM	Выполнена корректировка настроек TSIEM в части результата выполнения сообщений АМДЗ: изменен параметр «Результат выполнения»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр ScreenSaver Result = ScreenSaver_NUM	Выполнена корректировка настроек TSIEM в части результата выполнения операций с Хранителем экрана: изменен параметр «Результат выполнения»	Никаких действий выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	CFG: TSIEM Изменен фильтр ScreenSaver ScreenSaver включен по времени = ScreenSaver_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «ScreenSaver включен по времени»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр ScreenSaver ScreenSaver включен используя горячие клавиши = ScreenSaver_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «ScreenSaver включен используя горячие клавиши»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр ScreenSaver ScreenSaver включен с АРМ АБИ = ScreenSaver_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «ScreenSaver включен с АРМ АБИ»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр ScreenSaver ScreenSaver выключен с помощью ТМ = ScreenSaver_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «ScreenSaver выключен с помощью ТМ»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр ScreenSaver ScreenSaver выключен с АРМ АБИ = ScreenSaver_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «ScreenSaver выключен с АРМ АБИ»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр ScreenSaver ScreenSaver выключен с помощью ТМ АБИ = ScreenSaver_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «ScreenSaver выключен с помощью ТМ АБИ»	Никаких действий выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	CFG: TSIEM Изменен фильтр ScreenSaver Выключен временной контроль ScreenSaver-a = ScreenSaver_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «Выключен временной контроль ScreenSaver-a»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр ScreenSaver Включен временной контроль ScreenSaver-a = ScreenSaver_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «Включен временной контроль ScreenSaver-a»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр ScreenSaver Попытка разблокировать чужим ТМ = ScreenSaver_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «Попытка разблокировать чужим ТМ»	Никаких действий выполнять не нужно
Сообщения об изменении параметров конфигурации ПАК «Аккорд» на ПКО (сообщения с префиксом INI). Сообщения данного типа фиксируются в журнале ASM	INI: На ПКО WSNAME изменен список привилегированных процессов	Редактирование списка привилегированных процессов ПКО выполнено успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	INI: Изменен КЦ для роли ROLENAME	Список файлов для контроля целостности ПКО успешно изменен	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	INI: Изменена ЗС для роли ROLENAME	Редактирование списка задач для запуска выполнено успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	INI: WSNAME Механизм разграничения доступа Мандатный = No	Снят флаг «Мандатный» в параметрах конфигурации СЗИ	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	INI: WSNAME Механизм разграничения доступа Мандатный = Yes	Установлен флаг «Мандатный» в параметрах конфигурации СЗИ	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	INI: WSNAME Механизм разграничения доступа Процессы = No	Снят флаг «+процессы» в параметрах конфигурации СЗИ	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	INI: WSNAME Механизм разграничения доступа Процессы = Yes	Установлен флаг «+процессы» в параметрах конфигурации СЗИ	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	INI: На ПКО WSNAME Мягкий режим = No	Снят флаг «Мягкий режим» в параметрах конфигурации СЗИ	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	INI: На ПКО WSNAME Мягкий режим = Yes	Установлен флаг «Мягкий режим» в параметрах конфигурации СЗИ	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	INI: WSNAME Автоматический логин в ОС = No	Снят флаг «Автоматический логин в ОС» в параметрах конфигурации СЗИ	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	INI: WSNAME Автоматический логин в ОС = Yes	Установлен флаг «Автоматический логин в ОС» в параметрах конфигурации СЗИ	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	INI: WSNAME Синхронизация с базой пользователей NT = No	Снят флаг «Синхронизация с базой пользователей NT» в параметрах конфигурации СЗИ	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	INI: WSNAME Синхронизация с базой пользователей NT = Yes	Установлен флаг «Синхронизация с базой пользователей NT» в параметрах конфигурации СЗИ	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	INI: WSNAME Синхронизация с базой АМДЗ = No	Снят флаг «Синхронизация с базой АМДЗ» в параметрах конфигурации СЗИ	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	INI: WSNAME Синхронизация с базой АМДЗ = Yes	Установлен флаг «Синхронизация с базой АМДЗ» в параметрах конфигурации СЗИ	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	INI: На ПКО WSNAME Использовать полное имя в учетных записях NT = No	Снят флаг «Использовать полное имя в учетных записях NT» в параметрах конфигурации СЗИ	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	INI: На ПКО WSNAME Использовать полное имя в учетных записях NT = Yes	Установлен флаг «Использовать полное имя в учетных записях NT» в параметрах конфигурации СЗИ	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	INI: WSNAME Контроль доступа к устройствам = No	Снят флаг «Контроль доступа к устройствам» в параметрах конфигурации СЗИ	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	INI: WSNAME Контроль доступа к устройствам = Yes	Установлен флаг «Контроль доступа к устройствам» в параметрах конфигурации СЗИ	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	INI: На ПКО WSNAME Использовать полный путь процесса = No	Снят флаг «Использовать полный путь процесса» в параметрах конфигурации СЗИ	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	INI: На ПКО WSNAME Использовать полный путь процесса = Yes	Установлен флаг «Использовать полный путь процесса» в параметрах конфигурации СЗИ	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
Предупреждающие сообщения. Сообщения данного типа фиксируются в журнале ASM	VID и PID должны состоять из 4-х цифр!	При добавлении нового USB-устройства в базу ASM некорректно введены VID или PID устройства	Ввести корректные значения VID или PID устройства
	VID и PID должны состоять только из шестнадцатеричных цифр, или '*'!	При добавлении нового USB-устройства в базу ASM некорректно введены VID или PID устройства	Ввести корректные значения VID или PID устройства

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	Серийный номер должен состоять только из шестнадцатеричных цифр, или '*'!	При добавлении нового USB-устройства в базу ASM введен некорректный серийный номер устройства	Ввести корректный серийный номер устройства
Сообщение об ошибке. Сообщения данного типа фиксируются в журнале ASM	Error WSNAME ошибка получения журналов [ErrCode = ERRCODE, нет файлов журналов]	При попытке получения журналов от ПКО произошла ошибка из-за того, что либо на ПКО отсутствуют файлы журналов, либо система защиты комплекса «Аккорд» на ПКО не активирована	Обратиться к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка)
	Error WSNAME ошибка получения журналов [ErrCode = ERRCODE, станция не активна]	При попытке получения журналов от ПКО произошла ошибка из-за того, что ПКО выключен или не подключен к сети	Через некоторое время повторить попытку получения журналов, если ошибка повторится, обратиться к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка)
	Error WSNAME ошибка получения журналов [ErrCode = ERRCODE]	При попытке получения журналов от ПКО произошла ошибка	Обратиться к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка)
	WSNAME ошибка получения базы AMZ [ErrCode = ERRCODE, станция не активна]	При попытке получения базы AMZ от ПКО произошла ошибка из-за того, что ПКО выключен или не подключен к сети	Через некоторое время повторить попытку получения журналов, если ошибка повторится, обратиться к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка)

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	WSNAME ошибка получения базы AMZ [ErrCode = ERRCODE]	При попытке получения базы AMZ от ПКО произошла ошибка	Обратиться к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка)
	Error WSNAME Отправлена база пользователей. Ошибка установки TCP/IP соединения ErrCode = ERRCODE	При попытке отправить базу пользователей на ПКО произошла ошибка из-за того, что не удалось установить TCP/IP соединение между ASM и ПКО	Повторить попытку отправления базы пользователей на ПКО. Если ошибка повторится, обратиться к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка)
	Error WSNAME Отправлена база пользователей [Аккорд не активирован]. Ошибка установки TCP/IP соединения ErrCode = ERRCODE	При попытке отправить базу пользователей на ПКО произошла ошибка из-за того, что не удалось установить TCP/IP соединение между ASM и ПКО	Повторить попытку отправления базы пользователей на ПКО. Если ошибка повторится, обратиться к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка)
	Error WSNAME Отправлена база пользователей [отложенная]. Ошибка установки TCP/IP соединения ErrCode = ERRCODE	При попытке отправить отложенную базу пользователей на ПКО произошла ошибка из-за того, что не удалось установить TCP/IP соединение между ASM и ПКО	Повторить попытку отправления отложенной базы пользователей на ПКО. Если ошибка повторится, обратиться к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка)

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	Error WSNAME Отправлена база пользователей. Разрыв связи	При попытке отправить базу пользователей на ПКО произошла ошибка из-за разрыва связи	Повторить попытку отправления базы пользователей на ПКО. Если ошибка повторится, обратиться к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка)
	Error WSNAME Отправлена база пользователей [отложенная]. Разрыв связи	При попытке отправить отложенную базу пользователей на ПКО произошла ошибка из-за разрыва связи	Повторить попытку отправления базы пользователей на ПКО. Если ошибка повторится, обратиться к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка)
	Error WSNAME Отправлена база пользователей. Не прошел логин в АМДЗ [ErrCode = ERRCODE]	При попытке отправить базу пользователей на ПКО произошла ошибка при аутентификации сервера на АМДЗ	Повторить попытку отправления базы пользователей на ПКО. Если ошибка повторится, обратиться к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка)
	Error WSNAME Отправлена база пользователей [отложенная]. Не прошел логин в АМДЗ [ErrCode = ERRCODE]	При попытке отправить отложенную базу пользователей на ПКО произошла ошибка при аутентификации сервера на АМДЗ	Повторить попытку отправления отложенной базы пользователей на ПКО. Если ошибка повторится, обратиться к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка)

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	Error WSNAME Отправлена база пользователей [Аккорд не активирован]. Не прошел логин в АМДЗ [ErrCode = ERRCODE]	При попытке отправить базу пользователей на ПКО произошла ошибка при аутентификации сервера на АМДЗ	Повторить попытку отправления базы пользователей на ПКО. Если ошибка повторится, обратиться к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка)
	Error WSNAME Отправлена база пользователей [отложенная] [Аккорд не активирован]. Не прошел логин в АМДЗ [ErrCode = ERRCODE]	При попытке отправить отложенную базу пользователей на ПКО произошла ошибка при аутентификации сервера на АМДЗ	Повторить попытку отправления отложенной базы пользователей на ПКО. Если ошибка повторится, обратиться к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка)
	Error WSNAME Отправлена база пользователей [Аккорд не активирован]. Ошибка создания файла [ErrCode = ERRCODE]	При попытке отправить базу пользователей на ПКО произошла ошибка при создании файла для базы пользователей	Убедится, что каталог, в который установлен ПАК СЗИ от НСД «Аккорд» доступен для записи
	Error WSNAME Отправлена база пользователей. Ошибка создания файла FILENAME [ErrCode = ERRCODE]	При попытке отправить базу пользователей на ПКО произошла ошибка при создании файла для базы пользователей	При появлении данной ошибки необходимо обратиться в службу технической поддержки организации-разработчика
	Error WSNAME Отправлена база пользователей [отложенная]. Ошибка создания файла [ErrCode = ERRCODE]	При попытке отправить отложенную базу пользователей на ПКО произошла ошибка при создании файла для базы пользователей	Убедится, что каталог, в который установлен ПАК СЗИ от НСД «Аккорд» доступен для записи

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	Error WSNAME Отправлена база пользователей [отложенная] [Аккорд не активирован]. Ошибка создания файла FILENAME [ErrCode = ERRCODE]	При попытке отправить отложенную базу пользователей на ПКО произошла ошибка при создании файла для базы пользователей	Убедится, что каталог, в который установлен ПАК СЗИ от НСД «Аккорд» доступен для записи
	Error WSNAME Отправлена база пользователей. Ошибка создания файла [ErrCode = ERRCODE]	При попытке отправить базу пользователей на ПКО произошла ошибка при создании файла для базы пользователей	Убедится, что каталог, в который установлен ПАК СЗИ от НСД «Аккорд» доступен для записи
	Error WSNAME Отправлена база пользователей [отложенная]. Нет подтверждения о доставке	В результате выполнения процедуры отправки отложенной базы пользователей после включения ПКО база пользователей не была доставлена на ПКО	Повторите процедуру отправки отложенной базы пользователей на ПКО. Если ошибка повторится, обратитесь к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка)
	Error WSNAME Отправлена база пользователей [Аккорд не активирован]. Нет подтверждения о доставке	В результате выполнения процедуры отправки базы пользователей база пользователей не была доставлена на ПКО	Повторите процедуру отправки базы пользователей на ПКО. Если ошибка повторится, обратитесь к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка)

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	Error WSNAME Отправлена база пользователей [отложенная] [Аккорд не активирован]. Нет подтверждения о доставке	В результате выполнения процедуры отправки отложенной базы пользователей база пользователей не была доставлена на ПКО	Повторите процедуру отправки отложенной базы пользователей на ПКО. Если ошибка повторится, обратитесь к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка)
	Error WSNAME Отправлена база пользователей. Нет подтверждения о доставке	В результате выполнения процедуры отправки базы пользователей база пользователей не была доставлена на ПКО	Повторите процедуру отправки базы пользователей на ПКО. Если ошибка повторится, обратитесь к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка)
	Error WSNAME Передача базы. Для компьютера WSNAME не назначен Supervisor	При попытке передачи базы произошла ошибка из-за того, что на компьютере не назначен пользователь Гл.Администратор	Повторить попытку передачи базы. Если ошибка повторится, обратиться к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка)
	Для компьютера WSNAME учетная запись ACCOUNTNAME не назначена на пользователя	При попытке создать базу *.amz произошла ошибка, так как пользователям компьютера не присвоены соответствующие учетные записи	Обратиться к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка)

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	Для компьютера WSNAME нет группы Admins	При попытке создать базу *.amz произошла ошибка, так как не созданы пользователи в группе Admins	Обратиться к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка)
	Для компьютера WSNAME нет группы Everyone	При попытке создать базу *.amz произошла ошибка, так как не созданы пользователи в группе Everyone	Обратиться к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка)
	Error Ошибка ERRCODE отправки файла конфигурации СЗИ на WSNAME	При попытке передать обновленный файл конфигурации СЗИ на ПКО произошла ошибка	Повторить попытку передачи файла конфигурации СЗИ на ПКО. Если ошибка повторится, обратиться к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка)
	Ошибка отправки файла списка привилегированных процессов на WSNAME	При попытке передать файл со списком привилегированных процессов произошла ошибка	Повторить попытку передачи файла со списком привилегированных процессов на ПКО. Если ошибка повторится, обратиться к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка)

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	Файл списка КЦ для роли ROLENAME не отправлен на ПКО	Задания для контроля целостности не было отправлено на ПКО	Повторить попытку передачи файла задания для контроля целостности на ПКО. Для обеспечения возможности передачи баз на ПКО до разрешения данной ошибки следует в настройках сервера централизованного управления установить флажок «Не передавать базы, если нет актуального списка КЦ»
	Файл со списком КЦ для роли ROLENAME не получен от ПКО	Файл с эталонными контрольными суммами не получен от ПКО	Ожидайте получения .CRC файла от ПКО. Для обеспечения возможности передачи баз на ПКО до разрешения данной ошибки следует в настройках сервера централизованного управления установить флажок «Не передавать базы, если нет актуального списка КЦ»

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	Старый файл со списком КЦ для роли ACCOUNTNAME	Имеется файл с эталонными контрольными суммами, но он создан раньше файла с заданием для контроля целостности	Ожидайте получения нового .CRC файла от ПКО. Для обеспечения возможности передачи баз на ПКО до разрешения данной ошибки следует в настройках сервера централизованного управления установить флажок «Не передавать базы, если нет актуального списка КЦ»
Сообщения о НСД. Сообщения данного типа фиксируются в журнале ASM	НСД Попытка запуска при помощи идентификатора IDNAME	Попытка запуска ASM при помощи незарегистрированного идентификатора	Запустите ASM, используя зарегистрированный идентификатор
	НСД Попытка запуска, неверный идентификатор IDNAME или пароль	При попытке запуска ASM введен некорректный пароль	При запуске ASM введите корректный пароль
	НСД Ошибка установки соединения с ACCONNET.EXE = 3008	В ходе работы произошел сбой процесса ACCONNET.EXE	При появлении данной ошибки необходимо обратиться в службу технической поддержки организации-разработчика
	НСД Остановлен процесс ACCONNET.EXE	В ходе работы произошел сбой процесса ACCONNET.EXE	При появлении данной ошибки необходимо обратиться в службу технической поддержки организации-разработчика

7 Перечень событий ПАК «Аккорд» на подконтрольных объектах

Перечень сообщений, генерируемых ПАК «Аккорд» на подконтрольных объектах, и их описание приведены в таблице 5.

Таблица 5 – Перечень сообщений ПАК «Аккорд» на подконтрольных объектах

Сообщение	Описание
Login	Выполнен вход на ПКО
Комплекс СЗИ от НСД «Аккорд-WinXX», System:, Acrun.sys:, SN=	Описание установленного на ПКО комплекса СЗИ от НСД, ОС ПКО, версии драйвера разграничения доступа и серийного номера контроллера. Сообщение записывается в журнал событий после запуска ПКО и выполнения пользователем процедуры входа на ПКО (в журнале данное сообщение помещается после сообщения о выполнении входа на ПКО)
Settings: SM=, DA=, MA=, CP=, DNSD=, WLN=, FPP=	Собственные настройки ПАК «Аккорд»: – SM – мягкий режим; – DA –дискреционный механизм разграничения доступа; – MA – мандатный механизм разграничения доступа; – CP – контроль процессов; – DNSD – записывать в журнал логические имена дисков; – WLN – использовать логические имена в пути; – FPP – использовать полный путь процесса. Данным параметрам присваивается значение «Yes», если в утилите «Настройка комплекса «Аккорд» установлены соответствующие настройки, иначе присваивается значение «No». Данное сообщение записывается в журнал событий после выполнения пользователем процедуры входа на ПКО (в журнале данное сообщение помещается после сообщения с описанием установленного на ПКО комплекса СЗИ от НСД, ОС ПКО, версии драйвера разграничения доступа и серийного номера контроллера)
FullUserName=	Полное имя пользователя. Сообщение записывается в журнал событий после выполнения пользователем процедуры входа на ПКО (в журнале данное сообщение помещается после сообщения с описанием собственных настроек ПАК «Аккорд»)

Сообщение	Описание
User logoff from WS local	Выполнен выход из сессии пользователя ПКО
Logs collected user USERNAME	Журналы ПКО собраны пользователем USERNAME (в рамках децентрализованной схемы)
Insert USB: Vid_, Pid_, Sn_	Сообщение о подключении USB-устройства к ПКО с указанием Vid, Pid и серийного номера устройства
Remove USB: Vid_, Pid_, Sn_	Сообщение об отключении USB-устройства от ПКО с указанием Vid, Pid и серийного номера устройства
User Change Password	Выполнена процедура смены пароля пользователя ПКО (посредством команды Ctrl-Alt-Del -> «Сменить пароль»)
MSZI	Проверка активности ПКО. Компьютер работает
MSZI	Система снята. Данное сообщение генерируется ПАК СЗИ от НСД «Аккорд-Win32» / «Аккорд Win64» версий не ниже 4.0.9.46 / 5.0.9.46 соответственно.
MSZI	Система активирована. Данное сообщение генерируется ПАК СЗИ от НСД «Аккорд-Win32» / «Аккорд Win64» версий не ниже 4.0.9.46 / 5.0.9.46 соответственно.
Logout	Выполнен выход с ПКО
ChangeDir	Смена каталога
СЗИ	Сообщение СЗИ от НСД «Аккорд»
ChMod	Установка/смена атрибутов
CloseFile	Закрытие файла
CreateDir	Создание каталога
CreateFile	Создание файла
DeleteDir	Удаление каталога
DeleteFile	Удаление файла
DriveAccess	Доступ к диску
Exec	Запуск программы
Exit	Завершение программы
OpenFile	Открытие файла
RenameDir	Переименование каталога
RenameFile	Переименование файла

Сообщение	Описание
Search	Поиск файла/каталога
SetDate	Установка системной даты
SetTime	Установка системного времени
Traverse	Проверка существования пути
RegCloseKey	Закрытие ключа реестра
RegCreateKey	Создание ключа реестра
RegCreateValue	Создание переменной в ключе реестра
RegDeleteKey	Удаление ключа реестра
RegDeleteValue	Удаление переменной из ключа реестра
RegEnumKey	Поиск ключей реестра
RegEnumValue9	Поиск переменных в ключе реестра
RegOpenKey0	Открытие ключа реестра
RegQueryValue	Чтение переменной из ключа реестра
RegSetValue	Изменение значения переменной в ключе реестра
SSOffAtAdmin ScreenSaver	Разблокировка ПКО с помощью ТМ администратора АРМ АБИ (хранитель экрана выключен с помощью ТМ администратора АРМ АБИ)
SSOffAtRemoute ScreenSaver	Разблокировка ПКО с помощью АРМ АБИ (хранитель экрана выключен удаленно с помощью АРМ АБИ)
SSOffAtTM Screen-Saver	Разблокировка с помощью ТМ
SSOffBadTM	Попытка разблокировать не тем ТМ, которым осуществлялась блокировка
SSOnAtHotKey ScreenSaver	Блокировка с помощью клавиатуры
SSOnAtRemoute ScreenSaver	Блокировка с помощью АРМ АБИ
SSOnAtTimeout 0 ScreenSaver	Блокировка по времени неактивности
SSTimeDisable	Выключен временной контроль ScreenSaver-а (выполнена разблокировка ПКО)
SSTimeEnable	Включен временной контроль ScreenSaver-а (ПКО заблокирован)

Сообщение	Описание
EndCheck	Выполнена процедура проверки списка файлов. Достигнут конец проверки списка файлов
EndUpdate	Выполнена процедура обновления списка файлов. Достигнут конец обновления списка файлов
FileCheck	Выполняется процедура проверки файла
GetPrivateKey	Получение секретного ключа идентификатора пользователя (при выполнении процедуры расчета контрольных сумм)
StartCheck	Начало выполнения процедуры проверки списка файлов
StartUpdate	Начало выполнения процедуры обновления списка файлов
TotalEDS	Выполнена подпись списка файлов после завершения процедуры проверки
TotalHash	Выполнен расчет хэш-суммы списка файлов

Сообщения, генерируемые ПАК «Аккорд», подразделяются на следующие типы:

- информационные сообщения, передающие результат «ОК», означают, что соответствующее действие выполнено успешно. Информационные сообщения отображаются в журнале регистрации черным цветом;
- сообщения об ошибке, передающие результат «ОШИБКА», означают, что соответствующее действие выполнено некорректно вследствие программного сбоя или по иной причине. Сообщения об ошибке отображаются в журнале регистрации синим цветом;
- предупреждающие сообщения, передающие результат «WARNING», означают, что выполненное действие является потенциально опасным. Данные сообщения, как правило, используются в отладочных целях. Предупреждающие сообщения отображаются в журнале регистрации черным цветом;
- сообщения о НСД, передающие результат «НСД», означают, что выполнение соответствующего действия заблокировано механизмами ПАК «Аккорд». Сообщения о НСД отображаются в журнале регистрации красным цветом.

8 Перечень событий АРМ АБИ

В таблице 6 приведены сообщения журнала АРМ АБИ и описания этих сообщений. Приняты следующие условные обозначения:

- USER_NAME – имя пользователя;
- COMMAND – одна из следующих команд:
  - резервирование перед обновлением;
  - удаление файлов;
  - перезагрузка/выключение (при применении баз);
  - перечитывание LogConfig.ini;
  - перезагрузка AcWs32nt (при обновлении);
  - синхронизация АМДЗ и NT;
  - запись параметров времени на ввод пароля и предоставление идентификатора в АМДЗ;
- RESULT – результат выполнения команды RPC. Может принимать следующие значения:
  - 0 – команда RPC выполнена успешно;
  - 1 – ошибка выполнения команды;
  - -1 – ошибка RMQ;
- VERSION – номер версии драйвера (ПО). Представляет собой четыре группы цифр, разделённых точкой;
- AMDZ_BOARD_SERIAL_NUM – серийный номер платы АМДЗ;
- OBJECT_NAME – имя подконтрольного объекта или сервера;
- FILE_NAME – имя файла;
- FOLDER_NAME – полное имя каталога;
- NUM1, NUM2 – целые числа;
- COMMAND_RPC – команда удалённого вызова.

Таблица 6 – Перечень сообщений АРМ АБИ

Тип сообщения	Наименование сообщения	Описание сообщения
Базовые сооб-	Проверка соединения с ПКО	Выполнена проверка соединения с ПКО

Тип сообщения	Наименование сообщения	Описание сообщения
щения	Отправлена база пользователей	Процедура отправки базы пользователей на ПКО выполнена успешно
	Изменен пароль пользователя USER_NAME	Процедура смены пароля пользователя USER_NAME (пользователя ПКО) выполнена успешно
	Получение базы пользователей	Процедура получения базы пользователей ПКО выполнена успешно
	Получение журналов…начато	Начало процедуры получения журналов ПКО
	Получение журналов…завершено	Завершение процедуры получения журналов ПКО
	Передача файла списка привилегированных процессов ПКО	Процедура передачи списка привилегированных процессов ПКО выполнена успешно
	Передача файла конфигурации ПКО	Процедура передачи файла конфигурации ПКО выполнена успешно
	Передача фильтров оперативного журнала	Процедура передачи фильтров оперативного журнала выполнена успешно
	Получение списка USB-устройств…начато	Начало процедуры получения списка USB-устройств
	Получение списка USB-устройств…завершено	Процедура получения списка USB-устройств выполнена успешно
	Получение дополнительной информации	Процедура получения дополнительной информации (имени пользователя ПКО и версии ПО ПАК «Аккорд») выполнена успешно
	Получение каталога клиента	Процедура получения каталога клиента ПКО выполнена успешно
	Получение каталога журналов	Процедура получения каталога, в котором хранятся журналы *.low на ПКО
	Открытие файла	Процедура открытия файла на ПКО выполнена успешно
	Обновление ПО	Выполнено обновление программного обеспечения сетевого агента РАУ на подконтрольном объекте

Тип сообщения	Наименование сообщения	Описание сообщения
	Перезапуск службы клиента	Выполнен перезапуск сетевого агента РАУ на подконтрольном объекте
	Получение файла	Процедура получения файла ПКО выполнена успешно
	Запрос списка USB-устройств	Процедура импорта USB-устройств, подключенных к ПКО, выполнена успешно
Сообщения об ошибках	Драйвер Acrun не найден	Драйвер ПАК «Аккорд» не найден на ПКО. Возможно, на ПКО не установлен ПАК «Аккорд». Установите (переустановите) ПАК «Аккорд» на ПКО
	Ошибка получения версии прошивки АМДЗ	Ошибка получения версии прошивки АМДЗ. Если данная ошибка повторяется регулярно, обратитесь в службу технической поддержки ЗАО «ОКБ САПР»
	АМДЗ плата не обнаружена	Установите ПАК «Аккорд» на ПКО
	Ошибка получения версии ТМ-драйвера АМДЗ	Ошибка получения версии ТМ-драйвера АМДЗ на ПКО. Возможно, на ПКО не установлен ТМ-драйвер. Установите (переустановите) ТМ-драйвер на ПКО. Если данная ошибка повторяется регулярно, обратитесь в службу технической поддержки ЗАО «ОКБ САПР»
	Ошибка исполнения команды COMMAND	Исполнение полученной на ПКО от ASMT команды COMMAND завершилось ошибкой
	Ошибка получения текущего пользователя	Ошибка получения текущего пользователя от драйвера Аккорд на ПКО. Если данная ошибка повторяется регулярно, обратитесь в службу технической поддержки ЗАО «ОКБ САПР»
	Ошибка получения журналов Acrun	Ошибка получения оперативных событий от драйвера ПАК «Аккорд». Если данная ошибка повторяется регулярно, обратитесь в службу технической поддержки ЗАО «ОКБ САПР»

Тип сообщения	Наименование сообщения	Описание сообщения
	Ошибка получения журналов АМДЗ	Ошибка прочтения *.azl файлов с ПКО. Если данная ошибка повторяется регулярно, обратитесь в службу технической поддержки ЗАО «ОКБ САПР»
	Ошибка запроса статуса базы пользователей	Ошибка при получении информации о статусе блокирования базы ПАК «Аккорд». Если данная ошибка повторяется регулярно, обратитесь в службу технической поддержки ЗАО «ОКБ САПР»
	Ошибка получения IP-адреса для .VER файла	Ошибка получения IP адреса на ПКО (для заполнения *.VER файла для ASMT). Если данная ошибка повторяется регулярно, обратитесь в службу технической поддержки ЗАО «ОКБ САПР»
	Ошибка чтения базы пользователей из платы АМДЗ	Ошибка чтения *.amz базы из АМДЗ на ПКО. Если данная ошибка повторяется регулярно, обратитесь в службу технической поддержки ЗАО «ОКБ САПР»
	Ошибка при блокировании рабочей станции	Команда блокировки экрана на ПКО выполнилась с ошибкой. Если данная ошибка повторяется регулярно, обратитесь в службу технической поддержки ЗАО «ОКБ САПР»
	Ошибка переоткрытия журналов в Acrun	Ошибка переоткрытия журналов ПАК «Аккорд» по расписанию в 23 00 на ПКО. Если данная ошибка повторяется регулярно, обратитесь в службу технической поддержки ЗАО «ОКБ САПР»
	RPC команда COMMAND вернула RESULT	Возвращение результата выполнения вызванной RPC команды
	Ошибка записи базы пользователей в плату АМДЗ	Ошибка синхронизации базы .amz с АМДЗ на ПКО
	Ошибка синхронизации базы пользователей с NT	Ошибка синхронизации базы .amz с пользователями ОС на ПКО
	Ошибка записи конфигурации таймаутов в плату АМДЗ	Ошибка записи параметров времени на ввод пароля и предоставление идентификатора в АМДЗ на ПКО

Тип сообщения	Наименование сообщения	Описание сообщения
	Ошибка изменения статуса базы пользователей	Ошибка блокирования базы Аккорд при попытке записи
	Сбор журналов Acrun было неожиданно остановлен	Прекращен сбор оперативных событий от драйвера Аккорд
	Ошибка разблокирования рабочей станции	Команда разблокировки экрана на ПКО выполнилась с ошибкой
Информационные сообщения	Версия драйвера Acrun: VERSION	Информация о версии драйвера Аккорд на ПКО
	Версия драйвера АМДЗ: VERSION	Информация о версии драйвера АМДЗ на ПКО
	Версия прошивки АМДЗ: VERSION	Информация о версии прошивки АМДЗ на ПКО
	АМДЗ плата обнаружена	АМДЗ плата обнаружена на ПКО
	Серийный номер платы АМДЗ: AMDZ_BOARD_SERIAL_NUM	Серийный номер платы АМДЗ на ПКО
	Версия ТМ-драйвера АМДЗ: VERSION	Информация о версии ТМ-драйвера на ПКО
	Исполнение команды COMMAND завершено для OBJECT_NAME	Команда принята на ПКО (исполнение не начато)
	Исполнение команды COMMAND завершено	Полученная на ПКО команда от ASMT (или на AcConNet от ПКО) успешно исполнена
	Файл FILE_NAME был скопирован в FOLDER_NAME	Работа с файлами при экспорте/импорте логов/баз
	Инициализация работы с драйверами	Начало работы с драйверами Аккорд и ТМ на ПКО
	Взаимодействие с драйверами остановлено	Работа с драйверами Аккорд и ТМ завершена (при остановке сервиса)
	Команда перечитывания фильтров была отправлена на OBJECT_NAME	Команда на использование новых фильтров принята на ПКО (исполнение не начато)
	Файл журналов Acrun был успешно переоткрыт	На ПКО успешно переоткрыты журналы Аккорд по расписанию в 23:00

Тип сообщения	Наименование сообщения	Описание сообщения
	Файл FILE_NAME был сохранен. Байты: NUM1 to NUM2	Принятый файл был сохранен (на ПКО или AcConNet)
	Файл FILE_NAME был отправлен на OBJECT_NAME	Файл был успешно отправлен в RMQ (с ПКО для AcConnet или наоборот)
	Сообщение о смене пароля было отправлено	Сообщение о смене пароля передано в RMQ
Отладочные сообщения	Действие: удаление файла FILE_NAME завершено	Удаление файла на ПКО после его передачи на сервер успешно завершено
	Действие: удаление файла FILE_NAME начато	Начало выполнения удаления файла на ПКО после его передачи на сервер
	Действие: перемещение файла FILE_NAME завершено	Перемещения файла на ПКО после его передачи на сервер успешно завершено
	Действие: перемещение файла FILE_NAME начато	Начало выполнения перемещения файла на ПКО после его передачи на сервер
	Действие: ничего не делать	Файл с ПКО передан на сервер, никакое действие после этого не требуется
	Исполнение команды COMMAND для OBJECT_NAME	Команда была отправлена на ПКО (исполнение не начато)
	Команда COMMAND получена	На ПКО получена команда от ASMT
	Начато исполнение команды COMMAND	На ПКО начато исполнение полученной от ASMT команды (или на AcConNet от ПКО)
	Начато копирование файла FILE_NAME в FOLDER_NAME	Начата работа с файлами при экспорте/импорте логов/баз
	Файл FILE_NAME не был изменен	Файл на сервере централизованного управления идентичен передаваемому файлу с ПКО
	Журналы АМДЗ получены	Прочитан *.azl файл из АМДЗ на ПКО
	База пользователей успешно прочитана из платы АМДЗ	*.amz база прочитана из АМДЗ на ПКО
	Рабочая станция успешно заблокирована	Установлен экран блокировки на ПКО

Тип сообщения	Наименование сообщения	Описание сообщения
	Файл FILE_NAME был принят от OBJECT_NAME. Байты: NUM1 to NUM2	Файл принят от ПКО на AcConNet (или наоборот)
	Начата передача команды перечитывания фильтров на OBJECT_NAME	Команда на использование новых фильтров была отправлена на ПКО (исполнение не начато)
	RPC команда COMMAND_RPC была вызвана	RPC команда была вызвана (на ПКО или AcConNet)
	База пользователей успешно записана в плату АМДЗ	База .amz успешно записана в плату АМДЗ на ПКО
	База пользователей успешно синхронизирована с NT	База .amz успешно синхронизирована с базой пользователей ОС на ПКО
	Конфигурация таймаутов была успешно записана в плату АМДЗ	Параметры времени на ввод пароля и предоставление идентификатора записаны в АМДЗ на ПКО
	Часть файла FILE_NAME была отправлена на OBJECT_NAME. Байты: NUM1 to NUM2	Детализация информации о передаваемых файлах (по частям для больших файлов) с ПКО
	Начата передача части файла FILE_NAME на OBJECT_NAME. Байты: NUM1 to NUM2	Детализация информации о передаваемых файлах (по частям для больших файлов) с ПКО
	Начата передача файла FILE_NAME на OBJECT_NAME	Начата передача файла в RMQ (с ПКО для AcConNet или наоборот)
	Начата передача сообщения о смене пароля	Пользователь на ПКО сменил пароль, начата передача информации в RMQ
	Статус рабочей станции Online был изменен на Offline	В AcConNet изменен статус ПКО
	Статус рабочей станции Offline был изменен на Online	В AcConNet изменен статус ПКО
	СЗИ сообщение было отправлено	СЗИ сообщение с ПКО передано в RMQ
	Начата передача СЗИ сообщения	Начата передача СЗИ сообщения с ПКО в RMQ
	Сбор журналов Acrun был остановлен успешно	Сбор оперативных событий от драйвера Аккорд остановлен корректно (при остановке сервиса)

Тип сообщения	Наименование сообщения	Описание сообщения
	Рабочая станция была успешно разблокирована	Снят экран блокировки на ПКО
	USB файл был успешно создан	На ПКО создан файл с информацией о USB для ASMT (для дальнейшей пересылки)
	VER файл был успешно создан	На ПКО создан файл с информацией об используемых версиях программного и аппаратного обеспечения для ASMT (для дальнейшей пересылки)

При формировании базовых сообщений, сигнализирующих о возникновении ошибок в ходе выполнения тех или иных операций, в поле «Примечание» журнала АРМ АБИ приводятся следующие записи, детализирующие возникшие ошибки:

- Команда не поддерживается;
- Ошибка открытия сокета;
- Неверный адрес;
- Станция занята;
- Неверные параметры;
- Ошибка в подписи файла;
- Идет длительное выполнение команды;
- Критическая ошибка сети;
- Не загружен драйвер TmDrv32.dll;
- Не прошел логин в базу АМДЗ;
- Путь не найден;
- Файл не найден;
- Доступ запрещен;
- Неверный Handle файла;
- Нет памяти;
- Ошибка создания каталога;
- Ошибка удаления каталога;
- Ошибка создания файла;

- Ошибка удаления файла;
- Разрыв связи;
- Для компьютера не назначен Supervisor;
- Операция отменена Администратором.

Данные записи сигнализируют о возникновении критических ошибок в ASM. При их появлении необходимо обратиться в службу технической поддержки ЗАО «ОКБ САПР».

9 Перечень принятых сокращений

АИБ	Администратор информационной безопасности
АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
ИБ	Информационная безопасность
ИС	Информационная система
КТС	Комплекс технических средств
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
НШР	Нештатный режим
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
РАУ	Распределенный Аудит и Управление
СВТ	Средства вычислительной техники
СЗИ	Средство защиты информации
СУ	Система управления
УП	Управление персоналом

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

зм.	Номера листов (страниц)				Всего листов (стр.) в документе	№ документа	Входящий № сопроводительного документа	Подпись	Дата
	измененных	заменен-ных	новых	Аннулированных					

СОГЛАСОВАНО

Наименование организации, предприятия	Должность исполнителя	Фамилия, имя, отчество	Подпись	Дата