СПЕЦИАЛЬНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

«АККОРД-РАУ»

Руководство Администратора

Листов 87

Москва

2022

АННОТАЦИЯ

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

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

СОДЕРЖАНИЕ

1 Введение 6

1.1 Область применения 6

1.2 Функции Администратора РАУ 6

1.3 Комплект поставки 6

2 Назначение и условия применения 7

2.1 Назначение 7

2.2 Условия применения 7

2.2.1 Общие сведения 7

2.2.2 Условия применения сервера централизованного управления 8

2.2.3 Условия применения клиентов РАУ 10

3 Установка и настройка 13

3.1 Порядок развёртывания «Аккорд-РАУ» 13

3.2 Установка ПО сервера централизованного управления 13

3.3 Получение файла лицензии на использование РАУ 17

3.4 Установка ПО клиентов РАУ 17

3.5 Настройка правил разграничения доступа для клиентов РАУ 22

3.6 Создание сетевого идентификатора сервера централизованного управления 23

3.7 Создание в сетевом идентификаторе учетной записи «ASM_ACCOUNT» 25

3.8 Регистрация ПКО 25

3.8.1 Общие сведения 25

3.8.2 Регистрация с помощью сетевого идентификатора 26

3.8.3 Регистрация вручную 30

3.8.4 Регистрация из файла 31

3.8.5 Изменение списка зарегистрированных ПКО 32
3.9 Установка обновлений ПО РАУ 33
3.9.1 Обновление ПО сервера централизованного управления 33
3.9.2 Обновление ПО клиентов РАУ 34
4 Работа с сервером централизованного управления 36
4.1 Общие принципы управления 36
4.2 Вкладка «Пользователи системы» 36
4.2.1 Общие сведения 36
4.2.2 Добавление новых пользователей в систему 37
4.2.3 Импортирование пользователей в систему 38
4.2.4 Изменение параметров пользователя системы 42
4.2.5 Удаление пользователя 43
4.2.6 Поиск пользователя по идентификатору 44
4.2.7 Вывод на печать информации о пользователях 44
4.3 Вкладка «USB-устройства» 45
4.3.1 Общие сведения 45
4.3.2 Добавление USB-устройства 46
4.3.3 Импортирование информации о USB-устройствах от ПКО 47
4.3.4 Изменение информации о USB-устройствах 52
4.3.5 Удаление USB-устройств 52
4.4 Вкладка «Роли» 53
4.5 Вкладка «Идентификаторы» 55
4.6 Вкладка «Компьютеры» 59
4.7 Вкладка «Технологические участки» 64
4.8 Вкладка «Учётные записи» 65
4.9 Настройки сервера централизованного управления 69
4.9.1 Общие сведения 69

4.9.2 Основные настройки 70

5 Рекомендации по резервному копированию ПО сервера централизованного управления 72

6 Перечень оповещающих сообщений 74

7 Файлы конфигурации РАУ 79

7.1 Файл конфигурации ASM.INI 79

7.2 Файл конфигурации AcCon32.ini 80

7.3 Файл конфигурации AcWs32.ini 81

7.4 Файл конфигурации rabbitmq.config 83

8 Перечень принятых сокращений 85

1 Введение

1.1 Область применения

Деятельность Администратора РАУ.

1.2 Функции Администратора РАУ

Администратор РАУ:

- устанавливает компоненты РАУ, в том числе на подконтрольные объекты (при необходимости с привлечением администраторов ОС подконтрольных объектов (далее – ПКО));
- обеспечивает взаимодействие и функционирование технических и программных средств «Аккорд-РАУ»;
- формирует список пользователей «Аккорд-РАУ»;
- регистрирует рабочие станции и серверы в качестве участников информационного обмена в базе сервера централизованного управления (формирует базу подконтрольных объектов);
- формирует базу USB-устройств;
- поддерживает функционирование «Аккорд-РАУ».

1.3 Комплект поставки

В комплект поставки РАУ входят следующие компоненты:

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

2 Назначение и условия применения

2.1 Назначение

«Аккорд-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

2.2.1 Общие сведения

«Аккорд-РАУ» включает сервер централизованного управления (СЦУ) и подконтрольные объекты (клиенты РАУ).

Система базируется на сервис-ориентированной архитектуре. Большая часть логики вынесена в несколько различных типов сервисов, взаимодействующих друг с другом в процессе работы. В сервис вынесена в том числе логика поддержки очередей сообщений и обработки сообщений от различных элементов системы, т.е. фактически весь транспорт. В такой архитектуре при увеличении числа взаимодействующих сервисов растет нагрузка на транспортную службу. Поэтому в качестве транспорта в системе используется сервис RabbitMQ - программный брокер сообщений на основе стандарта AMQP. Он изначально предназначен для поддержки высоких нагрузок. Масштабируемость системы выполняется за счёт масштабируемости RabbitMQ - при росте нагрузки можно добавлять дополнительные службы RabbitMQ, запущенные на отдельных серверах, объединяя их в кластер, что позволяет адаптироваться к росту нагрузки (некластеризованный RabbitMQ поддерживает нагрузку порядка десятков тысяч сообщений в секунду).

Управление высоконагруженной частью системы (транспортом) несложное. Для нетранспортных сервисов достаточно указать в специальном конфигурационном файле список адресов нод кластера rmq. Настройка самого кластера произ-

водится стандартно выполнением нескольких команд на каждой ноде. Синхронизация очередей сообщений в кластере производится автоматически. Система устроена так, что при отказе отдельной ноды кластера балансировка и переход нетранспортных сервисов на работающие ноды производится в автоматическом режиме и не требует прямого вмешательства администратора.

2.2.2 Условия применения сервера централизованного управления

Для функционирования сервера централизованного управления необходим компьютер со следующими характеристиками:

- процессор – x64, 2 ядра или больше;
- ОЗУ – 4Гб или больше;
- жёсткий диск – 80Гб или больше;
- Ethernet 100Мбит.

Данный компьютер должен иметь статический IP-адрес.

На компьютере должен быть установлен комплекс СЗИ от НСД «Аккорд-АМДЗ», отвечающий требованиям, приведённым в таблице 1.

Таблица 1 - Требования к комплексу СЗИ от НСД «Аккорд-АМДЗ»

Тип контроллера	Версия ПО контроллера	Версия драйвера
Аккорд-5MX	02.01.014 и новее	3.54.0.0 и новее
Аккорд-5.5	02.01.014 и новее	3.54.0.0 и новее
Аккорд-5.5.e	02.01.014 и новее	3.54.0.0 и новее
Аккорд-GX	0.3.9.14 и новее	4.3.0 и новее
Аккорд-GXM	0.3.9.14 и новее	4.3.0 и новее
Аккорд-GXMH	0.3.9.14 и новее	4.3.0 и новее
Аккорд-M.2	0.3.9.14 и новее	4.3.0 и новее
Аккорд-LE	0.3.9.14 и новее	4.3.0 и новее

На компьютере должно быть установлено следующее программное обеспечение:

- операционная система – Windows Server 2008 R2 или новее;
- Microsoft.NET Framework версии 4.5 или новее;

Примечание. Для установки Microsoft .NET Framework необходимо предварительно установить на компьютер Windows Installer 3.1 или новее и Internet Explorer 5.01 или новее.

- серверная часть RabbitMQ;
- СПО СЗИ НСД «Аккорд-Win64 К».

Для корректной совместной работы СПО «Аккорд-Win64 К» и антивирусного ПО, установленного на сервере централизованного управления, в доверенную зону антивирусного ПО должны включаться каталог Accord.x64 и следующие системные файлы:

- \WINDOWS\SYSTEM32\ACCORD.SCR;
- \WINDOWS\SYSTEM32\ACGINA.DLL;
- \WINDOWS\SYSTEM32\ACNP.DLL;
- \WINDOWS\SYSTEM32\ACRUNNT.EXE;
- \WINDOWS\SYSTEM32\ACRUNVDD.DLL;
- \WINDOWS\SYSTEM32\ACRUNYDD.EXE;
- \WINDOWS\SYSTEM32\ACUSRMOD.DLL;
- \WINDOWS\SYSTEM32\AZIAHLP.DLL;
- \WINDOWS\SYSTEM32\DRIVERS\ACBOOT.SYS;
- \WINDOWS\SYSTEM32\DRIVERS\ACLOCK2K.SYS;
- \WINDOWS\SYSTEM32\DRIVERS\ACRUN.SYS;
- \WINDOWS\SYSTEM32\DRIVERS\ACXALLOW.SYS;
- \WINDOWS\SYSTEM32\DRIVERS\ACXLMSRV.SYS;
- \WINDOWS\SYSTEM32\TMATTACH.DLL;
- \WINDOWS\SYSTEM32\TMDRV32.DLL;
- \WINDOWS\SYSTEM32\ACNP.DLL;
- \WINDOWS\SYSTEM32\ACUSRM64.DLL;
- \WINDOWS\SYSTEM32\AZIAH64.DLL;
- \WINDOWS\SYSTEM32\TMATT64.DLL;
- \WINDOWS\SYSTEM32\TMDRV64.DLL.

Для запуска ПО сервера централизованного управления необходимы права локального администратора операционной системы.

2.2.3 Условия применения клиентов РАУ

Функционирование клиентов РАУ возможно на компьютерах со следующими характеристиками:

- 32-разрядный (x86) или 64-разрядный (x64) процессор с тактовой частотой 1 ГГц или выше;
- 1 ГБ (для 32-разрядного процессора) или 2 ГБ (для 64-разрядного процессора) ОЗУ;
- свободное место на жёстком диске – 2Гб.

На компьютерах может быть установлен комплекс СЗИ от НСД «Аккорд-АМДЗ», отвечающий требованиям, приведённым в таблице 1.

На клиентах РАУ должно быть установлено следующее программное обеспечение:

a) для компьютеров под управлением ОС Windows:

- операционная система – Windows 7 или новее;
- Microsoft.NET Framework версии 4.5 или новее;

Примечание. Для установки Microsoft .NET Framework необходимо предварительно установить на компьютер Windows Installer 3.1 или новее и Internet Explorer 5.01 или новее.

- библиотека клиентской части RabbitMQ;

Примечание. Установка библиотеки клиентской части RabbitMQ осуществляется в ходе инсталляции клиентского ПО (смотри подраздел 3.4).

- СПО СЗИ НСД «Аккорд-Win64 К»;

b) для компьютеров под управлением ОС Linux:

- операционные системы – Debian 7.8 (7.11), CentOS 7.0, Red Hat Enterprise Linux Server 7.0, Fedora 20 (24), OpenSUSE 12.3 (OpenSUSE leap 42);
- Microsoft .NET версии 5 или новее;
- библиотека клиентской части RabbitMQ.
- СПО СЗИ НСД «Аккорд-X К»

Примечание. Установка библиотеки клиентской части RabbitMQ осуществляется в ходе инсталляции клиентского ПО (смотри подраздел 3.4).

Для корректной совместной работы СПО СЗИ НСД «Аккорд-Win64 К» и антивирусного ПО, установленного на ПКО с 32-битными ОС, в доверенную зону антивирусного ПО должны включаться каталог Accord.NT и следующие системные файлы:

- \WINDOWS\SYSTEM32\ACCORD.SCR;
- \WINDOWS\SYSTEM32\ACGINA.DLL;
- \WINDOWS\SYSTEM32\ACNP.DLL;
- \WINDOWS\SYSTEM32\ACRUNNT.EXE;
- \WINDOWS\SYSTEM32\ACRUNVDD.DLL;
- \WINDOWS\SYSTEM32\ACRUNYDD.EXE;
- \WINDOWS\SYSTEM32\ACUSRMOD.DLL;
- \WINDOWS\SYSTEM32\AZIAHLP.DLL;
- \WINDOWS\SYSTEM32\DRIVERS\ACBOOT.SYS;
- \WINDOWS\SYSTEM32\DRIVERS\ACLOCK2K.SYS;
- \WINDOWS\SYSTEM32\DRIVERS\ACRUN.SYS;
- \WINDOWS\SYSTEM32\DRIVERS\ACXALLOW.SYS;
- \WINDOWS\SYSTEM32\DRIVERS\ACXLMSRV.SYS;
- \WINDOWS\SYSTEM32\TMATTACH.DLL;
- \WINDOWS\SYSTEM32\TMDRV32.DLL;
- \WINDOWS\SYSTEM32\AUTOEXEC.NT.

Для корректной совместной работы СПО СЗИ от НСД «Аккорд-Win64 К» и антивирусного ПО, установленного на ПКО с 64-битными ОС, в доверенную зону антивирусного ПО должны включаться каталог Accord.x64 и следующие системные файлы:

- \WINDOWS\SYSTEM32\ACCORD.SCR;
- \WINDOWS\SYSTEM32\ACGINA.DLL;
- \WINDOWS\SYSTEM32\ACNP.DLL;
- \WINDOWS\SYSTEM32\ACRUNNT.EXE;

- \WINDOWS\SYSTEM32\ACRUNVDD.DLL;
- \WINDOWS\SYSTEM32\ACRUNYDD.EXE;
- \WINDOWS\SYSTEM32\ACUSRMOD.DLL;
- \WINDOWS\SYSTEM32\AZIAHLP.DLL;
- \WINDOWS\SYSTEM32\DRIVERS\ACBOOT.SYS;
- \WINDOWS\SYSTEM32\DRIVERS\ACLOCK2K.SYS;
- \WINDOWS\SYSTEM32\DRIVERS\ACRUN.SYS;
- \WINDOWS\SYSTEM32\DRIVERS\ACXALLOW.SYS;
- \WINDOWS\SYSTEM32\DRIVERS\ACXLMSRV.SYS;
- \WINDOWS\SYSTEM32\TMATTACH.DLL;
- \WINDOWS\SYSTEM32\TMDRV32.DLL;
- \WINDOWS\SYSTEM32\ACNP.DLL;
- \WINDOWS\SYSTEM32\ACUSRM64.DLL;
- \WINDOWS\SYSTEM32\AZIAH64.DLL;
- \WINDOWS\SYSTEM32\TMATT64.DLL;
- \WINDOWS\SYSTEM32\TMDRV64.DLL.

В доверенную зону антивирусного ПО должен быть включен каталог ASM.

При использовании Антивируса Касперского для списка доверенных программ следует установить следующие исключения:

- «Не проверять открываемые файлы»;
- «Не контролировать активность программы»;
- «Не наследовать ограничения родительского процесса (программы)»;
- «Не контролировать активность дочерних программ»;
- «Не блокировать взаимодействие с интерфейсом программы»;
- «Не проверять сетевой трафик» (любые удаленные IP-адреса, любые порты).

3 Установка и настройка

3.1 Порядок развёртывания «Аккорд-РАУ»

Установка и настройка «Аккорд-РАУ» выполняется в следующей последовательности:

- установка комплекса «Аккорд-АМДЗ» на СЦУ. Установка комплекса на ПКО возможна опционально и не входит в обязанности Администратора;
- установка СПО СЗИ от НСД «Аккорд-Win64 К» на СЦУ. Установка СЗИ от НСД на подконтрольных объектах не входит в обязанности Администратора;
- установка ПО СЦУ. Установка описана в подразделе 3.2;
- получение файла лицензии на использование РАУ. Процедура получения файла лицензии на использование РАУ описана в подразделе 3.3;
- установка ПО клиентов РАУ на ПКО. Данная процедура должна выполняться для каждого ПКО. Установка клиентов РАУ описана в подразделе 3.4;
- настройка правил разграничения доступа для клиентов РАУ. Данная процедура описана в подразделе 3.5;
- создание сетевого идентификатора сервера РАУ. Процедура описана в подразделе 3.6;
- создание в сетевом идентификаторе учетной записи «ASM_ACCOUNT». Процедура описана в подразделе 3.7;
- регистрация подконтрольных объектов. Процедура описана в подразделе 3.8.

3.2 Установка ПО сервера централизованного управления

Установка ПО сервера централизованного управления осуществляется следующим образом:

- установить на СЦУ Microsoft .NET Framework 4.0 или выше (если он не установлен);

- выполнить на СЦУ находящийся на дистрибутивном носителе командный файл RMQ-prepare.bat, который создаёт в каталоге[1] %APPDATA% СЦУ папку RabbitMQ и копирует в неё конфигурационный файл rabbitmq.config;

- выполнить находящееся на дистрибутивном носителе приложение otp_win64_18.3.exe, осуществляющее установку erlang;

- выполнить находящееся на дистрибутивном носителе приложение rabbitmq-server-3.6.2.exe, осуществляющее установку сервера RabbitMQ;

- запустить на СЦУ с установочного диска РАУ программу RAU-SERVER-A.B.C.D.exe[2)], где A, B, C и D – десятичные числа, например, RAU-SERVER-3.0.0.230.exe. Данное приложение представляет собой мастер установки Комплекса СПО СЗИ «Аккорд-РАУ» (рисунок 1).

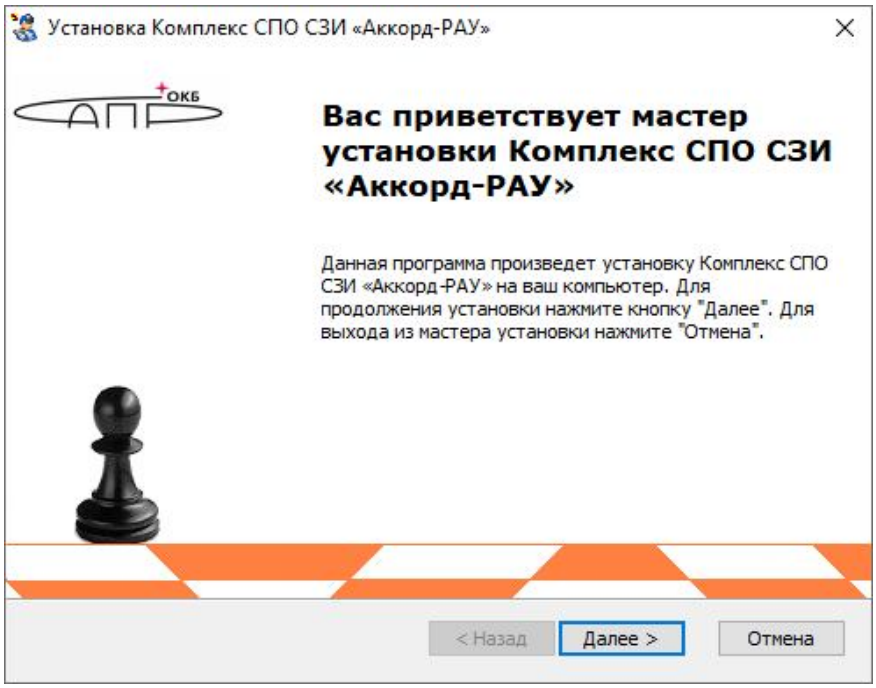

Рисунок 1 – Начало работы мастера установки Комплекса СПО СЗИ «Аккорд-РАУ»

При нажатии кнопки <Далее> появляется окно лицензионного соглашения. Приняв условия этого соглашения, в появившемся далее окне следует выбрать

[1] Указан каталог по умолчанию. При необходимости его изменения выполнить инструкцию из п.7.4

[2)] Если на СЦУ не установлена программа Microsoft.NET Framework или установлена версия ниже 4.0, то при установке ПО RAU-SERVER-A.B.C.D.exe автоматически выполняется установка .NET Framework 4.0

каталог установки Комплекса и нажать кнопку <Установить> (рисунок 2). Происходит установка Комплекса, после чего мастер завершает свою работу (рисунок 3).

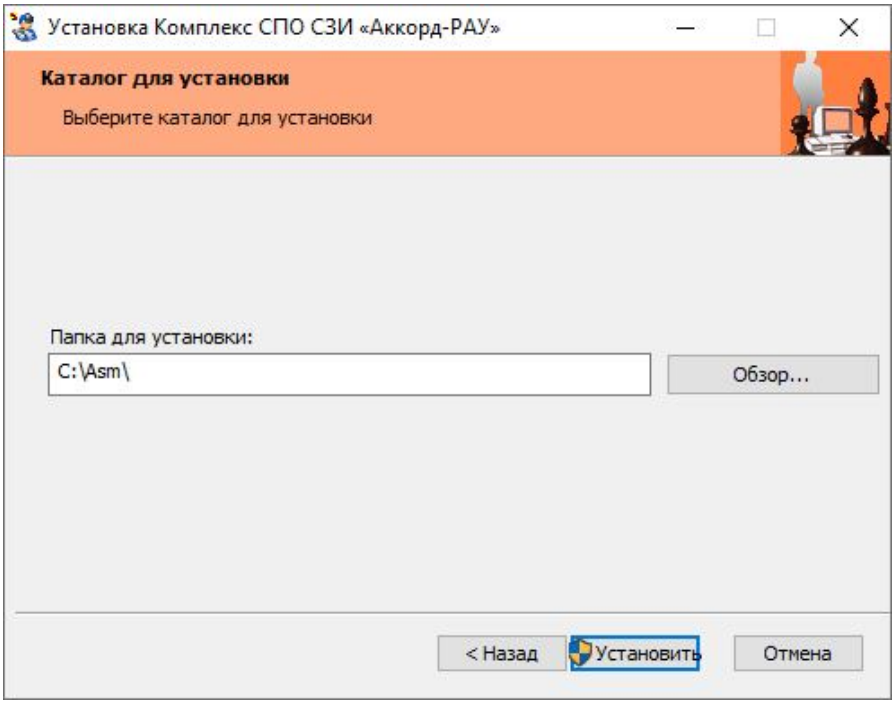

Рисунок 2 – Окно выбора каталога установки Комплекса СПО СЗИ «Аккорд-РАУ»

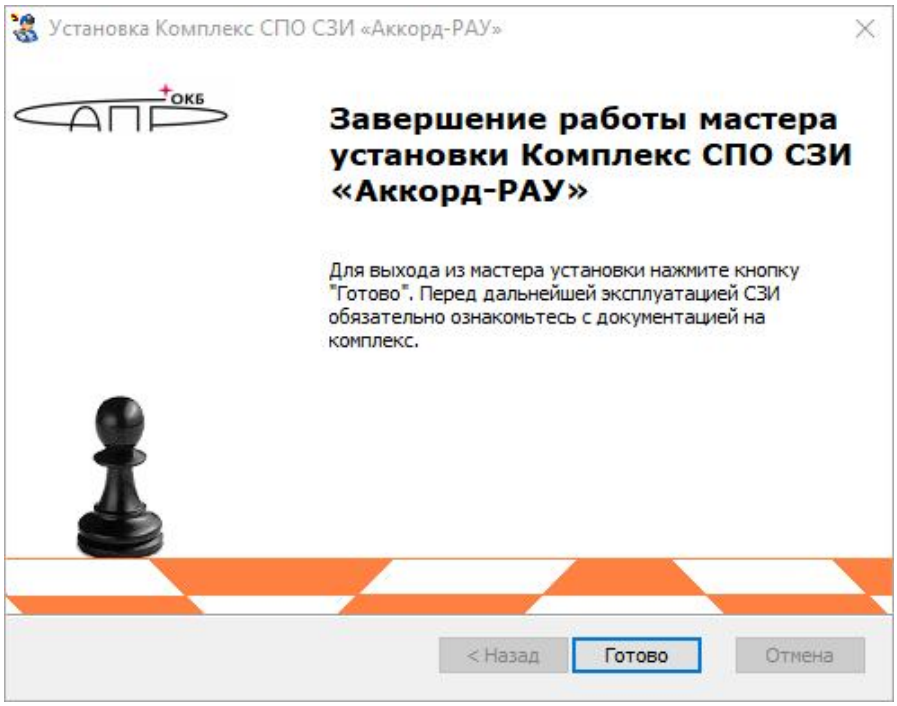

Рисунок 3 – Завершение работы мастера установки Комплекса СПО СЗИ «Аккорд-РАУ»

Обратите внимание, что при запуске мастера установки Комплекса на сервере с уже установленным ранее приложением мастер предложит выбрать для выполнения операцию изменения, восстановления или удаления Комплекса (рисунок 4).

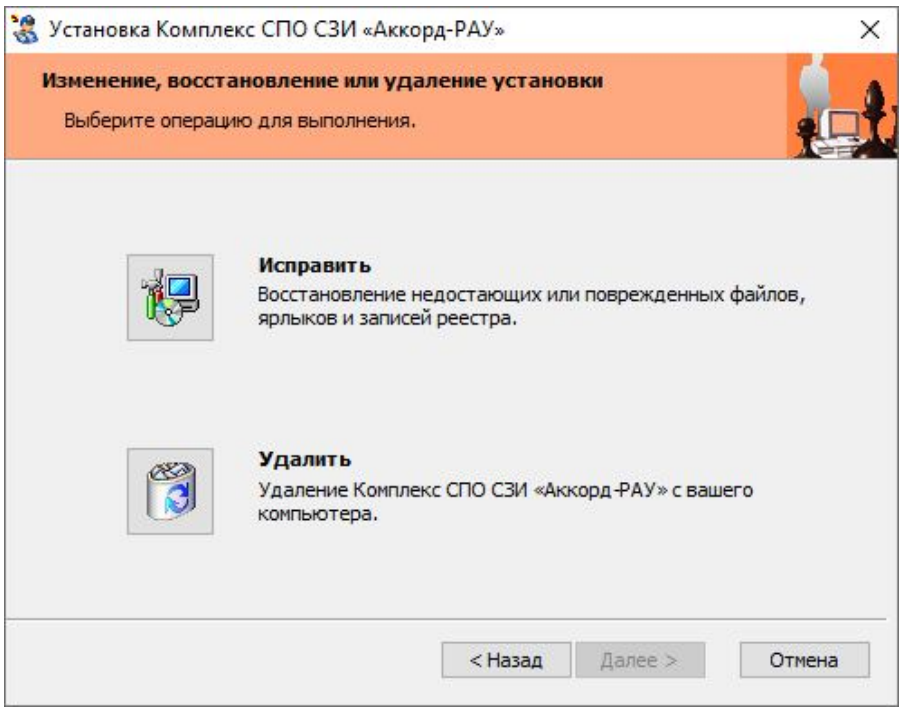

Рисунок 4 – Окно при запуске мастера установки Комплекса на сервере, где ранее уже был установлен Комплекс СПО СЗИ «Аккорд-РАУ»

При выборе операции удаления Комплекса появится окно подтверждения операции. После выполнения выбранного действия мастер установки завершит свою работу.

- открыть на СЦУ и на всех промежуточных сетевых устройствах между СЦУ и ПКО порт на входящие подключения сервера RabbitMQ. Номер данного порта прописан в параметре Port конфигурационного файла AcCon32.ini, расположенного на СЦУ и описанного в подразделе 7.2. Номер данного порта должен совпадать с номером порта, указанным в параметре tcp_listeners конфигурационного файла rabbitmq.config, описанного в подразделе 7.4. По умолчанию задаётся порт 28997;

- выполнить первичную настройку РАУ (регистрация администратора НШР, создание сетевого идентификатора, создание сетевой учетной записи);

- запустить сервис Acconnet.exe.

Если работа на СЦУ осуществляется пользователем операционной системы (ОС) Windows, который не имеет администраторских прав, то данному пользователю в ОС Windows необходимо предоставить полный доступ к папке, в которую была выполнена установка ПО СЦУ (по умолчанию C:\ASM), и ко всем вложенным в неё папкам.

При установке серверной части на сервер под управлением Windows 2012 R2 для пользователей, являющихся членами группы администраторов ОС, необходимо запускать AsmT.exe, используя правую кнопку мыши и пункт меню «Запуск от имени администратора». Это связано с особенностями работы ОС, в противном случае запуск выполняется с уровнем доступа «Пользователь ОС» и завершится ошибкой.

3.3 Получение файла лицензии на использование РАУ

Работа программы невозможна без файла лицензии.

Для получения файла лицензии после выполнения процедуры установки ПО СЦУ необходимо прислать письмо по адресу электронной почты key@okbsapr.ru, в котором указать следующие параметры:

- продукт: Аккорд-РАУ;
- серийный номер платы «Аккорд-АМДЗ» (установленной на сервере централизованного управления);
- количество ПКО.

В ответном письме будет отправлен сформированный файл лицензии. Данный файл нужно скопировать в папку, в которую было установлено ПО СЦУ (по умолчанию C:\Asm\ACCONNET) под именем «Acconnet.key» и продолжить настройку комплекса.

3.4 Установка ПО клиентов РАУ

Перед установкой ПО клиентов РАУ необходимо:

- для компьютеров под управлением ОС Windows провести установку Microsoft .NET Framework 4.0 или выше (если он не установлен);
- для компьютеров под управлением ОС Linux: провести установку Microsoft .NET 5 или выше (если он не установлен);
- открыть на данной рабочей станции и на всех промежуточных сетевых устройствах между данной рабочей станцией и СЦУ порт на входящие подключения сервера RabbitMQ. Номер данного порта прописан в параметре Port конфигурационного файла AcWs32.ini, который будет создан на рабочей станции после установки на неё ПО клиента РАУ. Номер данного порта должен совпадать с но-

мером порта, указанным в параметре tcp_listeners конфигурационного файла rabbitmq.config, описанного в подразделе 7.4. По умолчанию задаётся порт 28997.

Установка ПО клиентов РАУ осуществляется следующим образом.

а) Установка на компьютеры под управлением ОС Windows.

Запустить с установочного диска РАУ программу RAU-CLIENT-A.B.C.D.exe[1)], где A, B, C и D – десятичные числа, например, RAU-CLIENT-3.0.0.230.exe. При первом запуске программы появляется окно работы мастера установки Клиента СПО СЗИ «Аккорд-РАУ», приведённое на рисунке 5.

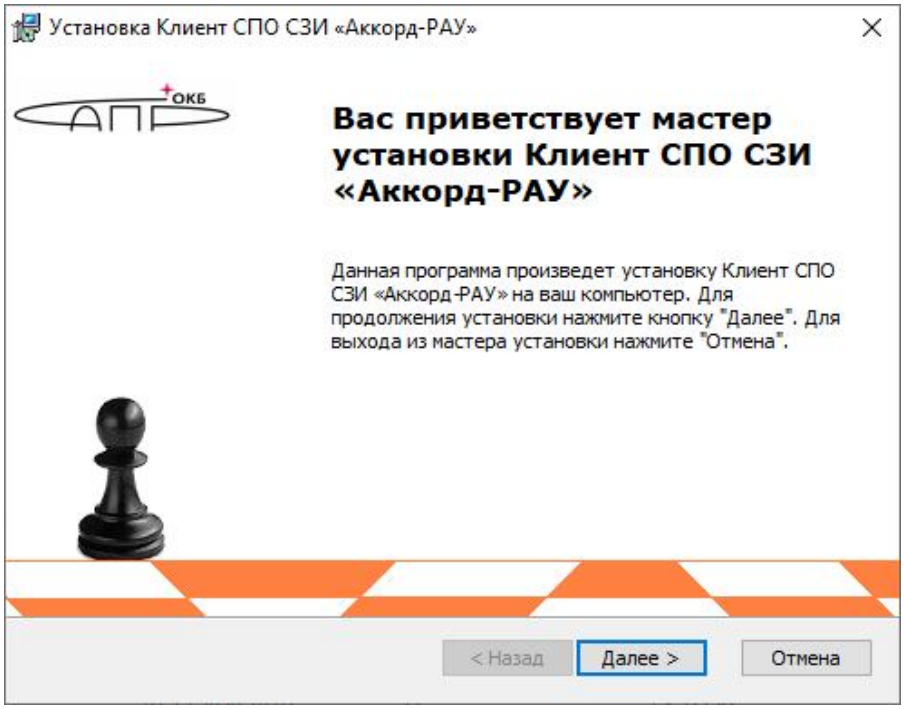

Рисунок 5 - Начало работы мастера установки Клиента СПО СЗИ «Аккорд-РАУ»

Приняв условия лицензионного соглашения и нажав <Далее>, в следующем окне выбрать каталог для установки ПО Клиента (рисунок 6). При выборе каталога обратите внимание на рекомендацию, показанную в этом окне.

[1)] Если на клиенте РАУ не установлена программа Microsoft.NET Framework или установлена версия ниже 4.0, то при установке ПО RAU-CLIENT-A.B.C.D.exe автоматически выполняется установка .NET Framework 4.0

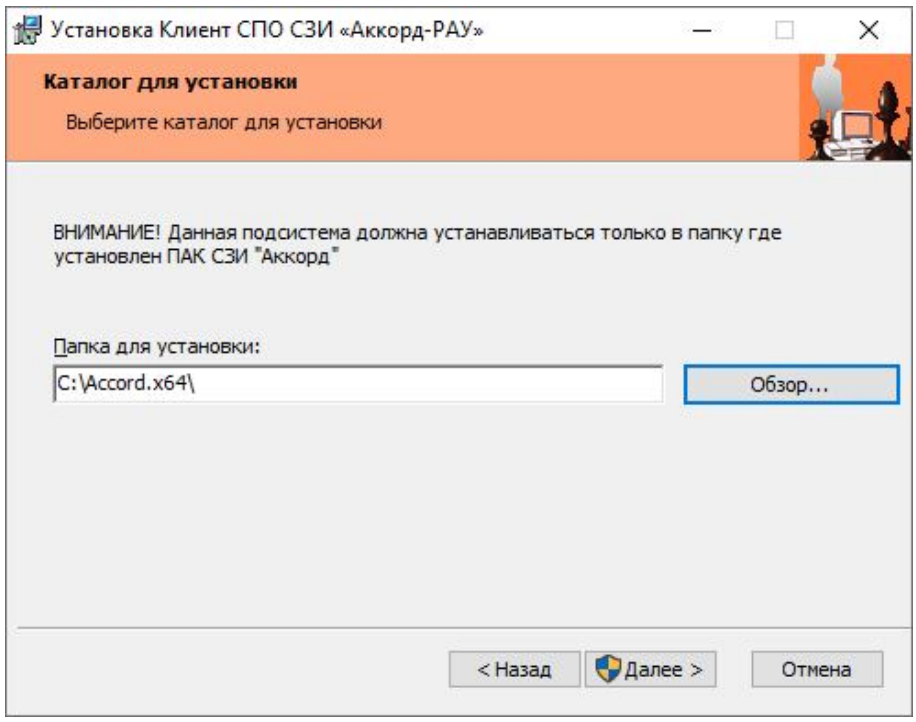

Рисунок 6 – Выбор каталога для установки Клиента СПО СЗИ «Аккорд-РАУ»

После нажатия кнопки <Далее> происходит установка Клиента СПО СЗИ «Аккорд-РАУ», и мастер завершает свою работу (рисунок 7).

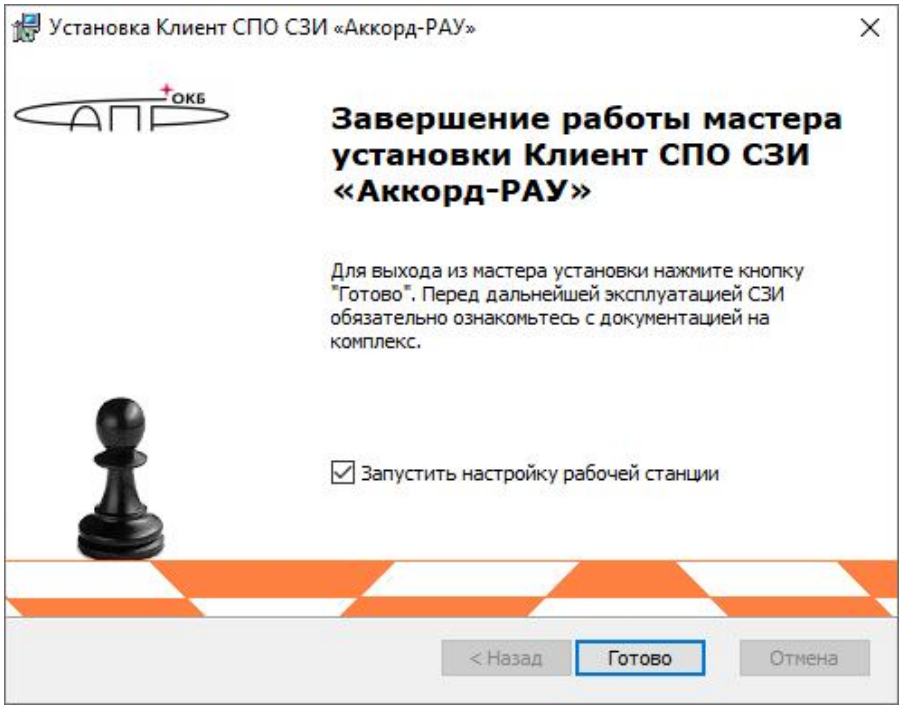

Рисунок 7 – Завершение работы мастера установки Клиента СПО СЗИ «Аккорд-РАУ»

Для настройки ПО Клиента следует установить флажок «Запустить настройку рабочей станции» и нажать кнопку <Готово>. Появится окно, приведённое на рисунке 8.

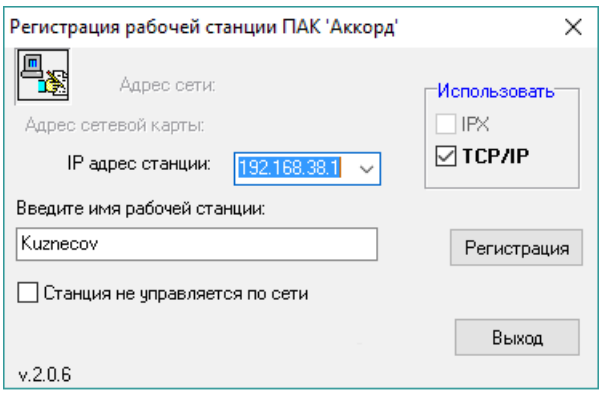

Рисунок 8 – Регистрация рабочей станции

В этом окне нужно установить необходимые параметры и нажать кнопку <Регистрация>.

Запустить редактор параметров доступа пользователей «ACED32.EXE». Установить флажок «Полный доступ для АРМ АБИ» в опциях настройки для всех пользователей (групп пользователей) СЗИ НСД на подконтрольном объекте. Порядок установки опций настройки описан в документе «Специальное программное обеспечение средств защиты информации от несанкционированного доступа «Аккорд-Win64 K». Установка правил разграничения доступа. Программа ACED32».

По выполнении процедуры регистрации рабочей станции (при нажатии кнопки <Выход> в окне 8) появляется сообщение о том, что для вступления в силу выполненных изменений необходимо перезагрузить компьютер. Следует выбрать кнопку <Да>, чтобы выполненные изменения вступили в силу.

Примечание. Если в окне завершения работы мастера установки ПО Клиента РАУ, приведённом на рисунке 7, не устанавливать флаг «Запустить настройку рабочей станции», то при нажатии кнопки <Готово> также появится оповещение о необходимости перезагрузки рабочей станции.

Обратите внимание, что при запуске мастера установки Клиента на компьютере с уже установленным ранее приложением мастер предложит выбрать для выполнения операцию изменения, восстановления или удаления Клиента (рисунок 9).

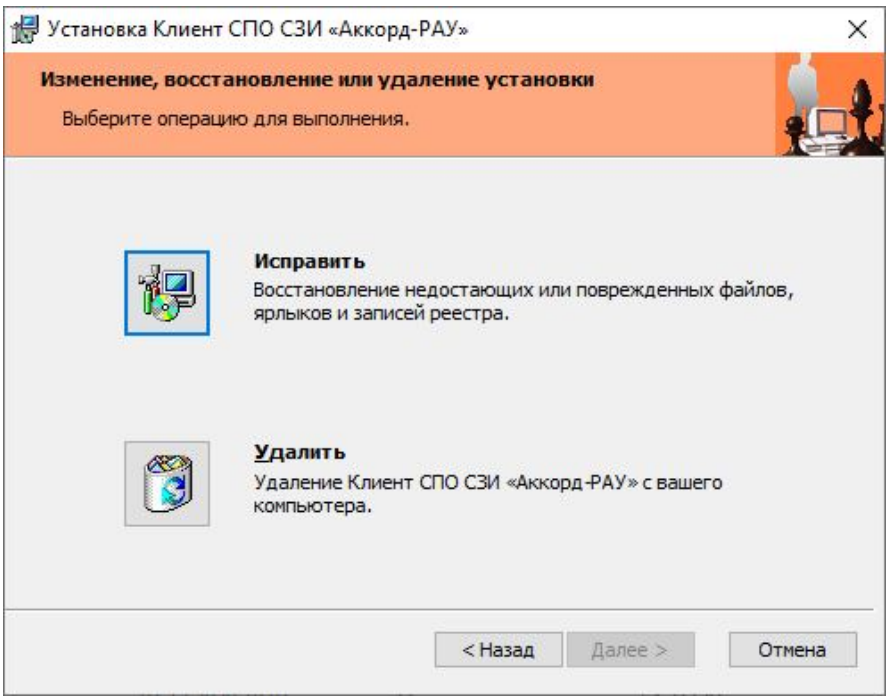

Рисунок 9 - Окно при запуске мастера установки Клиента на компьютере, где ранее уже был установлен Клиент СПО СЗИ «Аккорд-РАУ»

При выборе операции удаления Клиента появится окно для подтверждения данного действия. По выполнении выбранной операции мастер установки завершит свою работу.

б) Установка на компьютеры под управлением ОС Linux.

Для RPM-based дистрибутивов ОС Linux: выполнить установку пакета rau_client_A.B.C.D.rpm с установочного диска РАУ:

rpm -ivh rau_client_A.B.C.D.rpm, где A, B, C и D – десятичные числа, например, rau_client_3.1.0.989.rpm

При установке выполняется следующее:

- файлы клиента помещаются в /var/lib/RAUClient/
- конфигурация сервиса - в /etc/systemd/system
- сервис AcWs32L "активируется", но не запускается
- в конфигурационный файл AcWs32L.ini в параметр WsName прописывается значение hostname машины (имя ПКО), на которую установлен Клиент.

После установки необходимо добавить машину в домен безопасности, поместив ее в /var/lib/RAUClient/ ACNODE.LST с сервера РАУ, после чего запустить сервис "systemctl start AcWs32L" или перезагрузить машину. После перезагрузки сервис стартует автоматически.

Для Debian-based дистрибутивов ОС Linux: выполнить установку пакета rau-client.deb с установочного диска РАУ:

dpkg –i rau-client.deb

При установке выполняется следующее:

- файлы клиента помещаются в /var/lib/RAUClient/
- конфигурация сервиса - в /etc/init.d
- сервис RAUClient "активируется"
- в конфигурационный файл AcWs32L.ini в параметр WsName прописывается значение hostname машины (имя ПКО), на которую установлен Клиент.

После установки необходимо добавить машину в домен безопасности, то есть поместить в /var/lib/RAUClient/ ACNODE.LST с сервера РАУ, после чего запустить сервис "service RAUClient start" или перезагрузить машину.

После перезагрузки сервис стартует автоматически.

3.5 Настройка правил разграничения доступа для клиентов РАУ

На подконтрольном объекте импортировать в режиме объединения правила разграничения доступа из файла «acws32.prd», находящегося в каталоге установки СПО «Аккорд-Win64 К». Процедура импорта правил разграничения доступа описана в документе «Специальное программное обеспечение средств защиты информации от несанкционированного доступа «Аккорд-Win64 К». Установка правил разграничения доступа. Программа ACED32».

На ПКО запустить утилиту «MakePrc.EXE», входящую в состав ПАК СЗИ от НСД «Аккорд».

С помощью данной утилиты установить полный доступ с полным наследованием к объектам \DEVICE\ и \\ для следующих программ (процессов):

- AcWs32nt.exe;
- AcWs32.exe;
- CsrSS.exe;
- AcWsrst.exe;
- Services.exe.

Руководство по работе с программой «MakePrc.EXE» приведено в документе «Специальное программное обеспечение средств защиты информации от несанкционированного доступа «Аккорд-Win64 K». Установка правил разграничения доступа. Программа ACED32».

3.6 Создание сетевого идентификатора сервера централизованного управления

Сетевой идентификатор позволяет выполнить процедуру взаимной аутентификации СЦУ и ПКО. Решение об успешности / неуспешности аутентификации принимается по результатам проверки ЭЦП. Генерация ключевых пар для вычисления / проверки ЭЦП осуществляется специальной программой на основе последовательности случайных чисел, получаемой с аппаратного ДСЧ на плате контроллера «Аккорд-АМДЗ».

В качестве сетевого идентификатора может использоваться одно из следующих устройств:

- ТМ-идентификатор типа DS1996;
- USB-устройство ШИПКА;
- смарт-карта RuToken.

Для создания сетевого идентификатора необходимо запустить программу регистрации станций «ACSETCON.EXE» на СЦУ и нажать кнопку <Создать идентификатор>. На экран будет выведено окно, приведённое на рисунке 10.

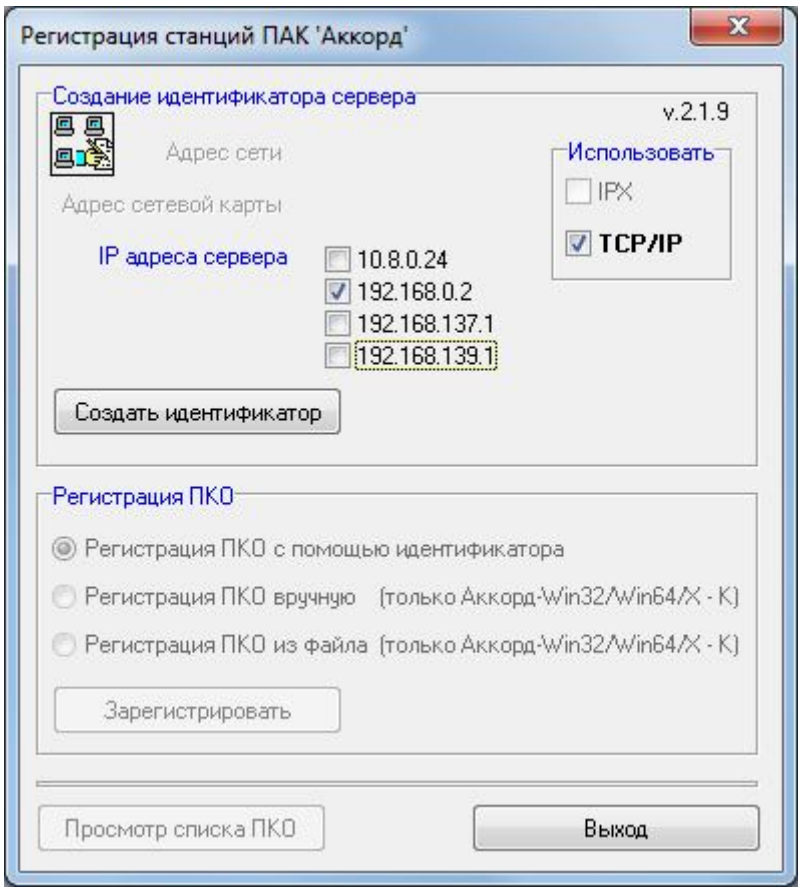

Рисунок 10 - Программа регистрации станций на сервере централизованного управления

На запрос ключа нужно присоединить сетевой идентификатор к съемнику информации. В идентификатор при этом заносится информация, которая будет использоваться при конфигурации ПКО. В каталоге, в который было установлено ПО СЦУ (по умолчанию C:\Asm\ACCONNET) создается файл ACNODE.LST, содержащий данные о СЦУ.

После завершения процедуры создания идентификатора СЦУ появляется сообщение, приведённое на рисунке 11, и становятся доступными элементы управления области «Регистрация ПКО».

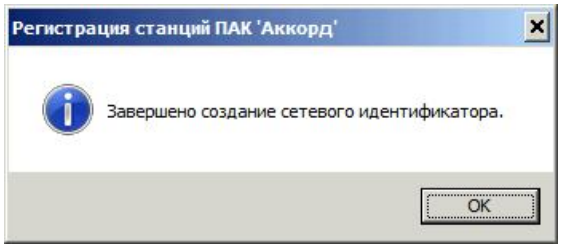

Рисунок 11 - Сообщение об успешном завершении процедуры создания сетевого идентификатора

В окне программы регистрации станций, приведённом на рисунке 10, нужно нажать кнопку <Выход>.

В результате выполнения процедуры создания сетевого идентификатора СЦУ на сетевой идентификатор будет записана информация, использующаяся при конфигурации ПКО.

3.7 Создание в сетевом идентификаторе учетной записи «ASM_ACCOUNT»

Если процедуру регистрации ПКО, описанную в пункте 3.8, планируется реализовывать способом «регистрация вручную» или «регистрация из файла», то выполнять данную процедуру не требуется.

Процедура создания в сетевом идентификаторе учетной записи «ASM_ACCOUNT», с помощью которой возможно выполнение процедур удаленного управления ПКО: добавление, удаление пользователей, смена пароля пользователя и т. д., выполняется Администратором РАУ согласно документу «СПО СЗИ НСД «Аккорд-РАУ». Руководство Администратора информационной безопасности».

3.8 Регистрация ПКО

3.8.1 Общие сведения

Регистрация ПКО возможна любым из трёх следующих способов:

- регистрация с помощью сетевого идентификатора (только для ПКО под управлением ОС Windows). При выполнении данного способа обмен аутентификационными данными между СЦУ и ПКО осуществляется путём передачи этих данных на сетевом идентификаторе СЦУ;

- регистрация вручную. При выполнении данного способа информация о ПКО вводится вручную, а обмен аутентификационными данными между СЦУ и ПКО осуществляется путём передачи этих данных по сети. ПКО под управлением ОС Linux регистрируются только этим способом;

- регистрация из файла. При выполнении данного способа информация о ПКО считывается из файла, а обмен аутентификационными данными между СЦУ и ПКО осуществляется путём передачи этих данных по сети.

Независимо от способа регистрации перед её выполнением необходимо создать сетевой идентификатор СЦУ (см. подраздел 3.6) и в нём создать учётную запись «ASM_ACCOUNT» (см. подраздел 3.7).

Существует возможность отменить регистрацию ПКО или изменить её параметры. Данная процедура описана в пункте 3.8.5.

3.8.2 Регистрация с помощью сетевого идентификатора

При регистрации ПКО с помощью сетевого идентификатора необходимо выполнить следующую последовательность действий.

а) доставить сетевой идентификатор на рабочую станцию, которую нужно зарегистрировать;

б) на данной рабочей станции запустить программу регистрации «ACSETWS.EXE», после чего на экран будет выведено окно, приведённое на рисунке 12;

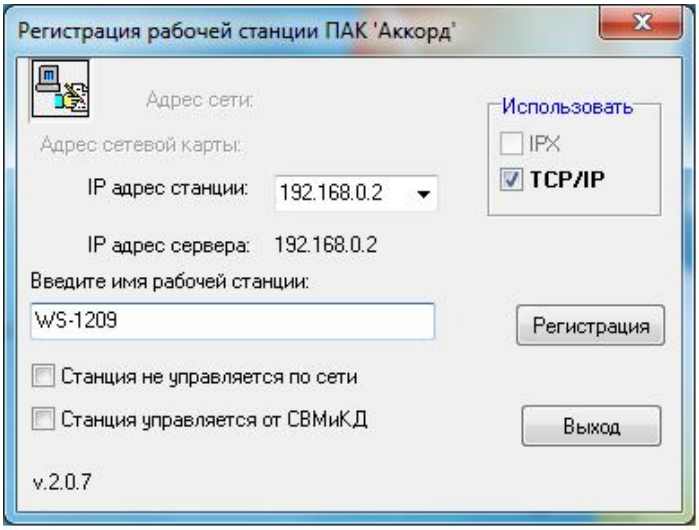

Рисунок 12 - Регистрация рабочей станции

в) в данном окне необходимо задать:

- имя станции. Под данным именем ПКО будет идентифицироваться на СЦУ. По умолчанию в качестве имени станции предлагается использовать имя компьютера;
- IP-адрес станции. Если компьютер получает адрес динамически при подключении к серверу, нужно выбрать параметр <Dynamic>.

После задания данных параметров необходимо нажать кнопку <Регистрация>.

г) на запрос ключа следует прислонить сетевой идентификатор к считывающему устройству;

д) на экран будет выведено сообщение, приведённое на рисунке 13.

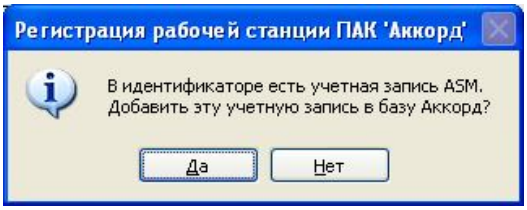

Рисунок 13 - Предложение добавить учетную запись ASM в базу «Аккорд»

Примечание. Если данное сообщение не будет выведено на экран, то это означает, что либо не был создан сетевой идентификатор СЦУ, либо в нём не была создана учётная запись «ASM_ACCOUNT» (смотри подразделы 3.6 и 3.7), и в этом случае необходимо прервать регистрацию ПКО, создать сетевой идентификатор и учётную запись «ASM_ACCOUNT», либо на шаге г) прислонили носитель, не являющийся сетевым идентификатором. В этом случае необходимо повторить регистрацию с правильным сетевым идентификатором.

В ответ на это сообщение необходимо нажать кнопку <Да>, ещё раз прислонить сетевой идентификатор к считывателю и ввести пароль Администратора ПАК СЗИ от НСД «Аккорд»;

После этого в сетевой идентификатор записывается информация о рабочей станции и открытый ключ станции. В каталоге, в который было установлено ПО клиента РАУ, создаётся файл «ACNODE.LST», содержащий данные о рабочей станции. На экран выводится сообщение об успешном добавлении учётной записи «ASM_ACCOUNT», приведённое на рисунке 14.

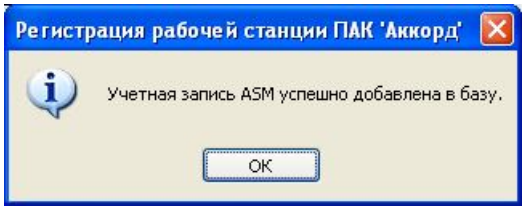

Рисунок 14 – Сообщение об успешном добавлении учетной записи «ASM_ACCOUNT» в базу ПАК СЗИ от НСД «Аккорд»

Следует нажать кнопку <Да> и предъявить сетевой идентификатор;

е) на экран выводится сообщение об успешном завершении процедуры регистрации рабочей станции, приведённое на рисунке 15.

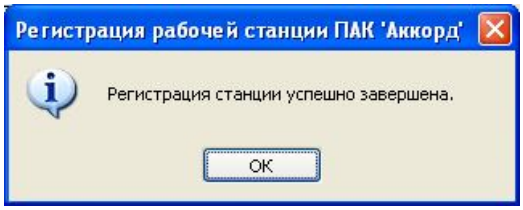

Рисунок 15 - Сообщение об успешном выполнении процедуры регистрации станции

Если в сетевом идентификаторе недостаточно свободной памяти для записи информации о ПКО и открытого ключа станции, то вместо сообщения об успешном завершении процедуры регистрации рабочей станции на экран выводится сообщение: «В идентификаторе нет свободных страниц для записи».

В этом случае нужно сохранить список зарегистрированных ПКО на СЦУ, после чего произойдёт очистка памяти сетевого идентификатора.

Примечание. Объем ТМ-идентификатора типа DS1996 обеспечивает хранение данных о 31 ПКО и их открытые ключи.

Операцию регистрации необходимо произвести на каждой рабочей станции;

ж) после сохранения в сетевом идентификаторе информации о рабочих станциях и открытых ключах станций нужно вернуться на СЦУ, в главном окне программы регистрации станций «ACSETCON.EXE», приведённом на рисунке 16, установить переключатель «Регистрация ПКО» в положение «Регистрация ПКО с помощью идентификатора» и нажать кнопку <Зарегистрировать>.

Примечание. Если элементы управления области «Регистрация ПКО» неактивны, как показано на рисунке 10, то это означает, что перед регистрацией ПКО не была проведена процедура создания сетевого идентификатора СЦУ. В этом случае необходимо создать сетевой идентификатор и учётную запись «ASM_ACCOUNT» (смотри подразделы 3.6 и 3.7) и ещё раз провести регистрацию ПКО.

На запрос идентификатора необходимо предъявить сетевой идентификатор. Информация о ПКО считывается из сетевого идентификатора, и память идентификатора очищается. После считывания из сетевого идентификатора информация о рабочих станциях и их открытые ключи фиксируется на СЦУ.

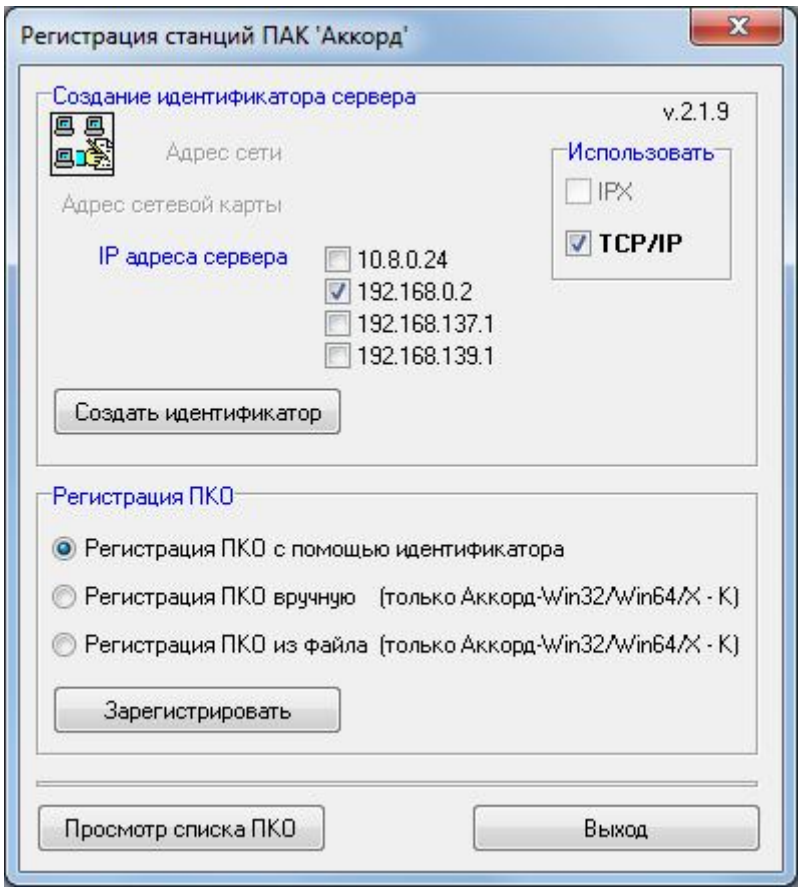

Рисунок 16 – Регистрация ПКО с помощью идентификатора

После завершения процедуры добавления информации о ПКО на СЦУ появляется сообщение, приведённое на рисунке 17.

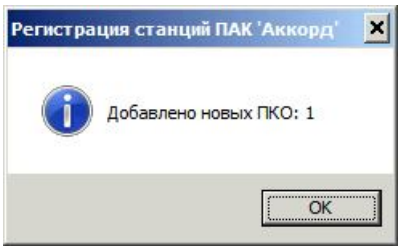

Рисунок 17 – Сообщение о добавлении информации на СЦУ

Для завершения процедуры регистрации необходимо перезагрузить ПКО и СЦУ.

Примечание. Регистрация ПКО, находящихся в отдельной подсети, разделённой с подсетью, в которой находится СЦУ РАУ, с помощью технологии Network Address Translation (NAT), должна осуществляться следующим образом.

1 На СЦУ переместить файл acnode.lst из C:\Asm\ACCONNET в любой другой каталог.

2 Используя ранее не используемый ТМ-идентификатор типа DS1996, создать новый сетевой идентификатор. Процедура создания сетевых идентификаторов описана в подразделах 3.6 и 3.7. При создании сетевого идентификатора в окне регистрации станций ПАК «Аккорд», приве-

дённом на рисунке 10, в качестве IP-адреса СЦУ указать IP-адрес устройства NAT для отдельной подсети.

3 На СЦУ вернуть перемещённый на шаге 1 файл acnode.lst в каталог C:\Asm\ACCONNET.

4 Зарегистрировать ПКО из отдельной подсети на созданный сетевой идентификатор. Процедура регистрации ПКО с помощью сетевого идентификатора описана в пункте 3.8.2.

5 На СЦУ зарегистрировать ПКО из нового сетевого идентификатора с помощью утилиты «ACSETCON.EXE». Данная процедура описана в пункте 3.8.2. При этом может потребоваться указание IP-адреса устройства NAT для отдельной подсети.

6 На СЦУ остановить службу Acconnet.

7 На СЦУ перезапустить RabbitMQ.

8 На СЦУ запустить службу Acconnet.

9 На зарегистрированных ПКО перезапустить службу acws32nt.

3.8.3 Регистрация вручную

При регистрации ПКО вручную необходимо на СЦУ запустить программу регистрации станций «ACSETCON.EXE». На экран будет выведено окно, приведённое на рисунке 16. В этом окне нужно установить переключатель «Регистрация ПКО» в положение «Регистрация ПКО вручную (только Аккорд- Win32/Win64/X K)» и нажать кнопку <Зарегистрировать>.

Примечание. Если элементы управления области «Регистрация ПКО» неактивны, как показано на рисунке 10, то это означает, что перед регистрацией ПКО не была проведена процедура создания сетевого идентификатора СЦУ. В этом случае необходимо создать сетевой идентификатор (смотри подраздел 3.6).

После этого будет выведено окно, приведённое на рисунке 18.

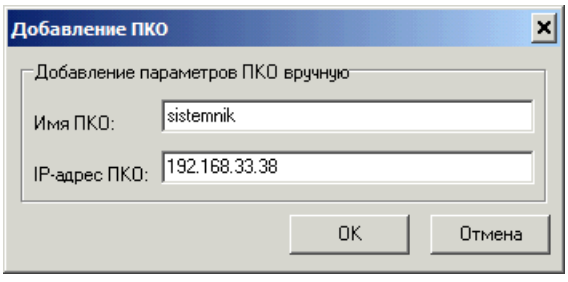

Рисунок 18 – Добавление ПКО вручную

В этом окне нужно ввести имя (hostname для ПКО под управлением ОС Linux) и IP-адрес ПКО и нажать кнопку <OK>. Информация о ПКО сохраняется на СЦУ в файле «AcNode.lst».

После добавления информации о ПКО на СЦУ появляется сообщение, приведённое на рисунке 17.

Если во время выполнения данной процедуры между ПКО и СЦУ отсутствовало сетевое соединение, то появляется сообщение, приведённое на рисунке 19, а в файле «AcNode.lst» IP-адресу данного ПКО присваивается значение 127.0.0.1.

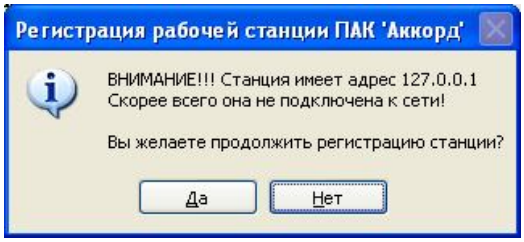

Рисунок 19 - Сообщение, возникающее при регистрации станций с IP-адресом 127.0.0.1

При появлении сообщения, приведённого на рисунке 19, необходимо нажать кнопку <Нет>, восстановить сетевое соединение между СЦУ и ПКО и повторить процедуру регистрации.

Если на ПКО запущена служба сетевого агента, то через шесть минут после установления сетевого соединения между данным ПКО и СЦУ ПКО автоматически подключаются к СЦУ. При этом в файл CompName.Ver (CompName – имя ПКО) записывается информация о ПКО, содержащая реальное значение IP-адреса ПКО.

Значения IP-адреса, содержащиеся в файлах CompName.Ver и AcNode.lst, для одного и того же ПКО могут не совпасть, что в дальнейшем не позволит полноценно управлять ПКО с СЦУ.

Такие ПКО следует удалить и заново провести процедуру регистрации, убедившись, что между ПКО и СЦУ установлено сетевое соединение.

3.8.4 Регистрация из файла

Для регистрации ПКО из файла необходимо заранее подготовить текстовый файл с произвольным именем, содержащий параметры всех регистрируемых ПКО. Каждая строка данного файла должна содержать имя ПКО и его IP-адрес, разделённые символом «;», например, WS_UBiZI_04;192.168.201.17.

При регистрации ПКО из файла необходимо на СЦУ запустить программу регистрации станций «ACSETCON.EXE». Появится окно, приведённое на рисунке 16. В этом окне нужно установить переключатель «Регистрация ПКО» в поло-

жение «Регистрация ПКО из файла (только Аккорд-Win32/Win64/X K)» и нажать кнопку <Зарегистрировать>.

Примечание. Если элементы управления области «Регистрация ПКО» неактивны, как показано на рисунке 10, то это означает, что перед регистрацией ПКО не была проведена процедура создания сетевого идентификатора СЦУ. В этом случае необходимо создать сетевой идентификатор (смотри подраздел 3.6).

После этого на экран будет выведено окно открытия файла, приведённое на рисунке 20.

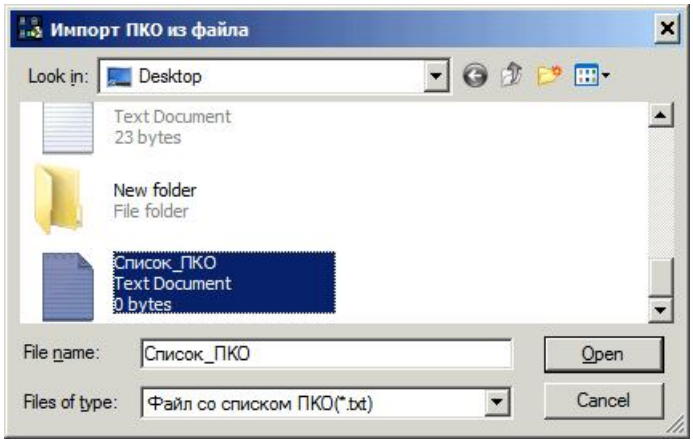

Рисунок 20 – Импорт параметров ПКО из файла

В данном окне нужно выбрать файл с параметрами регистрируемых ПКО и нажать кнопку <Открыть>, после чего будет выполнена процедура регистрации.

По завершении процедуры регистрации ПКО появляется сообщение, приведённое на рисунке 17.

3.8.5 Изменение списка зарегистрированных ПКО

На сервере централизованного управления запустить утилиту «AcSetCon.exe» «Пуск» → «Программы» → «ASM» → «Настройка сети». Появится окно регистрации ПКО, приведенное на рисунке 16.

В данном окне нажать кнопку <Просмотр списка ПКО>. Появится окно редактирования списка зарегистрированных ПКО, приведенное на рисунке 21.

Данное окно позволяет:

- просматривать список зарегистрированных ПКО;
- изменять сетевую карту, обеспечивающую взаимодействие выбранного ПКО с СЦУ;

- изменять протокол сетевого взаимодействия между выбранным ПКО и СЦУ;
- изменять параметры протокола сетевого взаимодействия;
- удалить компьютер из списка зарегистрированных ПКО.

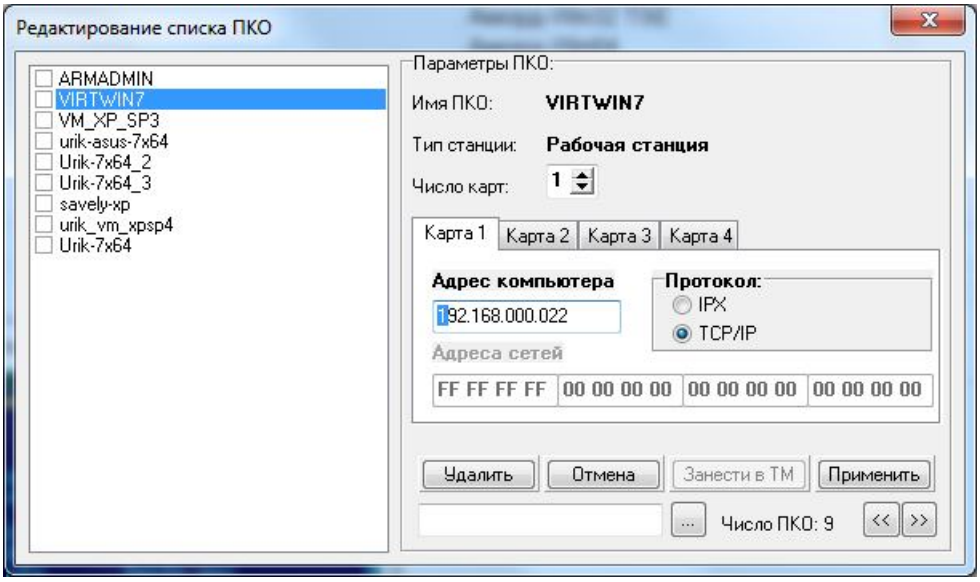

Рисунок 21 - Окно редактирования списка ПКО

3.9 Установка обновлений ПО РАУ

3.9.1 Обновление ПО сервера централизованного управления

Порядок обновления ПО РАУ (СЦУ и клиента РАУ) следующий:

1) запустить компьютер (убедиться, что он запущен);

2) завершить работу ПО РАУ (если оно запущено);

3) при использовании в режиме интеграции с СВМиКД остановить сервисы Acconnet и MttControlService;

4) удалить предыдущую версию ПО РАУ;

5) запустить обновленное ПО РАУ: программу RAU-SERVER-A.B.C.D.exe на СЦУ или RAU-CLIENT-A.B.C.D.exe/rau-cleint.deb/ rau_client_A.B.C.D.rpm - на ПКО (A, B, C и D – десятичные числа);

6) перезагрузить компьютер после завершения работы программы установки обновления.

3.9.2 Обновление ПО клиентов РАУ

Выполнять обновление ПО клиентов РАУ следует каждый раз после обновления ПО СЦУ.

Обновление установленного на подконтрольные объекты ПО клиентов РАУ под управлением ОС Windows осуществляется удалённо с СЦУ при помощи приложения «UpdateManager.exe». Данное приложение находится в папке, в которую установлено ПО СЦУ (по умолчанию C:\ASM).

После запуска данной утилиты выводится окно, приведённое на рисунке 22.

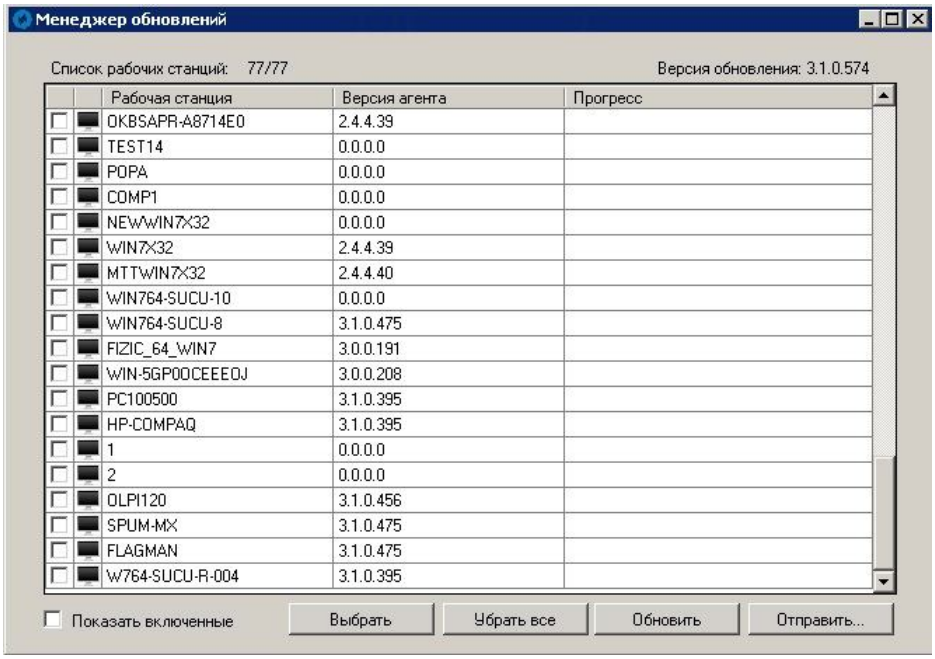

Рисунок 22 – Менеджер обновлений

Данное окно содержит список зарегистрированных на СЦУ ПКО с указанием в столбце «версия агента» версии клиентского ПО РАУ. Установка флажка «Показать включенные» приводит к исключению из данного списка выключенных ПКО и отображению только включенных в текущее время ПКО. Снятие флажка возвращает отображение всех зарегистрированных ПКО. Нажатие кнопки <Выбрать> обеспечивает выбор всех отображаемых ПКО. Нажатие кнопки <Убрать все> отменяет выбор всех отображаемых ПКО.

Для обновления ПО клиентов РАУ следует установить флажки напротив тех ПКО, на которых нужно выполнить обновление, и нажать кнопку <Обновить>. Рекомендуется выполнять обновление для всех зарегистрированных ПКО, если иное не предписывается специальными инструкциями, распоряжениями. Если обновляемый ПКО в момент нажатия кнопки <Обновить> выключен, то обновление кли-

ентского ПО РАУ на нём будет выполнено сразу после его включения и загрузки. После завершения обновления ПО клиентов РАУ на всех выбранных ПКО появится соответствующее сообщение (рисунок 23). В столбец «Прогресс» будет записана информация о результатах выполнения обновления ПО клиентов РАУ на ПКО.

Примечания:

1 Новые версии файлов обновления ПО клиентов РАУ копируются на СЦУ при выполнении процедуры обновления ПО СЦУ. Данные файлы находятся в папке C:\Asm\ACCONNET\Client.Upd\.

2 Помимо удалённого централизованного обновления ПО клиентов РАУ на ПКО приложение «UpdateManager.exe» обеспечивает передачу файлов на выбранные ПКО.

Для передачи файлов с помощью данного приложения нужно в окне, приведённом на рисунке 22, выбрать ПКО, на который нужно передать файлы, и нажать кнопку <Отправить>. В появившемся диалоговом окне Windows выбора файлов выбрать файлы, которые нужно передать. В появившемся окне ответить на запрос о необходимости перезагрузки ПО клиента РАУ на ПКО.

После передачи будет выведено сообщение о завершении отправки файлов, а в столбец «Прогресс» будет помещена информация о результатах отправки. Переданные файлы будут записаны в папку установки ПАК СЗИ от НСД «Аккорд» на ПКО.

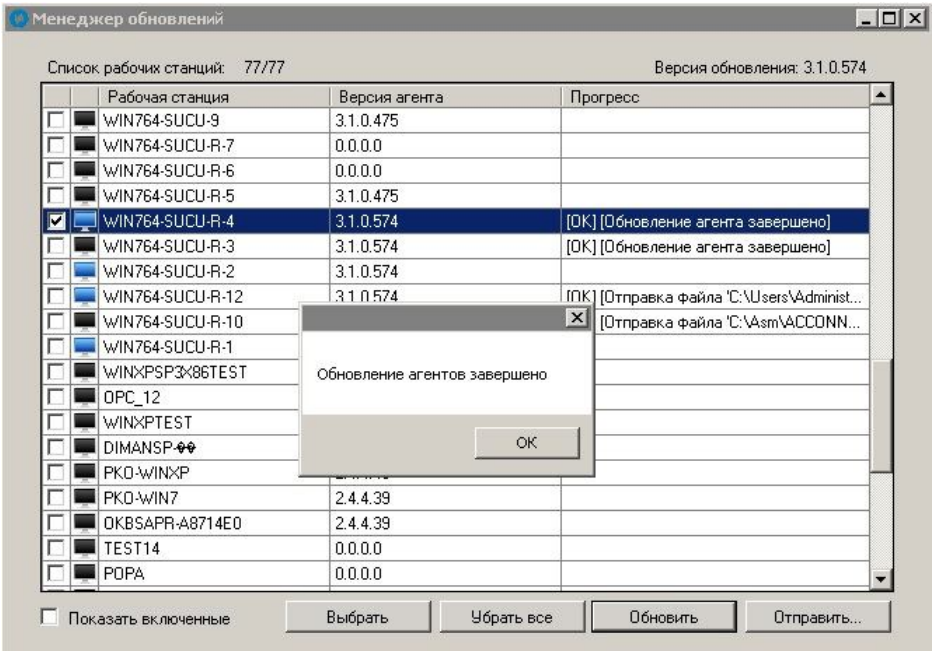

Рисунок 23 - Менеджер обновлений. Завершение обновления ПО клиентов РАУ

4 Работа с сервером централизованного управления

4.1 Общие принципы управления

Пользовательский интерфейс ПО СЦУ подчиняется следующим правилам:

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

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

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

В подразделах 4.2 - 4.9 описывается пользовательский интерфейс СЦУ, доступный администратору для выполнения его обязанностей.

4.2 Вкладка «Пользователи системы»

4.2.1 Общие сведения

Внешний вид вкладки «Пользователи системы» приведён на рисунке 24.

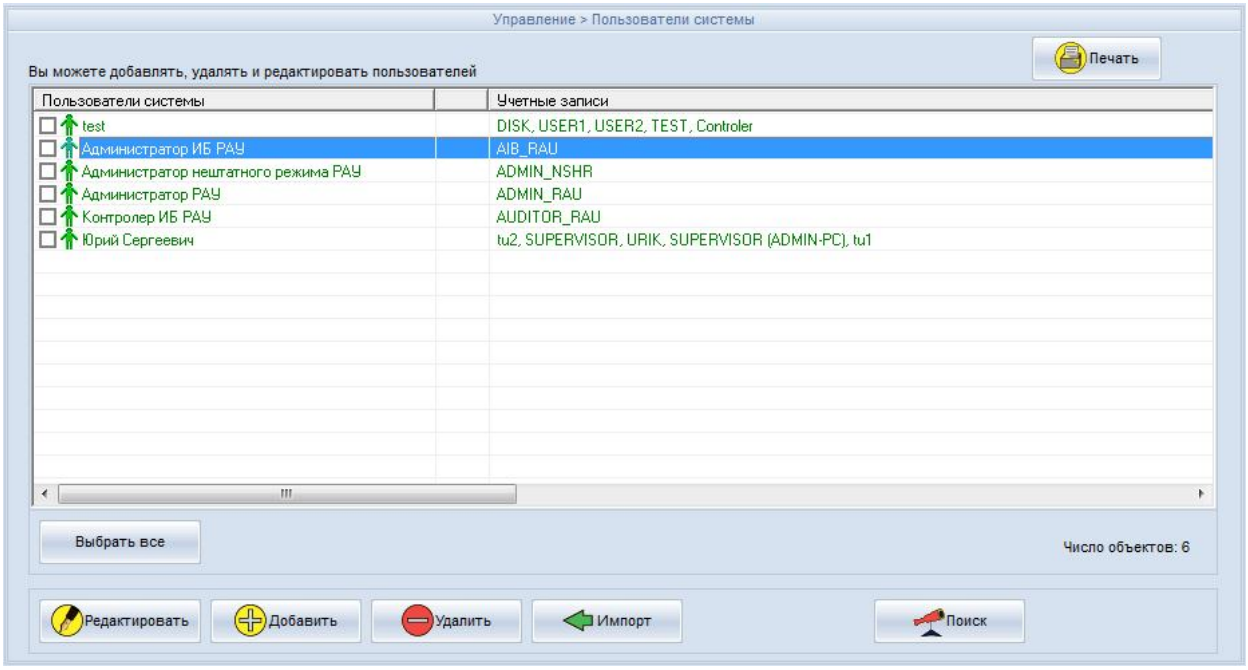

Рисунок 24 - Вкладка «Пользователи системы»

Используя элементы управления данной вкладки, Администратор РАУ может выполнять следующие функции:

- добавлять новых пользователей в систему. Данная функция описана в пункте 4.2.2;
- импортировать в систему пользователей из СПО СЗИ НСД «Аккорд-Win64 К» и пользователей из ОС Windows. Функция описана в пункте 4.2.3;
- изменять параметры пользователей системы. Функция описана в пункте 4.2.4;
- удалять пользователей системы. Функция описана в пункте 4.2.5;
- осуществлять поиск пользователя по идентификатору. Функция описана в пункте 4.2.6;
- выводить на печать выбранную информацию о пользователях. Функция описана в пункте 4.2.7.

4.2.2 Добавление новых пользователей в систему

Данная функция позволяет добавлять новых пользователей в систему.

Для добавления нового пользователя в систему следует в окне, приведённом на рисунке 24, нажать кнопку <Добавить>. На экран будет выведено окно, приведённое на рисунке 25.

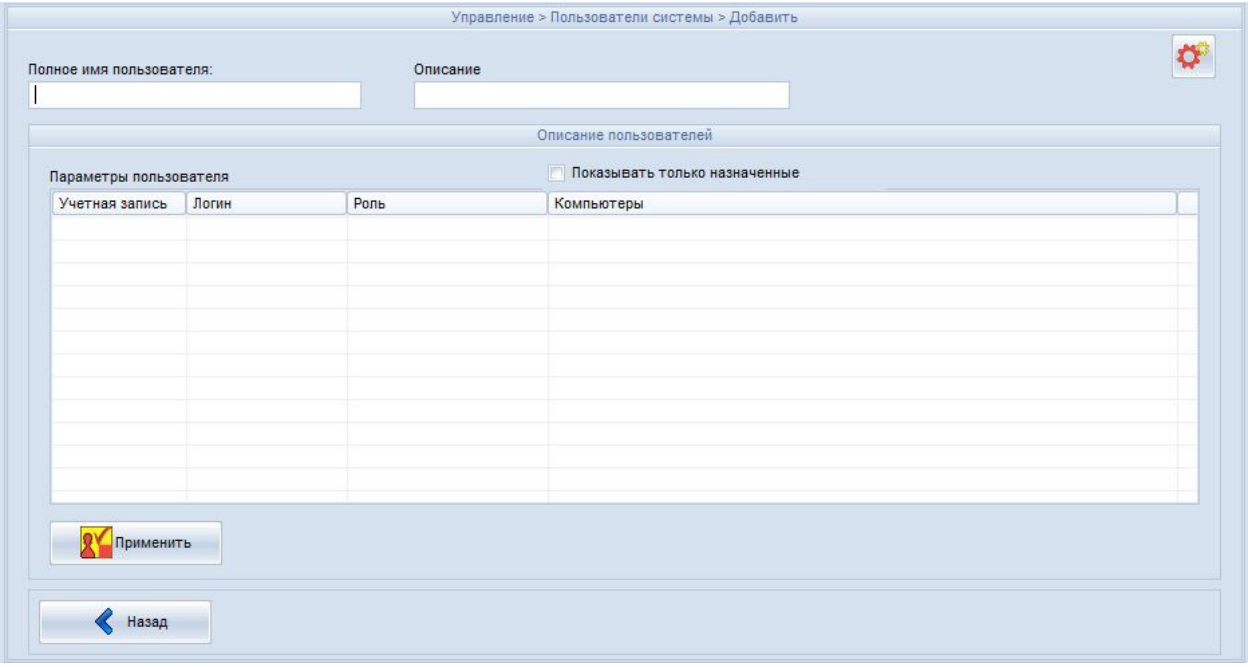

Рисунок 25 - Добавление нового пользователя

В данном окне следует ввести полное имя пользователя и его описание. После нажатия кнопки <Применить> пользователь с заданными параметрами будет добавлен в систему.

4.2.3 Импортирование пользователей в систему

4.2.3.1 Общие сведения об импортировании пользователей

ПО СЦУ позволяет импортировать в систему пользователей из СПО «Аккорд-Win64 К» и пользователей из ОС Windows. Импортирование в систему пользователей СПО «Аккорд-Win64 К» описано в подпункте 4.2.3.2. Импортирование в систему пользователей из ОС Windows описано в подпункте 4.2.3.3.

4.2.3.2 Импортирование пользователей из СПО СЗИ НСД «Аккорд-Win64 К»

Данная функция позволяет добавлять в систему пользователей, зарегистрированных в СПО «Аккорд-Win64 К», установленных на подконтрольных объектах. Подробная информация приведена в документе «Специальное программное обеспечение средств защиты информации от несанкционированного доступа «Аккорд-Win64 К». Установка правил разграничения доступа. Программа ACED32».

Необходимая для выполнения импортирования информация о пользователях передаётся подконтрольными объектами и хранится на СЦУ в так называе-

мых базах пользователей – файлах с расширением *.amz. Имена этих файлов совпадают с именами ПКО, от которых они были получены.

Для импортирования в систему пользователей следует в окне, приведённом на рисунке 24, нажать кнопку <Импорт>. В появившемся окне импорта пользователей, приведённом на рисунке 25, установить переключатель «Вы можете импортировать пользователей из:» в положение «базы Accord».

Далее в окне импорта пользователей (рисунок 25) нажать кнопку <Импортировать>. Появится стандартное диалоговое окно открытия файла, в котором Администратору РАУ следует выбрать файл с расширением *.amz (базу пользователей), содержащий информацию о пользователях, которых следует импортировать в систему. На СЦУ файлы с расширением *.amz хранятся в папке C:\Asm\ACCONNET\IN\, имена этих файлов совпадают с именами ПКО, от которых они были получены.

Рисунок 26 - Окно импорта пользователей. Импортирование пользователей СПО «Аккорд-Win64 К»

После выбора и открытия файла базы пользователей окно импорта пользователей примет вид, приведённый на рисунке 27.

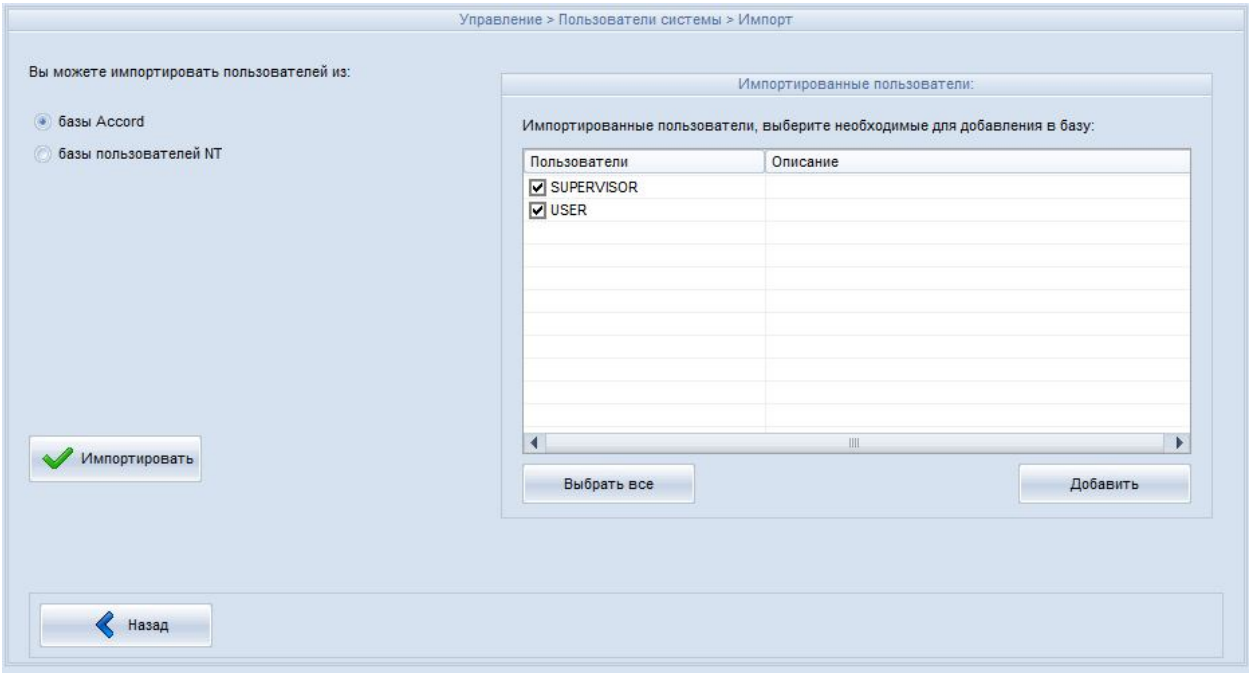

Рисунок 27 - Окно импорта пользователей. Импортирование пользователей из СПО «Аккорд-Win64 К». Выбор пользователей для импорта

В правой части окна импорта пользователей будет отображаться список пользователей, информация о которых содержится в выбранной базе пользователей. Администратору РАУ следует установить флажки напротив тех пользователей, которых нужно импортировать в систему, и нажать кнопку <Добавить>.

4.2.3.3 Импортирование пользователей ОС Windows

Данная функция позволяет добавлять в систему пользователей ОС Windows подконтрольных объектов.

Для импортирования в систему пользователей ОС Windows следует в окне, приведённом на рисунке 24, нажать кнопку <Импорт>. В появившемся окне импорта пользователей, приведённом на рисунке 28, установить переключатель «Вы можете импортировать пользователей из:» в положение «базы пользователей NT».

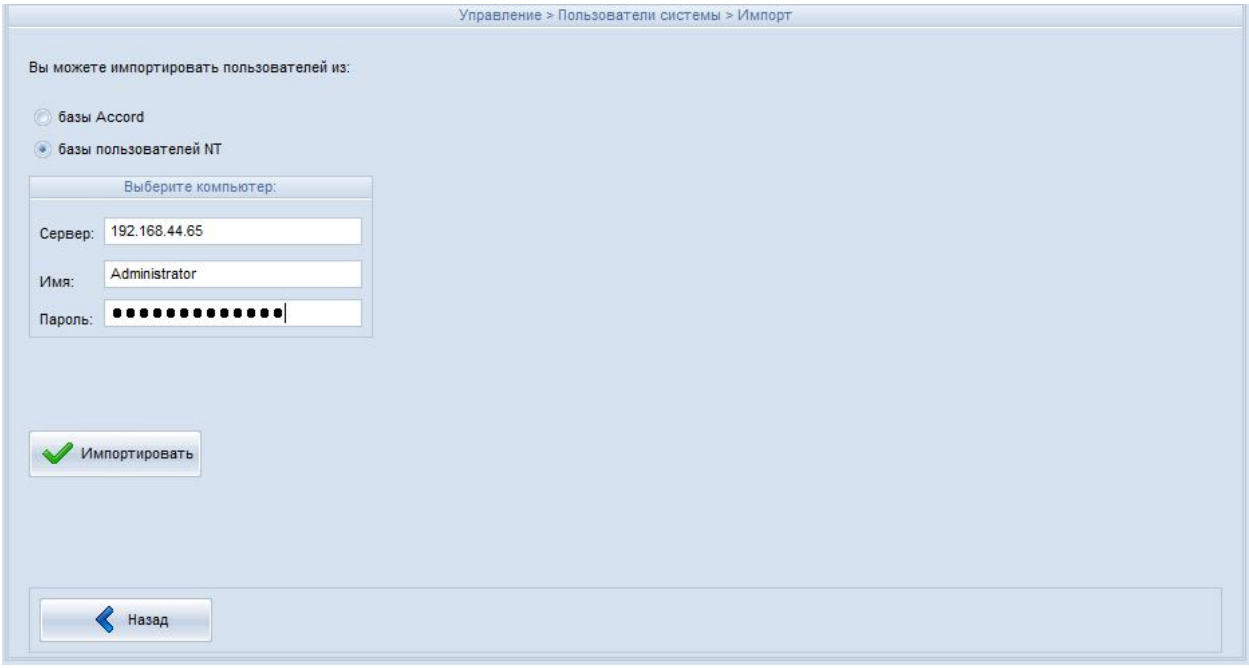

Рисунок 28 - Окно импорта пользователей. Импортирование пользователей ОС Windows

В окне импорта пользователей, приведённом на рисунке 28, в поле «Выберете компьютер:» нужно задать IP-адрес или имя ПКО, пользователей которого следует импортировать в систему, имя (логин) и пароль Администратора ОС данного ПКО. После этого окно импорта пользователей примет вид, приведённый на рисунке 29.

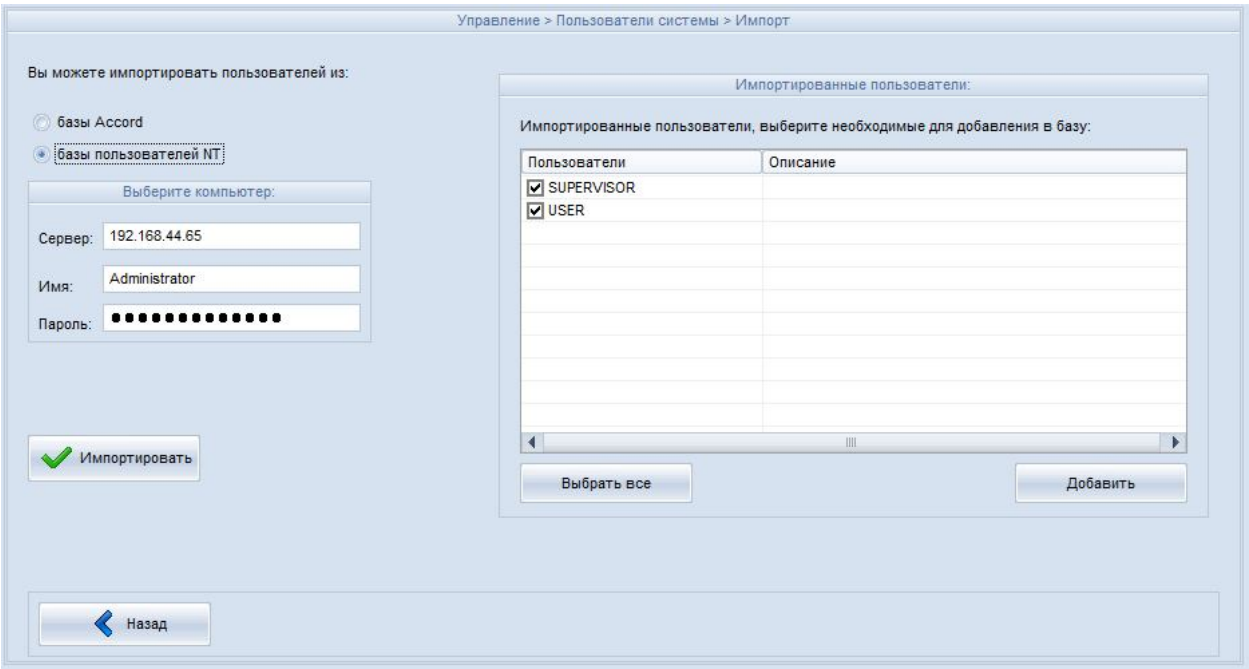

Рисунок 29 - Окно импорта пользователей. Импортирование пользователей ОС Windows. Выбор пользователей для импорта

В правой части окна импорта пользователей, приведённого на рисунке 29, будет отображаться список пользователей ОС выбранного ПКО. Администратору

РАУ следует установить флажки напротив тех пользователей, которых нужно импортировать в систему, и нажать кнопку <Добавить>.

4.2.4 Изменение параметров пользователя системы

Данная функция позволяет изменять имя и описание пользователей.

Для изменения параметров пользователя следует в окне, приведённом на рисунке 24, дважды щелкнуть по записи данного пользователя или, установив флажок напротив данного пользователя, нажать кнопку <Редактировать>. Появится окно, приведённое на рисунке 30.

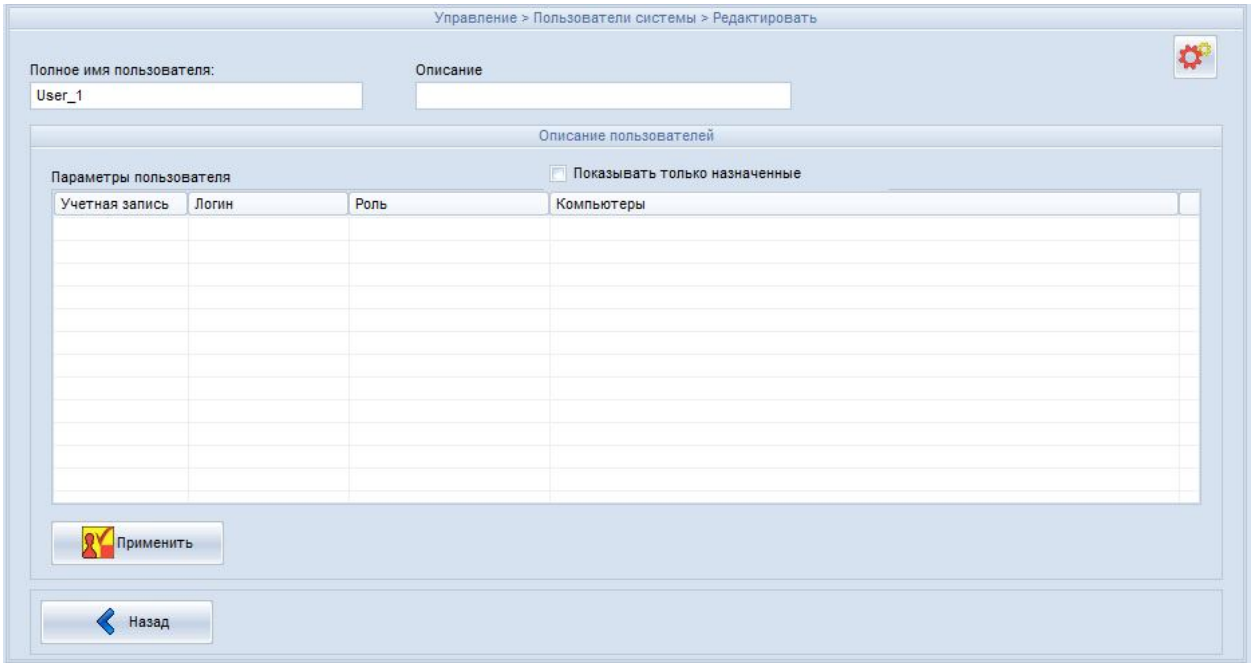

Рисунок 30 - Изменение параметров пользователя

В данном окне следует ввести новое имя пользователя и/или новое описание пользователя. Для сохранения внесённых изменений нужно нажать кнопку <Применить>.

Примечание. Если в описании параметров пользователя (рисунок 30) поля «Учётная запись» или «Роль» пусты, то это означает, что выполнена процедура удаления учётной записи, которая принадлежала данному пользователю РАУ, или удаления роли, назначенной данному пользователю (выполняет Администратор ИБ в соответствии с документом «11443195.4012-053 91. Руководство Администратора ИБ РАУ»).

Кнопка <Настройка отображения информации> позволяет в окне, приведённом на рисунке 30, отображать и скрывать информацию о задании роли, назначенной данному пользователю, списка файлов для контроля целостности, списка задач (*.act файлов), списка стартовых задач, а также информацию о том, управ-

ляется ли от СВМиКД ПКО, на котором зарегистрирован данный пользователь. После нажатия на кнопку <Настройка отображения информации> выводится окно, приведённое на рисунке 31. В данном окне нужно установить флажки напротив той информации, которую следует отображать.

После установки необходимых флажков в таблице описания пользователей появляется столбец под названием «ПКО». Наличие литеры «К» в данном столбце означает, что для роли, назначенной данному пользователю, определен список файлов для контроля целостности, наличие литеры «З» – определен список задач, литеры «С» – определен список стартовых задач, У – ПКО, на котором зарегистрирован данный пользователь, управляется от СВМиКД.

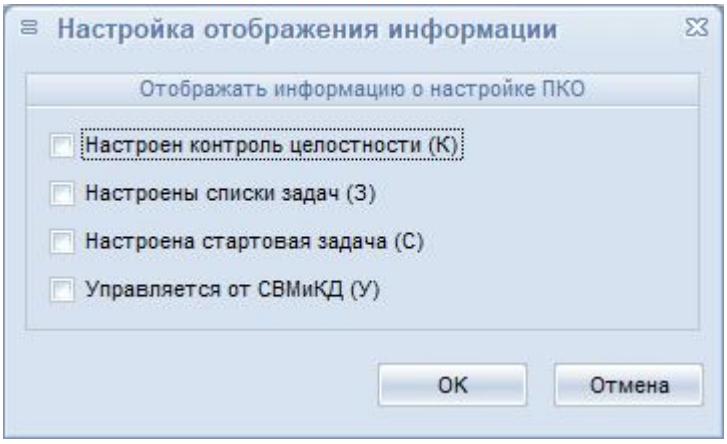

Рисунок 31 – Настройка отображения информации

4.2.5 Удаление пользователя

Данная функция позволяет удалять пользователей системы.

Для удаления пользователей следует в окне, приведённом на рисунке 24, установить флажки напротив пользователей, которых нужно удалить, нажать кнопку <Удалить> и утвердительно ответить на сообщение, запрашивающее подтверждение удаления пользователей.

В ПО РАУ при выполнении процедуры удаления пользователя системы предусмотрена возможность автоматического редактирования параметров учётной записи пользователя РАУ. По выполнении процедуры удаления пользователя системы в параметрах учётных записей, назначенных данным пользователям, содержимое поля «Назначенные пользователи» аннулируется.

4.2.6 Поиск пользователя по идентификатору

Данная функция позволяет осуществлять поиск пользователя по его идентификатору.

Для поиска пользователя по идентификатору следует в окне, приведённом на рисунке 24, нажать кнопку <Поиск>. Будет выведено сообщение «Предъявите идентификатор!».

Если предъявленный идентификатор назначен какому-либо пользователю системы, то в окне, приведённом на рисунке 24, будет выделена строка, содержащая информацию о данном пользователе.

Если предъявленный идентификатор никакому пользователю системы не назначен, то в строке состояния окна, приведённого на рисунке 24, красным шрифтом будет выведено сообщение «Идентификатор не зарегистрирован!».

4.2.7 Вывод на печать информации о пользователях

Данная функция позволяет выводить на печать и в файл выбранную информацию о пользователях системы.

Для вывода на печать или в файл выбранной информации о пользователях системы следует в окне, приведённом на рисунке 24, установить флажок напротив пользователей, информацию о которых нужно вывести, и нажать кнопку <Печать>. Появится окно, приведённое на рисунке 32.

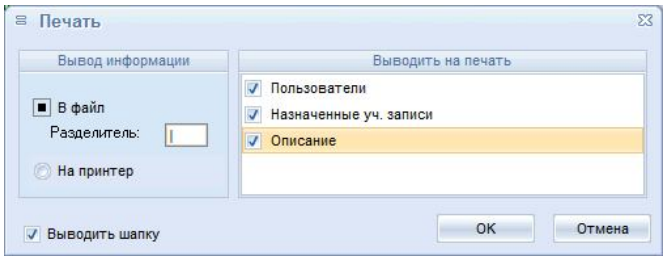

Рисунок 32 - Печать информации о пользователе

В данном окне следует выбрать способ вывода: в файл или на принтер, состав выводимой информации: имя пользователя, имя назначенной ему учетной записи, описание. При печати в файл также нужно задать разделитель.

4.3 Вкладка «USB-устройства»

4.3.1 Общие сведения

Внешний вид вкладки «USB-устройства» приведён на рисунке 33.

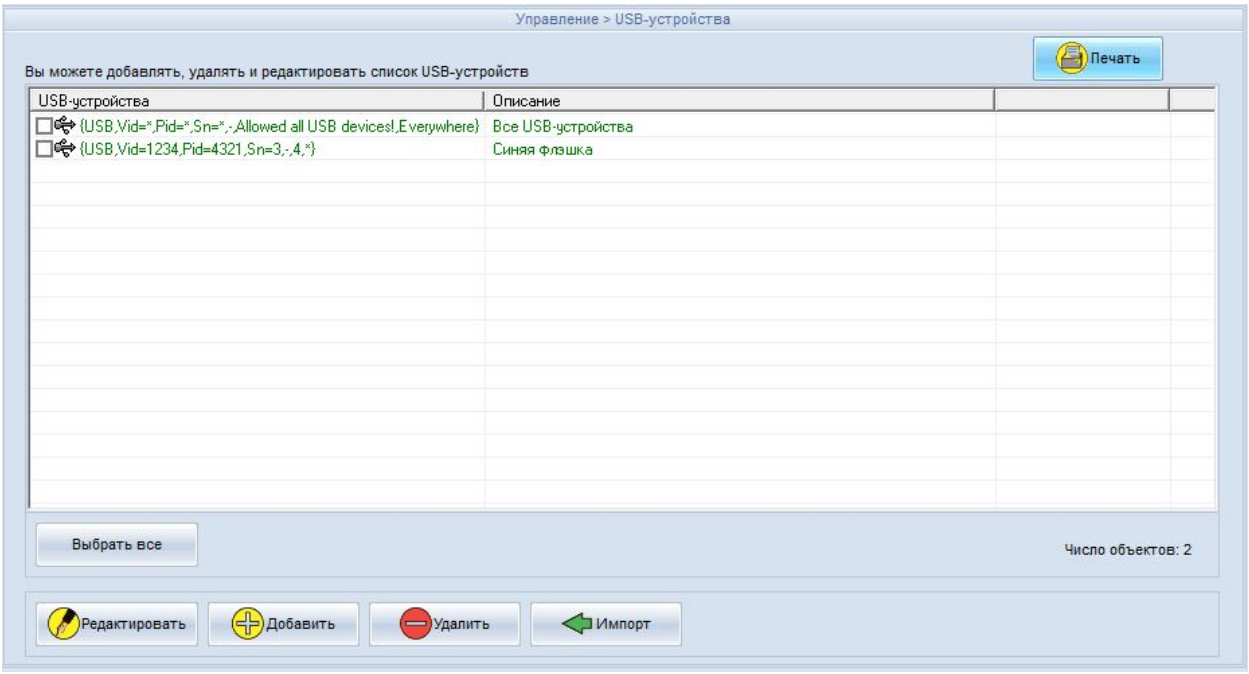

Рисунок 33 - Вкладка «USB-устройства»

Используя элементы управления данной вкладки, Администратор РАУ формирует список USB-устройств, с которыми разрешено работать на подконтрольных объектах системы. Данный список называется списком разрешённых USB-устройств системы. Для формирования данного списка Администратор РАУ использует следующие функции ПО СЦУ:

- добавление USB-устройства. Данная функция описана в пункте 0;
- импортирование информации о USB-устройствах от ПКО. Данная функция описана в пункте 4.3.3;
- изменение информации о USB-устройствах. Данная функция описана в пункте 4.3.4;
- удаление USB-устройств. Данная функция описана в пункте 4.3.5;
- вывод на принтер информации, приведённой во вкладке Управление> USB-устройства, а также сохранения данной информации в файл. Данная функция реализуется путём нажатия кнопки <Печать>.

По выполнении процедуры создания списка разрешенных устройств информация из поля «Описание» во вкладке Управление\USB-устройства отображается в соответствующей графе «Описание» программы ACED32.exe:

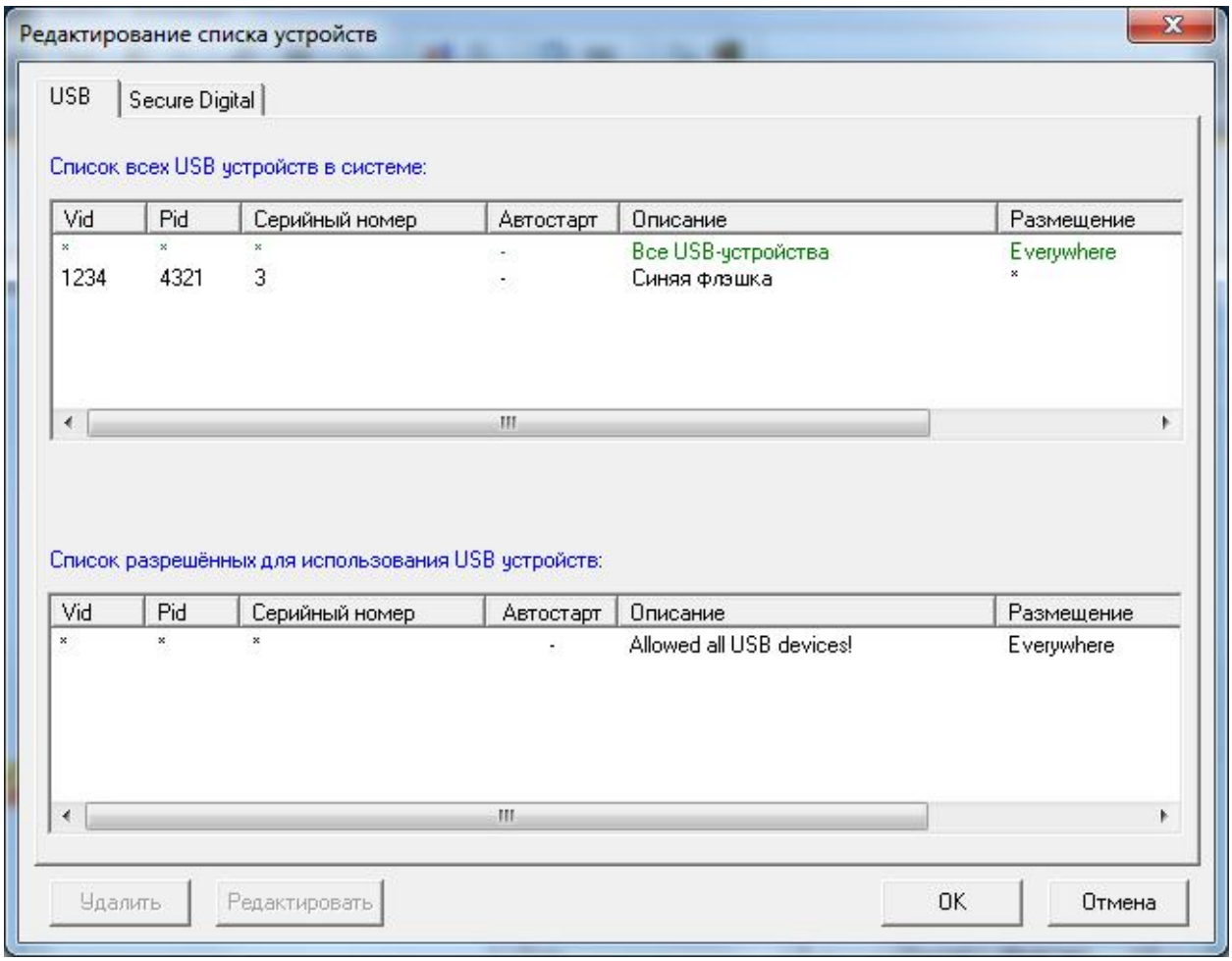

Рисунок 34 - Информация из поля «Описание» во вкладке Управление\USB-устройства совпадает с информацией в графе «Описание» программы ACED32.EXE

4.3.2 Добавление USB-устройства

Данная функция позволяет добавлять USB-устройства в список разрешённых USB-устройств системы.

Для добавления USB-устройства в список разрешённых USB-устройств системы следует в окне, приведённом на рисунке 33, нажать кнопку <Добавить>. На экран будет выведено окно, приведённое на рисунке 35.

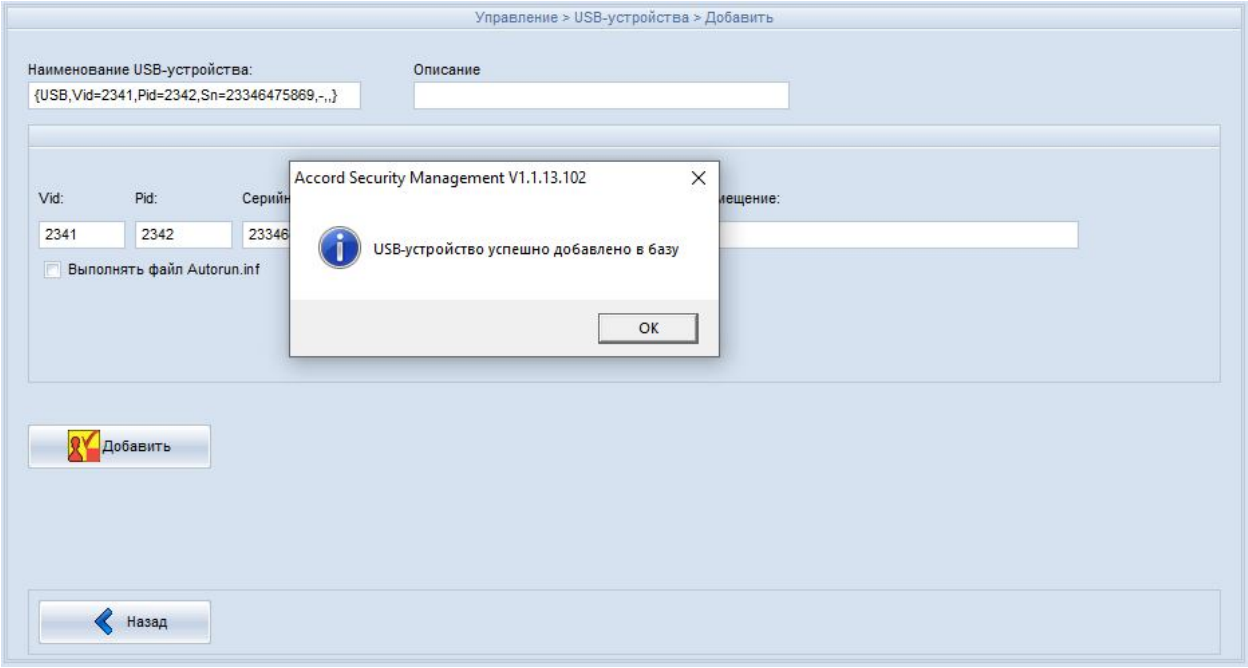

Рисунок 35 - Добавление USB-устройства в список разрешённых USB-устройств системы

В данном окне следует ввести Vid (идентификатор производителя), Pid (идентификатор устройства), серийный номер добавляемого USB-устройства, его размещение и описание (последние два поля не являются обязательными для заполнения). После нажатия кнопки <Добавить> USB-устройство с заданными параметрами будет добавлено в список разрешённых USB-устройств системы.

4.3.3 Импортирование информации о USB-устройствах от ПКО

4.3.3.1 Общие сведения об импортировании информации о USB-устройствах

ПО СЦУ позволяет импортировать в список разрешённых USB-устройств системы информацию о следующих USB-устройствах:

- USB-устройствах, подключенных к ПКО в настоящий момент либо подключаемых к ним когда-нибудь ранее. Импортирование данных USB-устройств описано в подпункте 4.3.3.2;
- USB-устройствах, которые СЗИ НСД разрешают использовать на ПКО. Импортирование данных USB-устройств описано в подпункте 4.3.3.3.

4.3.3.2 Импортирование информации о USB-устройствах, подключаемых к ПКО

Данная функция позволяет импортировать в список разрешённых USB-устройств системы информацию о USB-устройствах, подключенных к ПКО в настоящий момент либо подключаемых к ним когда-нибудь ранее.

Для выполнения данной операции следует в окне, приведённом на рисунке 33, нажать кнопку <Импорт>. В появившемся окне импорта USB-устройств, приведённом на рисунке 36, установить переключатель «Вы можете импортировать USB-устройства из:» в положение «включенных ПКО».

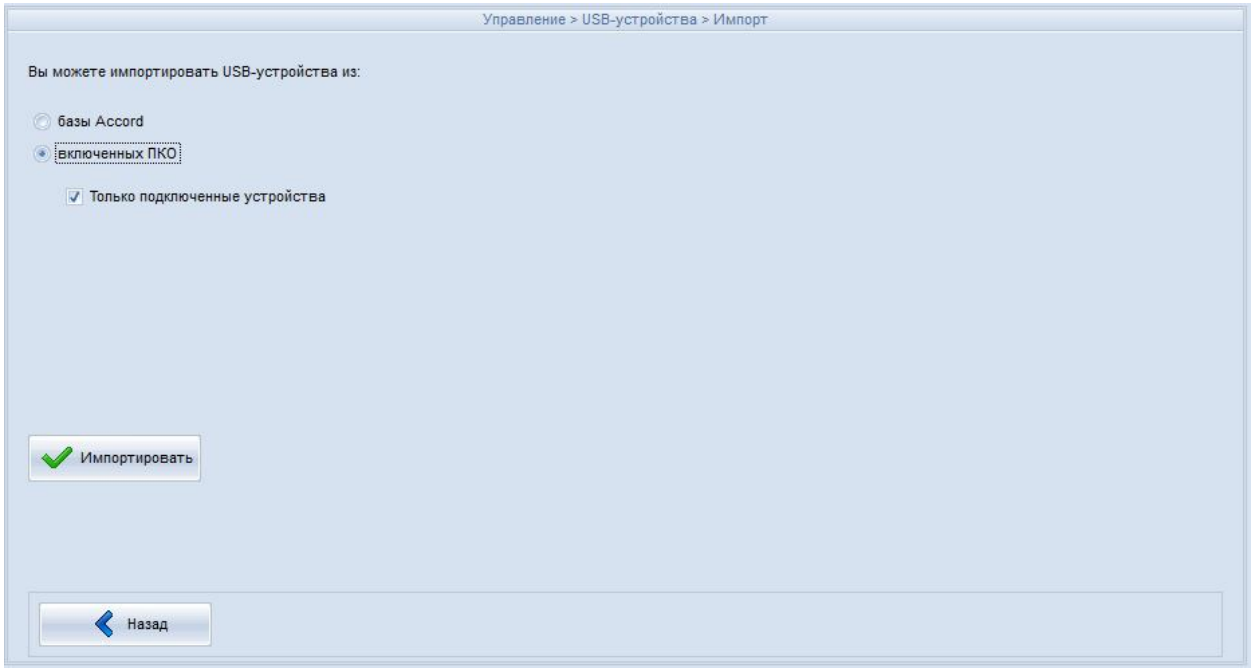

Рисунок 36 – Окно импорта USB-устройств. Импортирование информации о подключаемых к ПКО USB-устройствах

Если флажок «Только подключенные устройства» в окне импорта USB-устройств, приведённом на рисунке 36, установлен, то в список разрешённых USB-устройств системы будет импортирована информация о USB-устройствах, подключенных к подконтрольным объектам в настоящий момент времени.

Если флажок «Только подключенные устройства» в окне импорта USB-устройств, приведённом на рисунке 36, снят, то в список разрешённых USB-устройств системы будет импортирована информация о USB-устройствах, когда-либо подключаемых к подконтрольным объектам и сведения о которых сохранились операционной системой.

После нажатия кнопки <Импортировать> будет выведено окно, приведённое на рисунке 37.

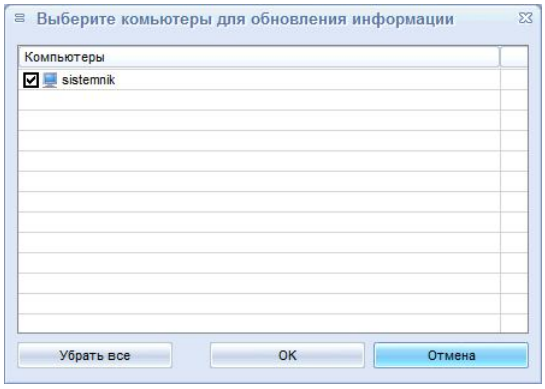

Рисунок 37 – Выбор ПКО, от которых будет получена информация о подключаемых USB-устройствах

Данное окно позволяет установить ПКО, от которых будет получена информация о подключаемых USB-устройствах. Следует выбрать нужные ПКО и нажать кнопку <OK>.

4.3.3.3 Импортирование информации о USB-устройствах, которые СЗИ НСД разрешают использовать на ПКО

Данная функция позволяет импортировать в список разрешённых USB-устройств системы информацию о разрешенных СЗИ НСД к использованию на ПКО USB-устройствах.

Необходимая для выполнения импортирования информация о разрешённых для использования на ПКО USB-устройствах передаётся подконтрольными объектами и хранится на СЦУ в так называемых базах пользователей – файлах с расширением *.amz. Имена этих файлов совпадают с именами ПКО, от которых они были получены.

Для импортирования в список разрешённых USB-устройств следует в окне, приведённом на рисунке 33, нажать кнопку <Импорт>. В появившемся окне импорта USB-устройств, приведённом на рисунке 38, установить переключатель «Вы можете импортировать USB-устройства из:» в положение «базы Accord».

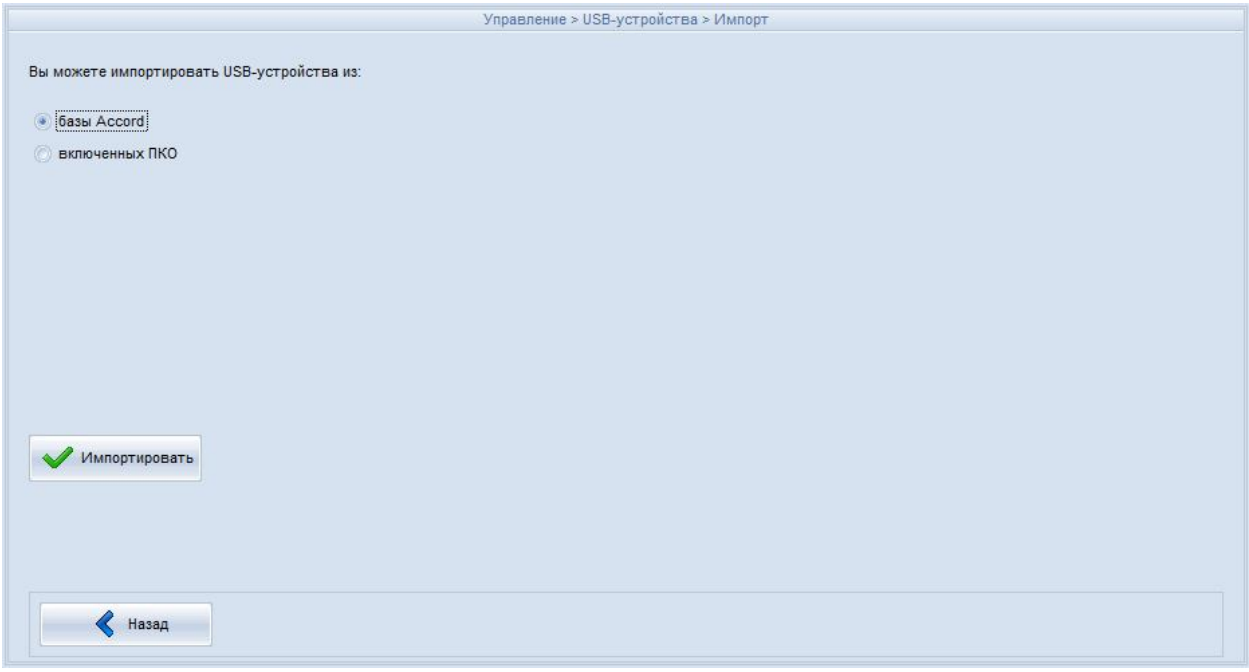

Рисунок 38 - Окно импорта USB-устройств. Импортирование информации о USB-устройствах, которые СПО «Аккорд-Win64 К» разрешает использовать на ПКО

Для импортирования информации о USB-устройствах следует в окне импорта USB-устройств (рисунок 38) нажать кнопку <Импортировать>. Появится стандартное диалоговое окно открытия файла, в котором Администратору РАУ следует выбрать файл с расширением *.amz (базу пользователей), содержащий информацию о USB-устройствах, которые следует импортировать в список разрешённых USB-устройств системы. На СЦУ файлы с расширением *.amz хранятся в папке C:\Asm\ACCONNET\IN\, имена этих файлов совпадают с именами ПКО, от которых они были получены.

После выбора и открытия файла базы пользователей окно импорта USB-устройств примет вид, приведённый на рисунке 39.

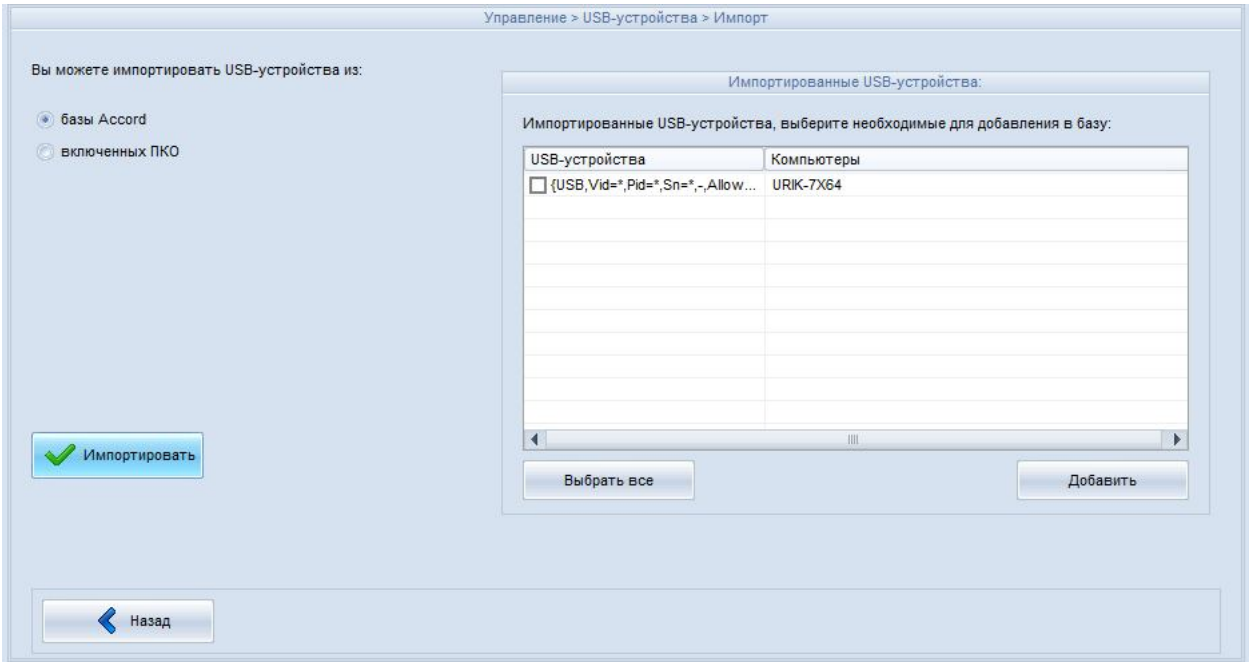

Рисунок 39 - Окно импорта USB-устройств. Импортирование информации о USB-устройствах, которые СПО «Аккорд-Win64 К» разрешает использовать на ПКО. Выбор USB-устройств для импорта

В правой части окна импорта USB-устройств, приведённого на рисунке 39, будет отображаться список USB-устройств, информация о которых содержится в выбранной базе пользователей. Администратору РАУ следует установить флажки напротив тех USB-устройств, которые нужно импортировать в список разрешённых USB-устройств системы и нажать кнопку <Добавить>.

Как показано на рисунке 40, список импортированных USB-устройств будет совпадать со списком разрешённых для использования USB-устройств, сформированным на ПКО средствами СПО СЗИ НСД «Аккорд-Win64 К».

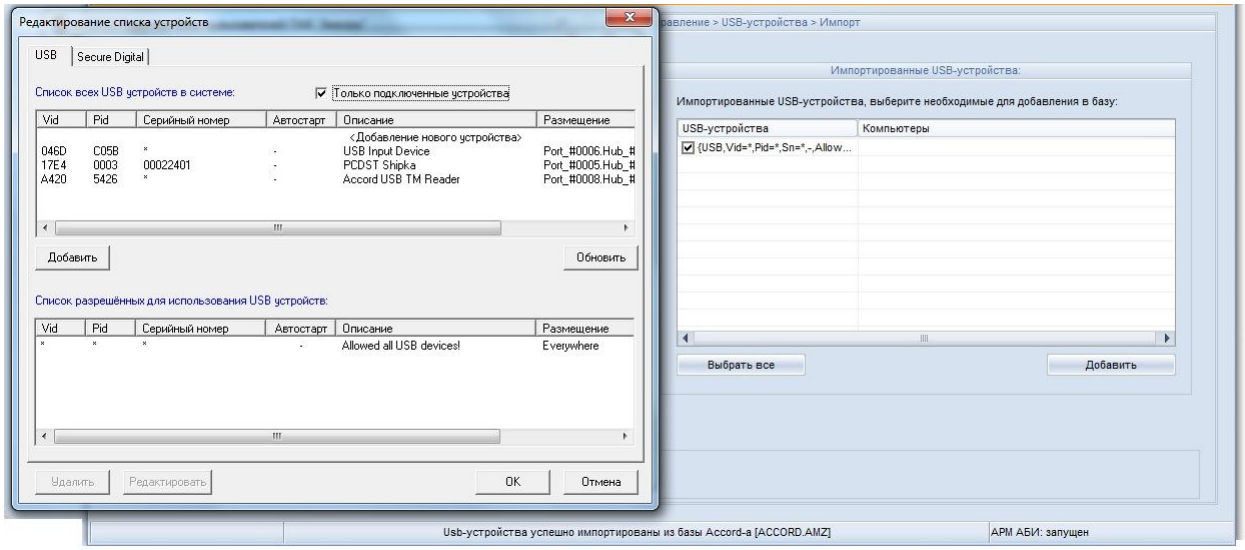

Рисунок 40 - Совпадение списка импортированных USB-устройств со списком разрешённых для использования на ПКО USB-устройств

4.3.4 Изменение информации о USB-устройствах

Данная функция позволяет изменять Vid, Pid, серийный номер, размещение и описание USB-устройств из списка разрешённых USB-устройств системы.

Для изменения информации о USB-устройстве следует в окне, приведённом на рисунке 33, дважды щелкнуть по записи, соответствующей данному USB-устройству, или, установив флажок напротив данного USB-устройства, нажать кнопку <Редактировать>. Появится окно, приведённое на рисунке 41.

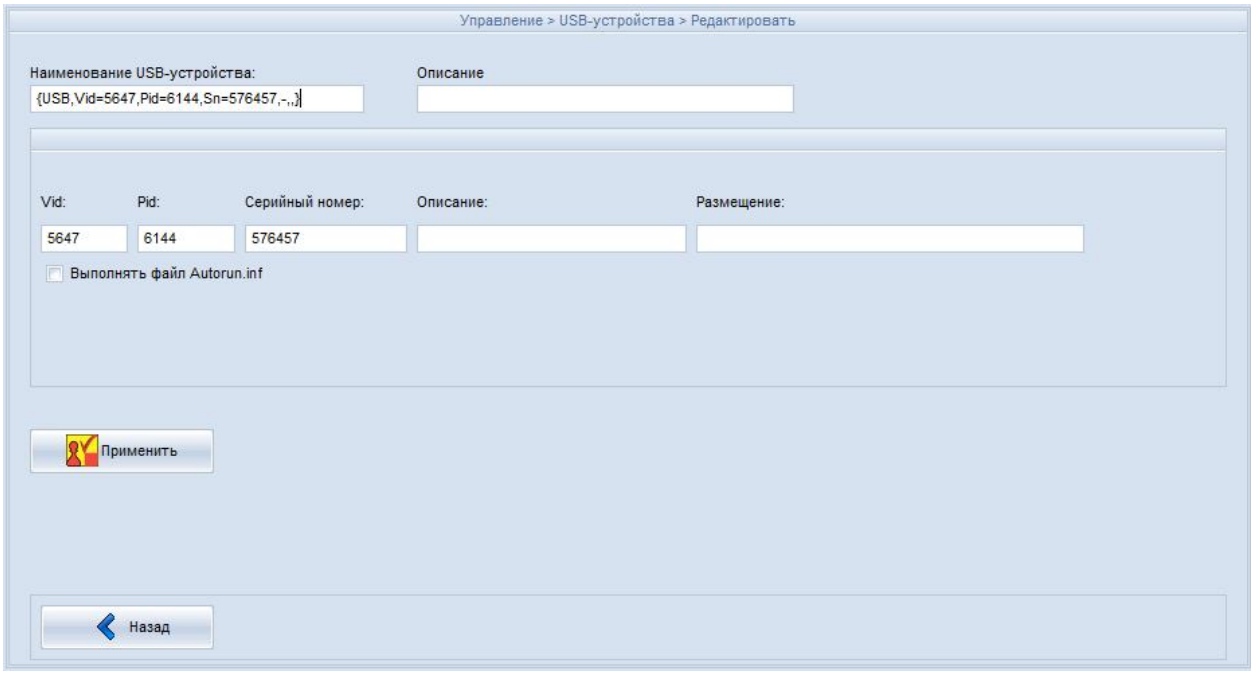

Рисунок 41 - Изменение информации о USB-устройстве

В данном окне следует внести необходимые изменения в информацию о USB-устройстве. Для сохранения внесённых изменений нажать кнопку <Применить>.

4.3.5 Удаление USB-устройств

Данная функция позволяет удалять USB-устройства из списка разрешённых USB-устройств системы.

Для удаления USB-устройств следует в окне, приведённом на рисунке 33, установить флажки напротив USB-устройств, которые нужно удалить, нажать кнопку <Удалить> и утвердительно ответить на сообщение, запрашивающее подтверждение удаления USB-устройств.

4.4 Вкладка «Роли»

Во вкладке Управление > Роли системы, приведённой на рисунке 42, Администратор РАУ может осуществлять просмотр параметров ролей: имени и описания роли, назначенных технологических участков, а также информации о наличии списков файлов контроля целостности, списков задач и стартовых задачах.

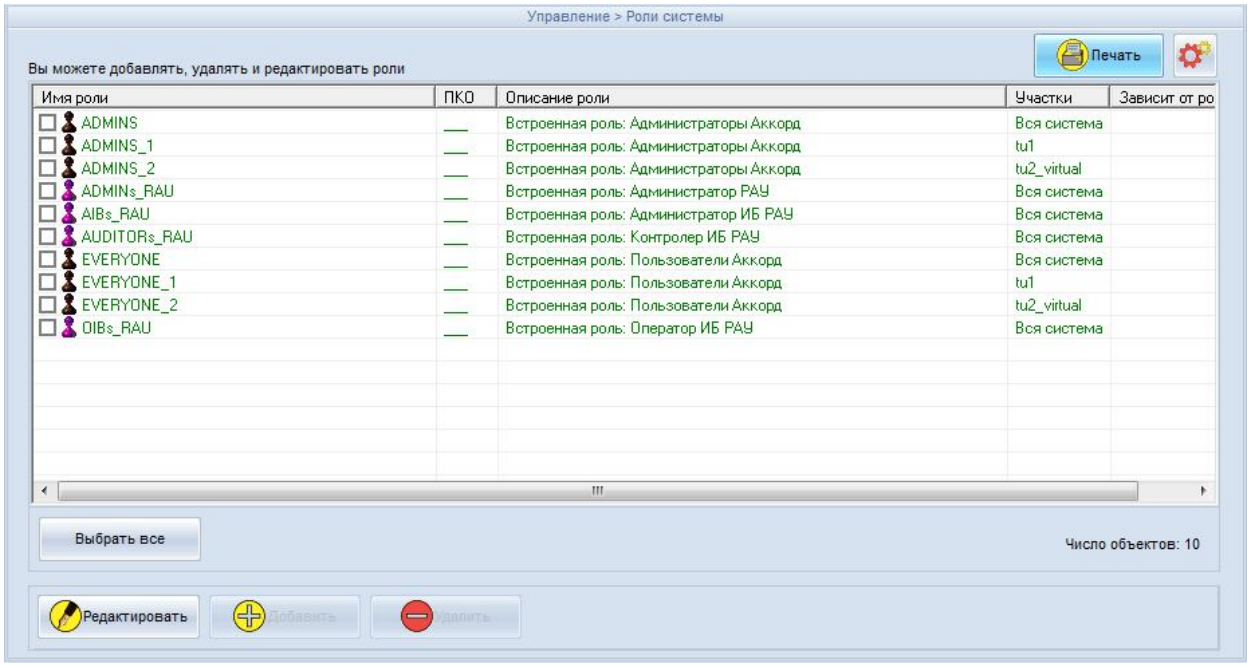

Рисунок 42 - Вкладка Управление > Роли системы

Для отображения в списке ролей вкладки Управление > Роли системы, приведённой на рисунке 42, информации о наличии списков файлов контроля целостности, списков задач и стартовых задачах нужно нажать кнопку <Настройка отображения информации>. Появится окно, приведённое на рисунке 43, в котором устанавливаются флаги напротив той информации о настройках ПКО, которую нужно отображать.

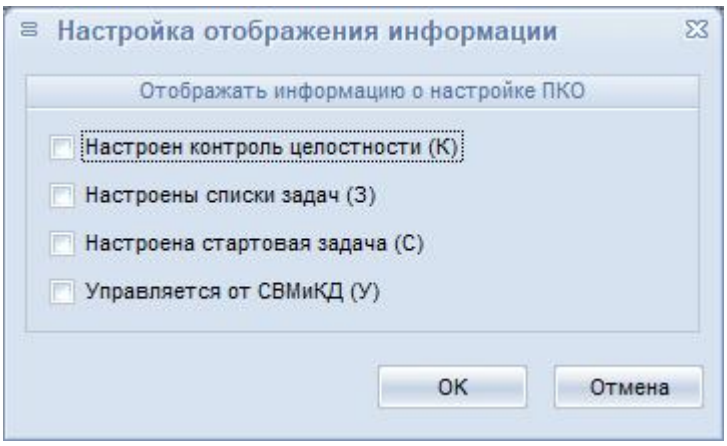

Рисунок 43 - Настройка отображения информации

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» – ПКО, на котором зарегистрирован данный пользователь, управляется от СВМиКД.

Кнопка <Печать> позволяет распечатать выбранную информацию на принтере, а также сохранить в файл (с указанным разделителем). При ее нажатии выводится окно, приведённое на рисунке 44, в котором нужно выбрать способ печати: в файл или на принтер, тип выводимой информации (имя роли, подконтрольный объект, описание роли, участки); при печати в файл следует также указать разделитель.

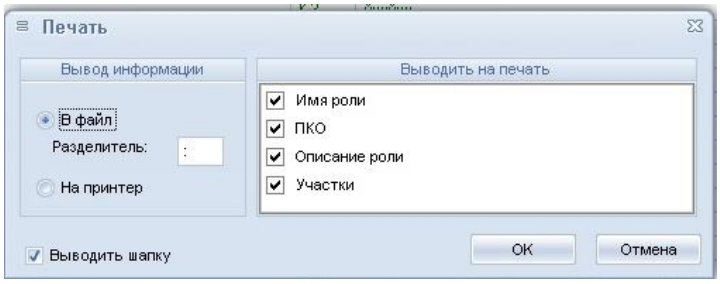

Рисунок 44 - Печать информации о ролях

Нажатие кнопки <Редактировать> выводит окно, приведённое на рисунке 45.

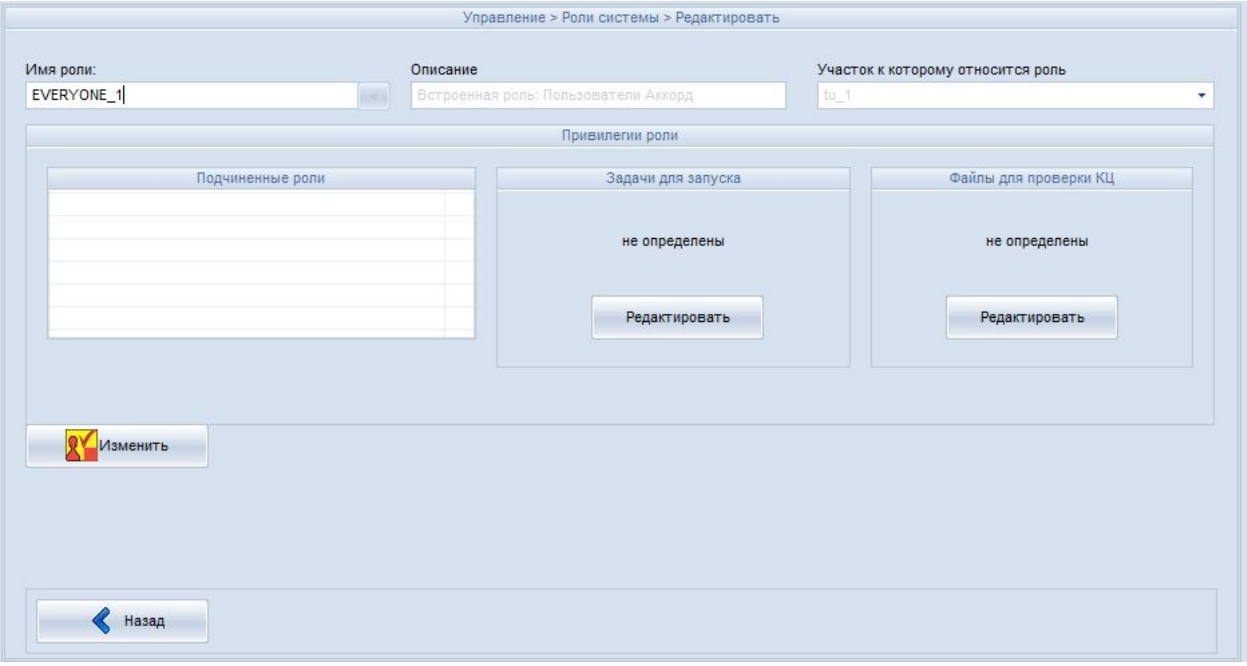

Рисунок 45 - Просмотр характеристик роли

Администратор может просмотреть следующие свойства роли:

- роли, подчиненные просматриваемой роли;
- список программ, которые может запускать данная роль. Для этого нужно нажать кнопку <Редактировать> в области «Задачи для запуска»;
- список файлов, целостность которых контролируется для данной роли ПАК СЗИ от НСД «Аккорд». Для этого нужно нажать кнопку <Редактировать> в области «Файлы для проверки КЦ».

Изменять эту информацию администратор не может. При попытке внести какие-либо изменения в данные свойства на экран выводится сообщение: «ВНИМАНИЕ!!! Вы зашли с правами контролёра. После выхода из программы база не будет модифицирована».

4.5 Вкладка «Идентификаторы»

Во вкладке Управление > Идентификаторы системы, приведённой на рисунке 46, Администратор РАУ выполняет процедуры просмотра списка зарегистрированных в системе идентификаторов, печати информации об идентификаторах, поиска идентификаторов в базе.

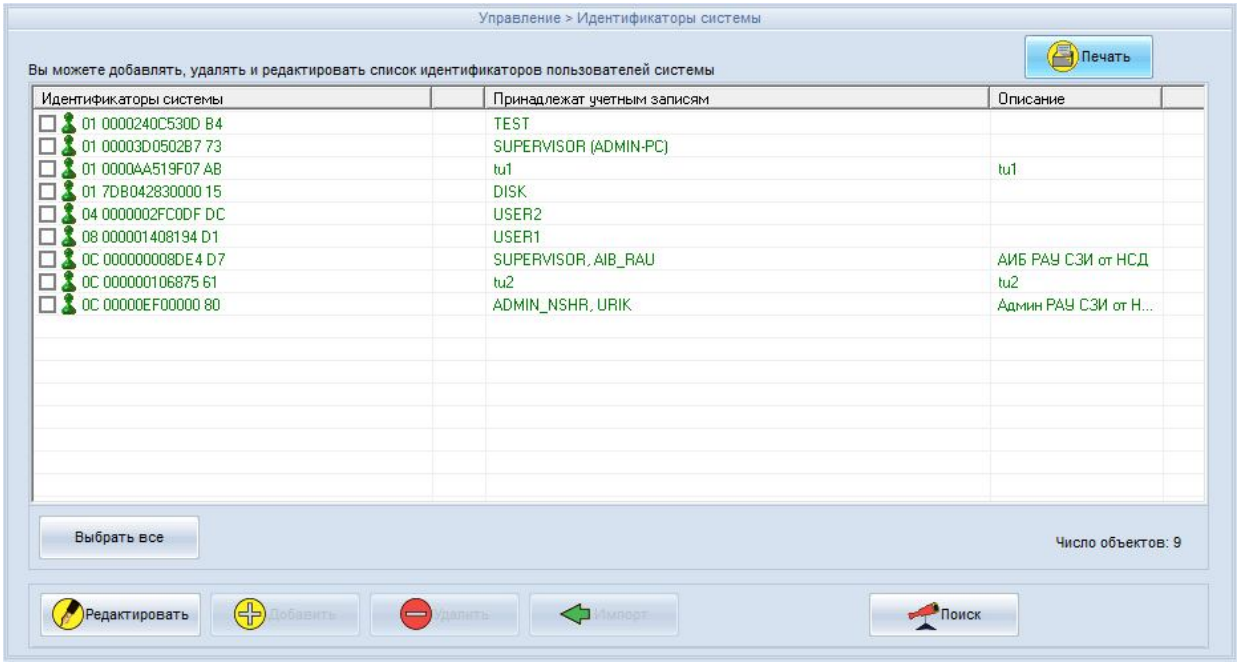

Рисунок 46 - Идентификаторы системы

Кнопка <Печать> позволяет распечатать выбранную информацию на принтере, а также сохранить в файл (с указанным разделителем). При ее нажатии появляется окно, приведённое на рисунке 47, в котором нужно выбрать способ печати: в файл или на принтер, тип выводимой информации (идентификаторы, учётные записи, которым принадлежит данный идентификатор, описание); при печати в файл следует также указать разделитель.

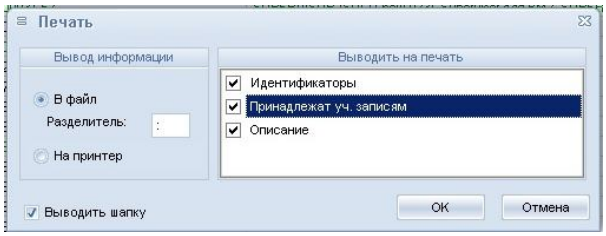

Рисунок 47 - Печать информации об идентификаторах

Если необходимо определить, добавлен ли идентификатор в базу РАУ, следует нажать кнопку <Поиск> во вкладке Управление > Идентификаторы системы. Появится окно с сообщением «Предъявите идентификатор», приведённое на рисунке 48.

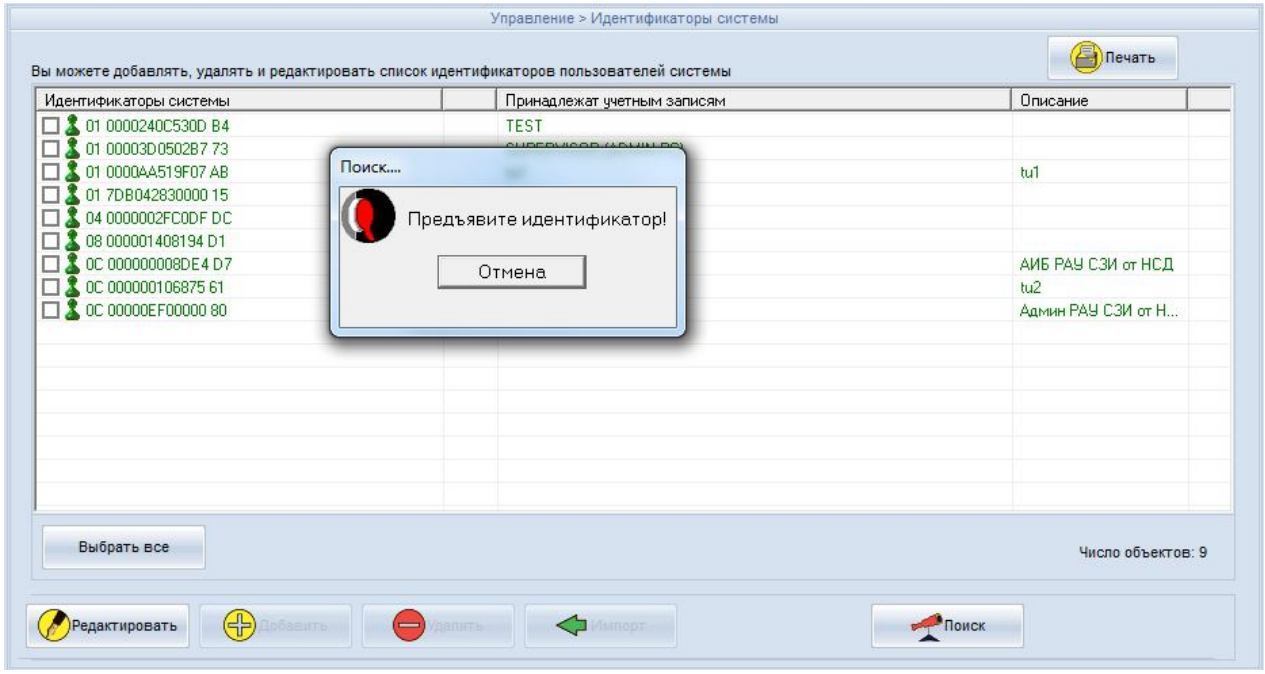

Рисунок 48 - Сообщение «Предъявите идентификатор»

Если предъявленный идентификатор имеется в базе, то этот идентификатор будет выделен, как показано на рисунке 49.

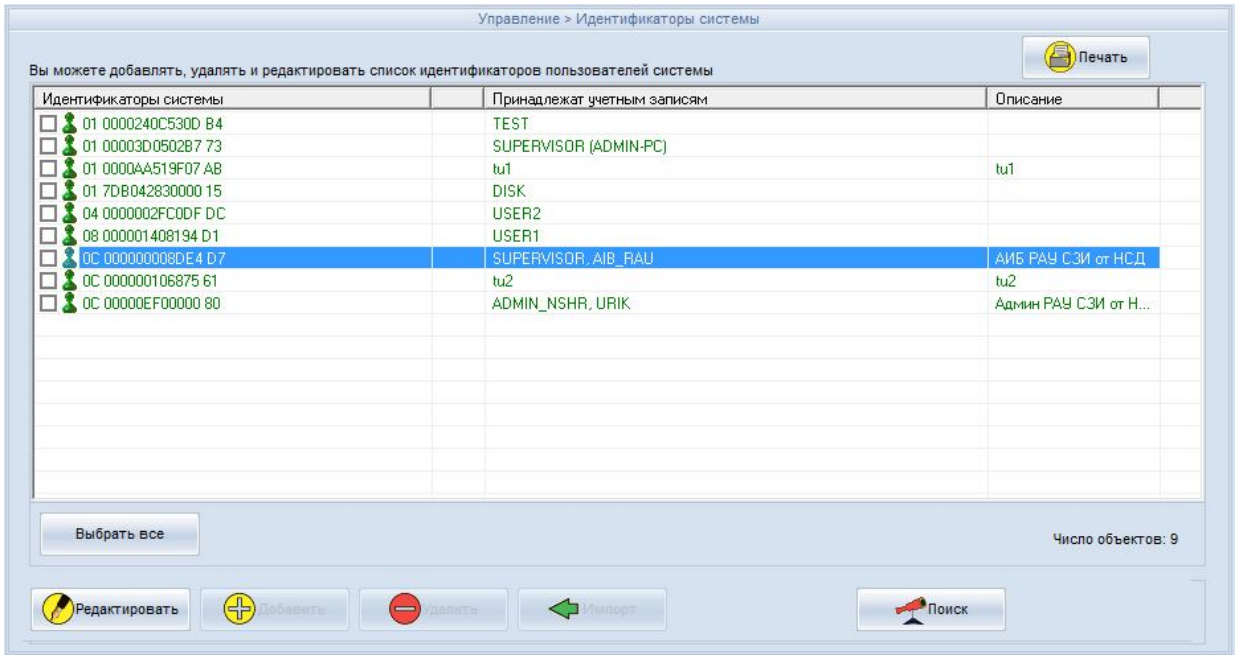

Рисунок 49 - Найдена учетная запись, которой назначен идентификатор

Если предъявленный идентификатор отсутствует в базе, то в нижней части окна появится сообщение «Идентификатор не зарегистрирован!», как показано на рисунке 50.

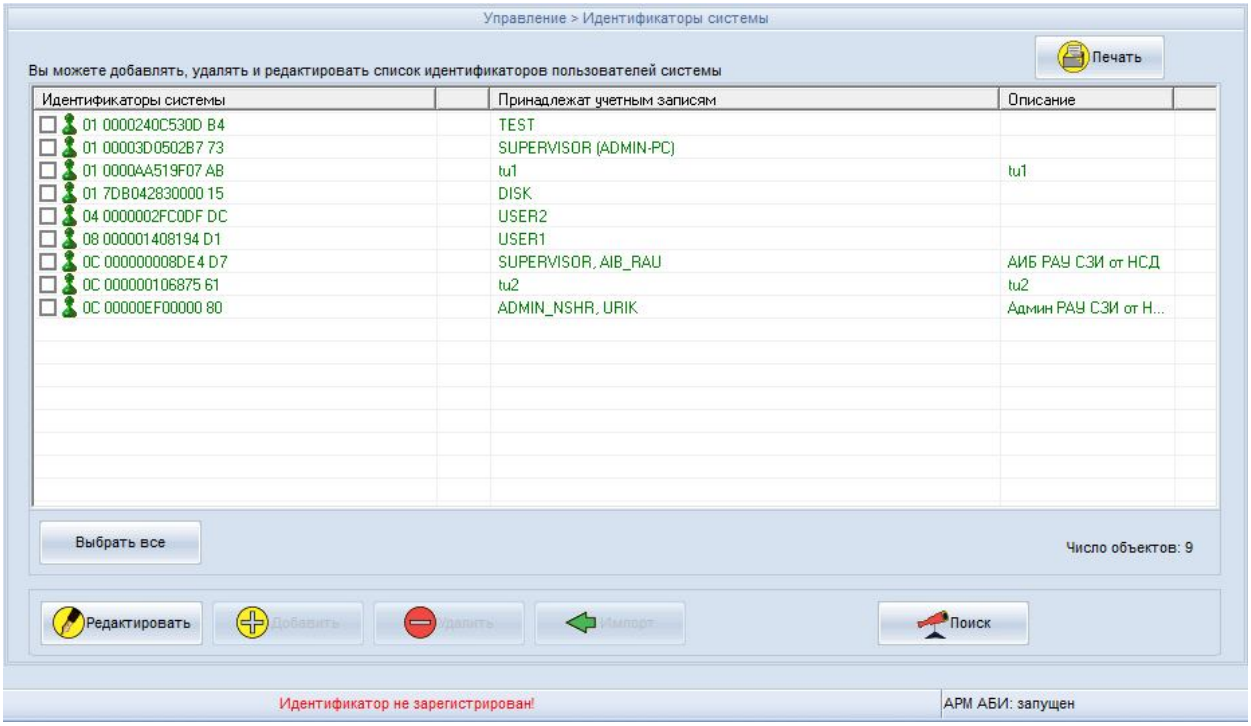

Рисунок 50 - Сообщение о том, что идентификатор не зарегистрирован

Нажатие кнопки <Редактировать> выводит окно, приведённое на рисунке 51.

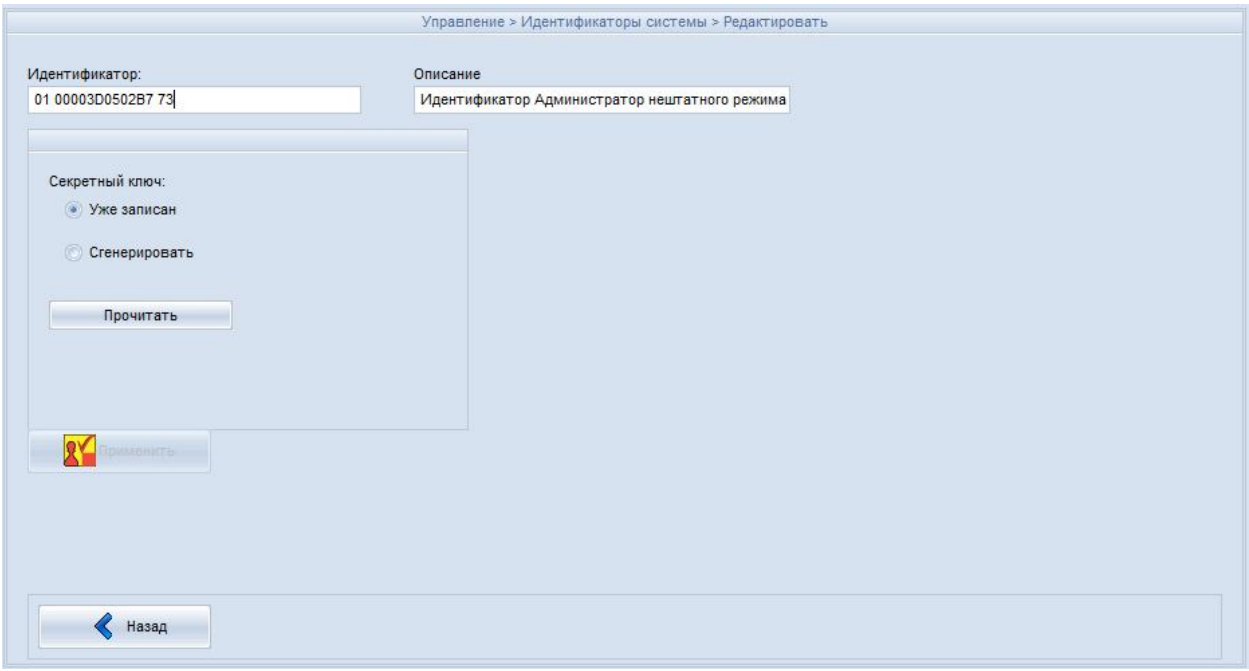

Рисунок 51 - Просмотр характеристик идентификатора

Администратор может просмотреть характеристики идентификатора, но изменять эту информацию он не может.

4.6 Вкладка «Компьютеры»

Во вкладке Управление > Компьютеры системы, приведённой на рисунке 52, Администратор РАУ может выполнять просмотр параметров ПКО, параметров ПАК СЗИ от НСД «Аккорд» и мандатные метки.

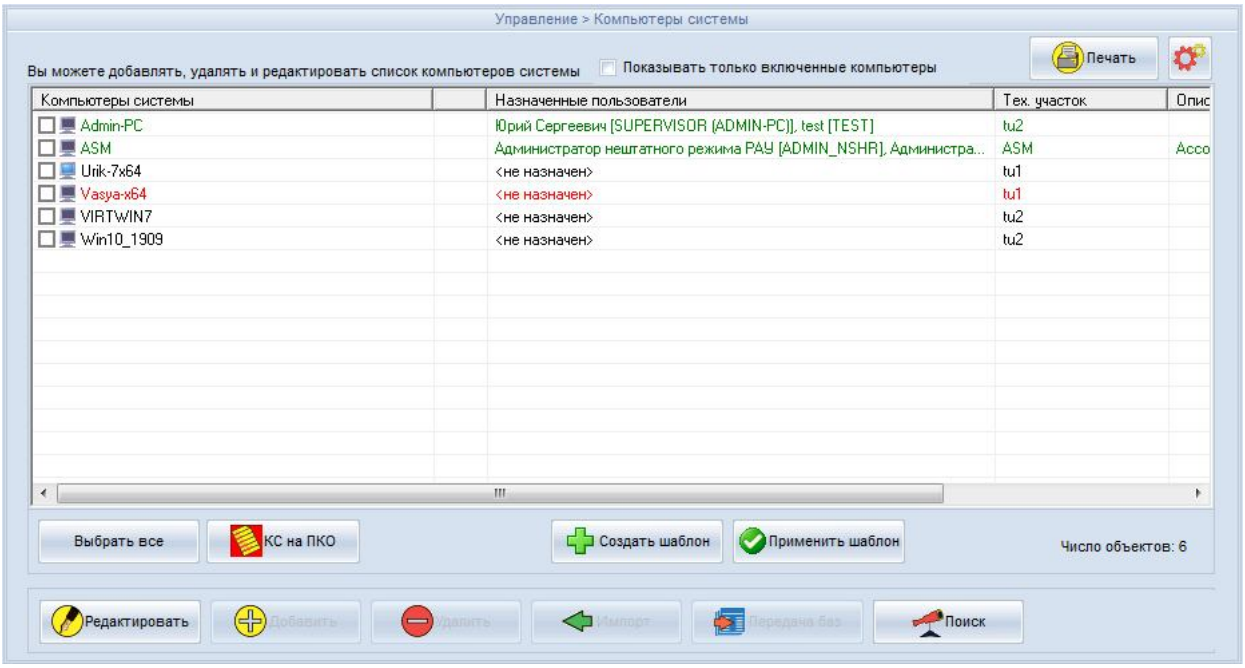

Рисунок 52 - Компьютеры системы

Для отображения в списке компьютеров информации о наличии списков файлов контроля целостности, списков задач (*.act файлов) и стартовых задачах следует в окне, приведенном на рисунке 52, нажать кнопку <Настройка отображения информации>. Появляется окно, приведённое на рисунке 31, в котором устанавливаются флаги напротив той информации о настройках ПКО, которую нужно отображать. 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» – ПКО, на котором зарегистрирован данный пользователь, управляется от СВМиКД.

Кнопка <Печать> позволяет распечатать выбранную информацию на принтере, а также сохранить в файл (с указанным разделителем). При ее нажатии появляется окно, приведённое на рисунке 53, в котором нужно выбрать способ печати: в файл или на принтер, тип выводимой информации (имя компьютера, описание компьютера, технологический участок, которому принадлежит данный компь-

ютер, IP-адрес компьютера, инвентарный номер компьютера, инвентарный номер платы АМДЗ Аккорд, серийный номер платы Аккорд, версия ПО Аккорд, версия сетевого агента, версия ПО контроллера, флаг получения журналов); при печати в файл следует также указать разделитель.

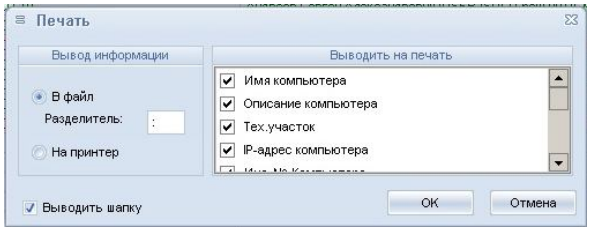

Рисунок 53 - Печать информации о компьютерах

Если необходимо определить, зарегистрирован ли компьютер в системе, следует нажать кнопку <Поиск> во вкладке Управление > Компьютеры системы (рисунок 52). Появится окно, приведённое на рисунке 54.

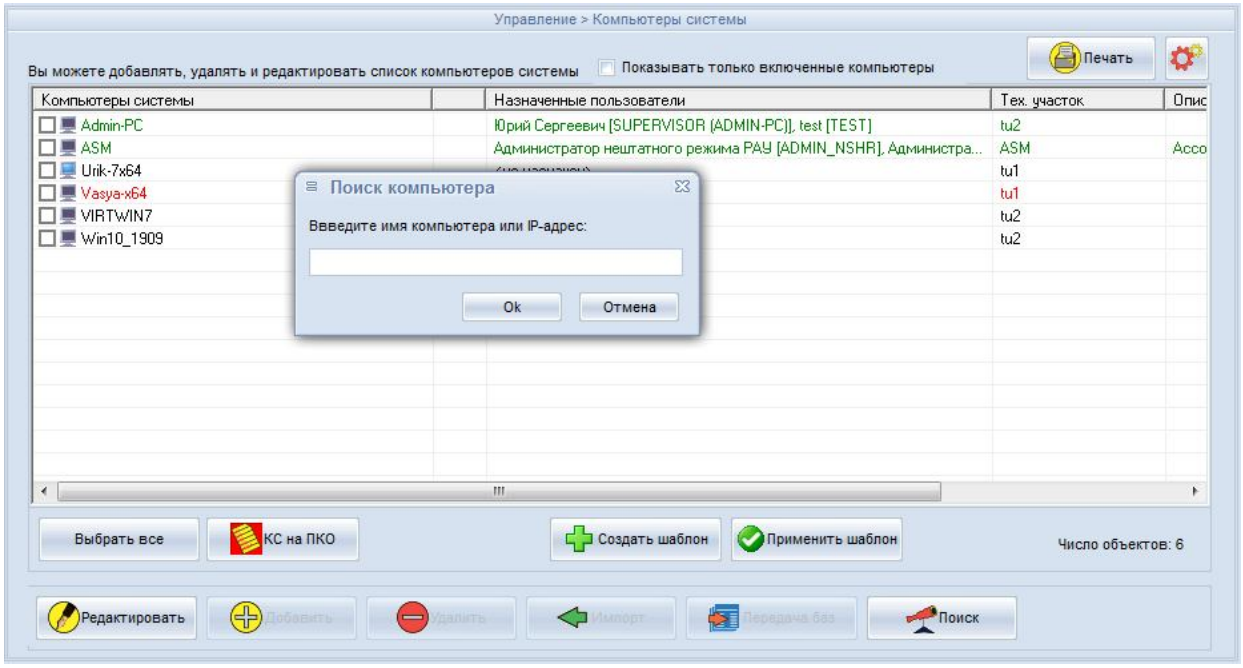

Рисунок 54 – Поиск компьютера по имени или IP-адресу

В данном окне необходимо указать IP-адрес компьютера или его имя. Если компьютер с таким именем или IP-адресом зарегистрирован в системе, то будет выделена соответствующая ему строка, как показано на рисунке 55.

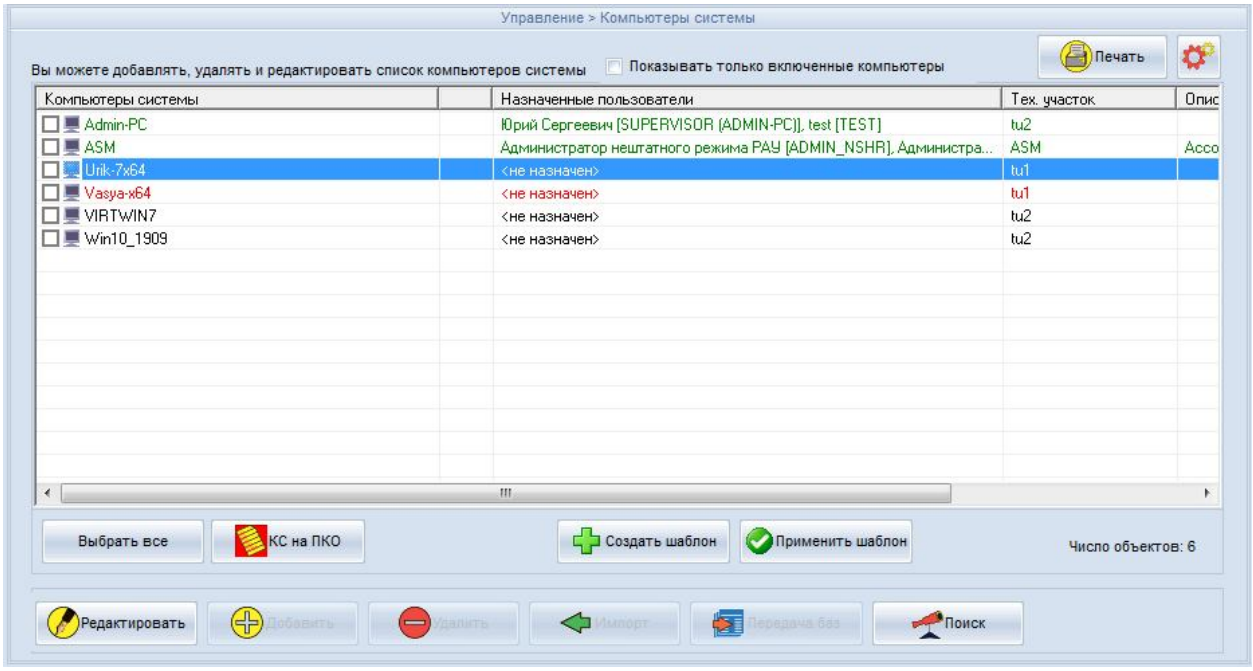

Рисунок 55 – Компьютер найден

Если компьютер с таким именем или IP-адресом не зарегистрирован в системе, то в нижней части окна появится сообщение «Компьютер не найден!», как показано на рисунке 56.

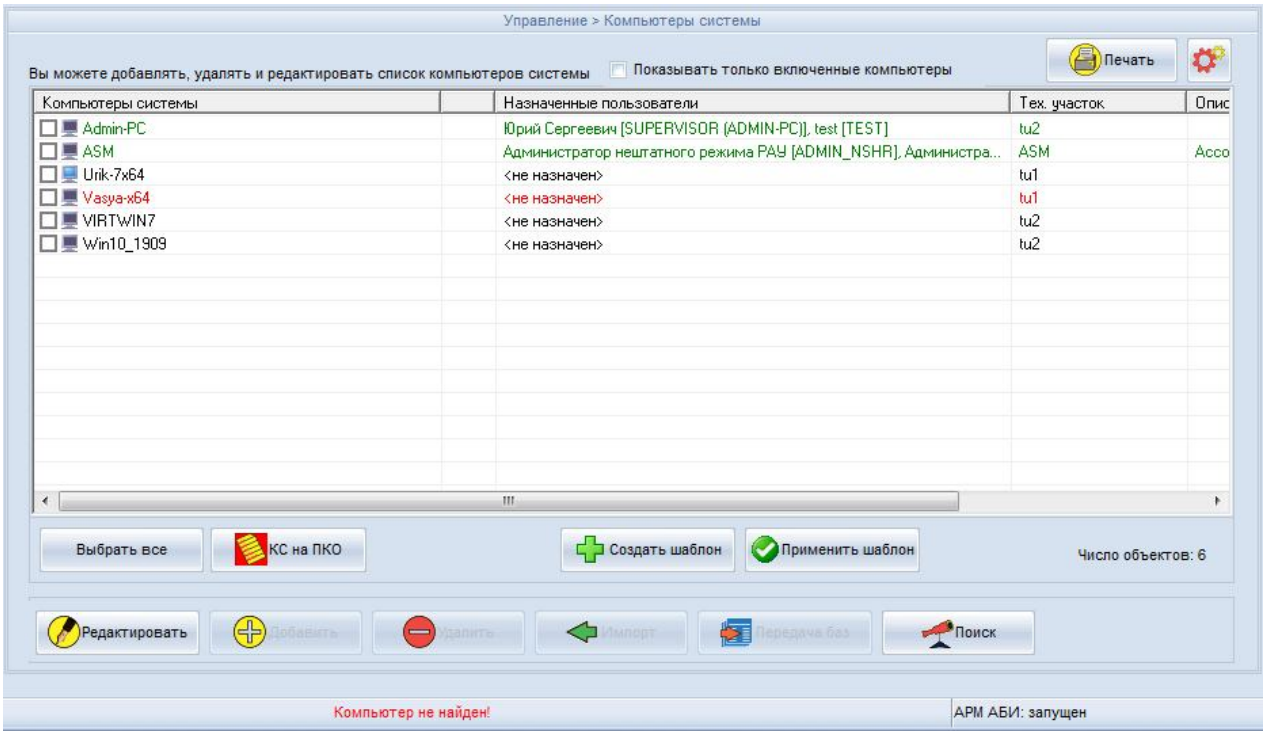

Рисунок 56 - Сообщение о том, что компьютер не найден

Кнопка <Создать шаблон> позволяет Администратору РАУ осуществлять просмотр задания для контроля целостности ПКО.

Нажатие кнопки <Редактировать> выводит на экран окно, приведённое на рисунке 57.

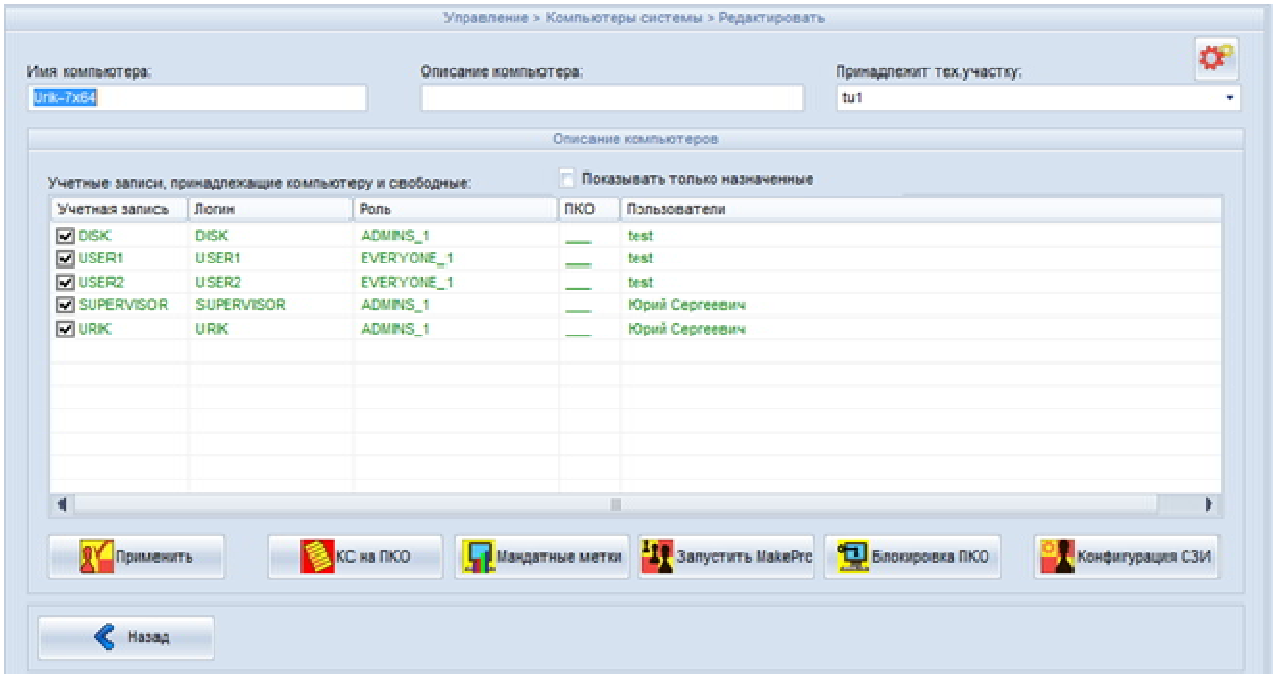

Рисунок 57 - Вкладка «Управление > Компьютеры системы > Редактировать»

Нажатие кнопки <Мандатные метки> выводит на экран окно, приведённое на рисунке 58.

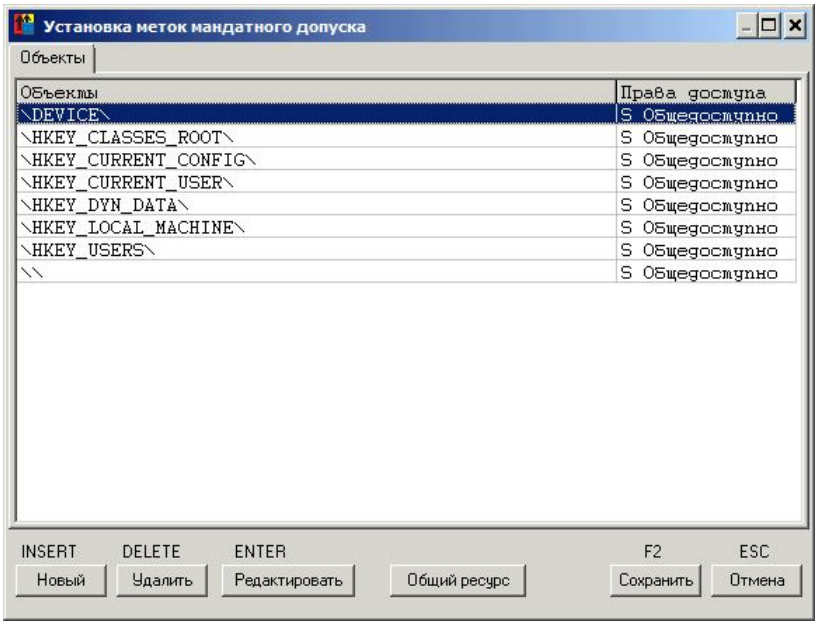

Рисунок 58 – Установка меток мандатного допуска

Администратор может просматривать метки мандатного доступа, но изменять их информацию он не может.

Нажатие кнопки <Конфигурация СЗИ> выводит окно, приведённое на рисунке 59, 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» (при наличии).

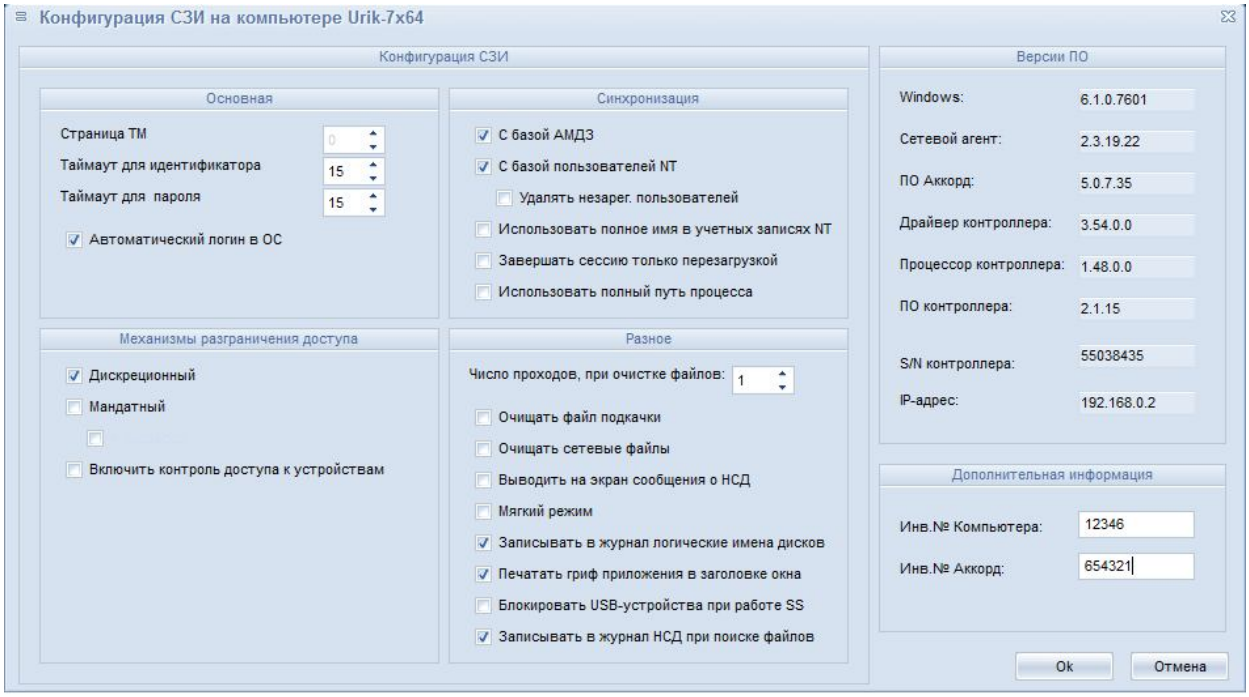

Рисунок 59 – Конфигурация СЗИ на подконтрольном объекте под управлением ОС Windows

На ПКО под управлением ОС Linux окно конфигурации СЗИ выглядит следующим образом:

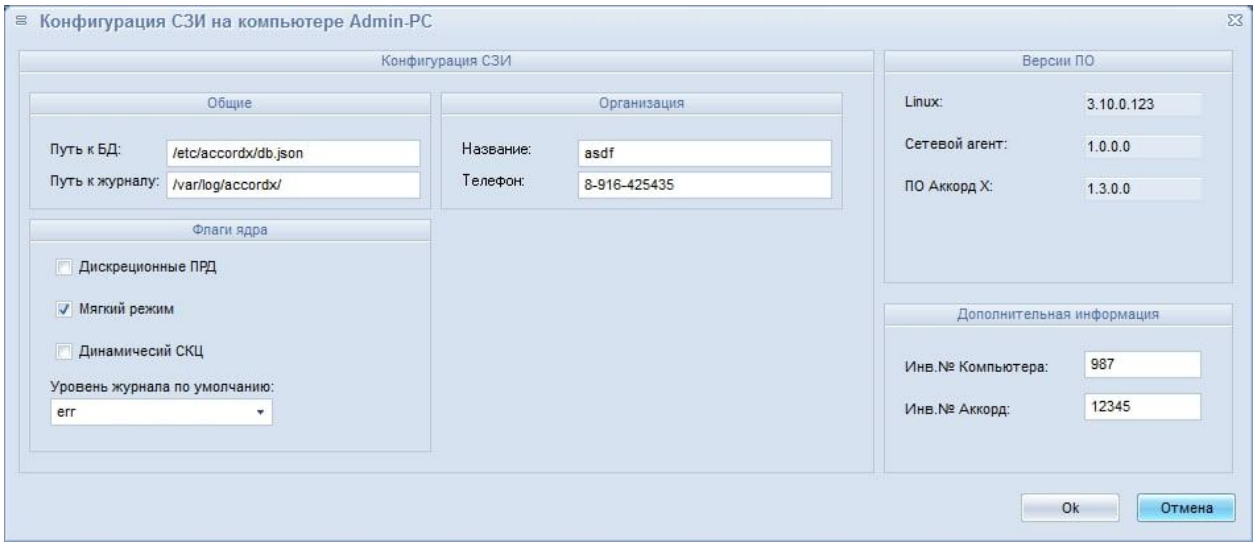

Рисунок 60 – Конфигурация СЗИ на подконтрольном объекте под управлением ОС Linux

В этом окне необходимо задать общие параметры и флаги ядра. Значение в строке «Путь к БД» (поле «Общие») соответствует параметру db-path конфигурационного файла, значение «Путь к журналу» - параметру log-dir-path. В поле "Фла-

ги ядра" задаются значения для флагов discr-acl (Дискреционные ПРД), soft-mode (Мягкий режим), icl (Динамический СКЦ) и default-log-level (Уровень журнала по умолчанию).

В поле «Организация» задаются параметры "Название" (company-name) и "Телефон" (company-phone), не влияющие на работоспособность СЗИ, которые могут быть использованы для удобства хранения справочной информации Администратором.

В поле "Версии ПО" указывается информация о версии ядра Linux (параметр Linux), версии клиента Аккорд-РАУ (Сетевой агент) и версии СЗИ (ПО Аккорд-X).

4.7 Вкладка «Технологические участки»

Во вкладке Управление > Технологические участки системы, приведённой на рисунке 61, Администратор РАУ может просматривать технологические участки.

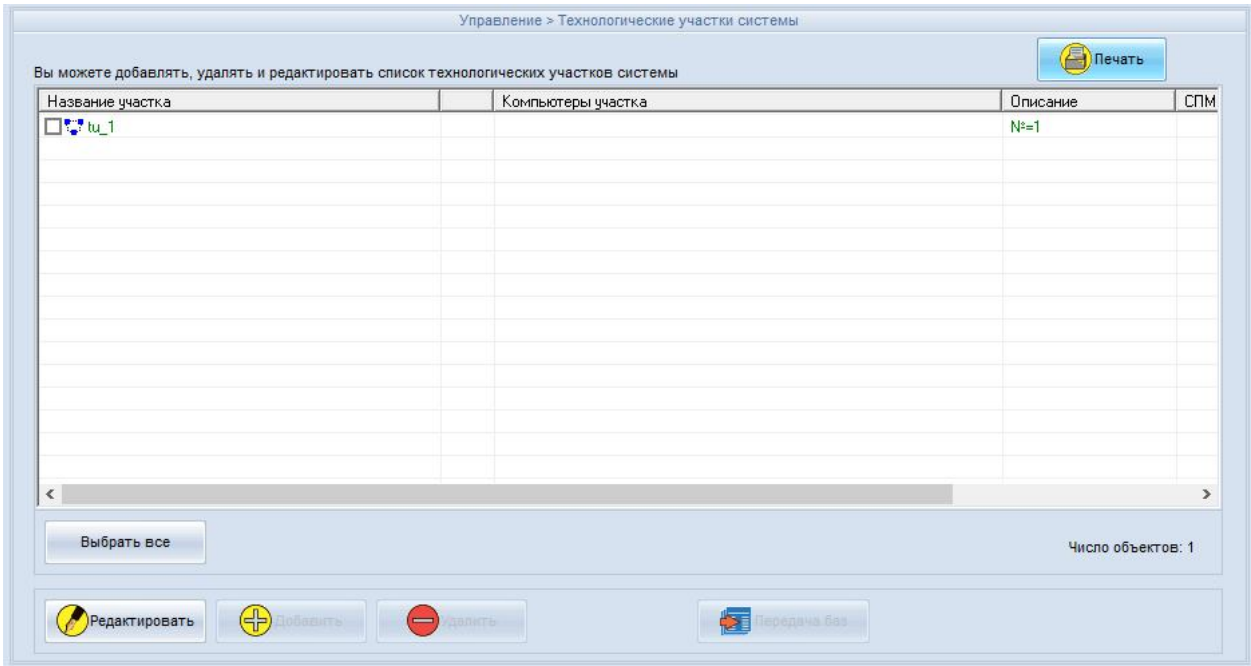

Рисунок 61 - Технологические участки системы

Кнопка <Печать> позволяет распечатать выбранную информацию на принтере, а также сохранить в файл (с указанным разделителем). После нажатия на данную кнопку на экран выводится окно, приведённое на рисунке 44, в котором нужно выбрать способ печати: в файл или на принтер, тип выводимой информации (имя участка, компьютеры, принадлежащие данному участку, описание техно-

логического участка, значение параметра синхронизации паролей доменных пользователей в технологическом участке (СПМТ)); при печати в файл следует также указать разделитель.

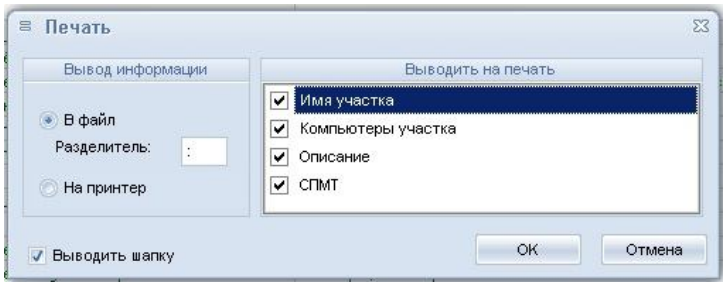

Рисунок 62 - Печать информации о технологических участках

Нажатие кнопки <Редактировать> выводит окно, приведённое на рисунке 63.

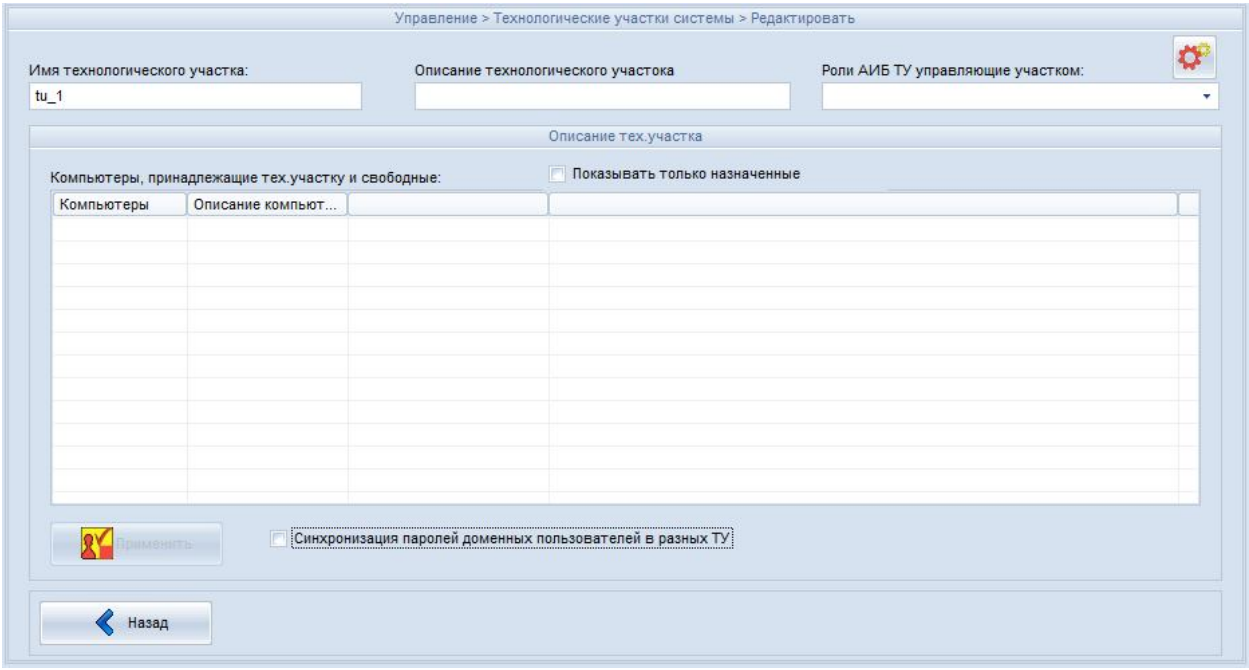

Рисунок 63 - Просмотр свойств технологического участка

Администратор может просматривать свойства технологического участка, но изменять их он не может.

4.8 Вкладка «Учётные записи»

Во вкладке Управление > Учётные записи, приведённой на рисунке 64, Администратор РАУ может просматривать учетные записи, печатать информацию об учетных записях и осуществлять поиск учетных записей по идентификатору.

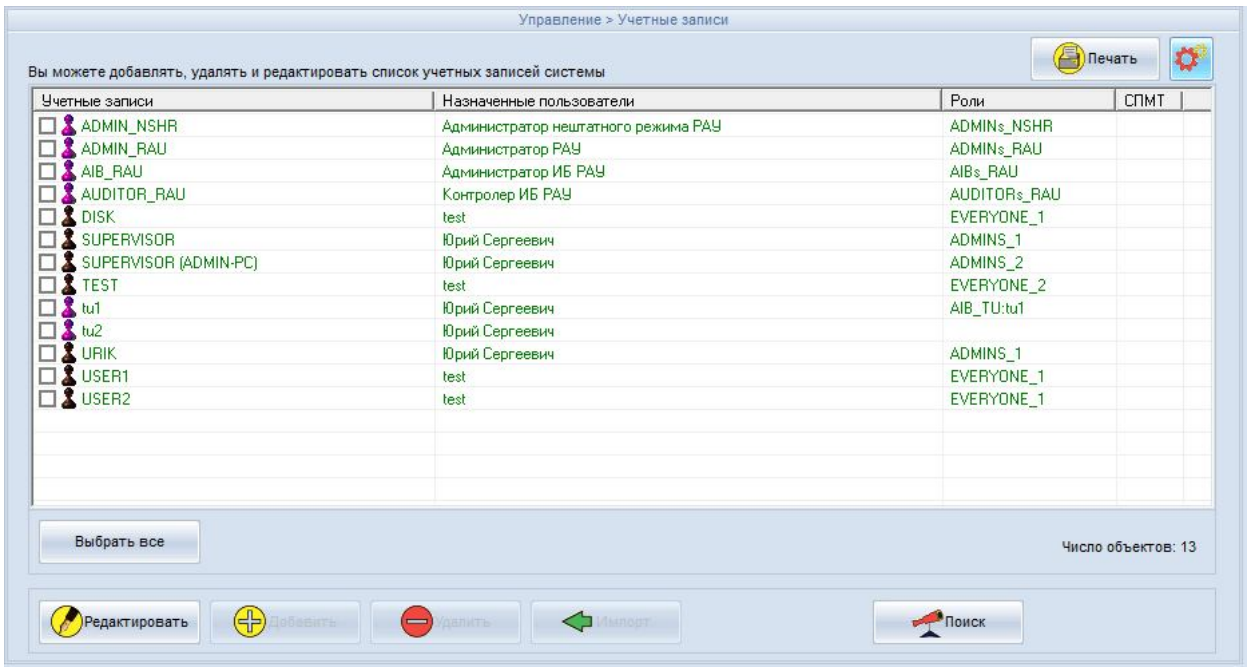

Рисунок 64 - Учётные записи

Для отображения в списке учётных записей информации о наличии списков файлов контроля целостности, списков задач и стартовых задачах следует в окне, приведенном на рисунке 64, нажать кнопку <Настройка отображения информации>. При ее нажатии появляется окно, приведённое на рисунке 31, в котором устанавливаются флаги напротив той информации, которую нужно отображать. После добавления отображаемой информации в таблице учётных записей появляется столбец под названием «ПКО». Наличие литеры «К» в данном столбце означает, что для данной учётной записи определён список файлов для контроля целостности, наличие литеры «З» – определён список задач, литеры «С» – определён список стартовых задач, литеры «У» – ПКО, на котором зарегистрирован данный пользователь, управляется от СВМиКД.

Кнопка <Печать> позволяет распечатать выбранную информацию на принтере, а также сохранить в файл (с указанным разделителем). При ее нажатии появляется окно, приведённое на рисунке 65, в котором нужно выбрать способ печати: в файл или на принтер, тип выводимой информации (учётные записи, назначенные пользователи, роли); при печати в файл следует также указать разделитель.

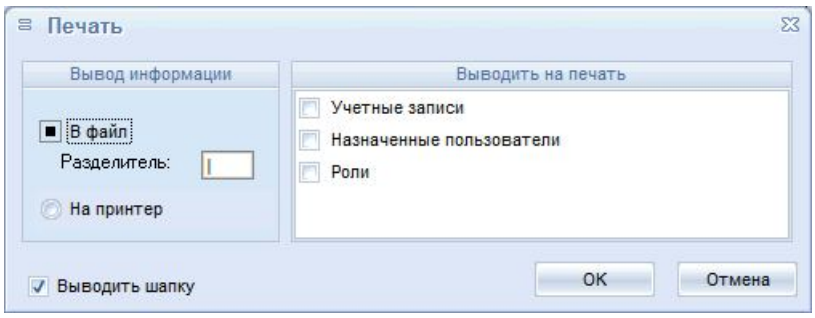

Рисунок 65 - Печать информации об учетных записях

Если необходимо определить, какой учётной записи принадлежит некоторый идентификатор, следует нажать кнопку <Поиск> на вкладке «Учётные записи». Появится сообщение «Предъявите идентификатор», приведённое на рисунке 66.

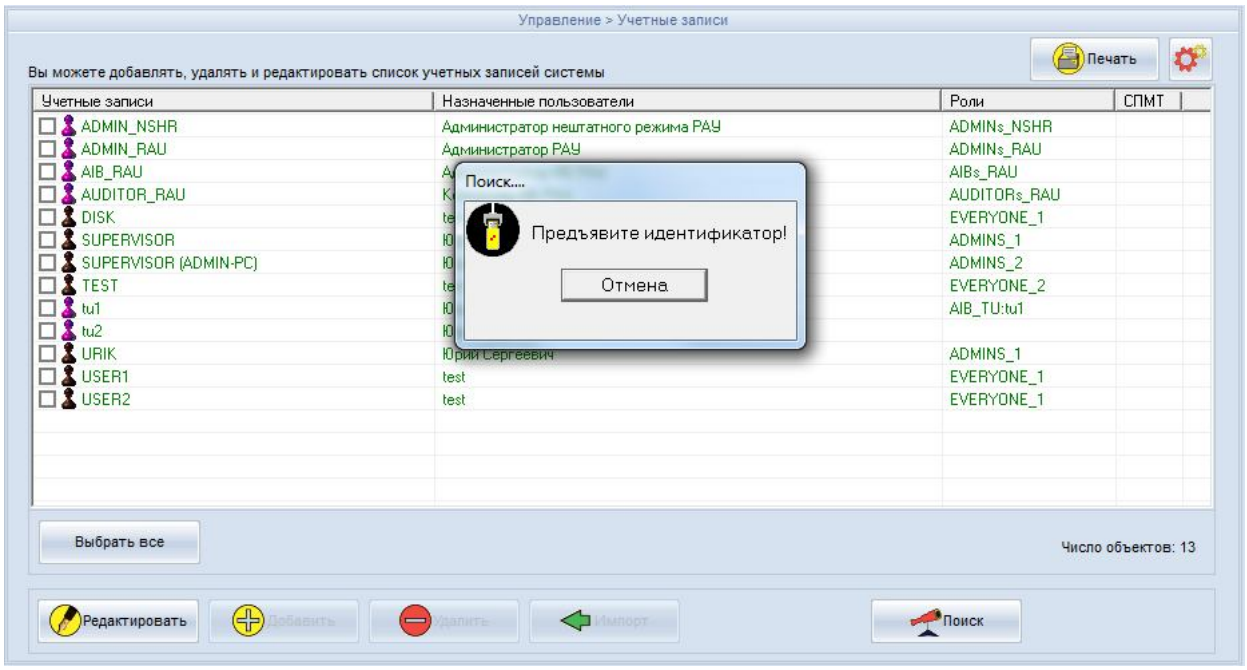

Рисунок 66 - Окно с сообщением «Предъявите идентификатор»

Если предъявленный идентификатор назначен какой-либо учётной записи, то эта учетная запись будет выделена, как показано на рисунке 67.

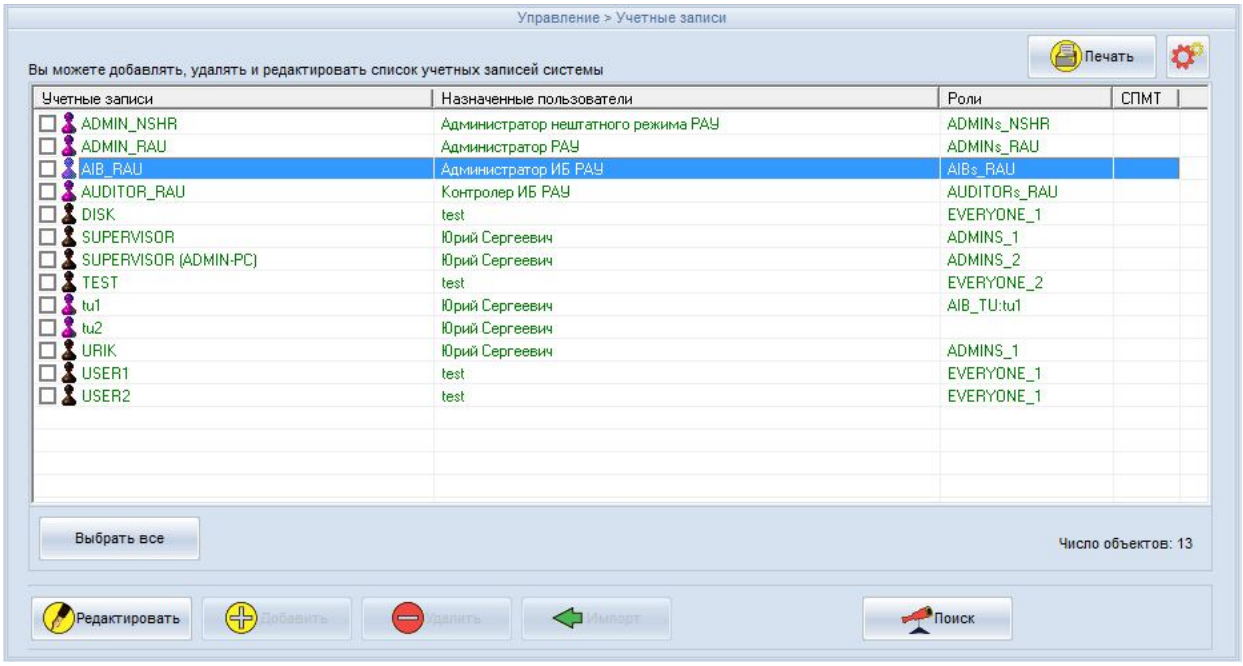

Рисунок 67 - Учетная запись, которой назначен идентификатор

Если предъявленный идентификатор не назначен никакой учётной записи, то в нижней части окна появится сообщение «Идентификатор не зарегистрирован!», как показано на рисунке 68.

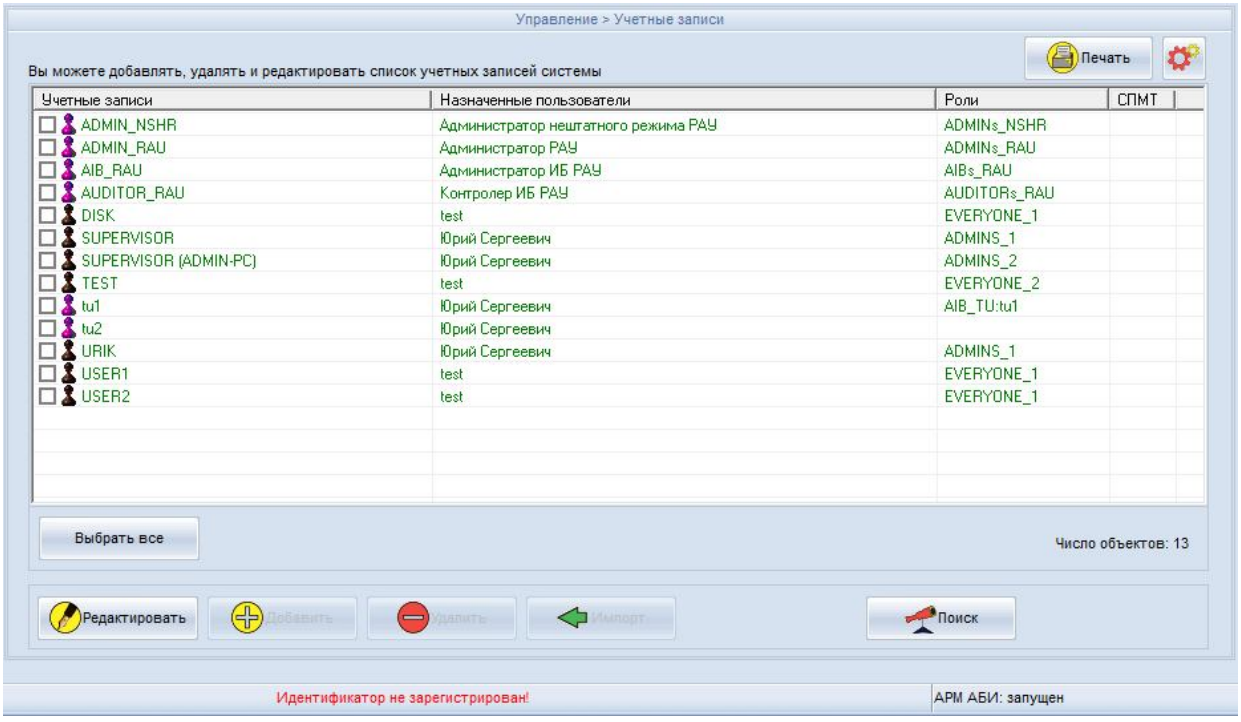

Рисунок 68 - Сообщение о том, что идентификатор не зарегистрирован

Нажатие кнопки <Редактировать> выводит окно, приведённое на рисунке 69.

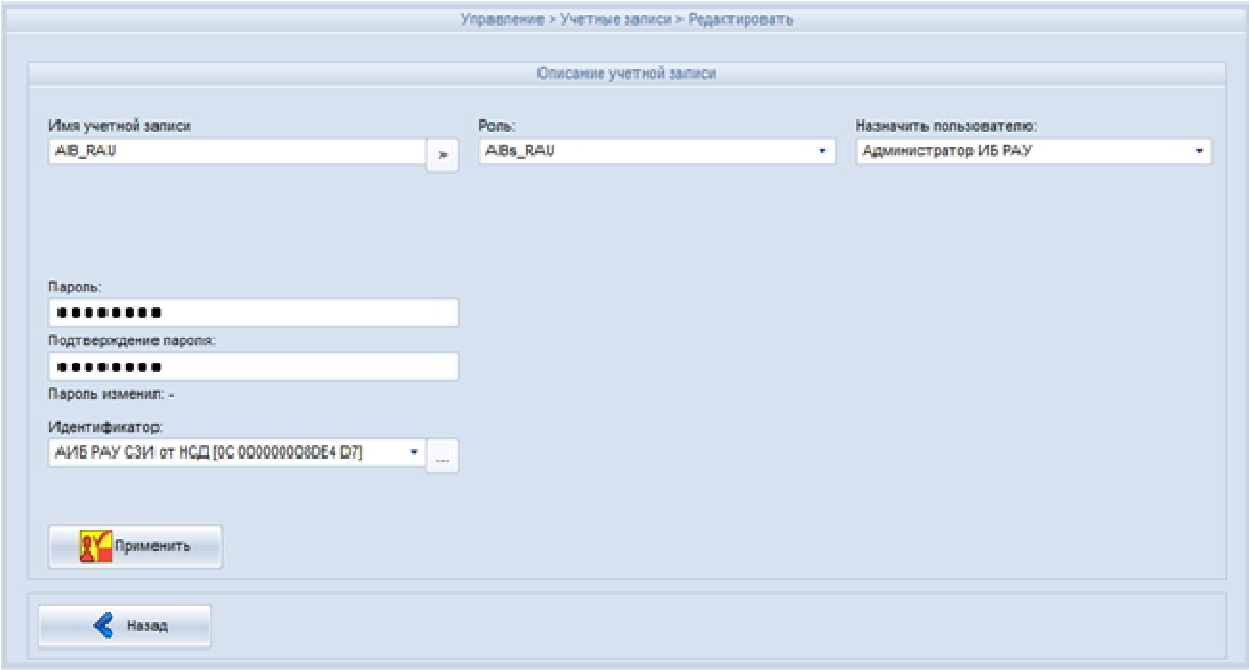

Рисунок 69 - Просмотр параметров учётной записи

Администратор может просматривать параметры учётной записи, но изменять их он не может.

4.9 Настройки сервера централизованного управления

4.9.1 Общие сведения

Администратор РАУ осуществляет настройку основных параметров ПО СЦУ.

Для сохранения сделанных настроек необходимо нажать кнопку <Применить>.

ПО СЦУ предоставляет возможность экспорта настроек в файл с именем ASM.CFG и последующего их импорта из файла.

Для экспорта настроек следует во вкладке Настройка > Основные настройки, приведённой на рисунке 70, нажать кнопку <Экспорт>. При ее нажатии будет выведено стандартное диалоговое окно выбора папки, в которую будет записан файл ASM.CFG.

Для импорта сохранённых в файле экспорта настроек следует во вкладке Настройка > Основные настройки, приведённой на рисунке 70, нажать кнопку <Импорт>. При ее нажатии будет выведено стандартное диалоговое окно выбора папки. Нужно указать папку, в которой находится файл экспорта ASM.CFG.

4.9.2 Основные настройки

Для настройки СЦУ администратором РАУ необходимо открыть вкладку Настройка > Основные настройки. Будет выведено окно, приведённое на рисунке 70. С помощью данного окна у администратора РАУ имеется возможность:

- задать максимально допустимое число строк в журналах регистрации событий;
- выполнить настройку АРМ АБИ Аккорд.

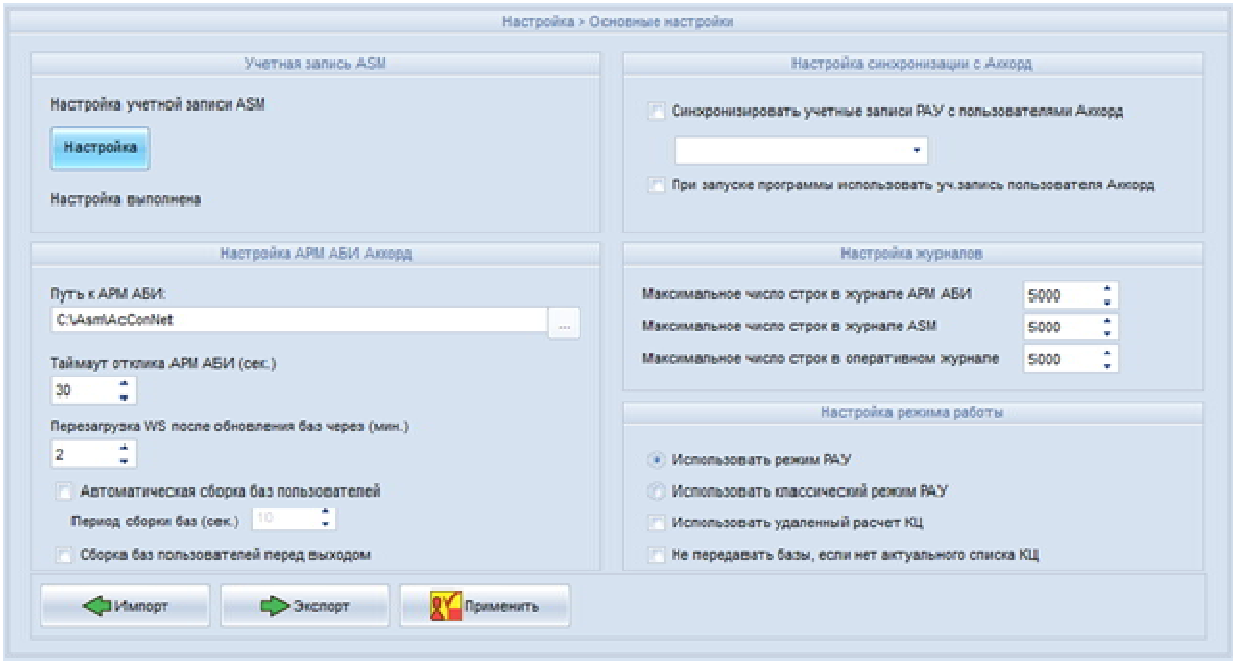

Рисунок 70 – Основные настройки СЦУ

Если установлен флажок «Сборка баз пользователей перед выходом», то для пользователя Администратор ИБ технологического участка выполняется автоматическая проверка базы пользователей с последующей ее передачей (в случае наличия изменений в базе) на ПКО.

Для применения сделанных настроек необходимо нажать кнопку <Применить>.

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

В случае сбоя сохранённые в файле настройки можно восстановить, используя механизм экспорта / импорта.

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

5 Рекомендации по резервному копированию ПО сервера централизованного управления

В случае перевода сервера централизованного управления на другую ОС или физическую платформу для обеспечения возможности восстановления ПО сервера, его баз и настроек рекомендуется выполнить резервное копирование следующих каталогов и файлов:

- файлы настройки и журнал РАУ:
  - C:\Asm\asm.ini;
  - C:\Asm\asm.log;
  - базы РАУ:
  - C:\Asm\Accounts.acc;
  - C:\Asm\Computers.acc;
  - C:\Asm\Frames.acc;
  - C:\Asm\Roles.acc;
  - C:\Asm\Tokens.acc;
  - C:\Asm\USB.acc;
  - C:\Asm\Users.acc;
- каталог шаблонов и ролей: C:\Asm\TEMPLATE\;
- каталог с подкаталогами актуальных баз подконтрольных объектов: C:\Asm\OutBases\;
- файл со списком подконтрольных объектов: C:\Asm\ACCONNET\ACNODE.LST;
- архивная база событий, зарегистрированных на подконтрольных объектах: C:\Asm\ACCONNET\CLIENT.ARC;
- каталог (с подкаталогами) журналов: C:\Asm\ACCONNET\Client.Log\;
- каталоги (с подкаталогами) временных баз подконтрольных объектов:
  - C:\Asm\ACCONNET\IN\;
  - C:\Asm\ACCONNET\OUT\.

Если после перевода СЦУ на другую ОС или физическую платформу планируется использовать тот же самый контроллер «Аккорд-АМДЗ», то также необходимо выполнить резервное копирование файла лицензии C:\Asm\Acconnet\Acconnet.key.

Если планируется использовать другой контроллер, то после перевода СЦУ на другую ОС или физическую платформу необходимо получить новый файл лицензии, для чего отправить письмо на почтовый адрес key@okbsapr.ru, указав серийный номер контроллера и количество планируемых подключений к серверу.

6 Перечень оповещающих сообщений

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

Таблица 2 - Перечень оповещающих сообщений

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

Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
«Доступ не разрешен!» (на красном фоне)	Использован недопустимый идентификатор пользователя или введен неправильный пароль при попытке входа в систему	Повторить попытку процедуры идентификации / аутентификации, если не поможет обратиться к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка)
«Требуется Администратор» (на красном фоне) «Разберитесь с ошибками» (на оранжевом фоне)	Попытка пользователя войти в систему	Несовпадение контрольных и текущих параметров аппаратной и программной частей системы. Необходимо обратиться к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка) для выявления и устранения причины изменения параметров
«Такую комбинацию символов недопустимо использовать в качестве пароля»	Попытка пользователя сменить пароль	Пользователь пытается задать в качестве нового пароля комбинацию символов, которую легко подобрать, например, qwerty. Необходимо ввести более сложную комбинацию символов. Желательно, чтобы пароль содержал цифры, буквы верхнего и нижнего регистра, а его 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 сервер 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 учетной 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 учетной 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 ПО сервера централизованного управления РАУ при первом его запуске не была сразу же выполнена предварительная настройка сетевого идентификатора	Выполнить предварительную настройку сетевого идентификатора и запустить службу AcConNet

7 Файлы конфигурации РАУ

7.1 Файл конфигурации ASM.INI

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

Параметры конфигурационного файла ASM.INI и их описание приведены в таблице 3.

Таблица 3 – Параметры конфигурационного файла ASM.INI

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

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

7.2 Файл конфигурации AcCon32.ini

Файл конфигурации AcCon32.ini содержит настроечные параметры сервера централизованного управления. Данный файл находится в установочном каталоге сервера централизованного управления (по умолчанию C:\ASM). Параметры конфигурационного файла AcCon32.ini и их описание приведены в таблице 4.

Таблица 4 – Параметры конфигурационного файла AcCon32.ini

Параметры конфигурационного файла	Значение параметров конфигурационного файла
[Options]	
Timeout	Таймаут соединения (в секундах)

Параметры конфигурационного файла	Значение параметров конфигурационного файла
TransportLogLevel	Детальность ведения журналов транспорта (0 – Error, 1 – Info, 2 – Debug)
ServiceLogLevel	Детальность ведения журналов сервиса (0 – Error, 1 – Info, 2 – Debug)
RetryCount	Количество попыток переподключения к RabbitMQ при старте (0 – бесконечно)
RetryInterval	Интервал попыток переподключения к RabbitMQ при старте (в секундах)
FileChunkSize	Максимальный размер данных, передаваемых за одну итерацию, в МБ. Если данный параметр отсутствует в конфигурационном файле, то максимальный размер принимается равным 64 МБ
[RabbitMQ]	
Port	Номер порта для подключения к RabbitMQ серверу. Данный номер должен совпадать с номером порта, указанным в параметре tcp_listeners конфигурационного файла rabbitmq.config, описанного в подразделе 7.4. На сервере централизованного управления порт с данным номером должен быть открыт на входящие подключения. По умолчанию для подключения к RabbitMQ серверу используется порт 28997
HeartbeatTimeout	Таймаут отправки сигналов для проверки соединения с RabbitMQ (в секундах)
ReconnectInterval	Интервал, после которого осуществляется попытка восстановить соединение с RabbitMQ (в секундах)
ConnectionTimeout	Таймаут попыток соединения при восстановлении связи с RabbitMQ (в миллисекундах)

7.3 Файл конфигурации AcWs32.ini

Файл конфигурации AcWs32.ini находится на ПКО и содержит его настроечные параметры. Параметры конфигурационного файла AcWs32.ini и их описание приведены в таблице 5.

Таблица 5 - Параметры конфигурационного файла AcWs32.ini

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

Параметры конфигурационного файла	Значение параметров конфигурационного файла
[RabbitMQ]	
Port	Номер порта для подключения к RabbitMQ серверу. Данный номер должен совпадать с номером порта, указанным в параметре tcp_listeners конфигурационного файла rabbitmq.config, описанного в подразделе 7.4. На ПКО порт с данным номером должен быть открыт на входящие подключения. По умолчанию для подключения к RabbitMQ серверу используется порт 28997
HeartbeatTimeout	Таймаут отправки сигналов для проверки соединения с RabbitMQ (в секундах)
ReconnectInterval	Интервал, после которого осуществляется попытка восстановить соединение с RabbitMQ (в секундах)
ConnectionTimeout	Таймаут попыток соединения при восстановлении связи с RabbitMQ (в миллисекундах)

7.4 Файл конфигурации rabbitmq.config

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

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

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

При необходимости изменить базовую директорию RabbitMQ следует выполнить следующие действия:

1. Через оснастку Службы (Services) остановить службу RabbitMQ и использующие его службы РАУ, если они используются.
2. Удалить RabbitMQ Server.

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

8 Перечень принятых сокращений

АИБ	Администратор информационной безопасности
АС	Автоматизированная система
ИБ	Информационная безопасность
ИС	Информационная система
КТС	Комплекс технических средств
НСД	Несанкционированный доступ
НШР	Нештатный режим
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
РФ	Российская Федерация
РАУ	Распределенный Аудит и Управление
СВТ	Средства вычислительной техники
СЗИ	Средство защиты информации
СУ	Система управления
ASM	Accord Security Management

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

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

СОГЛАСОВАНО

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