УТВЕРЖДЕН
11443195.4012-053 94 2012 ЛУ

СПЕЦИАЛЬНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

«АККОРД-РАУ»

Руководство Контролёра

Листов 111

Москва

2020

АННОТАЦИЯ

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

Данный документ описывает действия Контролера РАУ, связанные с мониторингом настроек комплекса Аккорд и правил разграничения доступа в штатном режиме функционирования.

СОДЕРЖАНИЕ

1 Введение

1.1 Область применения

Деятельность Контролера РАУ.

1.2 Функции Контролера РАУ

Контролер РАУ выполняет следующие функции:

- осуществляет контроль компонентов РАУ в части:
  - проверки настроек комплекса Аккорд для ПКО;
  - проверки правил разграничения доступа пользователей ПКО, в том числе в части настроек по блокированию и открытию доступа к коммуникационным портам и встроенным устройствам ввода-вывода информации на ПКО, добавлению на ПКО USB-устройств;
- обеспечивает мониторинг состояния информационной безопасности в части защиты от несанкционированного доступа средствами РАУ;
- осуществляет контроль журналов аудита в части выполнения порядка использования устройств ввода-вывода информации, коммуникационных портов и съемных машинных носителей.

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 Порядок работы

3.1 Проверка настроек комплекса «Аккорд» и правил разграничения доступа пользователей ПКО

Контролер РАУ имеет возможность осуществлять проверку настроек комплекса «Аккорд» и правил разграничения доступа пользователей ПКО.

3.2 Обеспечение мониторинга состояния информационной безопасности

Контролер обеспечивает мониторинг состояния информационной безопасности в части защиты от несанкционированного доступа средствами РАУ.

Кроме того, в РАУ происходит получение журналов регистрации работ ПАК СЗИ от НСД Аккорд в режиме реального времени, то есть все попытки НСД сразу же отображаются на экране СЦУ.

3.3 Контроль журналов аудита в части выполнения порядка использования устройств ввода-вывода информации, коммуникационных портов и съемных машинных носителей

Контролер имеет возможность осуществлять контроль журналов аудита в части выполнения порядка использования устройств ввода-вывода информации, коммуникационных портов и съемных машинных носителей.

4 Работа с ASM

4.1 Проверка правил разграничения доступа пользователей и настроек ПАК «Аккорд» ПКО

4.1.1 Вкладка «Пользователи»

Во вкладке «Управление > Пользователи системы», приведённой на рисунке 1, Контролер РАУ осуществляет процедуры просмотра списка пользователей, печати информации о пользователях и поиска пользователей по идентификатору. В данной вкладке Контролеру доступны только кнопки <Редактировать> и <Поиск>.

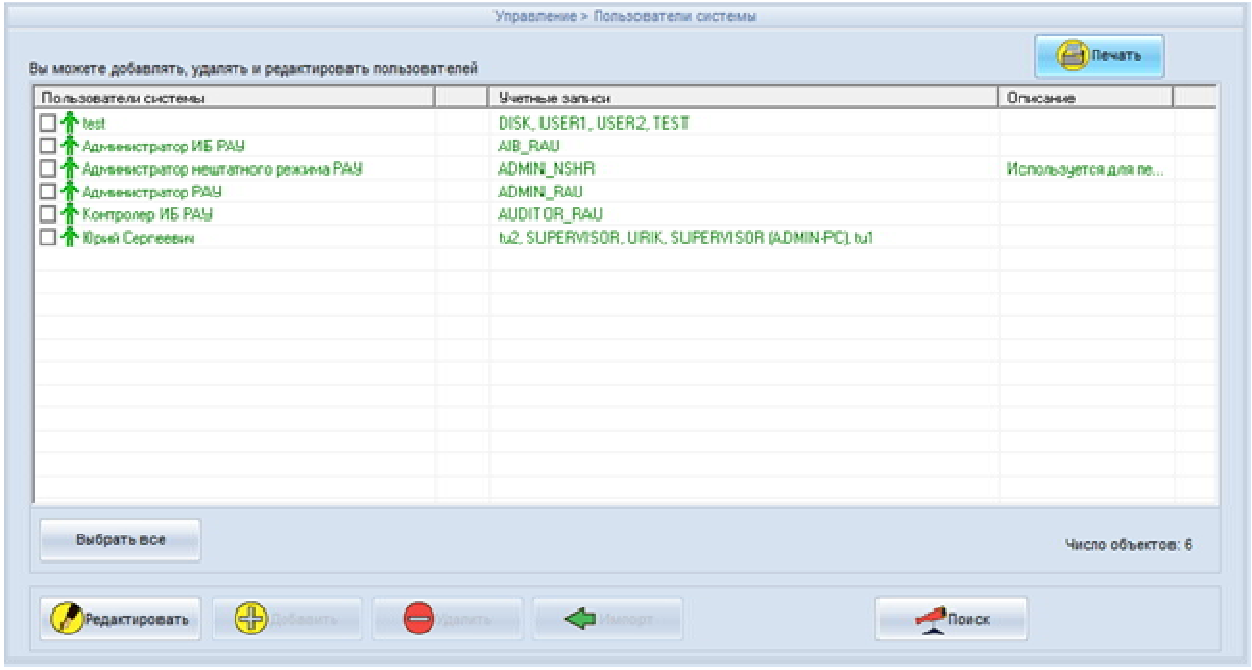

Рисунок 1 - Вкладка Управление > Пользователи системы

При нажатии кнопки <Редактировать> появляется окно, в котором Контролер может просмотреть параметры пользователя.

Если необходимо определить, какому пользователю принадлежит данный идентификатор, следует нажать кнопку <Поиск> во вкладке «Роли». Появится окно с сообщением «Предъявите идентификатор».

Если предъявленный идентификатор назначен какому-либо пользователю, этот пользователь будет выделен, как показано на рисунке 2.

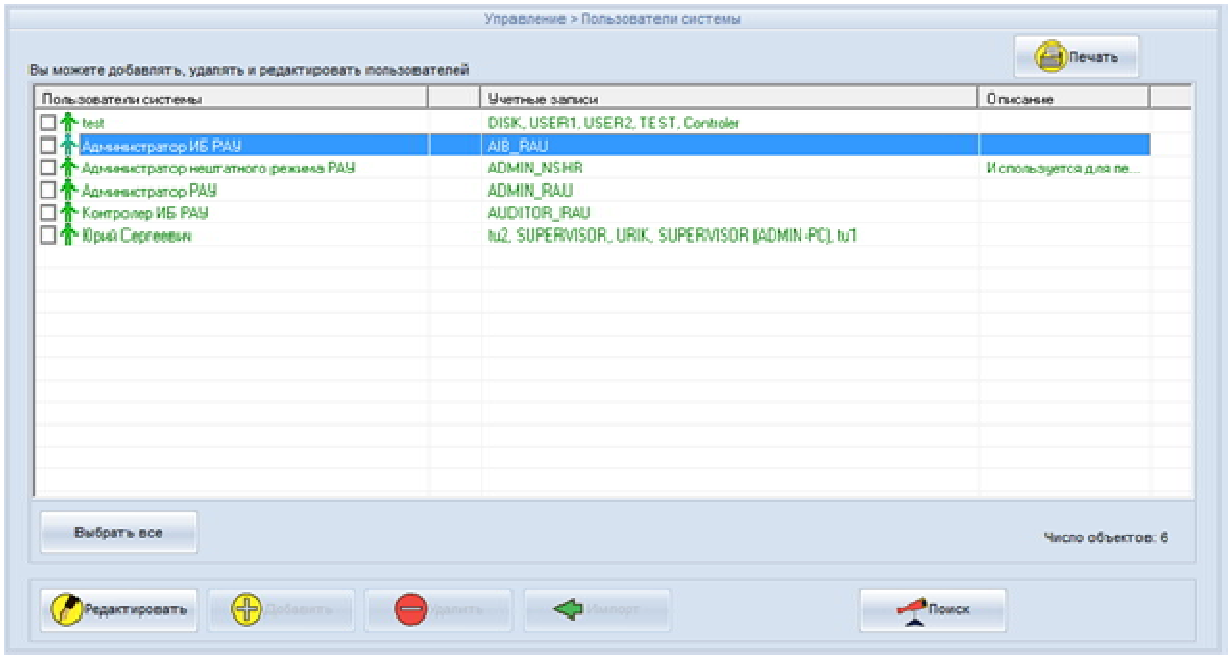

Рисунок 2 - Пользователь, которому назначен идентификатор

Если предъявленный идентификатор не назначен ни одному из пользователей системы, в нижней части окна появится сообщение «Идентификатор не зарегистрирован!», как показано на рисунке 3.

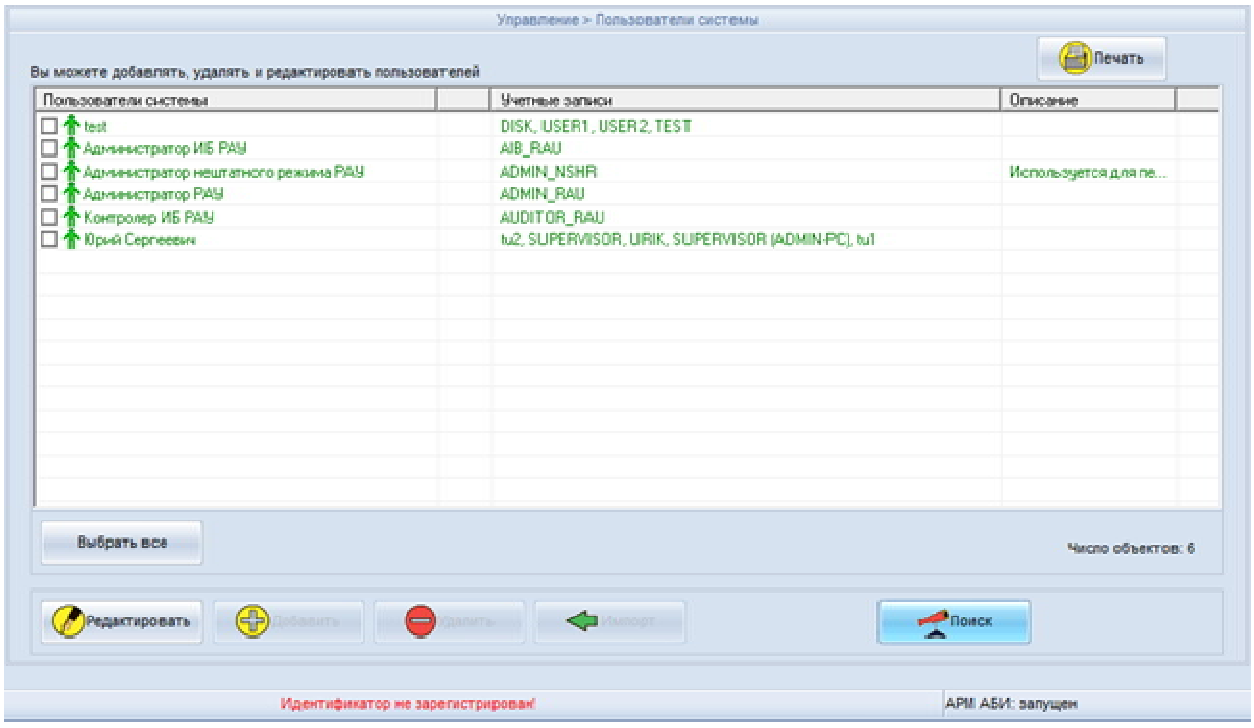

Рисунок 3 - Сообщение о том, что идентификатор не зарегистрирован

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

При её нажатии появляется окно, приведённое на рисунке 4, 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.

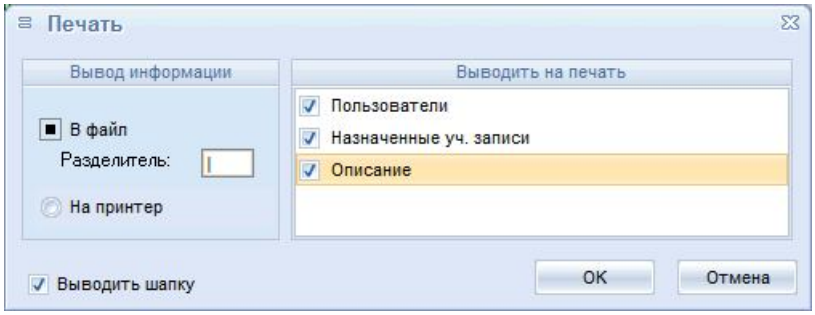

Рисунок 4 - Печать информации о пользователе

4.1.2 Вкладка «Роли»

Права доступа (ПРД) для учетной записи определяются ролью.

В РАУ предусмотрены следующие встроенные роли:

- 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 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.

Во вкладке «Управление > Роли системы», приведённой на рисунке 5, Контролер РАУ может осуществлять просмотр параметров ролей РАУ: имени и описания роли, назначенных технологических участков, а также информации о наличии списков файлов контроля целостности, списков задач и о стартовых задачах.

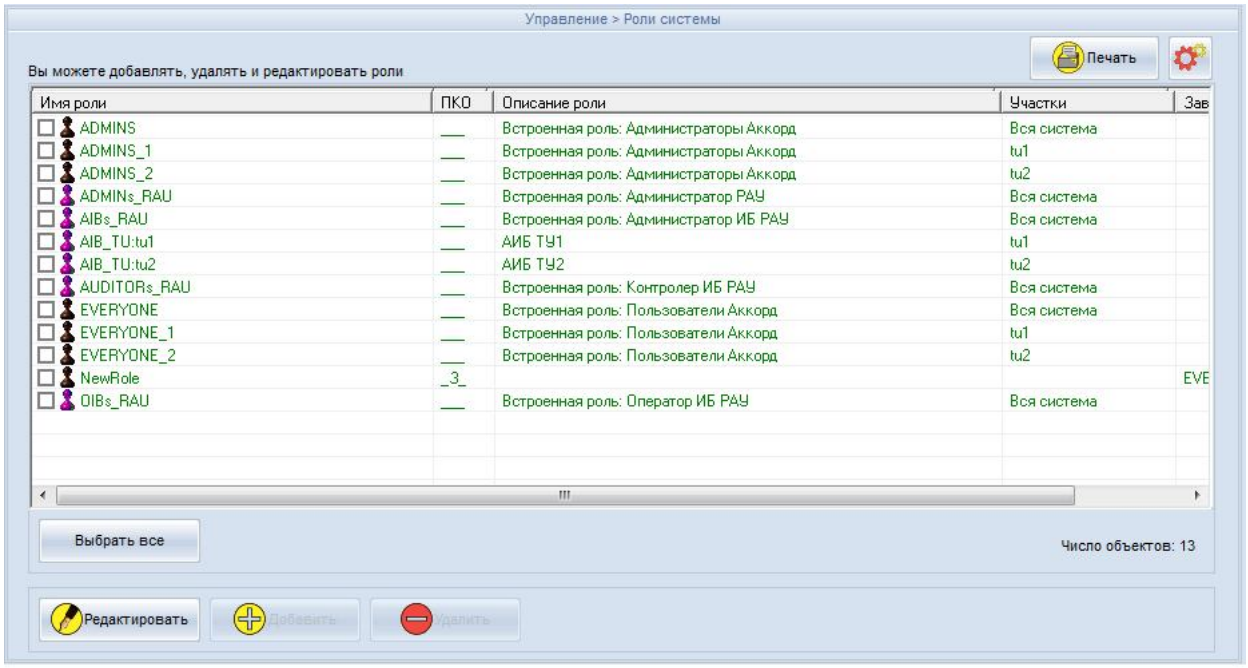

Рисунок 5 - Вкладка «Управление > Роли системы»

Для отображения в списке ролей вкладки «Управление > Роли системы», приведённой на рисунке 5, информации о наличии списков файлов контроля целостности, списков задач и стартовых задачах нужно нажать кнопку <Настройка отображения информации>. При её нажатии появляется окно, приведённое на рисунке 6, в котором устанавливаются флаги напротив той информации о настройках ПКО, которую следует отобразить.

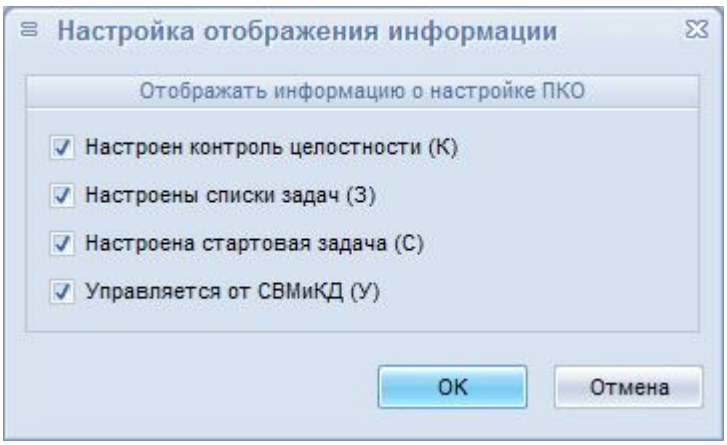

Рисунок 6 – Настройка отображения информации о ПКО

После добавления отображаемой информации во вкладке «Управление > Роли системы» в таблице ролей появляется столбец с названием «ПКО». 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.

4.1.3 Вкладка «Идентификаторы»

Во вкладке «Управление > Идентификаторы системы», приведённой на рисунке 7, Контролер РАУ выполняет процедуры просмотра списка идентификаторов ASM, печати информации об идентификаторах, поиска идентификаторов в базе РАУ.

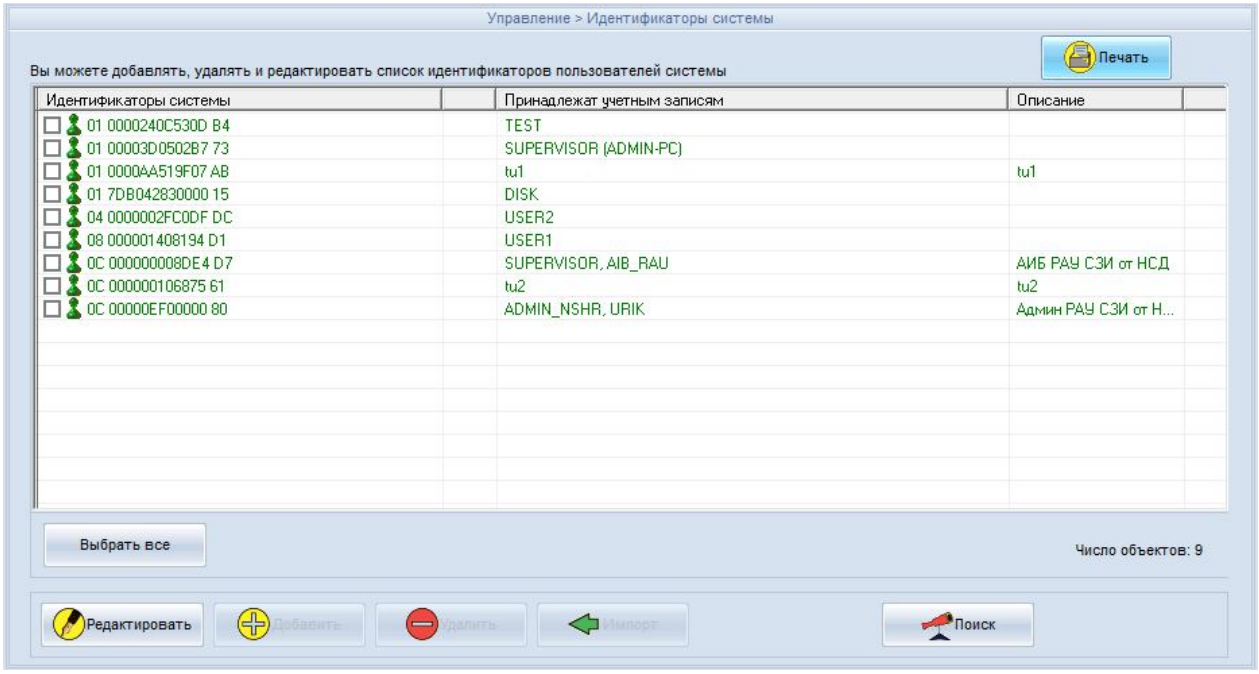

Рисунок 7 - Идентификаторы системы

Кнопка <Печать> позволяет распечатать выбранную информацию на принтере, а также сохранить в файл (с указанным разделителем). При её нажатии появляется окно, в котором следует выбрать способ печати: в файл или на принтер, тип выводимой информации (серийный номер идентификатора, принадлежность учетным записям и описание); при печати в файл следует также указать разделитель.

Если необходимо определить, добавлен ли идентификатор в базу РАУ, следует нажать кнопку <Поиск> во вкладке «Управление > Идентификаторы си-

стемы». Появится окно с сообщением «Предъявите идентификатор», приведённое на рисунке 8.

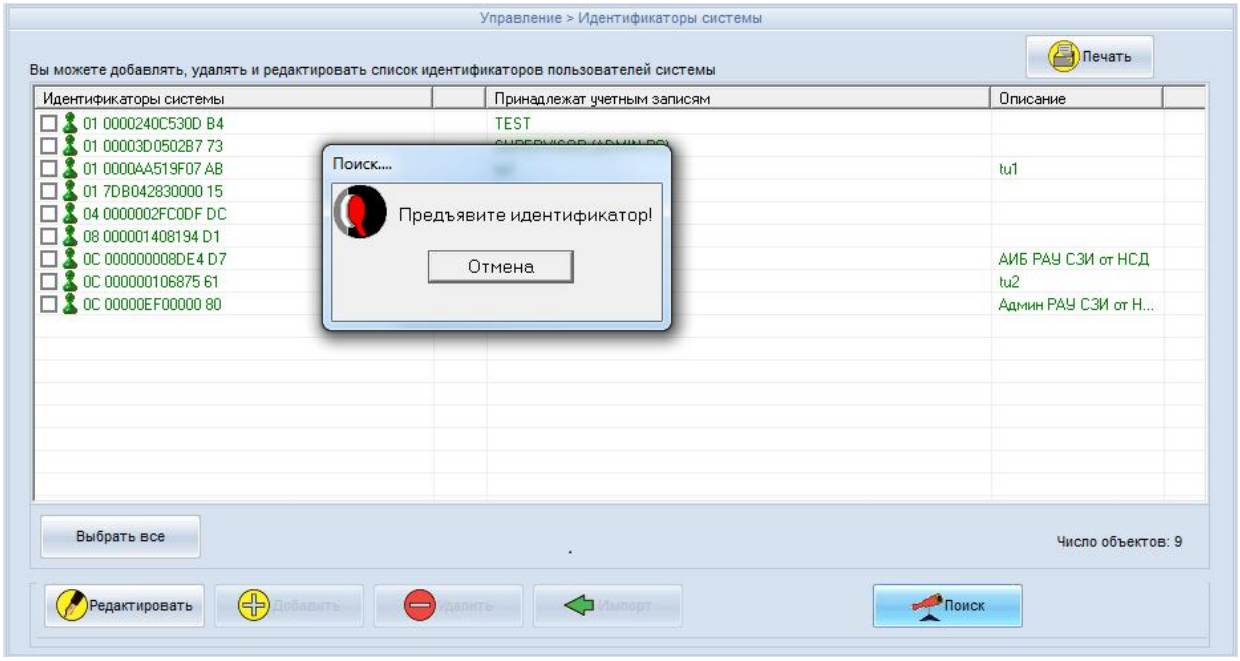

Рисунок 8 - Сообщение «Предъявите идентификатор»

Если предъявленный идентификатор добавлен в базу ASM, этот идентификатор будет выделен, как показано на рисунке 9.

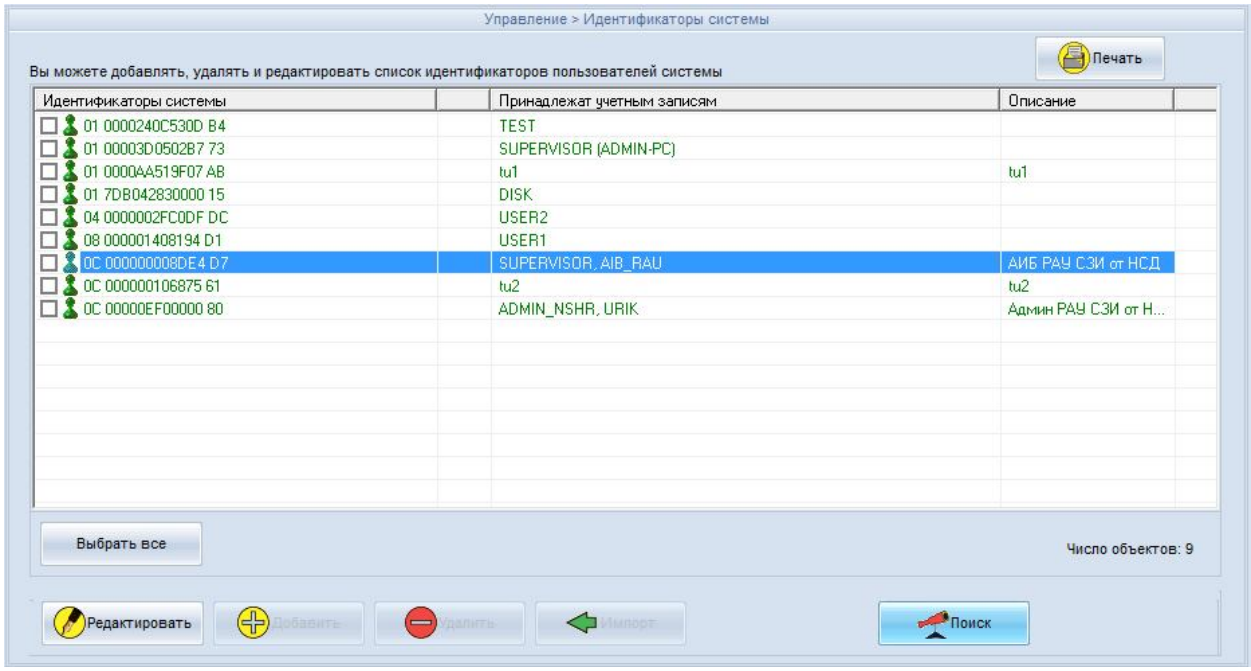

Рисунок 9 - Найдена учетная запись, которой назначен идентификатор

Если предъявленный идентификатор отсутствует в базе ASM, в нижней части окна появится сообщение «Идентификатор не зарегистрирован!», как показано на рисунке 10.

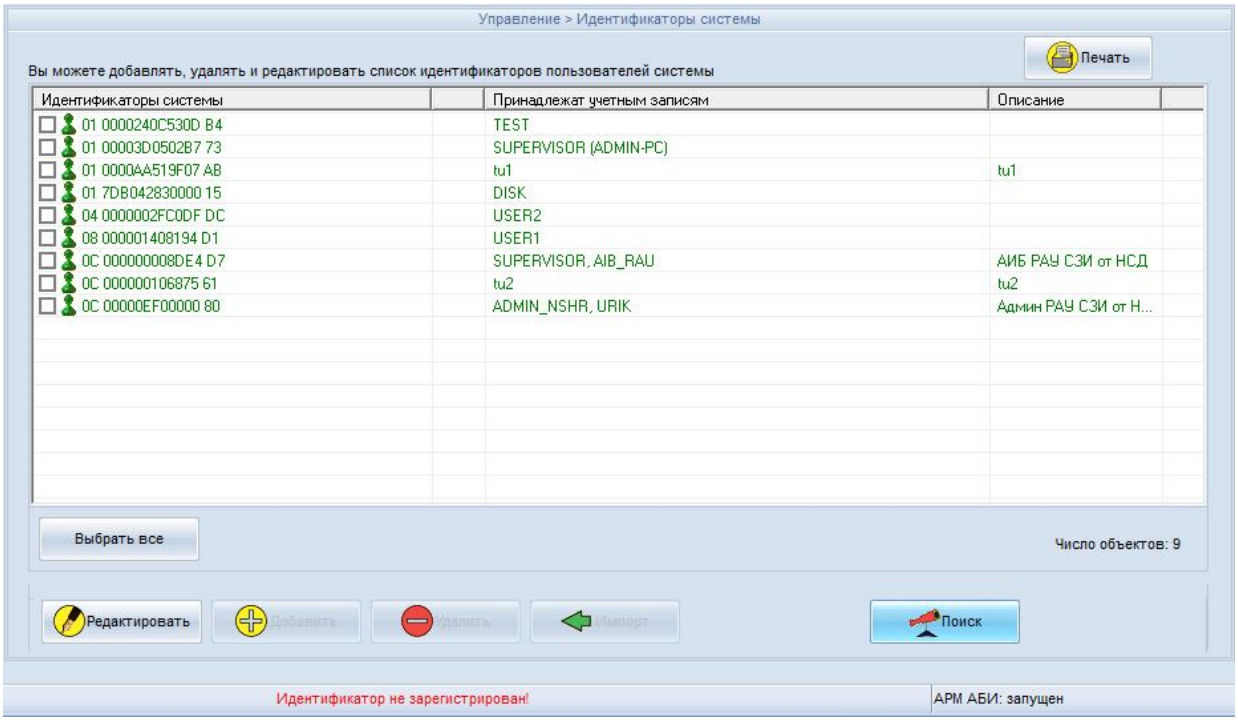

Рисунок 10 - Сообщение о том, что идентификатор не зарегистрирован в базе РАУ

4.1.4 Вкладка «Компьютеры»

Во вкладке «Управление > Компьютеры системы», приведённой на рисунке 11, Контролер РАУ выполняет процедуры просмотра параметров ПКО: настройку ПКО, настройку ПАК «Аккорд» и списка привилегированных процессов на ПКО, настройку списка мандатных меток и общих ресурсов ПКО.

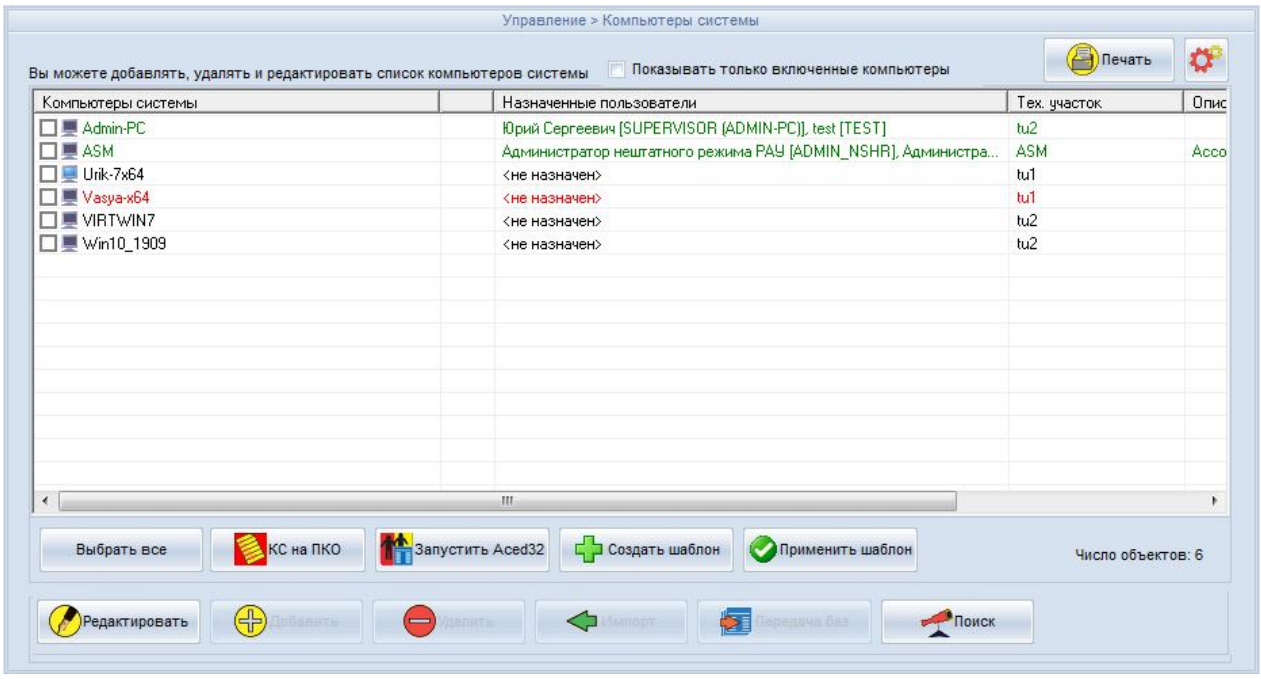

Рисунок 11 - Компьютеры системы

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

Для отображения в списке компьютеров информации о наличии списков файлов контроля целостности, списков задач (*.act файлов) и о стартовых задачах нужно в окне, приведенном на рисунке 11, нажать кнопку <Настройка отображения информации>. При её нажатии появляется окно, приведённое на рисунке 6, в котором устанавливаются флаги напротив той информации о настройках ПКО, которую следует отобразить. После добавления отображаемой информации в таблице компьютеров появляется столбец под названием «ПКО». Наличие литеры «К» в данном столбце означает, что для данного компьютера 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.

Чтобы просмотреть настройки комплекса «Аккорд», необходимо выбрать ПКО из списка и нажать кнопку <Редактировать> (рисунок 11). В появившемся окне, приведённом на рисунке 12, нажать кнопку <Конфигурация СЗИ>.

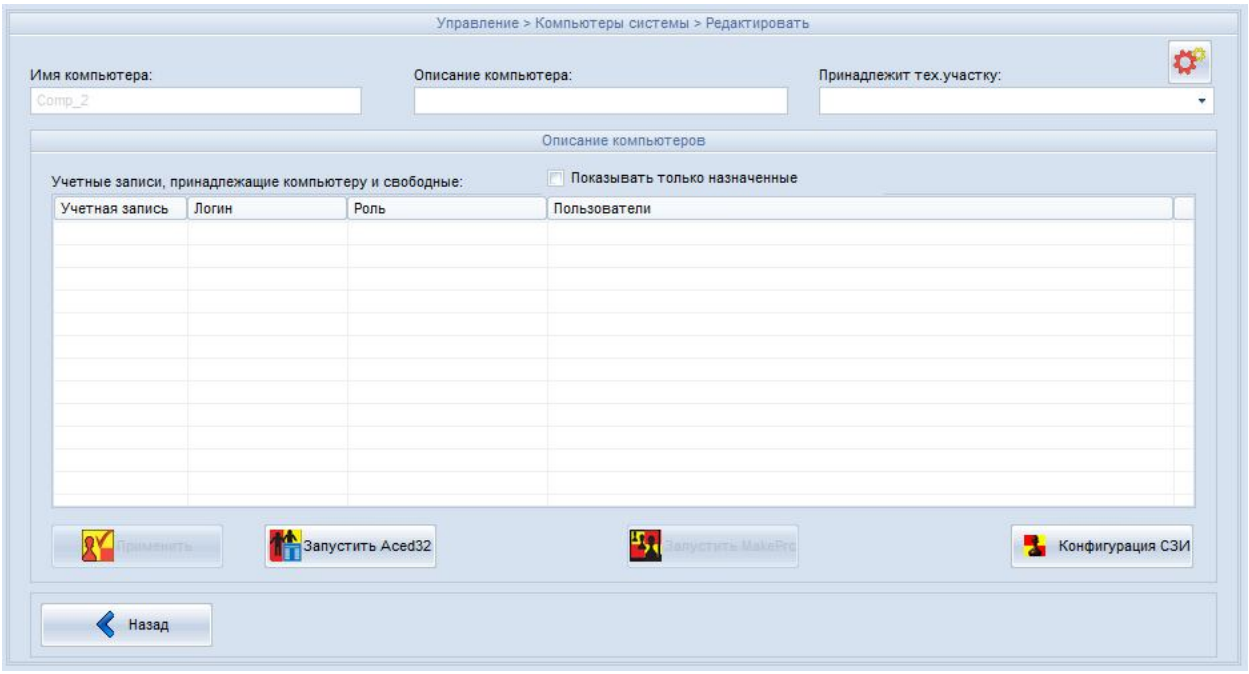

Рисунок 12 – Редактирование списка подконтрольных объектов

Чтобы просмотреть ПРД, необходимо выбрать ПКО из списка и нажать кнопку <Редактировать> (рисунок 11). В появившемся окне, приведённом рисунке 12, нажать кнопку <Запустить ACED32>.

Примечание. Кнопка <Запустить ACED32> доступна только при выборе классического режима работы РАУ (смотри документ 11443195.4012-053 91 «Руководство администратора информационной безопасности»).

При нажатии кнопки <Конфигурация СЗИ> появляется окно, приведённое на рисунке 13, в котором отображаются настройки ПАК «Аккорд» выбранного ПКО, версия его программного обеспечения, IP-адрес, серийный номер контроллера, а также инвентарные номера ПКО и контроллера «Аккорд-АМДЗ» (последние два поля заполняются вручную). Контролёр может просматривать установленные для данного ПКО настройки «Аккорда», однако не имеет возможности вносить какие-либо изменения в конфигурацию.

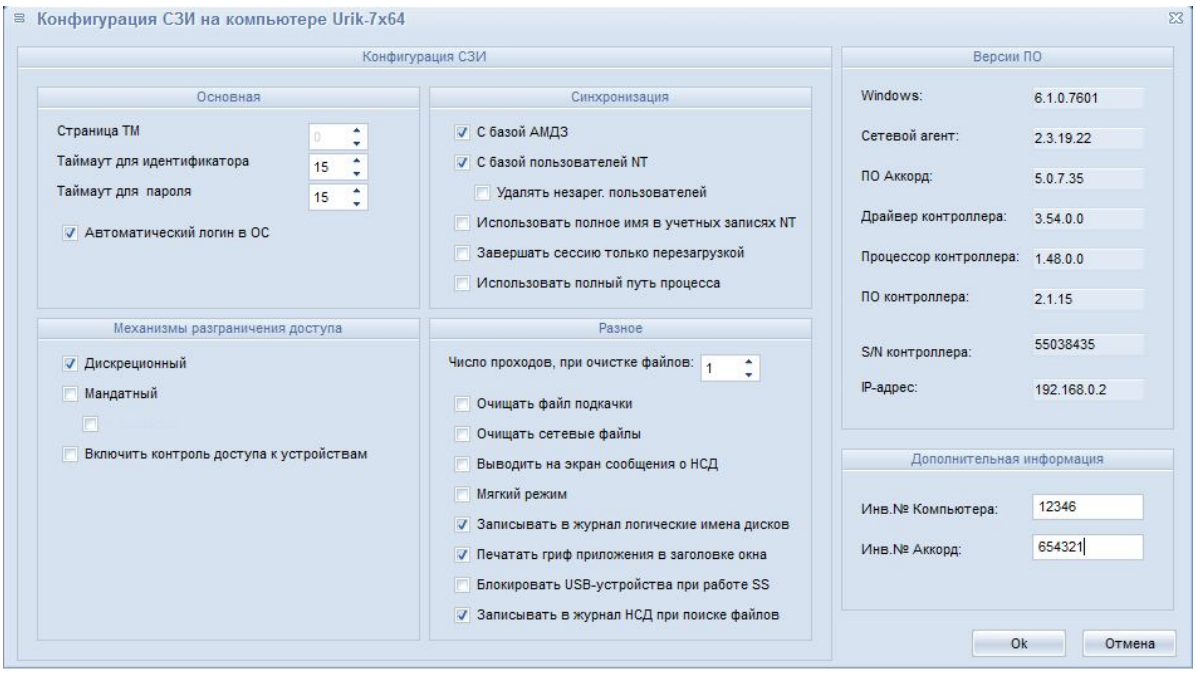

Рисунок 13 – Конфигурация СЗИ на подконтрольном объекте

При нажатии кнопки <Запустить ACED32> появляется сообщение, приведённое на рисунке 14, о невозможности модификации базы пользователей.

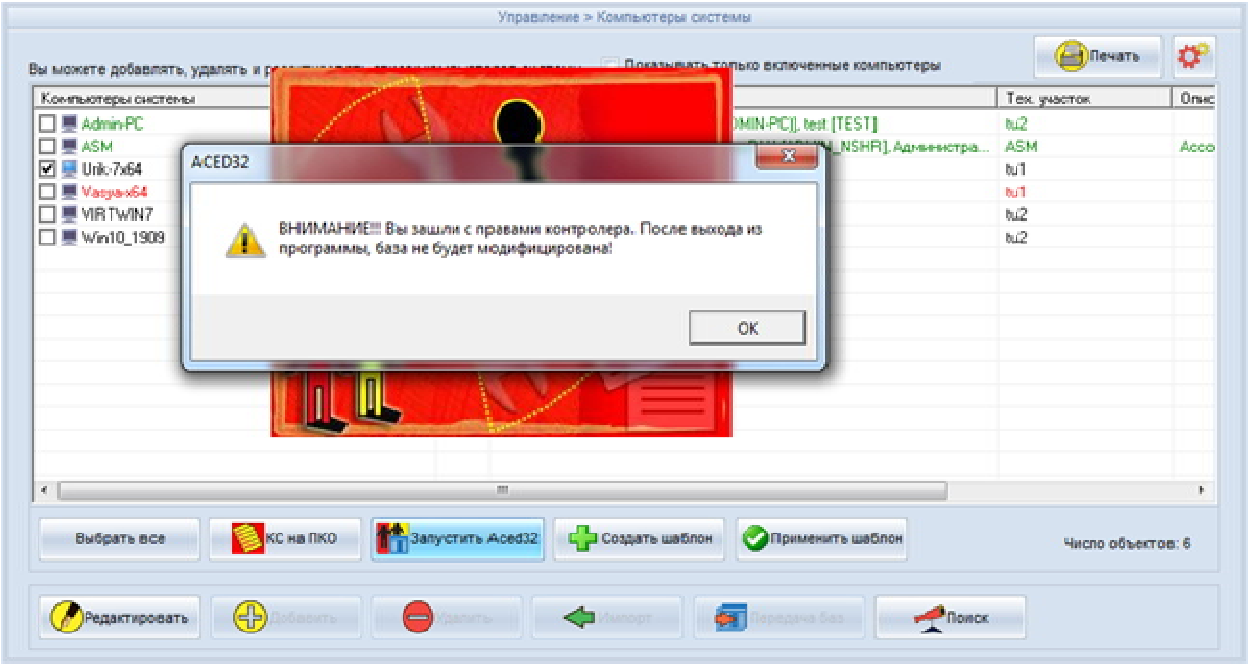

Рисунок 14 – Оповещение об отсутствии возможности модификации базы пользователей ПКО

При нажатии кнопки <OK> в сообщении, приведённом на рисунке 14, появляется главное окно программы ACED32.EXE, приведённое на рисунке 15, с помощью которого Контролер может выполнять просмотр правил разграничения доступа пользователей ПКО.

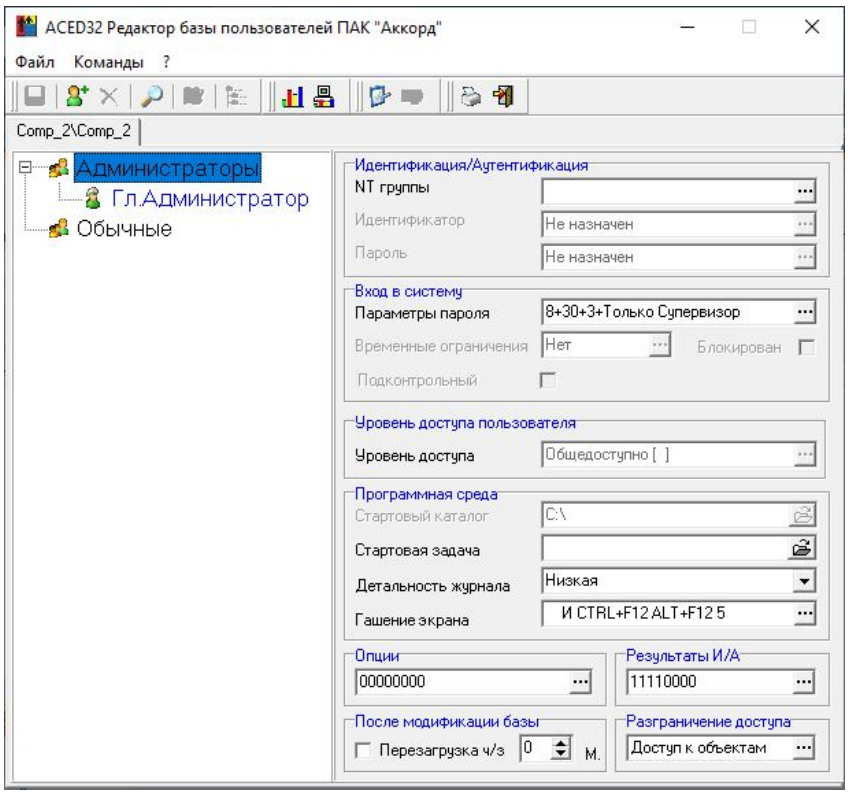

Рисунок 15 – Главное окно программы ACED32.EXE

После выхода из программы ACED32.EXE появляется сообщение о том, что база пользователей ПКО не модифицирована (рисунок 16).

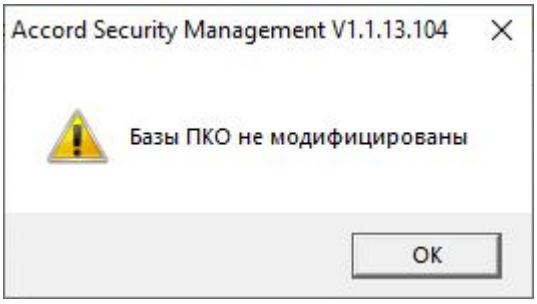

Рисунок 16 – Сообщение о том, что база ПКО не модифицирована

Если необходимо определить, зарегистрирован ли компьютер в системе, следует нажать кнопку <Поиск> во вкладке «Компьютеры» (рисунок 11). При нажатии кнопки появляется окно, приведённое на рисунке 17, в котором необходимо указать IP-адрес компьютера или его имя.

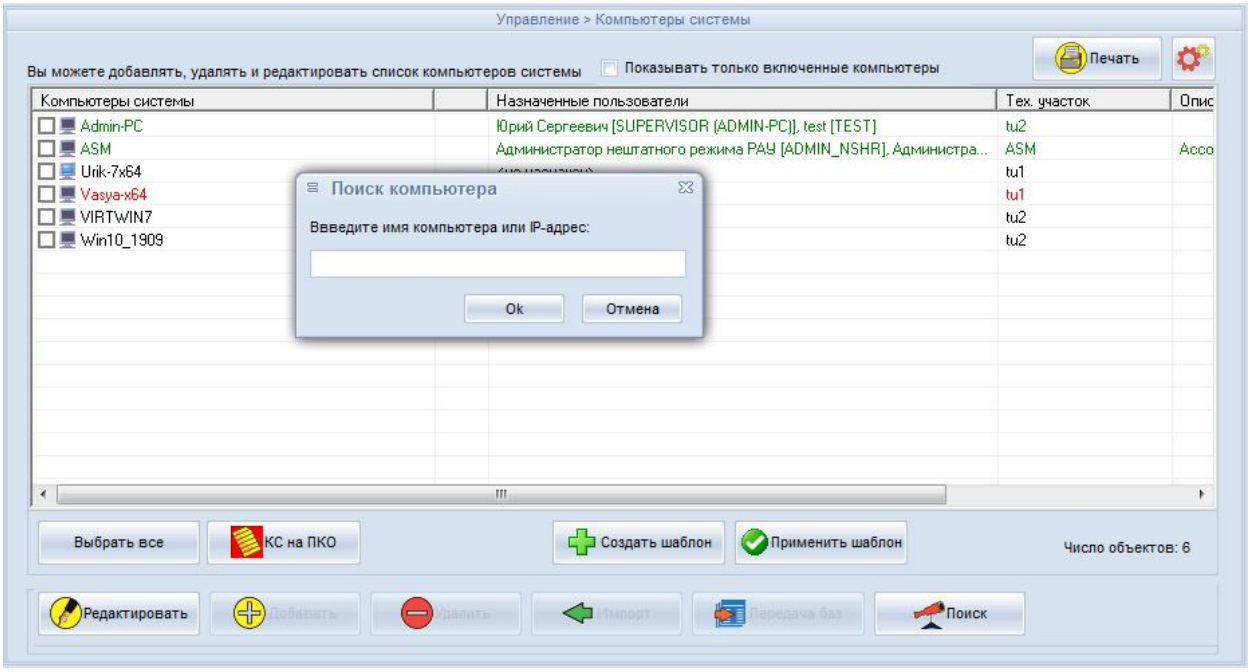

Рисунок 17 – Поиск компьютера по имени или IP-адресу

Если данный компьютер зарегистрирован в системе, будет выделена строка, соответствующая данному компьютеру, как показано на рисунок 18.

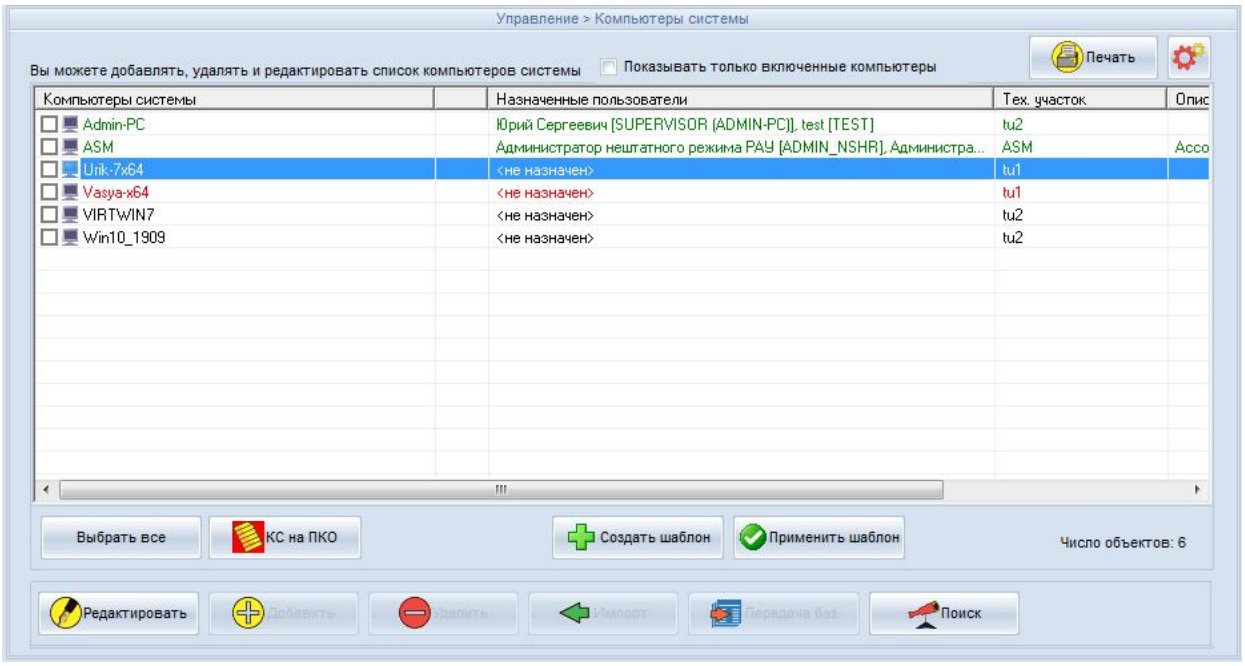

Рисунок 18 – Найден компьютер

Если данный компьютер не зарегистрирован в системе, в нижней части окна появится сообщение «Компьютер не найден!», как показано на рисунке 19.

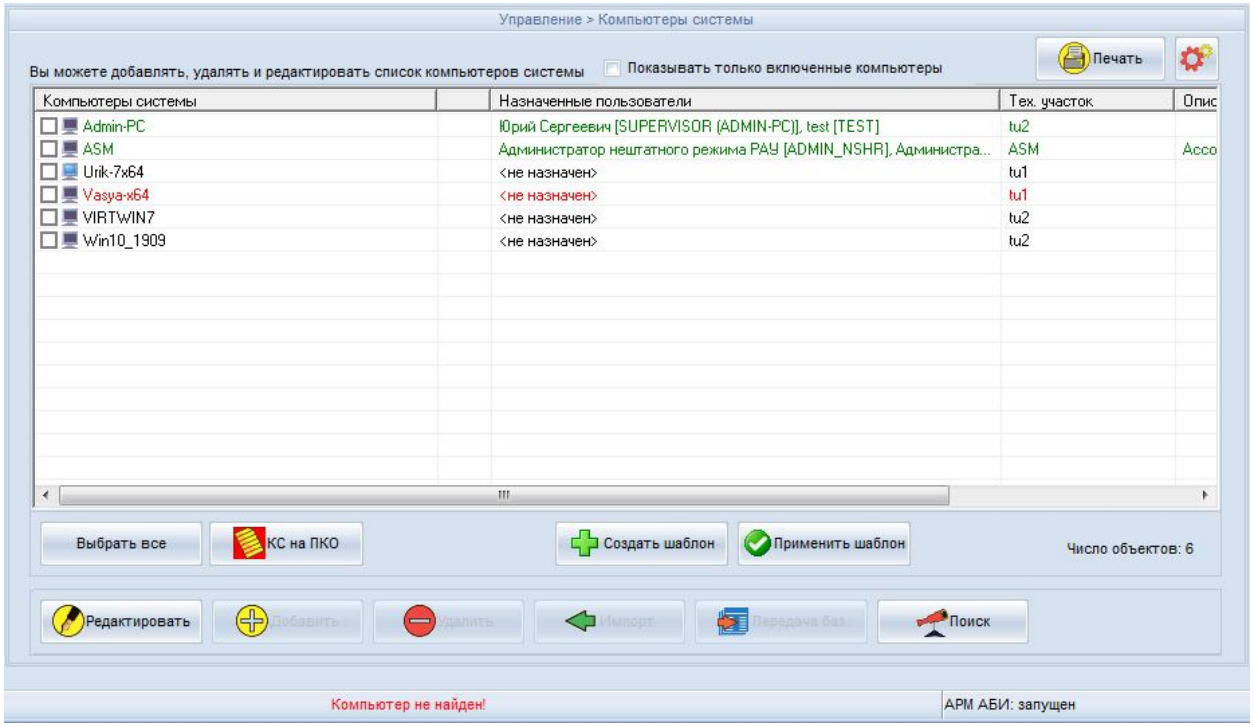

Рисунок 19 - Сообщение о том, что компьютер не найден

4.1.5 Вкладка «Технологические участки»

Во вкладке «Управление > Технологические участки системы», приведённой на рисунке 20, Контролер РАУ выполняет процедуры просмотра технологических участков.

Примечание. Просмотр технологических участков возможен только при выборе режима работы СЦУ (смотри документ 11443195.4012-053 91 «Руководство администратора информационной безопасности»).

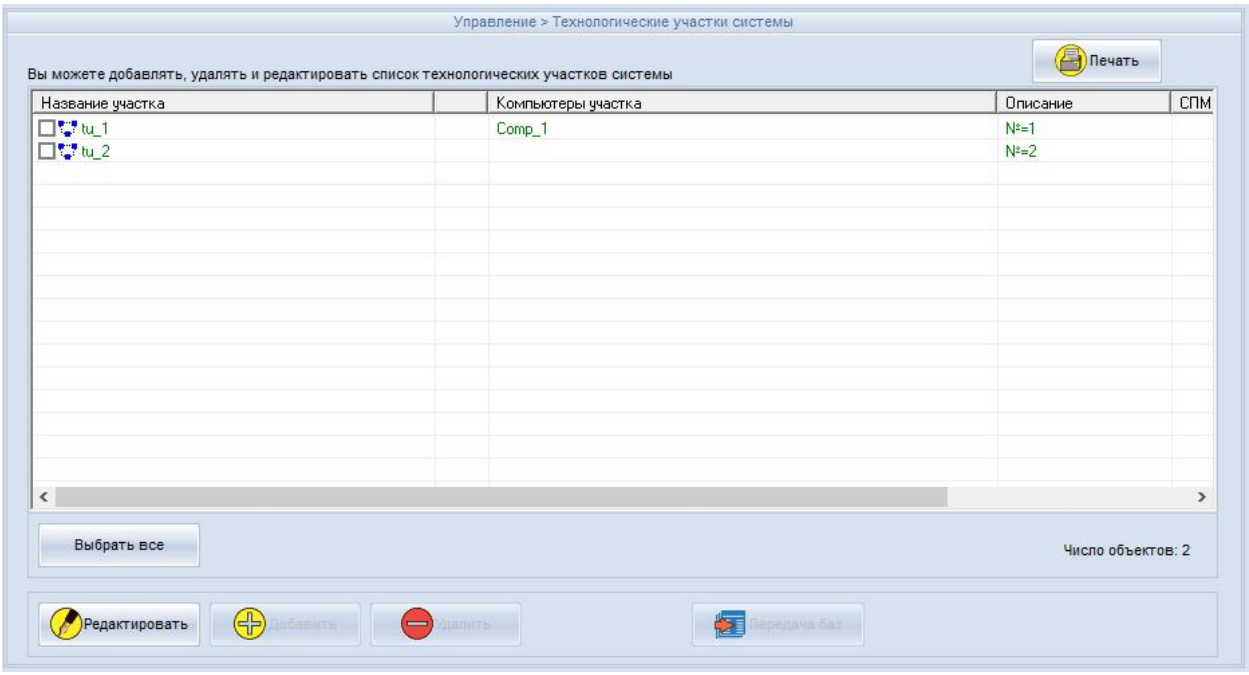

Рисунок 20 - Технологические участки системы

4.1.6 Вкладка «Учётные записи»

Во вкладке «Управление > Учётные записи», приведённой на рисунке 21, Контролер РАУ осуществляет процедуры просмотра списка учетных записей, печати информации об учетных записях и поиска учетных записей по идентификатору.

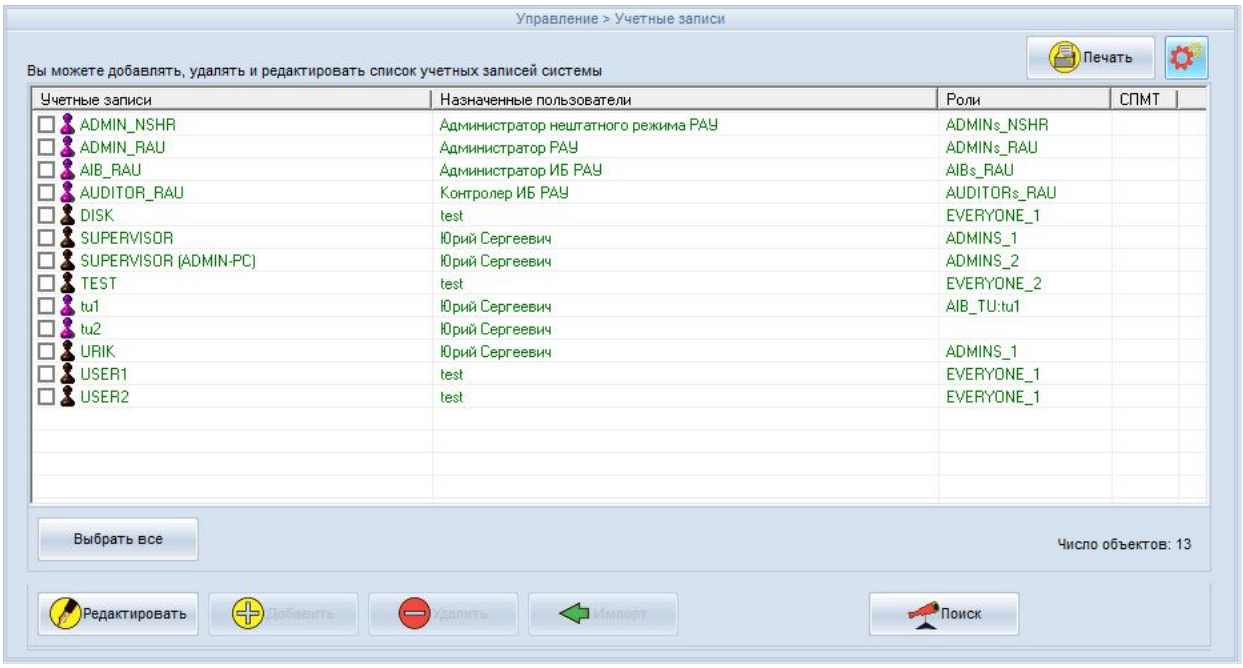

Рисунок 21 - Учётные записи

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

При ее нажатии появляется окно, приведённое на рисунке 22, в котором следует выбрать способ печати: в файл или на принтер, тип выводимой информации: имя учётной записи, имя назначенного ей пользователя, имя роли. При печати в файл следует также указать разделитель.

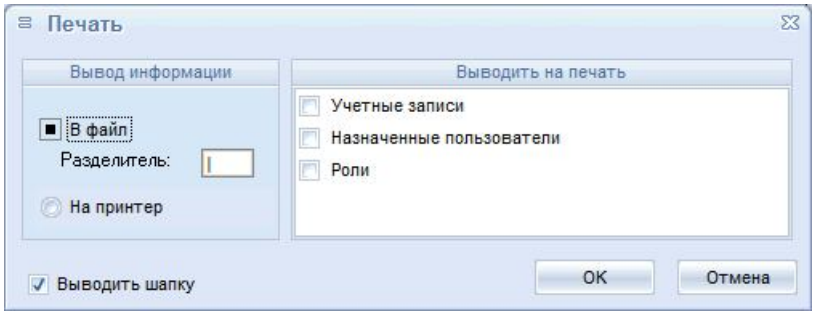

Рисунок 22 - Печать информации об учетной записи

Для отображения в списке учётных записей информации о наличии списков файлов контроля целостности, списков задач и о стартовых задачах нужно в окне, приведенном на рисунке 21, нажать кнопку <Настройка отображения информации>. При её нажатии появляется окно, приведённое на рисунке 6, в котором устанавливаются флаги напротив той информации, которую следует отобразить.

После добавления отображаемой информации в таблице учётных записей появляется столбец под названием «ПКО». Наличие литеры «К» в данном столб-

це 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.

Если необходимо определить, какой учётной записи принадлежит некоторый идентификатор, следует нажать кнопку <Поиск> на вкладке «Учётные записи» (рисунок 21). Появится сообщение «Предъявите идентификатор», приведённое на рисунке 23.

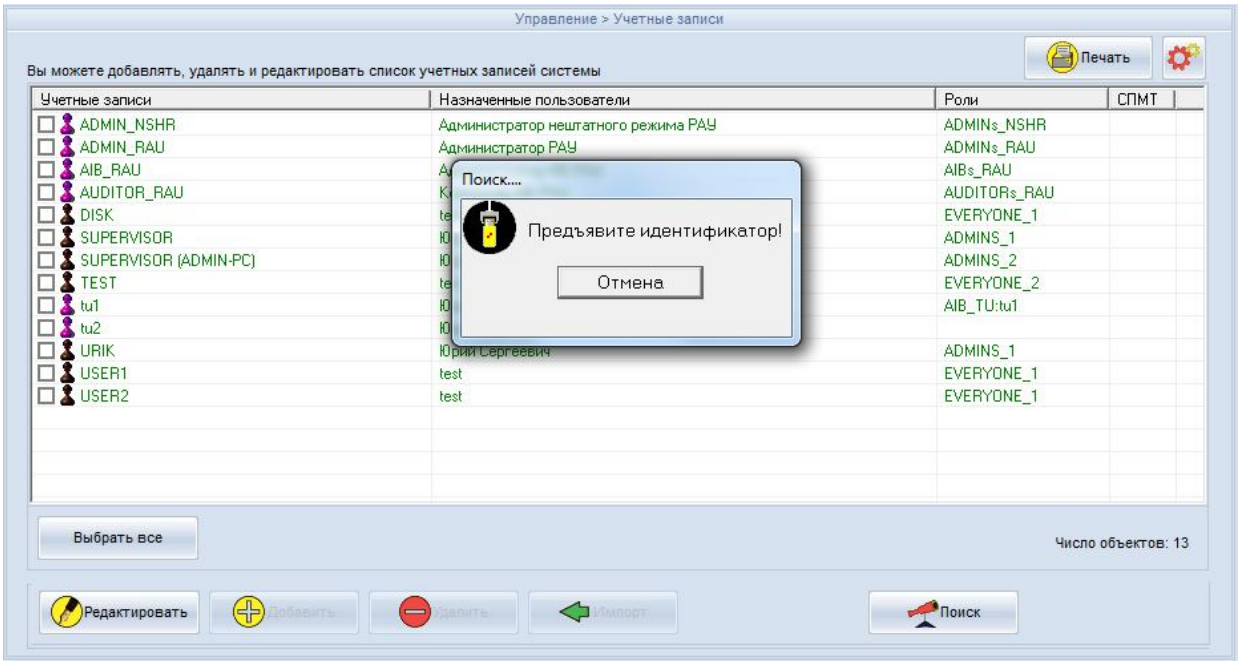

Рисунок 23 - Окно с сообщением «Предъявите идентификатор»

Если предъявленный идентификатор назначен какой-либо учётной записи, эта учетная запись будет выделена, как показано на рисунке 24.

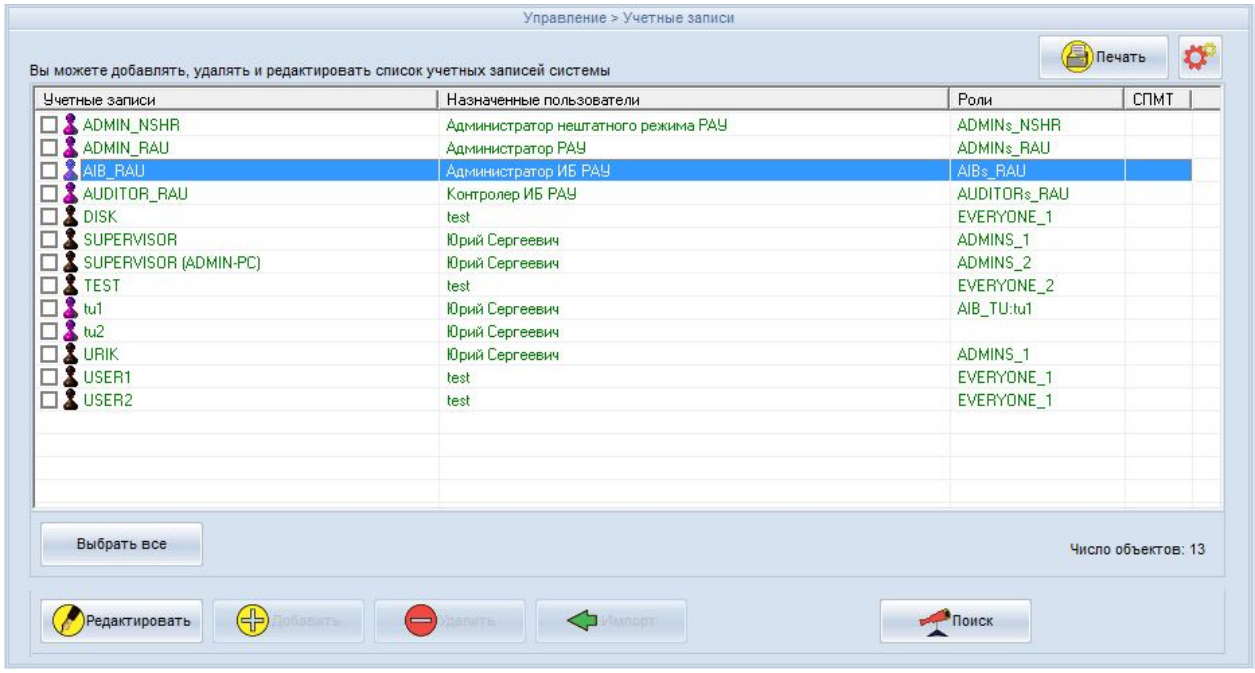

Рисунок 24 - Учетная запись, которой назначен идентификатор

Если предъявленный идентификатор не назначен никакой учётной записи, в нижней части окна появится сообщение «Идентификатор не зарегистрирован!», как показано на рисунке 25.

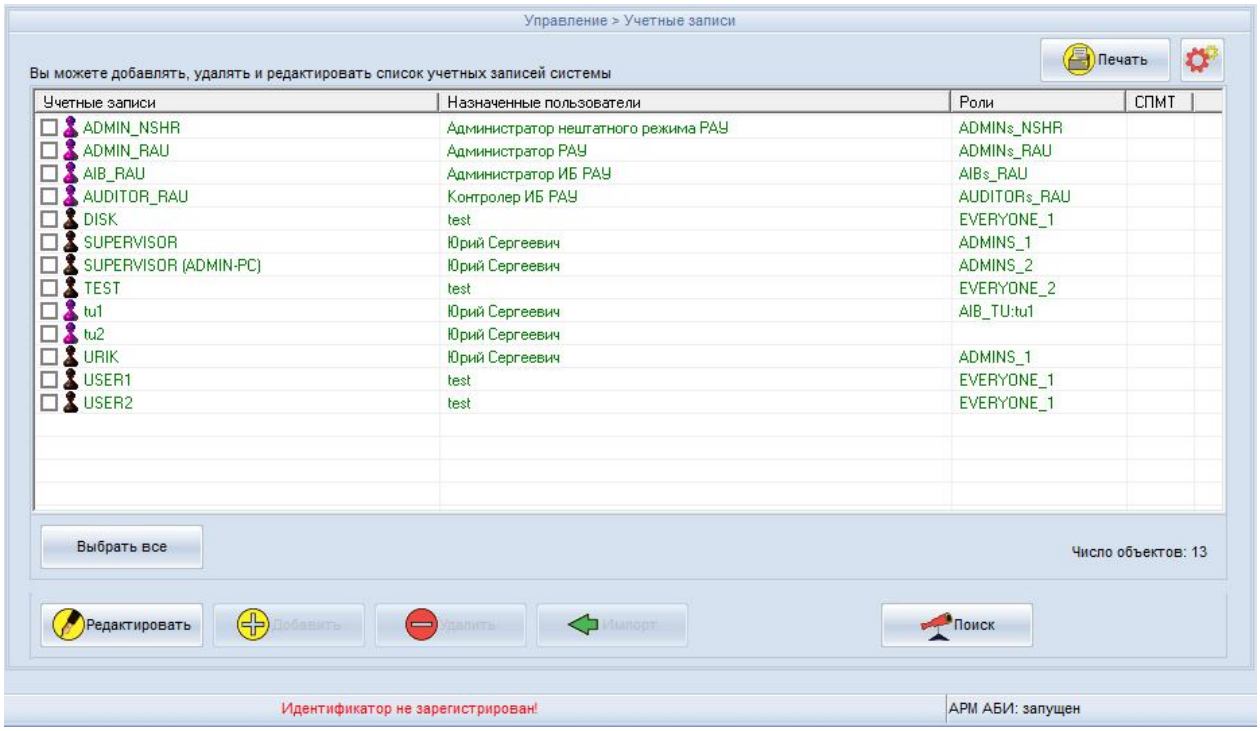

Рисунок 25 - Сообщение о том, что идентификатор не зарегистрирован

4.1.7 Вкладка «USB-устройства»

Во вкладке «Управление > USB-устройства», приведённой на рисунке 26, Контролер РАУ осуществляет просмотр списка разрешенных для использования USB-устройств.

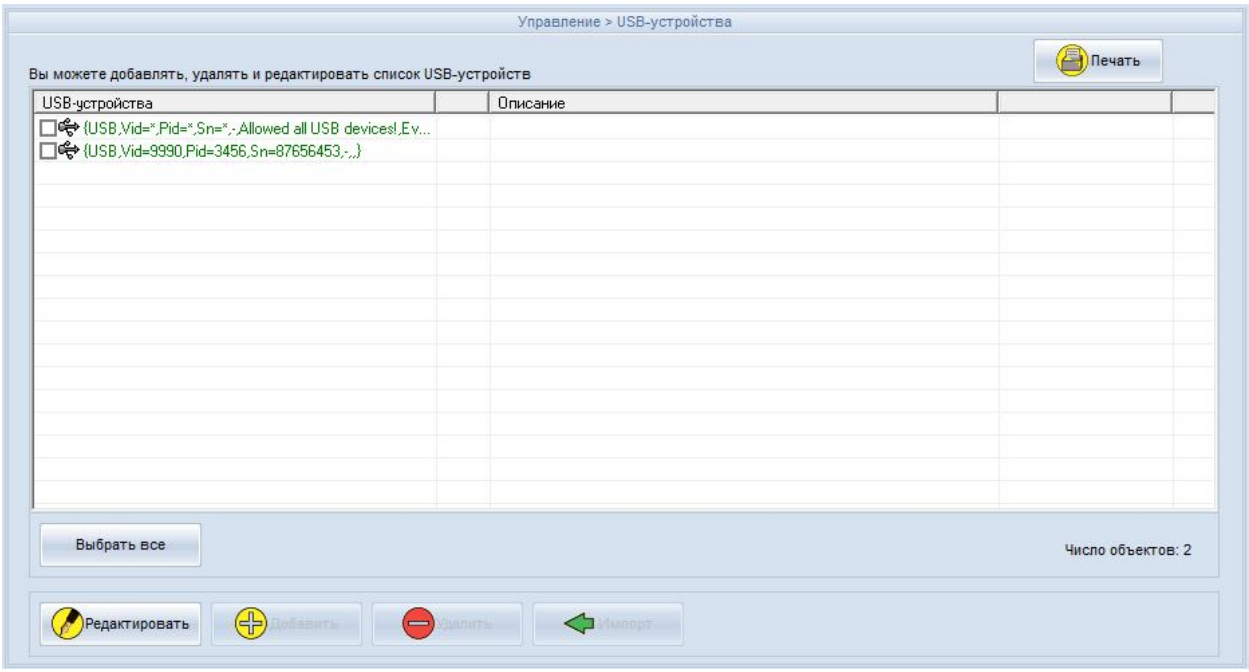

Рисунок 26 – Вкладка «USB-устройства»

4.2 Просмотр журналов событий

4.2.1 Общие сведения

Во вкладке «Журналы» Контролер РАУ осуществляет просмотр журналов, а также их экспорт для дальнейшего анализа в системах мониторинга.

В РАУ существуют журналы трех типов:

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

4.2.2 Оперативный журнал

4.2.2.1 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 сервере централизованного управления в следующих файлах:

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

дате в формате дата – месяц- год. В файлах хранится вся информация оперативного журнала, не записываемая в файл «AcSetup_YYY.log».

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

ВНИМАНИЕ! Чтобы 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 27.

С помощью элементов интерфейса окна, приведённого на рисунке 27, Администратор ИБ технологического участка выполняет следующие функции:

- просмотр сообщений оперативного журнала на СЦУ. Данная функция описана в пункте 4.2.2.2;
- конвертирование оперативного журнала. Данная функция описана в пункте 4.2.2.3;
- экспортирование оперативного журнала. Данная функция описана в пункте 4.2.2.4;
- импортирование оперативного журнала. Данная функция описана в пункте 4.2.2.5;
- создание фильтра оперативного журнала. Данная функция описана в пункте 4.2.2.6.

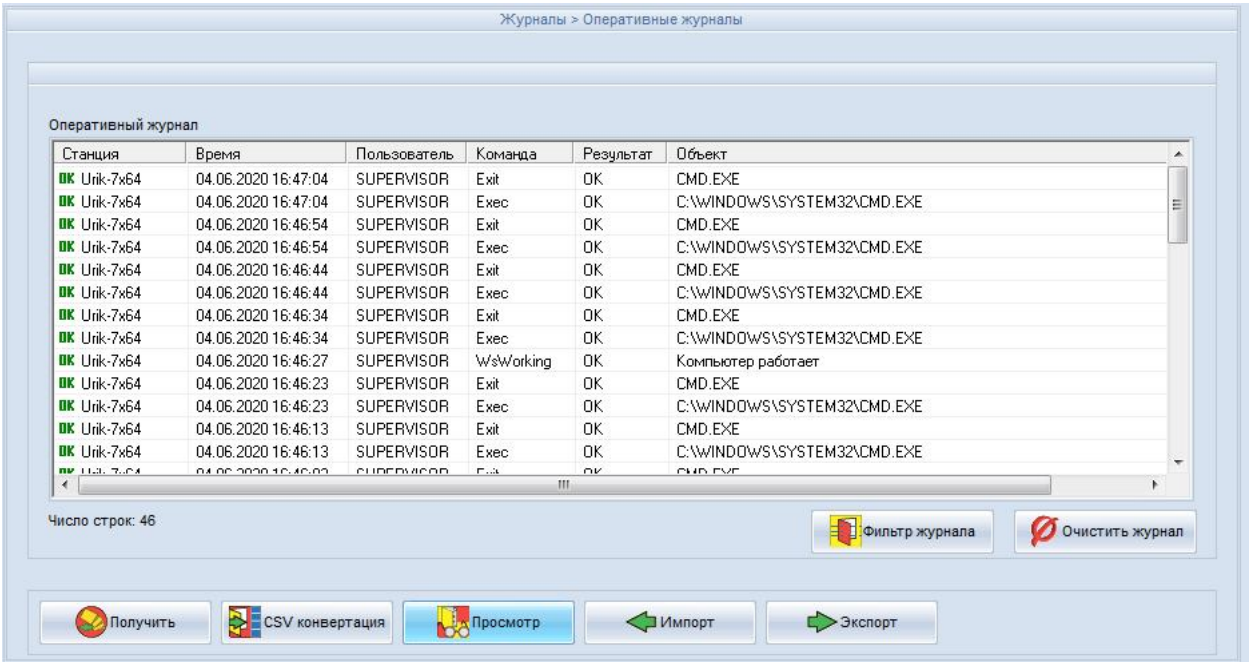

Рисунок 27 - Оперативные журналы

4.2.2.2 Просмотр сообщений оперативного журнала

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

Для просмотра оперативного журнала на СЦУ необходимо в окне, приведённом на рисунке 27, нажать кнопку <Просмотр>. После этого появляется окно выбора журналов, приведённое на рисунке 28.

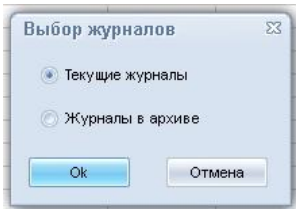

Рисунок 28 - Выбор журналов для просмотра

В данном окне осуществляется выбор журналов для просмотра: «Текущие журналы» позволяет выбрать файлы журналов в каталоге \Asm\AcConNet\Client.Log, «Журналы в архиве» – файлы журналов в каталоге \Asm\AcConNet\Client.Arc. При нажатии кнопки <Ok> будет выведено окно просмотрщика журналов событий с окном указания конкретного файла журнала. Примерный вид данных окон приведён на рисунке 29.

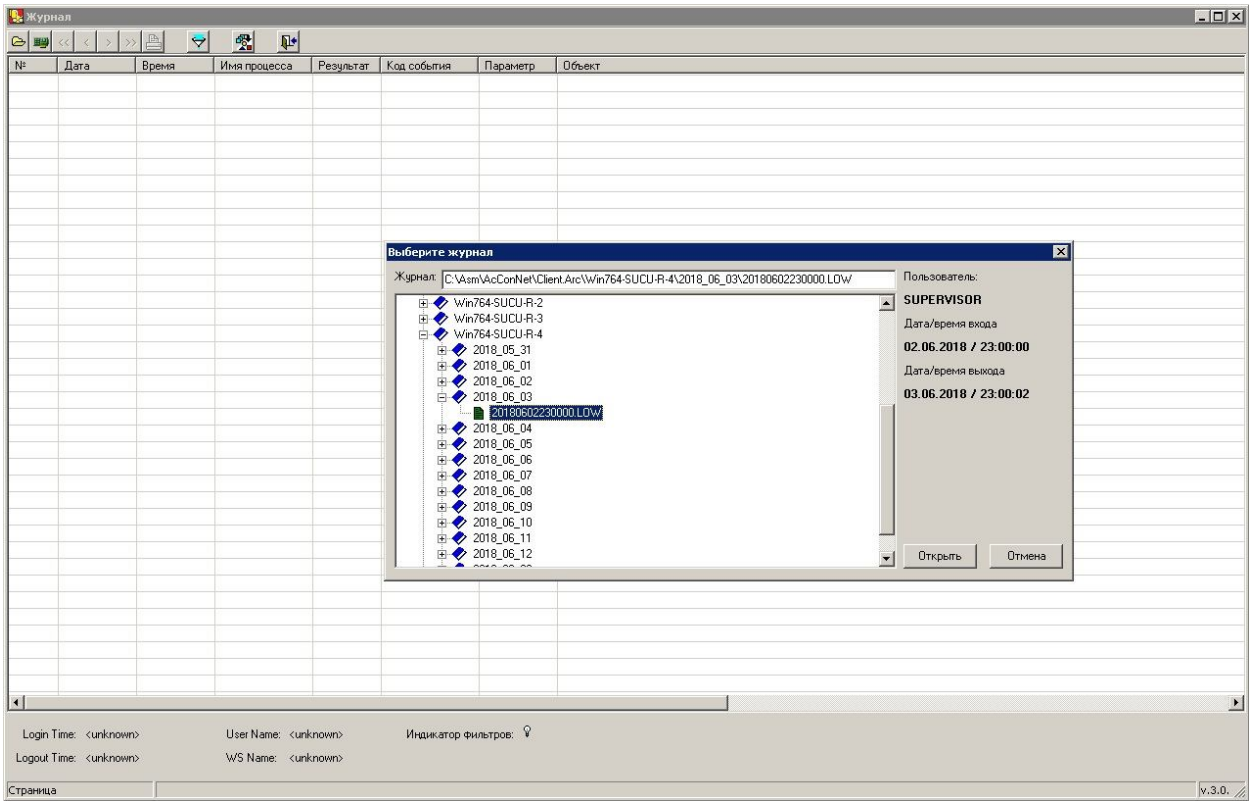

Рисунок 29 - Окно просмотрщика журналов событий

4.2.2.3 Конвертирование оперативного журнала

Администратору ИБ технологического участка предоставляется возможность конвертирования оперативного журнала в файл формата *.CSV или *.XML. Формат, в который будет конвертироваться журнал, выбирается в настройках фильтров подсистемы управления событиями информационной безопасности. Для конвертирования оперативного журнала необходимо в окне, приведенном на рисунке 27, нажать кнопку <CSV конвертация> или <XML конвертация> (в зависимости от выбранного формата файла экспорта). После этого в каталоге, указанном в поле «CSV файл для конвертации журналов:» или в поле «XML файл для конвертации журналов», будет создан файл выбранного формата, содержащий данные оперативного журнала. В данный файл помещаются все события из оперативных журналов. В зависимости от настроек параметров экспорта журналов после конвертации всё содержимое журналов может перемещаться в архив – каталог Asm\AcConNet\Client.Arc.

По завершении процедуры преобразования оперативного журнала в общепринятые форматы появляется следующее сообщение:

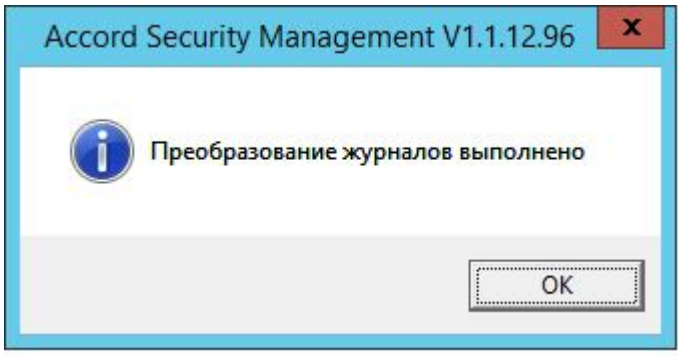

Рисунок 30 – Сообщение о выполненной процедуре конвертации оперативного журнала в общепринятые форматы

При выполнении процедуры конвертации оперативного журнала кнопками <CSV конвертация> или <XML конвертация> в консоли AsmT.exe информация о выполненной процедуре (дата и время запуска и окончания процедуры конвертации, список конвертированных файлов оперативного журнала) записывается в журнал Low2XmlCsv.log (рисунок 31).

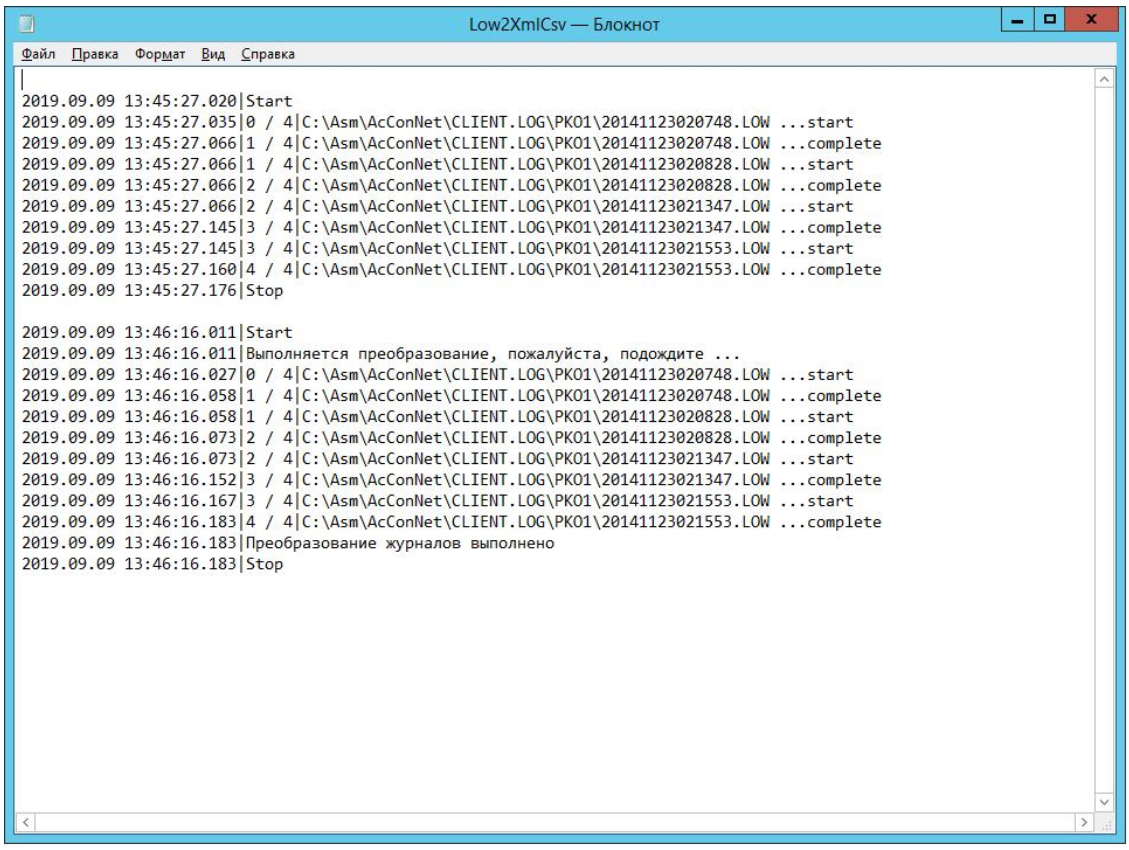

Рисунок 31 – Журнал Low2XmlCsv.log после выполнения процедуры конвертации кнопками <CSV конвертация> или <XML конвертация> в консоли AsmT.exe

Процедуру конвертации также можно выполнить утилитой Low2XmlCsv.exe[1]. Информация о выполненной процедуре также записывается в журнал Low2XmlCsv.log[2] (однако при этом в журнале не отображаются сообщения о начале и окончании выполнения преобразования журналов, рисунок 32).

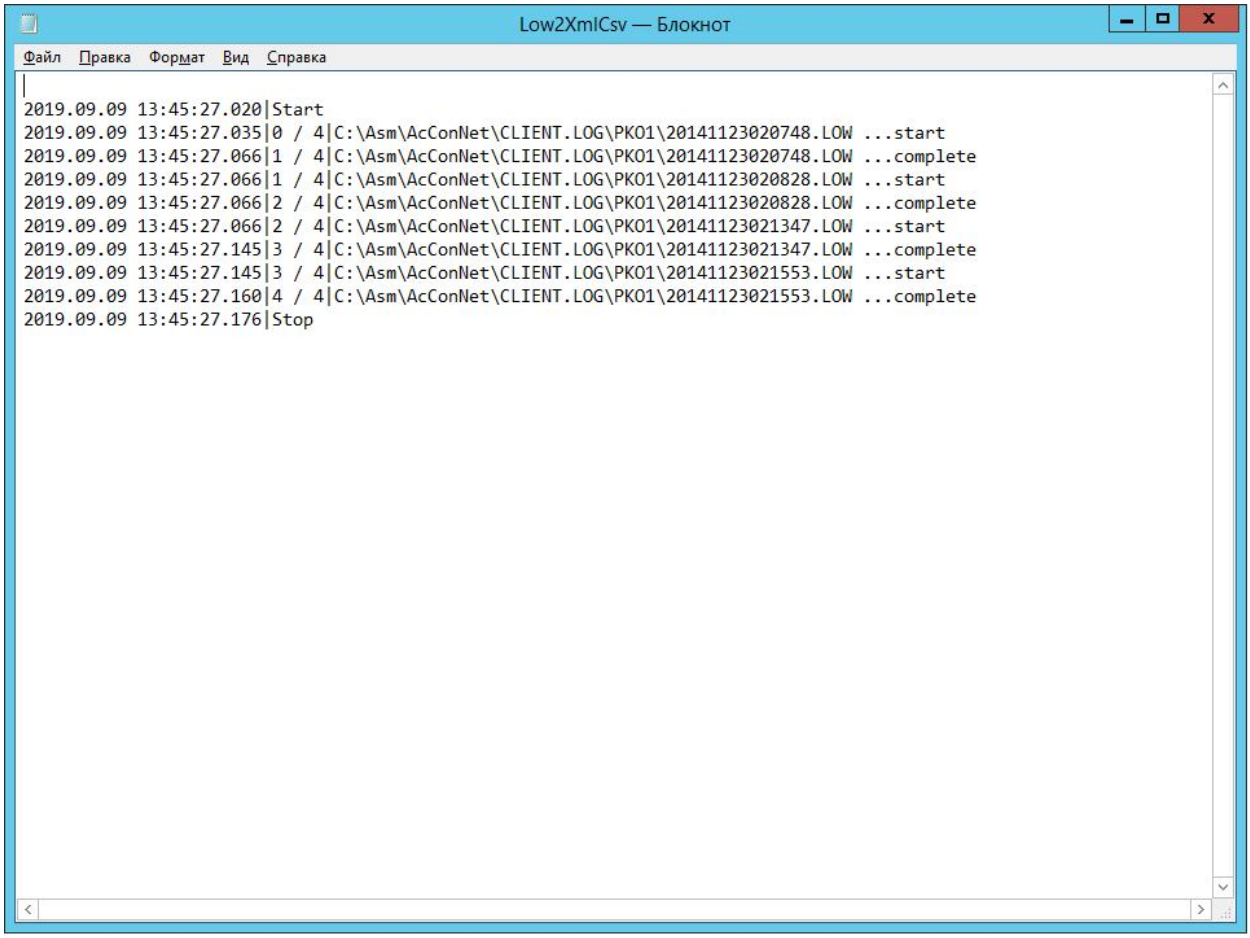

Рисунок 32 - Журнал Low2XmlCsv.log после выполнения процедуры конвертации утилитой LowToCsvXml.exe

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 появляется сообщение:

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

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

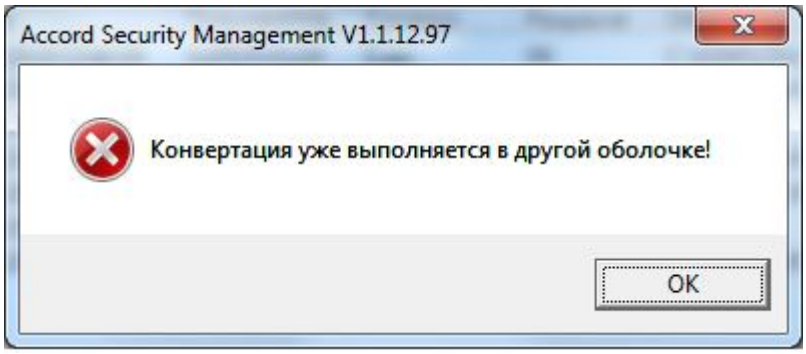

Рисунок 33 – Сообщение о невозможности запуска консоли при выполнении процедуры конвертации

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».

4.2.2.4 Экспортирование оперативного журнала

Чтобы экспортировать оперативный журнал (например, для дальнейшего анализа в системах мониторинга), необходимо в окне, приведённом на рисунке 27, нажать кнопку <Экспорт>. Появляется окно выбора каталога. Выбрав каталог для экспорта журнала, следует нажать <Применить>.

4.2.2.5 Импортирование оперативного журнала

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

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

- подключает полученный отчуждаемый носитель к СЦУ. При использовании в качестве отчуждаемого USB-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 27, нажимает кнопку <Импорт>;
- в появившемся окне выбирает необходимый каталог и нажимает кнопку <Применить>.

4.2.2.6 Создание фильтра оперативного журнала

Для создания фильтра оперативного журнала следует в окне, приведённом на рисунке 27, нажать кнопку <Фильтр журнала>. Появится окно, приведенное на рисунке 34.

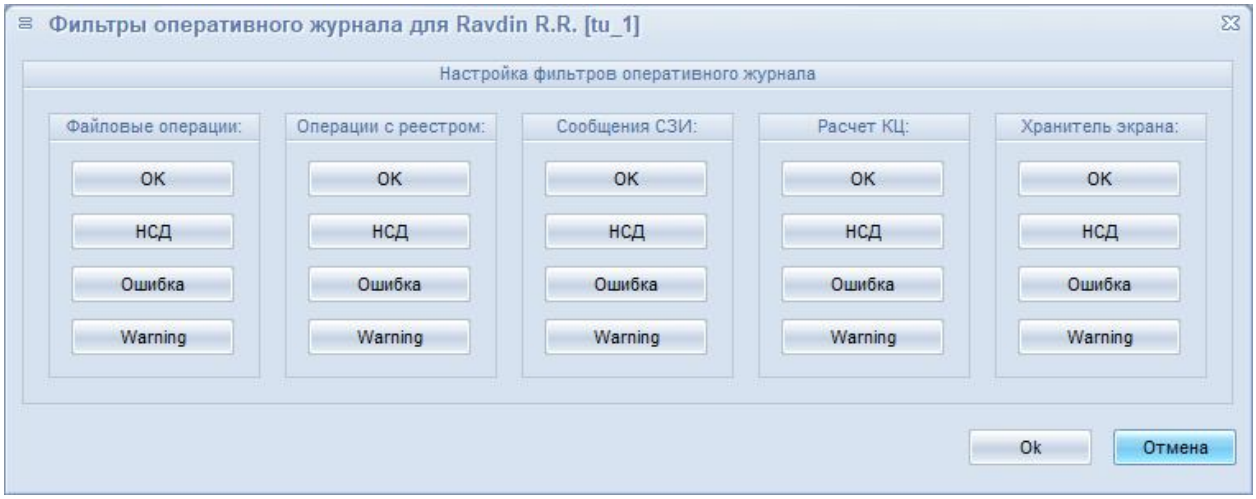

Рисунок 34 - Фильтры оперативного журнала для текущей учетной записи

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

4.2.3 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 35.

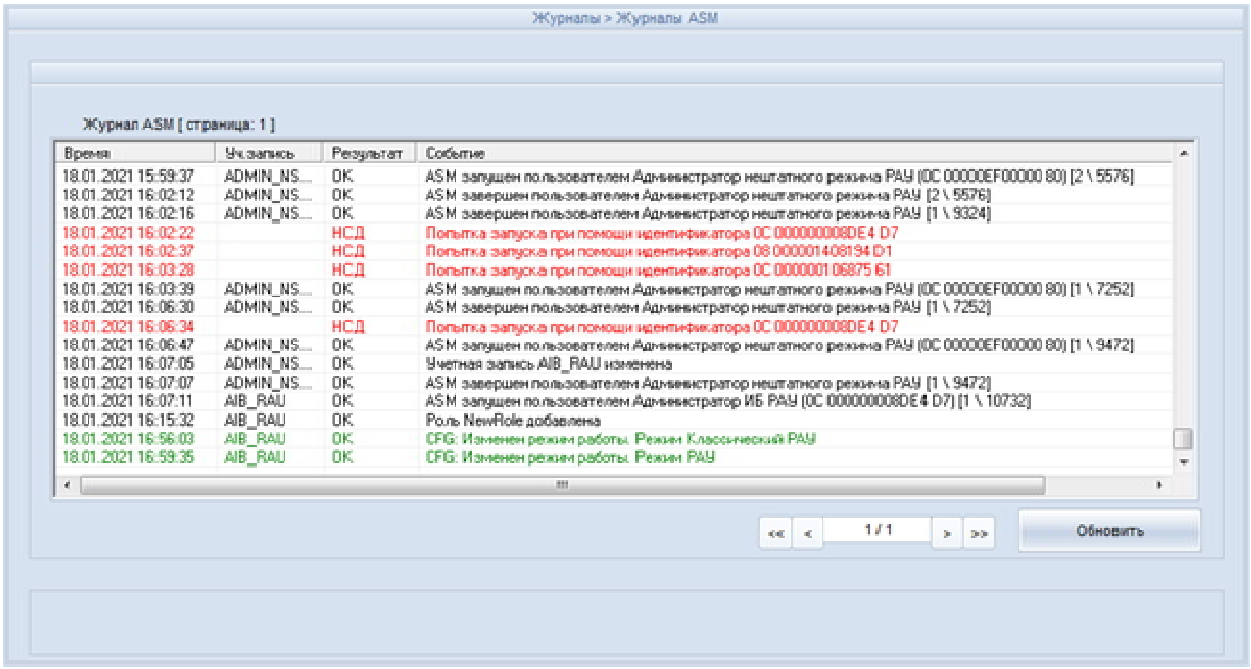

Рисунок 35 - Журнал ASM

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, данное поле будет содержать имя учётной записи Администратора ИБ. Если событием является изменение пароля пользователя на ПКО, данное поле будет содержать имя «SYSTEM». Если в поле «Сообщение о событии» отображается значение «НСД. Попытка запуска при помощи идентификатора IDNAME», 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 в 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 учетной записи.

4.2.4 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. 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 36.

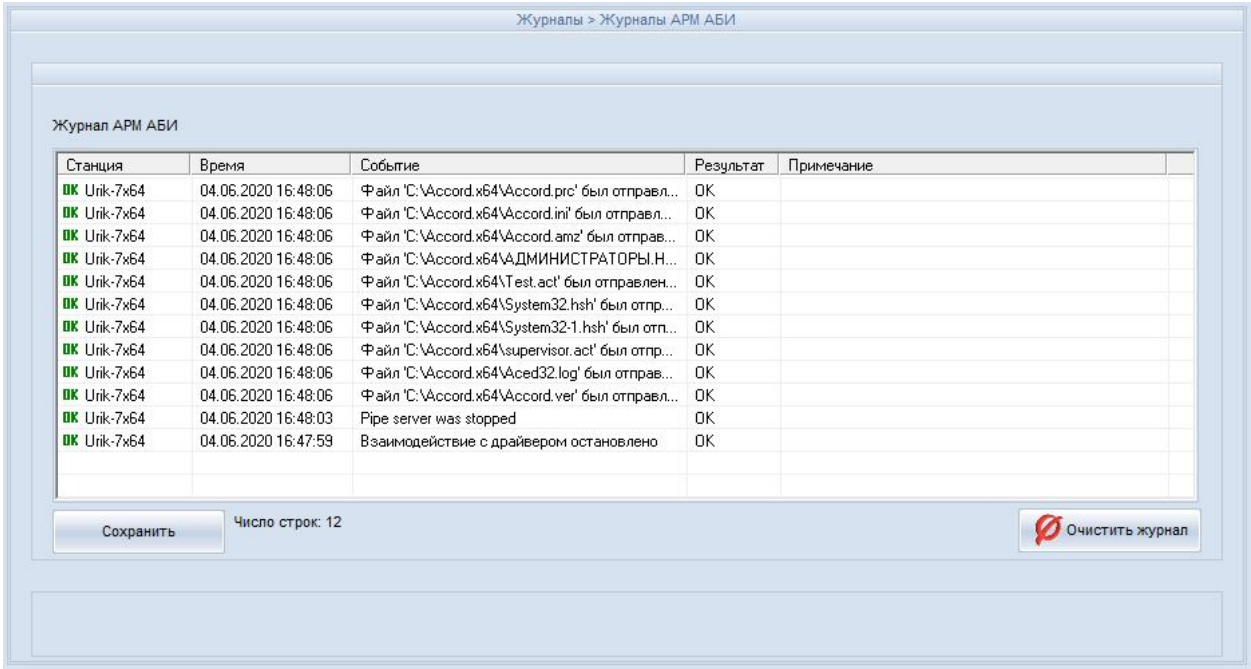

Рисунок 36 - Журнал АРМ АБИ

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

- если операция выполнена успешно, 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, 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 36, нажать кнопку <Сохранить>. В появившемся окне сохранения файла нужно задать имя файла, в который будет сохранён журнал АРМ АБИ, и нажать кнопку <Сохранить>.

4.3 Просмотр настроек РАУ

Во вкладке «Настройки» Контролер РАУ имеет возможность просматривать настройки РАУ, настройки фильтров оперативного журнала, настройки фильтров экспорта журналов РАУ.

Просмотр настроек РАУ осуществляется во вкладке «Настройки > Основные настройки», приведённой на рисунке 37.

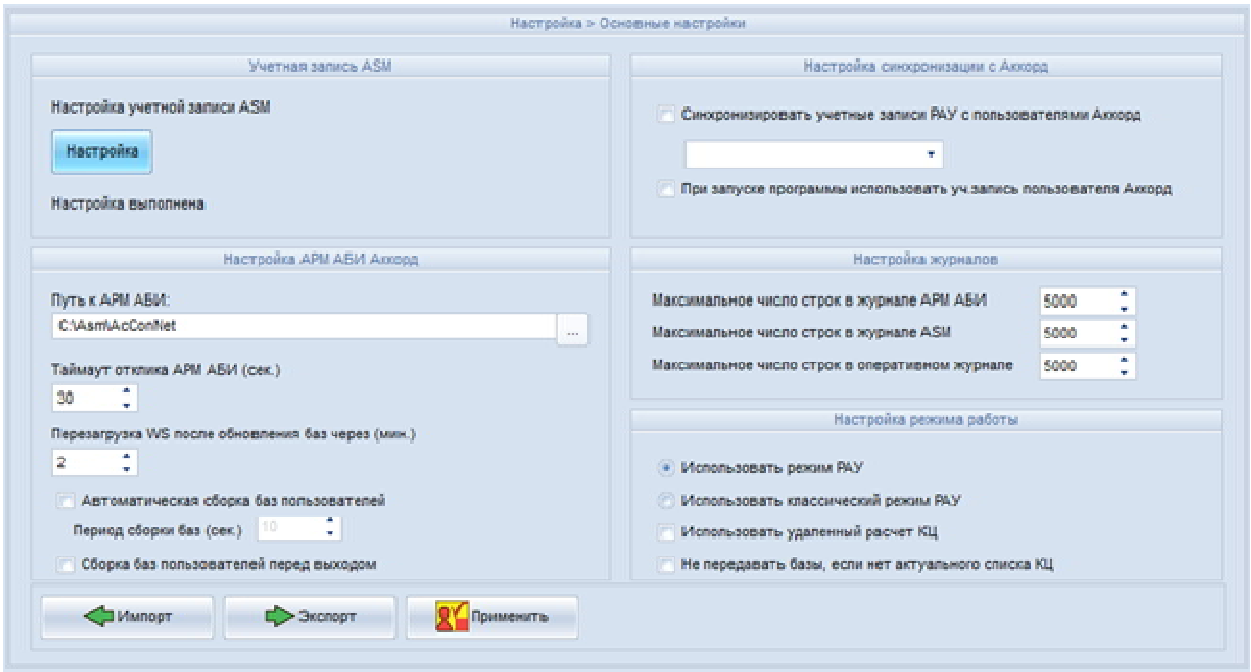

Рисунок 37 – Просмотр основных настроек РАУ

Просмотр настроек фильтров оперативного журнала осуществляется во вкладке «Настройки > Оперативный журнал», приведённой на рисунке 38.

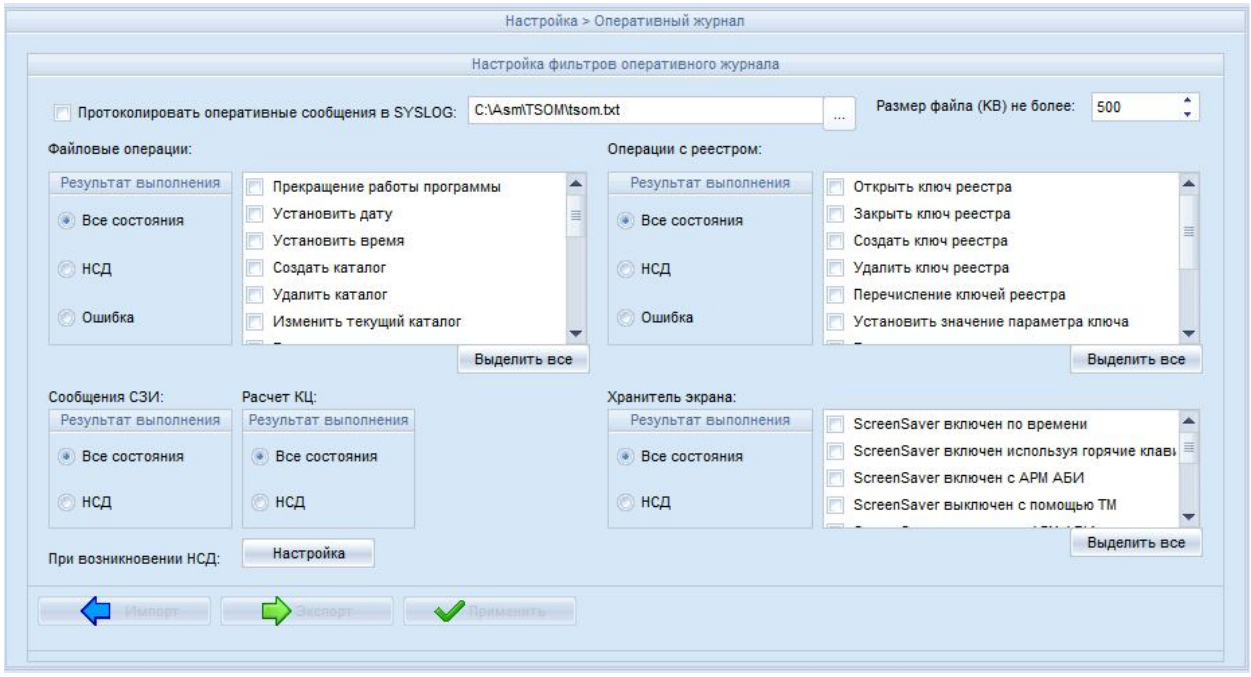

Рисунок 38 – Просмотр настроек фильтров оперативного журнала

Просмотр настроек фильтров экспорта журналов РАУ осуществляется во вкладке «Настройки > Оперативный журнал», приведённой на рисунке 39.

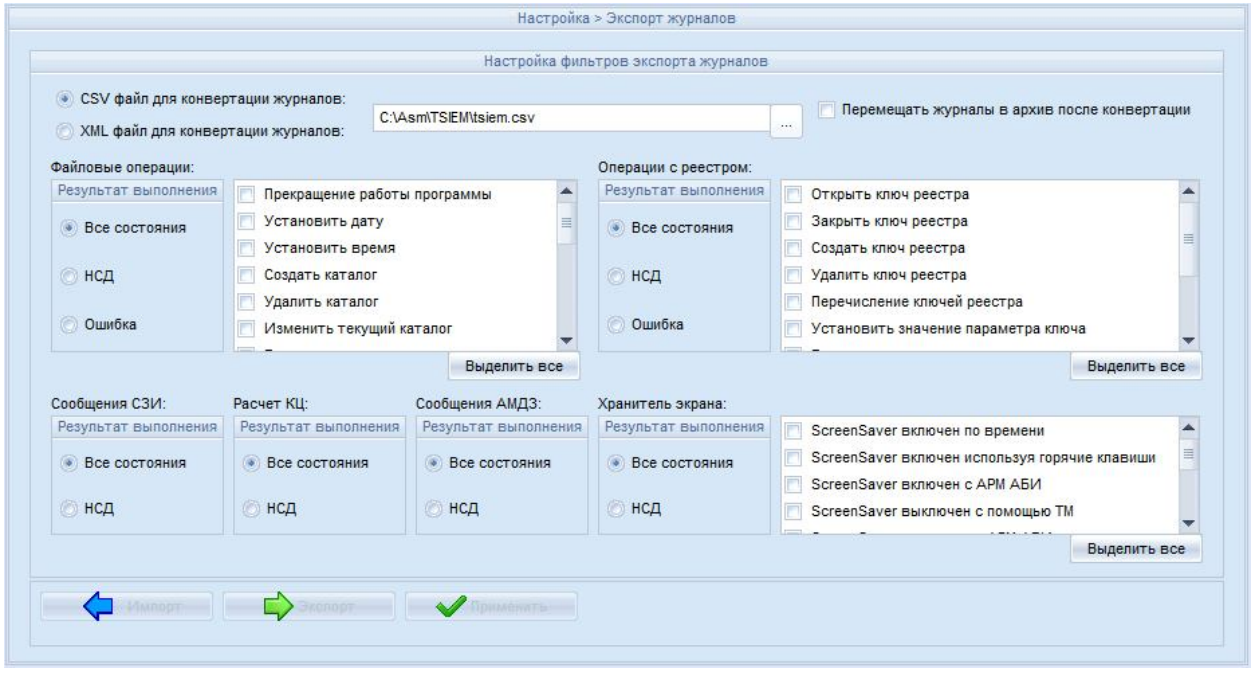

Рисунок 39 – Просмотр настроек фильтров экспорта журналов

5 Перечень оповещающих сообщений

Оповещающие сообщения выводятся только на экран и не фиксируются ни в каких журналах. Перечень оповещающих сообщений, действия, при которых генерируются данные сообщения, а также действия, которые необходимо предпринять при появлении данных сообщений, приведены в таблице 1.

Таблица 1 - Перечень оповещающих сообщений

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

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

Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
В идентификаторе нет свободных страниц для записи»	Попытка регистрации 32-ой рабочей станции без сохранения списка на 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 межу сервером централизованного управления и ПКО. При отсутствии связи, восстановите ее. 2 Обратитесь к Администратору ИБ для проверки существования на сервере централизованного управления учётной записи ASM, под которой произошла данная ошибка
Ошибка чтения ТМ-идентификатора	При работе в автономном режиме в ответ на запрос ТМ-идентификатор был неправильно прислонен к съемнику информации	Снова приложите ТМ-идентификатор к съемнику информации после появления нового запроса
Отправлена база пользователей	При работе в автономном режиме отправлена база пользователей	Данное сообщение информирует об успешной отправке базы пользователей в автономном режиме. Никаких действий при его появлении выполнять не нужно
Файлы баз были экспортированы	При работе в автономном режиме выполнен экспорт файлов	Данное сообщение информирует об успешном экспортировании файлов баз в автономном режиме. Никаких действий при его появлении выполнять не нужно
Файлы баз были импортированы	При работе в автономном режиме выполнен импорт файлов	Данное сообщение информирует об успешном импортировании файлов баз в автономном режиме. Никаких действий при его появлении выполнять не нужно

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

6 Перечень сообщений 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 3. Используются следующие условные обозначения:

USERNAME – имя пользователя;

IDNAME – уникальный идентификационный номер (UID) идентификатора;

WSNAME – имя компьютера;

FRAMENAME – название тех. участка;

ACCOUNTNAME – имя учетной записи пользователя;

ROLENAME – имя роли;

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

NT_GROUPNAME – имя группы пользователей NT;

TASKNAME – стартовая задача;

FILENAME – полное имя файла (включая путь);

LOG_DETAIL – детальность (уровень детализации) журнала;

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

ACCESS_LEVEL – уровень доступа пользователя;

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

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

SERVERNAME – имя сервера, на котором хранится база пользователей;

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

ровка печати, Блокировка клипборда, Может изменять дату/время, Запрет доступа к общим ресурсам, Полный доступ для АРМ 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 2.

Таблица 2 - 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 3 приводятся тексты в таком содержании, в котором они отображаются в окне журнала ASM. В файле журнала сообщения фиксируются в структуре, описанной в пункте 4.2.2.

Таблица 3 – 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
	Компьютеры успешно добавлены в базу	Процедура импорта компьютеров (ПКО) в базу ASM выполнена успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
	CFG: TSIEM Изменен фильтр ScreenSaver ScreenSaver выключен с помощью ТМ АБИ = ScreenSaver_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «ScreenSaver выключен с помощью ТМ АБИ»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр ScreenSaver Выключен временной контроль ScreenSaver-а = ScreenSaver_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «Выключен временной контроль ScreenSaver-а»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр ScreenSaver Включен временной контроль ScreenSaver-а = ScreenSaver_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «Включен временной контроль ScreenSaver-а»	Никаких действий выполнять не нужно
	CFG: TSIEM Изменен фильтр ScreenSaver Попытка разблокировать чужим ТМ = ScreenSaver_NUMBER	Выполнена корректировка настроек TSIEM: установлен / снят флаг «Попытка разблокировать чужим ТМ»	Никаких действий выполнять не нужно
Сообщения об изменении параметров конфигурации ПАК «Аккорд» на ПКО (сообщения с	INI: На ПКО WSNAME изменен список привилегированных процессов	Редактирование списка привилегированных процессов ПКО выполнено успешно	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно

Тип сообщения	Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
префиксом INI). Сообщения данного типа фиксируются в журнале ASM	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: WSNAME Механизм разграничения доступа Мандатный = No	Снят флаг «Мандатный» в параметрах конфигурации СЗИ	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	INI: WSNAME Механизм разграничения доступа Мандатный = Yes	Установлен флаг «Мандатный» в параметрах конфигурации СЗИ	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно
	INI: WSNAME Механизм разграничения доступа Процессы = No	Снят флаг «+процессы» в параметрах конфигурации СЗИ	Данное сообщение информирует об успешном выполнении операции. Никаких действий при его появлении выполнять не нужно

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

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

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

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

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

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

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

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

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

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

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

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

7 Перечень сообщений ПАК «Аккорд» на подконтрольных объектах

Перечень сообщений, генерируемых ПАК «Аккорд» на подконтрольных объектах, и их описание приведены в таблице 4.

Таблица 4 – Перечень сообщений ПАК «Аккорд» на подконтрольных объектах

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

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

Сообщение	Описание
Search	Поиск файла/каталога
SetDate	Установка системной даты
SetTime	Установка системного времени
Traverse	Проверка существования пути
RegCloseKey	Закрытие ключа реестра
RegCreateKey	Создание ключа реестра
RegCreateValue	Создание переменной в ключе реестра
RegDeleteKey	Удаление ключа реестра
RegDeleteValue	Удаление переменной из ключа реестра
RegEnumKey	Поиск ключей реестра
RegEnumValue9	Поиск переменных в ключе реестра
RegOpenKey0	Открытие ключа реестра
RegQueryValue	Чтение переменной из ключа реестра
RegSetValue	Изменение значения переменной в ключе реестра
SSOffAtAdmin ScreenSaver	Разблокировка ПКО с помощью ТМ администратора АРМ АБИ (хранитель экрана выключен с помощью ТМ администратора АРМ АБИ)
SSOffAtRemoute ScreenSaver	Разблокировка ПКО с помощью АРМ АБИ (хранитель экрана выключен удаленно с помощью АРМ АБИ)
SSOffAtTM ScreenSaver	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 АРМ АБИ

В таблице 5 приведены сообщения журнала АРМ АБИ и описания этих сообщений. Приняты следующие условные обозначения:

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

Таблица 5 – Перечень сообщений АРМ АБИ

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

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

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

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

Тип сообщения	Наименование сообщения	Описание сообщения
	Ошибка записи конфигурации таймаутов в плату АМДЗ	Ошибка записи параметров времени на ввод пароля и предоставление идентификатора в АМДЗ 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 выполнилась с ошибкой
Информационные сообщения	Версия драйвера Acrun: VERSION	Информация о версии драйвера Аккорд на ПКО
	Версия драйвера АМДЗ: VERSION	Информация о версии драйвера АМДЗ на ПКО
	Версия прошивки АМДЗ: VERSION	Информация о версии прошивки АМДЗ на ПКО
	АМДЗ плата обнаружена	АМДЗ плата обнаружена на ПКО
	Серийный номер платы АМДЗ: AMDZ_BOARD_SERIAL_NUM	Серийный номер платы АМДЗ на ПКО
	Версия ТМ-драйвера АМДЗ: VERSION	Информация о версии ТМ-драйвера на ПКО
	Исполнение команды COMMAND завершено для OBJECT_NAME	Команда принята на ПКО (исполнение не начато)
	Исполнение команды COMMAND завершено	Полученная на ПКО команда от ASMT (или на AcConNet от ПКО) успешно исполнена
	Файл FILE_NAME был скопирован в FOLDER_NAME	Работа с файлами при экспорте/импорте логов/баз
	Инициализация работы с драйверами	Начало работы с драйверами Аккорд и ТМ на ПКО
	Взаимодействие с драйверами остановлено	Работа с драйверами Аккорд и ТМ завершена (при остановке сервиса)
	Команда перечитывания фильтров была отправлена на OBJECT_NAME	Команда на использование новых фильтров принята на ПКО (исполнение не начато)

Тип сообщения	Наименование сообщения	Описание сообщения
	Файл журналов Acrun 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, никакое действие после этого не требуется
	Исполнение команды COMMAND для OBJECT_NAME	Команда была отправлена на ПКО (исполнение не начато)
	Команда COMMAND получена	На ПКО получена команда от ASMT
	Начато исполнение команды COMMAND	На ПКО начато исполнение полученной от ASMT команды (или на AcConNet от ПКО)
	Начато копирование файла FILE_NAME в FOLDER_NAME	Начата работа с файлами при экспорте/импорте логов/баз
	Файл FILE_NAME не был изменен	Файл на сервере централизованного управления идентичен передаваемому файлу с ПКО
	Журналы АМДЗ получены	Прочитан *.azl файл из АМДЗ на ПКО
	База пользователей успешно прочитана из платы АМДЗ	*.amz база прочитана из АМДЗ на ПКО
	Рабочая станция успешно заблокирована	Установлен экран блокировки на ПКО

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

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

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

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

- Для компьютера не назначен Supervisor;
- Операция отменена Администратором.

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

9 Перечень принятых сокращений

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

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

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

СОГЛАСОВАНО

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