

**СПЕЦИАЛЬНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ
НЕСАНКЦИОНИРОВАННОГО ДОСТУПА
«АККОРД-РАУ»**

Руководство Администратора информационной безопасности

Листов 182

Москва

2022

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, связанные с непосредственной эксплуатацией системы информационной безопасности (далее – система) в штатном режиме функционирования.

СОДЕРЖАНИЕ

1 Введение	5
1.1 Область применения	5
1.2 Функции Администратора ИБ РАУ	5
1.3 Комплект поставки	5
2 Назначение и условия применения.....	7
2.1 Назначение	7
2.2 Условия применения	7
3 Планирование работы и эксплуатация «Аккорд-РАУ»	8
3.1 Общие сведения	8
3.2 Изменение настроек средств защиты информации	9
3.3 Предварительная настройка сетевого идентификатора	10
3.4 Оперативное наблюдение за работой пользователей	11
3.5 Оперативное управление работой пользователей	11
3.6 Предварительная синхронизация базы на сервере централизованного управления с локальными базами пользователей ПКО 12	
4 Работа с сервером централизованного управления	14
4.1 Общие принципы управления	14
4.2 Вкладка «Пользователи»	14
4.3 Вкладка «Роли»	17
4.4 Вкладка «Тех. участки»	34
4.4.1 Общие сведения	34
4.4.2 Создание технологического участка	35
4.4.3 Изменение параметров технологического участка	38
4.4.4 Удаление технологического участка	40
4.5 Вкладка «Идентификаторы»	41

4.6 Вкладка «Компьютеры»	45
4.7 Вкладка «Учётные записи»	69
4.8 Работа с журналами.....	83
4.8.1 Общие сведения.....	83
4.8.2 Оперативный журнал	84
4.8.3 Журнал ASM	91
4.8.4 Журнал APM АБИ.....	93
4.9 Настройка ASM	95
4.9.1 Основные настройки	95
4.9.2 Настройка фильтров оперативного журнала	97
4.9.3 Настройка фильтров экспорта журналов	102
5 Перечень оповещающих сообщений	103
6 Перечень сообщений журнала ASM	108
7 Перечень сообщений ПАК «Аккорд» на подконтрольных объектах.....	161
8 Перечень сообщений журнала APM АБИ	165
9 Файлы конфигурации	174
9.1 Файл конфигурации ASM.INI.....	174
9.2 Файл конфигурации AcCon32.ini.....	175
9.3 Файл конфигурации AcWs32.ini	176
9.4 Файл конфигурации rabbitmq.config	178
10 Перечень принятых сокращений.....	180

1 Введение

1.1 Область применения

Деятельность Администратора информационной безопасности ИБ (далее – Администратора ИБ) РАУ.

1.2 Функции Администратора ИБ РАУ

Администратор ИБ РАУ

- производит следующие настройки:
 - настройка политик безопасности;
 - настройка правил доступа к коммутационным портам и периферийным устройствам;
- осуществляет контроль управляющего воздействия на компоненты РАУ в части:
 - изменения настроек (включая настройки мониторинга);
 - применения шаблонов настроек;
- управляет учетными записями персонала РАУ, включая назначение пользователей, выполняющих роли персонала РАУ;
- формирует логические группы из серверов и рабочих станций (технологические участки) с применением групповых политик для управления установленных на них СЗИ от НСД «Аккорд»;
- 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 (далее – 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»

3.1 Общие сведения

Планирование применения СЗИ от НСД «Аккорд» осуществляется на этапе общего планирования системы информационной безопасности. Содержание этого этапа заключается в составлении плана защиты. Обычно план защиты – это документ, в который входят данные о характере и составе обрабатываемой информации, составе технических и программных средств, возможных угрозах и способах их реализации, и соответственно описание выбранных методов и средств защиты от этих угроз.

Для настройки СЗИ от НСД «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 СЗИ от НСД «Аккорд» и поддержания уровня защищенности необходимы:

- физическая охрана всех компонентов автоматизированной системы обработки информации, в т. ч. обеспечение мер по не извлечению 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 РАУ получили юридическую основу.

При эксплуатации комплекса Администратор ИБ РАУ 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;

- проводит оперативное наблюдение за работой пользователей;

- обеспечивает оперативное управление работой пользователей.

3.2 Изменение настроек средств защиты информации

Администратор ИБ РАУ может изменять настройки его серверной части для подключения новых подконтрольных объектов, создания и изменения политик безопасности и правил контроля доступа.

Он также формирует шаблоны настроек для СЗИ от НСД «Аккорд», управляемых по децентрализованной схеме.

3.3 Предварительная настройка сетевого идентификатора

Администратор ИБ РАУ выполняет процедуру создания сетевого идентификатора, для чего осуществляет следующие действия:

- запускает ПО СЦУ (Пуск -> Программы -> ASM -> Запуск РАУ);
- предъявляет идентификатор Администратора ИБ;
- открывает вкладку Настройка > Основные настройки. На экран выводится окно, приведённое на рисунке 1;
- в поле «Учетная запись ASM» (рисунок 1) нажимает кнопку <Настройка>, затем предъявляет сетевой идентификатор. На сетевом идентификаторе создается учетная запись «ASM_ACCOUNT» и становится возможным выполнение процедур удаленного управления ПКО: добавление, удаление пользователей, смена пароля пользователя и т. д.

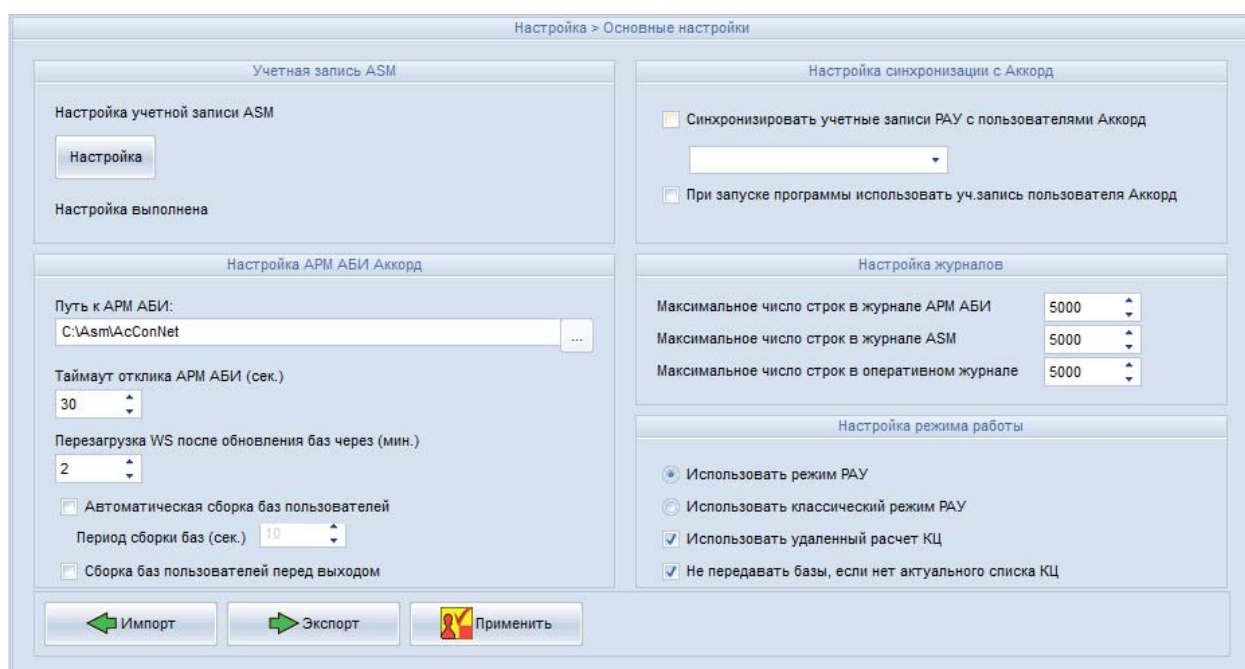


Рисунок 1 – Предварительная настройка сетевого идентификатора

После выполнения данных действий на экране появляется окно, содержащее сообщение об успешном завершении процедуры создания ключа идентификации, приведенное на рисунке 2, и в поле «Учетная запись ASM» статус «Настройка не выполнена» изменяется на «Настройка выполнена».

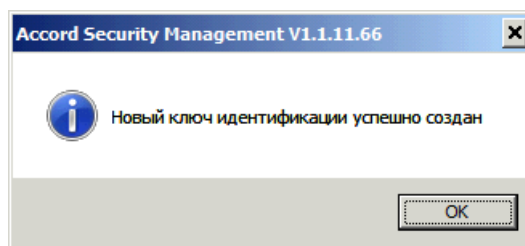


Рисунок 2 – Сообщение об успешном выполнении создания ключа идентификации

Дальнейшую работу с сетевым идентификатором выполняет Администратор РАУ согласно описанию в документе 11443195.4012-053 90 «СПО СЗИ НСД «Аккорд-РАУ». Руководство Администратора».

3.4 Оперативное наблюдение за работой пользователей

Администратор ИБ РАУ имеет возможность наблюдать за пользователями, работающими под контролем ПАК СЗИ от НСД «Аккорд» в составе ЛВС. В любой момент времени Администратор ИБ РАУ может получить информацию о том, кто работает на данной станции, версию операционной системы, под управлением которой идет работа, список задач, которые выполняются на этой станции в текущий момент времени.

Кроме того, СЦУ получает журналы регистрации от ПАК СЗИ от НСД «Аккорд» подконтрольных объектов в режиме реального времени, то есть все попытки НСД тут же отображаются на экране СЦУ.

Администратор ИБ РАУ имеет возможность просматривать все события со всех станций в одном окне.

3.5 Оперативное управление работой пользователей

Администратор ИБ РАУ имеет возможность осуществлять оперативное управление работой пользователей.

В случае возникновения ситуации, когда связь между работающим по централизованной схеме ПКО и Сервером РАУ 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 РАУ 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.

3.6 Предварительная синхронизация базы на сервере централизованного управления с локальными базами пользователей ПКО

После выполнения действий, связанных с установкой и настройкой ASM (установка контроллера «Аккорд-АМДЗ», установка ПО РАУ, регистрация ПКО) необходимо выполнить синхронизацию единой базы пользователей и персонала РАУ с локальными базами пользователей, хранящимися на ПКО. Синхронизация баз пользователей выполняется следующим образом:

- импортирование информации о ПКО в файл ACNODE.LST (регистрация ПКО). Данная операция выполняется Администратором РАУ согласно документу 11443195.4012-053 90 «СПО СЗИ НСД «Аккорд-РАУ». Руководство Администратора»;
- импортирование на СЦУ локальных баз пользователей, хранящихся на ПКО, выполняется Администратором РАУ согласно документу 11443195.4012-053 90 «СПО СЗИ НСД «Аккорд-РАУ». Руководство Администратора»;
- импортирование баз USB-устройств ПКО (создание единой базы «белых» и «черных» USB-устройств). Данная операция выполняется Администратором РАУ согласно документу 11443195.4012-053 90 «СПО СЗИ НСД «Аккорд-РАУ». Руководство Администратора»;
- создание технологических участков (формирование логических групп ПКО). Данная операция выполняется Администратором ИБ в соответствии с пунктом 4.4 настоящего документа;
- создание Администраторов ИБ технологических участков. Данная операция выполняется Администратором ИБ в соответствии с пунктом 4.2 настоящего документа;
- импортирование учётных записей пользователей ПКО (формирование единой базы учётных записей персонала и пользователей ПКО). Данная операция выполняется Администратором ИБ технологического участка в соответствии с документом 11443195.4012 053 92 «СПО СЗИ НСД «Аккорд-РАУ». Руководство Администратора ИБ СЗИ НСД (АИБ технологического участка)»;
- назначение учётных записей пользователям ПКО. Данная операция выполняется Администратором ИБ технологического участка в соответствии с

документом 11443195.4012 053 92 «СПО СЗИ НСД «Аккорд-РАУ». Руководство Администратора ИБ СЗИ НСД (АИБ технологического участка)»;

- передача скорректированной базы пользователей на ПКО. Данная операция выполняется Администратором ИБ технологического участка в соответствии с документом 11443195.4012 053 92 «СПО СЗИ НСД «Аккорд-РАУ». Руководство Администратора ИБ СЗИ НСД (АИБ технологического участка)».

Синхронизация баз пользователей в рамках децентрализованной схемы сводится к получению информации о пользователях ПКО при импортировании списка в единую базу пользователей на сервере централизованного управления или к передаче обновленных файлов на ПКО посредством транспортировки на внешних носителях.

4 Работа с сервером централизованного управления

4.1 Общие принципы управления

Пользовательский интерфейс ПО СЦУ 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 - 4.9 описывается пользовательский интерфейс СЦУ, доступный администратору ИБ для выполнения его обязанностей.

4.2 Вкладка «Пользователи»

Вкладка Управление > Пользователи системы, приведена на рисунке 3.

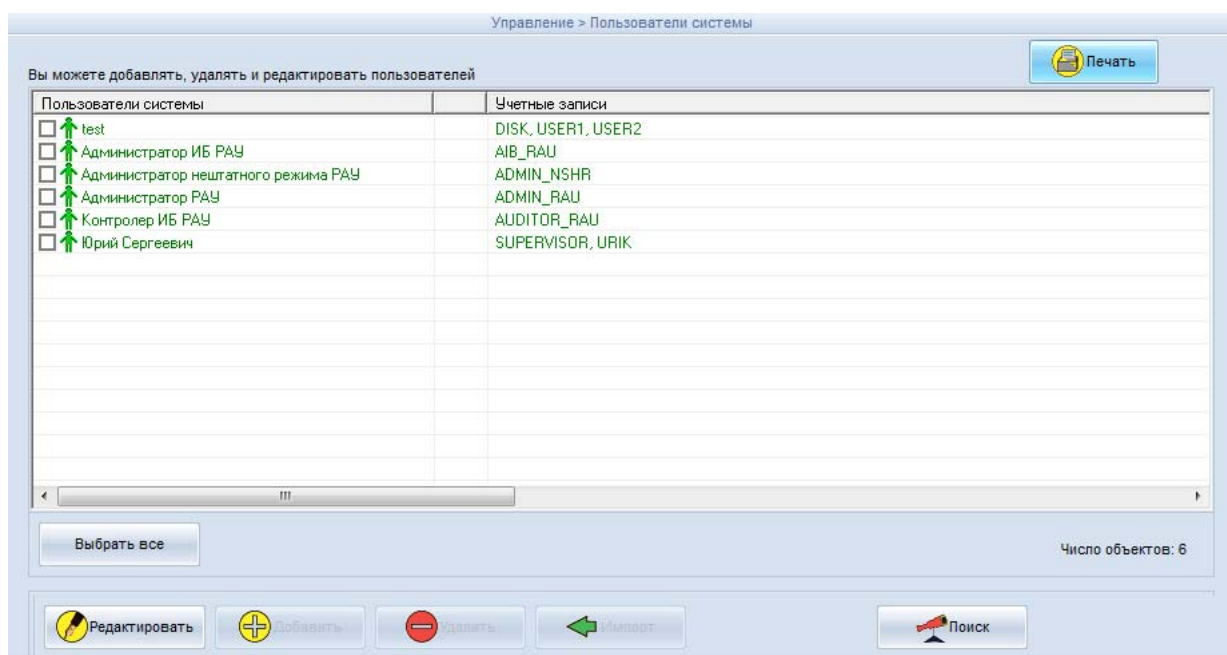


Рисунок 3 - Вкладка Управление > Пользователи системы

Данная вкладка позволяет Администратору ИБ осуществлять процедуры просмотра списка пользователей, печати информации о пользователях, поиска пользователей по идентификатору и просмотра параметров пользователей.

Если необходимо определить, какому пользователю принадлежит данный идентификатор, следует нажать кнопку <Поиск> во вкладке «Пользователи системы». Появится сообщение «Введите идентификатор». Если предъявленный идентификатор назначен какому-либо пользователю, то этот пользователь будет выделен, как показано на рисунке 4.

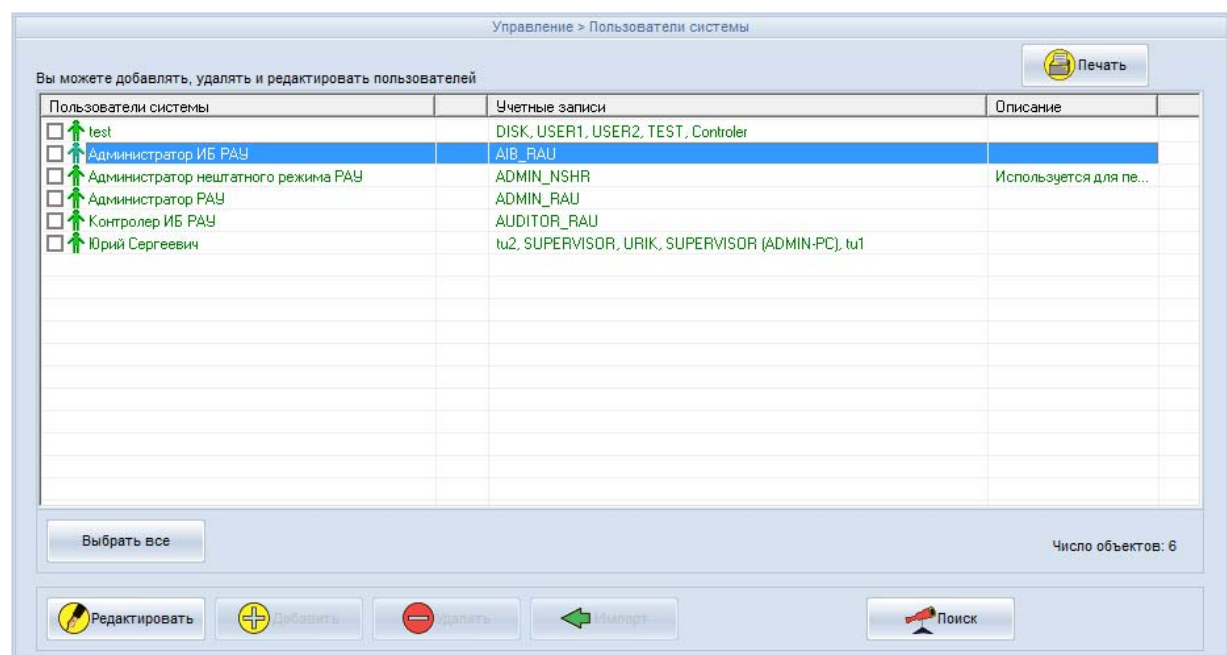


Рисунок 4 - Пользователь, которому назначен идентификатор

Если предъявленный идентификатор не назначен ни одному из пользователей системы, в нижней части окна появится сообщение «Идентификатор не зарегистрирован!», как показано на рисунке 5.

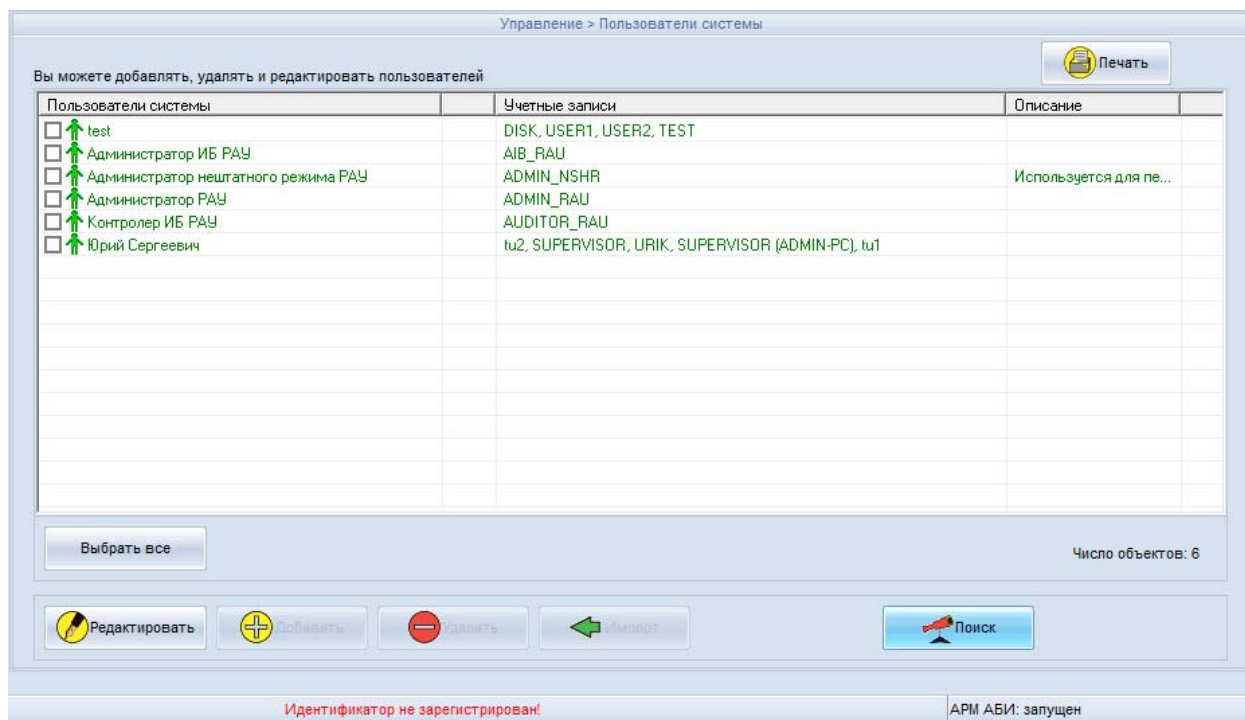


Рисунок 5 - Сообщение о том, что идентификатор не зарегистрирован

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

При ее нажатии выводится окно, приведённое на рисунке 6, в котором нужно выбрать способ печати: в файл или на принтер, тип выводимой информации (имя пользователя, имя назначенной ему учетной записи, описание); при печати в файл следует также указать разделитель.

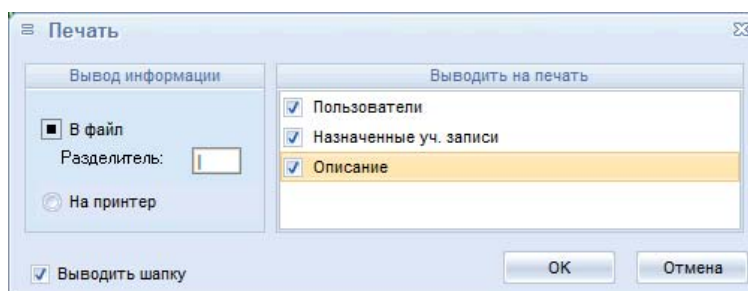


Рисунок 6 - Печать информации о пользователе

Нажатие кнопки <Редактировать> выводит окно, содержащее информацию об учётной записи выбранного пользователя, его логине, роли, настройках ПКО, на котором он работает, и имени компьютера. Изменять эту информацию АИБ технологического участка не может.

4.3 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 роли¹:

- **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;
- **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 «Аккорд-РАУ»;
- **AIB_TU: имя роли** – роль, под которой работает Администратор ИБ технологического, 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:

¹ Назначение роли возможно только на ПКО под управлением ОС Windows

- 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, приведённой на рисунке 7, указано, является ли данная роль базовой или подчинённой. В случае если роль является базовой, то данный столбец не заполняется. В случае если роль является подчинённой, то в данном столбце приводится информация, от какой базовой роли унаследована данная роль.

Управление > Роли системы

Вы можете добавлять, удалять и редактировать роли

Имя роли	ПКО	Описание роли	Участки	Зависит от ро
☐ ADMINS	—	Встроенная роль: Администраторы Аккорд	Вся система	
☐ ADMINS_1	—	Встроенная роль: Администраторы Аккорд	tu1	
☐ ADMINS_2	—	Встроенная роль: Администраторы Аккорд	tu2_virtual	
☐ ADMINs_RAУ	—	Встроенная роль: Администратор РАУ	Вся система	
☐ AIBs_RAУ	—	Встроенная роль: Администратор ИБ РАУ	Вся система	
☐ AUDITORs_RAУ	—	Встроенная роль: Контролер ИБ РАУ	Вся система	
☐ EVERYONE	—	Встроенная роль: Пользователи Аккорд	Вся система	
☐ EVERYONE_1	—	Встроенная роль: Пользователи Аккорд	tu1	
☐ EVERYONE_2	—	Встроенная роль: Пользователи Аккорд	tu2_virtual	
☐ OIBs_RAУ	—	Встроенная роль: Оператор ИБ РАУ	Вся система	

Выбрать все

Число объектов: 10

Редактировать Добавить Удалить

Рисунок 7 - 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 7, будет выведено окно добавления роли, приведённое на рисунке 8.

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.

The screenshot shows a window titled 'Управление > Роли системы > Добавить'. It contains three input fields at the top: 'Имя роли:' with the text 'NewRole', 'Описание', and 'Участок к которому относится роль'. Below these is a section titled 'Привилегии роли'. Inside this section, there is a sub-section 'Тех. участок' containing a checkbox 'Роль АИБ ТУ РАУ', a dropdown menu 'Роль управляет тех. участками:', and a checked checkbox 'Подчинённая роль. Зависит от базовой роли:' with a dropdown menu showing 'EVERYONE'. At the bottom left of the 'Привилегии роли' section is a button with a red icon and the text 'Добавить'. At the bottom left of the entire window is a button with a blue arrow and the text 'Назад'.

Рисунок 8 - Добавление роли

При создании роли по шаблону необходимо в окне добавления роли, приведённом на рисунке 8, левой кнопкой мыши выбрать раскрывающийся список в поле «Имя роли». Появится окно, приведённое на рисунке 9, в котором необходимо выбрать роль и нажать кнопку <Ok>.

The screenshot shows a dialog box titled 'Создать новую роль по шаблону'. It contains a table with two columns: 'Роль' and 'Тех.участок'. The table has several rows, each starting with a green 'OK' icon. The first row is highlighted in blue. At the bottom right of the dialog box are two buttons: 'Ok' and 'Отмена'.

Роль	Тех.участок
OK ADMINS	Вся система
OK ADMINS_1	Тех.участок_1
OK ADMINS_2	Тех.участок_2
OK EVERYONE	Вся система
OK EVERYONE_1	Тех.участок_1
OK EVERYONE_2	Тех.участок_2

Рисунок 9 - Создание роли по шаблону

При редактировании базовой роли на экран выводится окно, приведённое на рисунке 10.

При редактировании базовой роли соответствующим образом будут изменены синхронизируемые параметры зависящих от неё подчинённых ролей. Список подчинённых ролей базовой роли выводится в области «Подчиненные роли» окна, приведённого на рисунке 10. Индикатор в виде лампочки слева от имени роли указывает, что данная подчинённая роль по одной или нескольким группам параметров рассинхронизирована с базовой ролью.

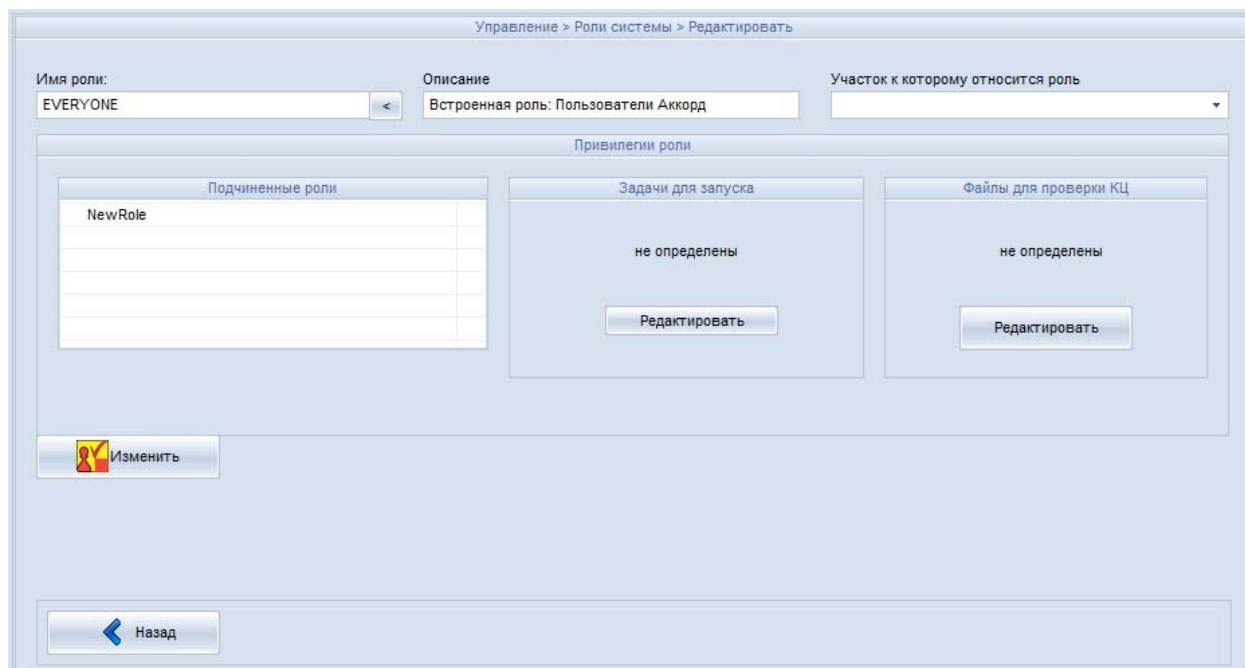


Рисунок 10 - Редактирование базовой роли

Если дважды щёлкнуть мышью по имени роли в списке подчинённых ролей, то будет выведено окно синхронизации, приведённое на рисунке 11.

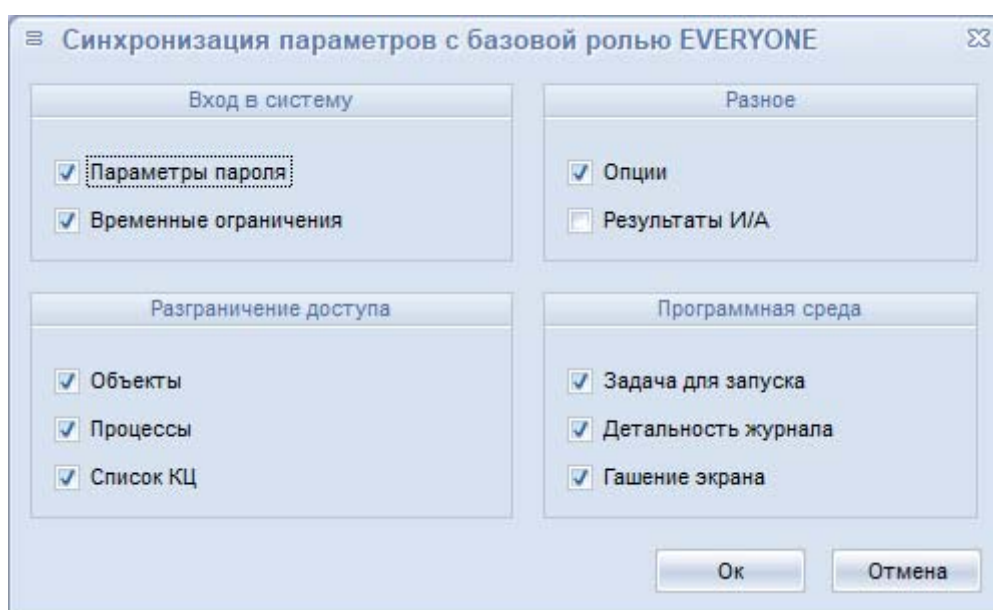


Рисунок 11 - Синхронизация групп параметров

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 данной 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 кнопку <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 12.

The screenshot shows a window titled 'Управление > Роли системы > Редактировать' (Management > System Roles > Edit). It contains the following elements:

- Fields for 'Имя роли:' (Role Name) with the value 'NewRole', 'Описание' (Description), and 'Участок к которому относится роль' (Area to which the role applies).
- A section titled 'Привилегии роли' (Role Privileges) containing two panels: 'Задачи для запуска' (Tasks for execution) with the status 'назначены' (assigned) and 'Файлы для проверки КЦ' (Files for KZ checking) with the status 'не определены' (not defined). Each panel has a 'Редактировать' (Edit) button.
- A checkbox labeled 'Подчиненная роль. Зависит от базовой роли:' (Subordinate role. Depends on the base role:), which is checked. Below it is a dropdown menu showing 'EVERYONE'.
- An 'Изменить' (Change) button with a yellow icon.
- A 'Назад' (Back) button at the bottom left.

Рисунок 12 - 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 нажатии кнопки <Изменить> на экране появляется редактор прав доступа (ACED32.EXE), посредством которого следует при необходимости изменить параметры выбранной подчиненной роли. 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 13.

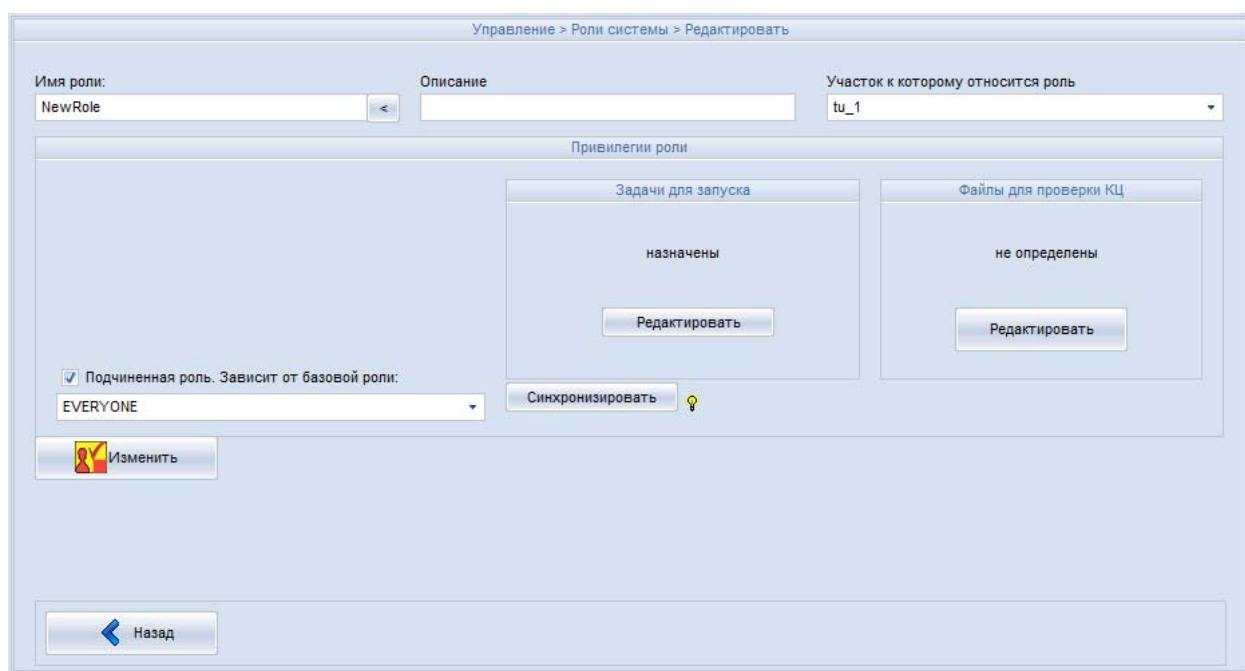


Рисунок 13 - Редактирование подчинённой роли. Рассинхронизация

После нажатия кнопки <Синхронизация> будет выведено окно, приведённое на рисунке 11.

Все встроенные роли ЦЦУ (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 14, в котором нужно задать необходимые задачи для запуска и нажать кнопку <Сохранить> (длина строки окна редактирования списка задач составляет 120 символов).

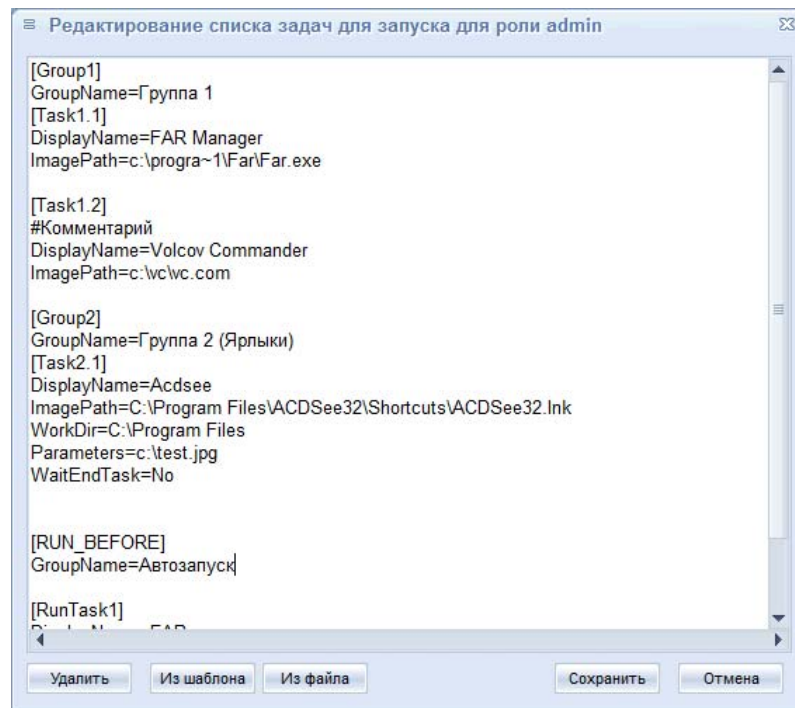


Рисунок 14 – Редактирование списка задач для запуска

При создании списка задач для запуска по шаблону необходимо в окне, приведённом на рисунке 14, нажать кнопку <Из шаблона>. Будет выведено окно, приведённое на рисунке 15.

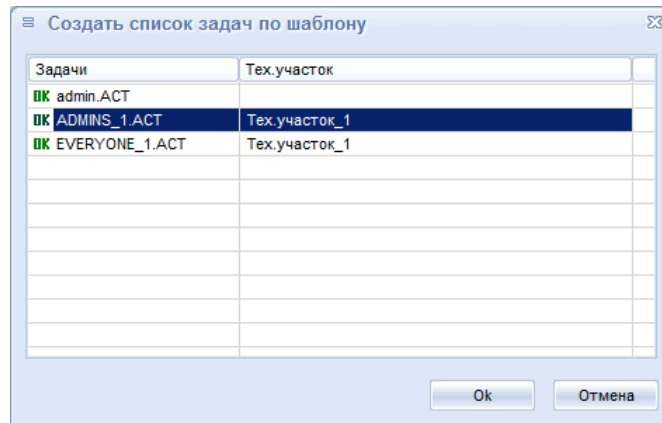


Рисунок 15 – Создание списка задач по шаблону

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>. При ее нажатии появляется окно выбора файла. В появившемся окне необходимо выбрать нужный файл и нажать кнопку <Открыть>.

После внесения изменений необходимо нажать кнопку <Сохранить> (рисунок 14), для отмены операции – кнопку <Отмена> (рисунок 14).

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 4.6.

При удалённом формировании списка контролируемых файлов 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 10 и 12.

При ее нажатии появится окно, примерный вид которого приведён на рисунке 16.

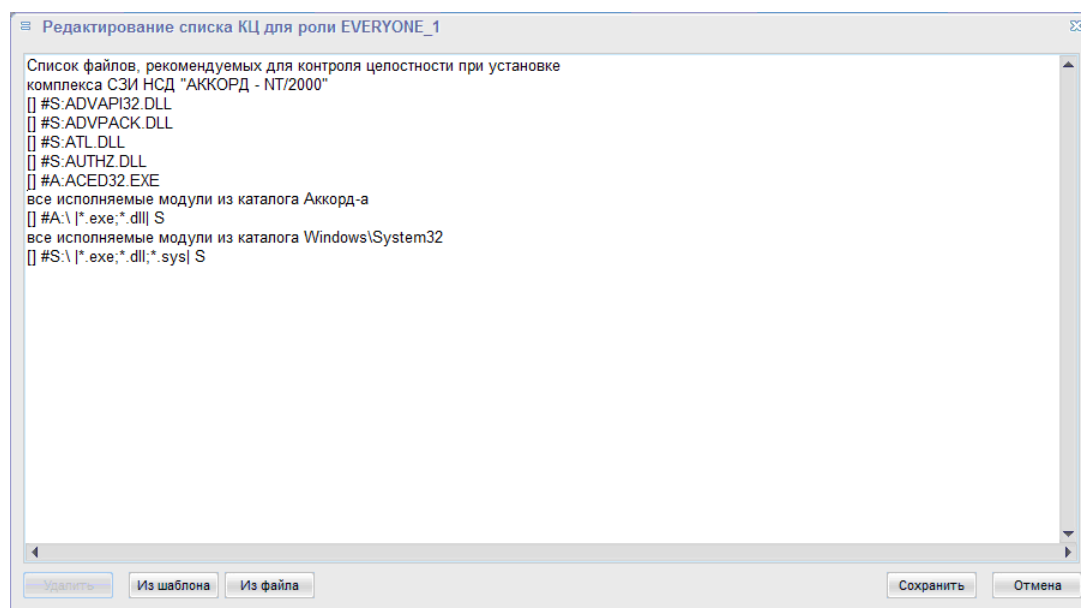


Рисунок 16 - Редактирование списка контролируемых файлов

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 папках 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 «а», библиотек dll, имя кото- рых 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 Win- dows\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 Win- dows\System32

Строка	Описание
☐ 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\
☐ #S:\ a*.exe; file?.dll; *.lo? S	Исключение исполняемых файлов, имя которых начинается на букву «а», 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 16, кнопки <Сохранить> будет выведено сообщение, приведённое на рисунке 17.

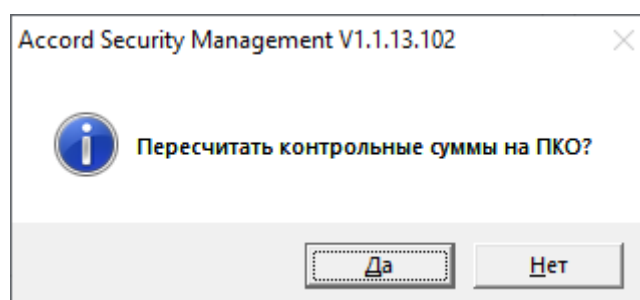


Рисунок 17 - Запрос пересчёта эталонных контрольных сумм

Для передачи задания для контроля целостности на подконтрольные объекты нужно нажать кнопку <Да>. При ее нажатии появится окно, содержащее список ПКО, на которых существует роль, в рамках редактирования которой создаётся

данное задание для контроля целостности. Пример такого окна приведён на рисунке 18.

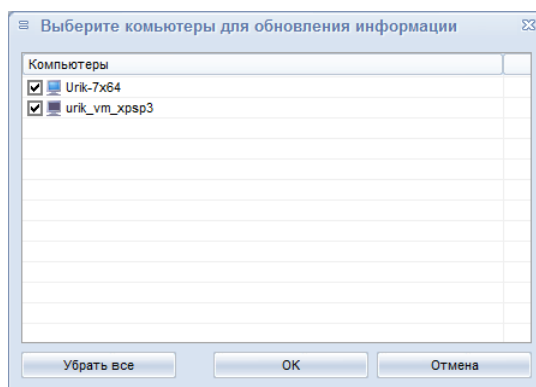


Рисунок 18 - Выбор ПКО для передачи задания для контроля целостности

После выбора нужных ПКО и нажатия <ОК> 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.

Примечания: 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 11.

Получив файл с заданием для контроля целостности, программное обеспечение ПКО выполняет расчёт эталонных контрольных сумм. Данный 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. Этот 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 сокра-

щений 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 с эталонными контрольными суммами;
- RoleName – роль, в рамках редактирования которой формируется список контроля целостности файлов.

После получения файла с эталонными контрольными суммами становится возможным формирование и отправление 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» нужно нажать кнопку <Настройка отображения информации> и в появившемся окне установить флажок «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, возникающие при формировании списка контролируемых файлов, следует в настройках СЦУ установить флажок «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 4.6.

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 с несформированными списками контролируемых файлов маркируются восклицательным знаком красного цвета.

Если нажать кнопку <Изменить> в окне, приведённом на рисунке 10 или рисунке 12, то появится окно редактора прав доступа ACED32, приведённое на рисунке 19. 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).

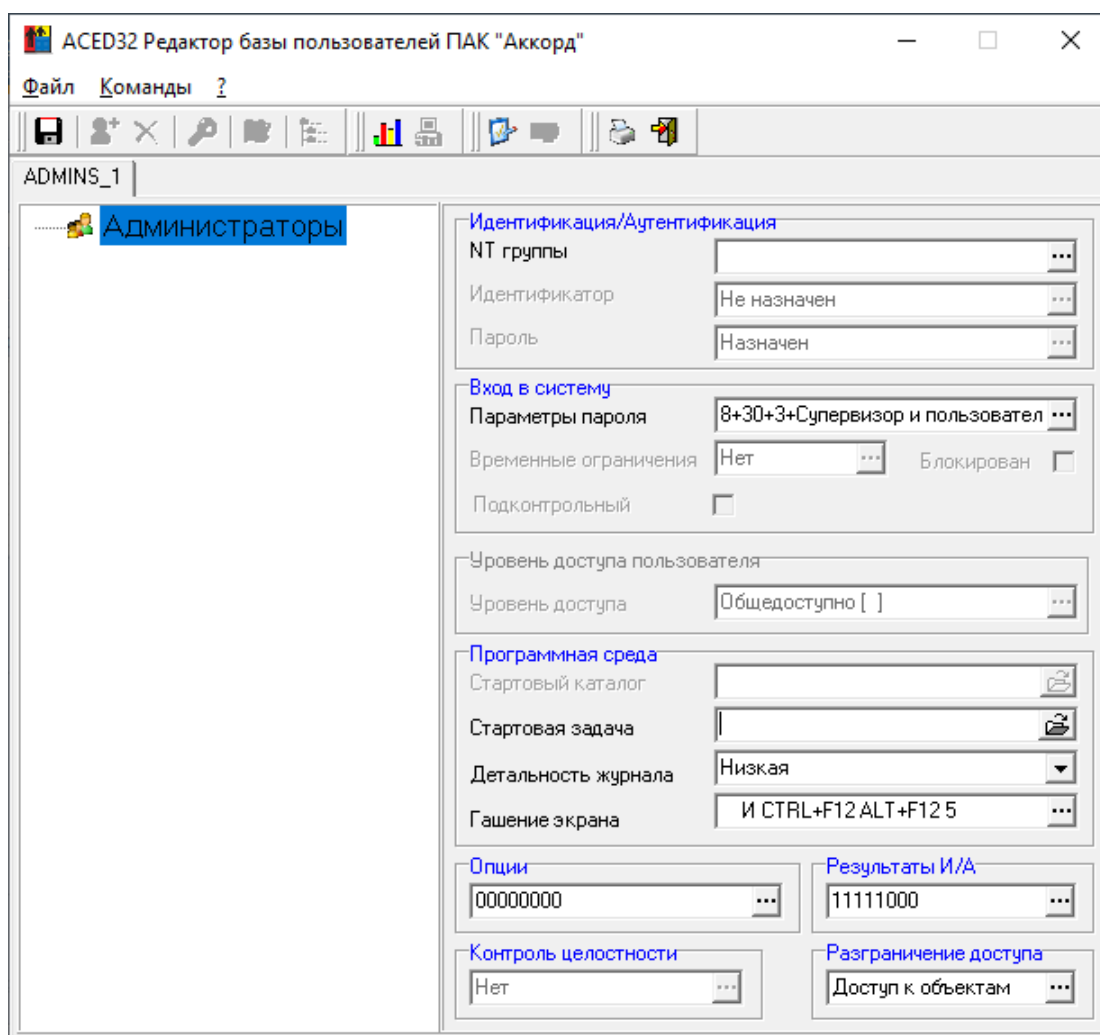


Рисунок 19 – Редактирование базы пользователей «Аккорд»

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

На рисунке 20 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».

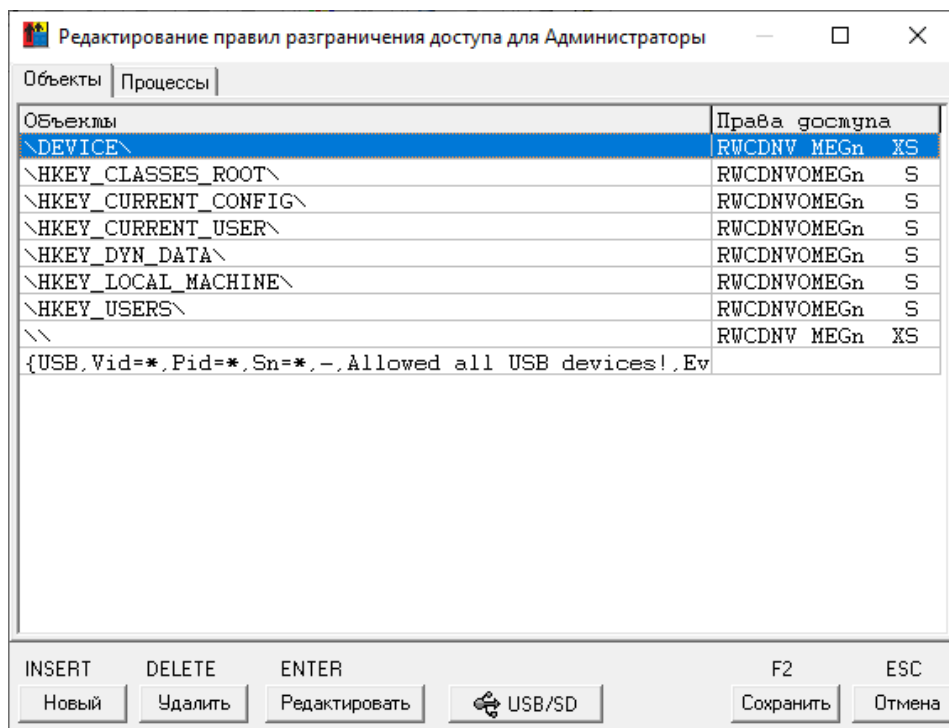


Рисунок 20 – Перечень объектов для установки прав доступа

Уровень детальности журнала ПАК «Аккорд» на ПКО должен быть установлен в значение не ниже уровня «Низкий», как показано на рисунке 19.

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

Для удаления роли необходимо во вкладке «Управление > Роли системы», приведённой на рисунке 7, выбрать роль и нажать кнопку <Удалить>. При ее нажатии появится сообщение, приведённое на рисунке 21.

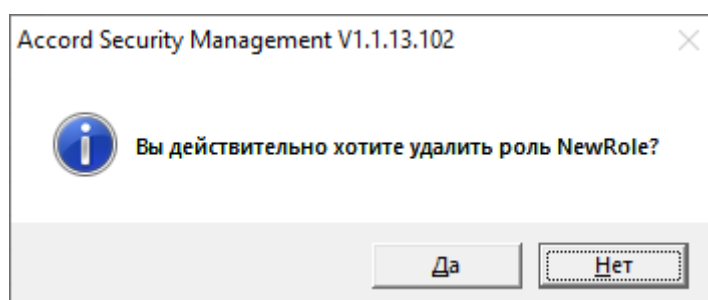


Рисунок 21 – Удаление роли

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

В ПО РАУ предусмотрена возможность автоматического редактирования параметров учётной записи пользователя системы (п.п. 4.7) при выполнении про-

цедуры 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 вывода на принтер информации, приведённой во вкладке «Управление > Роли системы», а также сохранения данной информации в файл нужно нажать кнопку <Печать>. При ее нажатии появится окно, в котором нужно выбрать способ печати: в файл или на принтер, тип выводимой информации (имя роли, настройки ПКО, описание роли, участки); при печати в файл следует также указать разделитель.

Для отображения в списке ролей информации о наличии списков файлов контроля целостности, списков задач (*.act файлов), стартовых задачах нужно нажать кнопку <Настройка отображения информации>. При ее нажатии появится окно, приведённое на рисунке 22, в котором устанавливаются флаги напротив той информации о настройках ПКО, которую нужно отображать.

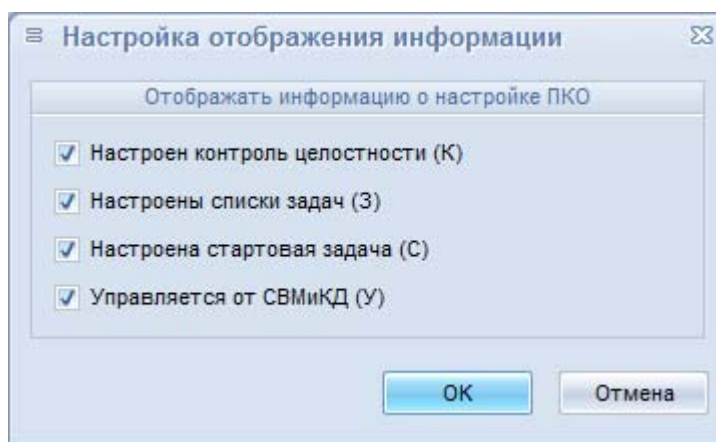


Рисунок 22 - Настройка отображения информации о ПКО

После добавления отображаемой информации в таблице ролей появляется столбец под названием «ПКО», как показано на рисунке 23. 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.

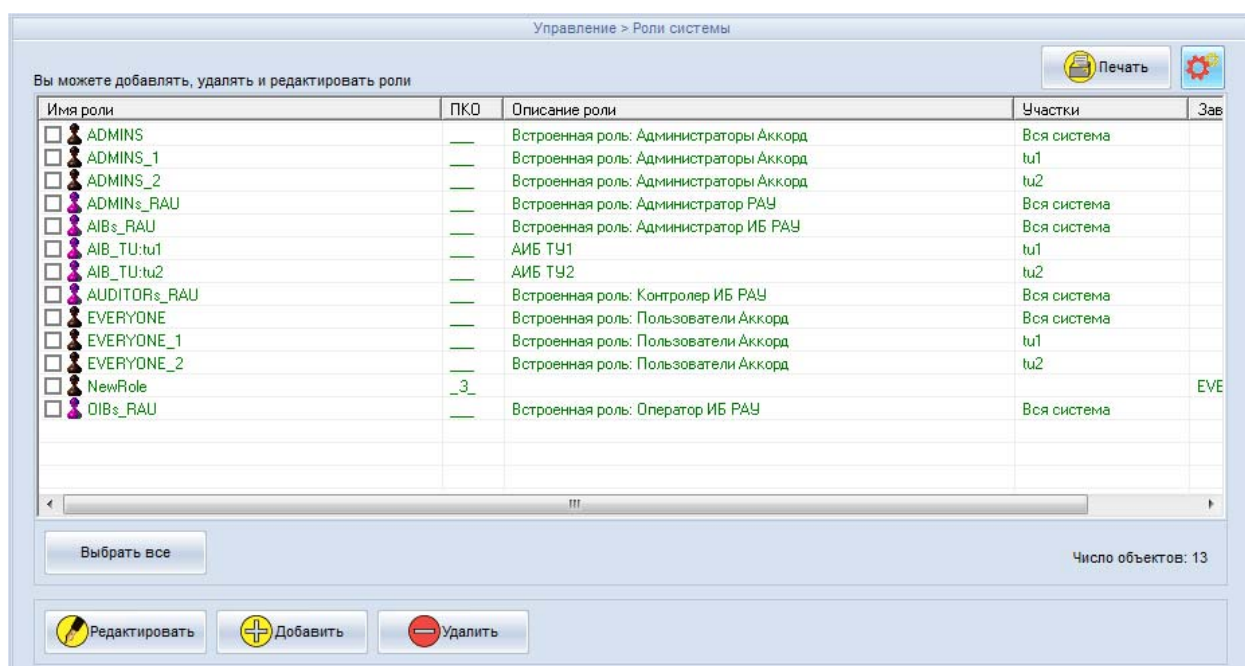


Рисунок 23 – Роли системы. Отображение информации о ПКО

4.4 Вкладка «Тех. участки»

4.4.1 Общие сведения

Для того чтобы работать с технологическими участками, необходимо открыть в ASM вкладку «Управление > Тех. Участки». Появится окно, приведённое на рисунке 24, которое содержит следующие элементы:

- список технологических участков системы (столбец «Название участка»);
- списки компьютеров, входящих в каждый технологический участок (столбец «Компьютеры участка»);
- описание технологического участка (столбец «Описание»);
- значение параметра синхронизации паролей доменных пользователей в ТУ (столбец «СПМТ»). Данный параметр может принимать значения либо «+», либо « ». Подробное описание параметра приведено в пункте 4.4.3;
- кнопка для изменения параметров технологических участков (<Редактировать>);
- кнопка для создания новых технологических участков (<Добавить>);
- кнопка для удаления существующих технологических участков (<Удалить>);

- [illegible]

4.4.2 Создание технологического участка

35

Управление > Технологические участки системы > Добавить

Имя технологического участка:
tu_3

Описание технологического участка

Роли АИБ ТУ управляющие участком:

Настройка

Описание тех.участка

Компьютеры, принадлежащие тех.участку и свободные:

☐ Показывать только назначенные

Компьютеры	Описание компьют...		
☒ Urik-7x64			

 Применить

☐ Синхронизация паролей доменных пользователей в разных ТУ

Назад

Затем следует перейти на вкладку «Компьютеры», выбрать компьютеры, которые должны входить в данный технологический участок, и нажать кнопку <Редактировать>. Далее выбрать из списка, какому технологическому участку должны принадлежать данные компьютеры, и нажать кнопку <Применить> (рисунок 26).

[illegible]

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

Для создания роли Администратора ИБ ТУ после добавления технологического участка необходимо перейти во вкладку «Управление > Роли системы», нажать кнопку <Добавить> и в появившемся окне (рисунок 27) выполнить следующую последовательность действий:

- ввести имя роли;
- в поле «Привилегии роли» установить флаг «Роль АИБ ТУ СЦУ». При этом имя роли изменится на «AIB_TU: имя роли»;
- выбрать технологический участок из списка «Тех. участок»;
- нажать кнопку <Добавить>.

The screenshot shows a web interface for adding a system role. At the top, the breadcrumb is 'Управление > Роли системы > Добавить'. There are three main input areas: 'Имя роли:' with the text 'AIB_TU:tu_1', 'Описание:' which is empty, and 'Участок к которому относится роль' which is a dropdown menu currently showing 'Вся система'. Below these is a section titled 'Привилегии роли'. Inside this section, there is a sub-section 'Тех. участок' containing a checked checkbox for 'Роль АИБ ТУ РАУ'. Below this checkbox is a label 'Роль управляет тех. участками:' followed by a list of checkboxes and labels: 'tu1' (checked), 'tu2' (unchecked), and an empty field. At the bottom left of the main form area is a button with a yellow icon and the text 'Добавить'. At the bottom of the entire window is a 'Назад' button with a blue arrow icon.

Рисунок 27 – Создание Администратора ИБ для технологического участка

Чтобы создать роль Администратора ИБ технологического участка по шаблону, следует выбрать раскрывающийся список в поле «Имя роли» и в появившемся окне со списком шаблонов, приведённом на рисунке 27, выбрать необходимый шаблон.

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

При создании Администратора ИБ СЗИ НСД (АИБ технологического участка) подконтрольного объекта, принадлежащего технологическому участку, в рамках децентрализованной схемы необходимо:

Предоставляется возможность изменения следующих параметров выделенного технологического участка:

- описание технологического участка;
- роли, которые наделяются правами управления данным участком;
- компьютеры, входящие в данный технологический участок;
- параметр синхронизации паролей доменных пользователей.

Параметр синхронизации паролей доменных пользователей в ТУ в зависимости от своего значения включает и выключает следующий режим смены пароля пользователя.

Если данный параметр включён, о чём сигнализирует установленный флажок «Синхронизация паролей доменных пользователей в разных ТУ» или символ «+» в столбце «СПМТ» (смотри п. 4.4.1), то при смене пароля пользователя на ПКО, входящем в состав данного технологического участка, происходит смена паролей всех учётных записей, для которых выполняются оба следующих условия:

- содержащееся в учётной записи полное имя пользователя совпадает с полным именем пользователя учётной записи, для которой выполняется смена пароля. При этом полное имя пользователя содержит хотя бы один из следующих символов: «@» или «\», например: user@okbsap.ru;

- учётная запись относится к компьютеру, входящему в состав технологического участка, параметр синхронизации паролей доменных пользователей которого включён.

Если данный параметр выключен, о чём сигнализирует снятый флажок «Синхронизация паролей доменных пользователей в разных ТУ» или отсутствие каких-либо символов в столбце «СПМТ» (смотри п. 4.4.1), или полное имя пользователя отсутствует, или не содержит ни одного символа «@» или «\», то при смене пароля пользователя на ПКО происходит смена паролей учётных записей, для которых выполняются все следующие условия:

- содержащееся в учётной записи имя пользователя совпадает с именем пользователя учётной записи, для которой выполняется смена пароля;

- относящийся к учётной записи идентификатор совпадает с идентификатором учётной записи, для которой выполняется смена пароля;

Появится окно с запросом подтверждения этого действия, приведённое на рисунке 30.

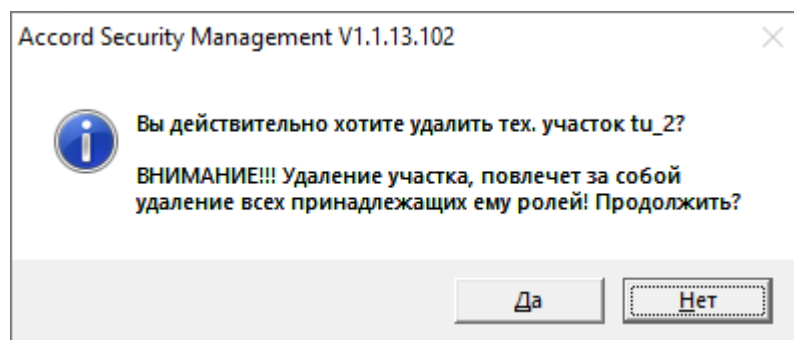


Рисунок 30 – Подтверждение удаления технологического участка

В ПО РАУ предусмотрена возможность автоматического редактирования параметров учётной записи пользователя системы при выполнении процедуры удаления технологического участка. По выполнении этой процедуры роли, которые наделяются правами управления соответствующим участком, автоматически удаляются. При этом в учётных записях, которым назначены данные роли, содержимое поля «Роль:» аннулируется.

4.5 Вкладка «Идентификаторы»

Для того чтобы работать с идентификаторами, следует открыть в ASM вкладку «Управление > Идентификаторы». Появится окно, приведенное на рисунке 31.

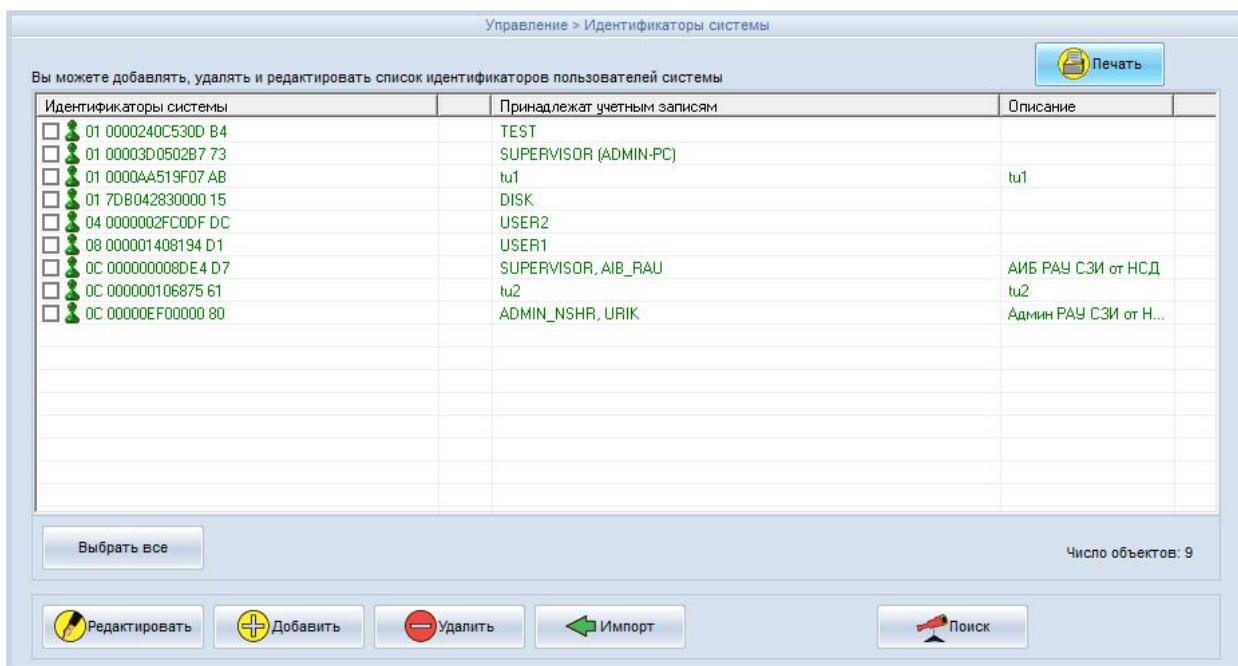


Рисунок 31 – Идентификаторы системы

Кнопка <Печать> позволяет распечатать информацию о выбранных идентификаторах на принтере или сохранить ее в файл (с указываемым разделителем). При ее нажатии появится окно, приведенное на рисунке 32, в котором выбирается, куда нужно вывести информацию: в файл или на принтер, какую информацию о выбранных идентификаторах нужно распечатать (серийный номер идентификатора, принадлежность учетным записям и описание). При печати в файл кроме этого нужно задать разделитель выводимых полей.

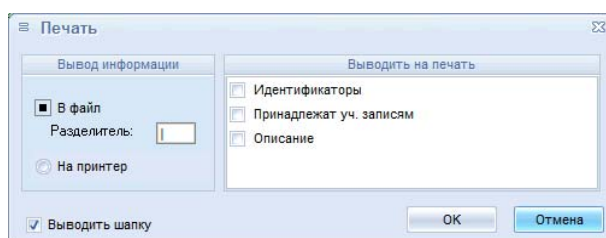


Рисунок 32 – Печать информации об идентификаторе

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 33).

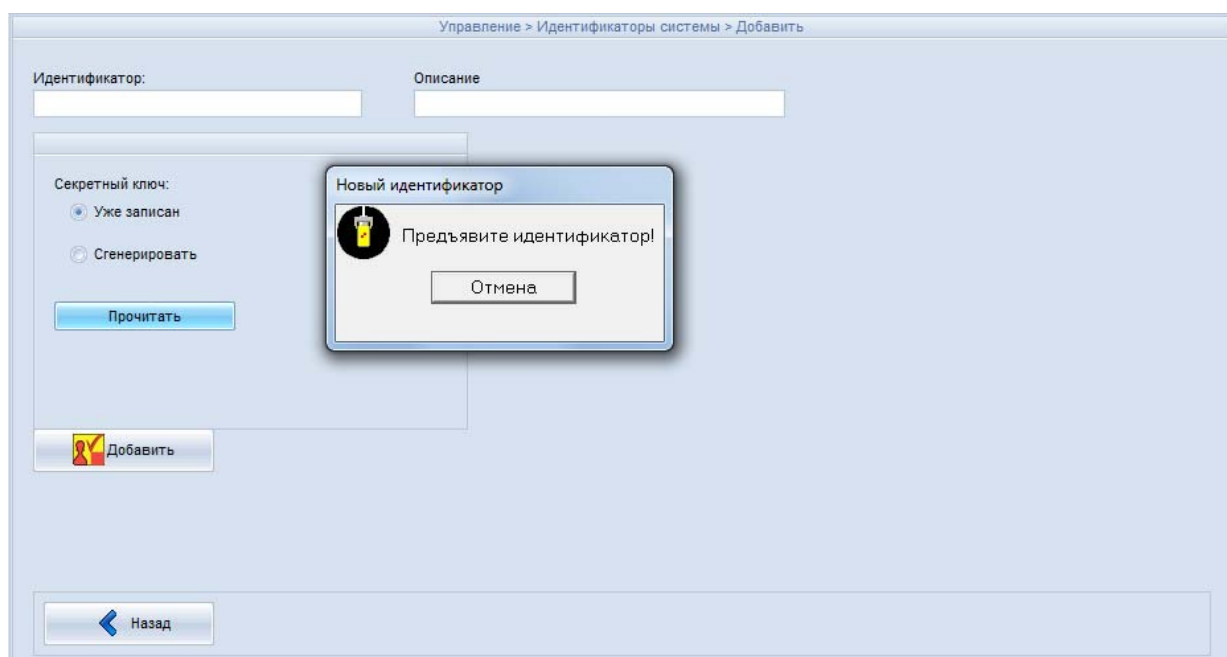


Рисунок 33 – Требование предъявить идентификатор

Для добавления идентификатора в базу необходимо нажать кнопку <Добавить>.

Чтобы удалить идентификатор, необходимо во вкладке «Идентификаторы» (рисунок 31) выбрать нужный идентификатор и нажать кнопку <Удалить>. При ее

нажатии появится сообщение о подтверждении действия, приведенное на рисунке 34.

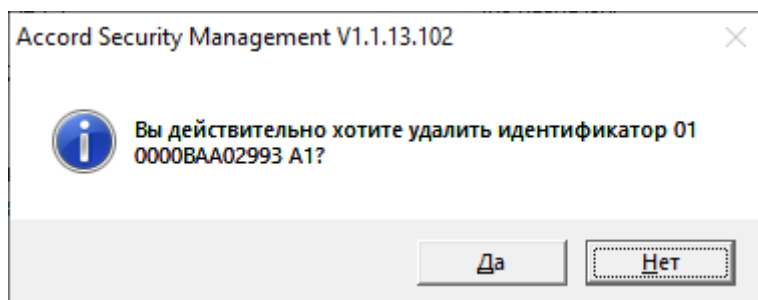


Рисунок 34 – Подтверждение удаления идентификатора

Идентификаторы можно импортировать из базы СЗИ от НСД «Аккорд» (например C:\Accord.NT\ ACCORD.AMZ). Для этого во вкладке «Идентификаторы» (рисунок 31) необходимо нажать кнопку <Импорт>. Появляется окно, приведенное на рисунке 35, в котором нажать кнопку <Импортировать>.



Рисунок 35 – Импорт идентификатора

При ее нажатии появится окно выбора файла. Нужно выбрать файл базы и нажать кнопку <Открыть>.

В правой части окна появятся импортированные идентификаторы, как показано на рисунке 36. Следует выбрать из них необходимые для добавления в базу (для выбора всех идентификаторов нужно нажать кнопку <Выбрать все>) и нажать кнопку <Добавить>.

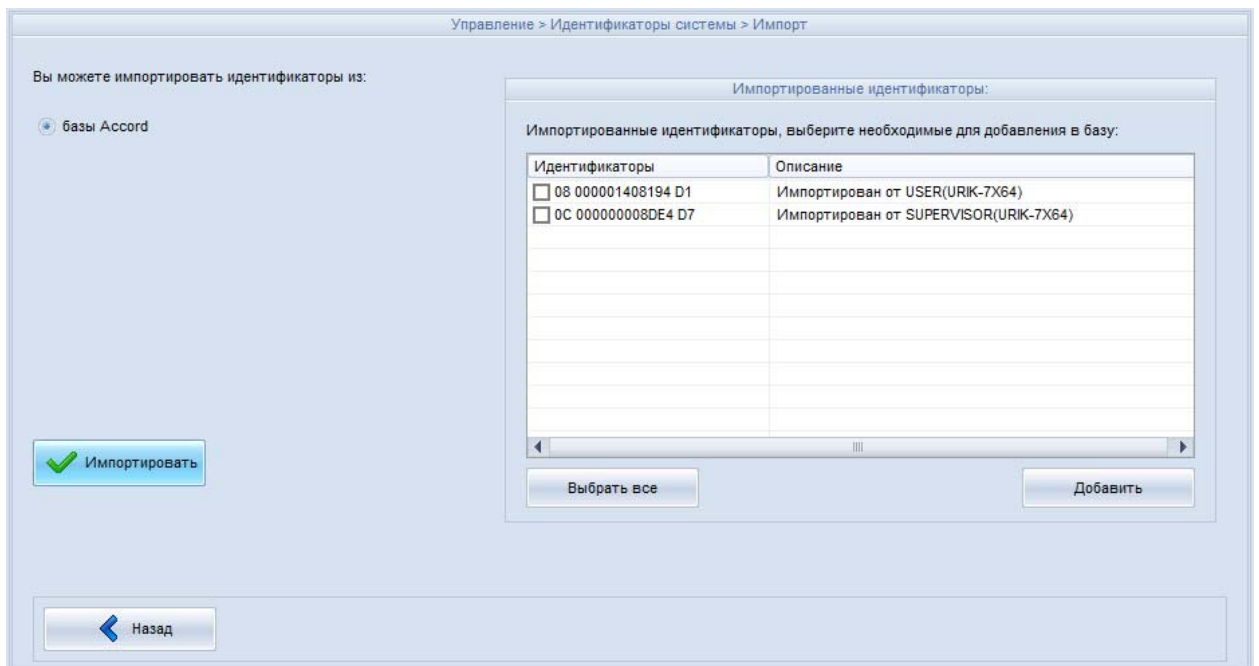


Рисунок 36 – Выбор импортированных идентификаторов (импорт из базы Аккорда)

Если необходимо определить, находится ли данный идентификатор в базе ASM, следует нажать кнопку <Поиск> на вкладке «Идентификаторы» (рисунок 31). Появится окно с сообщением «Предъявите идентификатор», приведенное на рисунке 37.

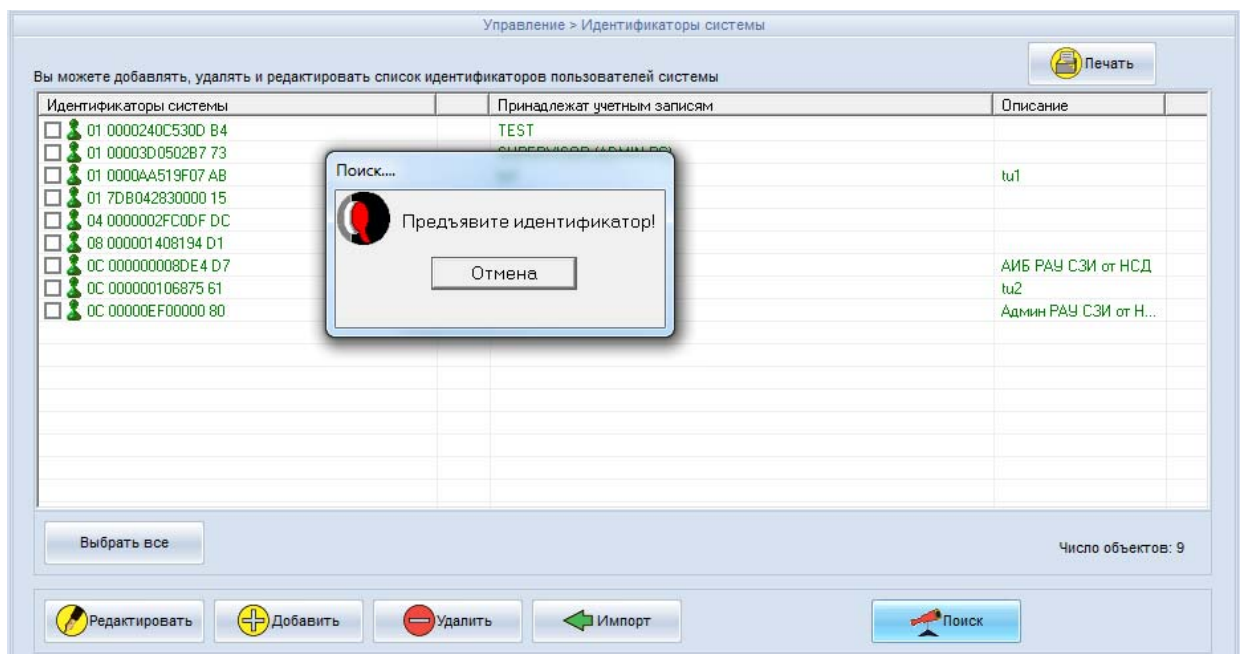


Рисунок 37 – Сообщение «Предъявите идентификатор»

Если данный идентификатор добавлен в базу ASM, то этот идентификатор будет выделен, как показано на рисунке 38.

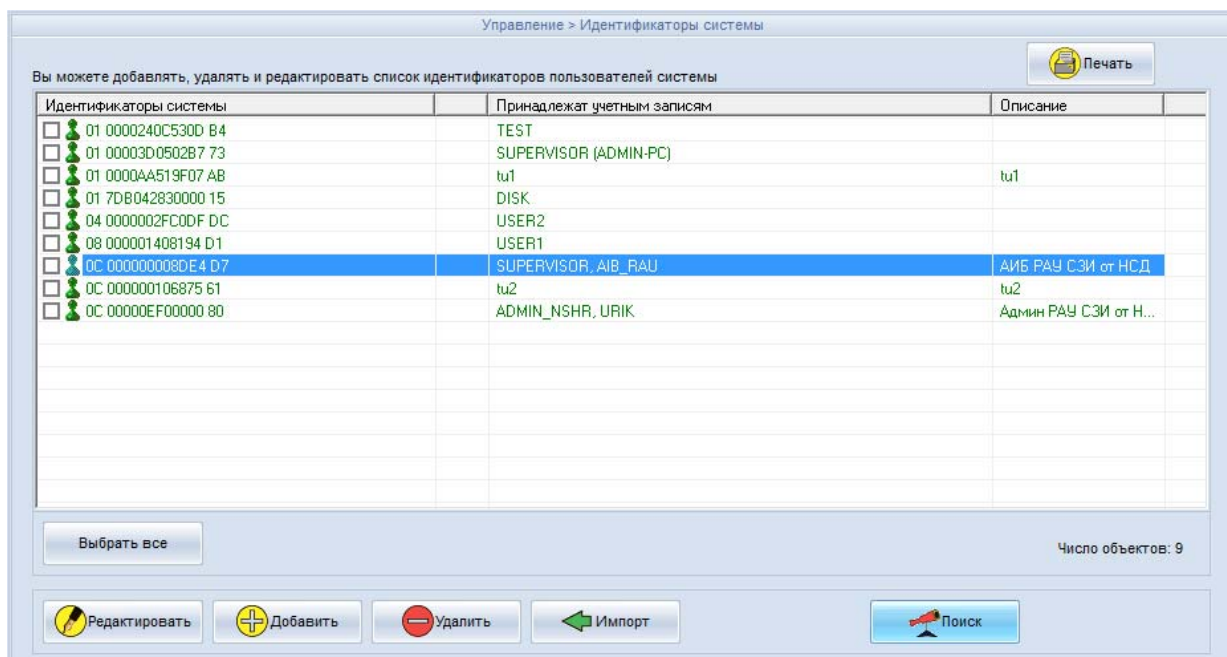


Рисунок 38 – Найдена учетная запись, которой назначен идентификатор

В ином случае в нижней части окна появится сообщение «Идентификатор не зарегистрирован!», приведенное на рисунке 39.

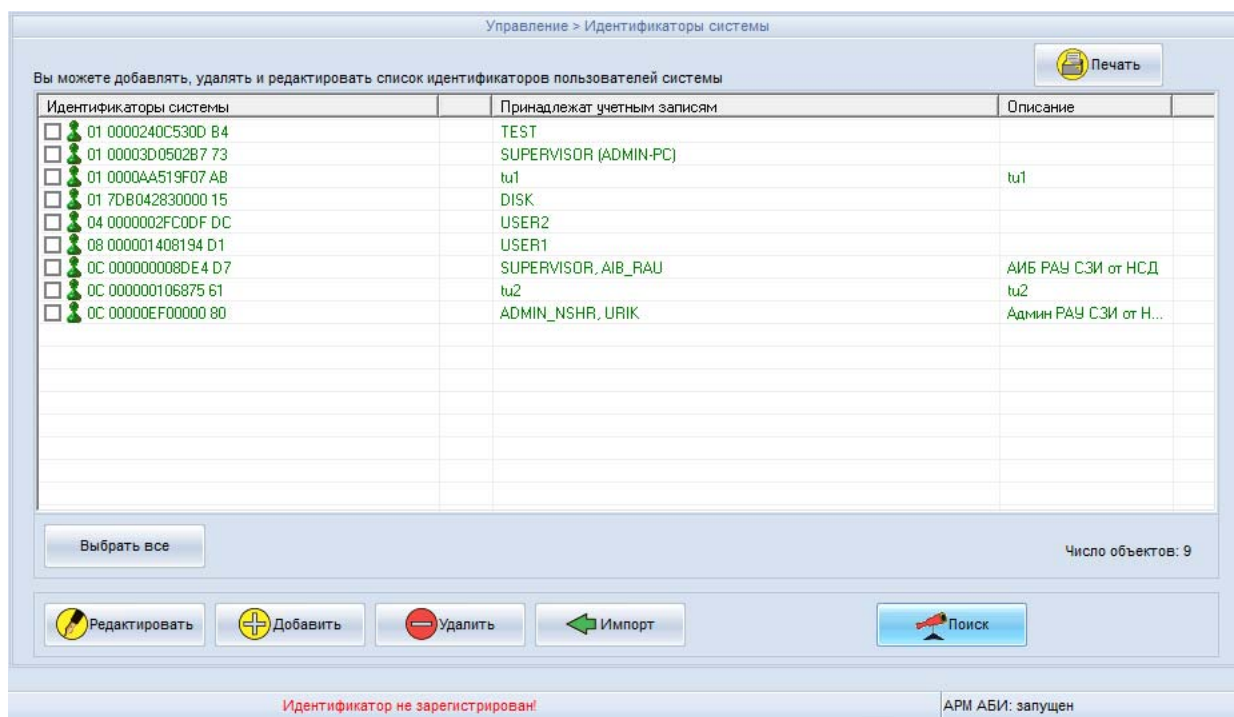


Рисунок 39 – Сообщение о том, что идентификатор не зарегистрирован

4.6 Вкладка «Компьютеры»

Для того чтобы начать работу с подконтрольными объектами, следует открыть в ASM вкладку «Управление > Компьютеры». Появится окно, показанное на рисунке 40.

Примечание. При работе в режиме «Классический РАУ» вид вкладки «Управление > Компьютеры» приведён на рисунке 73.

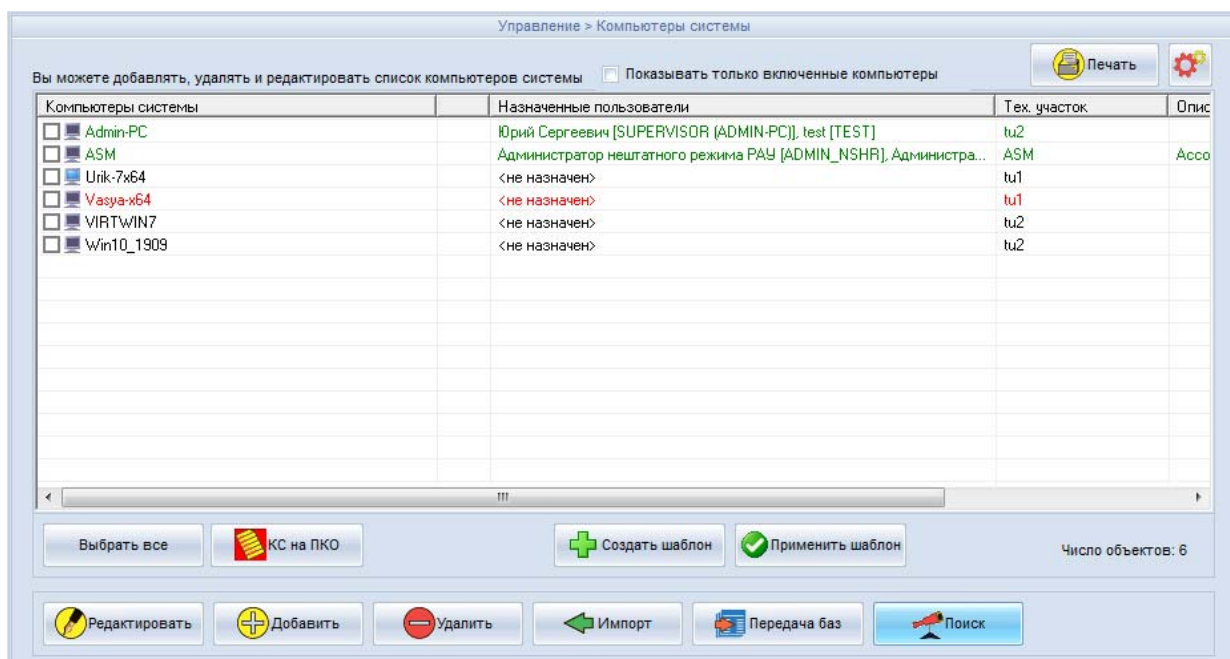


Рисунок 40 – Компьютеры системы

В данном окне красным цветом отображаются те ПКО, на которых не активирована система защиты ПАК «Аккорд».

Для отображения в списке компьютеров информации о наличии на них списков файлов контроля целостности, списков задач, стартовых задачах нужно в окне, приведенном на рисунке 40, нажать кнопку «Настройка отображения информации». При ее нажатии появится окно, приведённое на рисунке 22, в котором устанавливаются флаги напротив той информации о настройках ПКО, которую следует отображать. После добавления отображаемой информации в таблице компьютеров появляется столбец под названием «ПКО», как показано на рисунке 41.

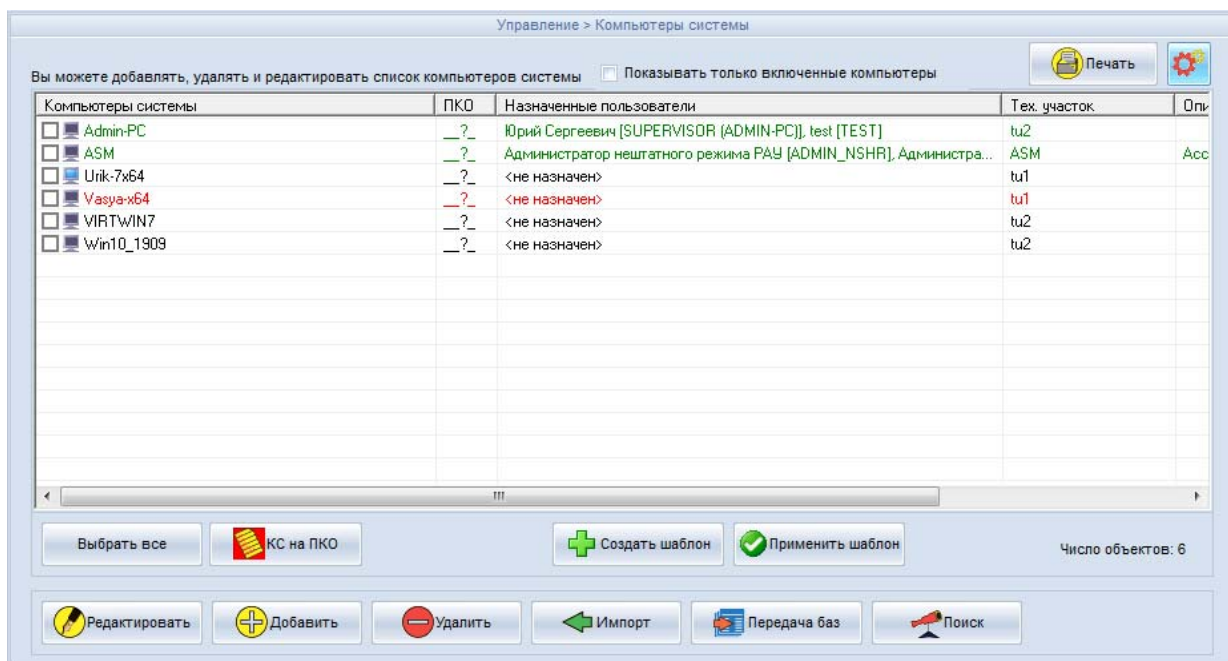


Рисунок 41 – Компьютеры системы. Отображение информации о ПКО

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 <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 42).

Совпадающие значения контрольных сумм (эталонной и вычисленной) помечаются знаком ОК. 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 имеет возможность пересчитать контрольные суммы на выбранном ПКО с последующей записью новых эталонных контрольных сумм. Для этого необходимо нажать кнопку <Обновить КС>.

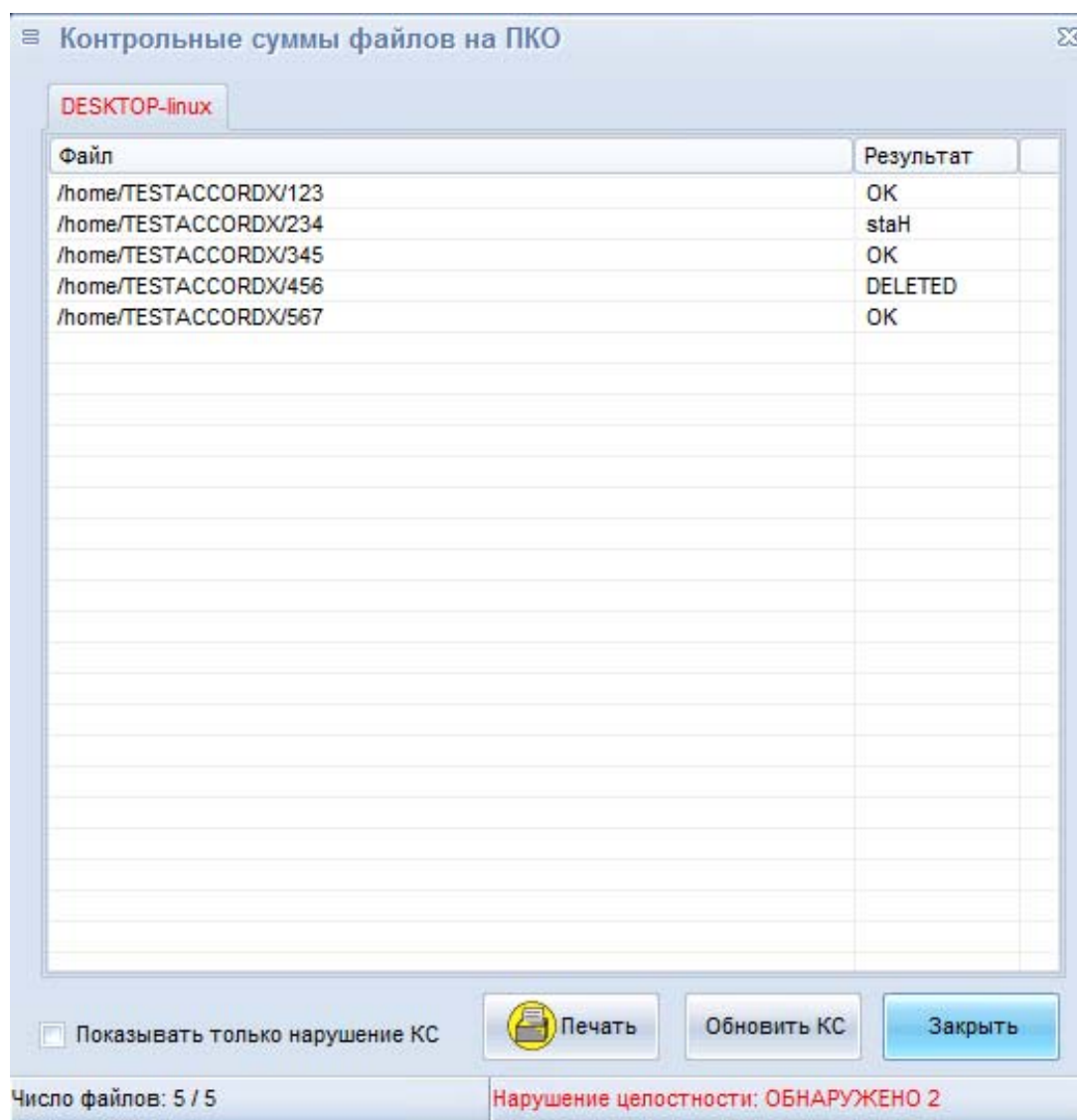


Рисунок 42 – Окно со списком контролируемых файлов для ПКО под управлением ОС Linux

Информация о выполненной процедуре удалённого расчёта контрольных сумм выбранного ПКО отображается в журналах ASM и APM АБИ. При этом в журнале ASM отображается информация о получении текущего списка контроля целостности ПКО и о выполнении команды перерасчёта контрольных сумм с указанием имени Администратора и имени ПКО. В журнале APM АБИ отображается информация об имени ПКО, на котором выполняется процедура удалённого расчёта контрольных сумм, времени и результата выполнения процедуры.

Кнопка <Печать> позволяет распечатать информацию о выбранных компьютерах на принтере или сохранить ее в файл (с указываемым разделителем). При ее нажатии появится окно, приведенное на рисунке 43 в котором выбирается, куда нужно вывести информацию: в файл или на принтер, какую информацию о выбранных компьютерах нужно распечатать (имя компьютера, описание компьюте-

ра, тех. участок и т. д.). При печати в файл кроме этого нужно задать разделитель выводимых полей.

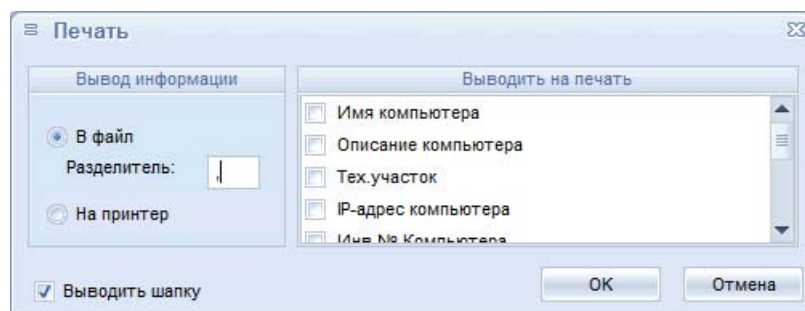


Рисунок 43 – Печать информации о подконтрольном объекте

Для добавления компьютера необходимо нажать кнопку <Добавить> в окне, приведенном на рисунке 40. В появившемся окне, приведенном на рисунке 44, задаются имя компьютера, его описание и технологический участок, которому он принадлежит (последние два условия не являются обязательными). Для сохранения изменений необходимо нажать кнопку <Применить>.

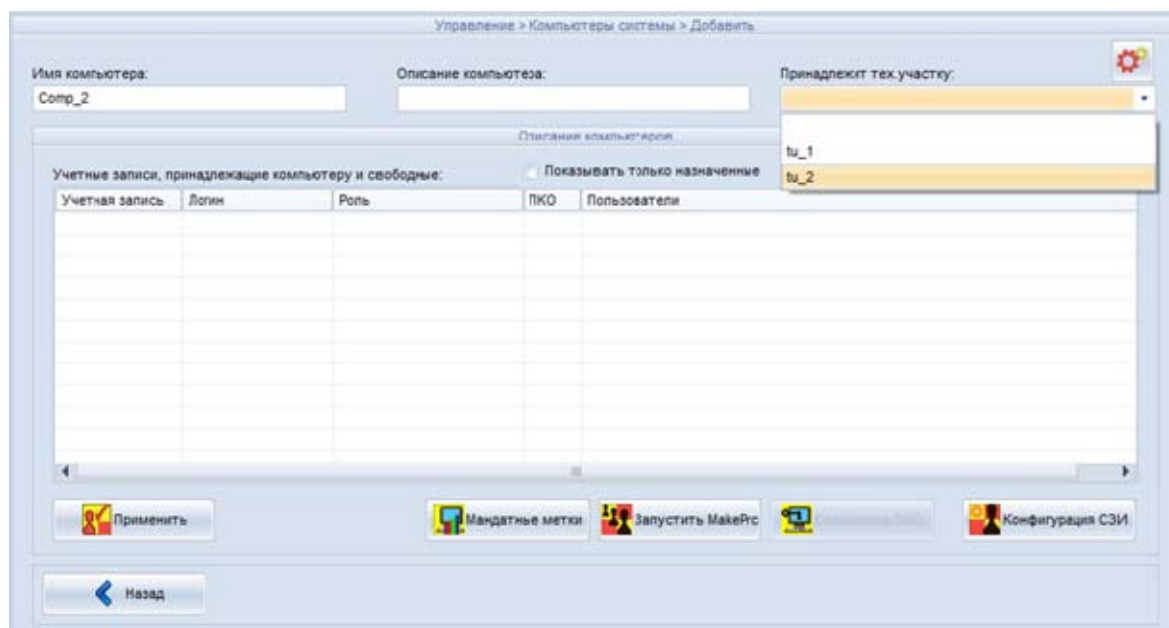


Рисунок 44 – Добавление компьютера

Чтобы редактировать компьютер, необходимо нажать кнопку <Редактировать> (рисунок 40). В появившемся окне (рисунок 45) можно изменить имя компьютера, его описание и назначить этот компьютер технологическому участку (последние два условия не являются обязательными для заполнения).

Кнопка <Мандатные метки>² предназначена для установки меток мандатного доступа к объектам ПКО (в случае использования на ПКО мандатного механизма разграничения доступа).

При ее нажатии появится главное окно программы ACED32.EXE, в котором необходимо выбрать функцию установки меток мандатного допуска (Команды\Метки мандатного допуска, рисунок 48).

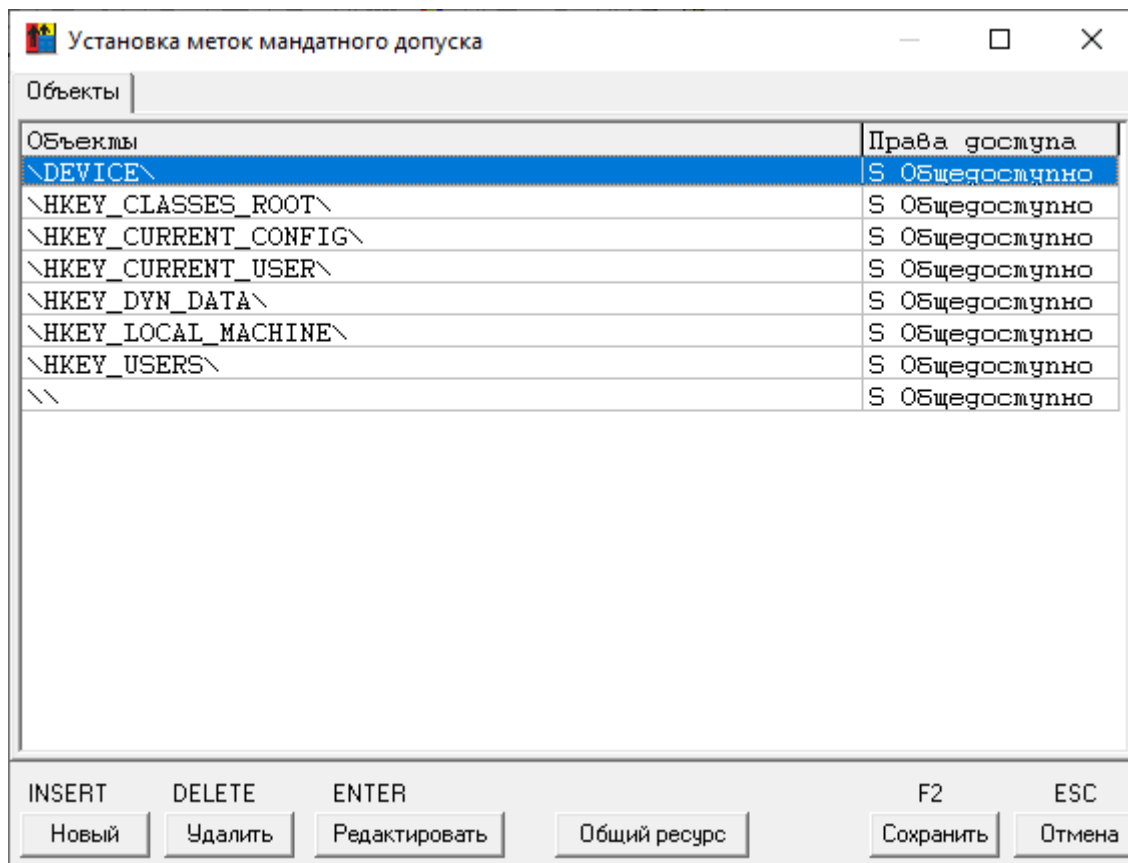


Рисунок 48 – Установка меток мандатного допуска

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

При нажатии кнопки <Конфигурация СЗИ> появляется окно, приведенное на рисунках 49/50, в котором отображаются настройки СЗИ выбранного ПКО, версия его программного обеспечения, IP-адрес, а также инвентарный номер ПКО (заполняется вручную).

² Только для ПКО под управлением ОС Windows



Рисунок 49 – Конфигурация СЗИ на ПКО под управлением ОС Windows

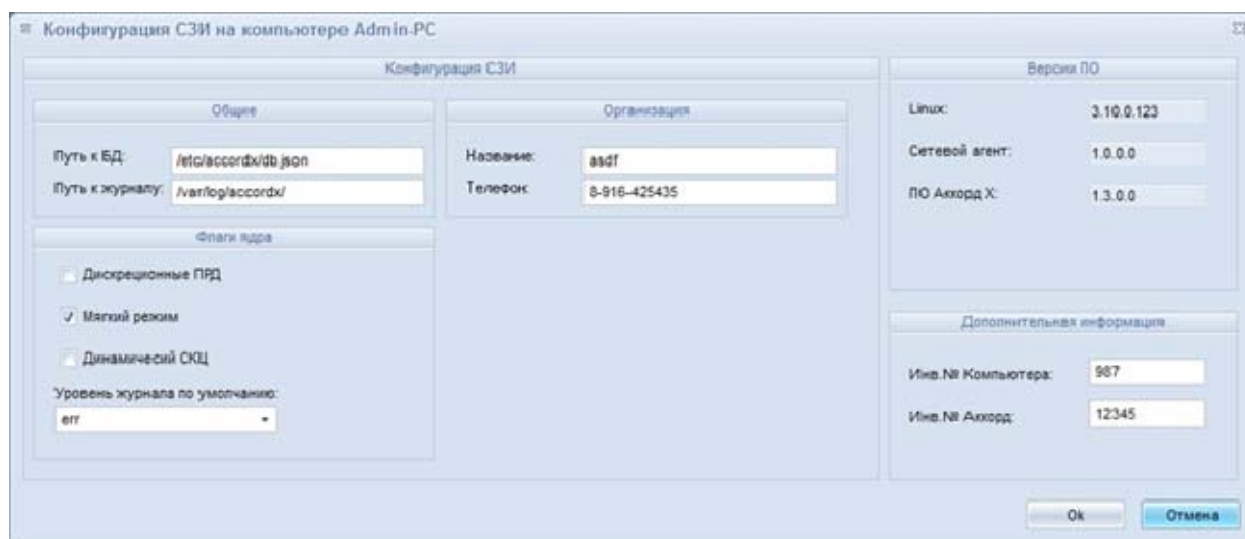


Рисунок 50 - Конфигурация СЗИ на подконтрольном объекте под управлением ОС Linux

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

При успешном сохранении настроек появляется сообщение:

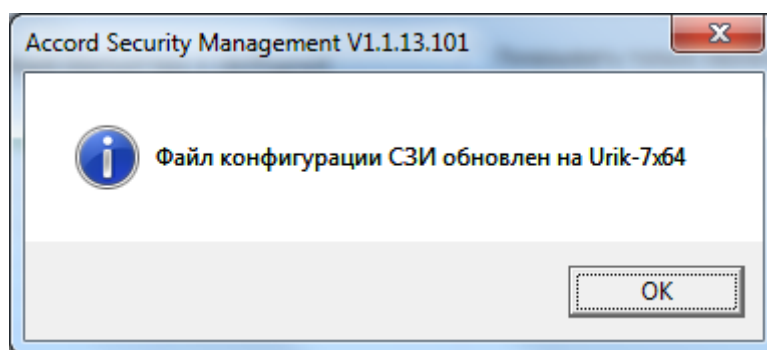


Рисунок 51 – Сообщение об успешном выполнении процедуры настройки ПКО

Существует возможность редактирования списка привилегированных процессов с последующей его передачей на ПКО. Для этого нужно нажать кнопку <Запустить MakePrc>³ (рисунок 45).

ВНИМАНИЕ! В целях оптимизации работы ПО ПАК «Аккорд» на ПКО (минимизации количества событий от системных процессов) при создании списка привилегированных процессов рекомендуется добавлять в файл *.PRC следующие процессы:

1) для ПКО с ОС Windows XP/7 (x86):

C:\ACCORD.NT\ACWS32.EXE

C:\ACCORD.NT\ACWS32NT.EXE

C:\ACCORD.NT\ACWSRST.EXE

C:\PROGRAM FILES\KASPERSKY LAB\KASPERSKY ENDPOINT SECURITY
10 FOR WINDOWS\AVP.EXE

C:\PROGRAM FILES\KASPERSKY LAB\KASPERSKY ENDPOINT SECURITY 8
FOR WINDOWS\AVP.EXE

C:\PROGRAM FILES\KASPERSKY LAB\NETWORKAGENT\VAPM.EXE

C:\WINDOWS\SYSTEM32\DFRGNTFS.EXE

C:\WINDOWS\SYSTEM32\SVCHOST.EXE

C:\WINDOWS\SYSTEM32\WBEM\WMIPRVSE.EXE

2) для ПКО с Windows 7 (x64):

C:\ACCORD.x64\ACWS32.EXE

³ Только для ПКО под управлением ОС Windows

C:\ACCORD.x64\ACWS32NT.EXE

C:\ACCORD.x64\ACWSRST.EXE

C:\PROGRAM FILES\KASPERSKY LAB\KASPERSKY ENDPOINT SECURITY
10 FOR WINDOWS\AVP.EXE

C:\PROGRAM FILES\KASPERSKY LAB\KASPERSKY ENDPOINT SECURITY 8
FOR WINDOWS\AVP.EXE

C:\PROGRAM FILES\KASPERSKY LAB\NETWORKAGENT\VAPM.EXE

C:\WINDOWS\SYSTEM32\SVCHOST.EXE

C:\WINDOWS\SYSTEM32\WBEM\WMIPRVSE.EXE

C:\WINDOWS\SYSTEM32\SERVICES.EXE

При этом на самих ПКО рекомендуется устанавливать на динамический контроль целостности следующие файлы:

1) для ПКО с ОС Windows XP (x86):

C:\WINDOWS\SYSTEM32\DFRGNTFS.EXE

C:\WINDOWS\SYSTEM32\SVCHOST.EXE

C:\WINDOWS\SYSTEM32\WBEM\WMIPRVSE.EXE

2) для ПКО с ОС Windows 7 (x86):

C:\WINDOWS\SYSTEM32\SVCHOST.EXE

C:\WINDOWS\SYSTEM32\WBEM\WMIPRVSE.EXE

3) для ПКО с ОС Windows 7 (x64):

C:\WINDOWS\SYSTEM32\SVCHOST.EXE

C:\WINDOWS\SYSTEM32\WBEM\WMIPRVSE.EXE

C:\WINDOWS\SYSTEM32\SERVICES.EXE

Если необходимо определить, зарегистрирован ли компьютер в системе, следует нажать кнопку <Поиск> во вкладке «Компьютеры» (рисунок 40). При ее нажатии появится окно (рисунок 52), в котором необходимо указать IP-адрес компьютера или его имя.

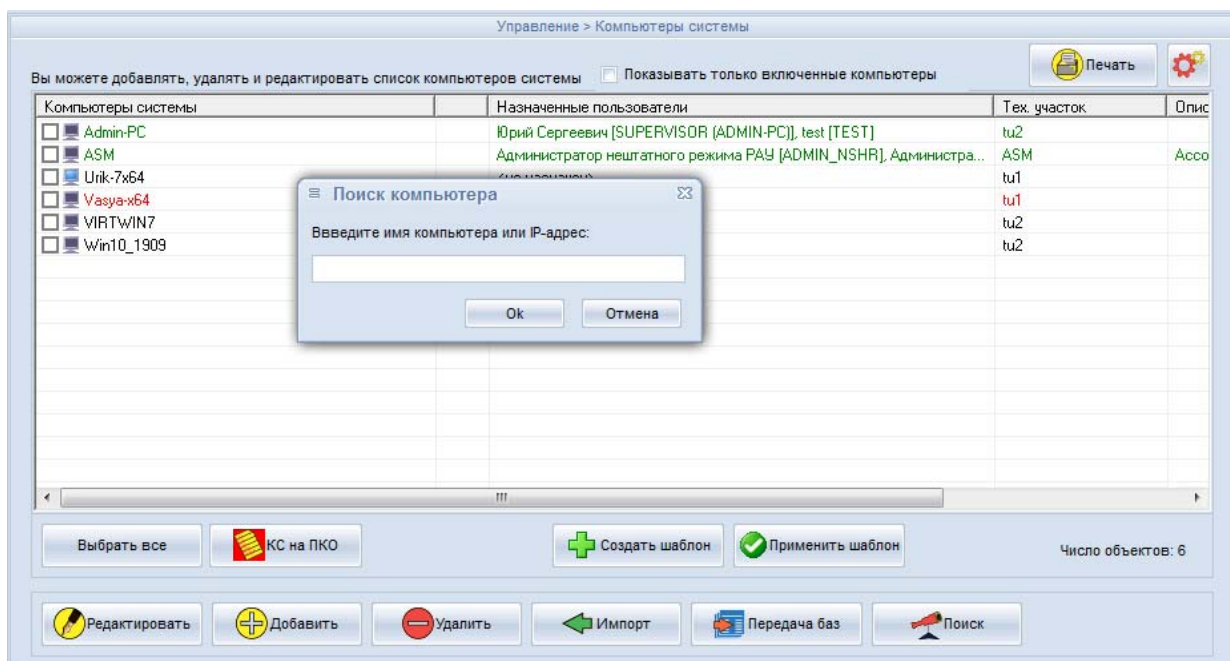


Рисунок 52 - Поиск компьютера по имени или IP-адресу

Если компьютер с таким именем или IP-адресом зарегистрирован в системе, то этот компьютер будет выделен, как показано на рисунке 53.

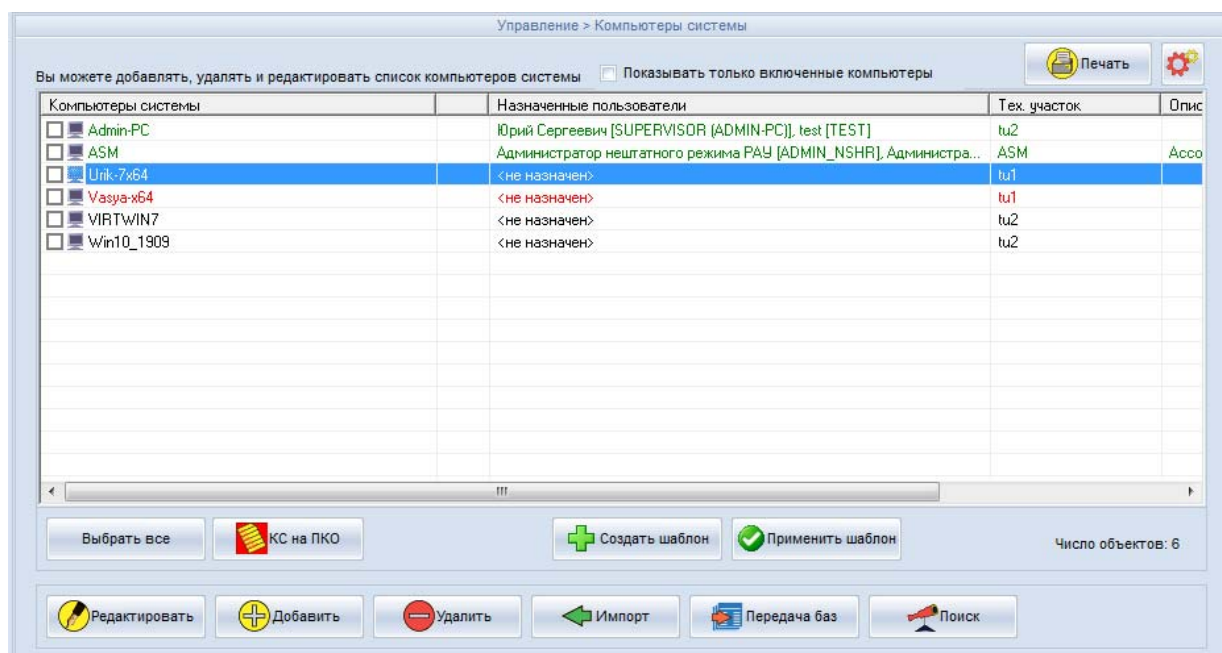


Рисунок 53 – Найден компьютер

В ином случае в нижней части окна появится сообщение «Компьютер не найден!», как показано на рисунке 54.

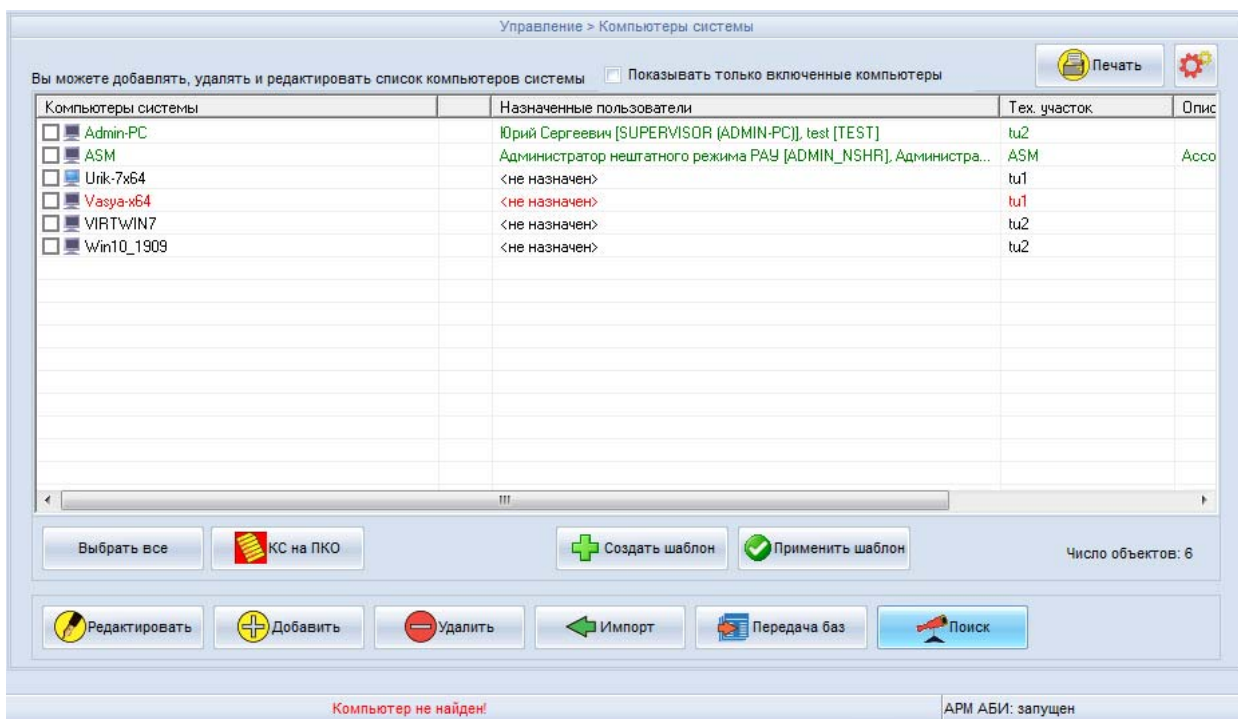


Рисунок 54 – Сообщение о том, что компьютер не найден

Чтобы удалить компьютер, необходимо выделить его и нажать кнопку <Удалить> на вкладке «Компьютеры» (рисунок 40). Появится окно подтверждения этого действия (рисунок 55).

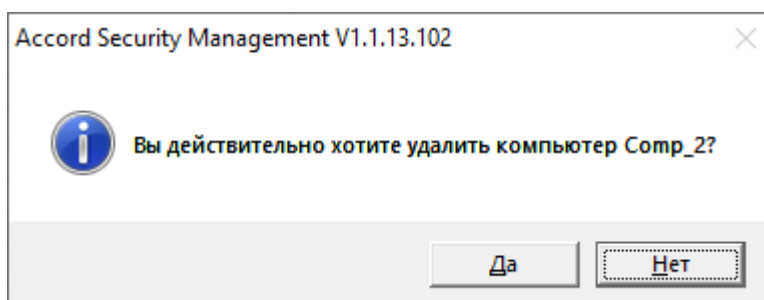


Рисунок 55 – Окно подтверждения удаления компьютера

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

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

Кнопка <Импорт> во вкладке «Компьютеры» (рисунок 40) необходима для регистрации ПКО. При ее нажатии появится окно импорта компьютеров (рисунок 56). Чтобы импортировать компьютеры из базы «Аккорд-ПАУ», необходимо установить соответствующий флаг («Вы можете импортировать компьютеры

из:» - «базы Accord-PAУ») в окне, показанном на рисунке 56, и нажать кнопку <Импортировать>.



Рисунок 56 – Импорт компьютеров

При ее нажатии появится окно, приведенное на рисунке 57, в котором следует указать файл, из которого необходимо импортировать компьютеры.

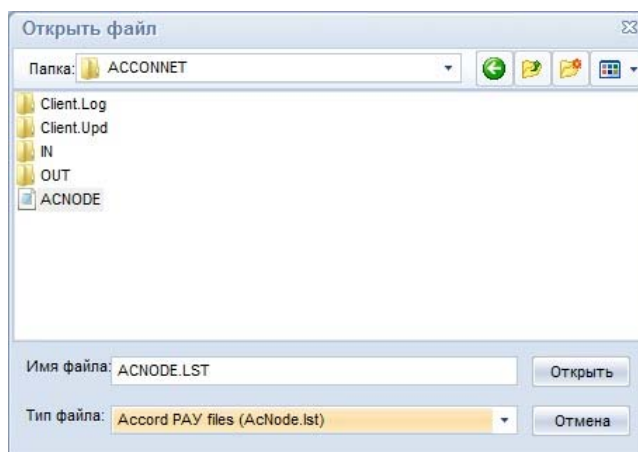


Рисунок 57 – Выбор каталога для импорта компьютеров

После этого в правой части окна появятся импортированные компьютеры; следует выбрать из них необходимые для добавления в базу (для выбора всех учетных записей нажать кнопку <Выбрать все>) и нажать кнопку <Добавить> (рисунок 58).

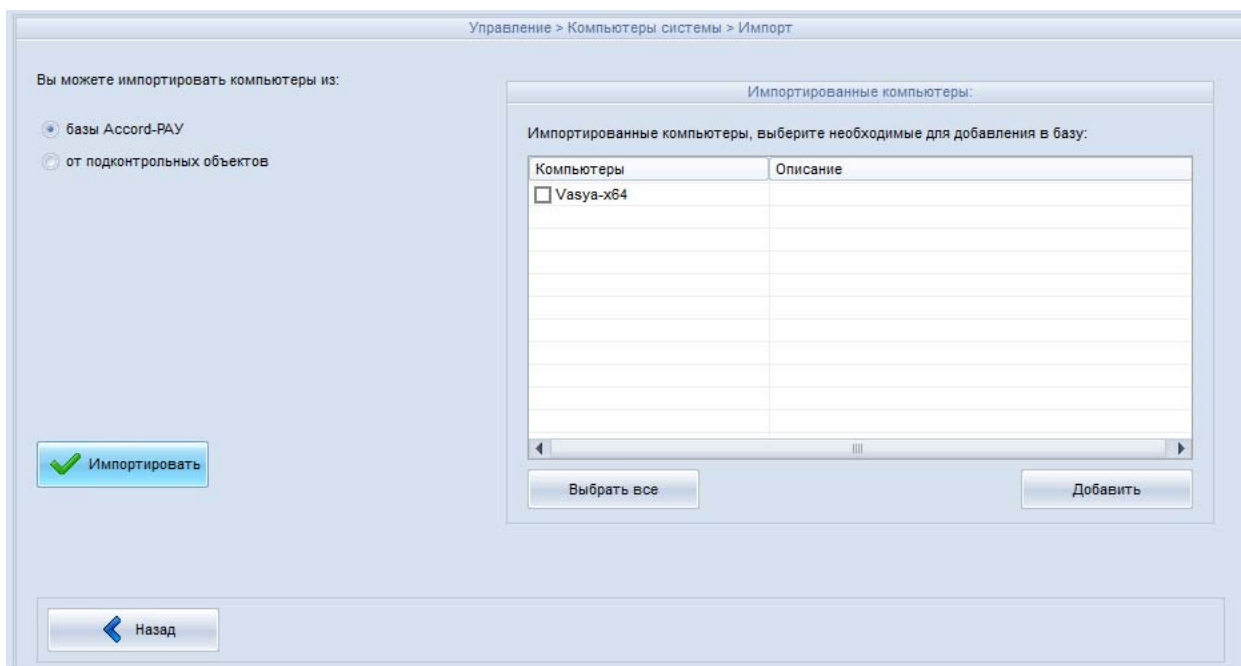


Рисунок 58 - Выбор импортированных компьютеров (импорт из базы «Аккорд-РАУ»)

Чтобы импортировать компьютеры от ПКО, необходимо установить соответствующий флаг («Вы можете импортировать компьютеры из:» - «от подконтрольных объектов») в окне, показанном на рисунок 59, и нажать кнопку <Импортировать>.

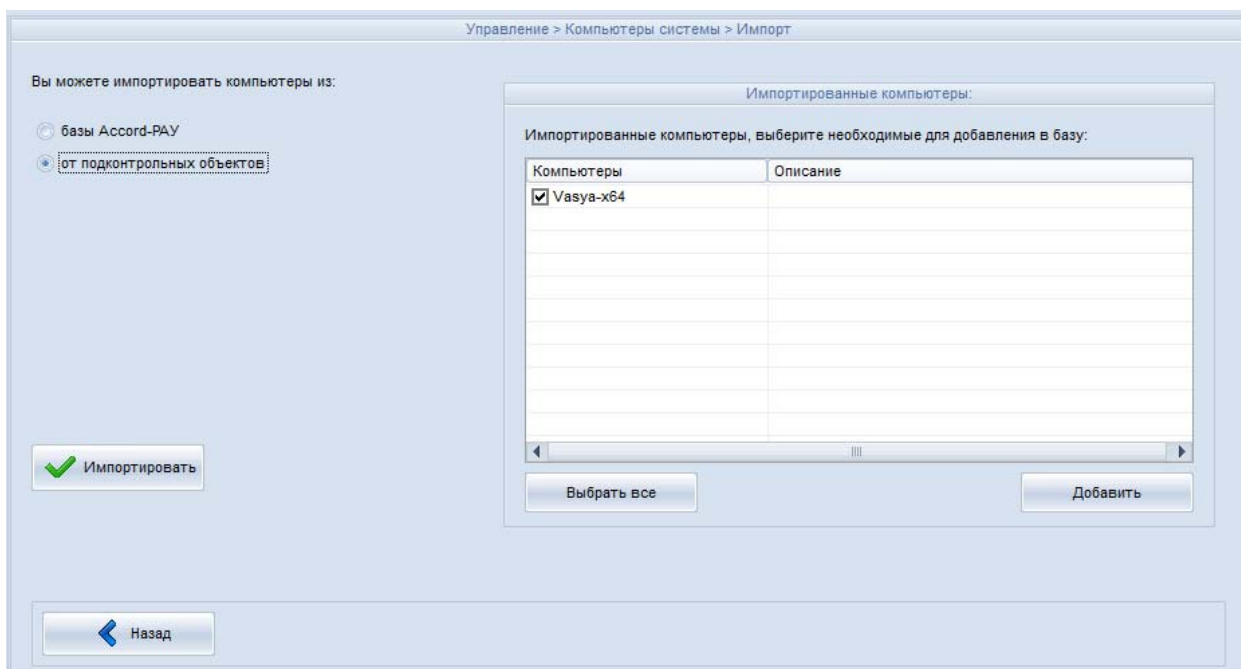


Рисунок 59 – Выбор импортированных компьютеров

После этого в правой части окна появятся импортированные компьютеры, следует выбрать из них необходимые для добавления в базу (для выбора всех

учетных записей нажать кнопку <Выбрать все>) и нажать кнопку <Добавить> (рисунок 59).

Существует возможность работать с базами пользователей (читать, добавлять, изменять) нескольким Администраторам ИБ (ТУ) одновременно. Сохранение внесённых изменений происходит при наступлении любого из следующих событий:

- смена пароля пользователем ПКО;
- нажатие Администраторам ИБ (ТУ) кнопки <Сохранить> в левом верхнем углу окна ASM.

При этом в статус баз окна ASM всех других Администраторов ИБ (ТУ), работающих в данный момент с ASM, будет выведено сообщение «Базы модифицированы другим администратором. Обновлено».

Передача баз пользователей на ПКО в рамках централизованной схемы осуществляется кнопкой <Передача баз> (предварительно необходимо выбрать компьютеры, на которые планируется передать базы (см. рисунок 40)). При ее нажатии появится окно передачи баз пользователей на ПКО, приведенное на рисунке 60.

Выбрать пункт «Используя АРМ АБИ» (рисунок 60) и нажать <ОК>.



Рисунок 60 – Передача баз пользователей по централизованной схеме

Если база пользователей передана на ПКО, появляется сообщение, приведенное на рисунке 61.

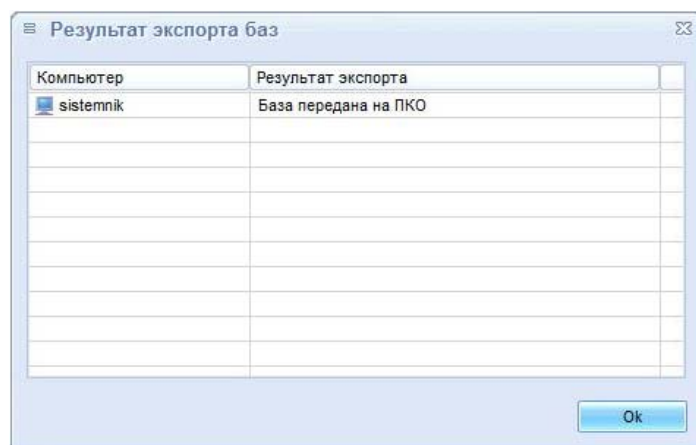


Рисунок 61 – Сообщение о том, что база пользователей передана на ПКО

Если во время выполнения процедуры передачи базы пользователей служба AcConNet загружена, появляется соответствующее сообщение (рисунок 62).

По истечении некоторого времени база пользователей автоматически передается на ПКО, и появляется сообщение, показанное на рисунке 61.

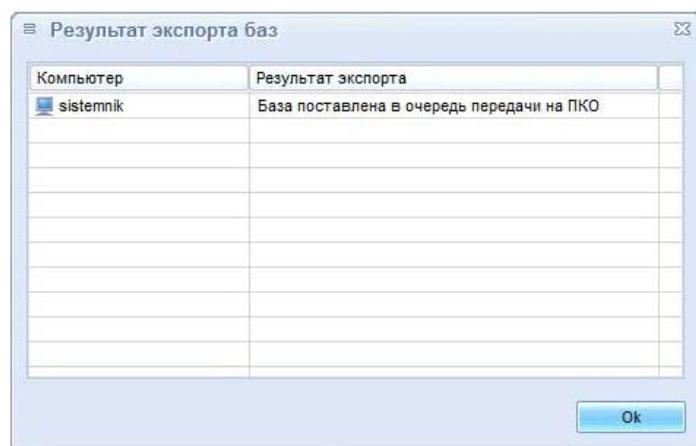


Рисунок 62 – Сообщение о том, что база пользователей поставлена в очередь передачи

Если во время выполнения процедуры передачи базы пользователей ПКО выключен, то появляется сообщение о готовности базы для передачи (рисунок 63):

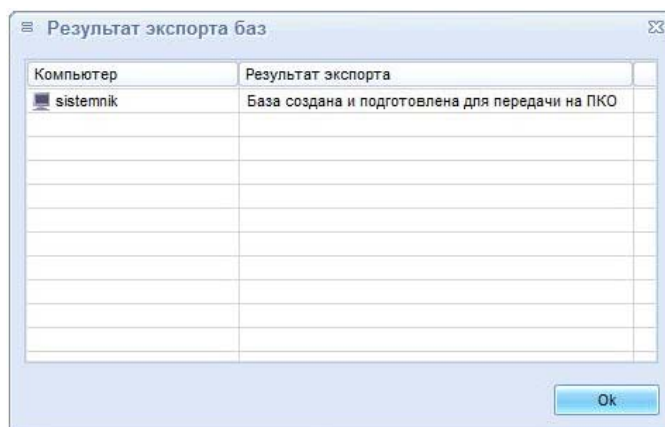


Рисунок 63 – Сообщение о создании и подготовке для передачи базы пользователей

База пользователей автоматически передается при следующем включении ПКО, и на экране появляется сообщение об этом (рисунок 64):

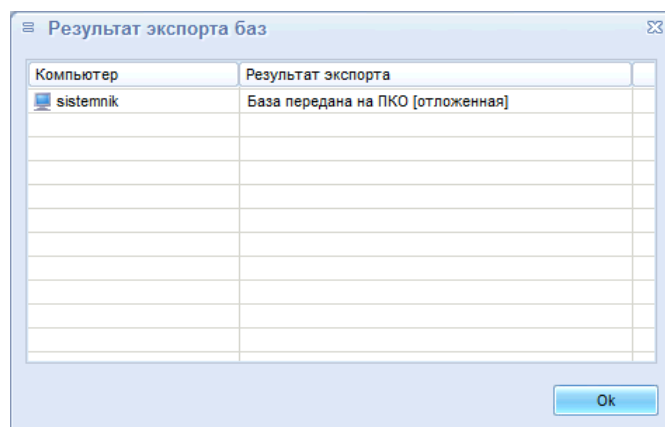


Рисунок 64 – Сообщение о том, что отложенная база передана на ПКО

Если процедура передачи базы пользователей выполняется на ПКО, на котором не активирована система защиты ПАК «Аккорд», то появляется сообщение с пометкой «[Аккорд не активирован]», приведенное на рисунке 65.

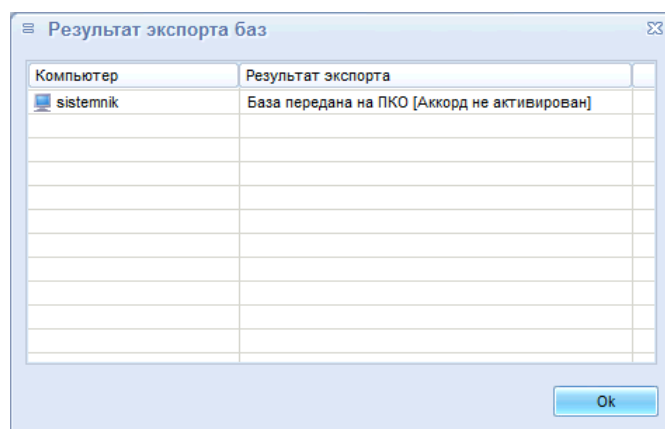


Рисунок 65 – Сообщение о передаче базы пользователей на ПКО, на котором не активирована система защиты «Аккорд»

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

Передача баз пользователей на ПКО в рамках децентрализованной схемы осуществляется кнопкой <Передача баз> (предварительно необходимо выбрать компьютеры (рисунок 40), на которые планируется передать базы). При этом производится копирование перечня учетных записей на внешний носитель, в качестве которого может использоваться флэш-накопитель USB или флоппи-диск. Если в качестве внешнего носителя используется флэш-накопитель USB, то перед тем как выполнить процедуру передачи баз пользователей на ПКО в рамках децентрализованной схемы, необходимо добавить флэш-накопитель в единую базу USB-носителей (эта процедура выполняется Администратором РАУ в соответствии с документом 11443195.4012-053 90 «СПО СЗИ НСД «Аккорд-РАУ». Руководство Администратора». При нажатии кнопки <Передача баз> появляется окно передачи баз пользователей на ПКО, в котором нужно выбрать пункт «Экспортировать на диск» (рисунок 66) и нажать кнопку <ОК>.

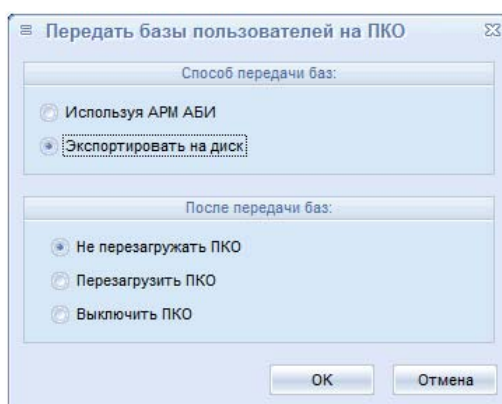


Рисунок 66 – Передача баз пользователей по децентрализованной схеме

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, то появляется соответствующее сообщение (рисунок 67):

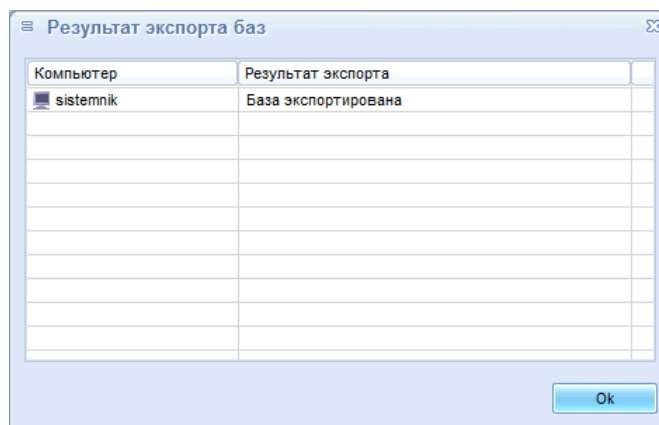


Рисунок 67 – Сообщение о том, что база пользователей экспортирована на диск

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.

Далее 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 нужно выбрать правой кнопкой мыши сетевой клиент ПАК «Аккорд», приведённый на рисунке 68;

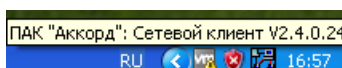


Рисунок 68 – Значок сетевого клиента ПАК «Аккорд» в трее

- появится меню, приведённое на рисунке 69;

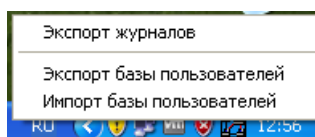


Рисунок 69 – Контекстное меню сетевого клиента ПАК «Аккорд» в трее

- в этом меню выбрать пункт «Импорт базы пользователей». Появляется сообщение «Введите идентификатор». Предъявить идентификатор Администратора «Аккорд» ПКО. После этого будет выведено окно ввода пароля, приведённое на рисунке 70;

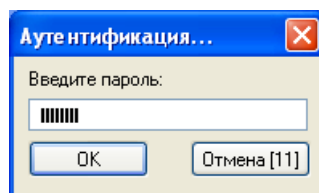


Рисунок 70 – Окно ввода пароля

- ввести пароль и нажать кнопку <OK>. Появится окно выбора каталога для импорта базы пользователей, приведённое на рисунке 71;

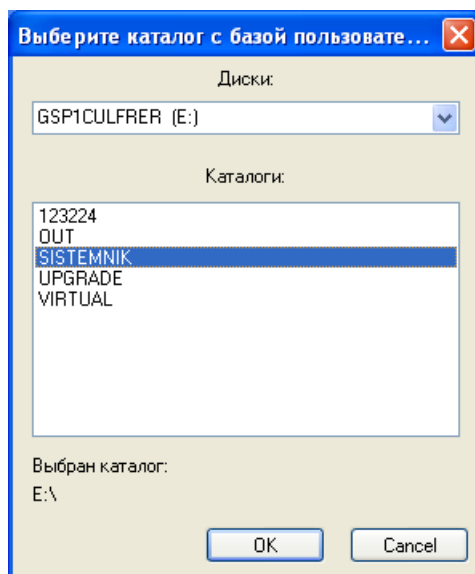


Рисунок 71 – Выбор каталога для импорта базы пользователей

- выбрать нужный каталог и нажать <OK>.

Если импорт базы пользователей выполнен успешно, то появится сообщение, приведённое на рисунке 72.

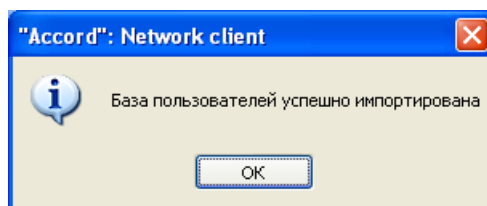


Рисунок 72 – Оповещение об успешном выполнении процедуры импорта базы пользователей

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, 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.

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 73, установить флажки напротив тех ПКО, для которых создаётся задание для контроля целостности, и нажать кнопку <Создать шаблон>.

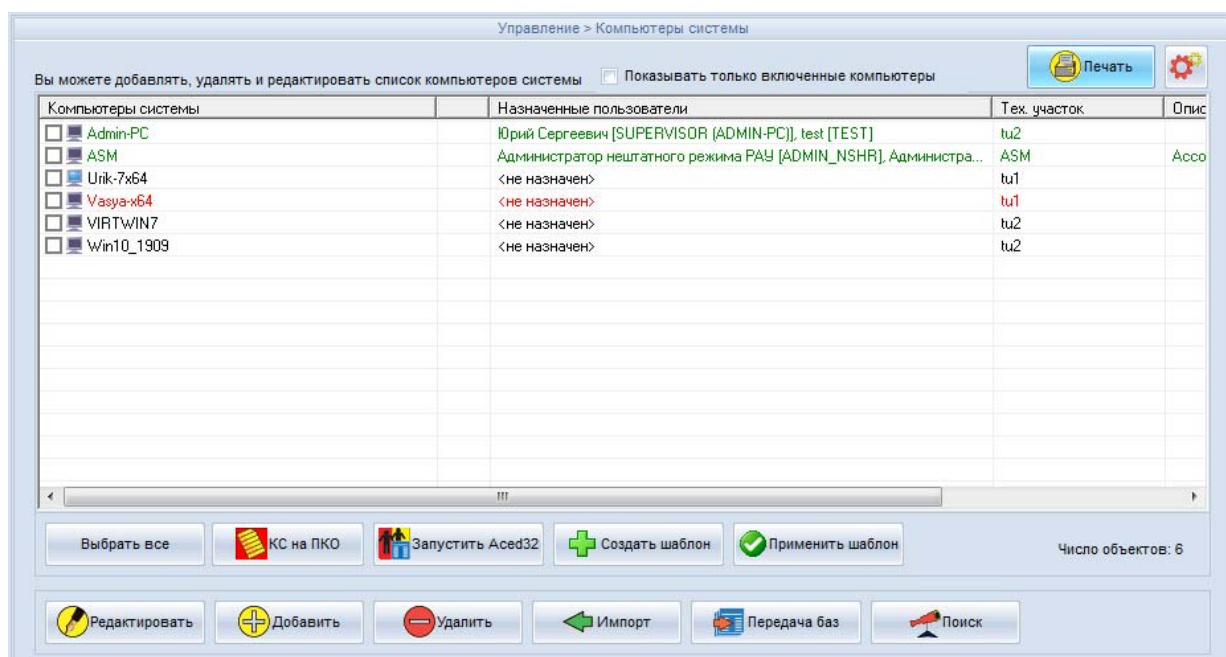


Рисунок 73 - Вкладка «Компьютеры системы» при работе в режиме «Классический РАУ»

При ее нажатии появится окно, приведённое на рисунке 74.



Рисунок 74 - 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 16. В данном окне указываются файлы, целостность которых нужно контролировать. При указании файлов должны соблюдаться правила, приведённые в подразделе 4.3. 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 16, 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, то файлы с заданием КЦ не будут переданы на ПКО.

Если в окне, приведённом на рисунке 73, были установлены флажки напротив некоторых ПКО, то сформированное задание сразу будет передано на выбранные ПКО.

Если ПКО выбраны не были, то в окне, приведённом на рисунке 73, нужно установить флажки 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 с эталонными контрольными суммами 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 73, выбрать данные ПКО и нажать кнопку <Запустить Aced32>. Появится главное окно

редактора базы пользователей ПАК СЗИ от НСД «Аккорд» – AcEd32, приведённое на рисунке 75.

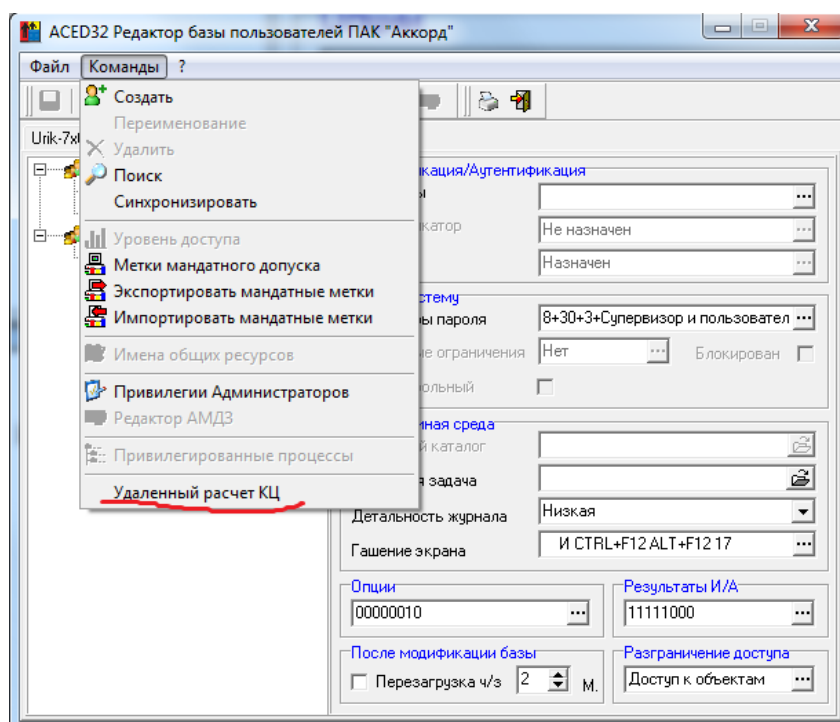


Рисунок 75 - Главное окно редактора базы пользователей ПАК СЗИ от НСД «Аккорд»

В главном меню данного окна или контекстном меню, появляющемся после нажатия правой кнопки мыши на группе пользователей, выбрать пункт «Удаленный расчет КЦ». Будет выведено окно контроля целостности файлов, приведённое на рисунке 76. Данное окно содержит список файлов, целостность которых контролируется на ПКО.

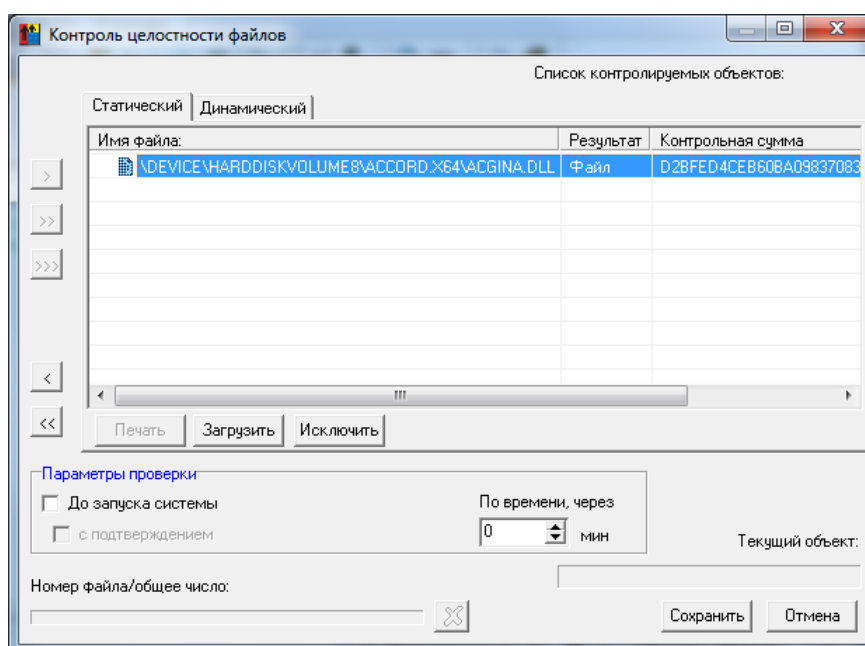


Рисунок 76 - Окно контроля целостности файлов

В окне 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 77.

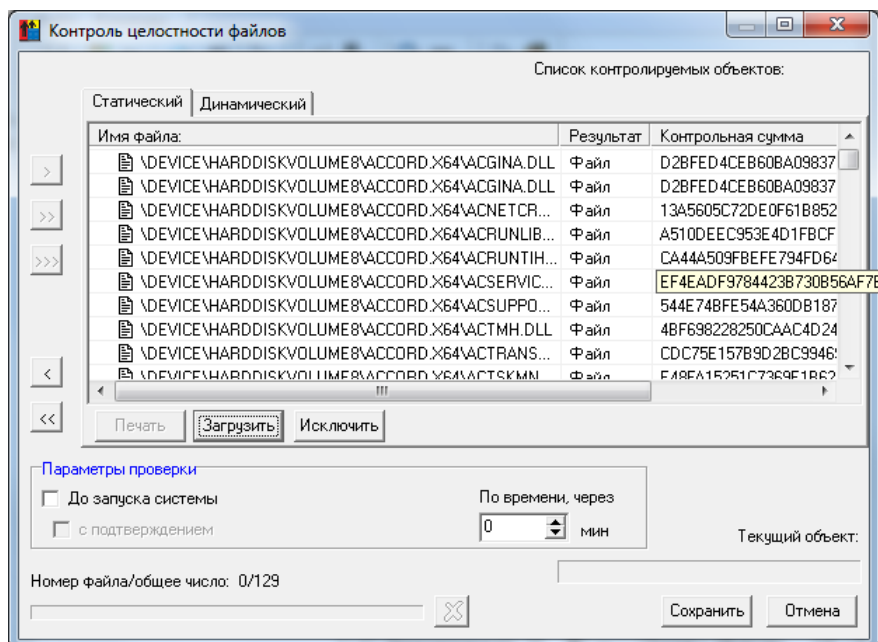


Рисунок 77 - Список файлов, целостность которых контролируется на ПКО

В окне контроля целостности файлов 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.

4.7 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 78.

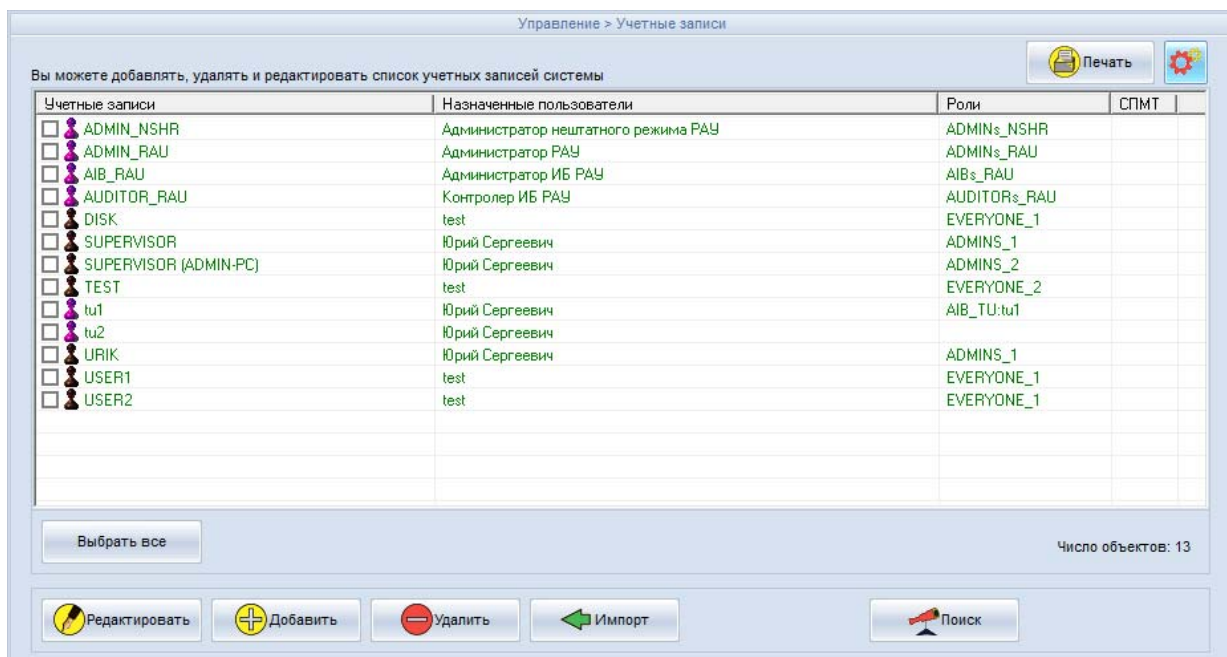


Рисунок 78 – Учётные записи

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 появится окно, приведённое на рисунке 22, в котором устанавливаются флаги напротив информации о настройках ПКО, которую нужно отображать. После добавления отображаемой информации в таблице учётных записей появляется столбец под названием «ПКО», как показано на рисунке 79.

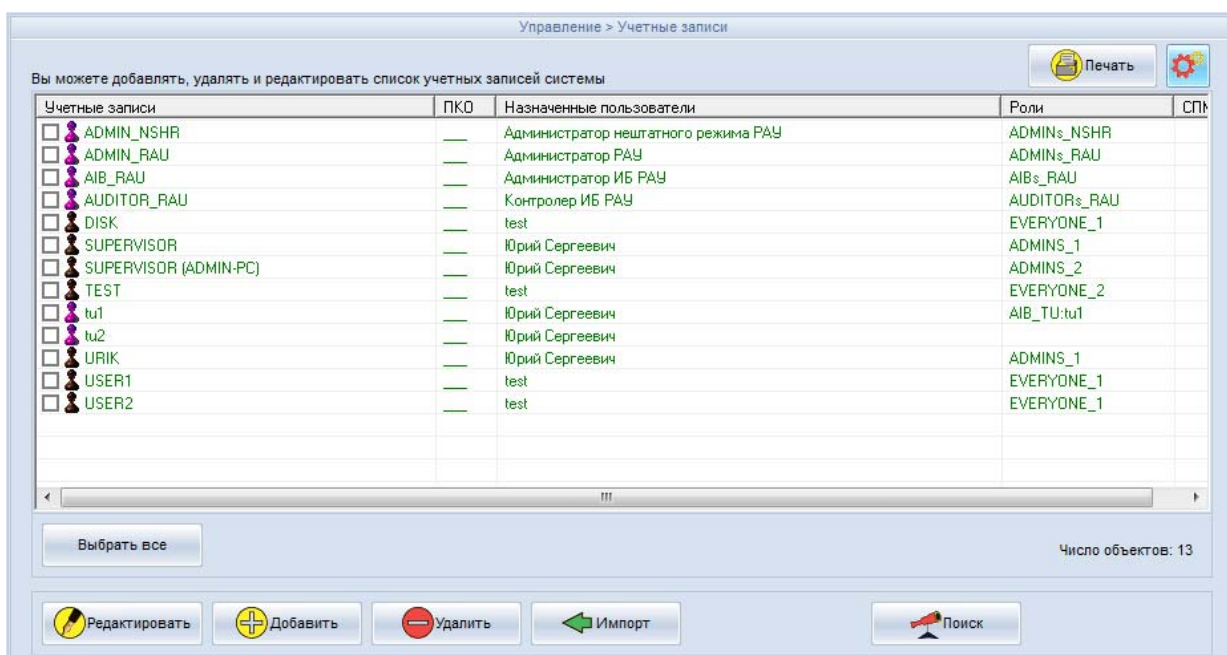


Рисунок 79 – Учётные записи. Отображение информации о ПКО

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 появится окно, приведённое на рисунке 80, в котором следует выбрать способ печати: в файл или на принтер, тип выводимой информации (имя учетной записи, имя назначенного ей пользователя, имя роли); при печати в файл следует также указать разделитель.

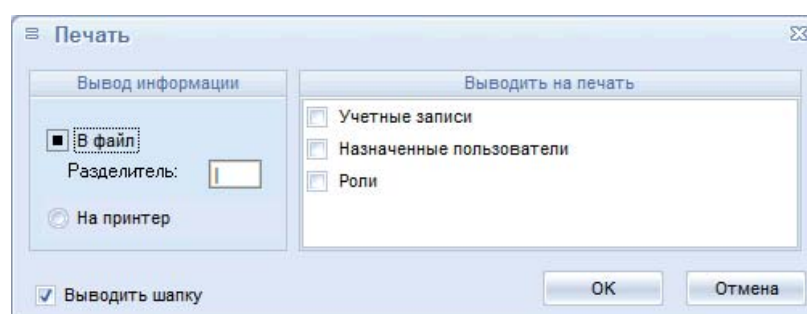


Рисунок 80 – Печать информации об учетной записи

Чтобы добавить новую учетную запись, необходимо нажать кнопку <Добавить>. В появившемся окне (рисунок 81) следует ввести имя учетной записи, указать роль, назначить пользователя (сотрудника как физического лица)⁴, которому назначается данная учетная запись, имя пользователя⁵, полное имя пользователя⁶, ввести пароль и подтвердить его ввод, назначить пользователю идентификатор и выбрать компьютеры, на которых будет создана данная учетная запись. После ввода этих параметров 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 запрещается её модификация

⁴ 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 «СПО СЗИ НСД «Аккорд-РАУ». Руководство Администратора».

⁵ Логин в базе пользователей АМДЗ.

⁶ Имя пользователя в домене.

При регистрации подконтрольного объекта РАУ создает на нём «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»).

Управление > Учетные записи > Добавить

Описание учетной записи

Имя учетной записи: User_1

Имя пользователя: Goryunov

Полное имя пользователя: GoryunovGG@domain

Пароль:

Подтверждение пароля:

Пароль изменил: -

Идентификатор: [01 00004A023221 E7]

Роль: EVERYONE_1

Назначить пользователю: Goryunov G.G.

Компьютеры:

- ☒ Comp_1

USB-устройства

Применить

Назад

Рисунок 81 – Добавление новой учётной записи

Чтобы изменить параметры учётной записи, следует выделить ее и нажать кнопку <Редактировать> на вкладке «Учётные записи» (смотри рисунок 78). Появится окно, приведённое на рисунке 82.

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

Управление > Учетные записи > Редактировать

Описание учетной записи

Имя учетной записи: User_1

Имя пользователя: Goryunov

Полное имя пользователя: GoryunovGG@domen

Пароль:

Подтверждение пароля:

Пароль изменил: АИБ АИБ_SCM: 2020.06.04 12:30:07

Идентификатор: [01 00004A023221 E7]

Роль: EVERYONE_1

Назначить пользователю: Goryunov G.G.

Компьютеры: ☒ Comp_1

USB-устройства

Применить

Назад

Рисунок 82 – Редактирование учётной записи

При нажатии кнопки <USB-устройства> появится окно, приведённое на рисунке 83.

Индивидуальный список USB-устройств для учетной записи USER

Список всех USB-устройств в системе:

Vid	Pid	Серийный номер	Автостарт	Описание	Размещение
*	*	*	-	All	All
17E4	0003	00013833	-	ПСКЗИ ШИПКА	Port_#0002.Hub_#0005
A420	5426	*	-	Аккорд USB-считыватель TM	Port_#0002.Hub_#0006
041E	0401	*	-	Составное USB устройство	Port_#0001.Hub_#0003
046D	C077	*	-	USB-устройство ввода	Port_#0001.Hub_#0002
058F	6362	058F312D81B	-	Запоминающее устройство для USB	Port_#0003.Hub_#0008
072F	2224	*	-	ACR1281 1S Dual Reader Bus Driver	ACR1281U
0E0F	0001	*	-	VMware USB Device	Port_#0001.Hub_#0001
0E0F	0003	*	-	Составное USB устройство	VMware Virtual USB Mouse
072F	2224	*	-	ACR1281 1S Dual Reader Bus Driver	Port_#0001.Hub_#0001

Добавить

Список USB-устройств для учетной записи

Vid	Pid	Серийный номер	Автостарт	Описание	Размещение
17E4	0003	00013833	-	ПСКЗИ ШИПКА	Port_#0002.Hub_#0005
A420	5426	*	-	Аккорд USB-считыватель TM	Port_#0002.Hub_#0006

Удалить ☐ Не использовать индивидуальный список USB-устройств

Ok Отмена

Рисунок 83 - Настройка списка разрешённых USB-устройств для учётной записи

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

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

Для удаления USB-устройства из списка разрешённых USB-устройств учётной записи необходимо 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 в окне на рисунке 82.

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 82, 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 системы (выполняет Администратор РАУ согласно документу «11443195.4012-053 90. Руководство Администратора»). При выполнении процедуры удаления пользователя системы в параметрах учётных записей, назначенных данным пользователям, содержимое поля «Назначить пользователю» аннулируется.

ВНИМАНИЕ! В ASM реализована функция централизованной смены паролей учётных записей пользователей ПКО. Для этого необходимо во вкладке Учётные записи\Редактировать изменить пароль учётной записи пользователя ПКО, затем выполнить процедуру передачи базы пользователей на ПКО (подробнее смотри подраздел 4.6).

При изменении пароля пользователя ПКО в случае, если редактируется существующая учётная запись пользователя ПКО или если для редактируемой учётной записи назначены два и более ПКО, выводится сообщение о необходимости передачи обновленных баз пользователей на ПКО, приведенное на рисунке 84.

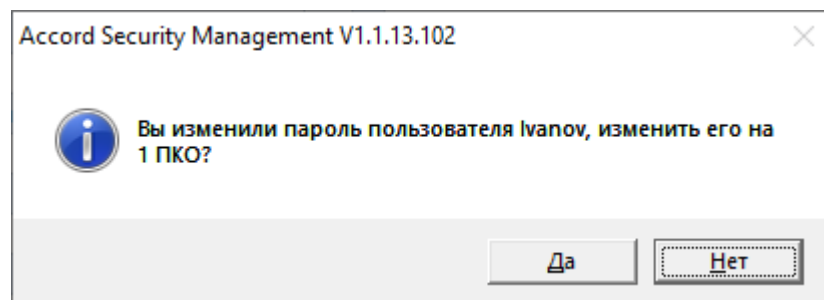


Рисунок 84 – Сообщение о необходимости передачи обновленных баз пользователей на ПКО

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

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

Базы учетных записей пользователей ПКО хранятся на СЦУ в каталоге C:\ASM\TEMPLATE\ (при удалении или обновлении ПО СЦУ базы учётных записей не удаляются).

Чтобы удалить учётную запись, необходимо выделить ее и нажать кнопку <Удалить> на вкладке «Учётные записи» (см. рисунок 78). Появится окно подтверждения этого действия, приведенное на рисунке 85.

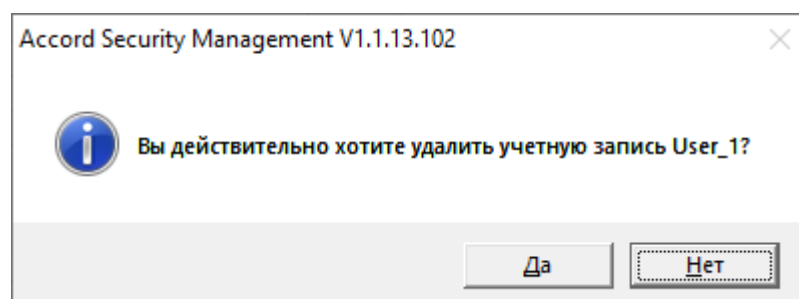


Рисунок 85 – Окно подтверждения удаления учётной записи

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.п. 4.3).

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»). При этом в параметрах учётных записей, назначенных компьютеру (п.п. 4.6), содержимое полей «Учётная запись» и «Пользователи» аннулируется.

Если необходимо определить, какой учётной записи принадлежит данный идентификатор, следует нажать кнопку <Поиск> на вкладке «Учётные записи» (см. рисунок 78). Появится окно с сообщением «Предъявите идентификатор», изображённое на рисунке 86.

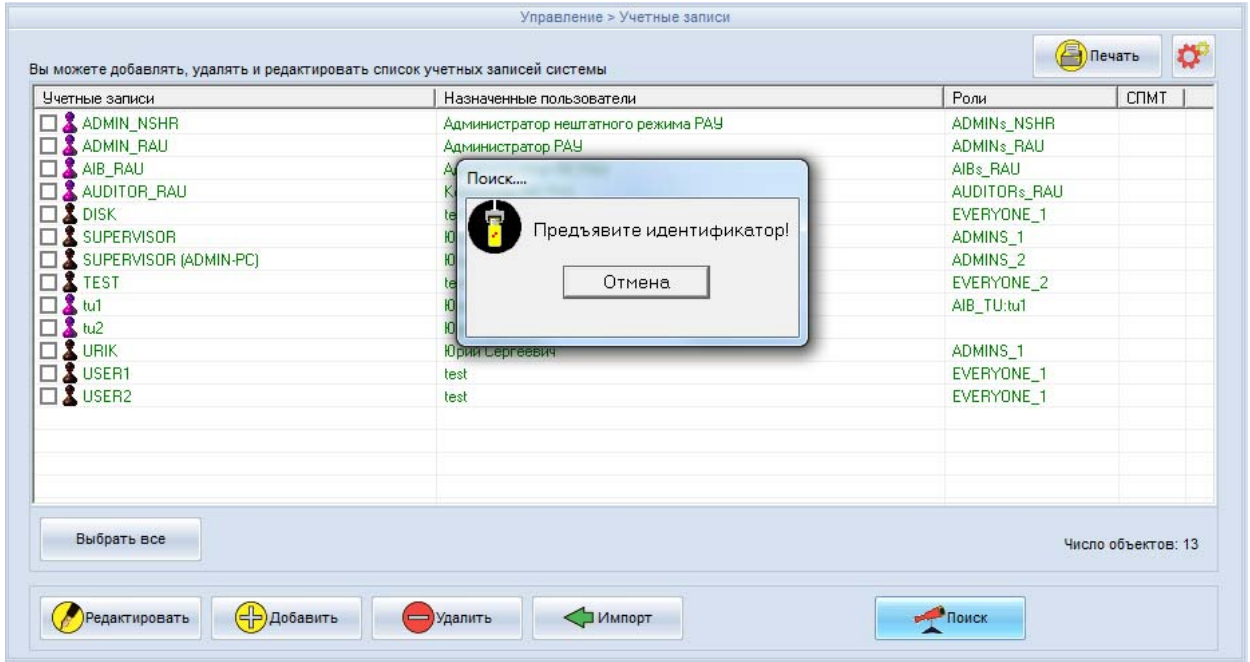


Рисунок 86 – Окно с сообщением «Предъявите идентификатор»

Если данный идентификатор назначен какой-либо учетной записи, то эта учетная запись будет выделена, как показано на рисунке 87.

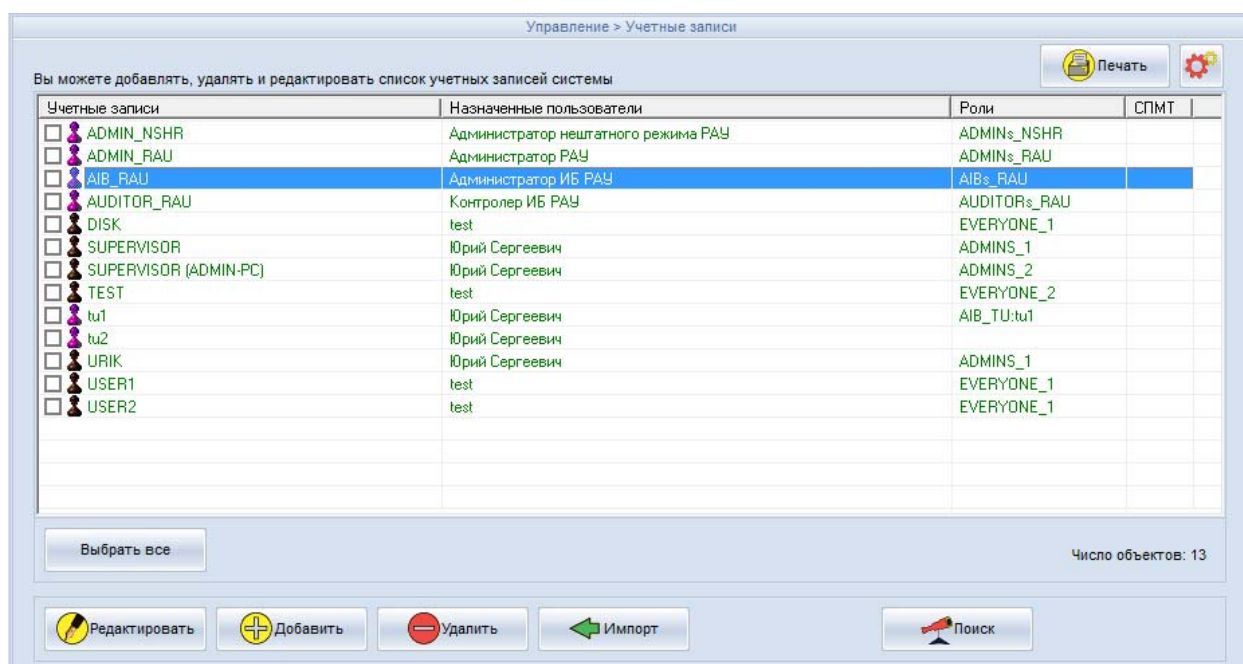


Рисунок 87 – Учетная запись, которой назначен идентификатор

В ином случае в нижней части окна появится сообщение «Идентификатор не зарегистрирован!», как показано на рисунке 86.

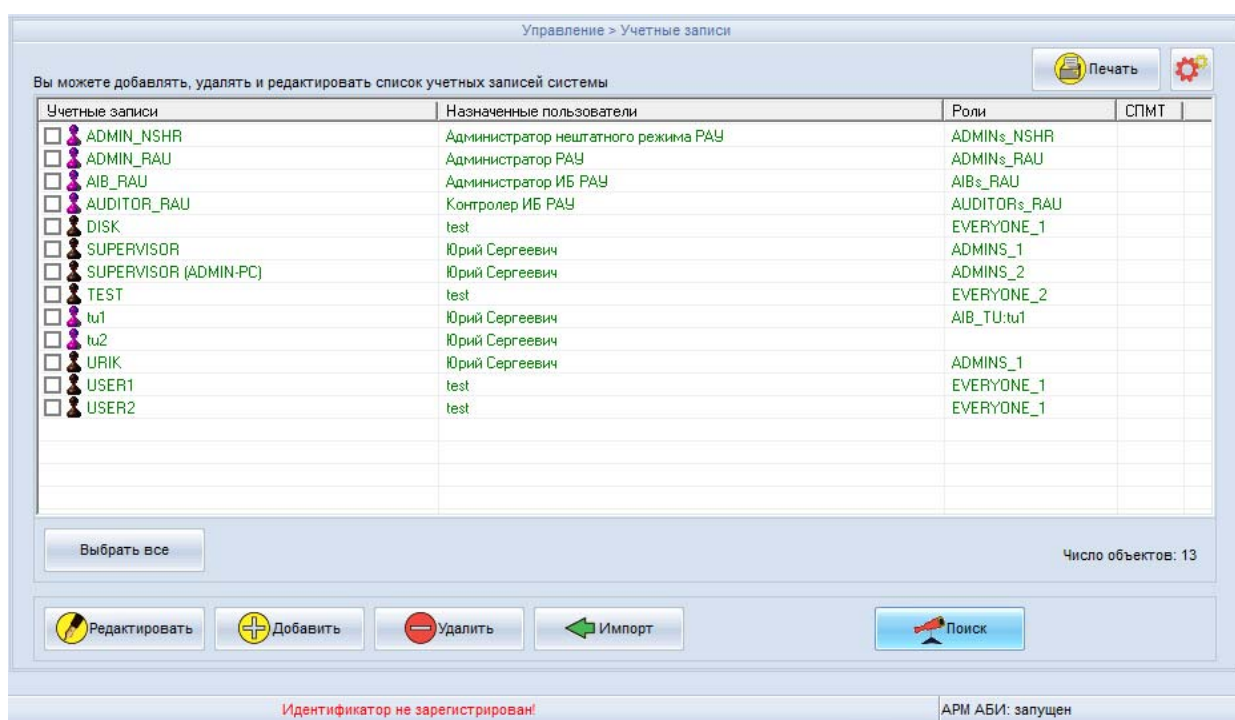


Рисунок 88 – Сообщение о том, что идентификатор не зарегистрирован

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 89). Далее в появившемся окне нужно выбрать кнопку <Изменить>.

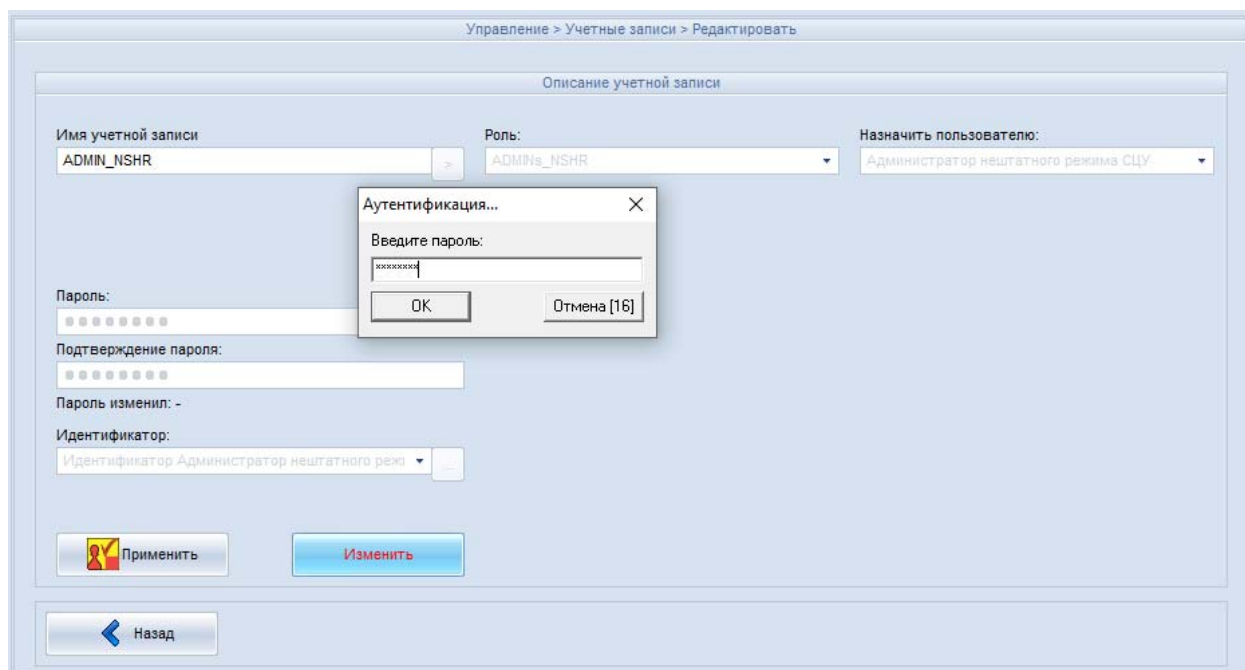


Рисунок 89 – Редактирование учетной записи Администратора НШР

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

- смена пароля Администратора НШР;
- выбор идентификатора для Администратора НШР (рисунок 90).

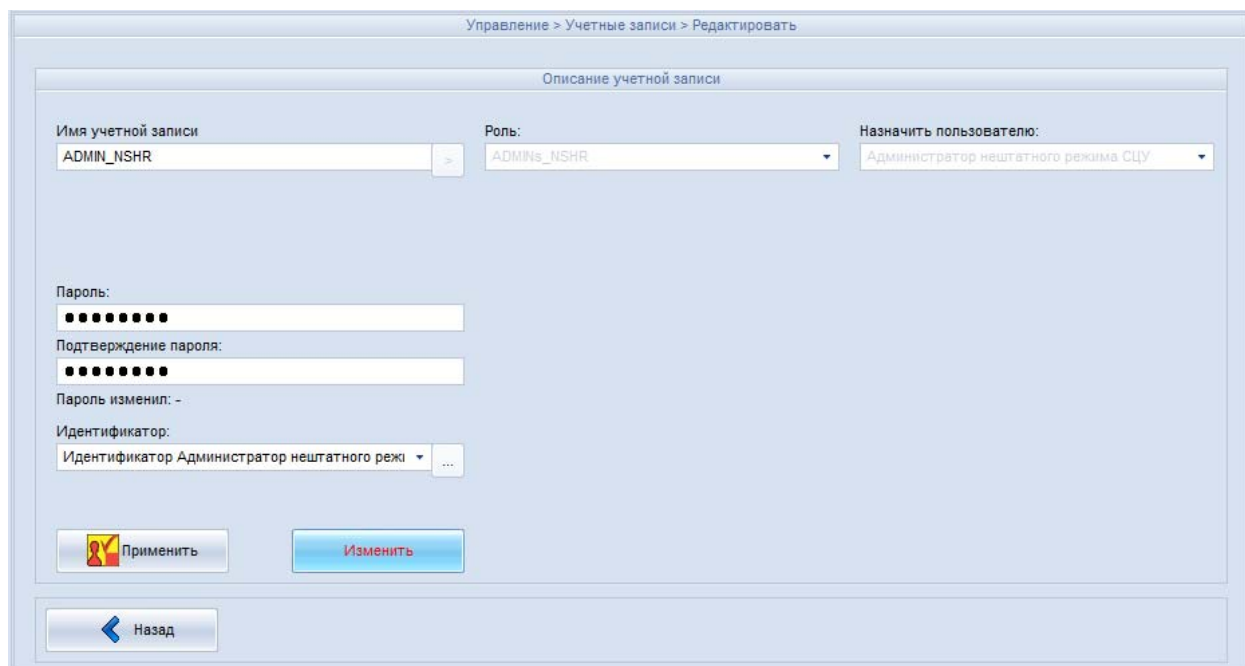


Рисунок 90 – Окно редактирования учётной записи Администратора НШР с доступными операциями смены пароля и идентификатора

После выполненных изменений нажать кнопку <Применить>. При ее нажатии появится сообщение о том, что учетная запись Администратора НШР изменена, приведенное на рисунке 91.

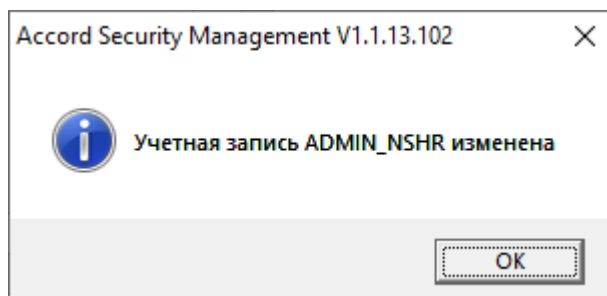


Рисунок 91 – Сообщение об изменении учётной записи Администратора НШР

Для получения данных об учётных записях пользователей ПКО в рамках централизованной схемы необходимо во вкладке «Учетные записи» нажать кнопку <Импорт> (рисунок 78). Далее в появившемся окне (рисунок 92) выбрать флаг «Вы можете импортировать учетные записи из:» - «базы пользователей NT».

После этого ввести IP-адрес или имя сервера, из базы пользователей которого будут импортированы учетные записи, а также имя и пароль Администратора данного сервера (рисунок 92).

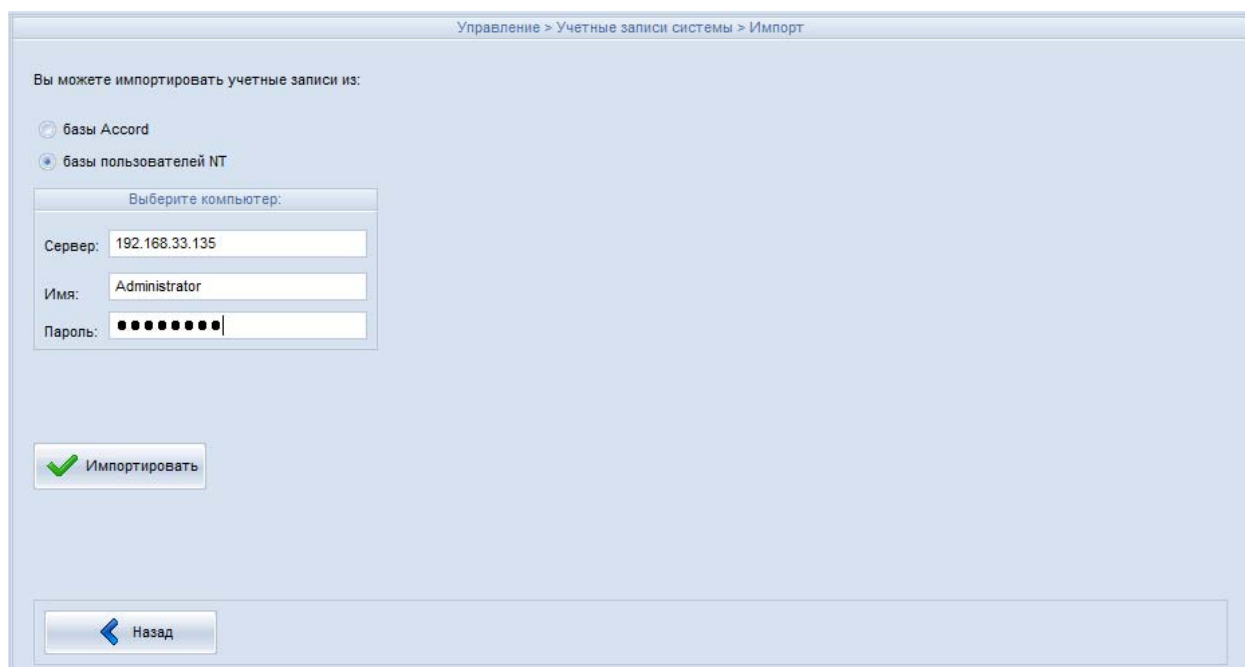


Рисунок 92 – Ввод данных о сервере, из базы пользователей которого будут импортированы учетные записи

После этого в правой части окна появятся импортированные учетные записи; следует выбрать из них необходимые для добавления в базу (для выбора всех

учетных записей нажать кнопку <Выбрать все>) и нажать кнопку <Добавить> (рисунок 93).

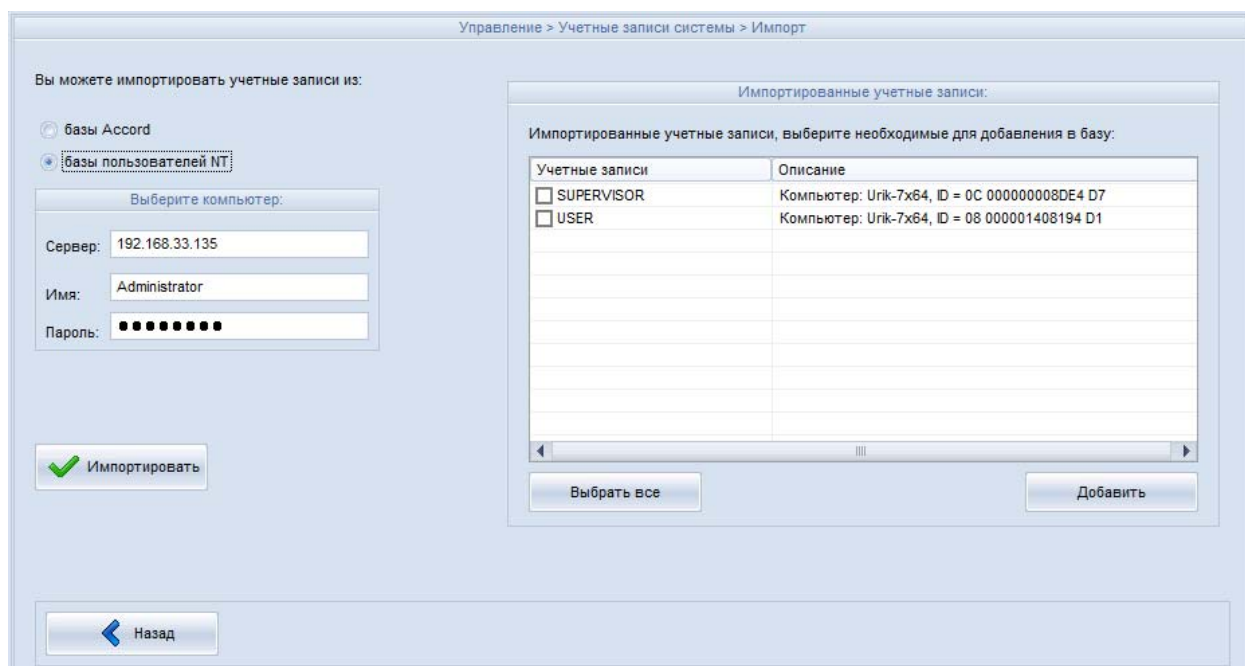


Рисунок 93 – Выбор импортированных учетных записей (импорт из базы пользователей NT)

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-накопитель, то перед тем, как выполнить процедуру получения баз пользователей ПКО в рамках децентрализованной схемы, необходимо добавить USB-накопитель в единую базу USB-носителей (эта процедура выполняется Администратором в соответствии с документом 11443195.4012-053 90 «СПО СЗИ НСД «Аккорд-РАУ». Руководство Администратора»).

Чтобы передать базы пользователей, необходимо на ПКО в трее выбрать правой кнопкой мыши сетевой клиент ПАК «Аккорд» (рисунок 68). Появляется контекстное меню (рисунок 69).

Далее выбрать команду «Экспорт базы пользователей» (рисунок 69).

Появляется сообщение «Введите идентификатор». Предъявить идентификатор Администратора «Аккорд» подконтрольного объекта.

Появится окно ввода пароля (см. рисунок 70). Ввести пароль и нажать ОК>.

Появляется окно выбора каталога для сохранения базы пользователей (рисунок 94). Выбрать нужный каталог и нажать кнопку <ОК>.

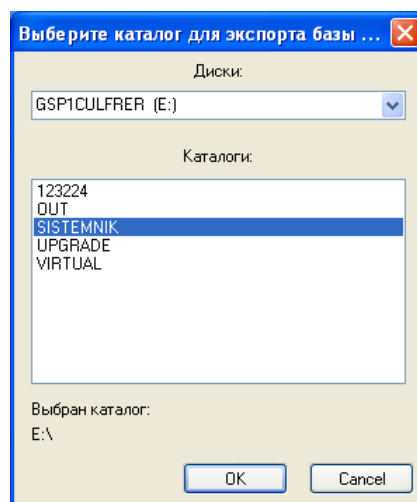


Рисунок 94 – Выбор каталога для сохранения базы пользователей

База пользователей экспортируется в каталог E:\IN\xxx\, где E – внешний носитель, xxx – имя ПКО. Каталог xxx содержит следующие файлы: xxx.AMZ – файл, в котором находится база пользователей ПКО, xxx.ini - файл, в котором содержатся параметры конфигурации ПКО, и www.act - файл, который содержит список задач, разрешенных для запуска пользователю (www – имя пользователя, для которого назначен список задач).

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

Если описанная процедура выполнена успешно, появляется сообщение, приведённое на рисунке 95.

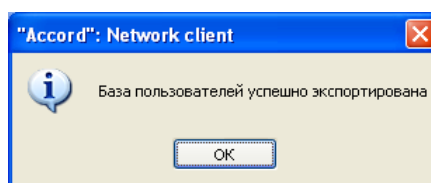


Рисунок 95 - Сообщение об успешном выполнении экспорта базы пользователей

Далее базы пользователей на внешнем носителе должны быть доставлены на СЦУ. Во вкладке «Учетные записи» СЦУ нажать кнопку <Импорт> (рисунок 78). В появившемся окне (рисунок 96) выбрать флаг «Вы можете импортировать учет-

ные записи из:» - «базы Accord» и нажать кнопку <Импортировать> (учетные записи при этом импортируются из каталога, E:\N\xxx\ xxx.AMZ, где E – внешний носитель, xxx – имя ПКО, xxx.AMZ – файл, в котором находится база пользователей ПКО).



Рисунок 96 – Импорт учетных записей из базы «Аккорда»

В появившемся окне (рисунок 97) следует указать файл с именем ПКО, с которого необходимо импортировать учетные записи.

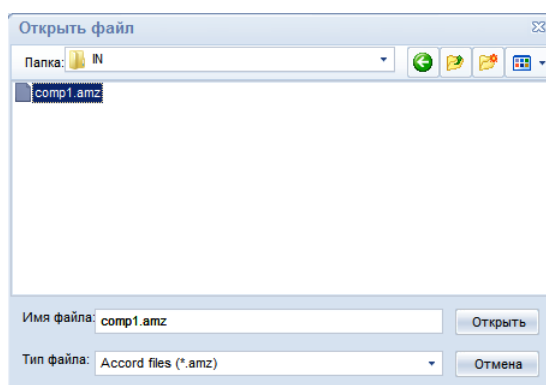


Рисунок 97 – Выбор файла *.amz, из которого необходимо импортировать учетные записи

После этого в правой части окна появятся импортированные учетные записи; следует выбрать из них необходимые для добавления в базу (для выбора всех учетных записей нажать <Выбрать все>) и нажать <Добавить> (рисунок 98).

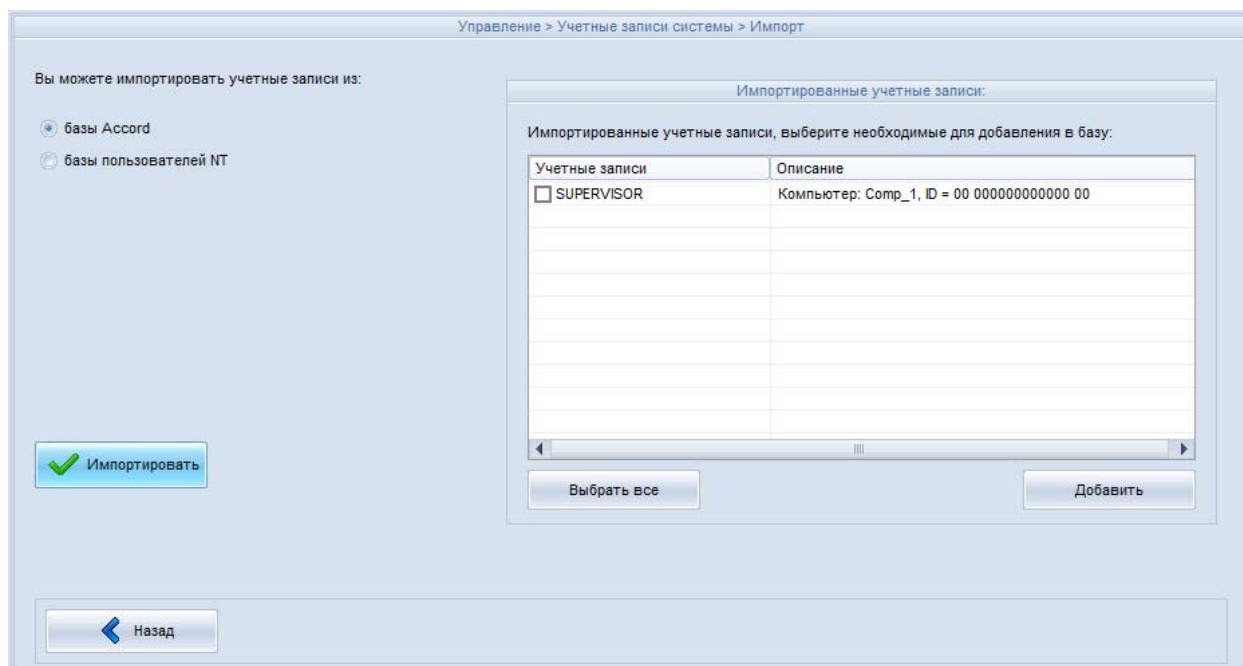


Рисунок 98 – Выбор импортированных учетных записей (импорт из базы «Аккорда»)

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.

4.8 Работа с журналами

4.8.1 Общие сведения

В РАУ существуют журналы трех типов:

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

4.8.2 Оперативный журнал

4.8.2.1 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/YYYY/, где XXX – имя каталога, соответствующего имени ПКО, YYYY – 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 при 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 99.

С помощью элементов интерфейса этого окна Администратор ИБ технологического участка выполняет следующие функции:

- просмотр сообщений оперативного журнала на СЦУ. Функция описана в пункте 4.8.2.2;
- конвертирование оперативного журнала. Функция описана в пункте 4.8.2.3;
- экспортирование оперативного журнала. Функция описана в пункте 4.8.2.4;
- импортирование оперативного журнала. Функция описана в пункте 4.8.2.5.

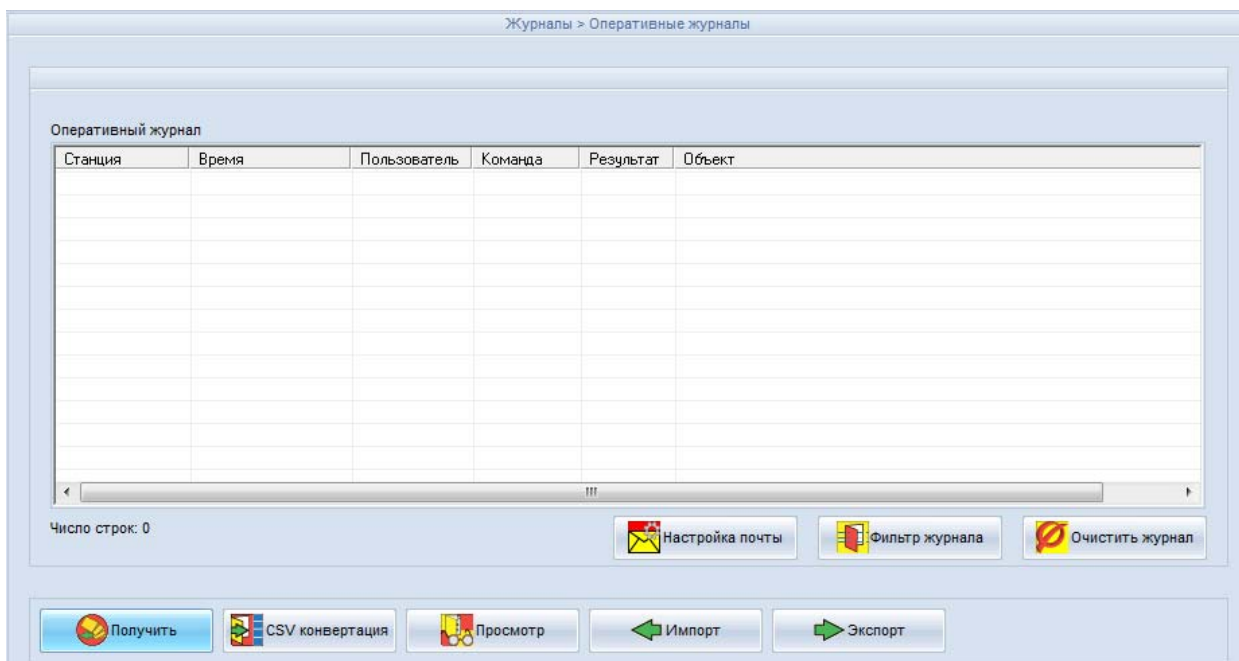


Рисунок 99 - Оперативные журналы

4.8.2.2 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 в окне, приведённом на рисунке 99, нажать кнопку <Просмотр>. Появляется окно выбора журналов, приведённое на рисунке 100.

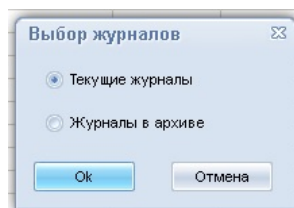


Рисунок 100 - Выбор журналов для просмотра

В данном окне осуществляется выбор журналов для просмотра: пункт «Текущие журналы» позволяет выбрать файлы журналов в каталоге \Asm\AcConNet\Client.Log, пункт «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 101.

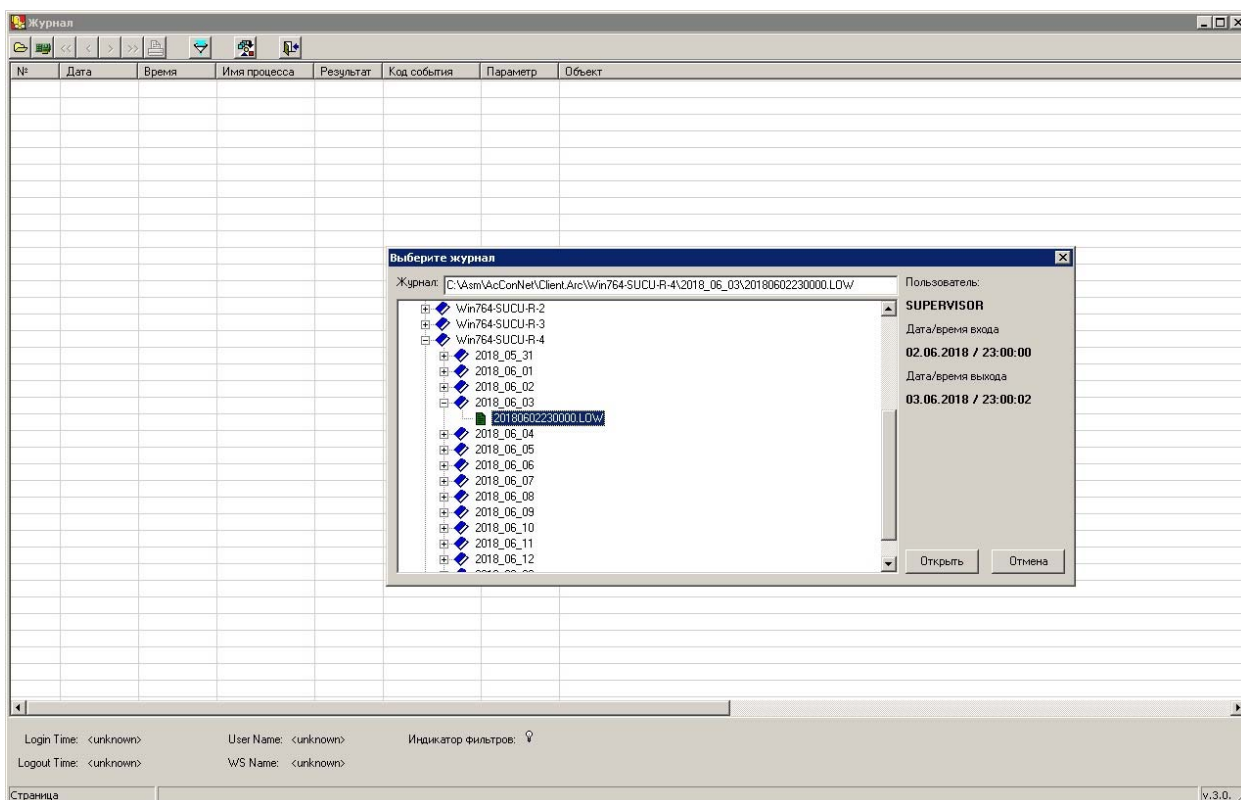


Рисунок 101 - Окно просмотрщика журналов событий

4.8.2.3 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 в окне, приведенном на рисунке 99, 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.

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

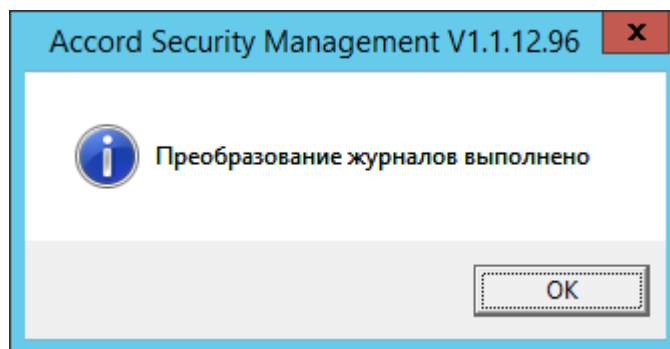


Рисунок 102 – Сообщение о выполненной процедуре конвертации оперативного журнала в общепринятые форматы

При выполнении процедуры конвертации оперативного журнала кнопками <CSV конвертация> или <XML конвертация> в консоли AsmT.exe информация о выполненной процедуре конвертации оперативного журнала (дата и время запуска и окончания процедуры конвертации, список конвертированных файлов оперативного журнала) записывается в журнал Low2XmlCsv.log (рисунок 103).

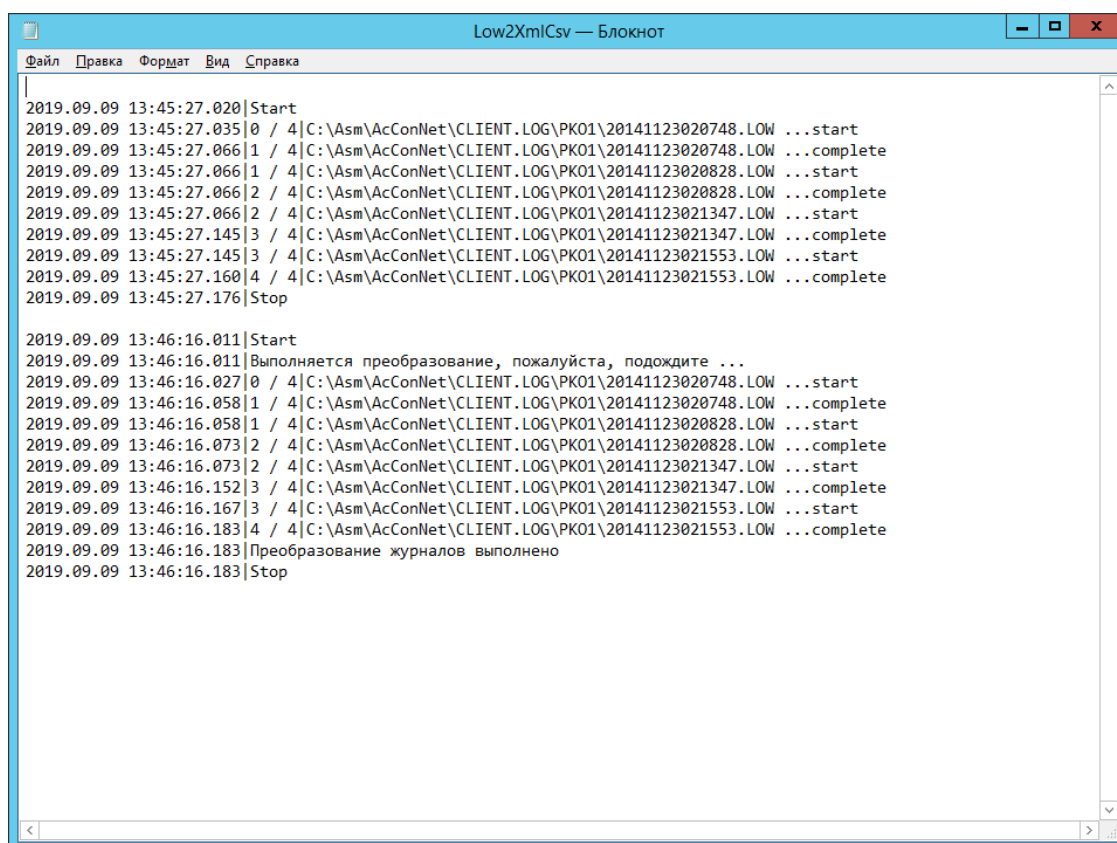


Рисунок 103 – Журнал Low2XmlCsv.log после выполнения процедуры конвертации кнопками <CSV конвертация> или <XML конвертация> в консоли AsmT.exe

Процедуру конвертации оперативного журнала также можно выполнить с помощью утилиты Low2XmlCsv.exe⁷. Информация о выполненной процедуре также записывается в журнал Low2XmlCsv.log⁸ (однако при этом в журнале не отображаются сообщения о начале и окончании выполнения преобразования журналов, рисунок 104).

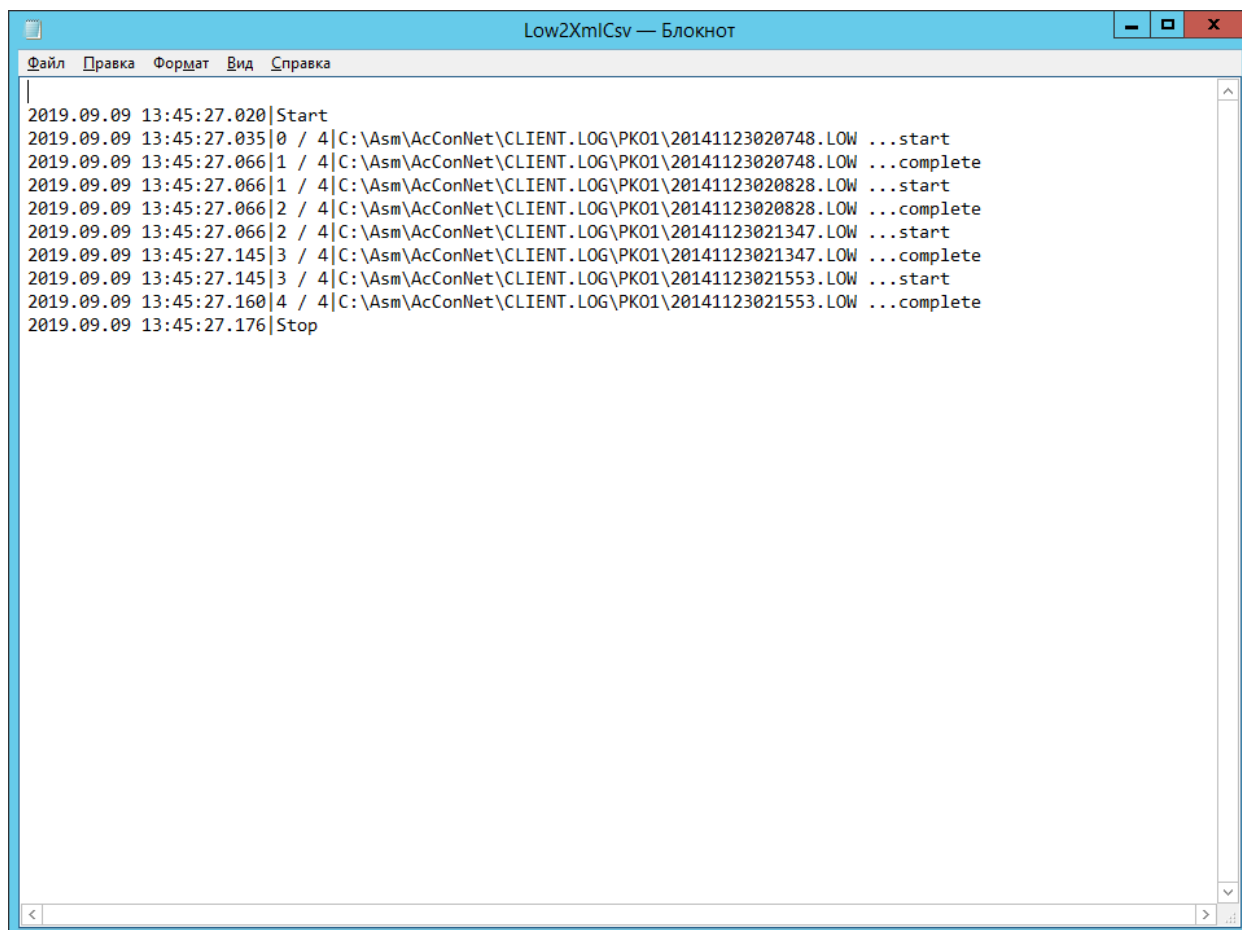


Рисунок 104 - Журнал Low2XmlCsv.log после выполнения процедуры конвертации утилитой LowToCsvXml.exe

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 на экране появится следующее сообщение:

⁷ Утилита находится в каталоге C:\Asm.

⁸ После каждой последующей конвертации оперативного журнала информация о процедуре добавляется в файл журнала Low2XmlCsv.log.

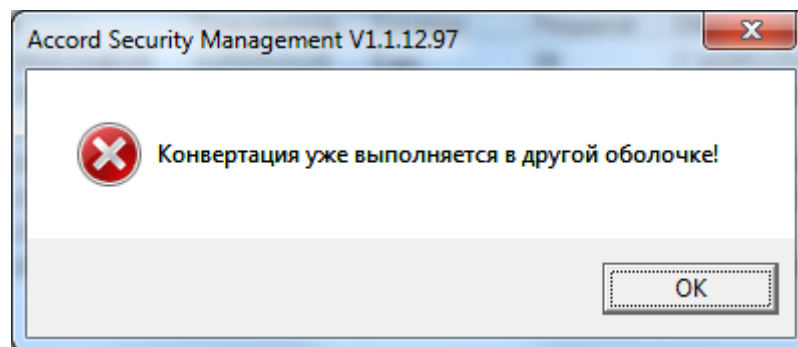


Рисунок 105 – Сообщение о невозможности запуска консоли при выполнении процедуры конвертации

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».

4.8.2.4 Экспортирование оперативного журнала

Чтобы экспортировать оперативный журнал (например, для дальнейшего анализа в системах мониторинга), необходимо в окне, приведённом на рисунке 99, нажать кнопку <Экспорт>. После этого на экране появляется окно выбора каталога. Выбрав каталог для экспорта журнала, следует нажать кнопку <Применить>.

4.8.2.5 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 носителя USB-носителя 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 99, нажимает кнопку <Импорт>;
- в появившемся окне выбирает необходимый каталог и нажимает кнопку <Применить>.

4.8.3 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 106.

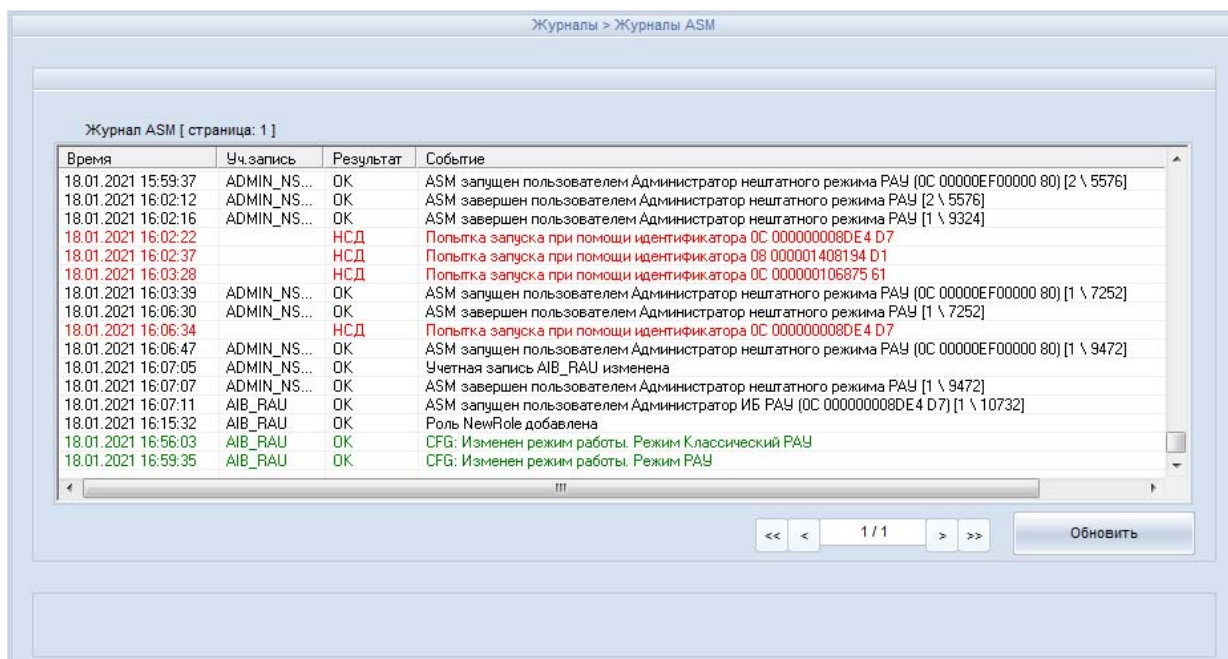


Рисунок 106 - Журнал ASM

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» отображается 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 6.

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 6;
- символ «|»;
- имя учётной записи.

4.8.4 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 на СЦУ может изменяться путём задания параметра ServiceLogLevel в конфигурационном файле AcCon32.ini на СЦУ. Конфигурационный файл AcCon32.ini описан в подразделе 9.2. Уровень детализации журналов АРМ АБИ на ПКО может изменяться путём задания параметра ServiceLogLevel в конфигурационном файле AcWs32.ini на данном ПКО.

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 данном поле приводится информация, детализирующая возникшие ошибки. Все возможные значения поля «Примечание» приведены в разделе 8.

Окно, отображающее журнал АРМ АБИ, приведено на рисунке 107.

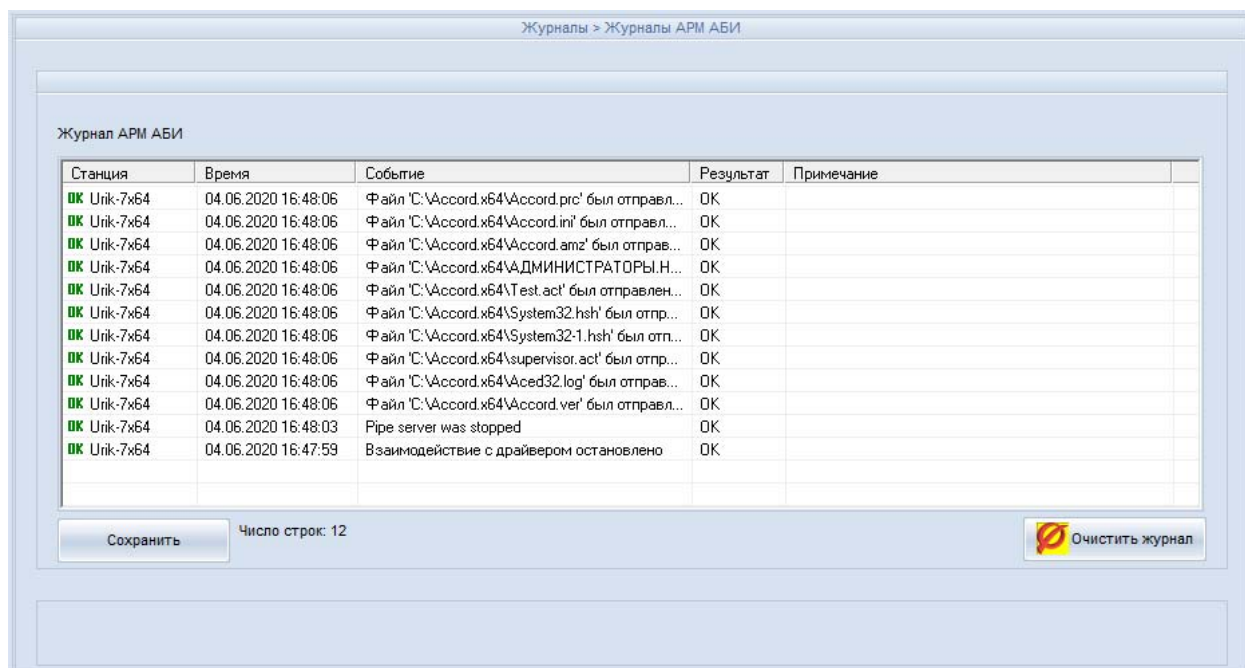


Рисунок 107 – Журнал АРМ АБИ

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.

Журнал АРМ АБИ можно сохранить в текстовый файл. Для этого необходимо в окне, приведённом на рисунке 107, нажать кнопку <Сохранить>. В появившемся окне сохранения файла задать имя файла, в который будет сохранён журнал АРМ АБИ, и нажать кнопку <Сохранить>.

4.9 Настройка ASM

4.9.1 Основные настройки

На рисунке 108 показана панель для задания основных настроек ASM, которая выводится на экран после открытия вкладки «Настройка -> Основные настройки».

С помощью этой вкладки имеется возможность:

- выполнить настройку учётной записи ASM;
- управлять включением/отключением механизма синхронизации учетных записей РАУ с пользователями Аккорд;
- выполнить настройку режимов работы РАУ.

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 учётной записью, то при запуске ASM нужно нажать и удерживать клавишу <Shift>.

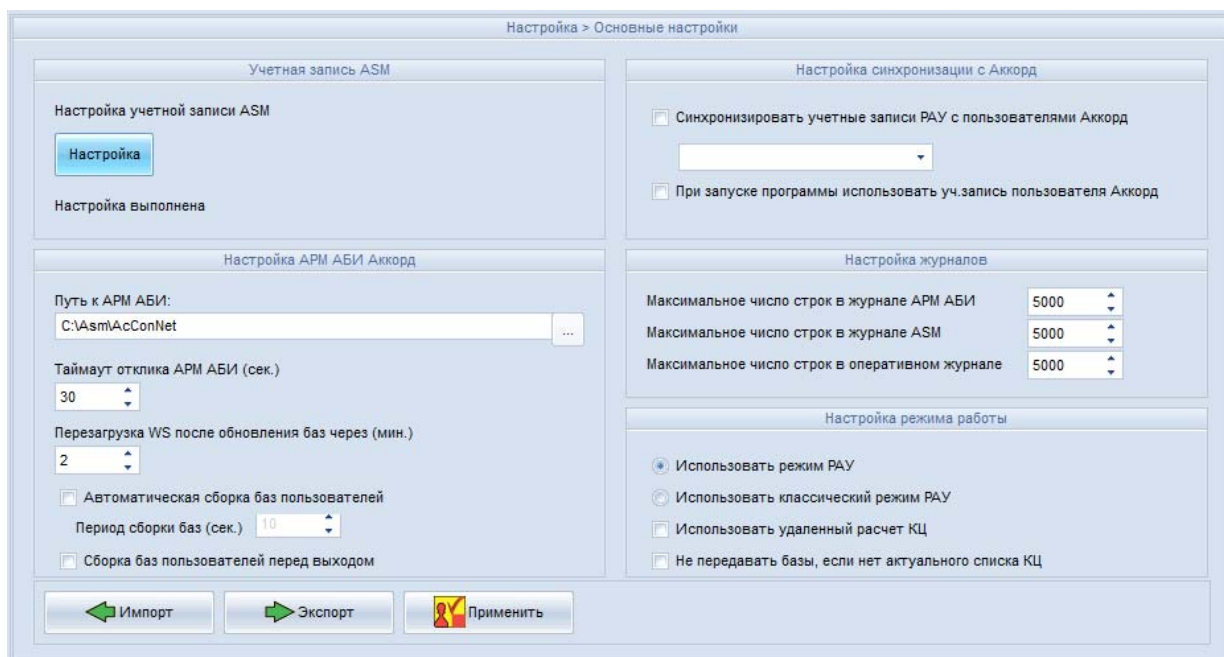


Рисунок 108 – Основные настройки ASM

Непрерывность процесса сборки баз обеспечивает установка флага «Не передавать базы, если нет актуального списка КЦ». Если данный флаг установлен, то при возникновении ошибок (в процессах формирования и передачи баз) процесс сборки остановлен не будет, а список файлов для контроля целостности и их эталонные контрольные суммы будут взяты из файла ...\\Asm\\AcConNet\\In\\CompName\\CompName.amz (при этом в журнал ASM запишется предупреждающая информация).

Если установлен флаг «Использовать удаленный расчет КЦ», то (на СЦУ) разрешено удаленное формирование списка контролируемых на выбранном ПКО файлов.

Для сохранения настроек нажать кнопку <Применить>.

ВНИМАНИЕ! Средствами ASM реализована возможность создания (или удаления) в базе пользователей СЗИ от НСД «Аккорд» учётной 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 СЦУ во вкладке «ASM > Настройка > Основные Настройки» в поле «Настройка синхронизации с Аккорд» поставить флажок «Синхронизировать учетные записи СЦУ 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 СЦУ необходимо выполнить процедуру настройки контроля целостности и правил разграничения доступа к собственному ПО. Для этого необходимо с использованием утилиты make.prc:

- установить полный доступ к каталогу установки ПО СЦУ (по умолчанию C:\ASM) только 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 СЦУ.

4.9.2 Настройка фильтров оперативного журнала

Настройка фильтров оперативного журнала осуществляется во вкладке «Настройка > Оперативный журнал», которая приведена на рисунке 109.

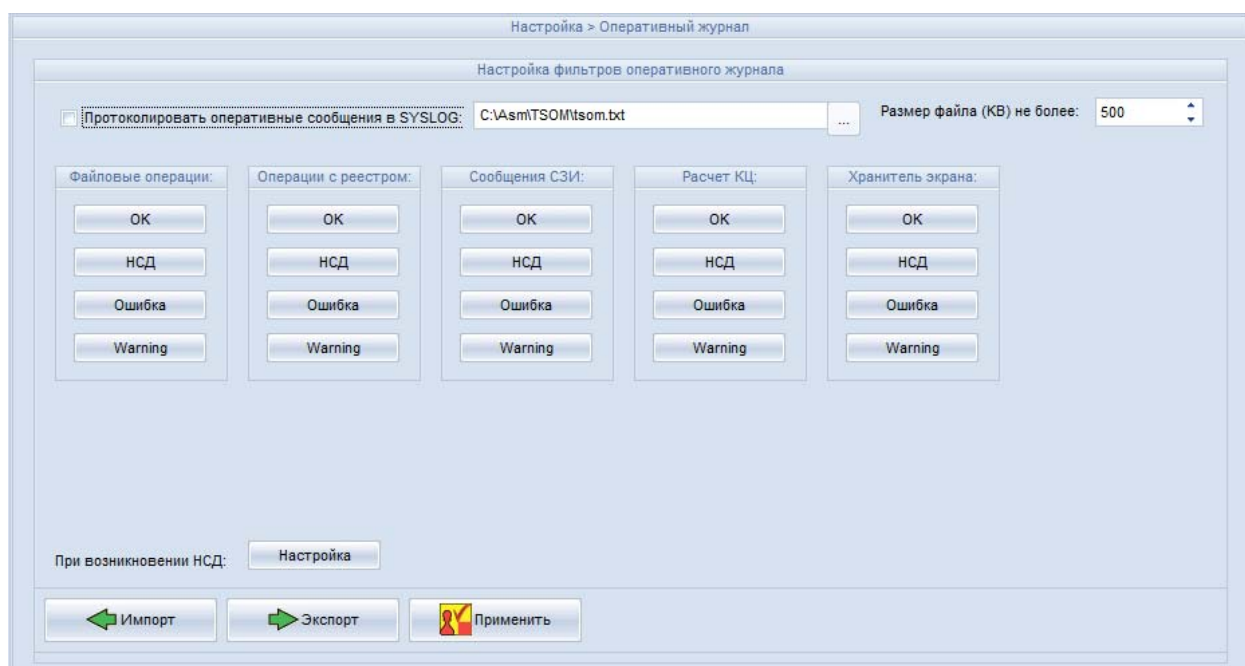


Рисунок 109 – Настройка фильтров оперативного журнала

Для сохранения выполненных настроек необходимо нажать кнопку <Применить>.

Для экспорта настроек в файл Администратору нужно нажать кнопку <Экспорт>. При ее нажатии появится окно выбора каталога, в который будет выполнен экспорт настроек. Настройки экспортируются в файл с именем «ASM.CFG».

Для восстановления настроек необходимо во вкладке «Настройка > Основные настройки» нажать кнопку <Импорт>. Появится окно выбора каталога. Нужно выбрать каталог, в котором находится файл с сохраненными настройками «ASM.CFG».

В качестве механизма передачи информации о критичных событиях ИБ используется журнал SYSLOG: СЦУ помещает полученную от ПКО информацию о критических событиях в журнал приложения Application ASM СЦУ. Для этого необходимо во вкладке Настройка > Оперативный журнал, приведённой на рисунке 109, установить флажок «Протоколировать оперативные сообщения в SYSLOG».

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

Существует возможность запускать заданное приложение при возникновении НСД. Для этого нажать кнопку <Настройка> в поле «При возникновении НСД» во вкладке Настройка > Оперативный журнал (рисунок 109).

При ее нажатии появится окно, приведённое на рисунке 110, позволяющее настроить реакцию РАУ при возникновении НСД. Реакцией РАУ на НСД может являться следующее:

- запуск заданного приложения;
- вывод на экран сообщения об НСД для Администраторов ИБ;
- вывод на экран сообщения об НСД для Контролеров;
- вывод на экран сообщения об НСД для Операторов ИБ;
- информирование о ситуациях НСД Администраторов ИБ по электронной почте.

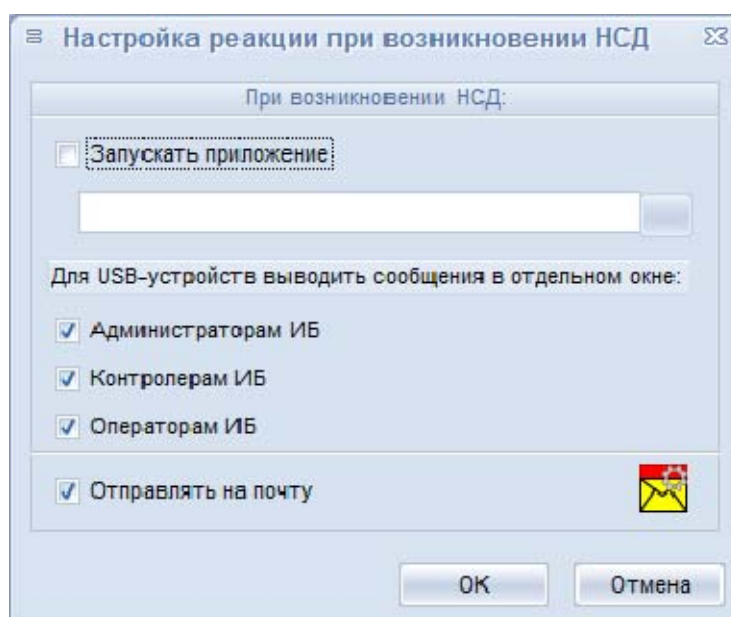


Рисунок 110 – Настройка реакции при возникновении НСД

При выборе информирования о ситуациях НСД по электронной почте можно настроить глобальный или индивидуальный механизм передачи информации о событиях НСД. Для настройки глобального механизма следует нажать значок  ('Настройка почтового клиента') в строке «Отправлять на почту» и заполнить необходимые поля в появившемся окне настройки (рисунок 111).

Настройка электронной почты

Данные отправителя:

Хост (smtp-сервер): smtp.mail.ru Логин пользователя: UserName

Порт: 465 Пароль пользователя: ●●●●●●●●

Адрес e-mail: UserName@mail.ru

Данные получателя:

Адрес e-mail: me2@mail.ru

Содержимое письма:

Заголовок: Сообщение от РАУ

ТЕСТ ОК Отмена

Рисунок 111 – Окно настройки электронной почты

Если 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 всех ПКО в системе. Классы передаваемых событий можно выбрать в окне настройки фильтров оперативного журнала (рисунок 109). При нажатии на кнопку <ТЕСТ> происходит отправка тестового письма.

При необходимости настроить индивидуальный почтовый адрес для отдельного ПКО следует отметить поле «Отправлять на почту» (рисунок 110) и далее на вкладке Журналы > Оперативные журналы (рисунок 99) нажать кнопку <Настройка почты>. При ее нажатии появится окно настройки индивидуальной почты (рисунок 112). Если поле «Хост (smtp-сервер)» в этом окне 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 кнопки <Фильтр журнала> (рисунок 99) появится окно настройки фильтров, в котором можно выбрать типы передаваемых событий (рисунок 113).

Рисунок 112 – Окно настройки индивидуальной почты для передачи событий НСД

Рисунок 113 – 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.

ВНИМАНИЕ! Если в файле `Asm.ini` присвоено значение параметру `OnWhatNameMaxLen=NUMBER_OF_BYTES` (где `NUMBER_OF_BYTES` – количество байт), то при записи информации о событии в поле `OnWhatName` файла формата `*.csv` данная информация (название события или путь) обрезается до указанного количества байт. При этом в поле `Info` файла формата `*.csv` записывается полная информация о событии.

4.9.3 Настройка фильтров экспорта журналов

Для настройки фильтров экспорта журналов следует выбрать вкладку «Настройка > Экспорт журналов». Появится окно, приведённое на рисунке 114. В данном окне нужно установить необходимые флажки в группах «Результат выполнения» для файловых операций и операций с реестром, для сообщений СЗИ, сообщений АМДЗ, расчета КЦ и хранителя экрана.

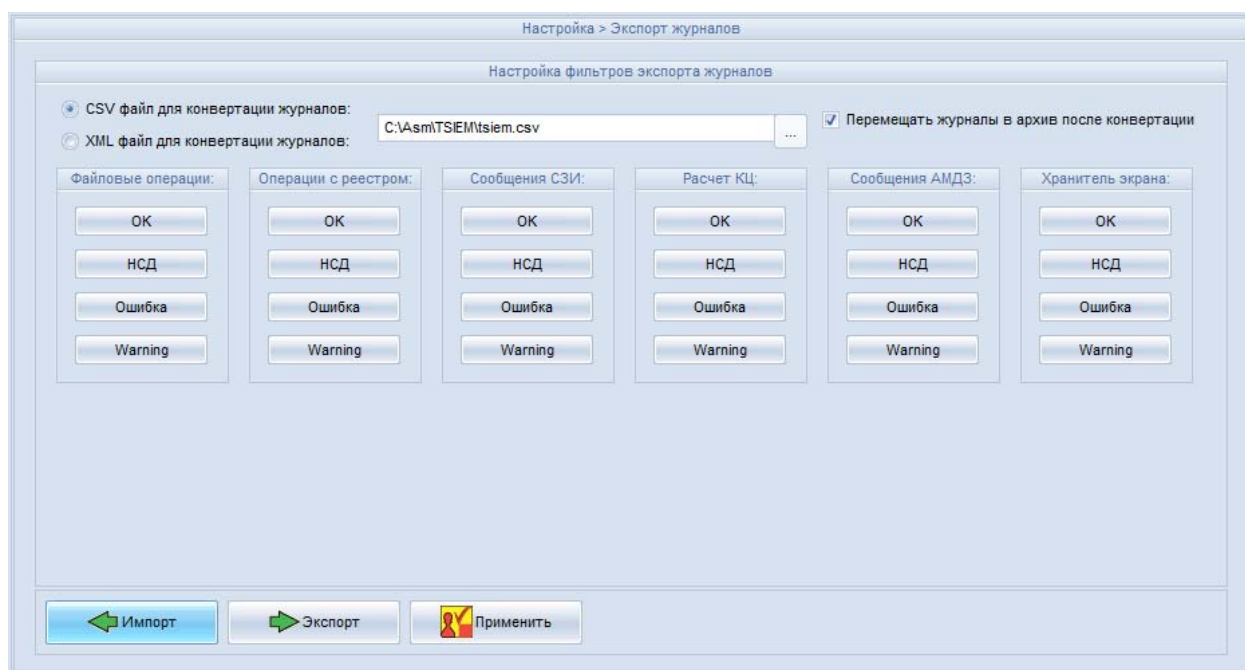


Рисунок 114 – Настройка фильтров экспорта журналов

Для сохранения выполненных настроек нажать кнопку <Применить>.

Для экспорта настроек в файл нажать кнопку <Экспорт>. При ее нажатии появится окно выбора каталога, в который будет выполнен экспорт настроек. Настройки экспортируются в файл с именем «ASM.CFG».

Для восстановления настроек необходимо во вкладке «Настройка > Основные настройки» нажать кнопку <Импорт>. Появится окно выбора каталога. Нужно выбрать каталог, в котором находится файл с сохраненными настройками «ASM.CFG».

5 Перечень оповещающих сообщений

Оповещающие сообщения выводятся 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 длина 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 сервере централизованного управления 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 сервере централизованного управления 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 между 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 съёмнику информации	Снова приложите ТМ-идентификатор к съёмнику 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 СЦУ при первом его запуске не была сразу же выполнена предварительная настройка сетевого идентификатора (смотри подраздел 3.3)	Выполнить предварительную настройку сетевого идентификатора и запустить службу AcConNet

6 Перечень сообщений журнала ASM

Перечень сообщений журнала 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, Маркировка печати, Блокировка клипборда, Может изменять дату/время, Запрет доступа к общим ресурсам, Полный доступ для APM АБИ, 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 106. В файле журнала сообщения фиксируются в структуре, описанной в пункте 4.8.2.1.

Таблица 4 – Перечень сообщений журнала 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

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	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
	Компьютеры WSNNAME успешно добавлены в базу	Процедура импорта ПКО WSNNAME 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

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	ASM завершен пользователем USERNAME [FRAMENAME]	Выполнено завершение работы ASM	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	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 WSNAMЕ удален	Процедура удаления 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
	Тех. участок FRAME_NAME удален	Процедура удаления тех. участка выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Учетная запись ACCOUNT_NAME удалена	Процедура удаления учетной записи выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Роль ROLE_NAME удалена	Процедура удаления роли ROLE_NAME выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	USB USB_NAME удален	Процедура удаления USB-устройства USB_NAME выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Идентификатор ID_NAME 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

Тип сообщения	Сообщение	Действия, при кото- рых генерируется со- общение	Действия, которые необходимо предпри- нять при появлении со- общения
	USB-устройство успешно добавлено в базу	Процедура добавления USB-устройства в базу ASM выполнена успеш- но	Данное сообщение ин- формирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	USB-устройство уже есть в базе, обновле- но!	В ходе выполнения до- бавления USB- устройств в базу оказа- лось, что одно USB- устройство уже есть в базе. USB-устройство в базе переписано на но- вое	Данное сообщение ин- формирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Роль ROLENAME из- менена	Процедура редактиро- вания роли выполнена успешно	Данное сообщение ин- формирует 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. 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 сделанные изменения	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	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

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	Роль ROLENAME изменена. Стартовая задача 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 [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
	Роль ROLENAME изменена. Детальность журнала 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

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	Роль ROLENAME изменена. Хранитель экрана (время) было 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
	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

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	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
	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

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	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 WSNNAME изменен	Процедура редактирования компьютера выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Компьютер WSNNAME изменен, новый TY 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 WSNNAME добавлен	Процедура добавления компьютера 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
	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
	Созданы базы: WSNAMES	Процедура создания баз *.amz выполнена успешно. В результате выполнения данной процедуры на компьютере WSNAMES 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

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	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
	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

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	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
	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

Тип сообщения	Сообщение	Действия, при кото- рых генерируется со- общение	Действия, которые необходимо предпри- нять при появлении со- общения
	Изменены мандатные метки для ПКО WSNAME. Список объектов изменен	Процедура редактиро- вания меток мандатного доступа для пользова- телей ПКО WSNAME выполнена успешно	Данное сообщение ин- формирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Учетная запись ACCOUNTNAME1 переименована в ACCOUNTNAME2	Процедура редактиро- вания параметров учетной записи выпол- нена успешно	Данное сообщение ин- формирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Добавлен объект OBJECTNAME [ACCESS_CONTROL]	Процедура добавления, удаления или измене- ния объекта	Данное сообщение ин- формирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Удален объект OBJECTNAME [ACCESS_CONTROL]	OBJECTNAME выпол- нена успешно. Данным сообщениям обяза- тельно предшествует	
	Изменен объект OBJECTNAME [ACCESS_CONTROL]	сообщение «Роль ROLENAME изменена. Список объектов изме- нен», в котором указы- вается для какой роли добавлен, удален или изменен объект	
	WSNAME Пользова- тель USERNAME из- менил пароль	Процедура смены па- роля пользователя ПКО (посредством команды Ctrl-Alt-Del -> «Сменить пароль») выполнена успешно	Данное сообщение ин- формирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно

Тип сообщения	Сообщение	Действия, при кото- рых генерируется со- общение	Действия, которые необходимо предпри- нять при появлении со- общения
	WSNAME Отправле- на база пользовате- лей. Успешно	Процедура отправки базы пользователей выполнена успешно	Данное сообщение ин- формирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	WSNAME Отправле- на база пользовате- лей [Аккорд не акти- вирован]. Успешно	Процедура отправки базы пользователей выполнена успешно	Данное сообщение ин- формирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	WSNAME Отправле- на база пользовате- лей [отложенная]. Успешно	Процедура отправки базы пользователей после включения ПКО выполнена успешно	Данное сообщение ин- формирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	WSNAME Отправле- на база пользовате- лей [отложенная] *.amz *.ini *.act *.prc. Успешно	Процедура отправки базы пользователей после включения ПКО выполнена успешно	Данное сообщение ин- формирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Базы модифицирова- ны другим админи- стратором. Обновле- ны	Динамическое обнов- ление баз пользовате- лей выполнено успешно	Данное сообщение ин- формирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно

Тип сообщения	Сообщение	Действия, при кото- рых генерируется со- общение	Действия, которые необходимо предпри- нять при появлении со- общения
	Базы актуальны	Выполнено динамиче- ское обновление баз пользователей. Модификаций баз со сторо- ны других учетных за- писей управляющего персонала не выявлено	Данное сообщение ин- формирует о том, что ба- зы пользователей нахо- дятся в актуальном со- стоянии. Никаких дей- ствий при его появлении выполнять не нужно
	Пользователи успеш- но импортированы из базы NT [SERVERNAME]	Процедура импорта пользователей из базы NT выполнена успешно	Данное сообщение ин- формирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Пользователи успеш- но импортированы из базы Accord-a [WSNAME.amz]	Процедура импорта пользователей из базы ПАК «Аккорд» выпол- нена успешно	Данное сообщение ин- формирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Идентификаторы успешно импортиро- ваны из базы Accord- a [WSNAME.amz]	Процедура импорта идентификаторов из базы Accord-a выпол- нена успешно	Данное сообщение ин- формирует 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] выпол- нена успешно	Данное сообщение ин- формирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно

Тип сообщения	Сообщение	Действия, при кото- рых генерируется со- общение	Действия, которые необходимо предпри- нять при появлении со- общения
	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
	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

Тип сообщения	Сообщение	Действия, при кото- рых генерируется со- общение	Действия, которые необходимо предпри- нять при появлении со- общения
	USB-устройства успешно импортиро- ваны из базы Accord- а [WSNAME.amz]	Процедура импорта USB-устройств из базы ПАК «Аккорд» выпол- нена успешно	Данное сообщение ин- формирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Роли успешно добав- лены в базу	Процедура импорта ро- лей, используемых на ПКО, в базу ASM вы- полнена успешно	Данное сообщение ин- формирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Процесс ACCONNET.EXE пе- резапущен	Выполнен автоматиче- ский перезапуск ACCONNET.EXE после его сбоя	При частом появлении данного сообщения (бо- лее пяти раз за сутки) необходимо обратиться в службу технической под- держки ЗАО «ОКБ САПР»
	WSNAME Передача базы. База поставле- на в очередь переда- чи на ПКО	Во время выполнения процедуры передачи баз пользователей на ПКО WSNAME служба AcConNet была загру- жена. По истечении не- которого времени база пользователей автома- тически передается на ПКО	Данное сообщение ин- формирует 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 создана и подготовлена для передачи на ПКО	Во время выполнения процедуры передачи базы пользователей ПКО WSNAME выключен. База пользователей автоматически передается 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
	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

Тип сообщения	Сообщение	Действия, при кото- рых генерируется со- общение	Действия, которые необходимо предпри- нять при появлении со- общения
	WSNAME Передача базы. База передана на ПКО [Аккорд не активирован]	Процедура передачи базы пользователей на ПКО WSNAME, на кото- ром не активирована система защиты ПАК «Аккорд», выполнена успешно	Данное сообщение ин- формирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Экспорт успешно за- вершен	Процедура экспорта журналов событий вы- полнена успешно	Данное сообщение ин- формирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Импорт успешно за- вершен	Процедура импорта журналов событий вы- полнена успешно	Данное сообщение ин- формирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	Экспорт настроек успешно завершен	Процедура формирова- ния шаблонов настроек выполнена успешно	Данное сообщение ин- формирует 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 ин- формирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
Сообщения об изменении параметров конфигурации ASM (со-	CFG: Включена синхронизация учетных записей РАУ с пользо- вателями Аккорд	Установлен флаг «Синхронизация учетных записей РАУ с пользо- вателями Аккорд»	Никаких действий выпол- нять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
общения с префиксом CFG). Сообщения данного типа фиксируются в журнале ASM	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
	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

Тип сообщения	Сообщение	Действия, при кото- рых генерируется со- общение	Действия, которые необходимо предпри- нять при появлении со- общения
	CFG: Изменена авто- матическая сборка баз пользователя = Выключена	Снят флаг «Автомати- ческая сборка баз поль- зователей»	Никаких действий выпол- нять не нужно
	CFG: Изменена авто- матическая сборка баз пользователя = Включена	Установлен флаг «Ав- томатическая сборка баз пользователей»	Никаких действий выпол- нять не нужно
	CFG: Изменена сбор- ка баз пользователя перед выходом = Включена	Установлен флаг «Сборка баз пользова- телей перед выходом»	Никаких действий выпол- нять не нужно
	CFG: Изменена сбор- ка баз пользователя перед выходом = Вы- ключена	Снят флаг «Сборка баз пользователей перед выходом»	Никаких действий выпол- нять не нужно
	CFG: Изменено мак- симальное число строк в журнале APM АБИ =	Скорректировано мак- симальное количество строк в журнале APM АБИ	Никаких действий выпол- нять не нужно
	CFG: Изменено мак- симальное число строк в журнале ASM =	Скорректировано мак- симальное количество строк в журнале ASM	Никаких действий выпол- нять не нужно
	CFG: Изменено мак- симальное число строк в журнале TSOM =	Скорректировано коли- чество строк в опера- тивном журнале	Никаких действий выпол- нять не нужно
	CFG: Выключена син- хронизация учетных записей РАУ с поль- зователями Аккорд	Снят флаг «Синхрони- зация учетных записей РАУ с пользователями Аккорд»	Никаких действий выпол- нять не нужно

Тип сообщения	Сообщение	Действия, при кото- рых генерируется со- общение	Действия, которые необходимо предпри- нять при появлении со- общения
	CFG: Включено про- токолирование опе- ративных сообщений в SYSLOG	Установлен флаг «Про- токолировать опера- тивные сообщения в SYSLOG»	Никаких действий выпол- нять не нужно
	CFG: Выключено про- токолирование опе- ративных сообщений в SYSLOG	Снят флаг «Протоколи- ровать оперативные сообщения в SYSLOG»	Никаких действий выпол- нять не нужно
	CFG: Изменен путь к файлу с оперативны- ми сообщениями TSOM =	Выполнена корректи- ровка пути к файлу с оперативными сообще- ниями TSOM	Никаких действий выпол- нять не нужно
	CFG: TSOM Изменен фильтр PM Создать каталог = PM_NUMBER	Выполнена корректи- ровка настроек TSOM: установлен / снят флаг «Создать каталог»	Никаких действий выпол- нять не нужно
	CFG: TSOM Изменен фильтр PM Удалить каталог = PM_NUMBER	Выполнена корректи- ровка настроек TSOM: установлен / снят флаг «Удалить каталог»	Никаких действий выпол- нять не нужно
	CFG: TSOM Изменен фильтр PM Изменить текущий каталог = PM_NUMBER	Выполнена корректи- ровка настроек TSOM: установлен / снят флаг «Изменить текущий ка- талог»	Никаких действий выпол- нять не нужно
	CFG: TSOM Изменен фильтр PM Переиме- новать каталог = PM_NUMBER	Выполнена корректи- ровка настроек TSOM: установлен / снят флаг «Переименовать ката- лог»	Никаких действий выпол- нять не нужно
	CFG: TSOM Изменен фильтр PM Создать файл = PM_NUMBER	Выполнена корректи- ровка настроек TSOM: установлен / снят флаг «Создать файл»	Никаких действий выпол- нять не нужно

Тип сообщения	Сообщение	Действия, при кото- рых генерируется со- общение	Действия, которые необходимо предпри- нять при появлении со- общения
	CFG: TSOM Изменен фильтр PM Открыть файл = PM_NUMBER	Выполнена корректи- ровка настроек TSOM: установлен / снят флаг «Открыть файл»	Никаких действий выпол- нять не нужно
	CFG: TSOM Изменен фильтр PM Закрывать файл = PM_NUMBER	Выполнена корректи- ровка настроек TSOM: установлен / снят флаг «Закрывать файл»	Никаких действий выпол- нять не нужно
	CFG: TSOM Изменен фильтр PM Удалить файл = PM_NUMBER	Выполнена корректи- ровка настроек TSOM: установлен / снят флаг «Удалить файл»	Никаких действий выпол- нять не нужно
	CFG: TSOM Изменен фильтр PM Атрибу- ты файла = PM_NUMBER	Выполнена корректи- ровка настроек TSOM: установлен / снят флаг «Атрибуты файла»	Никаких действий выпол- нять не нужно
	CFG: TSOM Изменен фильтр PM Запуск программы = PM_NUMBER	Выполнена корректи- ровка настроек TSOM: установлен / снят флаг «Запуск программы»	Никаких действий выпол- нять не нужно
	CFG: TSOM Изменен фильтр PM Выход из программы = PM_NUMBER	Выполнена корректи- ровка настроек TSOM: установлен / снят флаг «Выход из программы»	Никаких действий выпол- нять не нужно
	CFG: TSOM Изменен фильтр PM Найти первый файл = PM_NUMBER	Выполнена корректи- ровка настроек TSOM: установлен / снят флаг «Найти первый файл»	Никаких действий выпол- нять не нужно
	CFG: TSOM Изменен фильтр PM Найти следующий файл = PM_NUMBER	Выполнена корректи- ровка настроек TSOM: установлен / снят флаг «Найти следующий файл»	Никаких действий выпол- нять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	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
	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

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	CFG: TSOM Изменен фильтр REGISTRY Заккрыть ключ ре- естра = REGISTRY_NUMBER	Выполнена корректи- ровка настроек TSOM: установлен / снят флаг «Заккрыть ключ ре- естра»	Никаких действий выпол- нять не нужно
	CFG: TSOM Изменен фильтр REGISTRY Создать ключ ре- естра = REGISTRY_NUMBER	Выполнена корректи- ровка настроек TSOM: установлен / снят флаг «Создать ключ ре- естра»	Никаких действий выпол- нять не нужно
	CFG: TSOM Изменен фильтр REGISTRY Удалить ключ ре- естра = REGISTRY_NUMBER	Выполнена корректи- ровка настроек TSOM: установлен / снят флаг «Удалить ключ ре- естра»	Никаких действий выпол- нять не нужно
	CFG: TSOM Изменен фильтр REGISTRY Перечисление ключ- ей реестра = REGISTRY_NUMBER	Выполнена корректи- ровка настроек TSOM: установлен / снят флаг «Перечисление ключей реестра»	Никаких действий выпол- нять не нужно
	CFG: TSOM Изменен фильтр REGISTRY Установить значение параметра ключа = REGISTRY_NUMBER	Выполнена корректи- ровка настроек TSOM: установлен / снят флаг «Установить значение параметра ключа»	Никаких действий выпол- нять не нужно
	CFG: TSOM Изменен фильтр REGISTRY Прочитать значение параметра ключа = REGISTRY_NUMBER	Выполнена корректи- ровка настроек TSOM: установлен / снят флаг «Прочитать значение параметра ключа»	Никаких действий выпол- нять не нужно
	CFG: TSOM Изменен фильтр REGISTRY Удалить параметр ключа = REGISTRY_NUMBER	Выполнена корректи- ровка настроек TSOM: установлен / снят флаг «Удалить параметр ключа»	Никаких действий выпол- нять не нужно

Тип сообщения	Сообщение	Действия, при кото- рых генерируется со- общение	Действия, которые необходимо предпри- нять при появлении со- общения
	CFG: TSOM Изменен фильтр REGISTRY Создать параметр ключа = REGISTRY_NUMBER	Выполнена корректи- ровка настроек TSOM в части операций с ре- естром: установлен (или снят) флаг «Со- здать параметр ключа»	Никаких действий выпол- нять не нужно
	CFG: TSOM Изменен фильтр REGISTRY Перечисление пара- метров ключа = REGISTRY_NUMBER	Выполнена корректи- ровка настроек TSOM: установлен / снят флаг «Перечисление пара- метров ключа»	Никаких действий выпол- нять не нужно
	CFG: TSOM Изменен фильтр REGISTRY Result = REGISTRY_NUM	Выполнена корректи- ровка настроек TSOM в части результата вы- полнения операций с реестром: изменен па- раметр «Результат вы- полнения»	Никаких действий выпол- нять не нужно
	CFG: TSOM Изменен фильтр SZI Result = SZI_NUM	Выполнена корректи- ровка настроек TSOM в части результата вы- полнения сообщений СЗИ: изменен параметр «Результат выполне- ния»	Никаких действий выпол- нять не нужно
	CFG: TSOM Изменен фильтр Hash Result = Hash_NUM	Выполнена корректи- ровка настроек TSOM в части результата вы- полнения расчета КЦ: изменен параметр «Ре- зультат выполнения»	Никаких действий выпол- нять не нужно

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

Тип сообщения	Сообщение	Действия, при кото- рых генерируется со- общение	Действия, которые необходимо предпри- нять при появлении со- общения
	CFG: TSOM Изменен фильтр ScreenSaver ScreenSaver выключен с помощью TM АБИ = ScreenSaver_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «ScreenSaver выключен с помощью TM АБИ»	Никаких действий выполнять не нужно
	CFG: TSOM Изменен фильтр ScreenSaver Выключен временной контроль ScreenSaver-a = ScreenSaver_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «Выключен временной контроль ScreenSaver-a»	Никаких действий выполнять не нужно
	CFG: TSOM Изменен фильтр ScreenSaver Включен временной контроль ScreenSaver-a = ScreenSaver_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 TM = ScreenSaver_NUMBER	Выполнена корректировка настроек TSOM: установлен / снят флаг «Попытка разблокировать чужим TM»	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

Тип сообщения	Сообщение	Действия, при кото- рых генерируется со- общение	Действия, которые необходимо предпри- нять при появлении со- общения
	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
	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

Тип сообщения	Сообщение	Действия, при кото- рых генерируется со- общение	Действия, которые необходимо предпри- нять при появлении со- общения
	CFG: TSIEM Изменен фильтр PM Создать каталог = PM_NUMBER	Выполнена корректи- ровка настроек TSIEM: установлен / снят флаг «Создать каталог»	Никаких действий выпол- нять не нужно
	CFG: TSIEM Изменен фильтр PM Удалить каталог = PM_NUMBER	Выполнена корректи- ровка настроек TSIEM: установлен / снят флаг «Удалить каталог»	Никаких действий выпол- нять не нужно
	CFG: TSIEM Изменен фильтр PM Изменить текущий каталог = PM_NUMBER	Выполнена корректи- ровка настроек TSIEM: установлен / снят флаг «Изменить текущий ка- талог»	Никаких действий выпол- нять не нужно
	CFG: TSIEM Изменен фильтр PM Переиме- новать каталог = PM_NUMBER	Выполнена корректи- ровка настроек TSIEM: установлен / снят флаг «Переименовать ката- лог»	Никаких действий выпол- нять не нужно
	CFG: TSIEM Изменен фильтр PM Создать файл = PM_NUMBER	Выполнена корректи- ровка настроек TSIEM: установлен / снят флаг «Создать файл»	Никаких действий выпол- нять не нужно
	CFG: TSIEM Изменен фильтр PM Открыть файл = PM_NUMBER	Выполнена корректи- ровка настроек TSIEM: установлен / снят флаг «Открыть файл»	Никаких действий выпол- нять не нужно
	CFG: TSIEM Изменен фильтр PM Закреть файл = PM_NUMBER	Выполнена корректи- ровка настроек TSIEM: установлен / снят флаг «Закреть файл»	Никаких действий выпол- нять не нужно
	CFG: TSIEM Изменен фильтр PM Удалить файл = PM_NUMBER	Выполнена корректи- ровка настроек TSIEM: установлен / снят флаг «Удалить файл»	Никаких действий выпол- нять не нужно

Тип сообщения	Сообщение	Действия, при кото- рых генерируется со- общение	Действия, которые необходимо предпри- нять при появлении со- общения
	CFG: TSIEM Изменен фильтр PM Атрибу- ты файла = PM_NUMBER	Выполнена корректи- ровка настроек TSIEM: установлен / снят флаг «Атрибуты файла»	Никаких действий выпол- нять не нужно
	CFG: TSIEM Изменен фильтр PM Запуск программы = PM_NUMBER	Выполнена корректи- ровка настроек TSIEM: установлен / снят флаг «Запуск программы»	Никаких действий выпол- нять не нужно
	CFG: TSIEM Изменен фильтр PM Выход из программы = PM_NUMBER	Выполнена корректи- ровка настроек TSIEM: установлен / снят флаг «Выход из программы»	Никаких действий выпол- нять не нужно
	CFG: TSIEM Изменен фильтр PM Найти первый файл = PM_NUMBER	Выполнена корректи- ровка настроек TSIEM: установлен / снят флаг «Найти первый файл»	Никаких действий выпол- нять не нужно
	CFG: TSIEM Изменен фильтр PM Переиме- новать файл = PM_NUMBER	Выполнена корректи- ровка настроек TSIEM: установлен / снят флаг «Переименовать файл»	Никаких действий выпол- нять не нужно
	CFG: TSIEM Изменен фильтр PM Проверка существования пути = PM_NUMBER	Выполнена корректи- ровка настроек TSIEM: установлен / снят флаг «Проверка существова- ния пути»	Никаких действий выпол- нять не нужно
	CFG: TSIEM Изменен фильтр PM Result = PM_NUM	Выполнена корректи- ровка настроек TSIEM изменен параметр «Ре- зультат выполнения»	Никаких действий выпол- нять не нужно
	CFG: TSIEM Изменен фильтр REGISTRY Открыть ключ ре- естра = REGISTRY_NUMBER	Выполнена корректи- ровка настроек TSIEM: установлен / снят флаг «Открыть ключ ре- естра»	Никаких действий выпол- нять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	CFG: TSIEM Изменен фильтр REGISTRY Заккрыть ключ реестра = REGISTRY_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «Заккрыть 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
	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

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	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
	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

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	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
	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 APM АБИ = ScreenSaver_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «ScreenSaver включен с APM АБИ»	Никаких действий выполнять не нужно

Тип сообщения	Сообщение	Действия, при кото- рых генерируется со- общение	Действия, которые необходимо предпри- нять при появлении со- общения
	CFG: TSIEM Изменен фильтр ScreenSaver ScreenSaver выключен с помощью TM = ScreenSaver_NUMBER	Выполнена корректи- ровка настроек TSIEM: установлен / снят флаг «ScreenSaver выключен с помощью TM»	Никаких действий выпол- нять не нужно
	CFG: TSIEM Изменен фильтр ScreenSaver ScreenSaver выключен с APM АБИ = ScreenSaver_NUMBER	Выполнена корректи- ровка настроек TSIEM: установлен / снят флаг «ScreenSaver выключен с APM АБИ»	Никаких действий выпол- нять не нужно
	CFG: TSIEM Изменен фильтр ScreenSaver ScreenSaver выключен с помощью TM АБИ = ScreenSaver_NUMBER	Выполнена корректи- ровка настроек TSIEM: установлен / снят флаг «ScreenSaver выключен с помощью TM АБИ»	Никаких действий выпол- нять не нужно
	CFG: TSIEM Изменен фильтр ScreenSaver Выключен временной контроль ScreenSaver-a = ScreenSaver_NUMBER	Выполнена корректи- ровка настроек TSIEM: установлен / снят флаг «Выключен временной контроль ScreenSaver- a»	Никаких действий выпол- нять не нужно
	CFG: TSIEM Изменен фильтр ScreenSaver Включен временной контроль ScreenSaver-a = ScreenSaver_NUMBER	Выполнена корректи- ровка настроек TSIEM: установлен / снят флаг «Включен временной контроль ScreenSaver- a»	Никаких действий выпол- нять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	CFG: TSIEM Изменен фильтр ScreenSaver Попытка разблокировать чужим TM = ScreenSaver_NUMBER	Выполнена корректровка настроек TSIEM: установлен / снят флаг «Попытка разблокировать чужим TM»	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 WSNAMЕ 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
	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: WSNAMЕ 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

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	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
	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

Тип сообщения	Сообщение	Действия, при кото- рых генерируется со- общение	Действия, которые необходимо предпри- нять при появлении со- общения
	INI: WSNAME Авто- матический логин в ОС = No	Снят флаг «Автомати- ческий логин в ОС» в параметрах configura- ции СЗИ	Данное сообщение ин- формирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	INI: WSNAME Авто- матический логин в ОС = Yes	Установлен флаг «Ав- томатический логин в ОС» в параметрах кон- фигурации СЗИ	Данное сообщение ин- формирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	INI: WSNAME Син- хронизация с базой пользователей NT = No	Снят флаг «Синхрони- зация с базой пользо- вателей NT» в пара- метрах конфигурации СЗИ	Данное сообщение ин- формирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	INI: WSNAME Син- хронизация с базой пользователей NT = Yes	Установлен флаг «Син- хронизация с базой пользователей NT» в параметрах configura- ции СЗИ	Данное сообщение ин- формирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	INI: WSNAME Син- хронизация с базой АМДЗ = No	Снят флаг «Синхрони- зация с базой АМДЗ» в параметрах configura- ции СЗИ	Данное сообщение ин- формирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно

Тип сообщения	Сообщение	Действия, при кото- рых генерируется со- общение	Действия, которые необходимо предпри- нять при появлении со- общения
	INI: WSNAMЕ Син- хронизация с базой АМДЗ = Yes	Установлен флаг «Син- хронизация с базой АМДЗ» в параметрах конфигурации СЗИ	Данное сообщение ин- формирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	INI: На ПКО WSNAMЕ Использовать полное имя в учетных запи- сях NT = No	Снят флаг «Используй- вать полное имя в учетных записях NT» в параметрах configura- ции СЗИ	Данное сообщение ин- формирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	INI: На ПКО WSNAMЕ Использовать полное имя в учетных запи- сях NT = Yes	Установлен флаг «Ис- пользовать полное имя в учетных записях NT» в параметрах configura- ции СЗИ	Данное сообщение ин- формирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	INI: WSNAMЕ Кон- троль доступа к устройствам = No	Снят флаг «Контроль доступа к устройствам» в параметрах configura- ции СЗИ	Данное сообщение ин- формирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	INI: WSNAMЕ Кон- троль доступа к устройствам = Yes	Установлен флаг «Кон- троль доступа к устрой- ствам» в параметрах конфигурации СЗИ	Данное сообщение ин- формирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно

Тип сообщения	Сообщение	Действия, при кото- рых генерируется со- общение	Действия, которые необходимо предпри- нять при появлении со- общения
	INI: На ПКО WSNAMЕ Использовать полный путь процесса = No	Снят флаг «Используй- вать полный путь про- цесса» в параметрах конфигурации СЗИ	Данное сообщение ин- формирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	INI: На ПКО WSNAMЕ Использовать полный путь процесса = Yes	Установлен флаг «Ис- пользовать полный путь процесса» в парамет- рах конфигурации СЗИ	Данное сообщение ин- формирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
Предупреждаю- щие сообщения. Сообщения дан- ного типа фикси- руются в журнале ASM	VID и PID должны состоять из 4-х цифр!	При добавлении нового USB-устройства в базу ASM некорректно вве- дены VID или PID устройства	Ввести корректные значе- ния VID или PID устрой- ства
	VID и PID должны состоять только из шестнадцатеричных цифр, или '*!'	При добавлении нового USB-устройства в базу ASM некорректно вве- дены VID или PID устройства	Ввести корректные значе- ния VID или PID устрой- ства
	Серийный номер должен состоять только из шестнадца- теричных цифр, или '*!'	При добавлении нового USB-устройства в базу ASM введен некоррект- ный серийный номер устройства	Ввести корректный се- рийный номер устройства

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
Сообщение об ошибке. Сообщения данного типа фиксируются в журнале ASM	Error WSNAMЕ 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 WSNAMЕ 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 WSNAMЕ 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)
	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)

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	Error WSNNAME 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 WSNNAME 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 WSNNAME 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)
	Error WSNNAME 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)

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	Error WSNAMЕ 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 WSNAMЕ 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 WSNAMЕ 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)
	Error WSNAMЕ 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)

Тип сообщения	Сообщение	Действия, при кото- рых генерируется со- общение	Действия, которые необходимо предпри- нять при появлении со- общения
	Error WSNAMЕ От- правлена база поль- зователей [отложен- ная] [Аккорд не акти- вирован]. Не прошел логин в АМДЗ [ErrCode = ERRCODE]	При попытке отправить отложенную базу поль- зователей на ПКО про- изошла ошибка при аутентификации сервера на АМДЗ	Повторить попытку от- правления отложенной базы пользователей на ПКО. Если ошибка повто- рится, обратиться к Ад- министратору ИБ средств защиты информации от НСД (АИБ технологиче- ского участка)
	Error WSNAMЕ От- правлена база поль- зователей [Аккорд не активирован]. Ошибка создания файла [ErrCode = ERRCODE]	При попытке отправить базу пользователей на ПКО произошла ошибка при создании файла для базы пользовате- лей	Убедится, что каталог, в который установлен ПАК СЗИ от НСД «Аккорд» доступен для записи
	Error WSNAMЕ От- правлена база поль- зователей. Ошибка создания файла FILENAME [ErrCode = ERRCODE]	При попытке отправить базу пользователей на ПКО произошла ошибка при создании файла для базы пользовате- лей	При появлении данной ошибки необходимо обра- титься в службу техниче- ской поддержки организа- ции-разработчика
	Error WSNAMЕ От- правлена база поль- зователей [отложен- ная]. Ошибка созда- ния файла [ErrCode = ERRCODE]	При попытке отправить отложенную базу поль- зователей на ПКО про- изошла ошибка при со- здании файла для базы пользователей	Убедится, что каталог, в который установлен ПАК СЗИ от НСД «Аккорд» доступен для записи
	Error WSNAMЕ От- правлена база поль- зователей [отложен- ная] [Аккорд не акти- вирован]. Ошибка создания файла FILENAME [ErrCode = ERRCODE]	При попытке отправить отложенную базу поль- зователей на ПКО про- изошла ошибка при со- здании 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 WSNAMЕ 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 WSNAMЕ 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 WSNAMЕ 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)
	Error WSNAMЕ 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)

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	Error WSNAMЕ 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 WSNAMЕ Передача базы. Для компьютера WSNAMЕ 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 WSNAMЕ 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)
	Для компьютера WSNAMЕ 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 WSNAMЕ 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)

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	Error Ошибка ERRCODE отправки файла конфигурации СЗИ на WSNAMЕ	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 WSNAMЕ	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)
	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»

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	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»
	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

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	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 сообщений 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	Заккрытие 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 сообщений журнала APM АБИ

В таблице 6 приведены сообщения журнала APM АБИ и описания этих сообщений. В таблице 6 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 сообщения	Проверка соединения с ПКО	Выполнена проверка соединения с ПКО
	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

Тип сообщения	Наименование сообщения	Описание сообщения
	Обновление ПО	Выполнено обновление программного обеспечения сетевого агента РАУ на подконтрольном объекте
	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 Asrpn 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»

Тип сообщения	Наименование сообщения	Описание сообщения
	Ошибка получения журналов Aсrun	Ошибка получения оперативных событий от драйвера ПАК «Аккорд». Если данная ошибка повторяется регулярно, обратитесь в службу технической поддержки ЗАО «ОКБ САПР»
	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 выполнялась с ошибкой. Если данная ошибка повторяется регулярно, обратитесь в службу технической поддержки ЗАО «ОКБ САПР»
	Ошибка переоткрытия журналов в Aсrun	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

Тип сообщения	Наименование сообщения	Описание сообщения
	Ошибка синхронизации базы пользователей с NT	Ошибка синхронизации базы .amz с пользователями ОС на ПКО
	Ошибка записи конфигурации таймаутов в плату АМД3	Ошибка записи параметров времени на ввод пароля и предоставление идентификатора в АМД3 на ПКО
	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 выполнялась с ошибкой
Информационные сообщения	Версия драйвера Acrun: VERSION	Информация о версии драйвера Аккорд на ПКО
	Версия драйвера АМД3: VERSION	Информация о версии драйвера АМД3 на ПКО
	Версия прошивки АМД3: VERSION	Информация о версии прошивки АМД3 на ПКО
	АМД3 плата обнаружена	АМД3 плата обнаружена на ПКО
	Серийный номер платы АМД3: AMDZ_BOARD_SERIAL_NUM	Серийный номер платы АМД3 на ПКО
	Версия ТМ-драйвера АМД3: 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)

Тип сообщения	Наименование сообщения	Описание сообщения
	Команда перечитывания фильтров была отправлена на OBJECT_NAME	Команда на использование новых фильтров принята на ПКО (исполнение не начато)
	Файл журналов Asgrip был успешно переоткрыт	На ПКО успешно переоткрыты журналы Аккорд по расписанию в 23:00
	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, какое 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 АДЗ получены	Прочитан *.azl файл из АДЗ на ПКО

Тип сообщения	Наименование сообщения	Описание сообщения
	База пользователей успешно прочитана из платы АМДЗ	*.amz база прочитана из АМДЗ на ПКО
	Рабочая станция успешно заблокирована	Установлен экран блокировки на ПКО
	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

Тип сообщения	Наименование сообщения	Описание сообщения
	Начата передача СЗИ сообщения	Начата передача СЗИ сообщения с ПКО в RMQ
	Сбор журналов Ascpn был остановлен успешно	Сбор оперативных событий от драйвера Аккорд остановлен корректно (при остановке сервиса)
	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 Файлы конфигурации

9.1 Файл конфигурации ASM.INI

Параметры файла ASM.INI штатно изменяются с помощью оболочки ASMT.EXE. Возможно ручное редактирование данного файла с помощью текстового редактора, например, Notepad.

Параметры конфигурационного файла ASM.INI и их описание приведены в таблице 7.

Таблица 7 – Параметры конфигурационного файла ASM.INI

Параметры конфигурационного файла	Значение параметров конфигурационного файла
[options]	
ExportFolder	Выбор каталога для экспортирования настроек ASM
LoginAsAccordIA	Автоматическое использование для идентификации учетной записи пользователя ПАК «Аккорд» при запуске программы ASMT.exe
NewHash	Данный параметр разрешает и запрещает удалённое (на СЦУ) формирование списка контролируемых на ПКО файлов. Если данный параметр принимает значение Yes, то удаленное формирование списка контролируемых файлов разрешено, если No, то запрещено. Данный параметр может быть изменён с помощью оболочки «ASMT.EXE»: Настройка --> Основные настройки --> Дополнительные настройки: --> Использовать удаленный расчет КЦ. Значение по умолчанию – Yes (флажок в оболочке «ASMT.EXE» установлен)
WorkDir	Рабочий каталог, путь к файлам *.acc и *.ini. По умолчанию c:\asm
AccordRauFolder	Каталог утилит, реализующих сетевое соединение, а так же к входящим/исходящим файлам баз ПКО. По умолчанию c:\asm\acconnet
AccordRauTimeout	Тайм-аут отклика службы AcConNet
RebootTimeout	Время перезагрузки ПКО после обновления баз пользователей

AutoAssemble	Включает автоматическую пересборку баз пользователей ПКО и их передачу на ПКО (если были произведены изменения)
AutoAssembleTimeout	Таймаут действия флага AutoAssemble
AssemblePrevExit	Включает автоматическую пересборку баз пользователей ПКО и их передачу на ПКО (если были произведены изменения) при выходе из ASM
ArmAbiListCount	Лимит строк в журнале "Журнал АРМ АБИ"
AsmListCount	Лимит строк в журнале "Журнал ASM"
TSOMListCount	Лимит строк в журнале "Журнал Accord"
LoginAsAccordIA	Включает автоматическое подставление логина/пароля пользователей ASM используя логин/пароль пользователя сессии Аккорд
RauMode	Включает режим "Классический РАУ"
ActualHash	При передаче баз пользователей, сначала всегда дожидается получения актуального списка КЦ ПКО
NewPassword	Использовать при смене пароля пользователя, принадлежность его к ТУ
[TSOM]	
NSDWindowAib	При НСД подключении устройств выводит сообщение для АИБ
NSDWindowAudit	При НСД подключении устройств выводит сообщение для Аудитора
NSDWindowOib	При НСД подключении устройств выводит сообщение для Оператора

9.2 Файл конфигурации AcCon32.ini

Файл конфигурации AcCon32.ini содержит настроечные параметры сервера централизованного управления. Данный файл находится в установочном каталоге сервера централизованного управления (по умолчанию C:\ASM). Параметры конфигурационного файла AcCon32.ini и их описание приведены в таблице 8.

Таблица 8 – Параметры конфигурационного файла AcCon32.ini

Параметры конфигурационного файла	Значение параметров конфигурационного файла
[Options]	

Параметры конфигурационного файла	Значение параметров конфигурационного файла
Timeout	Таймаут соединения (в секундах)
TransportLogLevel	Детальность ведения журналов транспорта (0 – Error, 1 – Info, 2 – Debug)
ServiceLogLevel	Детальность ведения журналов сервиса (0 – Error, 1 – Info, 2 – Debug)
RetryCount	Количество попыток переподключения к RabbitMQ при старте (0 – бесконечно)
RetryInterval	Интервал попыток переподключения к RabbitMQ при старте (в секундах)
FileChunkSize	Максимальный размер данных, передаваемых за одну итерацию, в МБ. Если данный параметр отсутствует в конфигурационном файле, то максимальный размер принимается равным 64 МБ
[RabbitMQ]	
Port	Номер порта для подключения к RabbitMQ серверу. Данный номер должен совпадать с номером порта, указанным в параметре tcp_listeners конфигурационного файла rabbitmq.config, описанного в разделе 9.4. На сервере централизованного управления порт с данным номером должен быть открыт на входящие подключения. По умолчанию для подключения к RabbitMQ серверу используется порт 28997
HeartbeatTimeout	Таймаут отправки сигналов для проверки соединения с RabbitMQ (в секундах)
ReconnectInterval	Интервал, после которого осуществляется попытка восстановить соединение с RabbitMQ (в секундах)
ConnectionTimeout	Таймаут попыток соединения при восстановлении связи с RabbitMQ (в миллисекундах)

9.3 Файл конфигурации AcWs32.ini

Файл конфигурации AcWs32.ini находится на ПКО и содержит его настроечные параметры. Параметры конфигурационного файла AcWs32.ini и их описание приведены в таблице 9.

Таблица 9 - Параметры конфигурационного файла AcWs32.ini

Параметры конфигурационного файла	Значение параметров конфигурационного файла
[Options]	
Language	Используемый язык
HookWinReboot	Перехватывать перезагрузку Windows
HardReset	Жесткая перезагрузка (работает только в Win9x)
AlwaysReboot	Перегружать компьютер при любом завершении сеанса работы
MSNetAuth	Использовать усиленную аутентификацию для сети MicroSoft
WaitStartTime	Задержка в секундах при старте клиента AcWs32.exe
WsName	Имя рабочей станции
UseSound	Звуковой сигнал при выводе сообщений
NoNetManaged	Станция не управляется по сети
TransportLogLevel	Детальность ведения журналов транспорта (0 – Error, 1 – Info, 2 – Debug)
ServiceLogLevel	Детальность ведения журналов сервиса (0 – Error, 1 – Info, 2 – Debug)
RetryCount	Количество попыток переподключения к RabbitMQ при старте (0 – бесконечно)
RetryInterval	Интервал попыток переподключения к RabbitMQ при старте (в секундах)
ChecksumRecvInterval	Таймаут отправки файлов *.CRC на сервере централизованного управления в секундах. Если данный параметр отсутствует в конфигурационном файле, то значение таймаута принимается равным 30 секундам
FileChunkSize	Максимальный размер данных, передаваемых за одну итерацию, в МБ. Если данный параметр отсутствует в конфигурационном файле, то максимальный размер принимается равным 64 МБ
[RabbitMQ]	

Параметры конфигурационного файла	Значение параметров конфигурационного файла
Port	Номер порта для подключения к RabbitMQ серверу. Данный номер должен совпадать с номером порта, указанным в параметре tcp_listeners конфигурационного файла rabbitmq.config, описанного в подразделе 9.4. На ПКО порт с данным номером должен быть открыт на входящие подключения. По умолчанию для подключения к RabbitMQ серверу используется порт 28997
HeartbeatTimeout	Таймаут отправки сигналов для проверки соединения с RabbitMQ (в секундах)
ReconnectInterval	Интервал, после которого осуществляется попытка восстановить соединение с RabbitMQ (в секундах)
ConnectionTimeout	Таймаут попыток соединения при восстановлении связи с RabbitMQ (в миллисекундах)

9.4 Файл конфигурации rabbitmq.config

В конфигурационном файле rabbitmq.config задаются параметры транспортного сервера RabbitMQ. Данный файл находится в базовой директории %APPDATA%\RabbitMQ на сервере централизованного управления. Данный файл имеет следующее содержание:

```
[{rabbit, [{tcp_listeners, [28997]}, {loopback_users, []}]}].
```

В данном файле в настроечном параметре tcp_listeners задается номер порта, через который осуществляются входящие подключения к серверу RabbitMQ. На сервере централизованного управления порт с данным номером должен быть открыт на входящие подключения. По умолчанию используется порт 28997.

При необходимости изменить базовую директорию RabbitMQ следует выполнить следующие действия:

1. Через оснастку Службы (Services) остановить службу RabbitMQ и использующие его службы PAУ, если они используются.
2. Удалить RabbitMQ Server.
3. Переместить конфигурационный файл «rabbitmq.config» из прежней базовой директории (по умолчанию – «%APPDATA@\RabbitMQ») в новую базовую директорию.

4. Установить RabbitMQ Server через пакет rabbitmq-server-X.Y.Z.exe, где X.Y.Z – номер версии. При установке использовать настройки по умолчанию, исключив RabbitMQ Service в диалоге выбора компонентов для установки.
5. Открыть Command Prompt с правами администратора и перейти в директорию sbin, находящуюся в папке установки RabbitMQ.
6. Выполнить команду установки переменной RABBITMQ_BASE, указав базовую директорию RabbitMQ, например, «set RABBITMQ_BASE=C:\ProgramData\RabbitMQData».
7. Выполнить команду установки сервиса RabbitMQ «rabbitmq-service install».
8. Удалить прежнюю папку базовой директории RabbitMQ.
9. Запустить службу «RabbitMQ» через оснастку Службы (Services). Запустить службы PAU.

10 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	Средство вычислительной техники
СЗИ	Средство защиты информации
СУ	Система управления
ASM	Accord Security Management

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Изм.	Номера листов (страниц)				Всего ли- стов (стр.) в документе	№ доку- мента	Входящий № сопро- водитель- ного доку- мента	Под- пись	Дата
	изме- нен- ных	замене- нен- ных	новых	аннули- рованных					

СОГЛАСОВАНО

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