УТВЕРЖДЕН
11443195.4012-053 91 2012 ЛУ

СИСТЕМА УДАЛЕННОГО ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ СЗИ ОТ НСД АККОРД

Руководство Администратора информационной безопасности

Листов 65

Москва
2014

Формат А4

АННОТАЦИЯ

Специализированная система удаленного централизованного управления средствами защиты информации от несанкционированного доступа Аккорд (в дальнейшем также СУЦУ, Система) предназначена для реализации требований нормативных документов Банка России по ИБ, централизованного мониторинга событий ИБ и управления средствами защиты информации от несанкционированного доступа, функционирующими в АС Банка России.

Данный документ описывает действия Администратора ИБ СУЦУ связанные с непосредственной работой СУЦУ в штатном режиме функционирования.

СОДЕРЖАНИЕ

1 Введение

1.1 Область применения

Деятельность Администратора ИБ СУЦУ.

1.2 Функции Администратора ИБ СУЦУ

Администратор ИБ СУЦУ

- Производит следующие настройки:
  - настройка политик безопасности;
  - настройка правил доступа к коммутационным портам и периферийным устройствам.
- Управляет учетными записями персонала СУЦУ, включая назначение пользователей, выполняющих роли персонала СУЦУ.
- Осуществляет контроль управляющего воздействия на компоненты СУЦУ в части:
  - изменения настроек (включая настройки мониторинга);
  - применения шаблонов настроек.
- Формирует логические группы из серверов и АРМ (технологические участки) с применением групповых политик для управления СЗИ от НСД, установленных на них.
- Участвует в разборе и устранении нештатных ситуаций, связанных как с работой СУЦУ, так и с работой СЗИ от НСД.

1.3 Комплект поставки

СУЦУ является подсистемой, внедряемой путем поставки, установки и настройки следующих компонентов:

- сервер централизованного управления.
- клиент централизованного управления (на каждый АРМ, являющийся подконтрольным объектом).
- серверные и клиентские компоненты, реализующие транспортные функции (подсистема распределенного аудита и управления), серверные компоненты, реализующие функции управления (подсистема Accord Security Management Special Edition (ASM SE)) СЗИ от НСД подконтрольных объектов (далее по тексту ПКО) – на CD;
- лицензии на подключения управляемых объектов к СУЦУ на DS 1996;
- комплект рабочей документации на CD.

2 Назначение и условия применения

2.1 Назначение

СУЦУ обеспечивает:

- централизованный сбор и хранение информации о зарегистрированных событиях доступа к подконтрольным объектам;
- возможность централизованного управления средствами защиты информации от несанкционированного доступа на подконтрольных объектах;
- единую точку контроля доступа к периферийным устройствам и контроля использования отчуждаемых машинных носителей.

2.2 Условия применения

Обязательным условием применения Системы является оснащение элементов АС следующими программно-аппаратными средствами:

На рабочих станциях

- ПАК СЗИ от НСД «Аккорд»;
- клиент централизованного управления.

На сервере централизованного управления

- ПАК СЗИ от НСД «Аккорд»;
- сервер централизованного управления.

3 Планирование работы и эксплуатация комплекса

3.1 Общие сведения

Планирование применения СЗИ Аккорд осуществляется на этапе общего планирования защиты. Содержание этого этапа заключается в составлении плана защиты. Обычно план защиты - это документ, в который входят данные о характере и составе обрабатываемой локальной сети информации, составе технических и программных средств, возможных угрозах системе и способах их возможной реализации, и соответственно описание выбранных методов и средств защиты от этих угроз.

Для настройки средств защиты комплекса Аккорд рекомендуется выявить и отразить в плане защиты следующие характеристики защищаемой системы:

- перечень задач, решаемых сотрудниками организации с использованием автоматизированной системы;
- полный перечень используемых при решении каждой конкретной задачи программ;
- полный перечень используемых при решении каждой задачи данных;
- подробный перечень имеющихся в защищаемой локальной сети технических средств (рабочих станций, серверов и т. д.) с указанием их состава, конфигурации и характеристик;
- перечень размещенных на каждой рабочей станции и сервере системных и прикладных программ, файлов и баз данных;
- перечень установленных на рабочих станциях и серверах программно-аппаратных средств защиты;
- списки пользователей системы с указанием решаемых ими задач из общего перечня задач и предоставляемых им полномочий по доступу к рабочим станциям и серверам сети.

Для более эффективного применения комплекса Аккорд и поддержания уровня защищенности необходимы:

- физическая охрана всех компонентов автоматизированной системы обработки информации, в т.ч. обеспечение мер по неизвлечению контроллера комплекса;
- использование в автоматизированной системе технических и программных средств, сертифицированных как в Системе ГОСТ Р, так и в системе Государственной системы безопасности информации (ГСЗИ);
- периодическое тестирование средств защиты комплекса;

- разработка и ведение учетной и объектовой документации (инструкция администратора, инструкций пользователей, журнал учета идентификаторов и отчуждаемых носителей пользователей и др.). Все разработанные учетные и объектовые документы должны быть согласованы, утверждены у руководства и доведены до сотрудников (пользователей). Это необходимо для того, чтобы План защиты организации (предприятия, фирмы и т. д.) и действия Администратора ИБ получили юридическую основу.

При эксплуатации комплекса Администратор ИБ решает 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;

- проводит оперативное наблюдение за работой пользователей;

- обеспечивает оперативное управление работой пользователей.

3.2 Изменение настроек средств защиты информации

Администратор ИБ может изменять настройки серверной части СУЦУ для подключения новых объектов, политики безопасности, контроля доступа, разрешенных коммуникационных портов.

3.3 Предварительная настройка сетевого идентификатора

Администратор ИБ СУЦУ выполняет процедуру предварительной настройки сетевого идентификатора:

- запускает ASM (Пуск -> Программы -> ASM -> Запуск СУЦУ СЗИ от НСД);

- предъявляет идентификатор Администратора ИБ;

- открывает вкладку Настройка>Основные настройки;

- в поле «Учетная запись ASM» нажимает кнопку <Настройка>, затем предъявляет сетевой идентификатор (при этом в сетевом идентификаторе создается учетная запись «ASM_ACCOUNT»[1)]).

Дальнейшую работу с сетевым идентификатором выполняет Администратор СУЦУ в соответствии с подразделом 3.1.2.2 документа «Руководство Администратора СУЦУ» 11443195.4012-053 90.

[1)] С помощью учетной записи «ASM_ACCOUNT» становится возможным выполнение процедур удаленного управления ПКО: добавление, удаление пользователей, смена пароля пользователя и т.д.

3.4 Оперативное наблюдение за работой пользователей

Администратор ИБ имеет возможность осуществлять оперативное управление работой пользователей.

4 Работа с ASM

4.1 Управление

Пункты 4.1.1-4.1.5 посвящены описанию функций управления ASM.

Пользовательский интерфейс вкладок ASM, доступных для обслуживающего персонала СУЦУ в рамках реализации процедур управления, подчиняется единому принципу:

- кнопка <Добавить> предназначена для добавления той или иной сущности;
- кнопка <Удалить> предназначена для удаления той или иной сущности;
- с помощью кнопки <Импорт> можно импортировать настройки с компьютеров Системы в ASM.
- с помощью кнопки <Экспорт> можно экспортировать настройки из ASM на компьютеры системы.

При работе с ASM следует помнить, что максимальное количество символов в именах ролей, технологических участков, компьютеров и учетных записей пользователей составляет 100 символов.

4.1.1 Вкладка «Роли»

Права доступа (ПРД) для учетной записи определяются ролью.

В ASM предусмотрены следующие встроенные роли:

- **Admins_NSHR** - используется для первоначальной настройки системы, характеризуется правом полного доступа в ASM, под этой ролью работает Администратор нештатного режима (Администратор НШР) СУЦУ;
- **Admins_SCM** - под этой ролью работает Администратор СУЦУ.
- **Admins** – соответствует группе ‘Администраторы’ в «Аккорде»;
- **Admins_XXX**[1)] - 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»; в ASM;
- **Everyone_XXX** - автоматически создается при создании нового технологического участка и уничтожается только при удалении данного участка; соответствует группе ‘Обычные’ в «Аккорде»; в ASM;
- **AIBs_SCM** – Администратор информационной безопасности специализированной подсистемы управления и мониторинга средств защиты информации от несанкционированного доступа;
- **AIB_TU: имя роли** – роль, под которой работает Администратор ИБ технологического участка; создается после добавления технологического участка Администратором ИБ;

[1)] Номер **XXX** соответствует номеру участка.

- **OIBs_SCM** - под этой ролью работает Оператор информационной безопасности СУЦУ.

Для того чтобы создать новую роль, редактировать или удалить уже существующую, следует открыть в ASM вкладку Управление>Роли (рис. 1).

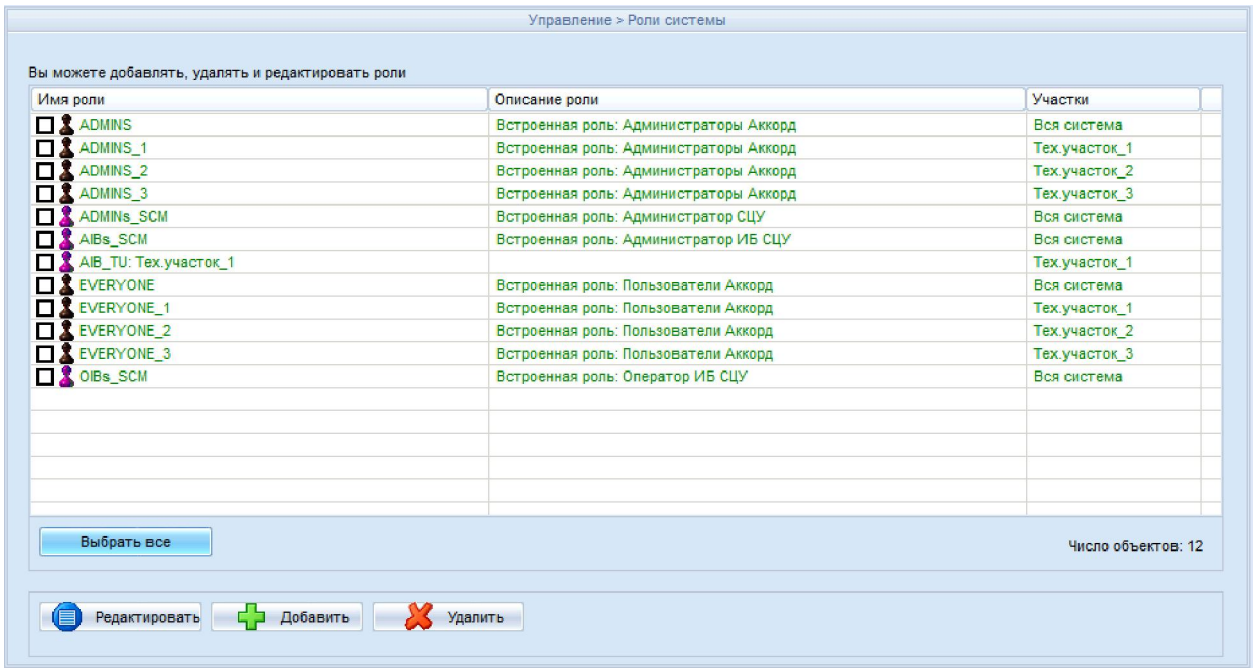

Рисунок 1 - Роли системы

Для добавления новой роли необходимо нажать кнопку <Добавить>. В появившемся окне (рисунок 2) можно задать роли имя (имя роли следует вводить корректно, так как после создания роли изменить имя нельзя). Также можно дать описание роли и назначить эту роль для технологического участка (эти параметры не являются обязательными для заполнения).

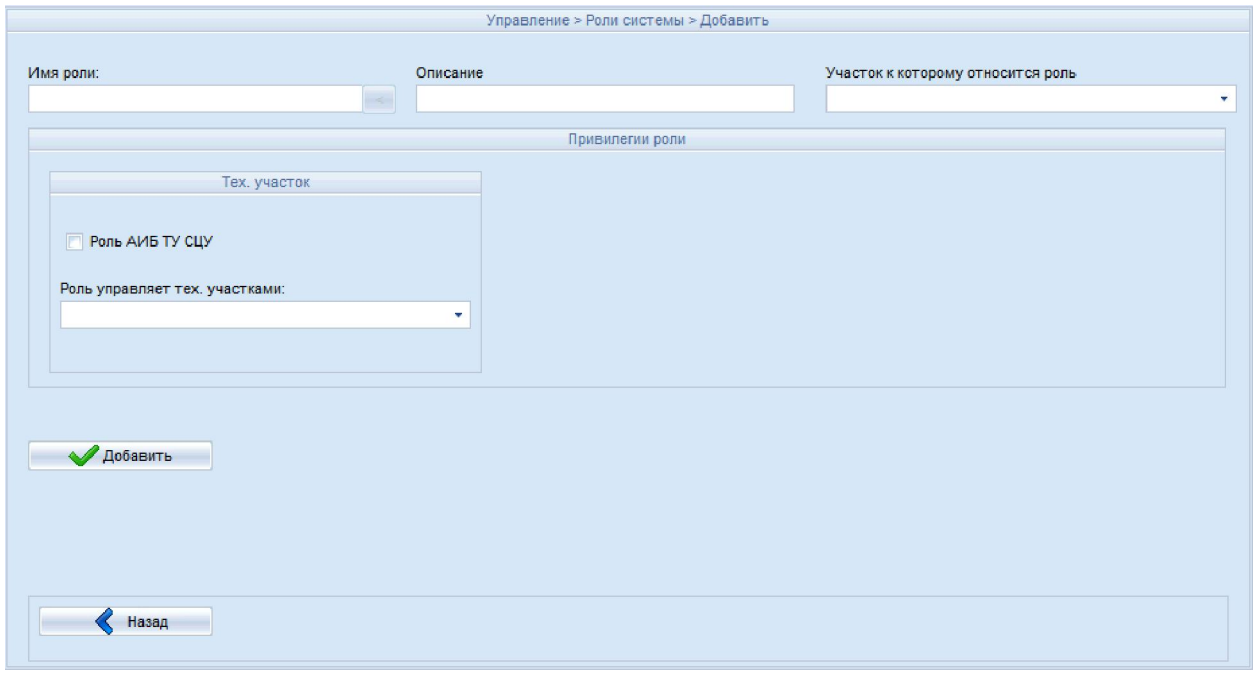

Рисунок 2 – Создание роли

По нажатии кнопки <Добавить> (рисунок 2) на экране появляется редактор ПРД, в котором следует выбрать необходимые параметры роли.

При создании роли по шаблону необходимо левой кнопкой мыши выбрать раскрывающийся список в поле «Имя роли» (рисунок 2). На экране появляется окно, в котором необходимо выбрать роль и нажать кнопку <Ok> (рисунок 3).

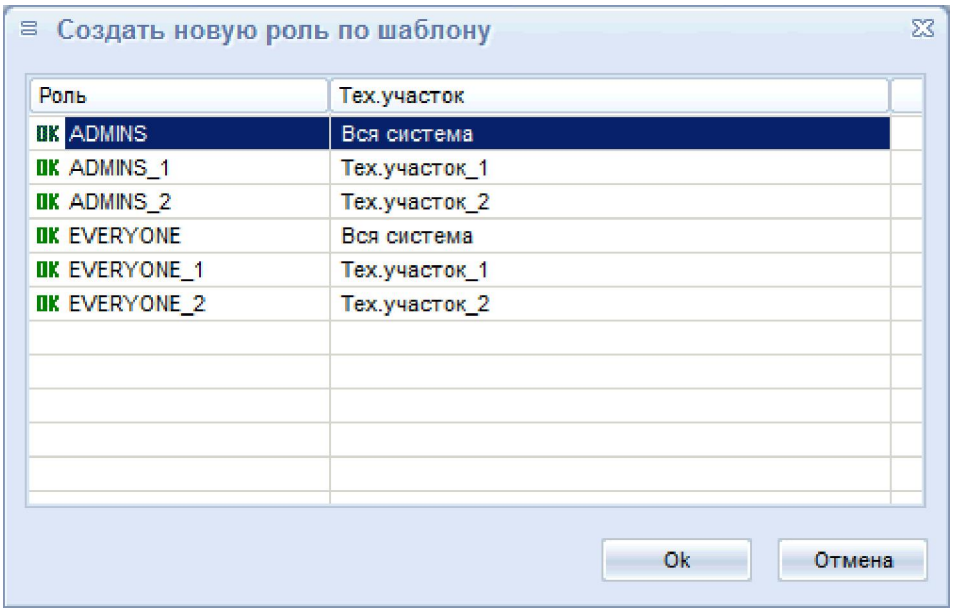

Рисунок 3 – Создание роли по шаблону

После выполнения данной процедуры у новой роли будут определены такие же задачи для запуска и файлы для проверки КЦ, как и у выбранной из шаблона роли.

Для редактирования следует дважды щелкнуть по роли системы либо нажать кнопку <Редактировать>, после чего на экране появляется следующее окно (рисунок 4):

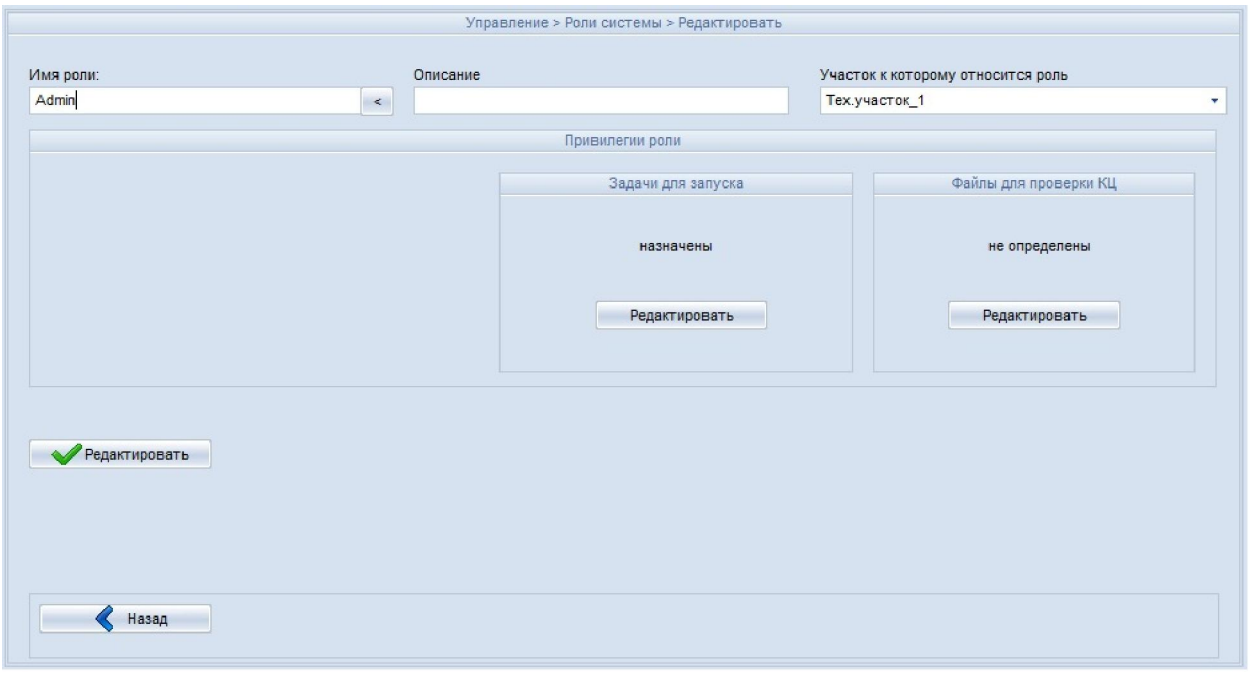

Рисунок 4 - Редактирование роли

Чтобы задать или редактировать задачи для запуска роли необходимо нажать кнопку <Редактировать> в поле «Задачи для запуска». После этого на экране появляется окно (рисунок 5), в котором нужно редактировать необходимые параметры и нажать кнопку <Сохранить>.

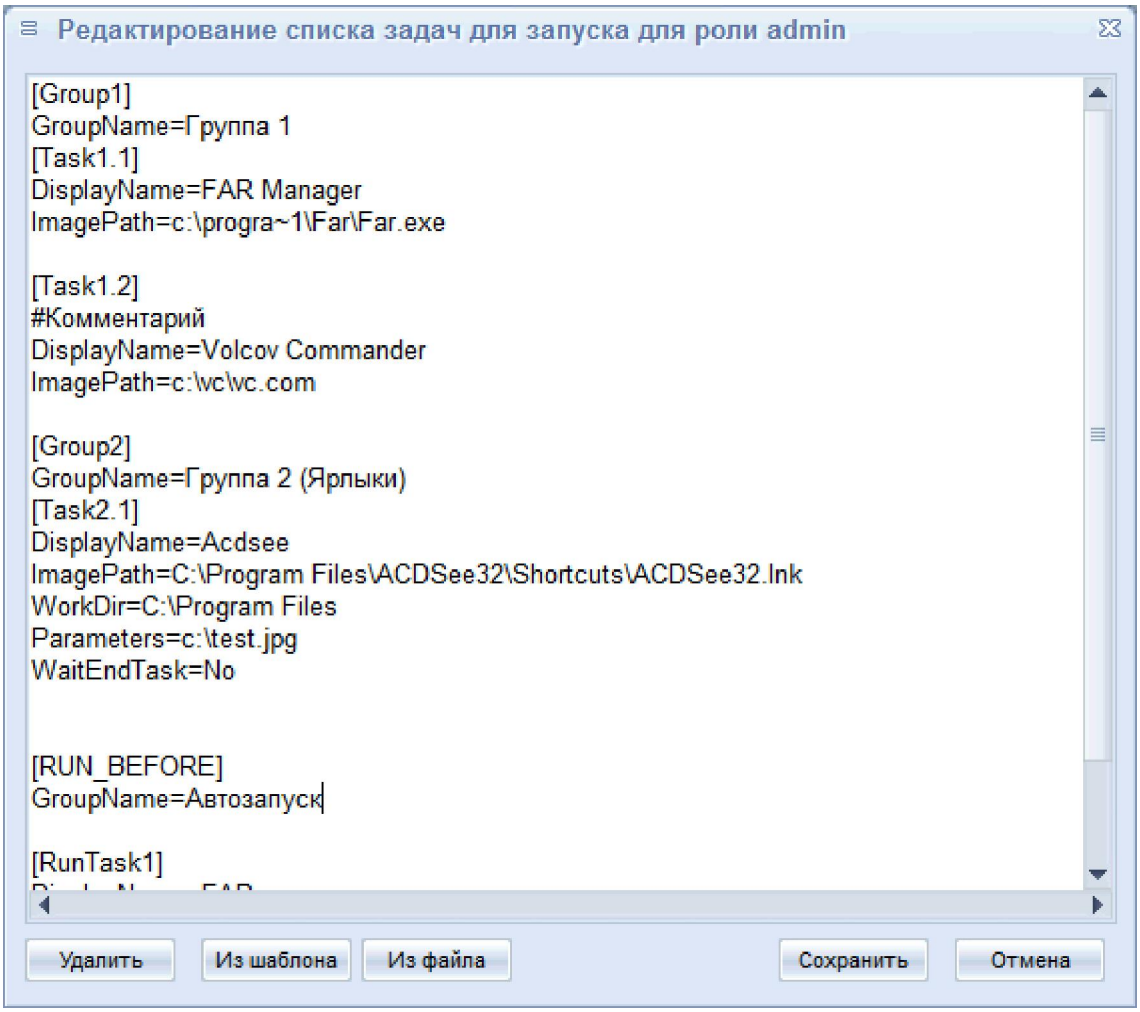

Рисунок 5 – Редактирование списка задач для запуска

При создании списка задач для запуска по шаблону необходимо нажать кнопку <Из шаблона> (рисунок 5). После выполнения описанной процедуры на экране появляется окно:

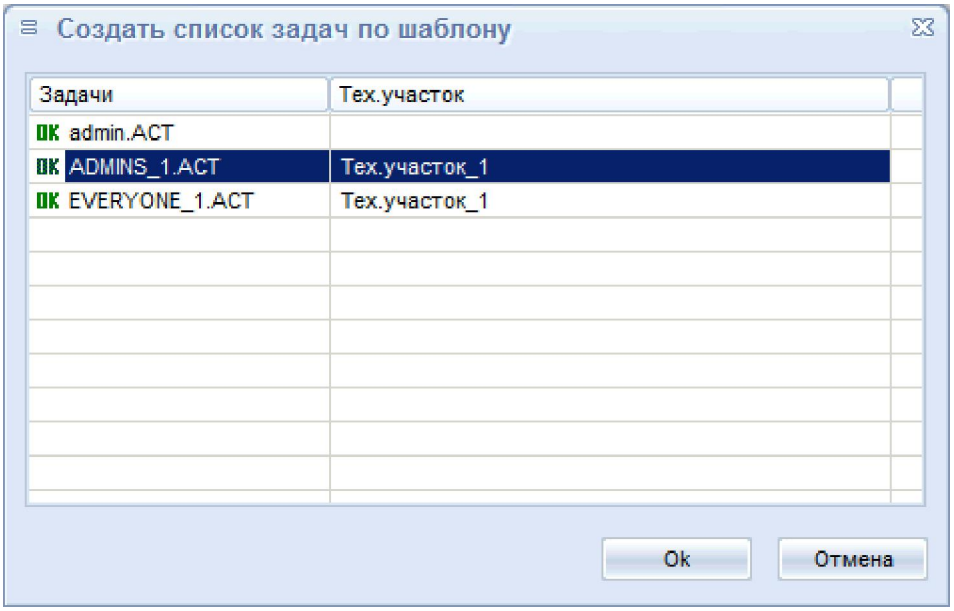

Рисунок 6 – Создание списка задач по шаблону

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 необходимо нажать кнопку <Из файла>. После выполнения описанной процедуры на экране появляется окно:

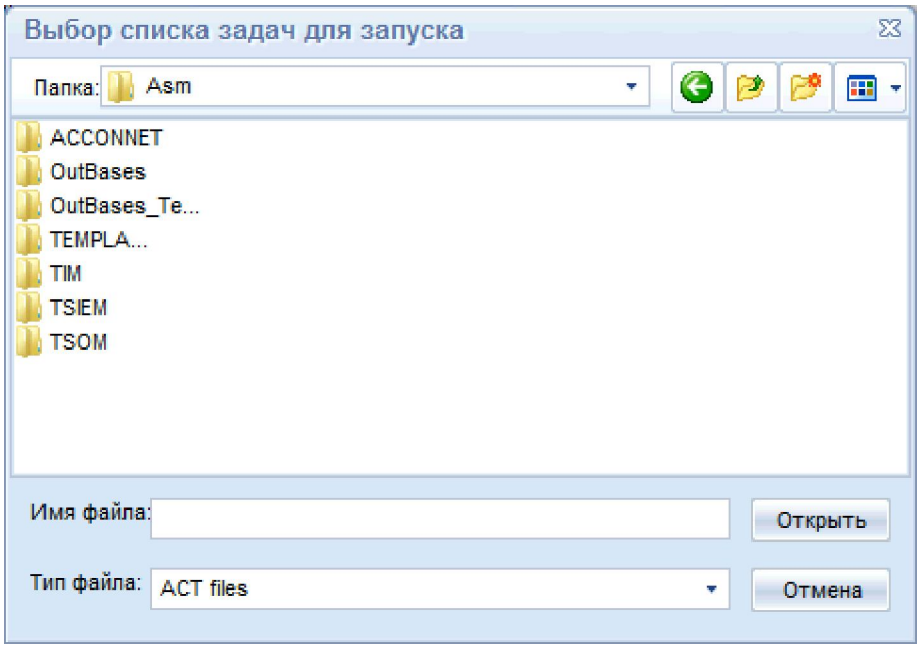

Рисунок 7 – Создание списка задач из файла

Необходимо выбрать нужный каталог (рисунок 7) и нажать кнопку <Открыть>.

В появившемся на экране окне необходимо выбрать нужный файл (рисунок 8) и нажать кнопку <Открыть>.

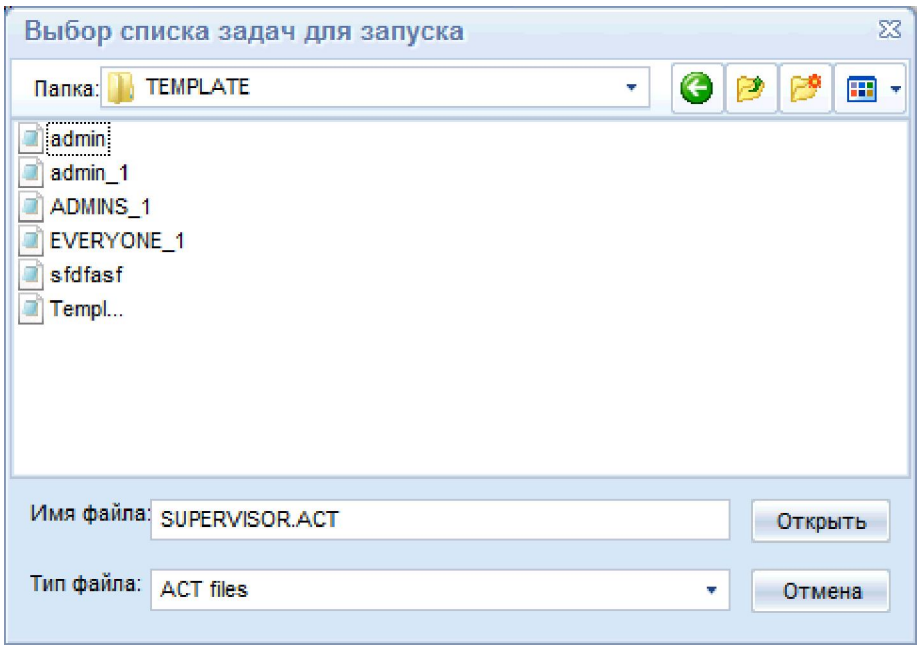

Рисунок 8 – Выбор задач для запуска из файла

После того, как изменения внесены, необходимо нажать кнопку <Сохранить> (рисунок 5), для отмены операции – кнопку <Отмена> (рисунок 5).

Чтобы задать или редактировать файлы для проверки КЦ необходимо нажать кнопку <Редактировать> в поле «Файлы для проверки КЦ». После этого на экране появляется окно:

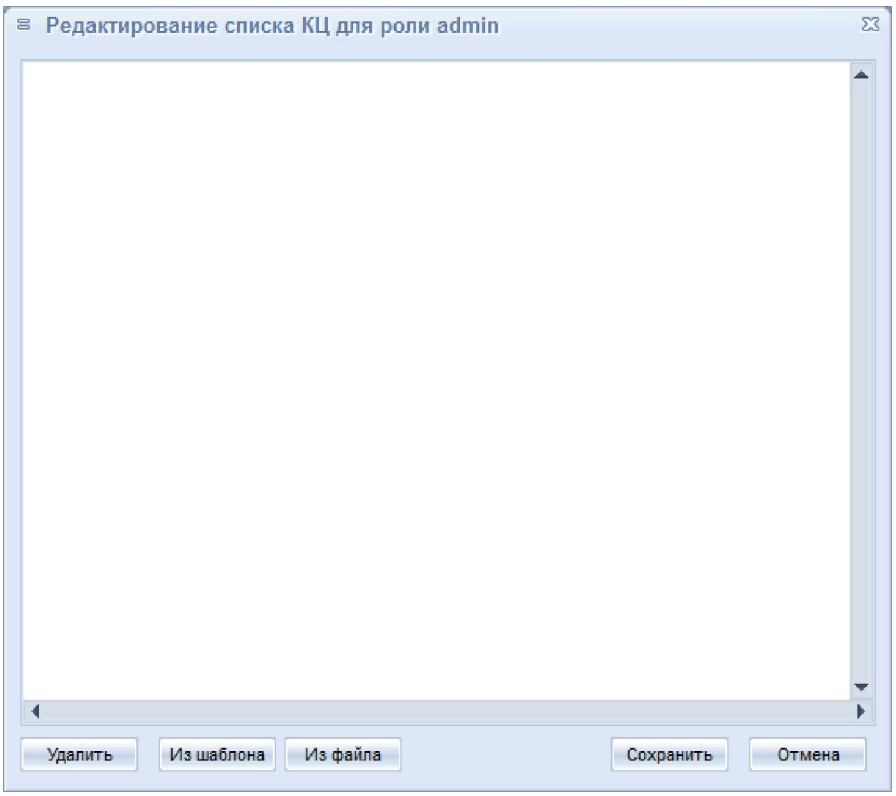

Рисунок 9 – Редактирование списка КЦ для роли

Для создания списка файлов для проверки КЦ по шаблону необходимо нажать кнопку <Из шаблона> (рисунок 9). После выполнения описанной процедуры

на экране появляется окно (рисунок 10), в котором необходимо выбрать нужный шаблон и нажать кнопку <Ok>.

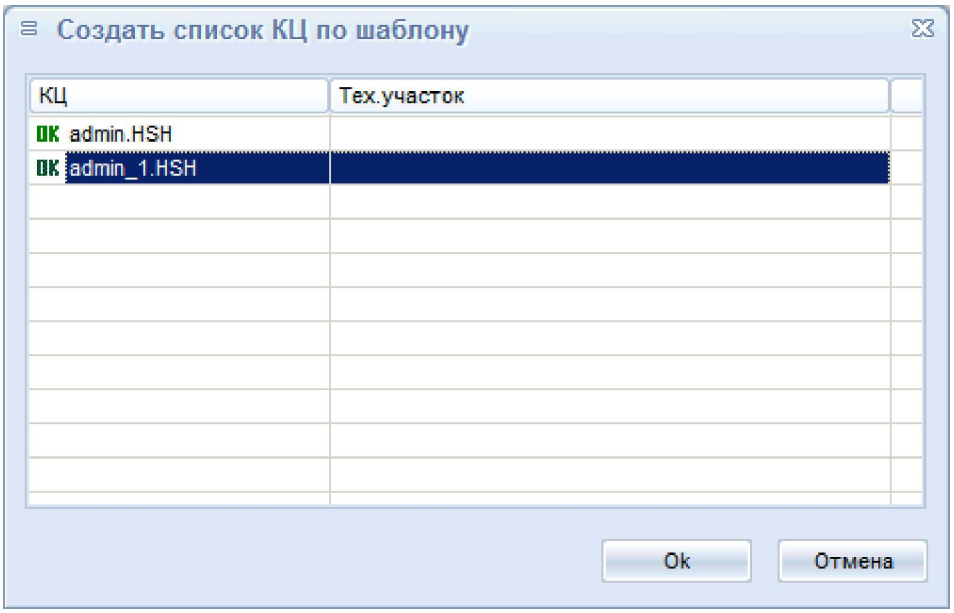

Рисунок 10 – Создание списка файлов для проверки КЦ по шаблону

Для создания списка файлов для проверки КЦ из файла необходимо нажать кнопку <Из файла> (рисунок 9). После выполнения описанной процедуры на экране появляется окно выбора каталога. Необходимо выбрать нужный каталог и нажать кнопку <Открыть>.

В появившемся на экране окне необходимо выбрать нужный файл и нажать кнопку <Открыть> (рисунок 11).

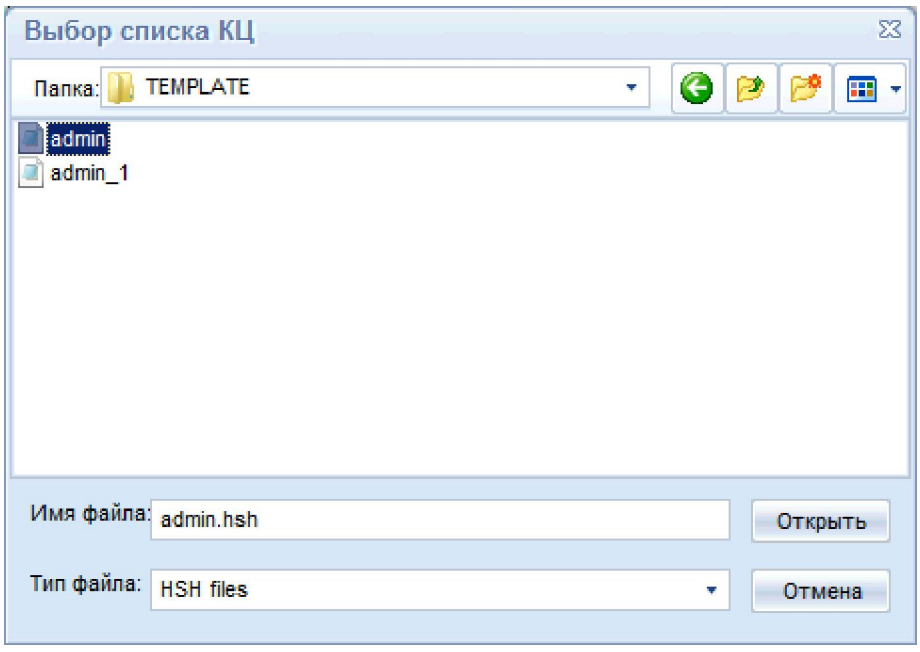

Рисунок 11 – Выбор файлов для проверки КЦ

После того, как изменения внесены, необходимо нажать кнопку <Сохранить> (рисунок 9), для отмены операции – кнопку <Отмена> (рисунок 9).

Далее необходимо нажать кнопку <Редактировать> (рисунок 4). На экране появляется редактор прав доступа ACED32 (рисунок 12), в котором можно изме-

нить ПРД роли, 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).

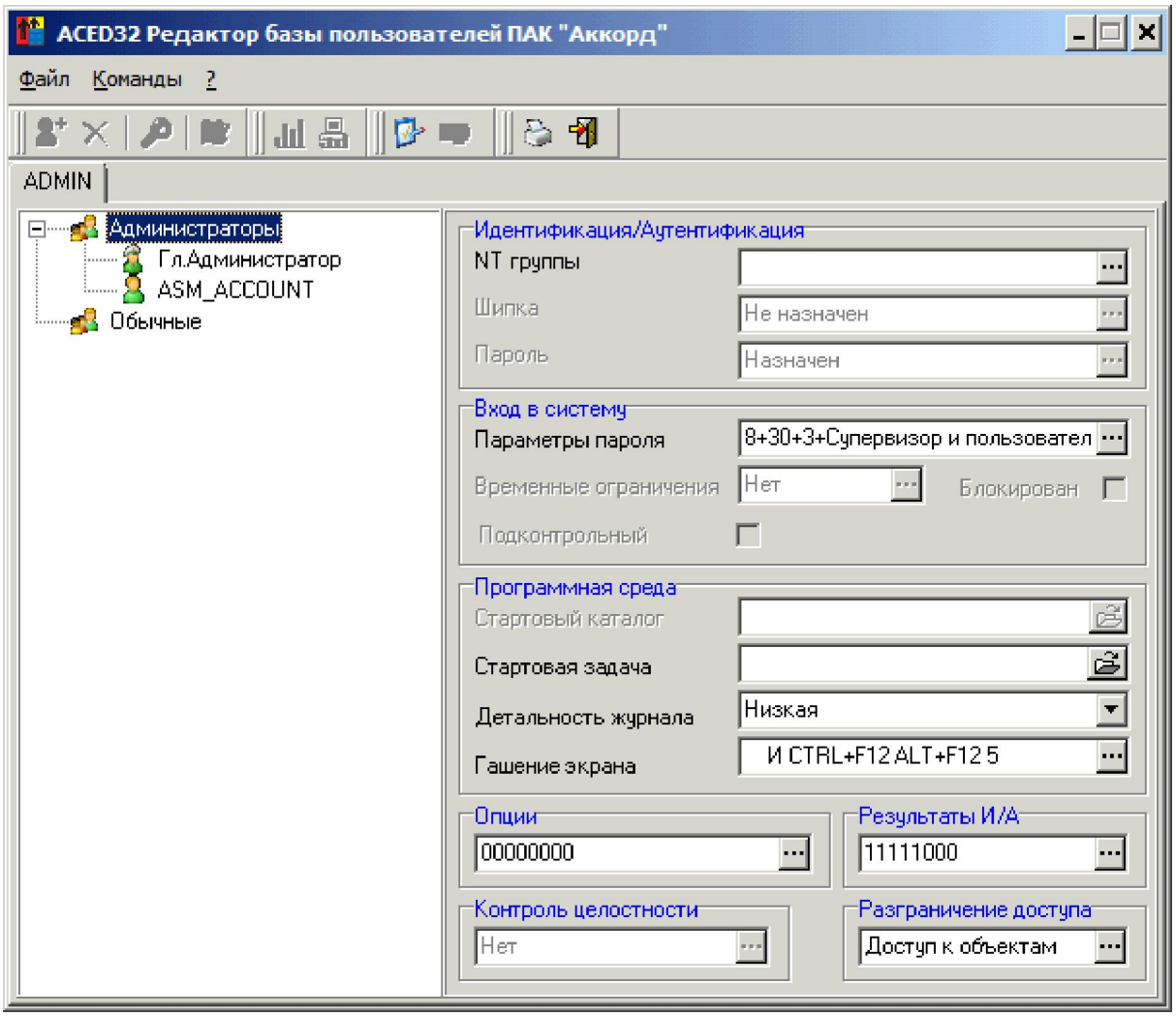

Рисунок 12 - Редактирование базы пользователей «Аккорд»

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 13 показан список объектов (устройства, файловая система, реестр), для которых могут быть заданы правила разграничения доступа (подробнее см. документ «ПАК “Аккорд-Win32“ (версия 4.0). Установка правил разграничения доступа. Программа ACED32» 11443195.4012-036 97”», подраздел 6.15 или «ПАК “Аккорд-Win64“ (версия 5.0). Установка правил разграничения доступа. Программа ACED32» 11443195.4012-036 97”», подраздел 6.15).

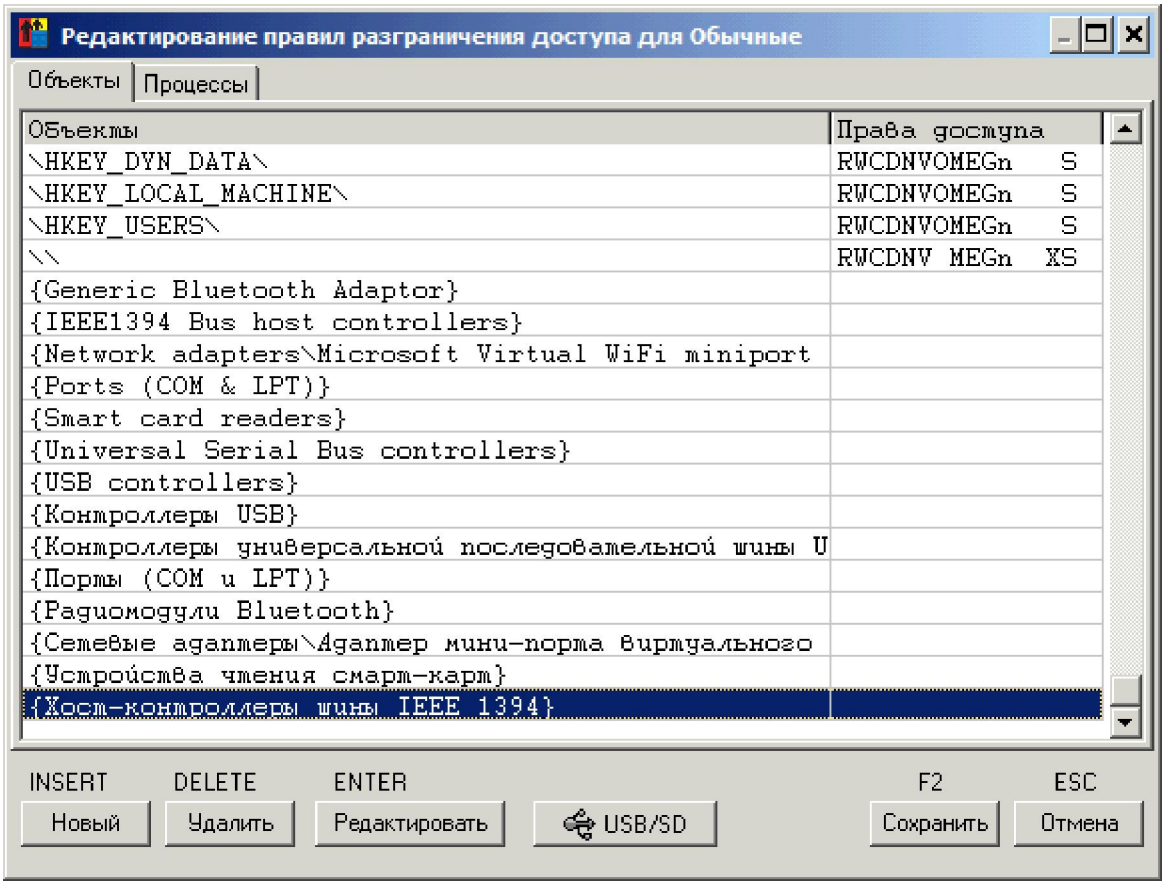

Рисунок 13 – Перечень объектов для установки прав доступа

Для удаления роли во вкладке Управление>Роли необходимо выбрать роль и нажать кнопку <Удалить> (рисунок 1). После этого на экране появляется следующее сообщение (рисунок 14):

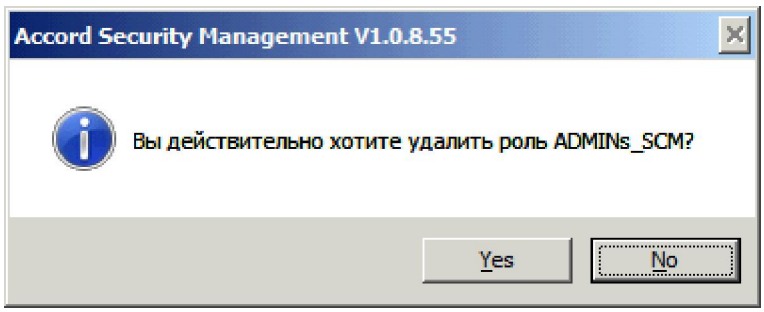

Рисунок 14 – Удаление роли

Если действительно необходимо удалить роль, следует нажать кнопку <Да>.

ВНИМАНИЕ! Если роль сопоставлена некоторому технологическому участку, ее могут редактировать только Администратор ИБ соответствующего технологического участка!

4.1.2 Вкладка «Тех. участки»

Для того чтобы работать с технологическими участками, необходимо открыть в ASM вкладку Управление>Тех. участки. Для создания технологического участка следует нажать кнопку <Добавить> (рисунок 15).

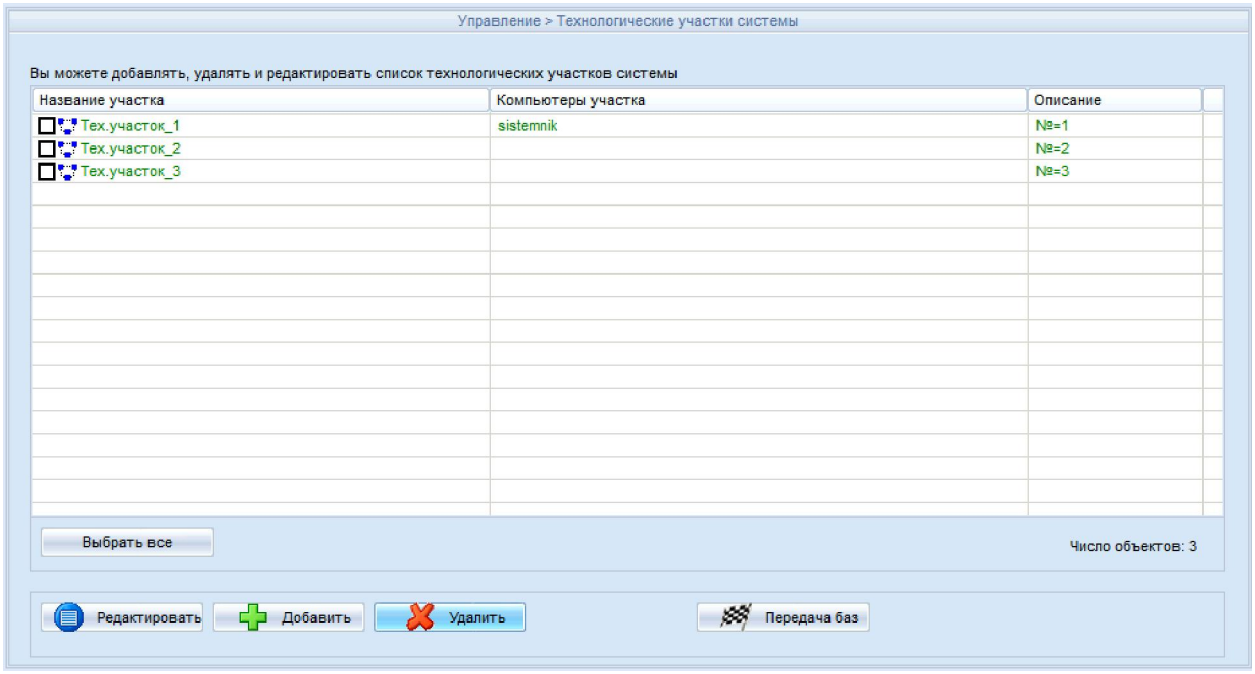

Рисунок 15 - Технологические участки системы

Есть возможность ввести название и описание технологического участка, роли, управляющие участком. Для сохранения изменений следует нажать кнопку <Применить> (рисунок 16).

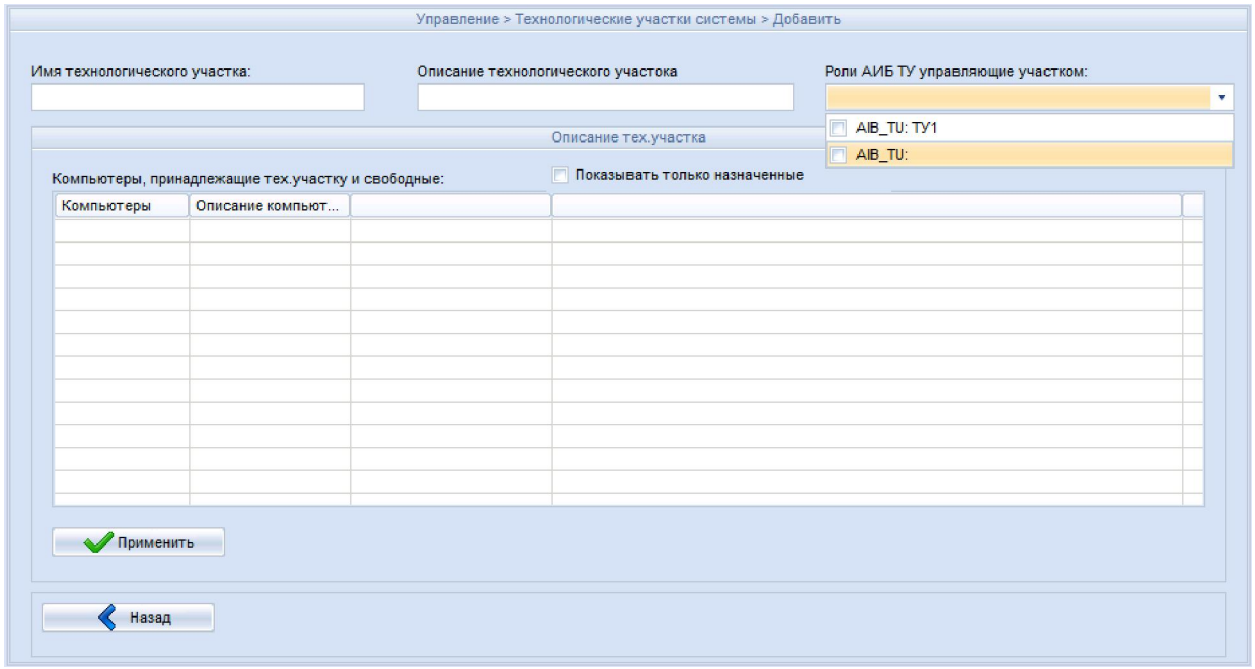

Рисунок 16 - Создание технологического участка

Далее следует добавить Администратора ИБ для созданного технологического участка. Администратор ИБ СУЦУ может настраивать полномочия по администрированию технологических участков.

Для этого после добавления технологического участка необходимо перейти на вкладку «Роли» и нажать кнопку <Добавить>. Затем ввести имя роли (чтобы создать роль Администратора ИБ технологического участка по шаблону, следует выбрать раскрывающийся список в поле «Имя роли» и в появившемся списке шаблонов (рисунок 3) выбрать необходимый), установить флаг «Роль АИБ ТУ». При этом имя роли изменится на «AIB_TU: имя роли». Ниже нужно выбрать технологический участок из списка «Тех. участок» и нажать кнопку <Добавить> (рисунок 17). Администратор ИБ технологического участка может управлять несколькими технологическими участками.

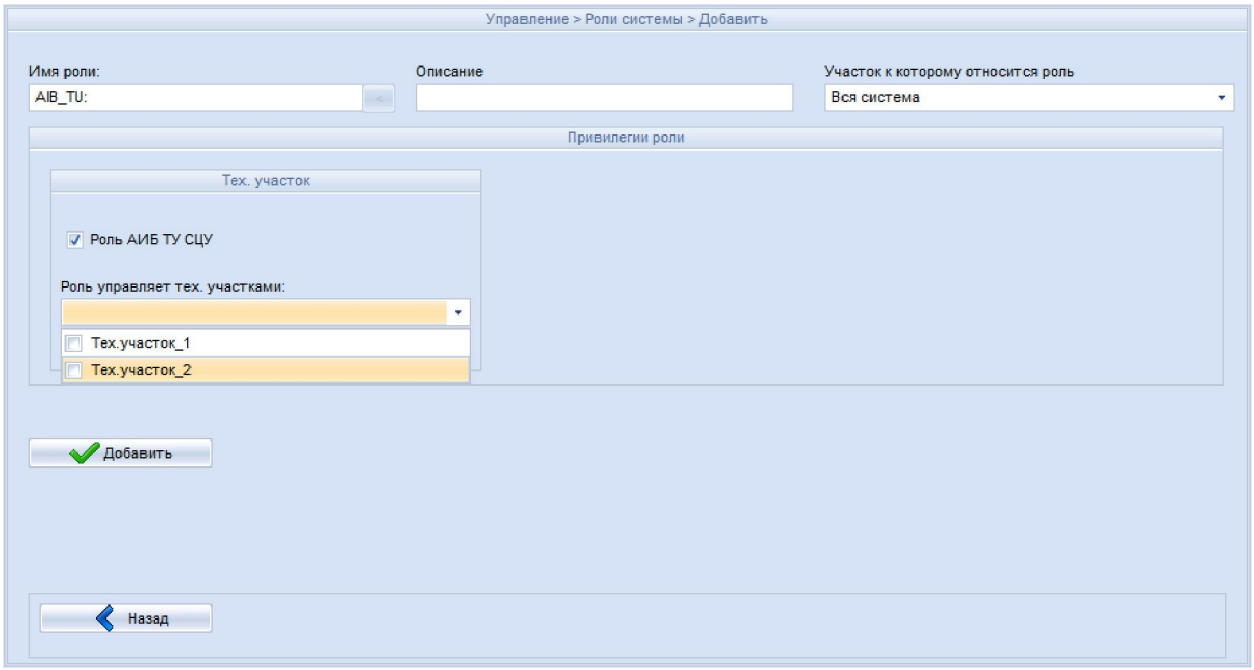

Рисунок 17 - Сопоставление роли Администратора ИБ ТУ с технологическим участком

Затем следует перейти на вкладку «Компьютеры», выбрать компьютер, который должен принадлежать данному технологическому участку, дважды щелкнуть по соответствующей записи левой кнопкой мыши или нажать кнопку <Редактировать>. Далее необходимо выбрать из списка, какому технологическому участку должен принадлежать данный компьютер, и нажать кнопку <Применить> (рисунок 18).

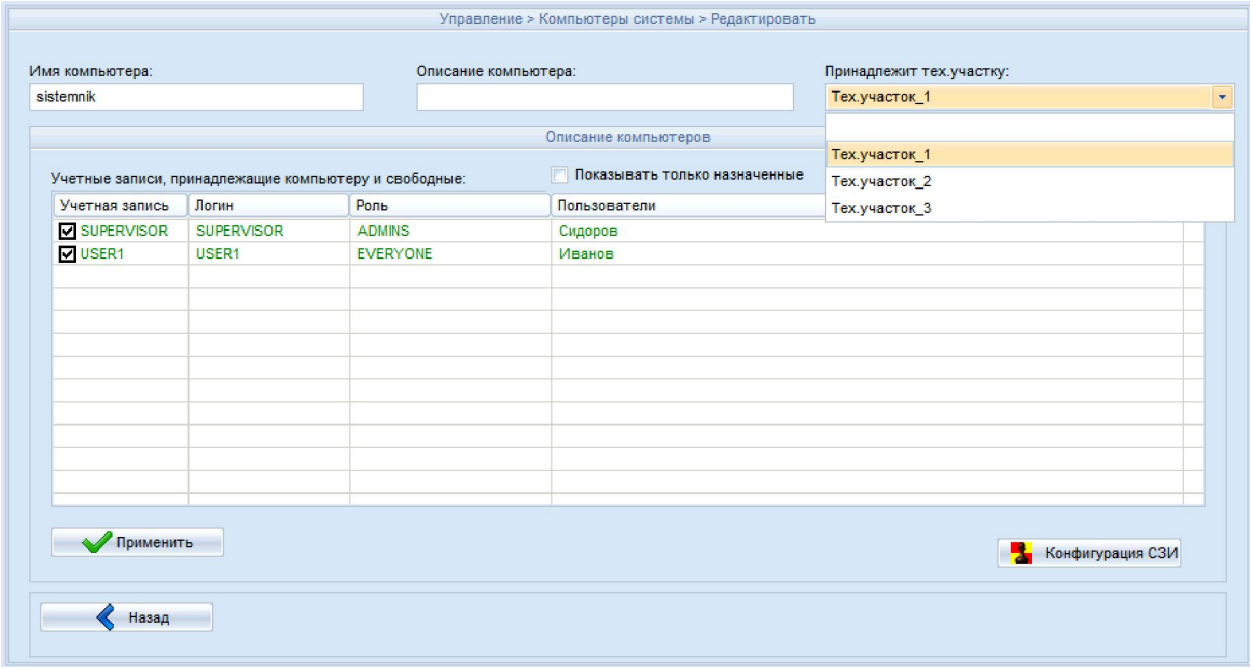

Рисунок 18 - Выбор компьютеров, принадлежащих технологическому участку

Чтобы убедиться, что после выполнения этих действий выбранный компьютер принадлежит технологическому участку, следует открыть вкладку «Тех. участки» (рисунок 19).

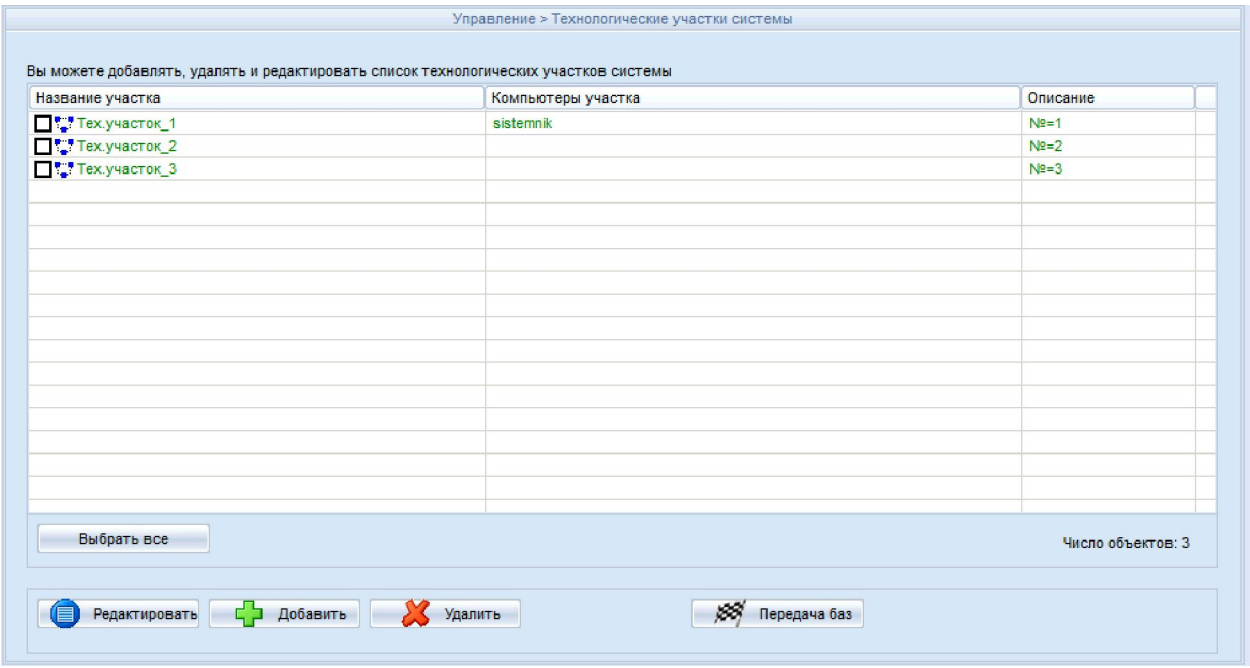

Рисунок 19 - Компьютер принадлежит технологическому участку

После выполнения перечисленных действий окно настроек технологического участка будет выглядеть так, как показано на рисунке 20.

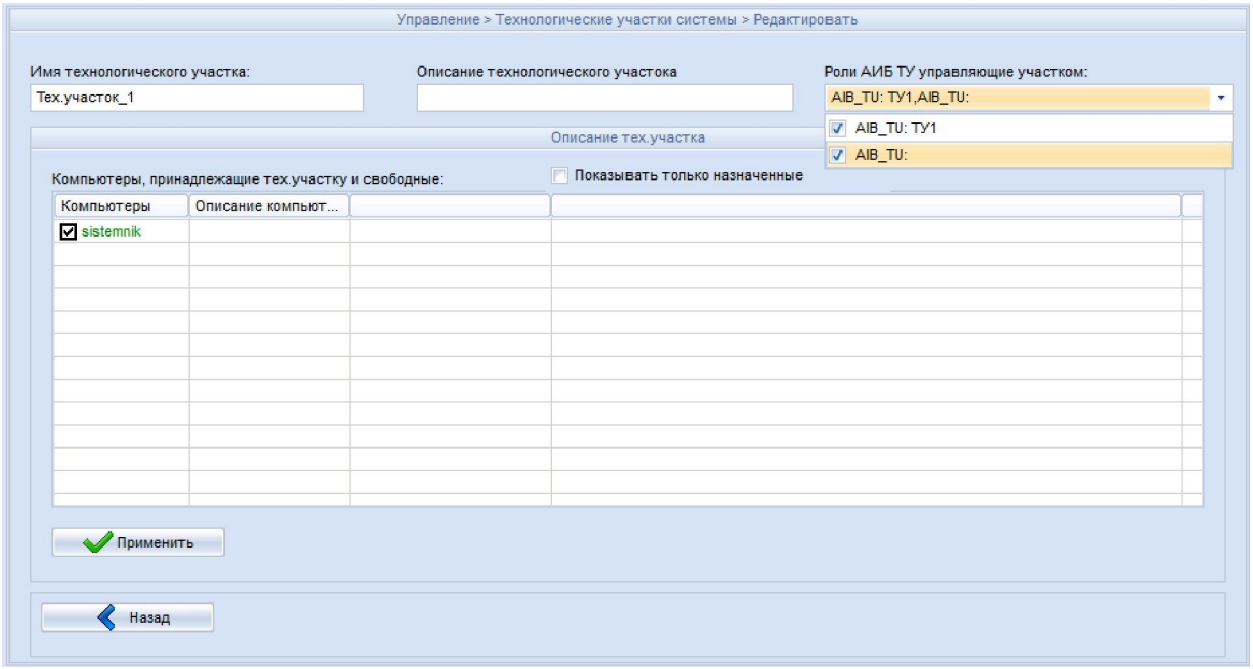

Рисунок 20 - Просмотр настроек технологического участка

Администратор ИБ СУЦУ может как сопоставлять роли АИБ ТУ с участками (при этом Администратор ИБ технологического участка может управлять несколькими технологическими участками), так и участкам назначать роли, посредством которых они будут управляться.

Затем следует создать учетную запись (подробнее см. пункт 4.1.5) и назначить ей созданную ранее роль. Также необходимо создать пользователя, которому назначить вышеуказанную учетную запись.

Таким образом, пользователь с учетной записью «AIB_TU: название участка» имеет те же привилегии что и Администратор ИБ СУЦУ, но только с теми компьютерами, которые принадлежат его участку. Он не может создавать технологические участки и роли «AIB_TU:».

При создании Администратора ИБ (АИБ подразделения) подконтрольного объекта, принадлежащего технологическому участку, в рамках децентрализованной схемы необходимо:

- создать учетную запись Администратора ИБ (АИБ подразделения) с помощью средств ASM (п. 4.1.5);
- во вкладке «Компьютеры» выбрать кнопку <Передача баз> (подробнее см.п. 4.1.4);
- в появившемся окне выбрать пункт «Экспортировать на диск» (подробнее см.п. 4.1.4);
- копировать базы на съемный носитель;
- доставить съемный носитель на ПКО;
- на ПКО в трее правой кнопкой мыши выбрать сетевой клиент ПАК «Аккорд» (подробнее см.п. 4.1.4);
- выбрать пункт далее «Импорт базы пользователей» (подробнее см. п. 4.1.4).

Чтобы удалить технологический участок, необходимо выделить его во вкладке «Тех. участки» (рисунок 15) и нажать кнопку <Удалить>. Появится окно с запросом подтверждения этого действия (рисунок 21), в котором следует нажать кнопку <Да>, если действительно нужно удалить технологический участок.

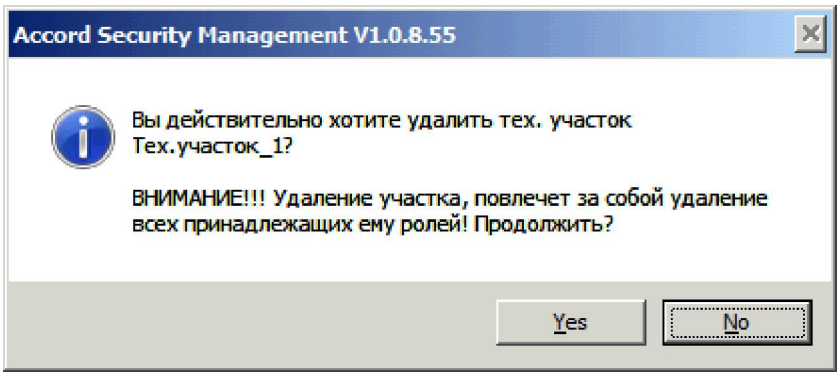

Рисунок 21 - Подтверждение удаления технологического участка

4.1.3 Вкладка «Идентификаторы»

Для того чтобы работать с идентификаторами, следует открыть в ASM вкладку Управление>Идентификаторы (рисунок 22).

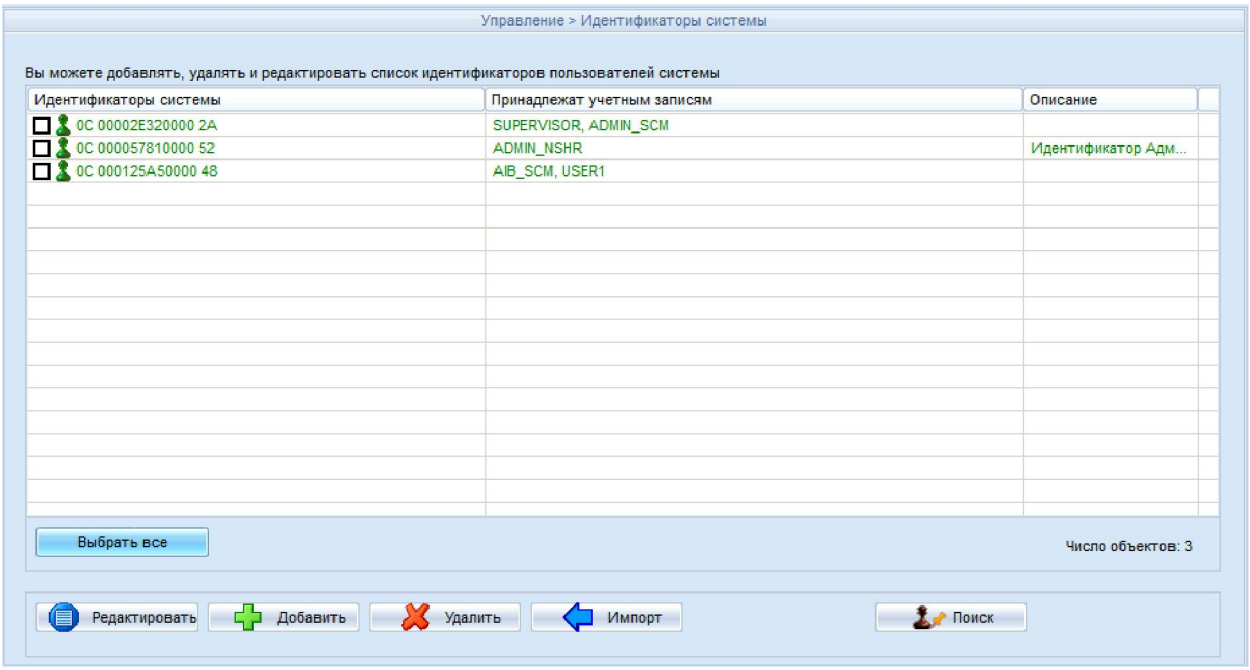

Рисунок 22 - Идентификаторы системы

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 прислонить ТМ-идентификатор (рисунок 23). Для добавления идентификатора в базу необходимо нажать кнопку <Добавить>.

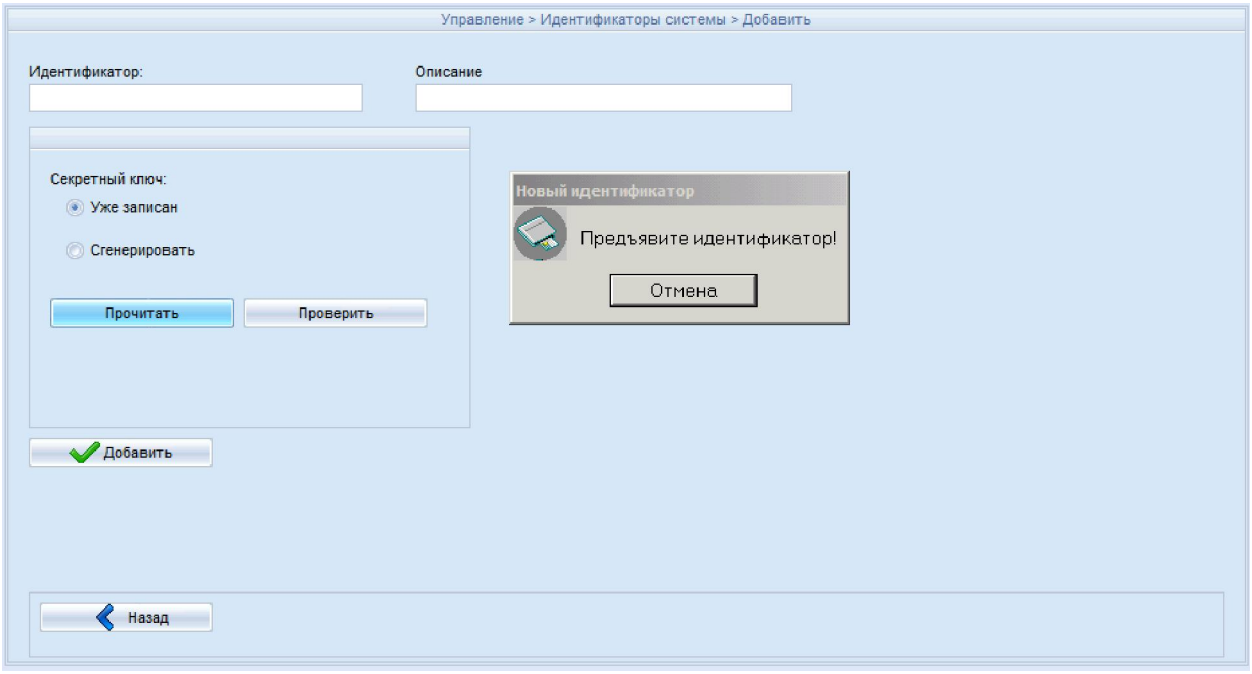

Рисунок 23 - Требование предъявить идентификатор

По нажатии кнопки <Проверить> осуществляется проверка соответствия открытых ключей базам ПКО. Если открытые ключи соответствуют базам ПКО, на экране появляется соответствующее сообщение (рисунок 24):

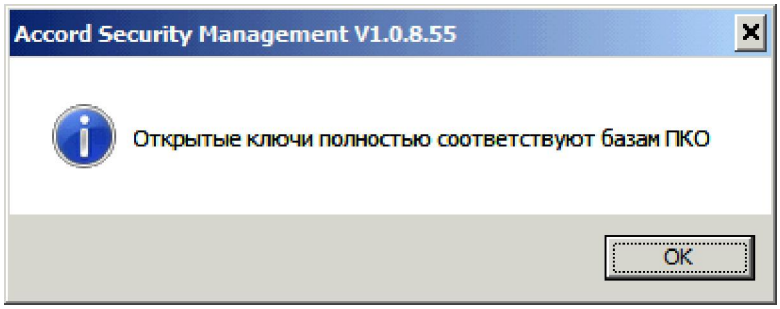

Рисунок 24 – Проверка соответствия открытых ключей базам ПКО

Чтобы удалить идентификатор, необходимо во вкладке «Идентификаторы» (рисунок 22) выбрать нужный идентификатор и нажать кнопку <Удалить>. После выполнения данной процедуры на экране появляется следующее сообщение:

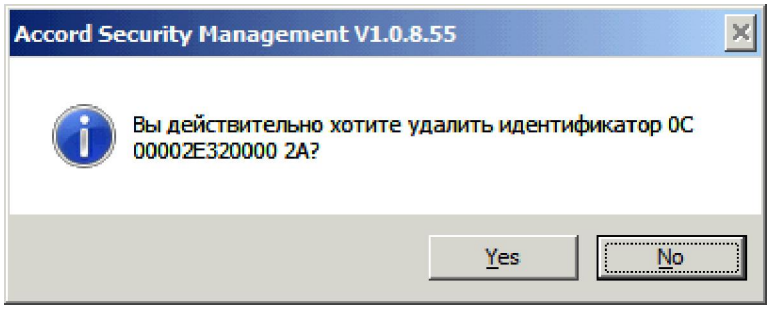

Рисунок 25 – Удаление идентификатора

Если действительно необходимо удалить идентификатор, следует нажать кнопку <Да> (рисунок 25).

Идентификаторы можно импортировать из базы СЗИ от НСД «Аккорд» (например C:\Accord.NT\ ACCORD.AMZ). Для этого во вкладке «Идентификаторы» (рисунок 22) необходимо нажать кнопку <Импорт>. На экране появляется окно (рисунок 27), в котором нужно нажать кнопку <Обновить>. По нажатии кнопки <Обновить> на экране появляется окно (рисунок 42), в котором следует отметить необходимые ПКО и нажать кнопку <OK> (в окне, показанном на рисунке 42, отображаются только те компьютеры, которые находятся в сети).

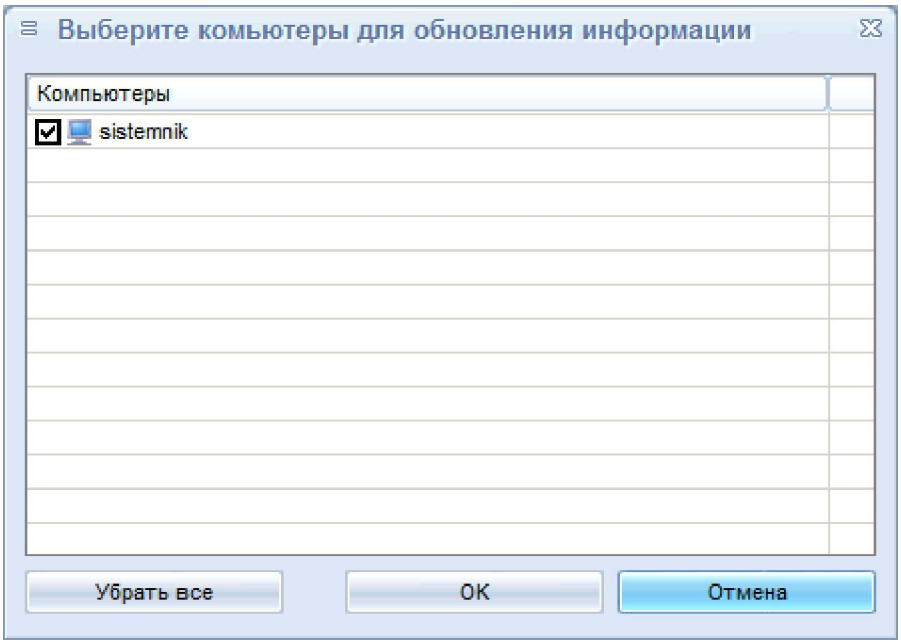

Рисунок 26 – Выбор компьютеров для обновления информации

Далее необходимо и нажать кнопку <Импортировать> (рисунок 27).

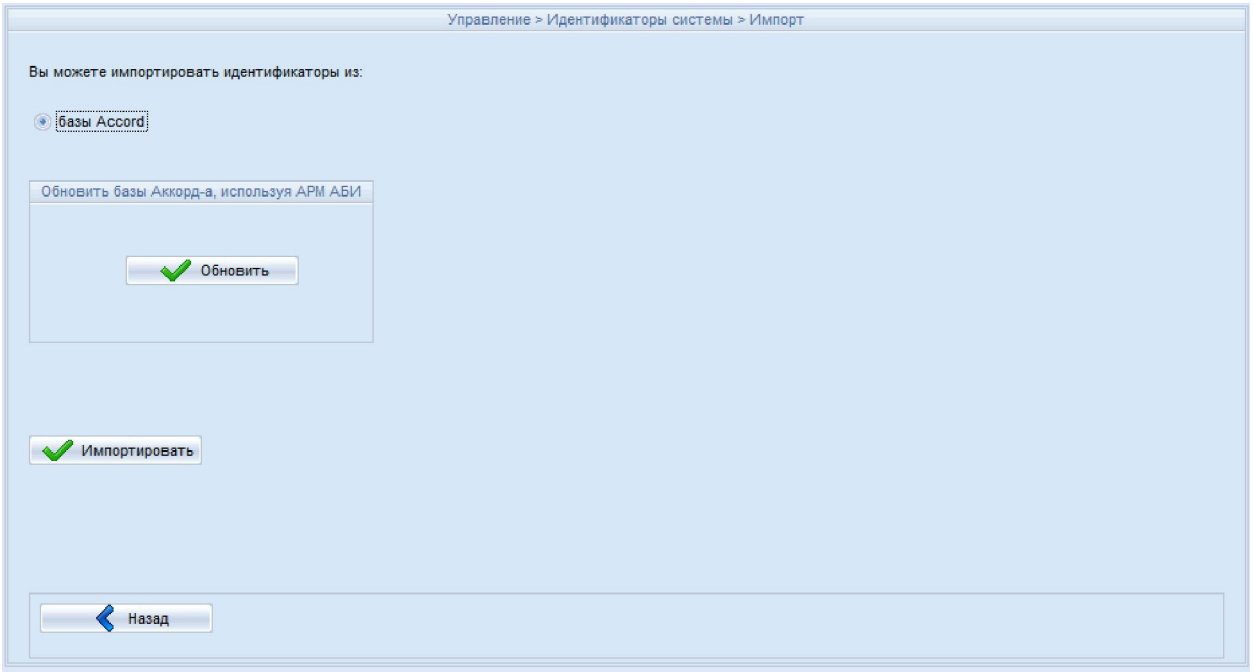

Рисунок 27 – Импорт идентификатора

По нажатии кнопки <Импортировать> (рисунок 27) на экране появляется окно выбора каталога (рисунок 28), в котором следует выбрать необходимый файл.

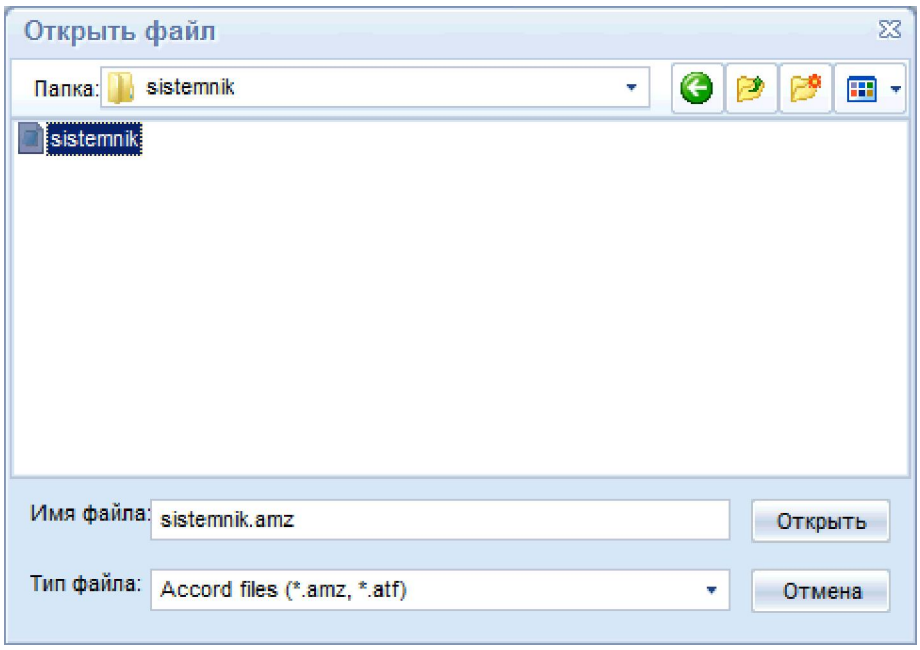

Рисунок 28 – Окно выбора каталога

После этого в правой части окна появятся импортированные идентификаторы, следует выбрать из них необходимые для добавления в базу (для выбора всех идентификаторов нужно нажать кнопку <Выбрать все>) и нажать кнопку <Добавить> (рисунок 29).

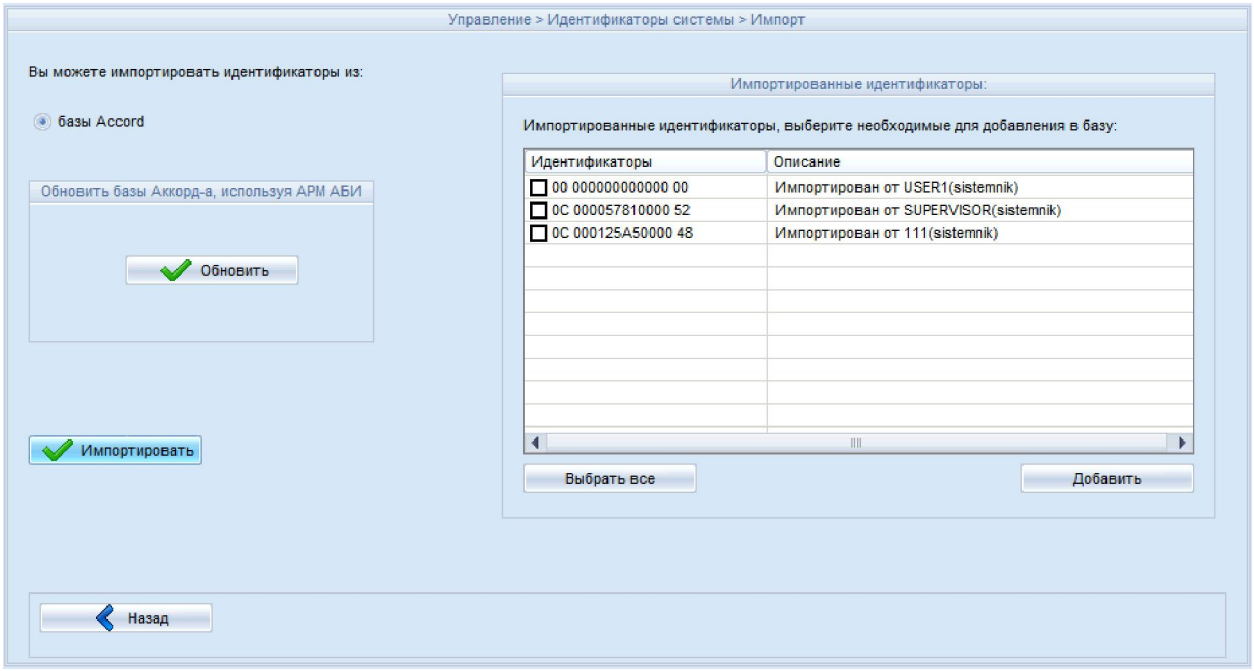

Рисунок 29 - Выбор импортированных идентификаторов(импорт из базы Аккорда)

Если необходимо определить, добавлен ли идентификатор в базу ASM, следует нажать кнопку <Поиск> на вкладке «Идентификаторы» (рисунок 22). Появится окно с сообщением «Предъявите идентификатор» (рисунок 30).

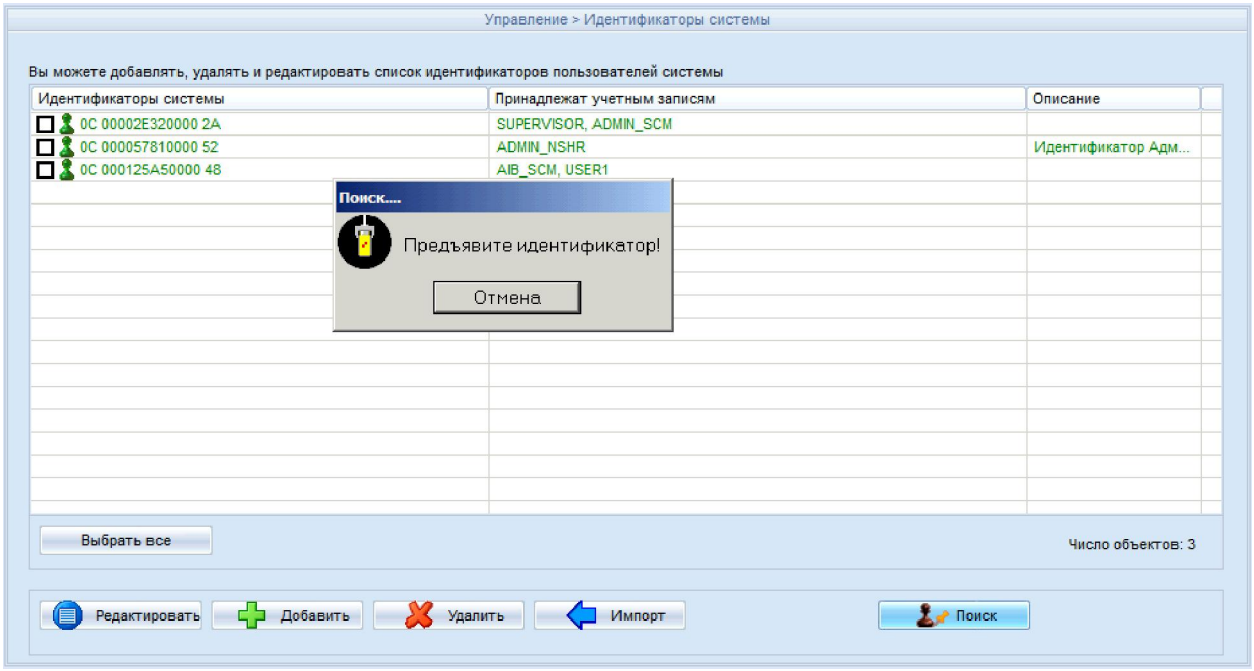

Рисунок 30 - Сообщение «Предъявите идентификатор»

Если данный идентификатор добавлен в базу ASM, то этот идентификатор будет выделен (рисунок 23), иначе в нижней части окна появится сообщение «Идентификатор не зарегистрирован!» (рисунок 32).

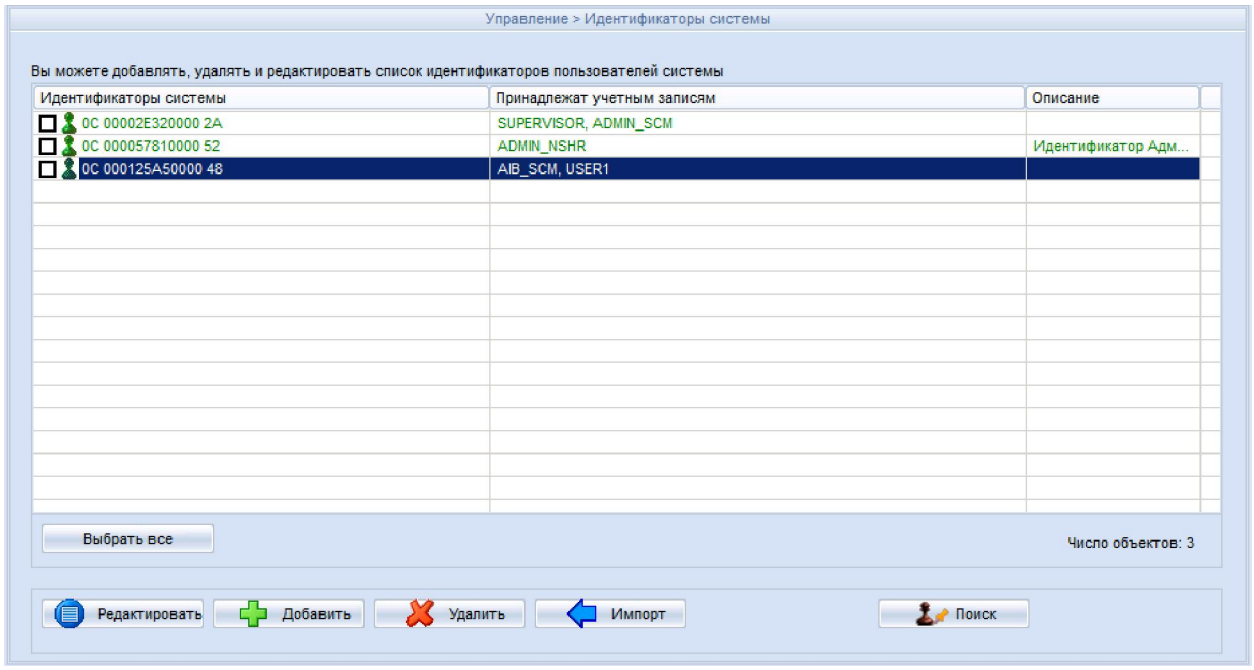

Рисунок 31 - Найдена учетная запись, которой назначен идентификатор

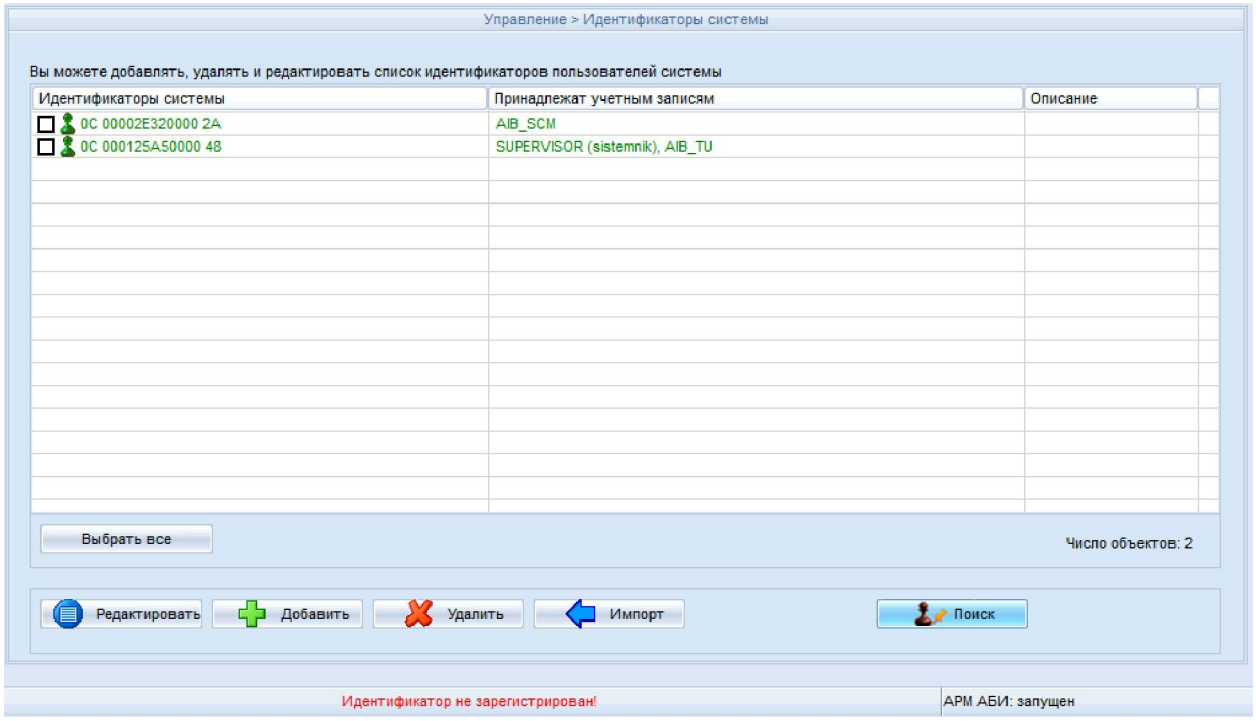

Рисунок 32 - Сообщение о том, что идентификатор не зарегистрирован в базе ASM

4.1.4 Вкладка «Компьютеры»

Для того чтобы работать с компьютерами, следует открыть в ASM вкладку Управление>Компьютеры (рисунок 33).

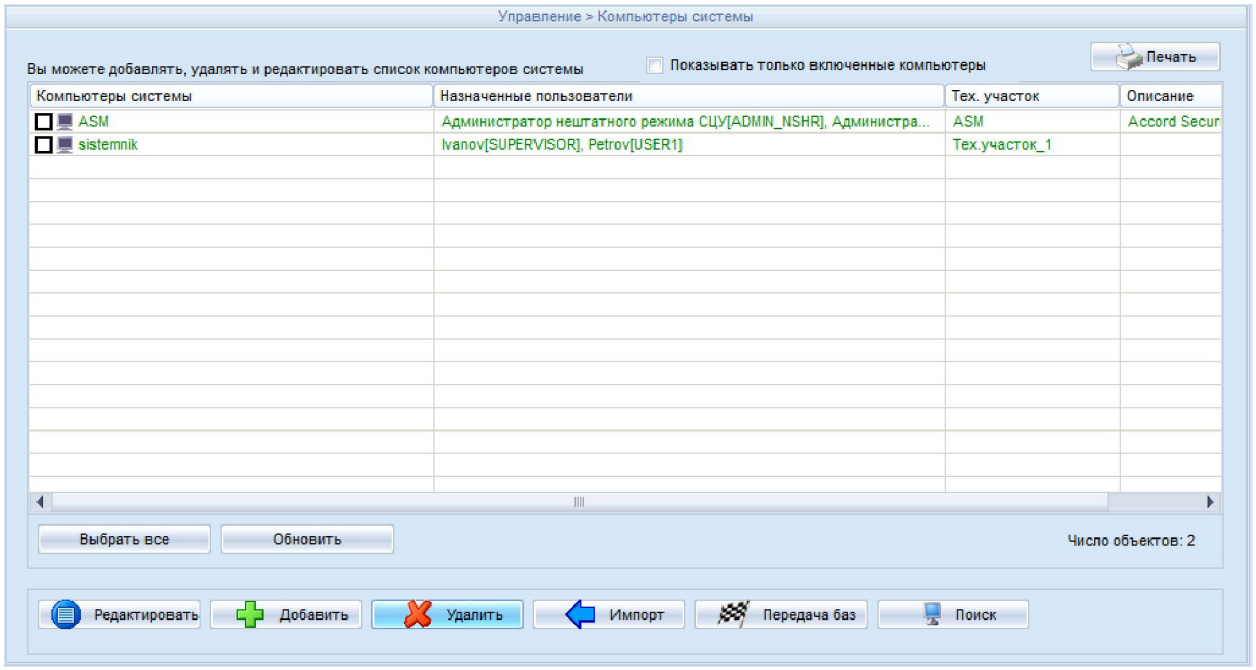

Рисунок 33 - Компьютеры системы

Кнопка <Печать> позволяет распечатать выбранную информацию на принтере, а также сохранить в файл (с указанным разделителем). По нажатии кнопки <Печать> на экране появляется окно, в котором следует 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 34). В случае печати в файл выбранные параметры сохраняются в файле ASM\AccountName_PrinterParam.ini, где AccountName – имя учетной записи.

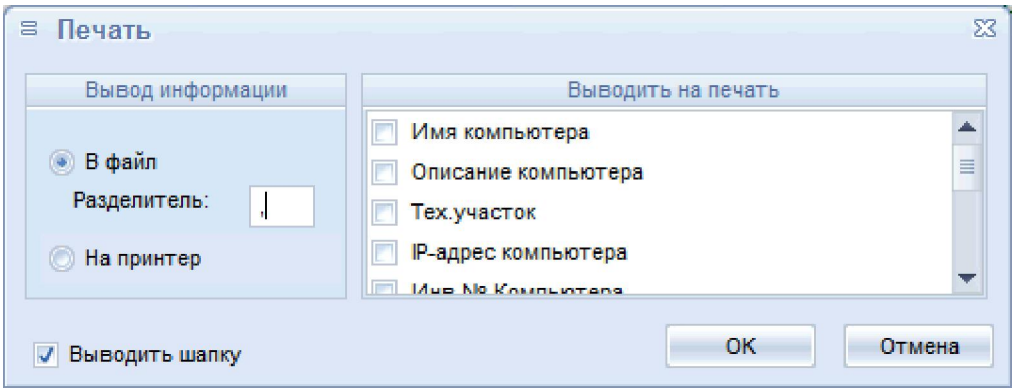

Рисунок 34 – Печать информации о подконтрольном объекте

Для добавления компьютера необходимо нажать кнопку <Добавить> (рисунок 33). В появившемся окне (рисунок 35) можно задать имя компьютера, его описание и назначить этот компьютер технологическому участку (последние два условия не являются обязательными для выполнения).

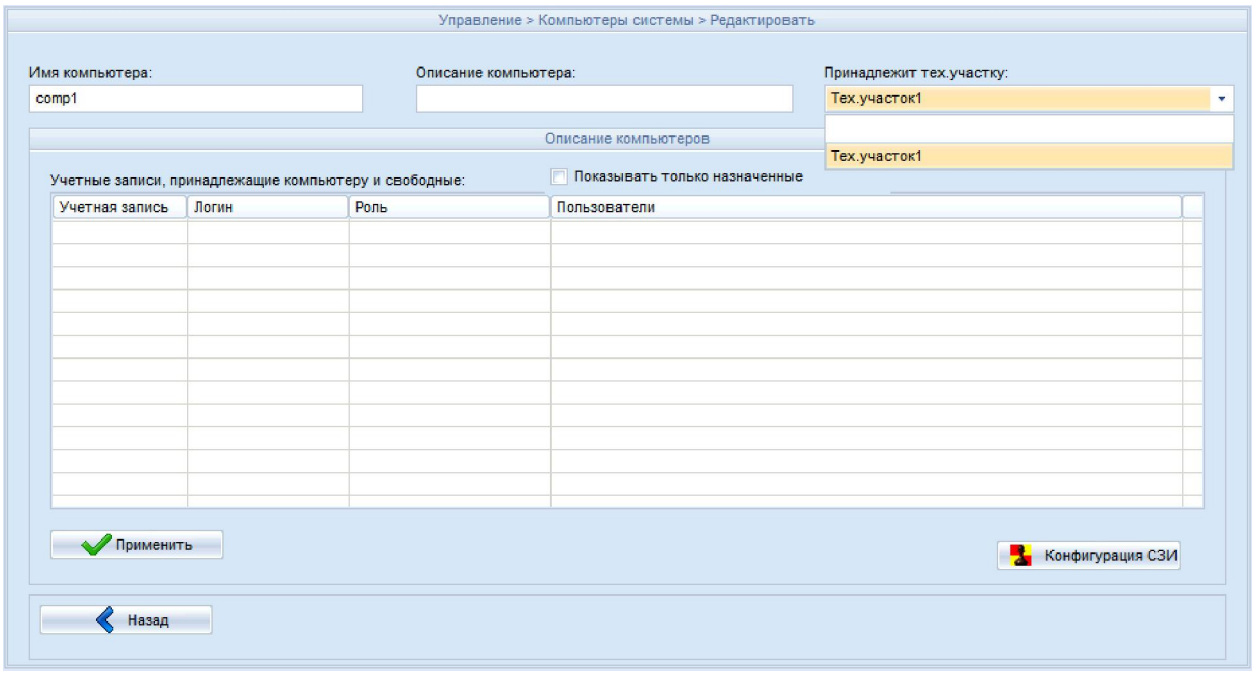

Рисунок 35 – Добавление компьютера

Чтобы редактировать компьютер, необходимо нажать кнопку <Редактировать> (рисунок 33). В появившемся окне (рисунок 36) можно изменить имя компьютера, его описание и назначить этот компьютер технологическому участку (последние два условия не являются обязательными для заполнения).

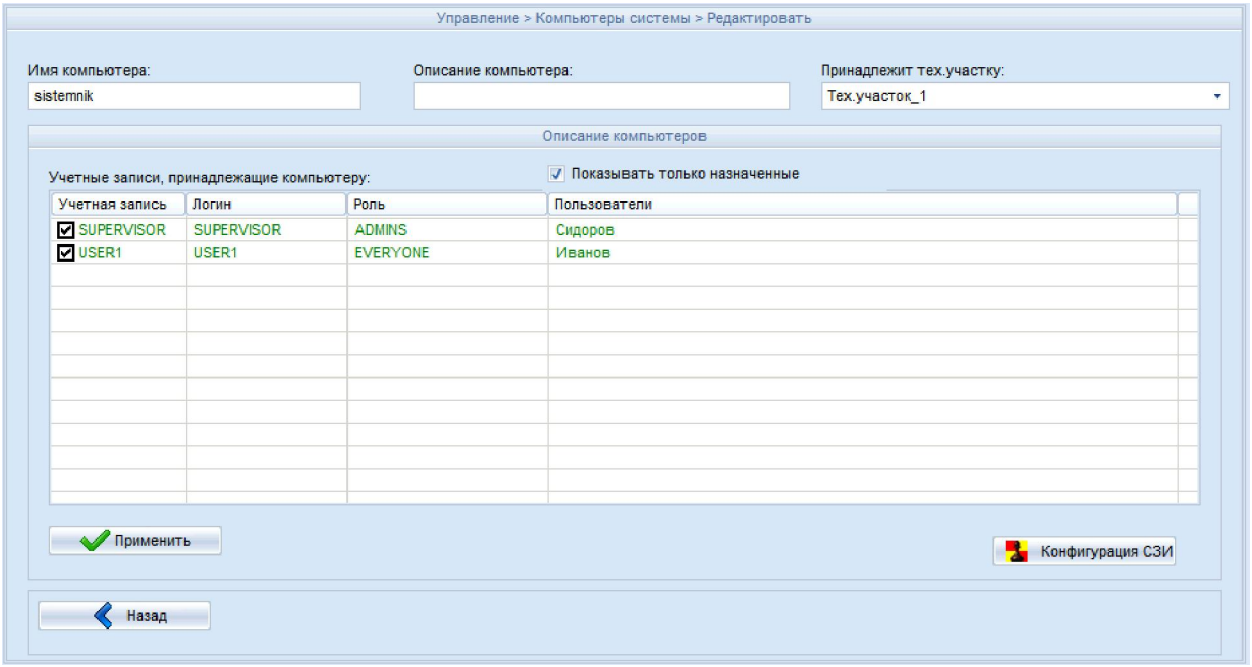

Рисунок 36 – Редактирование списка подконтрольных объектов

По нажатии кнопки <Конфигурация СЗИ> на экране появляется окно, в котором отображаются настройки СЗИ выбранного ПКО, версия его программного обеспечения, IP-адрес, серийный номер контроллера, а также инвентарные номера ПКО и контроллера «Аккорд-АМДЗ» (последние поля заполняются вручную, рисунок 37).

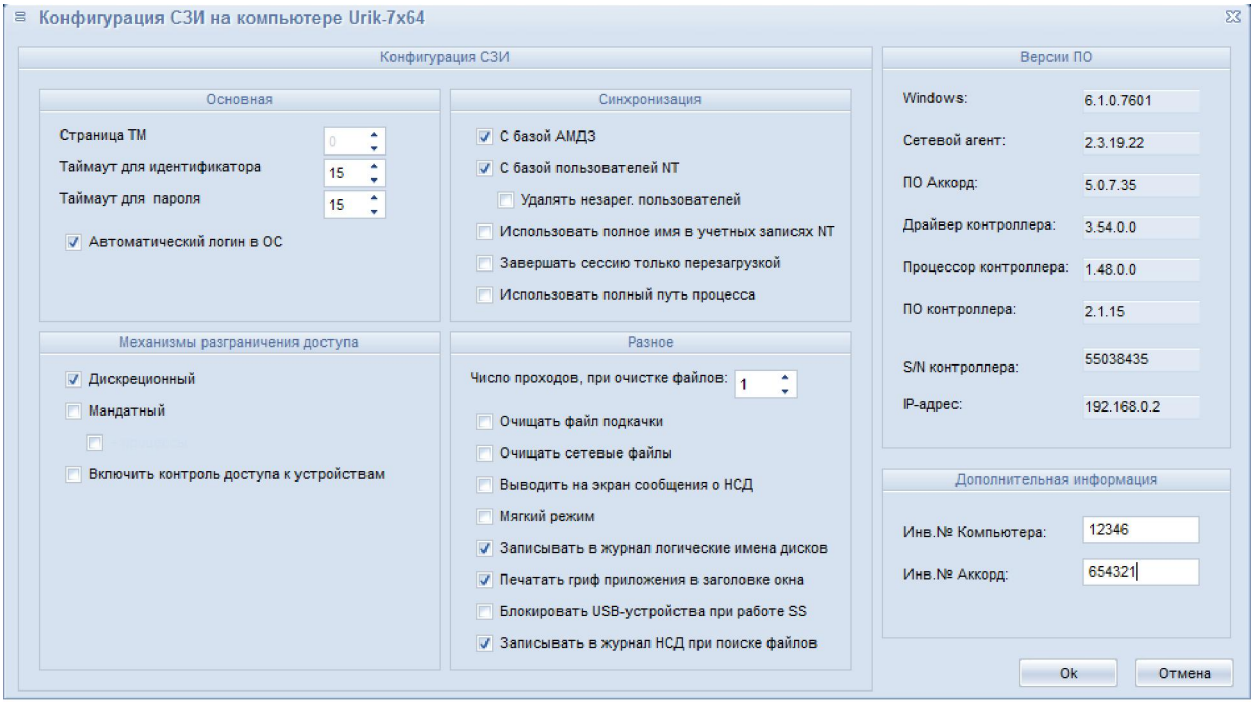

Рисунок 37 – Конфигурация СЗИ на подконтрольном объекте

ВНИМАНИЕ! Для получения версии ПО требуется наличие сетевого клиента не ниже v.2.3.15.15. Версию ПО контроллера можно получить в том случае, если на ПКО имеется «Аккорд-АМДЗ» (DOS) v. 2.1.15. Для ранних версий «Аккорда-АМДЗ» (DOS) и «Аккорда» (LE) версия предоставляется на основании версии прошивки процессора.

По нажатии кнопки <Передача баз> базы пользователей передаются на ПКО (подробнее ниже).

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

Если необходимо определить, зарегистрирован ли компьютер в системе, следует нажать кнопку <Поиск> во вкладке «Компьютеры» (рисунок 33). По нажатии кнопки на экране появляется окно (рисунок 38), в котором необходимо указать IP-адрес компьютера или его имя (либо маску сети).

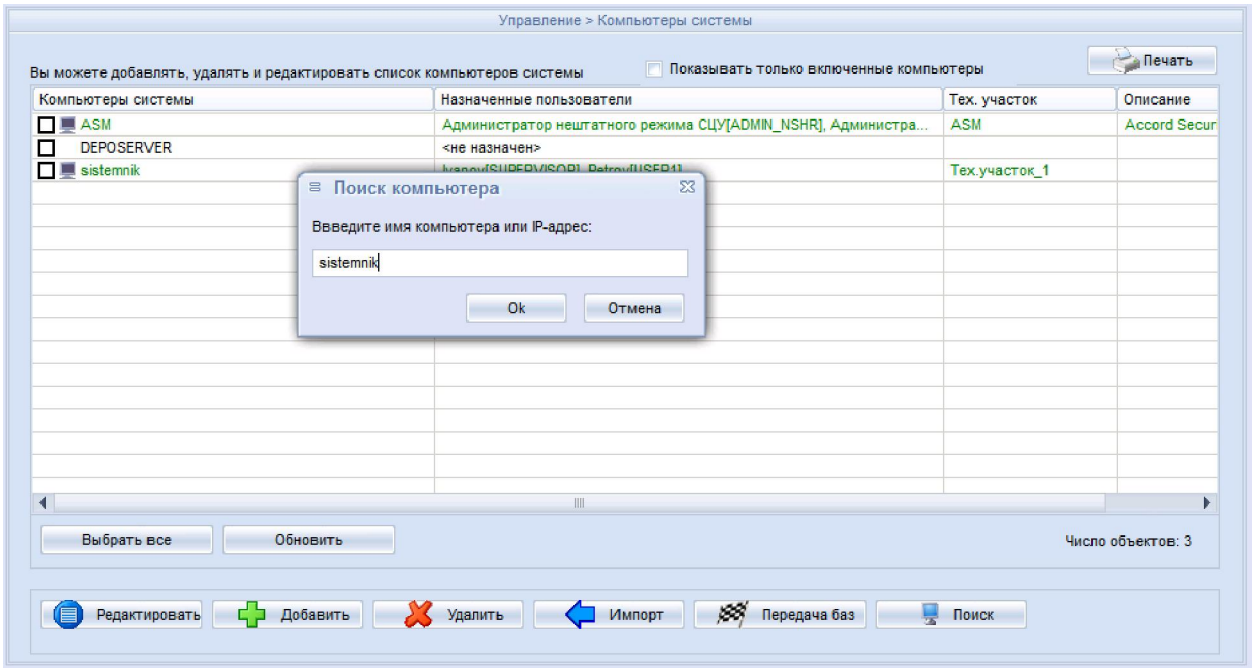

Рисунок 38 – Поиск компьютера по имени или IP-адресу

Если данный компьютер зарегистрирован в системе, то этот компьютер будет выделен (рисунок 39), иначе в нижней части окна появится сообщение «Компьютер не найден!» (рисунок 40).

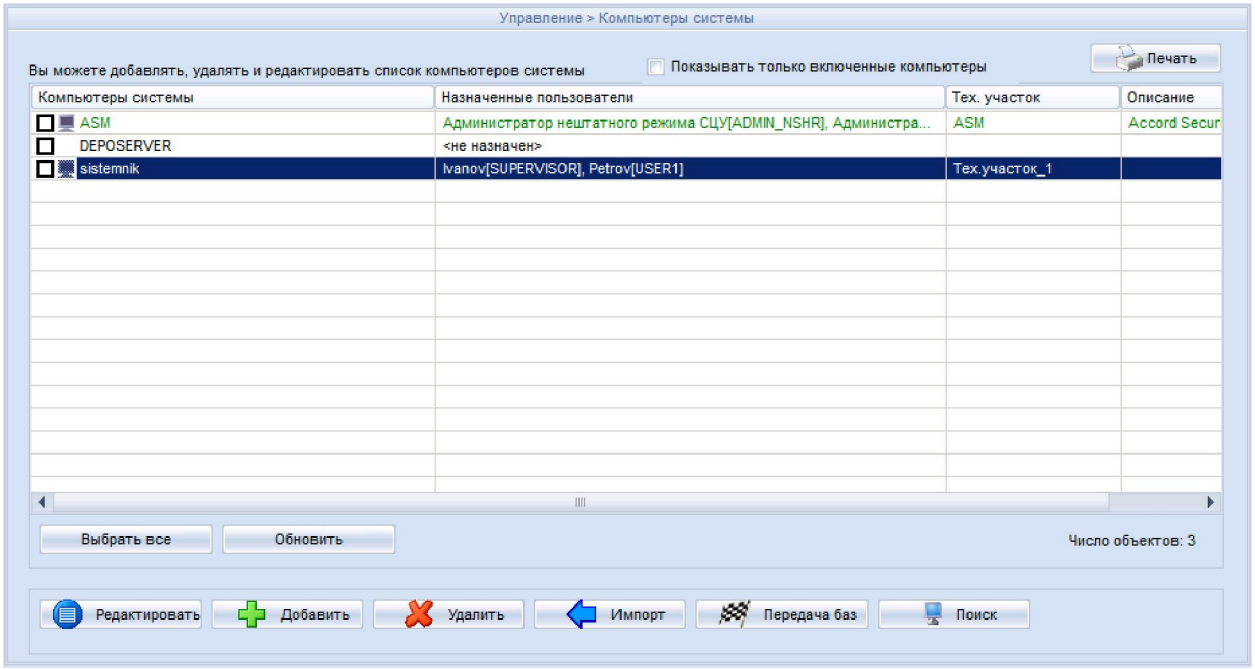

Рисунок 39 – Найден компьютер

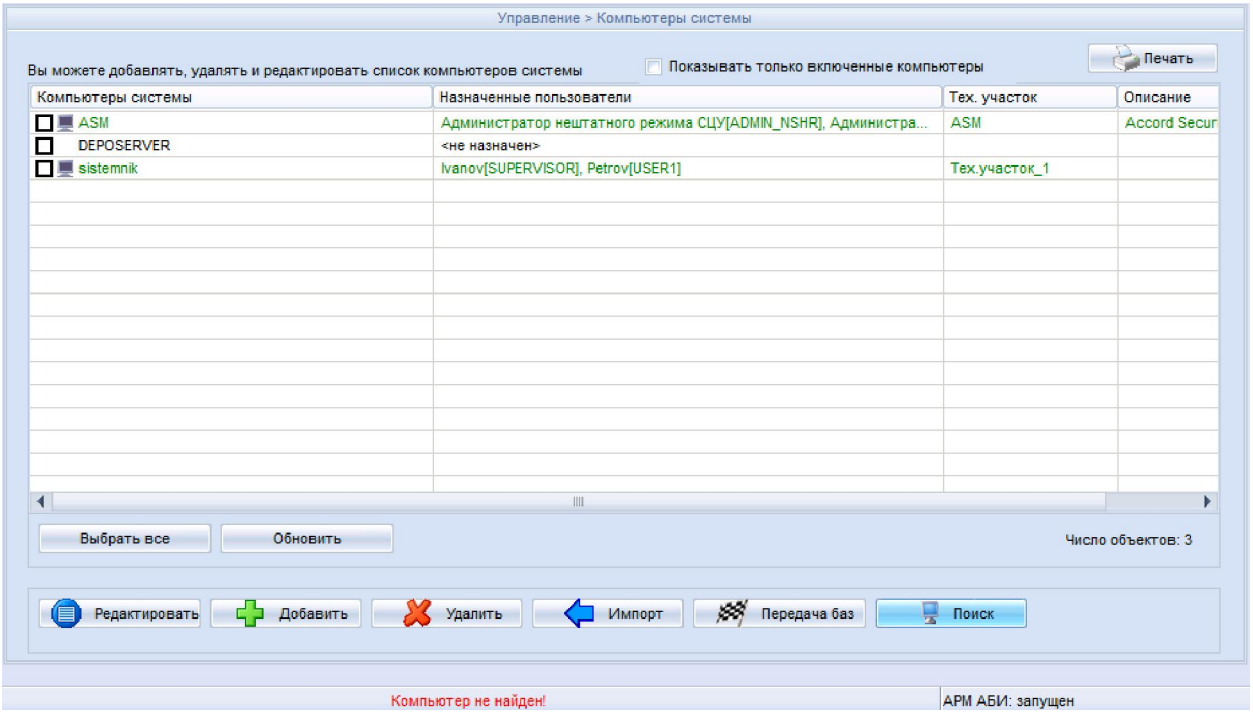

Рисунок 40 - Сообщение о том, что компьютер не найден

Чтобы удалить компьютер, необходимо выделить его и нажать кнопку <Удалить> на вкладке «Компьютеры» (рисунок 33). Появится окно подтверждения этого действия (рисунок 41), следует нажать кнопку <Да>, если действительно нужно удалить компьютер.

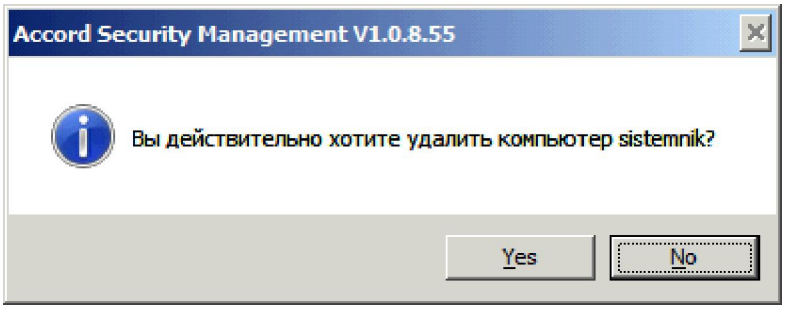

Рисунок 41 – Окно подтверждения удаления компьютера

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

Кнопка <Обновить> во вкладке «Компьютеры» (рисунок 33) необходима для обновления списка активных ПКО.

Кнопка <Импорт> во вкладке «Компьютеры» (рисунок 33) необходима для регистрации ПКО. По нажатии данной кнопки на экране появляется окно импорта компьютеров (рисунок 43). Чтобы импортировать компьютеры из базы «Аккорда-РАУ», необходимо установить соответствующий флаг («Вы можете импортировать компьютеры из:» - «базы Accord -РАУ») в окне, показанном на рисунок 43. При необходимости обновить базы перед выполнением этой операции следует нажать кнопку <Обновить>.

По нажатии кнопки <Обновить> на экране появляется окно (рисунок 42), в котором следует отметить необходимые ПКО и нажать кнопку <OK> (в окне, пока-

занном на рисунке 42, отображаются только те компьютеры, которые находятся в сети).

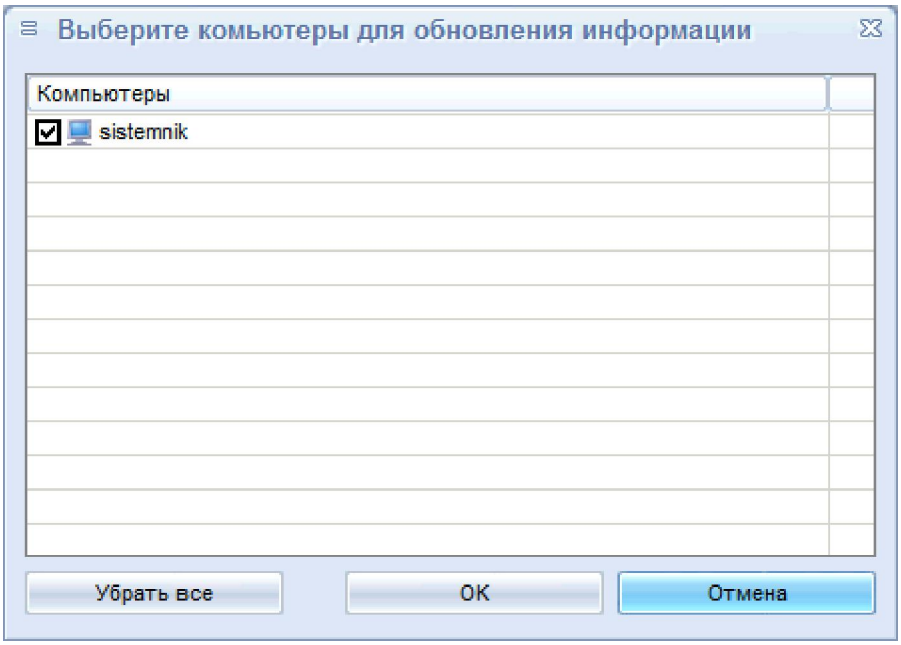

Рисунок 42 – Выбор компьютеров для обновления информации

Далее необходимо и нажать кнопку <Импортировать> (рисунок 43).

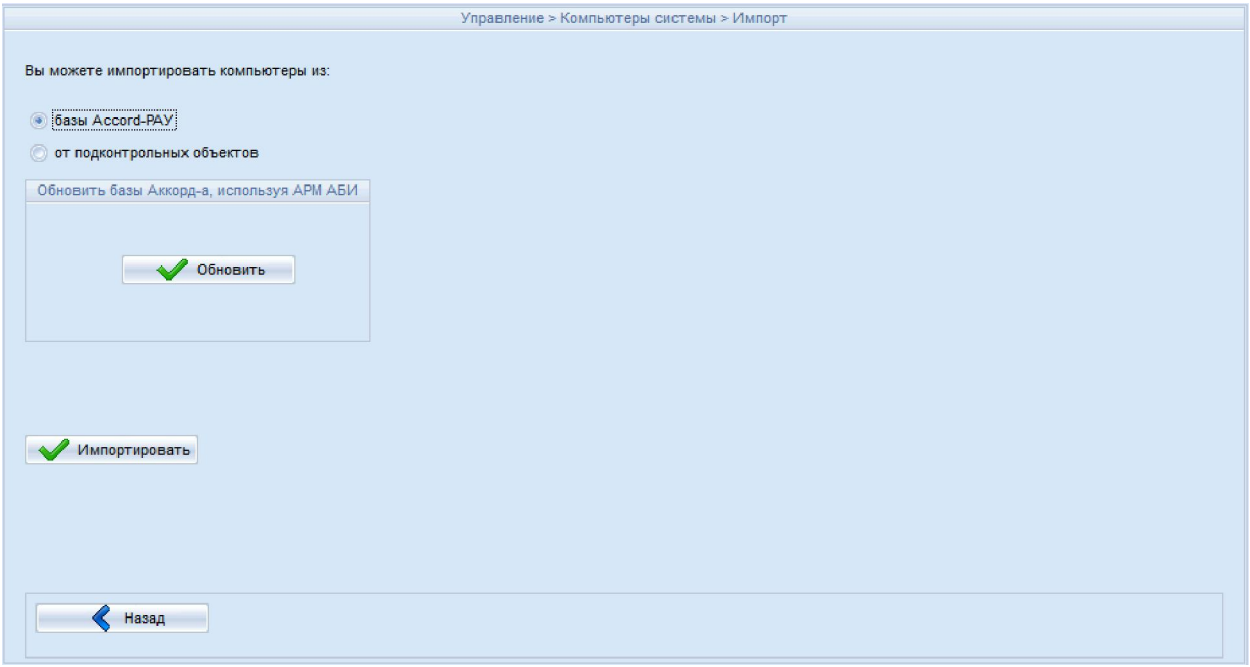

Рисунок 43 - Импорт компьютеров

По нажатии кнопки <Импортировать> на экране появляется окно (рисунок 44), в котором следует указать файл, из которого необходимо импортировать компьютеры.

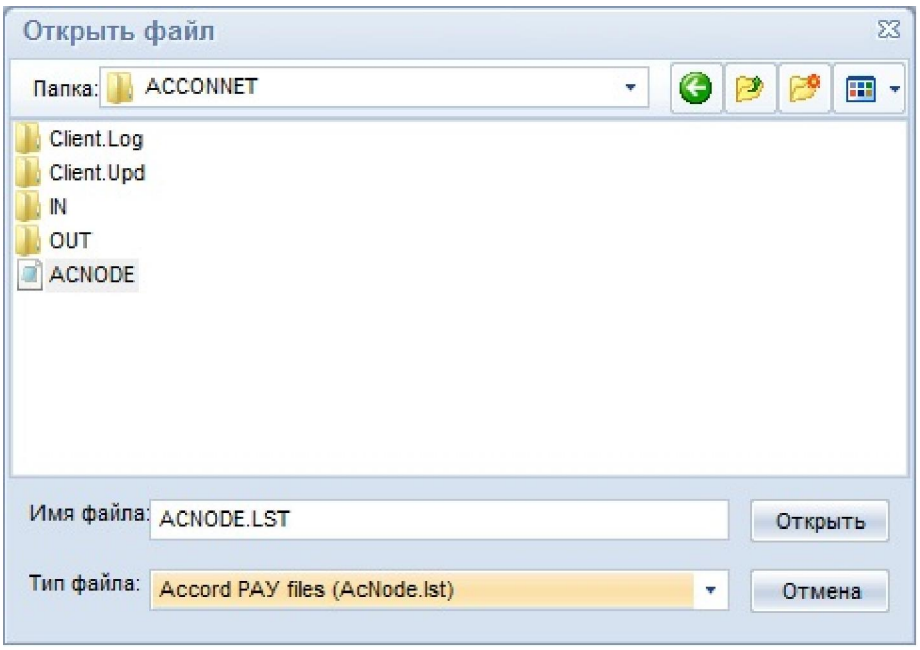

Рисунок 44 - Выбор каталога для импорта компьютеров

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).

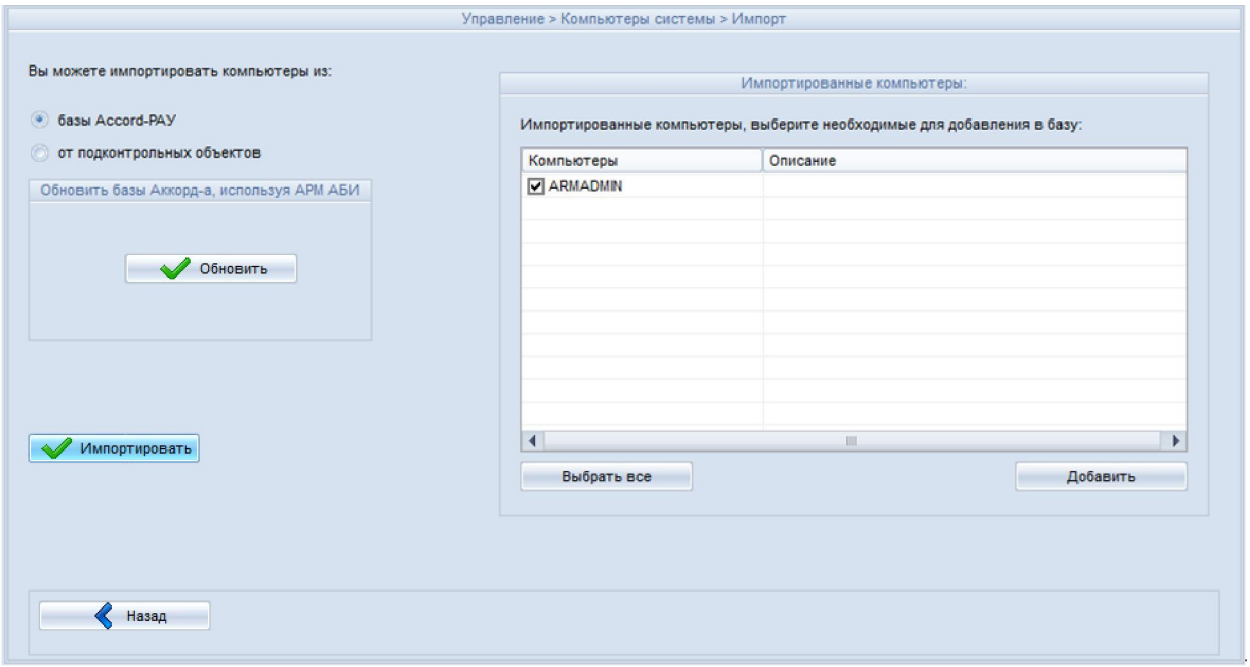

Рисунок 45 - Выбор импортированных компьютеров (импорт из базы «Аккорда -РАУ»)

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>.

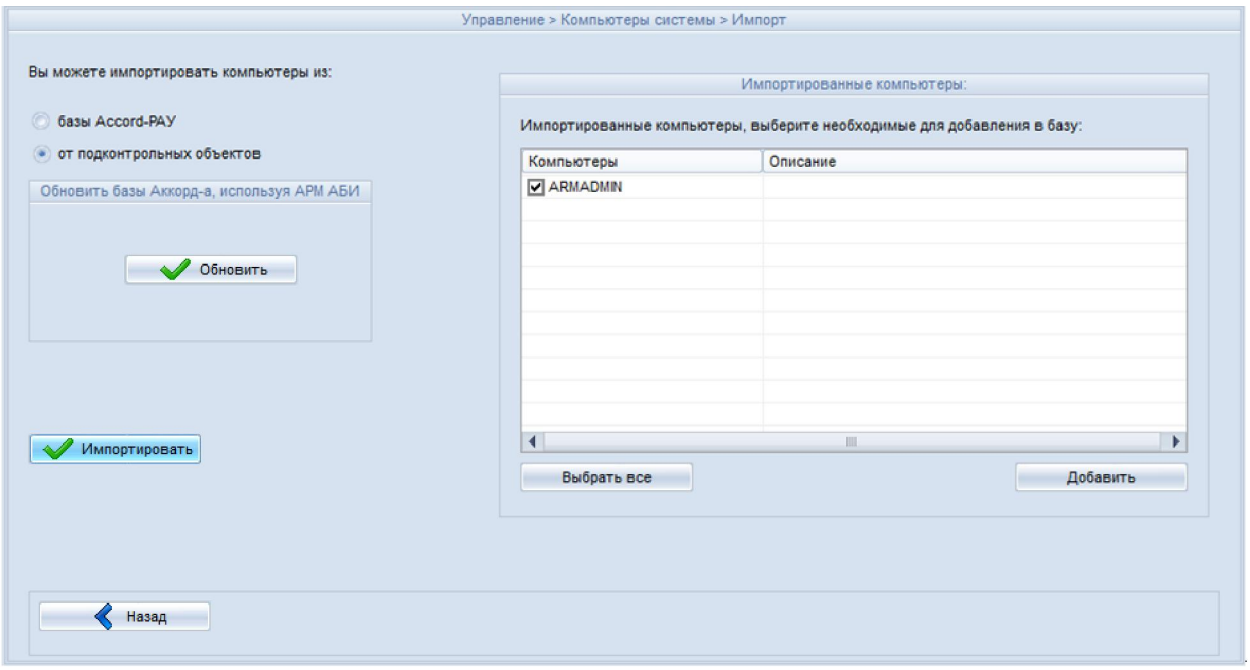

Рисунок 46 - Выбор импортированных компьютеров (импорт от ПКО)

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).

Передача баз пользователей на подконтрольные объекты (далее по тексту ПКО) осуществляется посредством кнопки <Передача баз> (предварительно необходимо выбрать компьютеры (рисунок 47), на которые планируется передать базы). По нажатии этой кнопки на экране появляется окно передачи баз пользователей на ПКО.

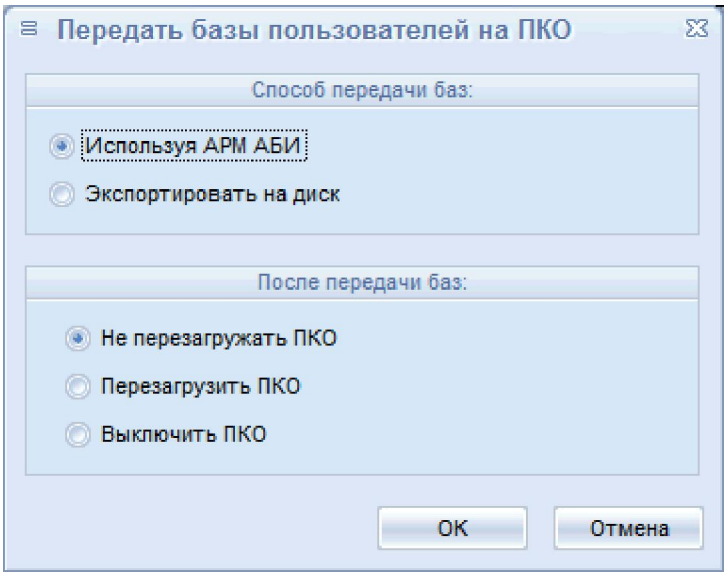

Рисунок 47 - Передача баз пользователей

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

Если база пользователей передана на ПКО, на экране появляется сообщение (рисунок 48):

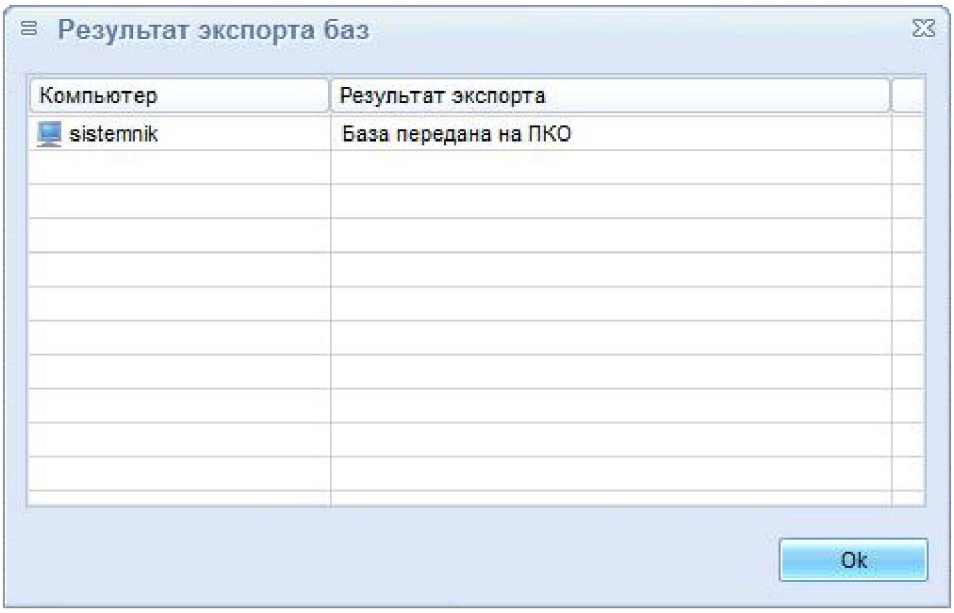

Рисунок 48 – Сообщение о том, что база пользователей передана на ПКО

Если во время выполнения процедуры передачи базы пользователей служба AcConNet загружена, на экране появляется сообщение (рисунок 49).

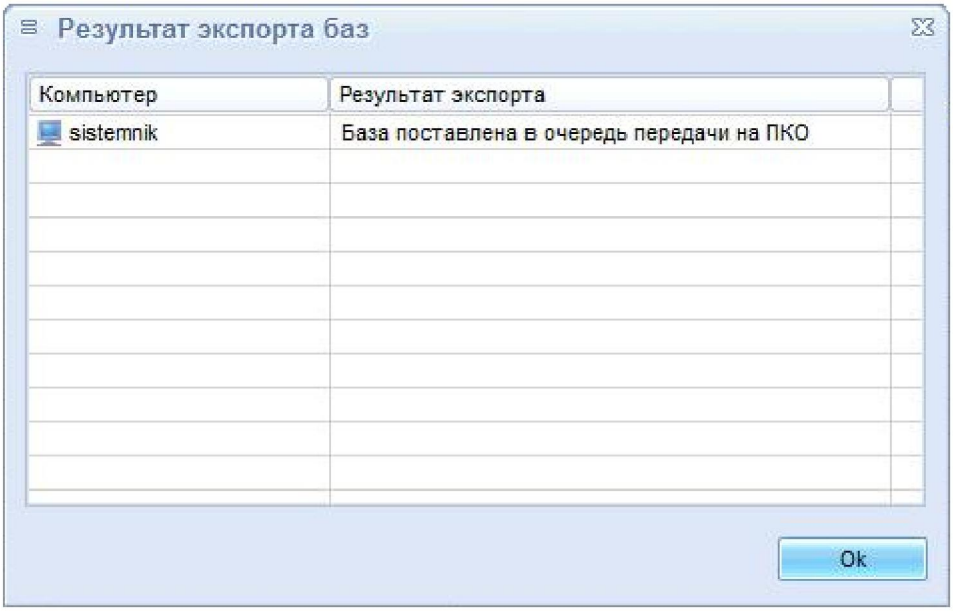

Рисунок 49 – Сообщение о том, что база пользователей поставлена в очередь передачи на ПКО

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 (рисунок 50):

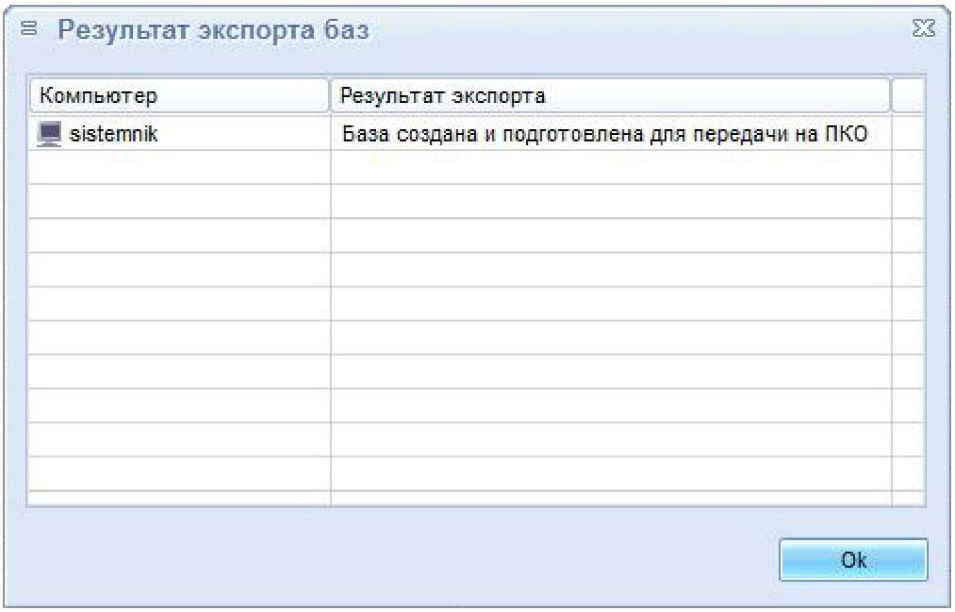

Рисунок 50 – Сообщение о том, что база пользователей создана и подготовлена для передачи на ПКО

База пользователей автоматически передается при следующем включении ПКО, и на экране появляется сообщение, показанное на рисунке 48.

Передача баз пользователей на ПКО в рамках децентрализованной схемы осуществляется посредством кнопки <Передача баз> (предварительно необходимо выбрать компьютеры (рисунок 33), на которые планируется передать базы). 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 передачи баз пользователей на ПКО в рамках децентрализованной схемы, необходимо добавить флеш - накопитель в единую базу USB-носителей (эта процедура выполняется Администратором СУЦУ в соответствии с документом «Руководство Администратора» 11443195.4012-053 90).

По нажатии кнопки <Передача баз> на экране появляется окно передачи баз пользователей на ПКО, в котором нужно выбрать пункт «Экспортировать на диск» (рисунок 51) и нажать кнопку <OK>.

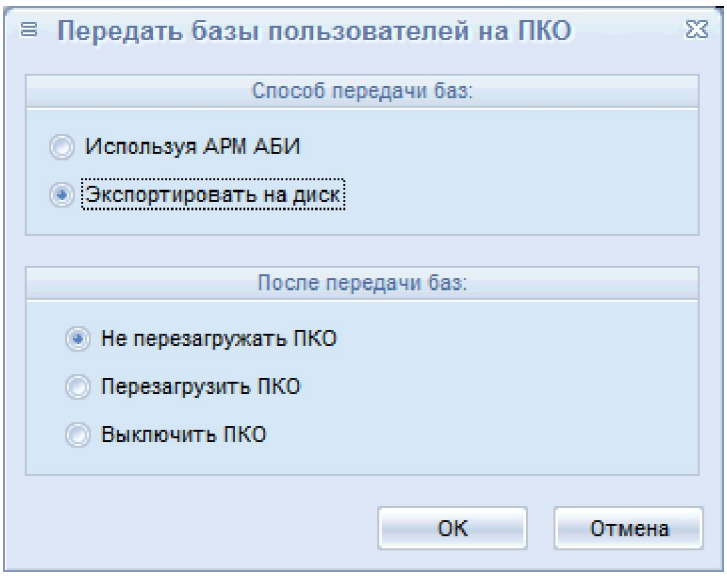

Рисунок 51 - Передача баз пользователей по децентрализованной схеме

Далее на экране появляется окно выбора каталога, в котором нужно выбрать любой каталог на внешнем носителе и нажать кнопку <Применить>. Если процедура экспорта баз пользователей выполнена успешно, то на экране появляется сообщение (рисунок 52):

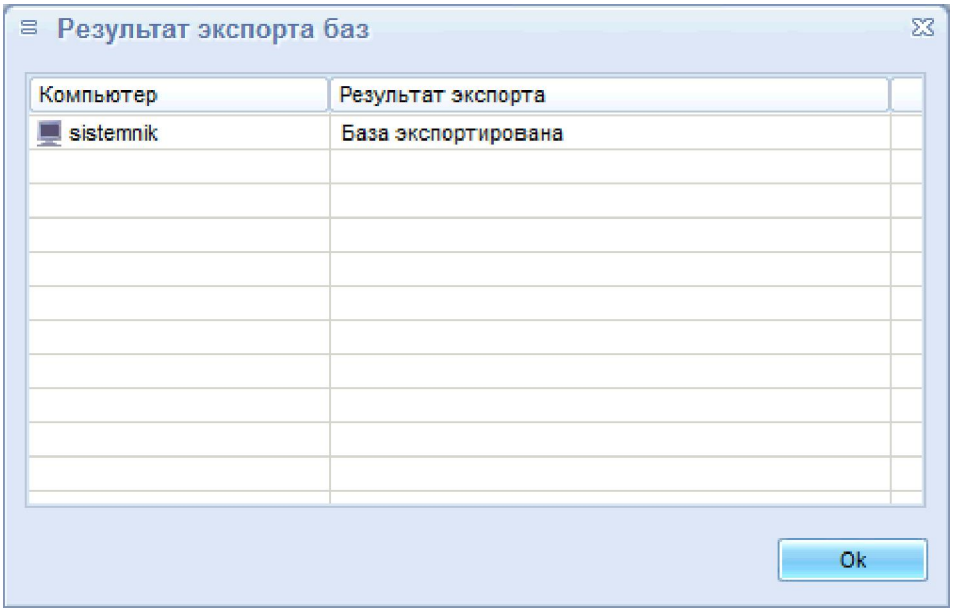

Рисунок 52 – Сообщение о том, что база пользователей экспортирована на диск

Базы пользователей экспортируются в <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.

На ПКО необходимо выполнить следующие действия (чтобы функция импорта баз 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 нужно выбрать правой кнопкой мыши сетевой клиент ПАК «Аккорд» (рисунок 53), на экране появляется меню (рисунок 54);

– далее необходимо выбрать пункт «Импорт базы пользователей»;

– на экране появляется сообщение «Предъявите идентификатор». Необходимо предъявить идентификатор Администратора «Аккорд» подконтрольного объекта.

– в появившемся на экране окне ввода пароля следует ввести пароль и нажать кнопку <OK> (рисунок 55);

– далее на экране появляется окно выбора каталога для импорта базы пользователей (рисунок 56), необходимо выбрать нужный каталог и нажать кнопку <OK>.

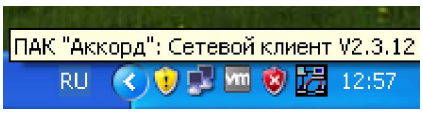

Рисунок 53 – Значок сетевого клиента ПАК «Аккорд» в трее

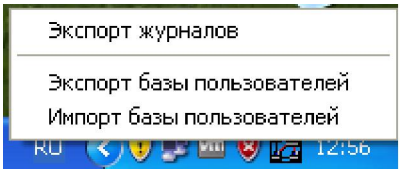

Рисунок 54 - Контекстное меню сетевого клиента ПАК «Аккорд» в трее

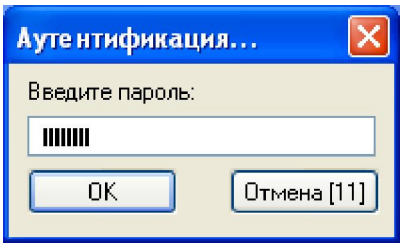

Рисунок 55 – Окно ввода пароля

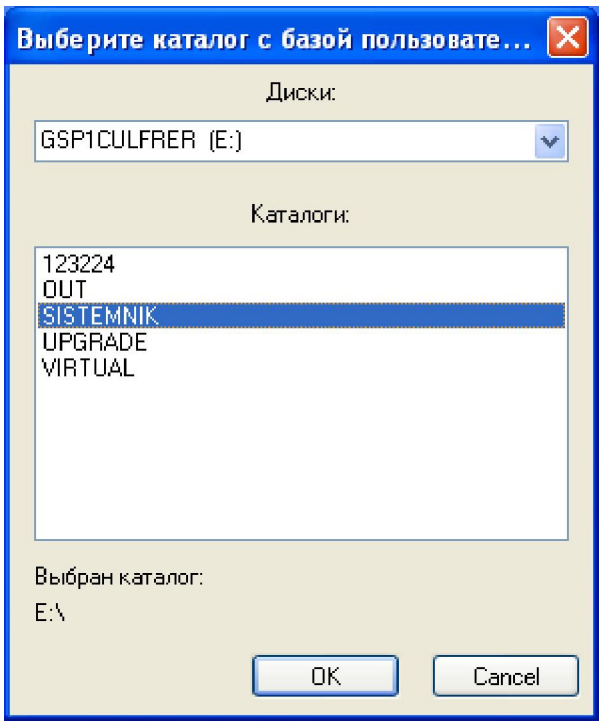

Рисунок 56 - Выбор каталога для импорта базы пользователей

Если описанная процедура выполнена успешно, то на экране появляется следующее оповещение (рисунок 57).

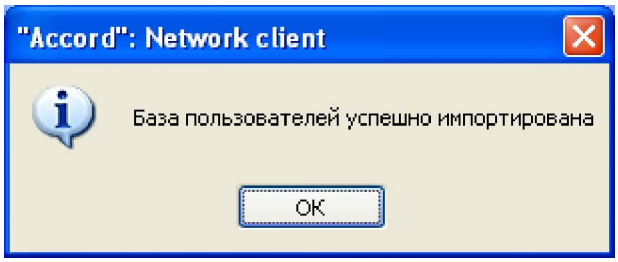

Рисунок 57 - Оповещение об успешном выполнении процедуры импорта базы пользователей

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

Далее при выполнении процедуры передачи баз пользователей на ПКО на сервере централизованного управления создается 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, то процедура передачи файлов базы пользователей на ПКО не производится. Если различия имеются, то файлы из каталога C:\Asm\OutBases\CompName переписываются в каталог C:\Asm\ACCONET\OUT\CompName и передаются на ПКО.

4.1.5 Вкладка «Учетные записи»

Для того чтобы работать с учетными записями, следует открыть в ASM вкладку Управление>Учетные записи (рисунок 58).

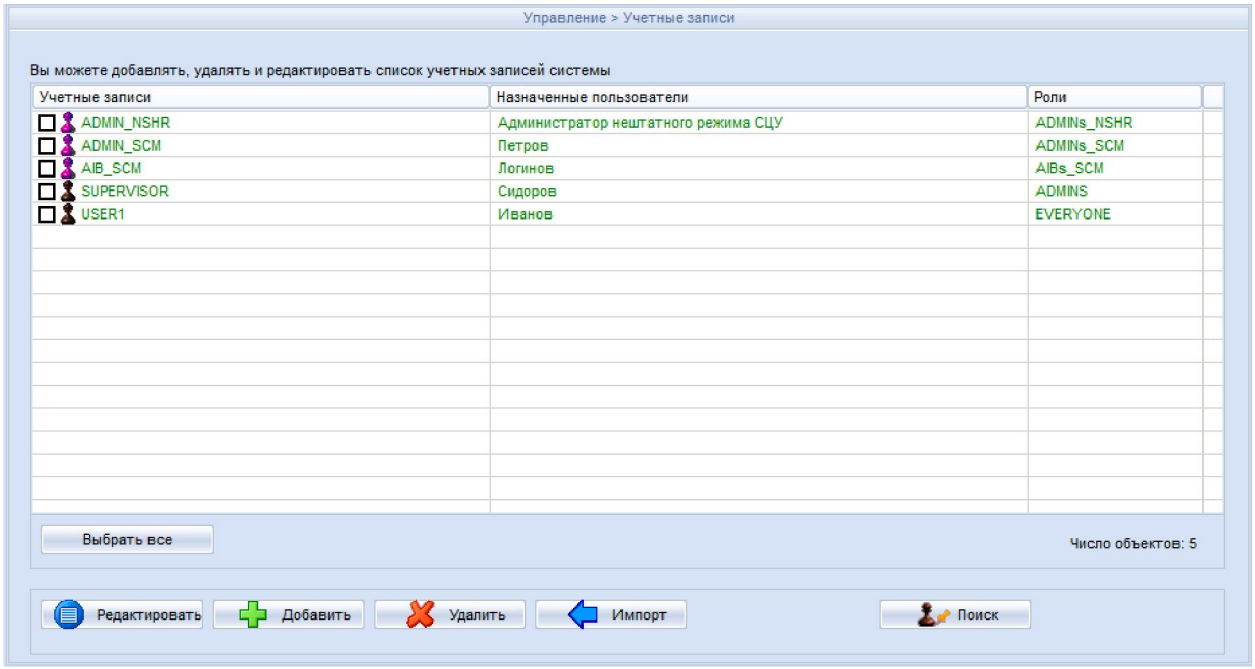

Рисунок 58 - Учетные записи

Чтобы добавить новую учетную запись, необходимо нажать кнопку <Добавить>.

В появившемся окне (рисунок 59) следует ввести имя учетной записи, указать роль, назначить пользователя (сотрудника как физического лица)[1], которому назначается данная учетная запись, имя пользователя[2)], полное имя пользователя[3)], ввести пароль и подтвердить его ввод, назначить пользователю идентификатор и выбрать компьютеры, на которых будет создана данная учетная запись. После ввода этих параметров необходимо нажать кнопку <Применить>.

При добавлении учетной записи Администратора ИБ для нового технологического участка проверяется принадлежность выбранной учетной записи роли Администратора информационной безопасности ранее созданных технологических участков. Если учетная запись принадлежит Администратору ИБ одного из ранее созданных технологических участков, то её модификация запрещается.

При регистрации ПКО СУЦУ СЗИ НСД создает «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 подсисте-

---

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

[2)] Логин в базе пользователей АМДЗ.

[3)] Имя пользователя в домене.

му 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 см. документ «Установка правил разграничения доступа. Программа ACED32» 11443195.4012-036 97).

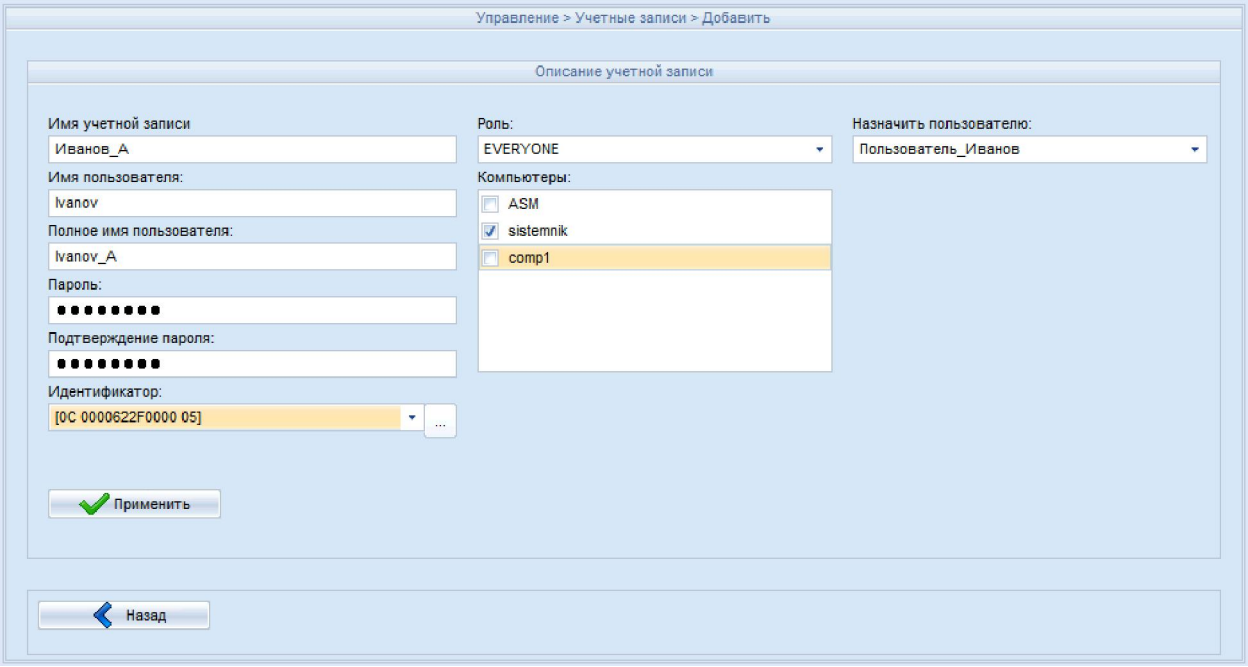

Рисунок 59 - Добавление новой учетной записи

Чтобы отредактировать настройки учетной записи, следует выделить ее и нажать кнопку <Редактировать> на вкладке «Учетные записи» (рисунок 58), в появившемся окне (рисунок 60) изменить параметры учетной записи[1)]. После завершения редактирования необходимо нажать кнопку <Применить>.

[1)] Во вкладке «Учетные записи>Редактировать» при выборе роли для редактируемой учетной записи отображаются только те компьютеры, которые принадлежат такому же технологическому участку, как и выбранная роль

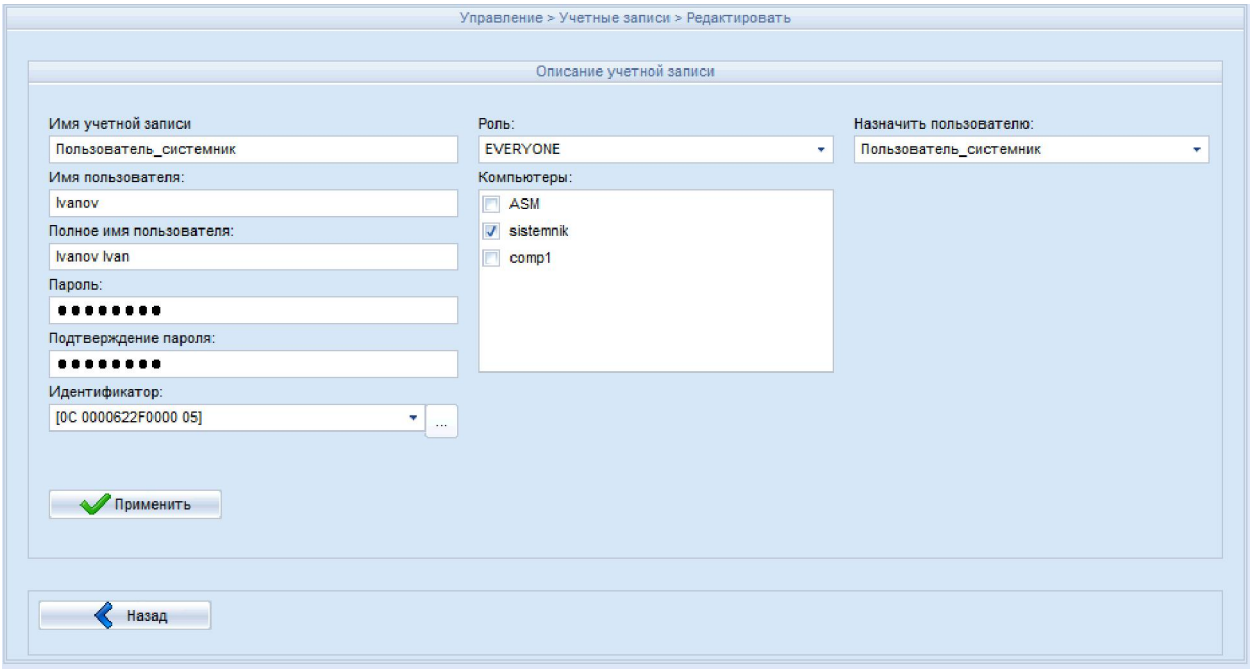

Рисунок 60 - Редактирование параметров учетной записи

ВНИМАНИЕ! В ASM реализована функция централизованной смены паролей учетных записей пользователей ПКО. Для этого необходимо во вкладке Учетные записи\Редактировать изменить пароль учетной записи пользователя ПКО, затем выполнить процедуру передачи базы пользователей на ПКО (подробнее см.подраздел 4.1.4).

Базы учетных записей пользователей ПКО хранятся на сервере централизованного управления в каталоге C:\ASM\TEMPLATE\ (при удалении или обновлении ПО СУЦУ СЗИ от НСД базы учетных записей не удаляются).

Чтобы удалить учетную запись, необходимо выделить ее и нажать кнопку <Удалить> на вкладке «Учетные записи» (рисунок 58). Появится окно подтверждения этого действия (рисунок 61), следует нажать кнопку <Да>, если действительно нужно удалить учетную запись.

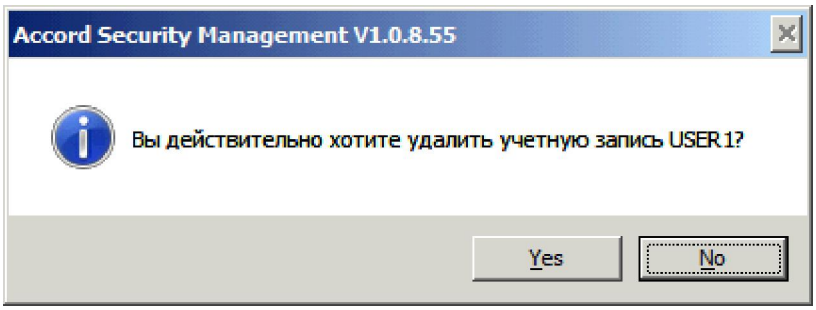

Рисунок 61 - Окно подтверждения удаления учетной записи

Если необходимо определить, какой учетной записи принадлежит данный идентификатор, следует нажать кнопку <Поиск> на вкладке «Учетные записи» (рисунок 58). Появится окно с сообщением «Предъявите идентификатор» (рисунок 62).

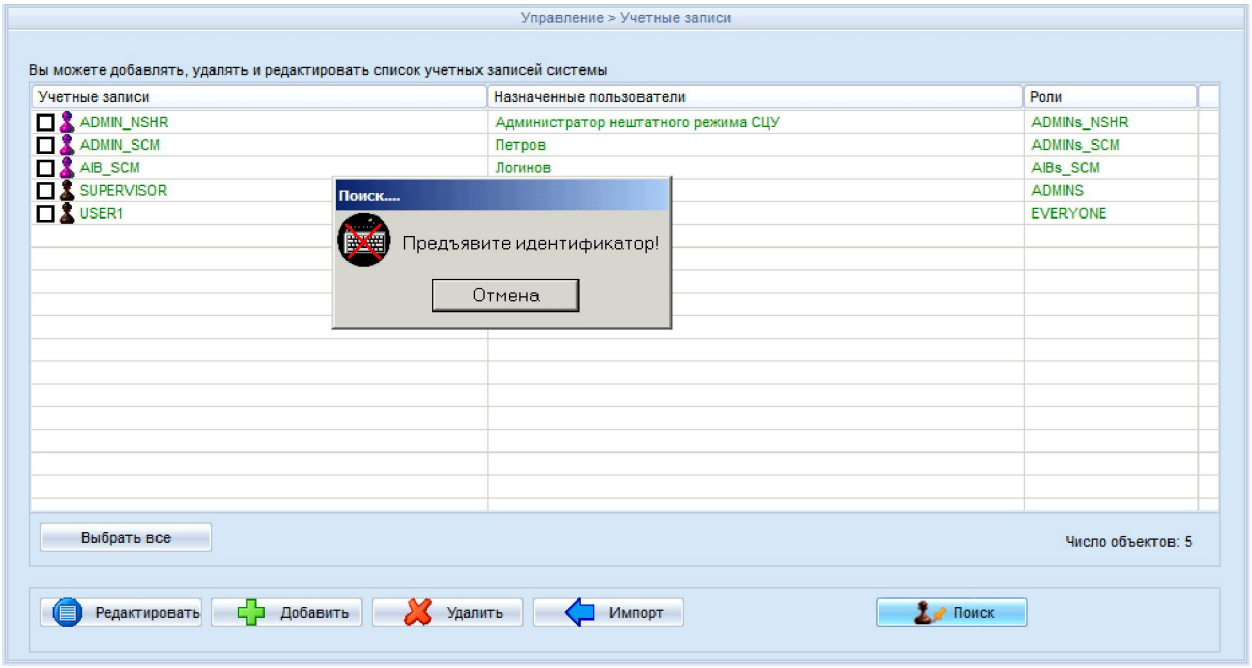

Рисунок 62 - Окно с сообщением «Предъявите идентификатор»

Если данный идентификатор назначен какой-либо учетной записи, то эта учетная запись будет выделена (рисунок 63), иначе в нижней части окна появится сообщение «Идентификатор не зарегистрирован!» (рисунок 64).

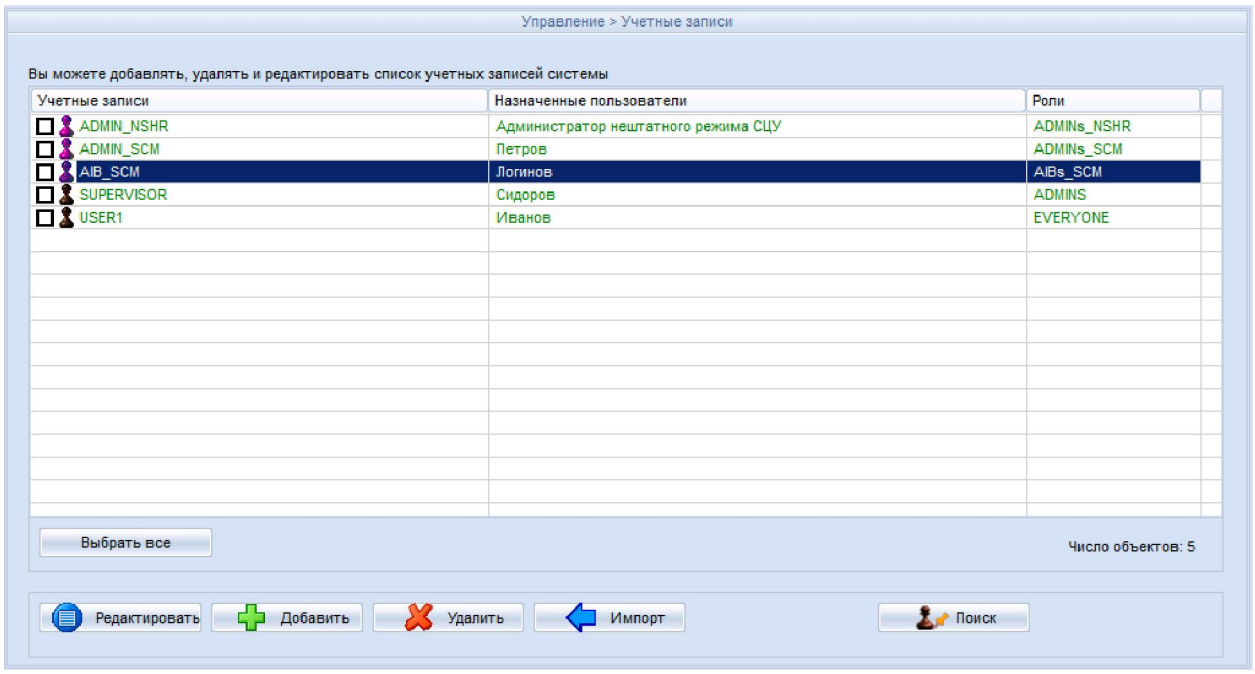

Рисунок 63 - Учетная запись, которой назначен идентификатор

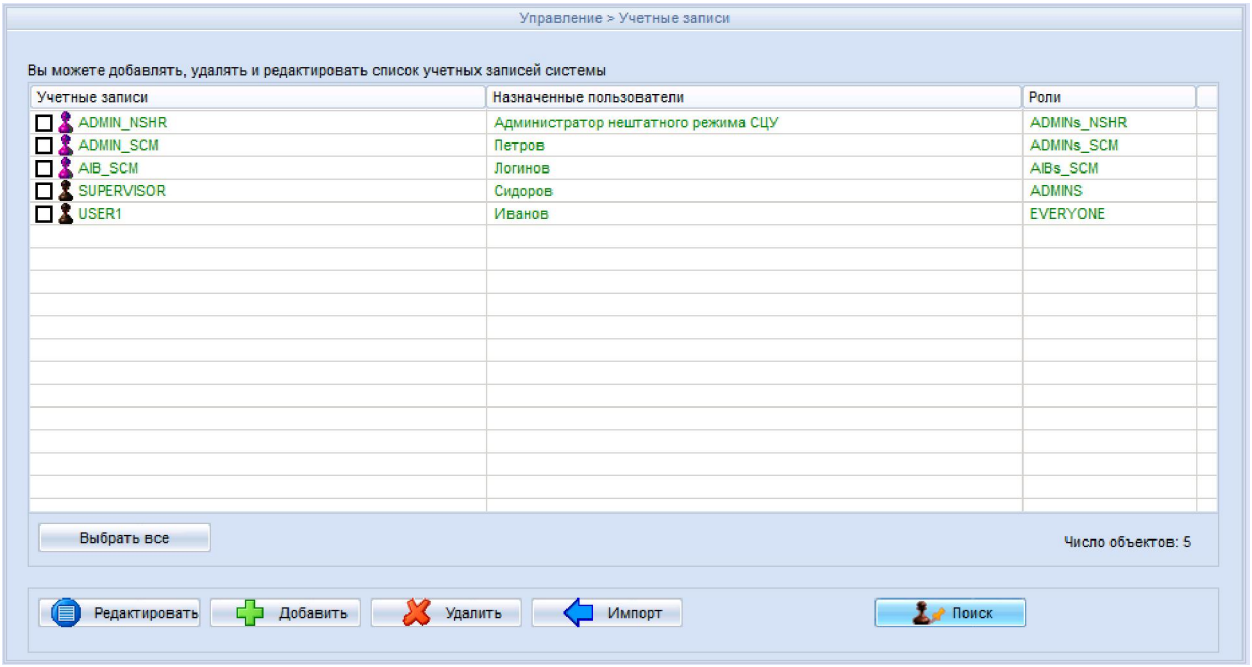

Рисунок 64 - Сообщение о том, что идентификатор не зарегистрирован

Администратор ИБ не может редактировать учетную запись Администратора, однако (при совместном участии (авторизации) Администратора) может редактировать учетную запись Администратора НШР. Для этого необходимо во вкладке «Учетные записи» выбрать учетную запись Администратора НШР и нажать кнопку <Редактировать> (рисунок 65). Далее необходимо к USB-порту сервера централизованного управления подключить идентификатор Администратора СУЦУ и выбрать кнопку <Изменить>.

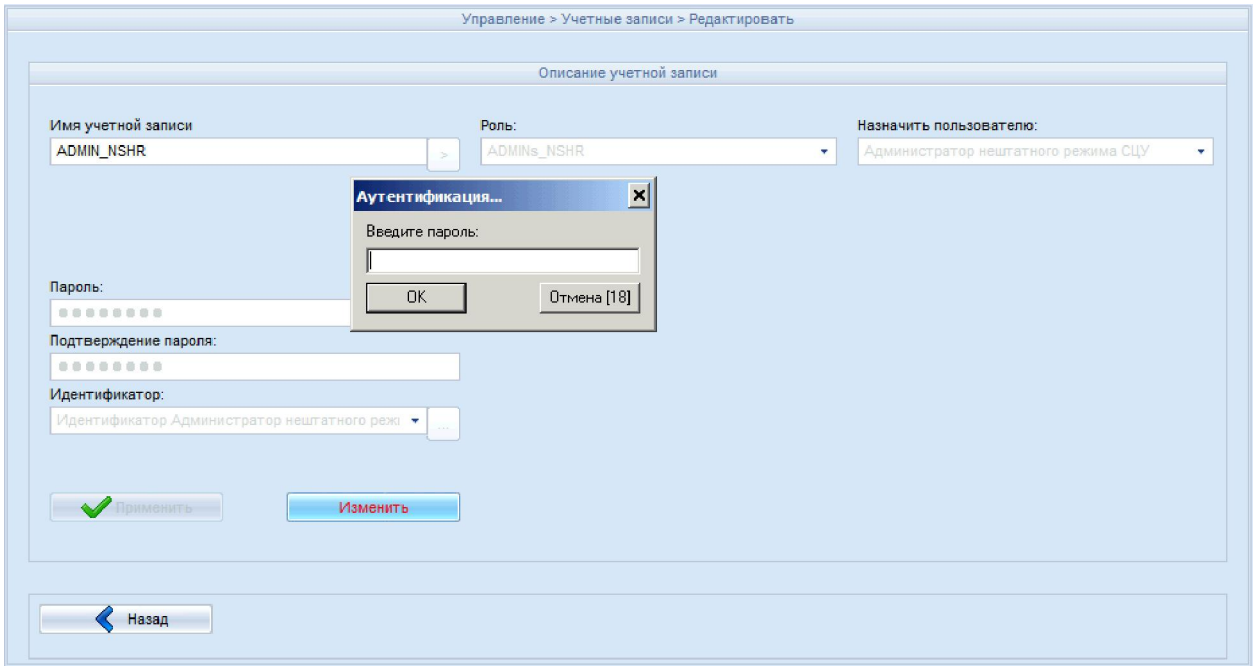

Рисунок 65 – Редактирование учетной записи Администратора НШР

В появившемся окне необходимо ввести пароль Администратора СУЦУ и нажать кнопку <OK>. После выполнения процедуры аутентификации становятся доступными следующие операции:

- смена пароля Администратора нештатного режима функционирования;
- выбор идентификатора для Администратора нештатного режима функционирования (рисунок 66).

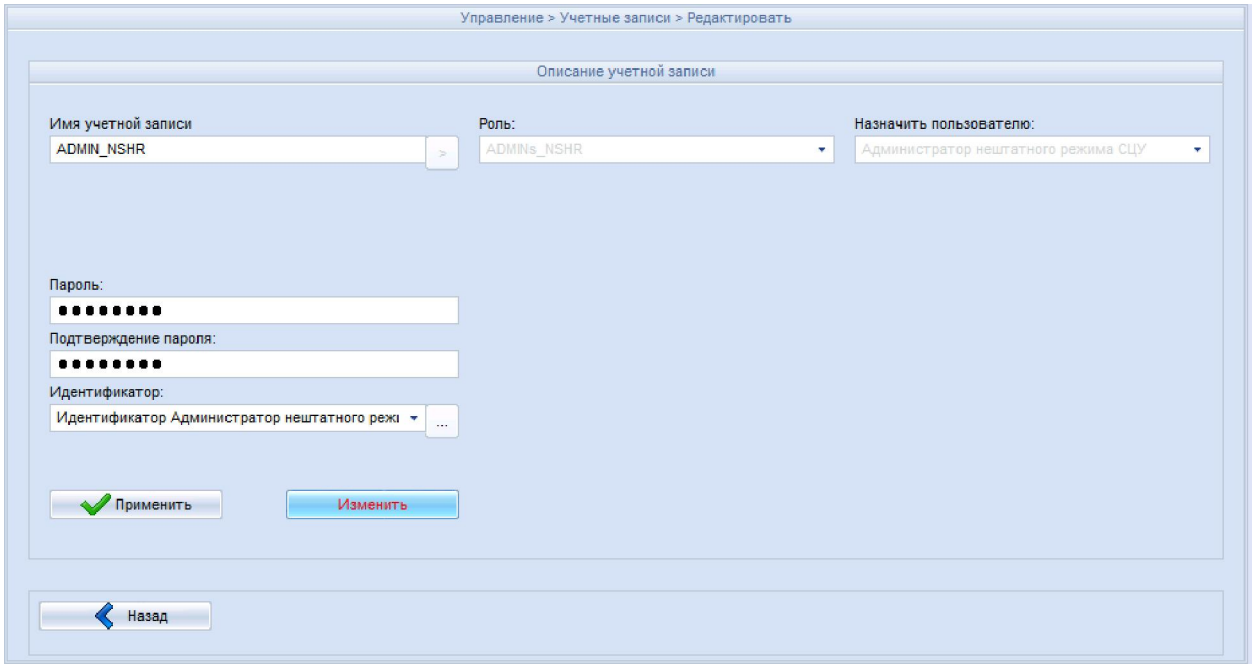

Рисунок 66 – Окно редактирования учетной записи Администратора НШР с доступными операциями смены пароля и идентификатора

После выполненных изменений нужно нажать кнопку <Применить>. По нажатии кнопки на экране появляется сообщение о том, что учетная запись Администратора НШР изменена (рисунок 67):

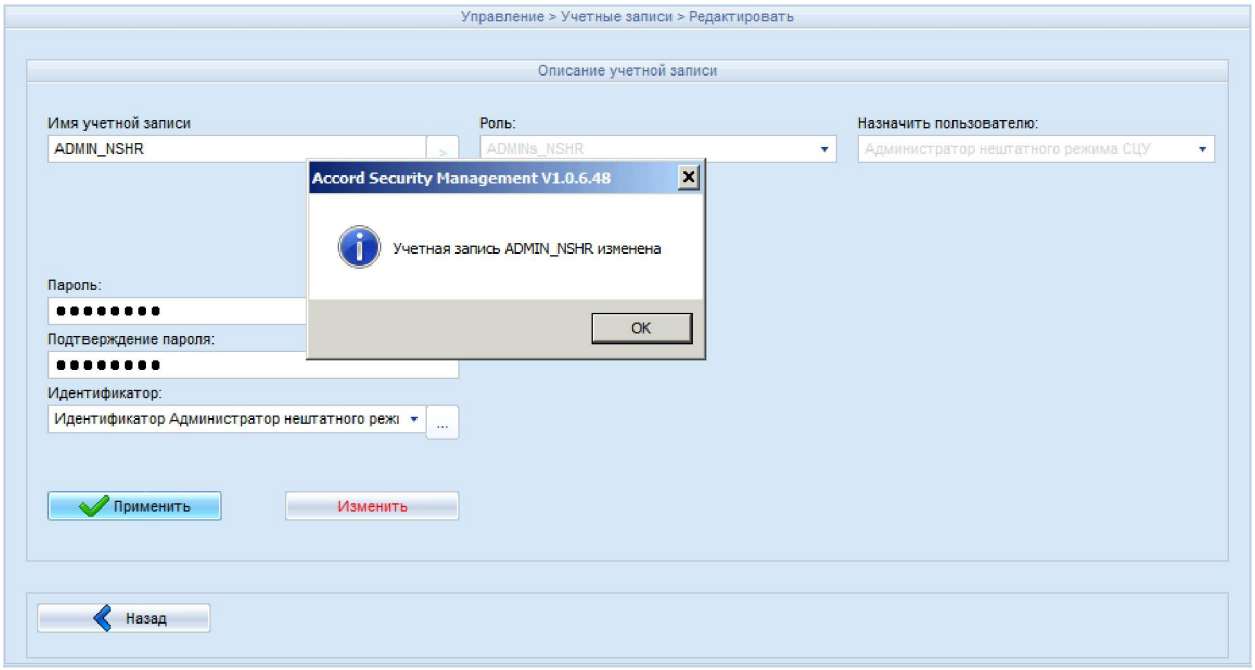

Рисунок 67 – Сообщение об изменении учетной записи Администратора НШР

Для получения данных об учетных записях пользователей в рамках централизованной схемы необходимо во вкладке «Учетные записи» нажать кнопку <Импорт> (рисунок 58). Далее в появившемся окне (рисунок 68) нужно выбрать флаг «Вы можете импортировать учетные записи из:» - «базы пользователей NT».

После этого следует ввести IP-адрес или имя сервера, из базы пользователей которого будут импортированы учетные записи, а также имя и пароль Администратора данного сервера (рисунок 68).

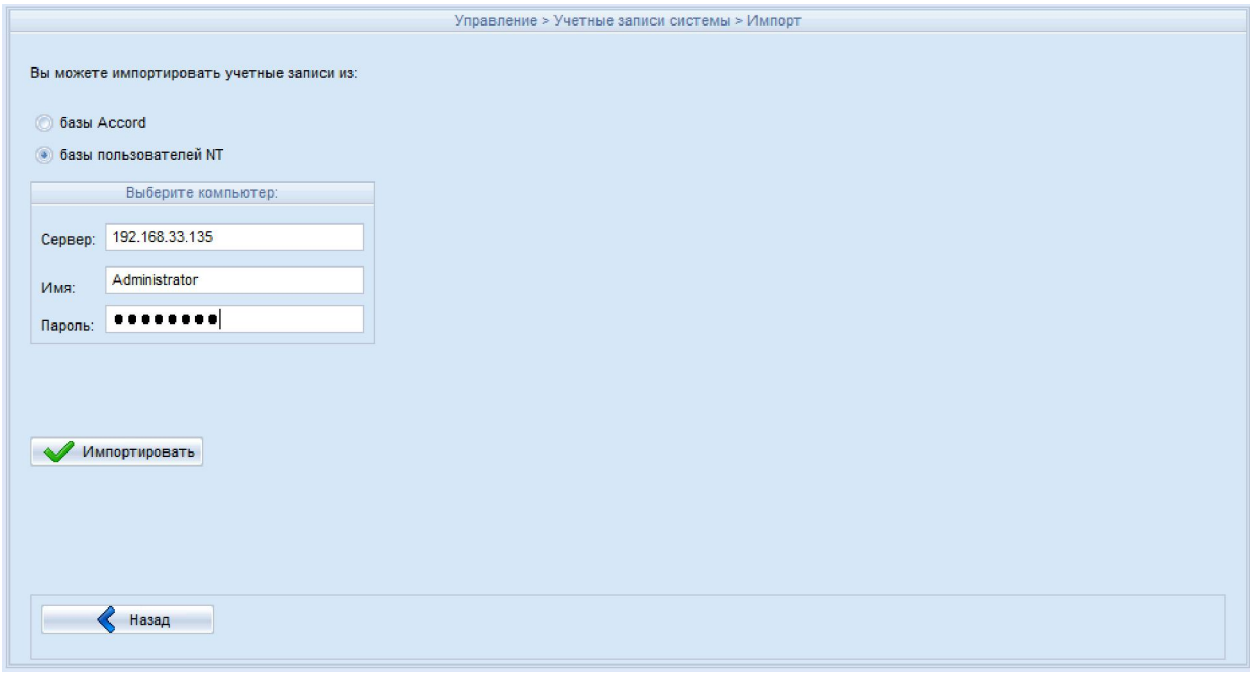

Рисунок 68 - Ввод данных о сервере, из базы пользователей которого будут импортированы учетные записи

После этого в правой части окна появятся импортированные учетные записи, следует выбрать из них необходимые для добавления в базу (для выбора всех учетных записей нужно нажать кнопку <Выбрать все>) и нажать кнопку <Добавить> (рисунок 69).

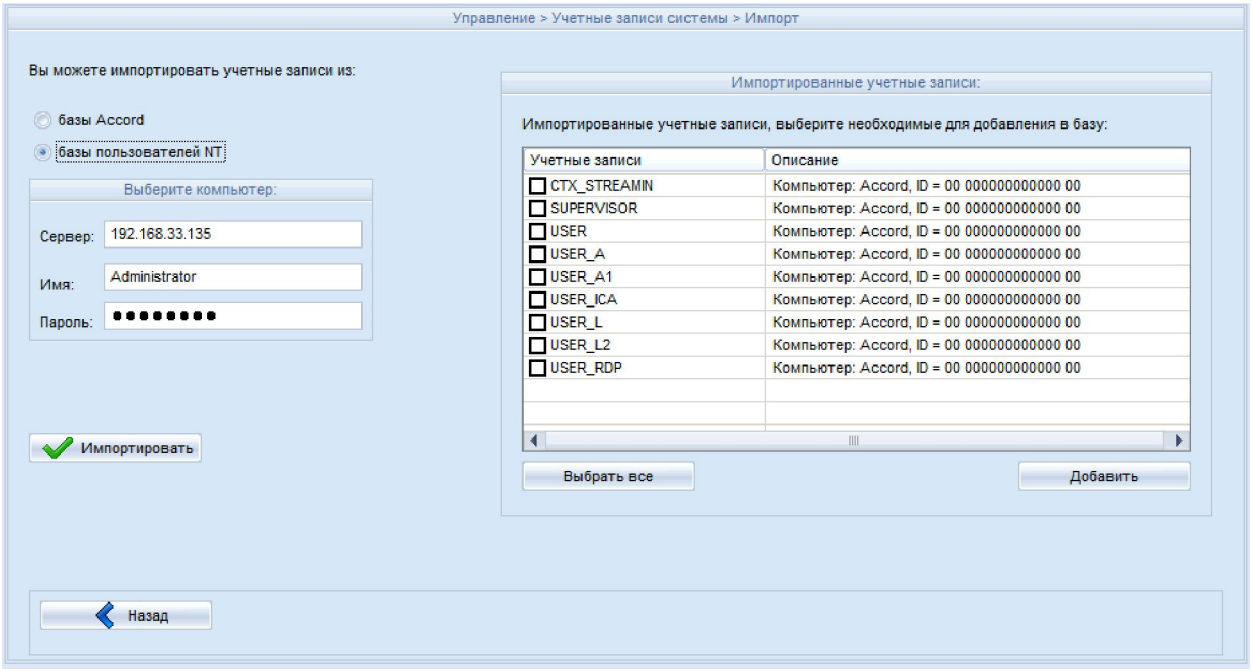

Рисунок 69 - Выбор импортированных учетных записей (импорт из базы пользователей NT)

Для получения данных об учетных записях пользователей ПКО в рамках децентрализованной схемы используется функция экспорта списка пользователей СЗИ от НСД 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 передачи баз пользователей на ПКО в рамках децентрализованной схемы, необходимо добавить флеш -накопитель в единую базу USB-носителей (эта процедура выполняется Администратором СУЦУ в соответствии с документом «Руководство Администратора» 11443195.4012-053 90).

Чтобы передать базы пользователей, необходимо на ПКО в трее выбрать правой кнопкой мыши сетевой клиент ПАК «Аккорд» (рисунок 53). После этого на экране появляется контекстное меню (рисунок 54).

Далее необходимо выбрать команду «Экспорт базы пользователей» (рисунок 54).

После этого на экране появляется сообщение «Предъявите идентификатор». Необходимо установить идентификатор Администратора ИБ в свободный USB-разъем компьютера.

После этого на экране появится окно ввода пароля. Следует ввести пароль и нажать кнопку <OK> (рисунок 55):

После выполнения операции ввода пароля на экране появляется окно выбора каталога для сохранения базы пользователей (рисунок 70), необходимо выбрать нужный каталог и нажать кнопку <OK>.

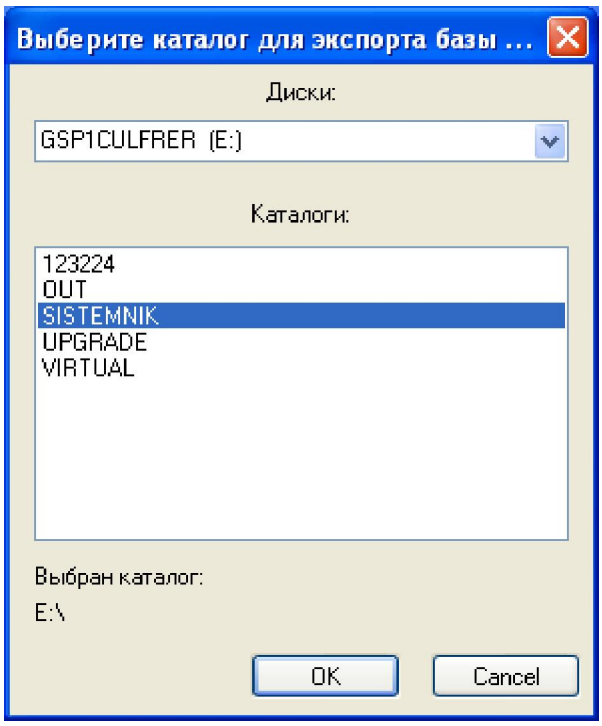

Рисунок 70 – Выбор каталога для сохранения базы пользователей

Если описанная процедура выполнена успешно, то на экране появляется следующее оповещение (рисунок 71):

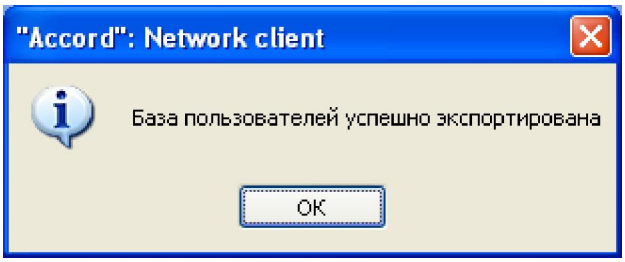

Рисунок 71 - Оповещение об успешном выполнении процедуры экспорта базы пользователей

Далее базы пользователей на внешнем носителе должны быть доставлены на сервер централизованного управления.

Во вкладке «Учетные записи» ПО ASM на сервере централизованного управления необходимо нажать кнопку <Импорт> (рисунок 58). В появившемся окне (рисунок 72) необходимо выбрать флаг «Вы можете импортировать учетные записи из:» - «базы Accord» (предварительно следует обновить базы, нажав кнопку <Обновить>) и нажать кнопку <Импортировать>. (учетные записи при этом импортируются из каталога, <выбранный_каталог>\IN\xxx\ xxx.AMZ, где <выбранный_каталог> – каталог на внешнем носителе, xxx – имя ПКО, xxx.AMZ – файл, в котором находится список баз пользователей).

Рисунок 72 - Импорт учетных записей из базы «Аккорда»

В появившемся на экране окне (рисунок 73) следует указать файл с именем ПКО, с которого необходимо импортировать учетные записи.

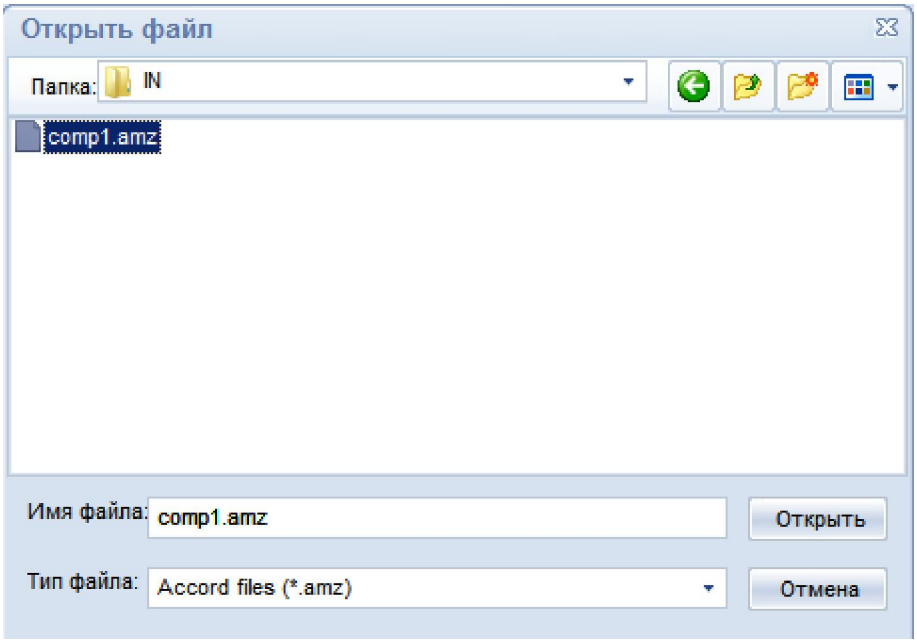

Рисунок 73 - Выбор файла *.amz, из которого необходимо импортировать учетные записи

После этого в правой части окна появятся импортированные учетные записи; следует выбрать из них необходимые для добавления в базу (для выбора всех учетных записей нужно нажать кнопку <Выбрать все>) и нажать кнопку <Добавить> (рисунок 74).

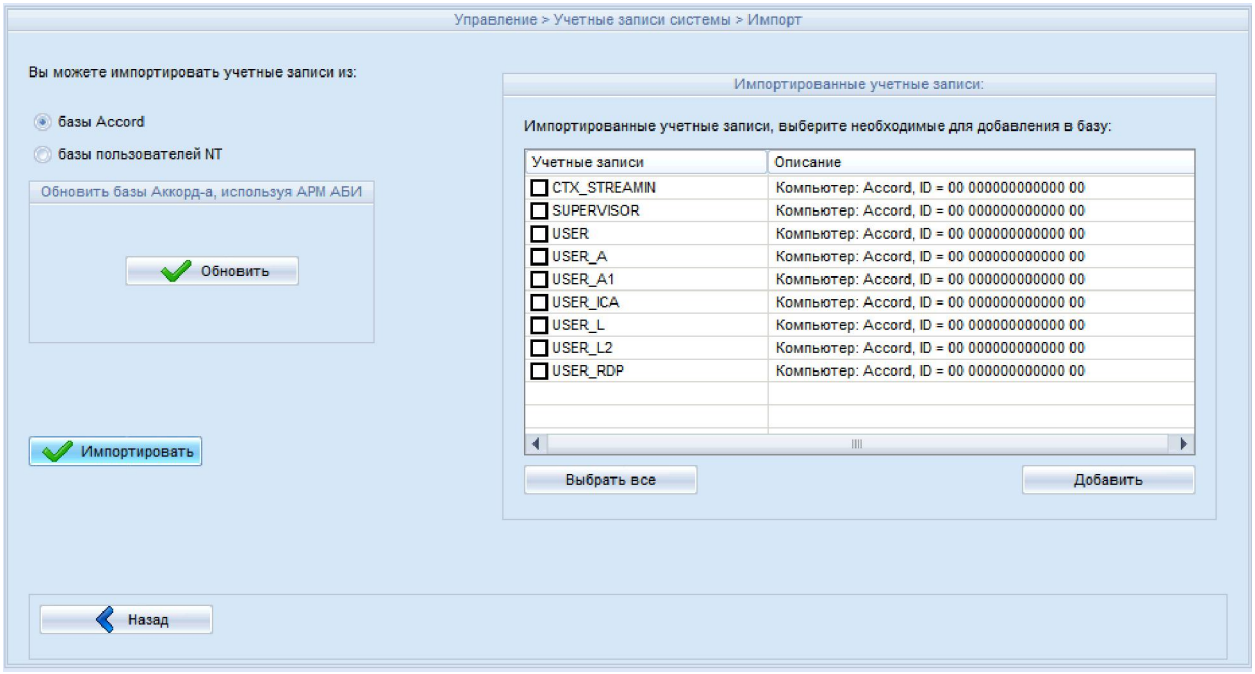

Рисунок 74 - Выбор импортированных учетных записей (импорт из базы «Аккорда»)

При первом выполнении процедуры получения базы пользователей ПКО на сервере централизованного управления создается каталог C:\Asm\ACCONET\IN\CompName (где «CompName» – имя ПКО), в котором хранятся файлы базы пользователей ПКО. Сервер централизованного управления 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.

4.2 Работа с журналами

Открыв вкладку «Журналы», Администратор ИБ СУЦУ может работать с тремя типами журналов.

Первый тип – Журналы «Аккорд», в которых содержатся сведения о работе пользователей на рабочих местах (рисунок 75). (Журналы «Аккорд» 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.

Например: C:/Asm/ACCONNET/Client.Log/Demo_PC/18_01_2013/20131005172617.LOW). Маска файла журнала следующая: «*******.LOW», где знак «*******» обозначает дату с точностью до секунды).

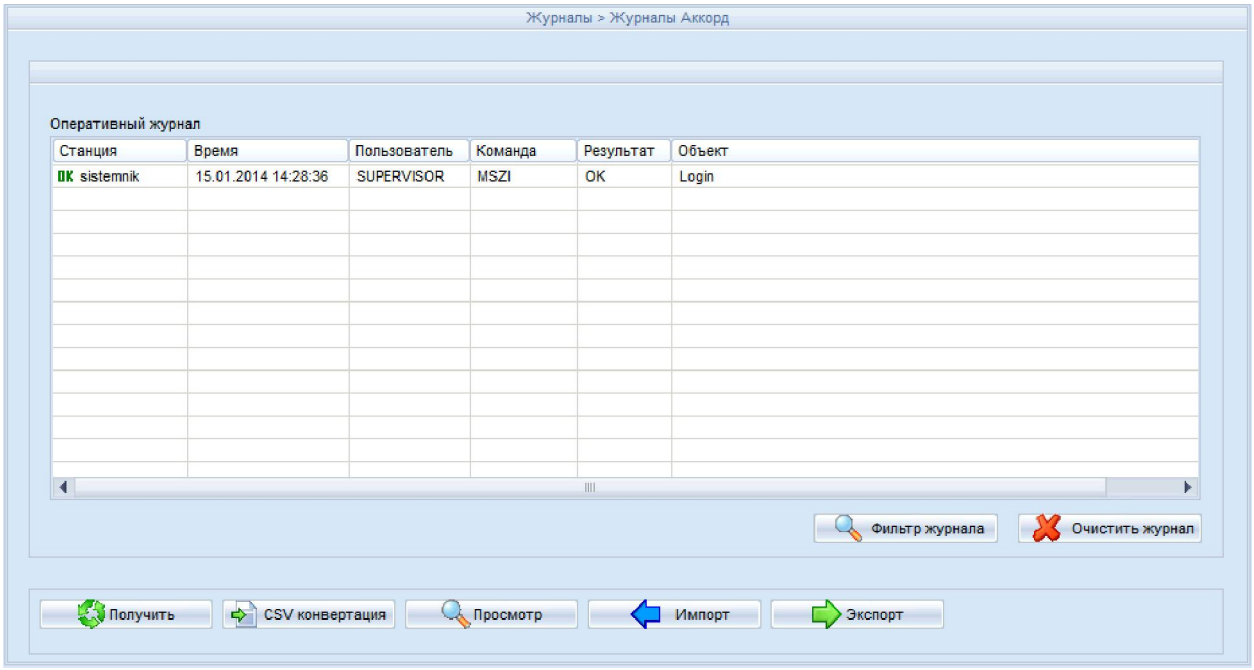

Рисунок 75 - Журналы «Аккорд»

Сведения, хранящиеся в журнале, обновляются в режиме реального времени.

Получить журналы с ПКО (по централизованной схеме) можно по нажатии кнопки <Получить>. По нажатии кнопки на экране появляется окно, в котором следует выбрать ПКО, с которых планируется получить журналы (рисунок 76).

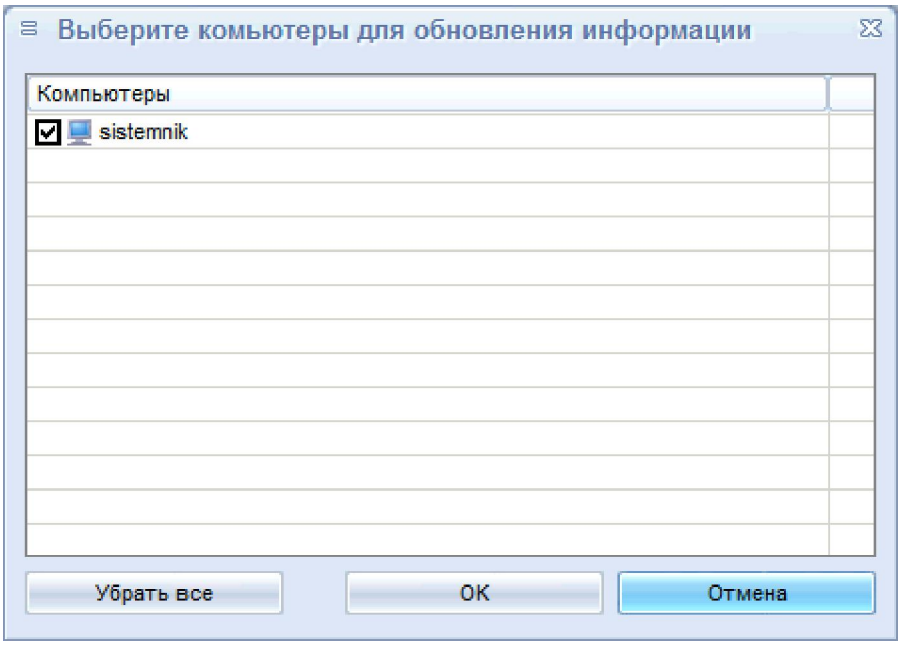

Рисунок 76 – Выбор ПКО, с которых планируется получить журналы[1)]

Для просмотра журнала необходимо нажать кнопку <Просмотр>. После этого на экране появляется окно выбора каталога, в котором нужно выбрать необходимый файл.

[1)] В случае эксплуатации ПП СУЦУ СЗИ от НСД версии 1.0.8.52 и выше сбор журналов происходит в автоматическом режиме.

Журнал «Аккорд» можно экспортировать (например, для дальнейшего анализа в системах мониторинга), для этого необходимо нажать кнопку <Экспорт>. Далее на экране появляется окно выбора каталога, в котором необходимо выбрать каталог и нажать кнопку <Применить>.

Конвертировать журнал в общепринятые форматы можно, нажав кнопку <CSV конвертация> (или <XML конвертация>, если в настройках фильтров экспорта журналов выбрать пункт «XML файл для конвертации журналов», подробнее об этом см. подраздел 4.3.3 настоящего документа) в окне, показанном на рисунке 75. В результате этой операции в каталоге, указанном в поле «CSV файл для конвертации журналов:» (или в каталоге, указанном в поле «XML файл для конвертации журналов» (в зависимости от выбранных настроек) рисунок 86), появится файл в формате csv (или в формате xml в зависимости от выбранных настроек), предназначенный для работы с фильтрами экспорта журналов.

ВНИМАНИЕ! Файл *.csv по умолчанию имеет разделители в виде символа «=». Чтобы изменить указанный символ на другой, следует в файле asm.ini указать параметр «Separator».

Кнопка <Импорт> необходима для получения журналов с ПКО по децентрализованной схеме (см. ниже).

По нажатии кнопки <Фильтр журнала> на экране появляется окно смены фильтров оперативного журнала (рисунок 77).

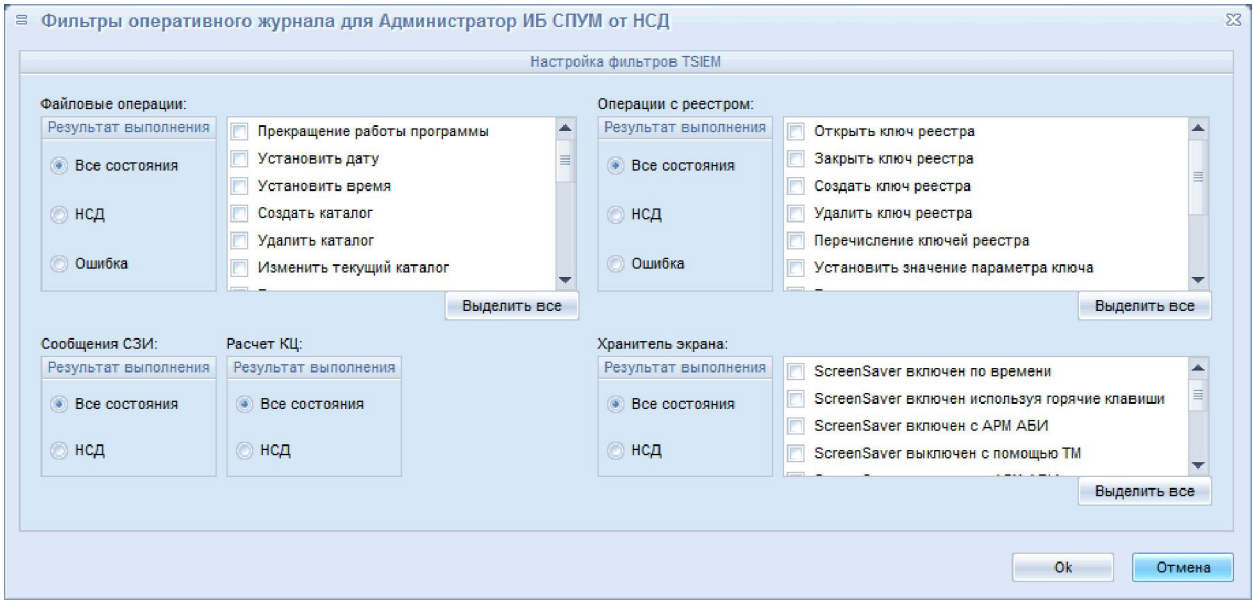

Рисунок 77 – Фильтры оперативного журнала для текущей учетной записи

В нем можно выбрать типы событий, информация о которых передается в оперативный журнал, для текущей учетной записи (в данном случае для Администратора ИБ, см. рисунок 77). События хранятся в каталоге ASM\AccountName_FilterParam.ini, где параметр «AccountName» – это имя учетной записи.

Второй тип – журналы ASM, касающиеся работы утилиты ASM (рисунок 78). В них записываются дата и время выполнения операций в ASM, сами эти операции, информация о попытках несанкционированного доступа, информация об изменении параметров ASM (сообщения об изменении параметров имеют префикс CFG). (Журналы ASM хранятся в каталоге ASM/ACCONNET/Client.Log в следующей форме: «asm*****.LOW», где знак «*****» обозначает дату с точностью до секунды).

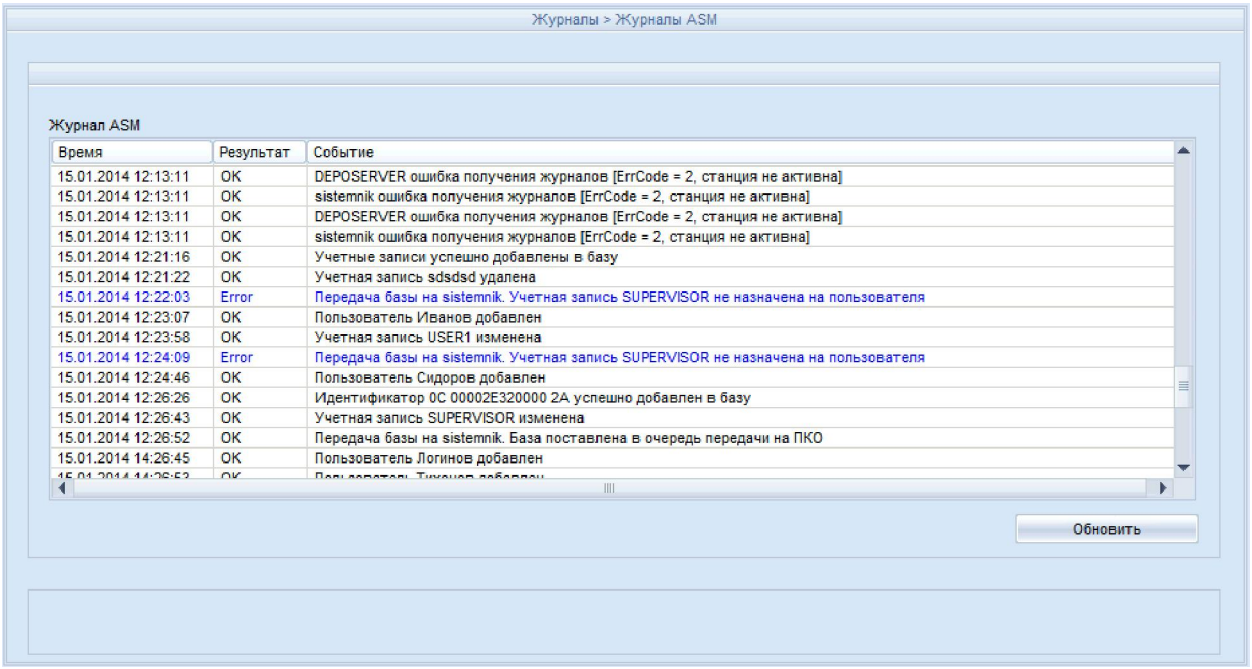

Рисунок 78 - Журнал ASM

Третий тип журналов - журнал АРМ АБИ, касающийся работы утилиты AcConnet (рисунок 79). Он необходим для просмотра сетевых сообщений.

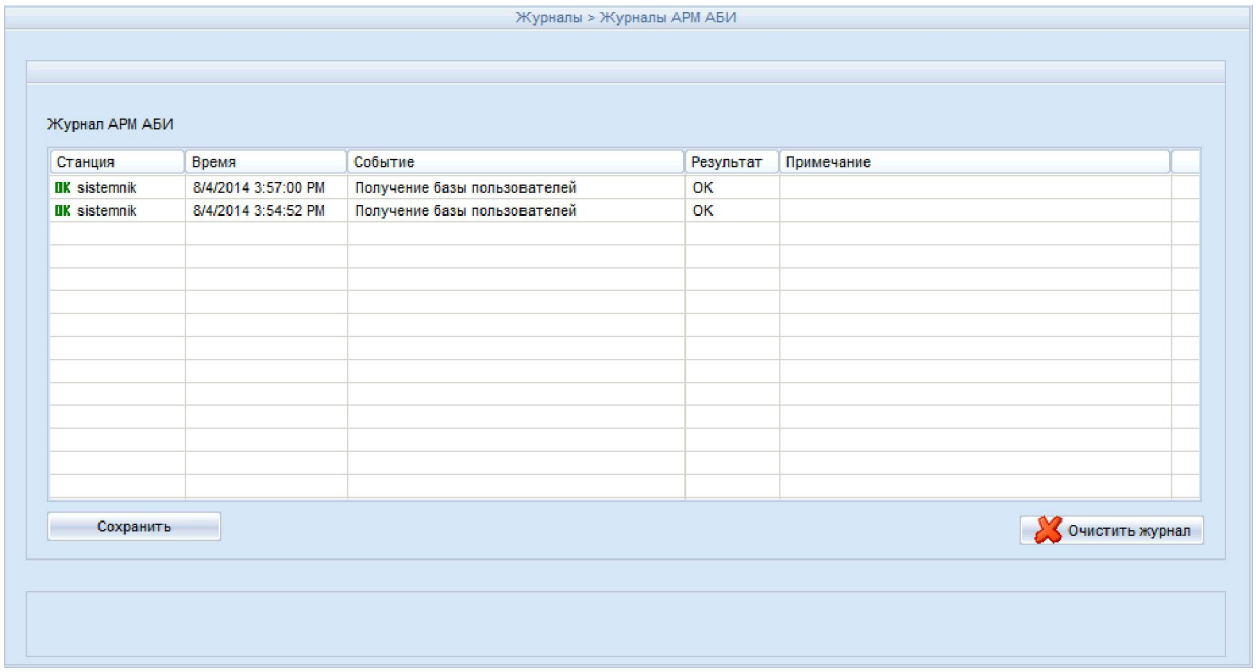

Рисунок 79 – Журнал АРМ АБИ

Журнал АРМ АБИ можно сохранить в текстовый файл с разделителем «|». Для этого необходимо нажать кнопку <Сохранить> (рисунок 79). По нажатии кнопки на экране появляется окно, в котором нужно ввести название файла и нажать кнопку <Сохранить> (рисунок 80).

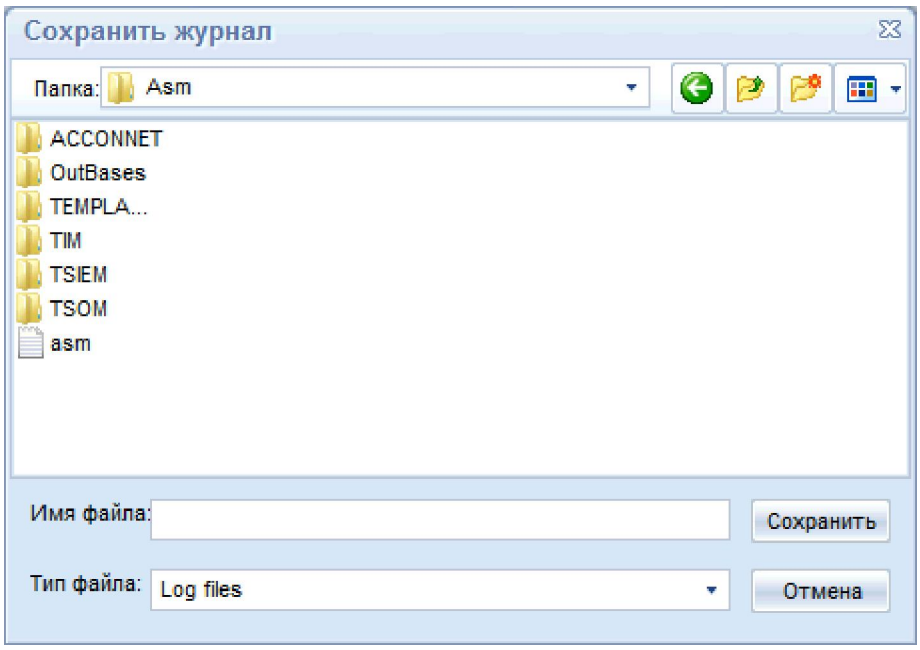

Рисунок 80 – Сохранение журнала АРМ АБИ в текстовый файл

Для получения журналов ПКО в рамках децентрализованной схемы используется функция экспорта журналов СЗИ от НСД ПКО. При этом производится копирование перечня журналов на внешний носитель, в качестве которого может использоваться USB флэш-накопитель или флоппи-диск (журналы экспортируются в каталог <выбранный_каталог>:\IN\xxxx\, где <выбранный_каталог> – каталог на внешнем носителе, xxx - имя станции.). Далее перечень на внешнем носителе должен быть доставлен на сервер централизованного управления.

Получив каталог с журналами ПКО, Администратор ИБ должен выполнить следующие действия:

- копировать каталог с журналами на сервер централизованного управления;
- во вкладке «Журналы» нажать кнопку <Импорт> (рисунок 75);
- далее в появившемся окне выбрать необходимый каталог и нажать кнопку <Применить>.

4.3 Настройка ASM

4.3.1 Основные настройки

На рисунке 81 показана панель для задания основных настроек ASM, которое выводится на экран после открытия вкладки Настройка - > Основные настройки. Посредством пользовательского интерфейса «Основные настройки» имеется возможность:

- выполнить настройку учётной записи ASM;
- управлять включением/отключением механизма синхронизации учетных записей СУЦУ с учетными записями Аккорд.

Если во вкладке Настройки>Основные настройки установлен флаг «При запуске программы использовать уч.запись пользователя Аккорд», то при запуске ASM, идентификатор и пароль считываются из текущей сессии пользователя Аккорд.

Если установлен флаг «При запуске программы использовать уч.запись пользователя Аккорд», но необходимо войти в систему под другой учетной записью, то при запуске программы ASM нужно нажать и удерживать клавишу <Shift>.

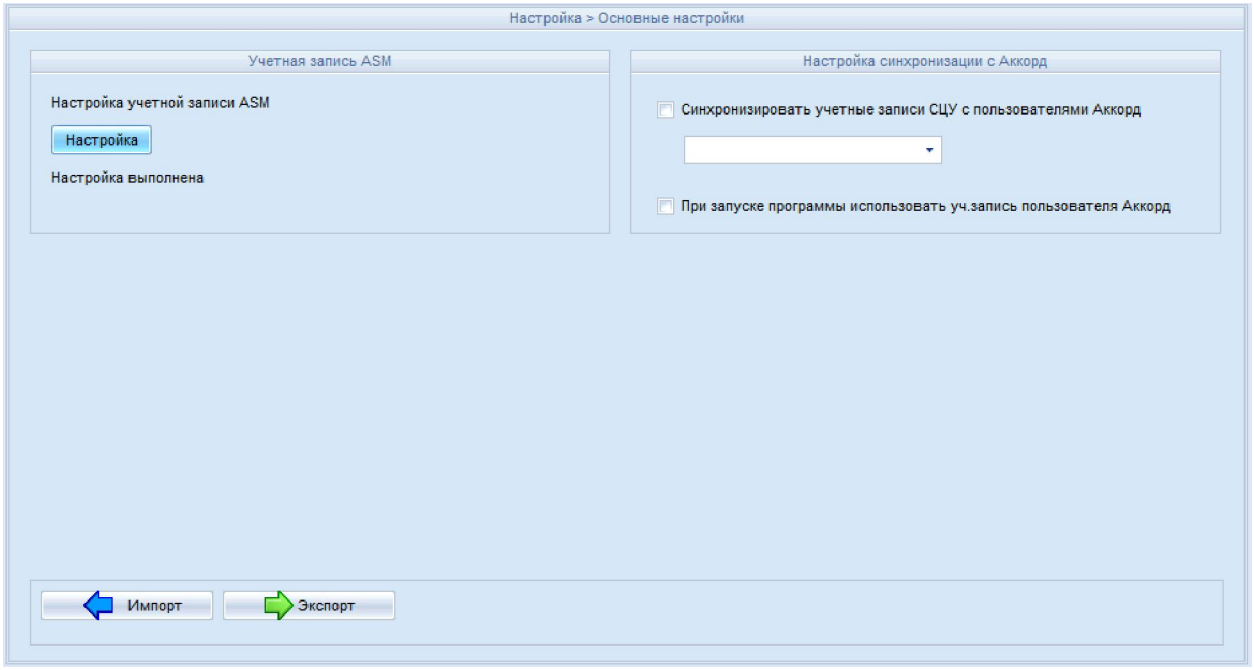

Рисунок 81 – Основные настройки ASM

ВНИМАНИЕ! Средствами ASM реализована возможность создания (или удаления) в базе пользователей СЗИ от НСД «Аккорд» учетной записи пользователя ПКО при условии создания (или удаления) аналогичной учетной записи в ASM.

Для этого необходимо выполнить следующие действия:

- на подконтрольном объекте в СЗИ от НСД «Аккорд» имеется пользователь «ASM_ACCOUNT». Если такого пользователя нет, то его необходимо создать (с помощью программы AcSetWs.exe);

- на ПКО запустить программу MAKEPRC.EXE, добавить в нее процесс AsmT.exe, присвоить процессу полный доступ к каталогу C:\Accord.x64;

- на сервере централизованного управления во вкладке ASM->Настройка->Основные Настройки в поле «Настройка синхронизации с Аккорд» поставить галку «Синхронизировать учетные записи СУЦУ с пользователями Аккорд»;

- ниже выбрать группу базы пользователей СЗИ от НСД «Аккорд».

После выполнения описанных действий при создании новой учетной записи в ASM аналогичная запись создается в базе пользователей СЗИ от НСД «Аккорд» (файл Accord.AMZ).

Если в редакторе прав доступа ACED32 отмечен пункт «Синхронизация с базой АМДЗ», то учетная запись пользователя ПКО (после создания в ASM) создается и в контроллере (именно для этого нужна учетная запись «ASM_ACCOUNT»).

Если процесс ASMT.exe имеет привилегии Windows по добавлению пользователей в систему и в редакторе прав доступа отмечен флаг «Синхронизация с

базой NT», то учетная запись пользователя ПКО (после создания в ASM) создается и в базе пользователей Windows.

После установки ПО СУЦУ необходимо выполнить процедуру настройки контроля целостности и правил разграничения доступа к собственному ПО СУЦУ. Для этого необходимо с использованием утилиты make.prc:

- установить полный доступ к каталогу установки ПО СУЦУ на сервере централизованного управления (C:\ASM) исключительно для процессов ASM_T.EXE, ACED32.EXE, LOGVIEW.EXE;

- установить полный доступ для каждого из процессов ASM_T.EXE, ACED32.EXE, LOGVIEW.EXE к ресурсам "\DEVICE\" и "\\";

- в списке объектов для контроля целостности указать процессы ASM_T.EXE, ACED32.EXE, LOGVIEW.EXE, а также файлы с расширением *.dll из каталога установки ПО СУЦУ на сервере централизованного управления (C:\ASM).

4.3.2 Настройка фильтров оперативного журнала

Для настройки взаимодействия фильтров оперативного журнала и ASM следует выбрать вкладку Настройка->Оперативный журнал и установить необходимый флаг в группах «Результат выполнения» для файловых операций и операций с реестром, для сообщений СЗИ, расчета КЦ и хранителя экрана (рисунок 82).

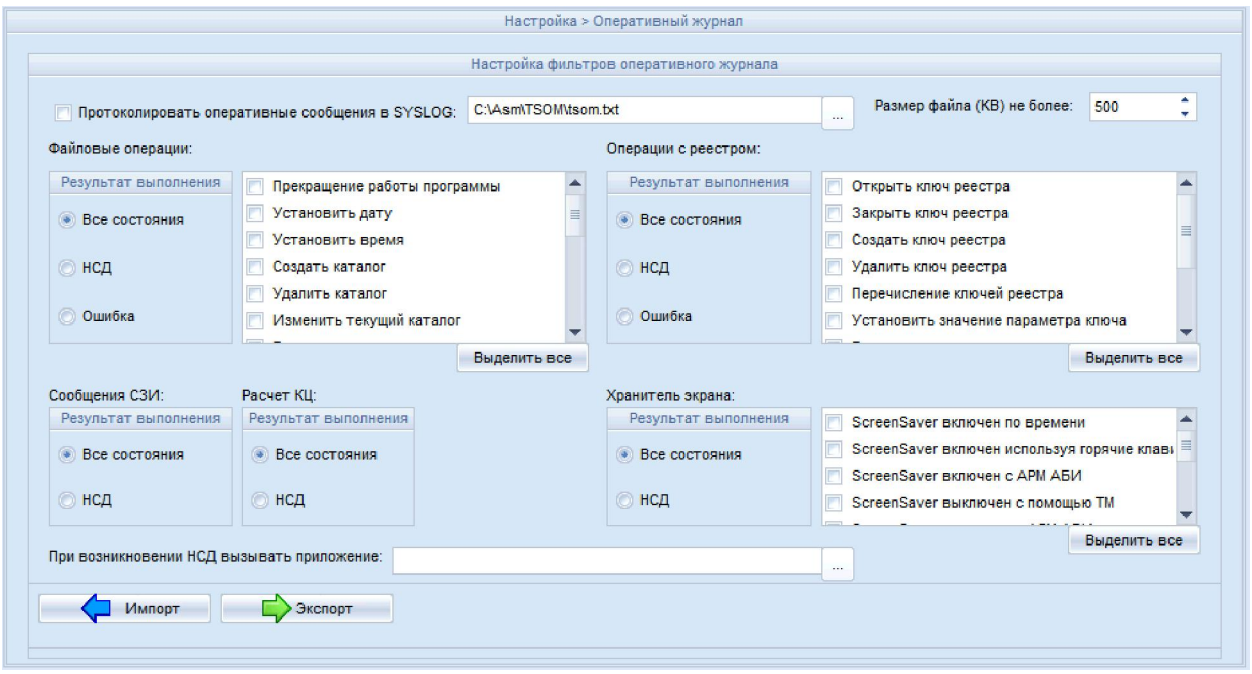

Рисунок 82 – Настройка фильтров оперативного журнала

В окне настроек фильтров оперативного журнала так же можно выбрать максимальный размер файла оперативного журнала. Для этого следует выбрать необходимое значение в поле «Размер файла (КВ) не более» (рисунок 82).

Для формирования шаблонов настроек журналов, с которыми отсутствует сетевое соединение, по децентрализованной схеме Администратор ИБ ТУ может выбрать нужные настройки (рисунок 82), экспортировать их (посредством кнопки <Экспорт> во вкладке Настройка->Оперативный журнал) на внешний носитель, в качестве которого может использоваться USB флэш-накопитель или флоппи-диск.

По нажатии кнопки <Экспорт> на экране появляется окно выбора каталога (рисунок 83).

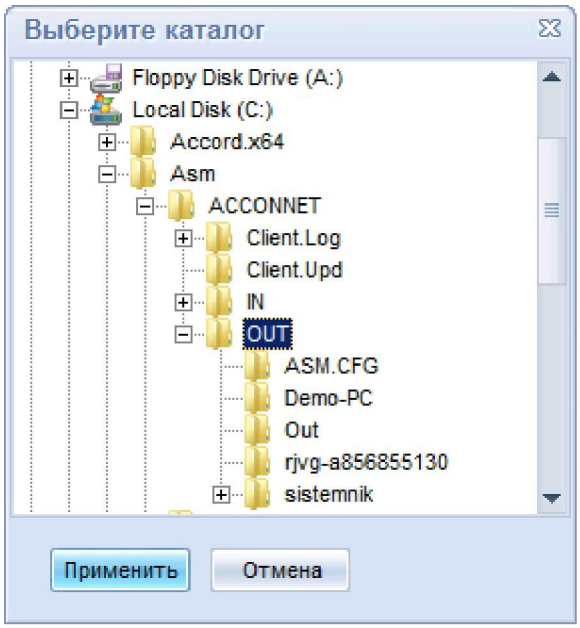

Рисунок 83 - Окно выбора каталога импорта/экспорта настроек журналов

Настройки экспортируются в каталог E:\ASM.CFG, где E – внешний носитель. Следует нажать кнопку <Применить> (рисунок 83). В случае сбоя работы системы можно вернуть первоначальные настройки, используя шаблоны.

Чтобы применить шаблоны настроек журналов, управляемых по децентрализованной схеме, необходимо во вкладке Настройка->Оперативный журнал нажать <Импорт>. После этого на экране появляется окно выбора каталога (рисунок 83). Необходимо выбрать каталог, в котором сохранены шаблоны настроек и нажать кнопку <Применить>. Далее на экране появляется окно выбора типов настроек (рисунок 84), в котором следует выбрать те настройки, которые планируется импортировать и нажать кнопку <Импорт>.

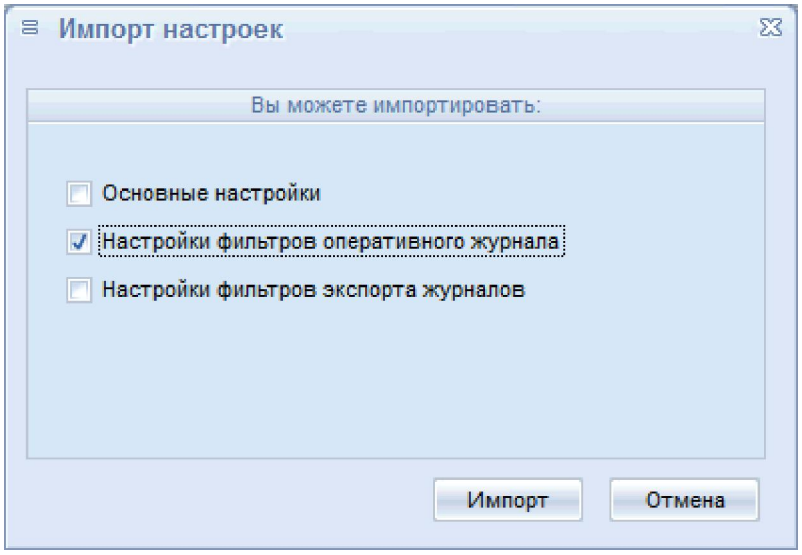

Рисунок 84 – Импорт настроек фильтров оперативного журнала

В качества механизма передачи информации о критичных событиях ИБ используется журнал SYSLOG: ASM помещает полученную от ПКО информацию о

критических событиях в журнал приложения Application ASM сервера централизованного управления. Для этого необходимо установить флаг «Протоколировать оперативные сообщения в SYSLOG» в окне, показанном на рисунке 82.

После выполнения данных настроек информация о критичных событиях информационной безопасности будет записываться в журнал SYSLOG.

Существует возможность произвести настройки, чтобы при возникновении НСД вызывалось какое-либо стороннее приложение. Для этого необходимо указать путь к этому приложению в поле «При возникновении НСД вызывать приложение:» во вкладке Настройка>Оперативный журнал (рисунок 82). В данном случае при возникновении НСД будет вызываться Internet Explorer (рисунок 85).

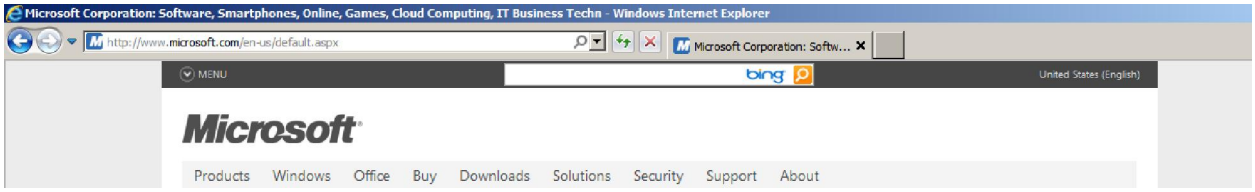

Рисунок 85 - Вызов Internet Explorer при возникновении НСД

4.3.3 Настройка фильтров экспорта журналов

Для настройки взаимодействия фильтров экспорта журналов и ASM следует выбрать вкладку Настройка>Экспорт журналов и установить необходимый флаг в группах «Результат выполнения» для файловых операций и операций с реестром, для сообщений СЗИ, сообщений АМДЗ, расчета КЦ и хранителя экрана (рисунок 86).

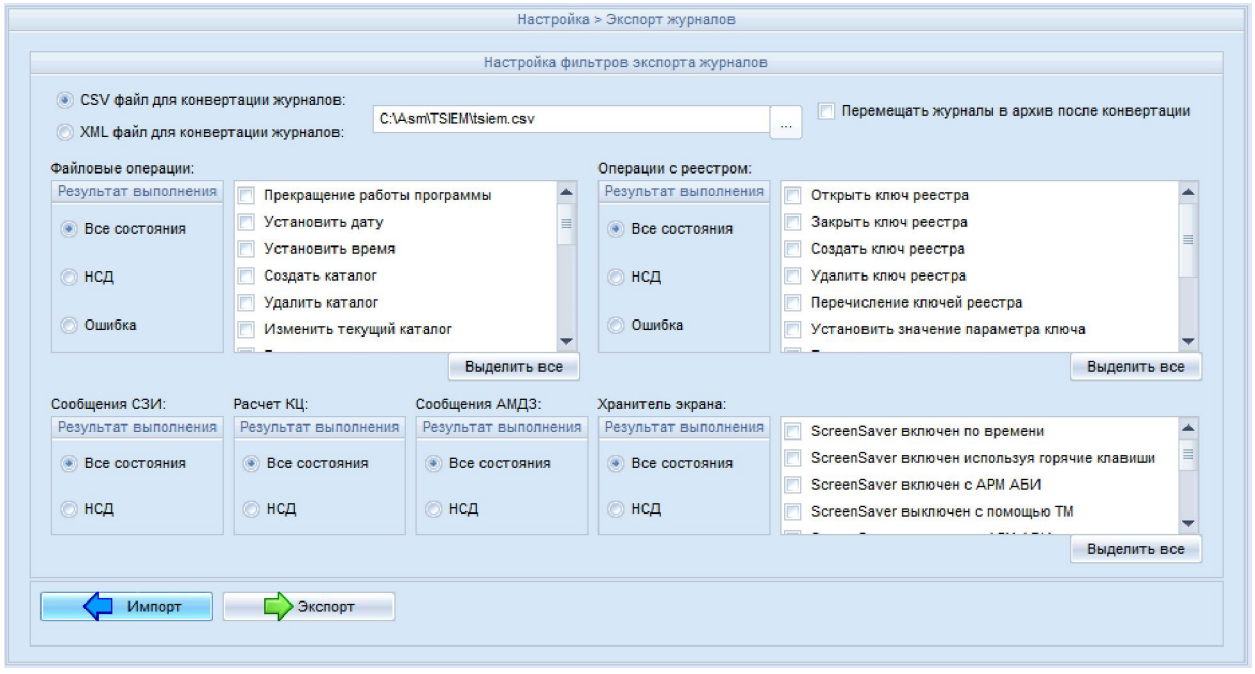

Рисунок 86 – Настройка фильтров экспорта журналов

Для формирования шаблонов настроек, с которыми отсутствует сетевое соединение, по децентрализованной схеме Администратор ИБ ТУ может выбрать нужные настройки (рисунок 87), экспортировать их (посредством кнопки <Экспорт> во вкладке Настройка->Экспорт журналов) на внешний носитель, в качестве которого может использоваться USB флэш-накопитель или флоппи-диск.

По нажатии кнопки <Экспорт> на экране появляется окно выбора каталога (рисунок 87).

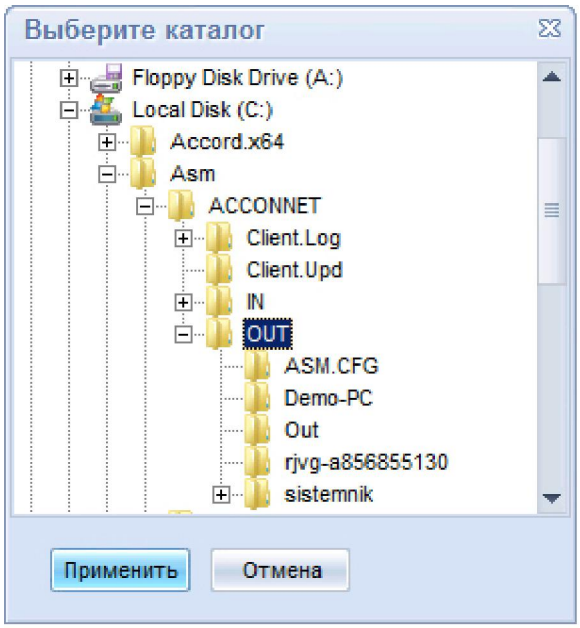

Рисунок 87 - Окно выбора каталога экспорта настроек

Настройки экспортируются в каталог E:\ASM.CFG, где E – внешний носитель. Следует нажать кнопку <Применить> (рисунок 87). В случае сбоя работы системы можно вернуть первоначальные настройки, используя шаблоны.

Чтобы применить шаблоны настроек, сформированных по децентрализованной схеме, необходимо во вкладке Настройка->Экспорт журналов нажать кнопку <Импорт>. После этого на экране появляется окно выбора каталога (рисунок 87). Необходимо выбрать каталог, в котором сохранены шаблоны настроек и нажать кнопку <Применить>.

Далее на экране появляется окно выбора типов настроек (рисунок 88), в котором следует выбрать те настройки, которые планируется импортировать и нажать кнопку <Импорт>.

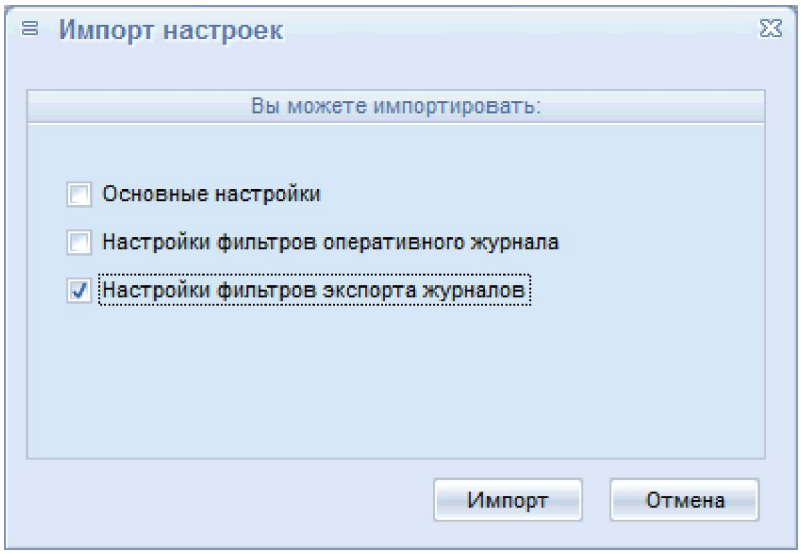

Рисунок 88 – Импорт настроек фильтров экспорта журналов

5 Описание межсегментного обмена

В некоторых случаях существует потребность в использовании сервера централизованного управления в рамках нескольких сегментов сети, отделенных друг от друга с помощью межсетевых экранов. При этом возникает потребность в информационном обмене между сегментами.

Средствами СУЦУ обеспечивается возможность организации межсегментного обмена. Для этого необходимо выполнить корректировку настроек сетевого оборудования – необходимо открыть следующие порты:

UDP: 17767 (0x4567) – порт на подконтрольных объектах (для процесса AcWs32.exe или, в случае работы с ОС Windows Vista и выше, – AcWs32nt.exe);

UDP: 17768 (0x4568), 17769 (0x4569), 17776 (0x4570) – порты на сервере централизованного управления (для процесса AcConnet.exe);

TCP/IP: 28997 (0x7145) – порт на сервере централизованного управления и подконтрольных объектах.

Начиная с версий 2.33.0.26 для серверного ПО и 2.4.3.28 для клиентов подконтрольных объектов, имеется возможность передачи данных посредством использования протоколов TCP/IP.

Для передачи данных на сервер централизованного управления необходимо в файле «AcCon32.ini» установить параметр «ServerUseTcp=Yes». Для передачи данных на подконтрольные объекты необходимо в файле «AcCon32.ini» установить параметр «ClientUseTcp=Yes».

В состав подконтрольных объектов также могут входить АРМ и серверы, размещенные в изолированном сегменте сети и функционирующие, таким образом, по децентрализованной схеме (не имеют сетевого взаимодействия с АРМ АБИ).

Информационный обмен между сегментами сети в рамках децентрализованной схемы осуществляется посредством внешнего носителя информации: данные об учетных записях пользователей ПКО одного сегмента сети экспортируются на внешний носитель (подраздел 4.1.4). Затем список на внешнем носителе должен быть доставлен на ПКО другого сегмента сети.

На ПКО соответствующего сегмента данные об учетных записях пользователей необходимо импортировать с внешнего носителя (подраздел 4.1.5).

6 Сообщения программных средств комплекса и порядок действий по ним

При работе на СВТ, оснащенном комплексом «Аккорд» и ASM, могут возникать ситуации, при появлении которых комплекс выдает сообщения. Выводимые на экран монитора сообщения, причины их появления и методы их устранения приведены в таблице 1.

Таблица 1 – Сообщения программных средств комплекса и методы их устранения

Сообщение на экране	Причины появления сообщения	Порядок действий
«Ошибка чтения ТМ…» (на красном фоне)	ТМ-идентификатор был неправильно прислонен к съемнику информации.	Снова приложить ТМ-идентификатор к съемнику информации после появления соответствующего запроса.
«Это не сетевой ТМ»	Прислонен неверный ТМ-идентификатор	Прислонить правильный ТМ-идентификатор
«В данное время вход в систему запрещен»	Для данного пользователя не разрешен вход в систему в данное время	Вызвать Администратора ИБ и уточнить разрешенное время работы
«Ваш пароль просрочен. Обратитесь к Администратору для смены» (на красном фоне)	Окончилось время жизни пароля. Закончились все попытки смены пароля.	Вызвать Администратора ИБ. Изменить параметры пароля.
«Доступ не разрешен!» (на красном фоне)	Не зарегистрированный идентификатор. Не правильно введен пароль. В данное время работают временные ограничения.	Обратиться к Администратору ИБ для регистрации. Повторить процедуры идентификации / аутентификации.
«Требуется Администратор» (на красном фоне) «Разберитесь с ошибками» (на оранжевом фоне)	Несовпадение контрольных и текущих параметров аппаратной и программной частей системы.	Вызвать Администратора ИБ. Выявить и устранить причины изменения параметров.
«Такую комбинацию символов недопустимо использовать в качестве пароля»	Это сообщение появляется в случае, если пользователь вводит комбинацию символов, которую легко подобрать (например, qwerty).	Ввести более сложную комбинацию символов.
«Отсутствует разрешение на смену пароля»	Это сообщение появляется, если у пользователя нет прав на смену пароля.	Попросить Администратора дать пользователю права на самостоятельную смену пароля.
«В идентификаторе нет свободных страниц для записи»	Объем идентификатора DS1996 позволяет хранить данные о 31 рабочей станции и их открытые ключи. Если Вы уже зарегистрировали 31 станцию, то при попытке зарегистрировать следующую выдается сообщение	Если в сети остались незарегистрированные станции, то следует добавить список на АРМ АИБ и после очистки памяти ТМ провести регистрацию остальных рабочих станций.

7 Сообщения программных средств подконтрольных объектов

Сообщения на экране	Описание сообщений
События работы с реестром	
RegOpenKey	Открыть ключ реестра
RegCloseKey	Закрыть ключ реестра
RegCreateKey	Создать ключ реестра
RegDeleteKey	Удалить ключ реестра
RegEnumKey	Перечисление ключей реестра
RegSetValue	Установить значение параметра ключа
RegQueryValue	Прочитать значение параметра ключа
RegDeleteValue	Удалить параметр ключа
RegCreateValue	Создать параметр ключа
RegEnumValue	Перечисление параметров ключа
События работы со скрин-сейвером	
SSOnTime	ScreenSaver включен по времени
SSOnKey	ScreenSaver включен используя горячие клавиши
SSOnRemote	ScreenSaver включен внешней программой
SSOffTM	ScreenSaver выключен с помощью ТМ
SSOffRemote	ScreenSaver выключен с АРМ АБИ
SOffTMRemote	ScreenSaver выключен с помощью ТМ АБИ
SSTimeOff	Выключен временной контроль ScreenSaver-а
SSTimeOn	Включен временной контроль ScreenSaver-а
SSBadTM	Попытка разблокировать чужим ТМ
События контроля объектов	
StartCheck	Начало проверки списка объектов
EndCheck	Завершение проверки списка объектов
StartUpdate	Начало обновления списка объектов
EndUpdate	Завершение обновления списка объектов
TotalHash	Хэш списка объектов
TotalEDS	Подпись списка объектов
GetPrivateKey	Получение секретного ключа
FileCheck	Проверка объекта
События типа «РМ»	
Term00	Прекращение работы программы
SetDate	Установить дату
SetTime	Установить время
MkDir	Создать каталог
RmDir	Удалить каталог
ChDir	Изменить текущий каталог
RenameDir	Переименовать каталог
CreateFile	Создать файл
OpenFileR	Открыть файл на чтение
OpenFileW	Открыть файл на запись
OpenFileRW	Открыть файл на чтение/запись
CloseFile	Закрыть файл
DeleteFile	Удалить файл
ChMod	Установить атрибуты файла
Exec	Запуск программы
Exit	Выход из программы
FindFirst	Найти первый файл
FindNext	Найти следующий файл
RenameFile	Переименовать файл
Traverse	Проверка существования пути

8 Перечень принятых сокращений

АБИ	Администратор безопасности информации (то же, что АИБ)
АИБ	Администратор информационной безопасности (то же, что АИБ)
АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
ИБ	Информационная безопасность
ИС	Информационная система
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
НШР	Нештатный режим
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПКО	Подконтрольный объект
ПО	Программное обеспечение
СВТ	Средства вычислительной техники
СЗИ	Средство защиты информации
СУЦУ	Система централизованного управления
СУ	Система управления
ASM	Accord Security Management

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Изм.	Номера листов (страниц)				Всего листов (стр.) в документе	№ документа	Входящий № сопроводительного документа	Подпись	Дата
	измененных	замененных	новых	аннулированных					

СОГЛАСОВАНО

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