УТВЕРЖДЕН
11443195.4012-053 90 2012 ЛУ

СИСТЕМА УДАЛЁННОГО ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ СЗИ ОТ НСД АККОРД

Руководство Администратора

Листов 85

Москва

2020

АННОТАЦИЯ

Система удаленного централизованного управления средствами защиты информации от несанкционированного доступа «Аккорд» (далее – Система, СУЦУ) предназначена для централизованного мониторинга событий ИБ и управления средствами защиты информации от несанкционированного доступа «Аккорд».

Данный документ описывает действия Администратора СУЦУ, связанные с непосредственной эксплуатацией подсистемы в штатном режиме функционирования.

СОДЕРЖАНИЕ

1 Введение

1.1 Область применения

Деятельность Администратора СУЦУ.

1.2 Функции Администратора СУЦУ

Администратор СУЦУ:

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

1.3 Комплект поставки

В комплект поставки СУЦУ 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 СУЦУ СЗИ от НСД на touch memory (далее – TM) типа DS 1996;
- комплект рабочей документации на компакт диске (далее – CD).

2 Назначение и условия применения

2.1 Назначение

СУЦУ обеспечивает:

- централизованный сбор и хранение информации о зарегистрированных событиях доступа к подконтрольным объектам;
- возможность централизованного управления 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

СУЦУ включает сервер централизованного управления и подконтрольные объекты (клиенты СУЦУ).

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 данном 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 данном 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;
- ПАК СЗИ от НСД «Аккорд-Win64» версии 5.0.9.45 или новее.

Для корректной совместной работы ПАК СЗИ от НСД «Аккорд-Win64» 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 СУЦУ

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

На данных компьютерах должно быть установлено следующее программное обеспечение:

- 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).

- ПАК СЗИ от НСД «Аккорд-Win32» версии 4.0.9.45 или новее, или ПАК СЗИ от НСД «Аккорд-Win64» версии 5.0.9.45 или новее в зависимости от разрядности установленной операционной системы.

Для корректной совместной работы ПАК СЗИ от НСД «Аккорд-Win32» и антивирусного ПО, установленного на ПКО, 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 ПАК СЗИ от НСД «Аккорд-Win64» и антивирусного ПО, установленного на ПКО, 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 корректной работы 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 Системы

Установка и настройка Системы выполняется в следующей последовательности:

- установка комплекса «Аккорд-АМДЗ» (в случае отсутствия). Комплекс «Аккорд-АМДЗ» должен быть установлен на сервере централизованного управления (СЦУ) и на всех подконтрольных объектах (ПКО). Установка комплекса выполняется в соответствии с документом 11443195.4012-006 98 03 «Комплекс средств защиты информации от НСД для ПЭВМ (PC) «Аккорд–АМДЗ» (Аппаратный модуль доверенной загрузки) Руководство по установке». В обязанности Администратора Системы входит установка комплекса «Аккорд-АМДЗ» только на СЦУ. Установка комплекса на ПКО не входит в обязанности Администратора СУЦУ;

- установка ПАК СЗИ от НСД «Аккорд-Win32» или ПАК СЗИ от НСД «Аккорд-Win64» (в случае отсутствия). ПАК СЗИ от НСД должны быть установлены на СЦУ и на всех ПКО. На ПКО рекомендуется устанавливать ПО ПАК СЗИ от НСД «Аккорд-Win32» версии 4.0.9.45 и выше, или ПО ПАК СЗИ от НСД «Аккорд-Win64» версии 5.0.9.45 и выше. Установка ПАК СЗИ от НСД «Аккорд-Win32» выполняется в соответствии с документом 11443195.4012-036 98 «Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-Win32» (версия 4.0). Руководство по установке», установка ПАК СЗИ от НСД «Аккорд-Win64» – в соответствии с документом 11443195.4012-037 98 «Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «АККОРД-Win64» (версия 5.0). Руководство по установке». В обязанности Администратора СУЦУ входит установка ПАК СЗИ от НСД только на сервере подконтрольных объектов. Установка ПАК СЗИ от НСД на подконтрольных объектах не входит в обязанности Администратора СУЦУ;

Примечания:

1 Версия ПО ПАК СЗИ от НСД «Аккорд-Win32» / «Аккорд-Win64» определяется по полю «Версия файла» в свойствах файла «AcRun.sys», находящегося в установочном каталоге ПО.

2 Для обеспечения функционирования в автономном режиме ПО клиентов СУЦУ на подконтрольных объектах с ПО ПАК СЗИ от НСД «Аккорд-Win32» версии ниже 4.0.9.45 и ПО ПАК СЗИ от НСД «Аккорд-Win64» версии ниже 5.0.9.45 необходимо заменить файл UsrToAz.dll в каталоге установки ПО ПАК СЗИ от НСД «Аккорд». Для получения нового файла UsrToAz.dll нужно обратиться в службу технической поддержки ОКБ САПР.

- установка ПО сервера централизованного управления. Установка ПО сервера централизованного управления описана в подразделе 3.2;

- получение файла лицензии на использование СУЦУ. Процедура получения файла лицензии на использование СУЦУ описана в подразделе 3.3;

- установка ПО клиентов СУЦУ на подконтрольные объекты. Данная процедура должна выполняться для каждого подконтрольного объекта. Установка клиентов СУЦУ описана в подразделе 3.4;

- настройка правил разграничения доступа для клиентов СУЦУ. Данная процедура описана в подразделе 3.5;

- создание сетевого идентификатора сервера СУЦУ. Данная процедура описана в подразделе 3.6;

- создание в сетевом идентификаторе учетной записи «ASM_ACCOUNT». Данная процедура описана в подразделе 3.7;

- регистрация подконтрольных объектов. Данная процедура описана в подразделе 3.8.

3.2 Установка ПО сервера централизованного управления

Установка ПО сервера централизованного управления осуществляется следующим образом:

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

- на сервере централизованного управления выполнить находящийся на дистрибутивном носителе командный файл RMQ-prepare.bat, который создаёт в папке %APPDATA% сервера централизованного управления папку RabbitMQ и копирует в неё конфигурационный файл rabbitmq.config;

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

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

- на сервере централизованного управления запустить с установочного диска СУЦУ программу SUCU-SERVER-A.B.C.D.exe[1)], где A, B, C и D – десятичные числа, например, SUCU-SERVER-3.0.0.230.exe. Данное приложение представляет собой мастер установки ПО сервера централизованного управления. Следуя указаниям мастера, установить ПО на СЦУ;

- открыть на сервере централизованного управления и на всех промежуточных сетевых устройствах между сервером централизованного управления и ПКО порт на входящие подключения сервера RabbitMQ. Номер данного порта прописан в параметре Port конфигурационного файла AcCon32.ini, расположенного на сервере централизованного управления, 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 СУЦУ СЗИ от НСД (регистрация администратора НШР, создание сетевого идентификатора, создание сетевой учетной записи);

- запустить сервис Acconnet.exe.

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

[1)] Если на сервере централизованного управления не установлена программа Microsoft.NET Framework или установлена версия ниже 4.0, то при установке ПО SUCU-SERVER-A.B.C.D.exe автоматически выполняется установка .NET Framework 4.0

При установке серверной части на сервер под управлением Windows 2012R2 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 СУЦУ

Работа программы невозможна без файла лицензии.

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

- продукт: Аккорд-СУЦУ;
- 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 сервера централизованного управления (по умолчанию C:\Asm\ACCONNET) под именем «Acconnet.key» и продолжить настройку комплекса.

3.4 Установка ПО клиентов СУЦУ

Перед установкой ПО клиентов СУЦУ необходимо:

- провести установку Microsoft .NET Framework 4.0 или выше (если он не установлен).
- открыть на данной рабочей станции и на всех промежуточных сетевых устройствах между данной рабочей станцией сервером централизованного управления 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 СУЦУ. 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.

Установка ПО клиентов СУЦУ осуществляется следующим образом.

Запустить с установочного диска СУЦУ программу SUCU-CLIENT-A.B.C.D.exe[1)], где A, B, C и D – десятичные числа, например, SUCU-CLIENT-3.0.0.230.exe. После запуска программы на экране появляется первое окно работы мастера установки ПО клиента СУЦУ, приведённое на рисунке 1.

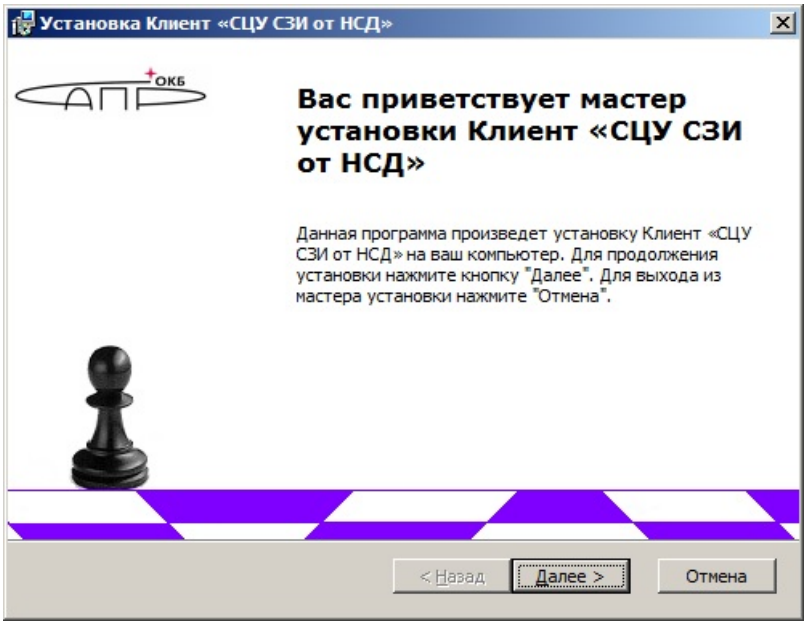

Рисунок 1 - Начало работы мастера установки Клиента СУЦУ

После нажатия кнопки <Далее> на экране появляется окно с лицензионным соглашением, приведённое на рисунке 2. Необходимо отметить пункт «Я принимаю условия лицензионного соглашения» и нажать кнопку <Далее>.

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

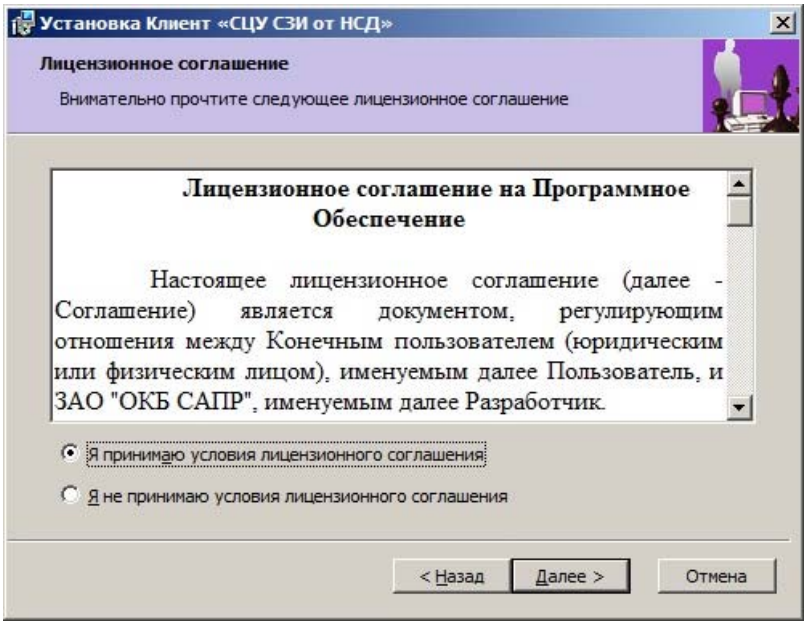

Рисунок 2 - Лицензионное соглашение на установку Клиента СУЦУ

После нажатия кнопки <Далее> на экране появляется окно выбора директории установки ПО клиента СУЦУ, приведённое на рисунке 3.

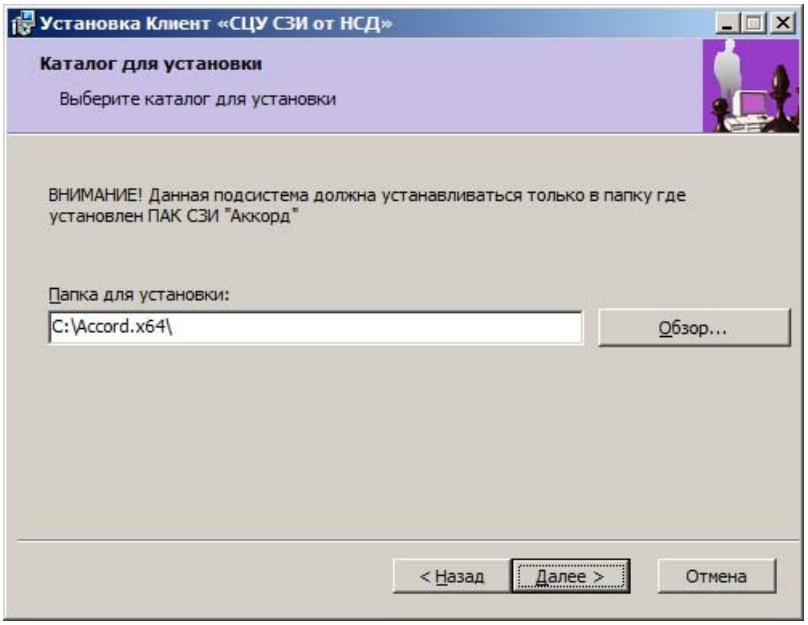

Рисунок 3 - Выбор директории установки Клиента СУЦУ

В этом окне следует выбрать папку для установки и нажать кнопку <Далее>.

После этого на экране появляется окно завершения работы мастера установки ПО клиента СУЦУ, приведённое на рисунке 4.

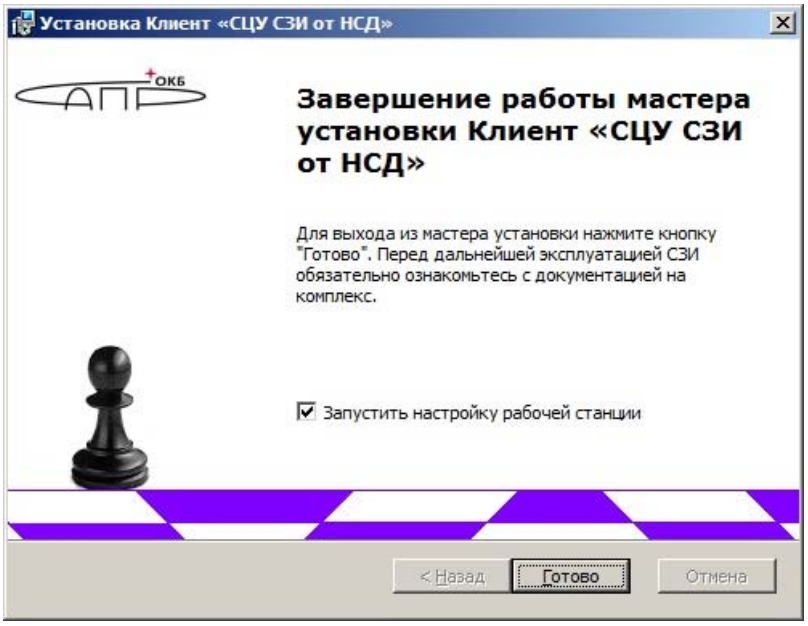

Рисунок 4 - Завершение работы мастера установки Клиента СУЦУ

Для настройки ПО клиента СУЦУ следует установить флажок «Запустить настройку рабочей станции» и нажать кнопку <Готово>. На экран будет выведено окно, приведённое на рисунке 5.

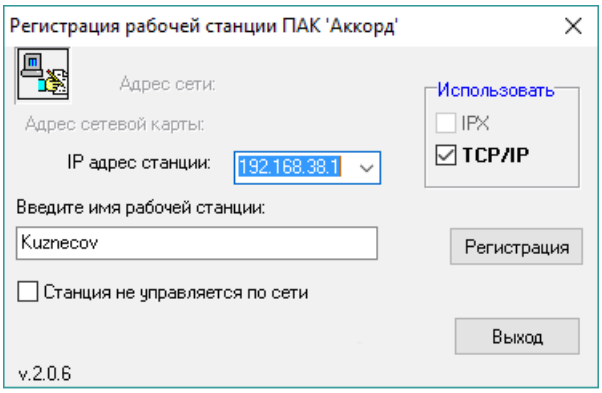

Рисунок 5 – Регистрация рабочей станции

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) программно-аппаратного комплекса средств защиты информации от несанкционированного доступа «Аккорд-Win32» / «Аккорд-Win64» на подконтрольном объекте. Порядок установки опций настройки описан в документах 11443195.4012-036 97 «Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-Win32» (версия 4.0). Установка правил разграничения доступа. Программа ACED32» или

11443195.4012-037 97 «Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-Win64» (версия 5.0). Установка правил разграничения доступа. Программа ACED32».

По выполнении процедуры регистрации рабочей станции (по нажатии кнопки <Выход> в окне 5) на экране 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 СУЦУ СЗИ от НСД, приведённом на рисунке 4, не устанавливать флаг «Запустить настройку рабочей станции», то по нажатии кнопки <Готово> на экране также появится оповещение о необходимости перезагрузки рабочей станции.

3.5 Настройка правил разграничения доступа для клиентов СУЦУ

На подконтрольном объекте импортировать в режиме объединения правила разграничения доступа из файла «acws32.prd», находящегося в каталоге установки программно-аппаратного комплекса средств защиты информации от несанкционированного доступа «Аккорд-Win32» / «Аккорд-Win64». Процедура импорта правил разграничения доступа описана в документах 11443195.4012-036 97 «Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-Win32» (версия 4.0). Установка правил разграничения доступа. Программа ACED32» или 11443195.4012-037 97 «Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-Win64» (версия 5.0). Установка правил разграничения доступа. Программа ACED32».

На подконтрольном объекте 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 документах 11443195.4012-036 97 «Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-Win32» (версия 4.0). Установка правил разграничения доступа. Программа ACED32» или 11443195.4012-037 97 «Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-Win64» (версия 5.0). Установка правил разграничения доступа. Программа ACED32».

3.6 Создание сетевого идентификатора сервера централизованного управления

Сетевой идентификатор позволяет выполнить процедуру взаимной аутентификации сервера централизованного управления 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:

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

Для создания сетевого идентификатора необходимо запустить программу регистрации станций «ACSETCON.EXE» на сервере централизованного управления и нажать кнопку <Создать идентификатор>. На экран будет выведено окно, приведённое на рисунке 6.

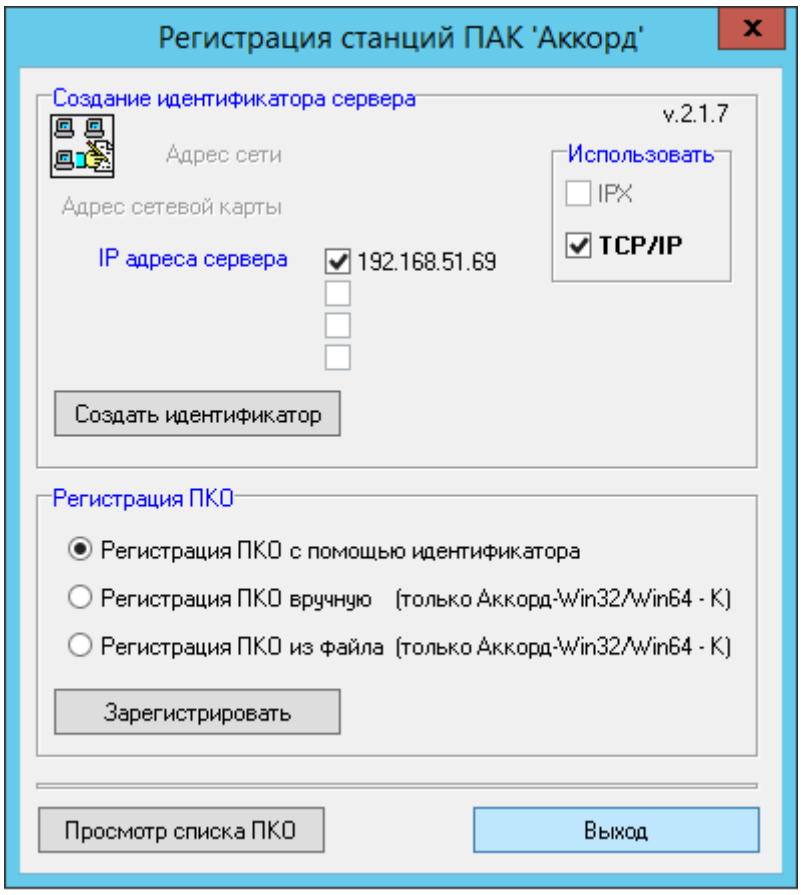

Рисунок 6 - Программа регистрации станций на сервере централизованного управления

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 сервера централизованного управления (по умолчанию C:\Asm\ACCONNET) создается файл ACNODE.LST, содержащий данные о сервере централизованного управления.

После завершения процедуры создания идентификатора сервера централизованного управления на экране появляется сообщение, приведённое на рисунке 7 и становятся доступными элементы управления области «Регистрация ПКО».

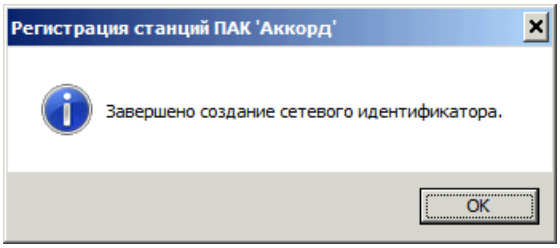

Рисунок 7 - Сообщение об успешном завершении процедуры создания сетевого идентификатора

В окне программы регистрации станций, приведённом на рисунке 6, нужно нажать кнопку <Выход>.

В результате выполнения процедуры создания сетевого идентификатора сервера централизованного управления 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 СУЦУ согласно документу 11443195.425710.002.91 «Система удалённого централизованного управления. 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. При выполнении данного способа обмен аутентификационными данными между сервером централизованного управления и ПКО осуществляется путём передачи этих данных на сетевом идентификаторе сервера централизованного управления;

- регистрация вручную. При выполнении данного способа информация о ПКО вводится вручную, а обмен аутентификационными данными между сервером централизованного управления и ПКО осуществляется путём передачи этих данных по сети;

- регистрация из файла. При выполнении данного способа информация о ПКО считывается из файла, а обмен аутентификационными данными между сер-

вером централизованного управления и ПКО осуществляется путём передачи этих данных по сети.

Независимо от способа регистрации перед её выполнением необходимо создать сетевой идентификатор сервера централизованного управления (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 8;

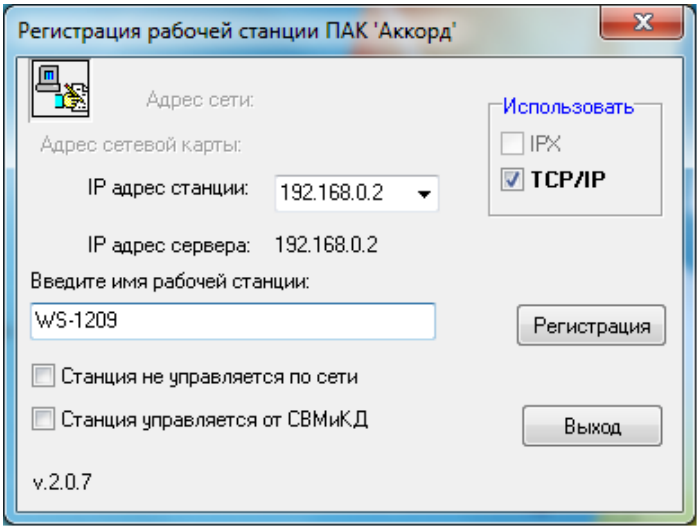

Рисунок 8 - Регистрация рабочей станции

в) в данном окне необходимо задать:

- имя станции. Под данным именем ПКО будет идентифицироваться на сервере централизованного управления. 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 9.

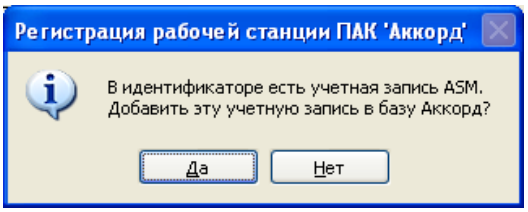

Рисунок 9 - Предложение добавить учетную запись ASM в базу «Аккорд»

Примечание. Если данное сообщение не будет выведено на экран, то это означает, что-либо не был создан сетевой идентификатор сервера централизованного управления и в нём не была создана учётная запись «ASM_ACCOUNT» (смотри подразделы 3.6 и 3.7). 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 СУЦУ, создаётся файл «ACNODE.LST», содержащий данные о рабочей станции. На экран выводится сообщение об успешном добавлении учётной записи «ASM_ACCOUNT», приведённое на рисунке 10.

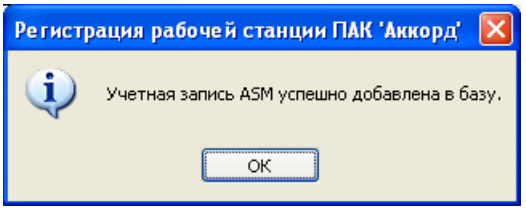

Рисунок 10 – Сообщение об успешном добавлении учетной записи «ASM_ACCOUNT» в базу ПАК СЗИ от НСД «Аккорд»

Следует нажать кнопку <Да> и предъявить сетевой идентификатор;

е) на экран выводится сообщение об успешном завершении процедуры регистрации рабочей станции, приведённое на рисунке 11.

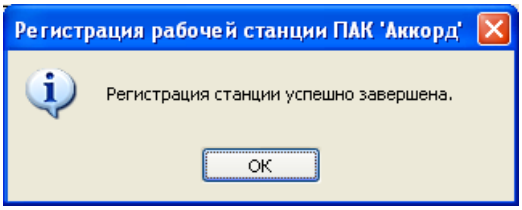

Рисунок 11 - Сообщение об успешном выполнении процедуры регистрации станции

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 сервере централизованного управления. После сохранения списка зарегистрированных ПКО сервере централизованного управления 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 ключей станций нужно вернуться на сервер централизованного управления и в главном окне программы регистрации станций «ACSETCON.EXE», приведённом на рисунке 12, 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 6, то это означает, что перед регистрацией ПКО не была проведена процедура создания сетевого идентификатора сервера централизованного управления. 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 сервере централизованного управления.

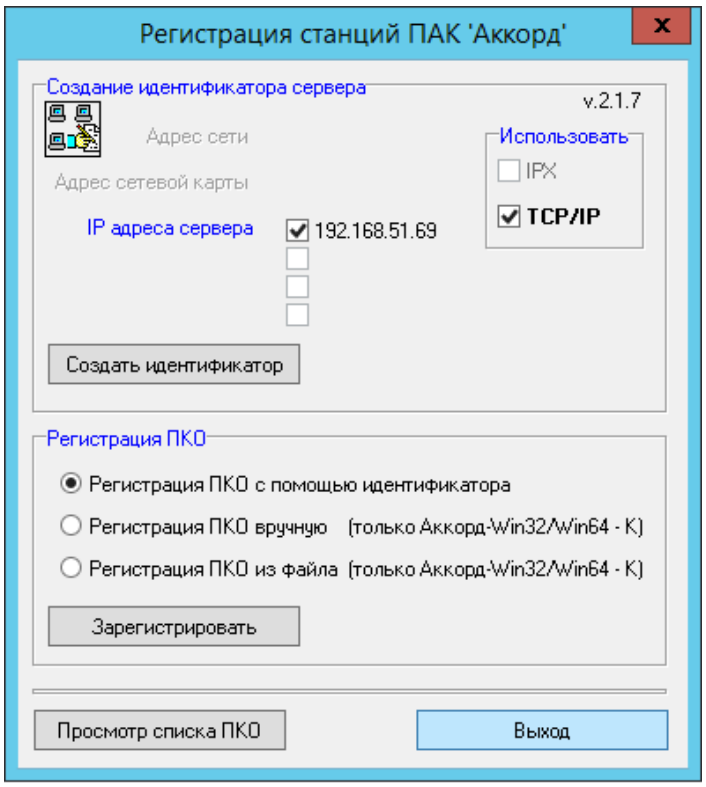

Рисунок 12 – Регистрация ПКО с помощью идентификатора

После завершения процедуры добавления информации о ПКО на сервере централизованного управления на экране появляется сообщение, приведённое на рисунке 13.

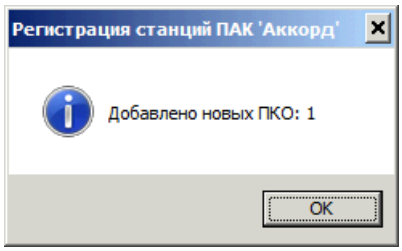

Рисунок 13 – Сообщение о добавлении информации на сервере централизованного управления

Для завершения процедуры регистрации необходимо перезагрузить ПКО и СЦУ.

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

1 На сервере централизованного управления переместить файл acnode.lst из C:\Asm\ACCONNET в какой-нибудь 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 6, в качестве IP-адреса сервера централизованного управления указать IP-адрес устройства NAT для отдельной подсети.

3 На сервере централизованного управления 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 сервере централизованного управления 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 сервере централизованного управления остановить службу Acconnet.

7 На сервере централизованного управления перезапустить RabbitMQ.

8 На сервере централизованного управления запустить службу Acconnet.

9 На зарегистрированных ПКО перезапустиь службу acws32nt.

3.8.3 Регистрация вручную

При регистрации ПКО вручную необходимо на сервере централизованного управления запустить программу регистрации станций «ACSETCON.EXE». На экран будет выведено окно, приведённое на рисунке 12. В этом окне нужно установить переключатель «Регистрация ПКО» в положение «Регистрация ПКО вручную (только Аккорд-Win32/Win64 K)» и нажать кнопку <Зарегистрировать>.

Примечание. Если элементы управления области «Регистрация ПКО» неактивны, как показано на рисунке 6, то это означает, что перед регистрацией ПКО не была проведена процедура создания сетевого идентификатора сервера централизованного управления. В этом случае необходимо создать сетевой идентификатор (смотри подраздел 3.6).

После этого на экран будет выведено окно, приведённое на рисунке 14.

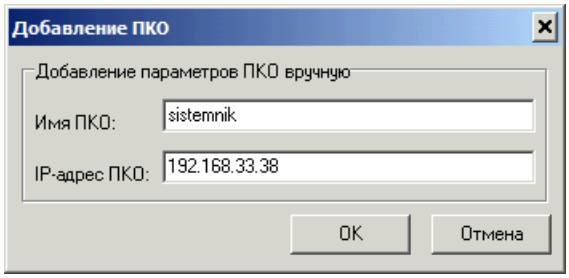

Рисунок 14 – Добавление ПКО вручную

В этом окне нужно ввести имя и IP-адрес ПКО и нажать кнопку <OK>. Информация о ПКО сохраняется на сервере централизованного управления в файле «AcNode.lst».

После добавления информации о ПКО на сервер централизованного управления на экране появляется сообщение, приведённое на рисунке 13.

Если во время выполнения данной процедуры между ПКО и сервером централизованного управления отсутствовало сетевое соединение, то на экране появляется сообщение, приведённое на рисунке 15, а в файле «AcNode.lst» IP-адресу данного ПКО присваивается значение 127.0.0.1.

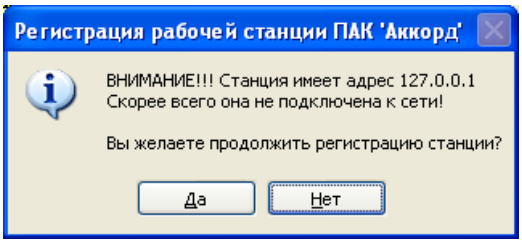

Рисунок 15 - Сообщение, возникающее при регистрации станций с IP-адресом 127.0.0.1

При появлении сообщения, приведённого на рисунке 15, необходимо нажать кнопку <Нет>, восстановить сетевое соединение между сервером централизованного управления 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 сервером централизованного управления ПКО автоматически подключаются к серверу централизованного управления. 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 сервера централизованного управления.

Такие ПКО следует удалить и заново провести процедуру регистрации, убедившись, что между ПКО и сервером централизованного управления 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 регистрируе-

мых 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 сервере централизованного управления запустить программу регистрации станций «ACSETCON.EXE». На экран будет выведено окно, приведённое на рисунке 12. В этом окне нужно установить переключатель «Регистрация ПКО» в положение «Регистрация ПКО из файла (только Аккорд-Win32/Win64 K)» и нажать кнопку <Зарегистрировать>.

Примечание. Если элементы управления области «Регистрация ПКО» неактивны, как показано на рисунке 6, то это означает, что перед регистрацией ПКО не была проведена процедура создания сетевого идентификатора сервера централизованного управления. В этом случае необходимо создать сетевой идентификатор (смотри подраздел 3.6).

После этого на экран будет выведено окно открытия файла, приведённое на рисунке 16.

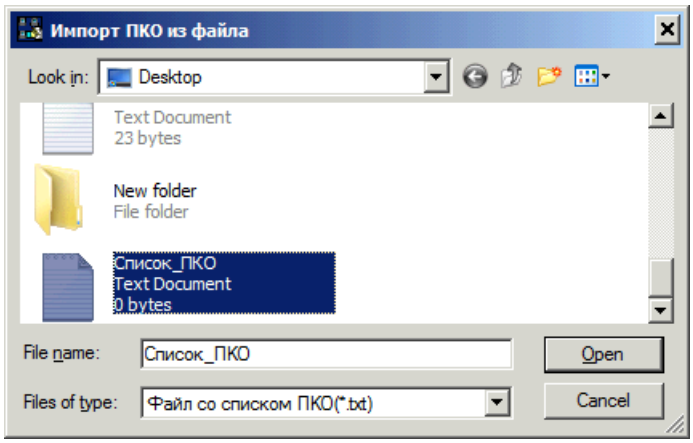

Рисунок 16 – Импорт параметров ПКО из файла

В данном окне нужно выбрать файл с параметрами регистрируемых ПКО и нажать кнопку <Открыть>. После нажатия данной кнопки будет выполнена процедура регистрации.

По завершении процедуры регистрации ПКО на экране появляется сообщение, приведённое на рисунке 13.

3.8.5 Изменение списка зарегистрированных ПКО

На сервере централизованного управления запустить утилиту «AcSetCon.exe» «Пуск» → «Программы» → «ASM» → «Настройка сети». На экране появится окно регистрации ПКО, приведенное на рисунке 12.

В данном окне нажать кнопку <Просмотр списка ПКО>. На экран будет выведено окно редактирования списка зарегистрированных ПКО, приведенное на рисунке 17.

Данное окно позволяет:

- просматривать список зарегистрированных ПКО;
- изменять сетевую карту, обеспечивающую взаимодействие выбранного ПКО с сервером централизованного управления;
- изменять протокол сетевого взаимодействия между выбранным ПКО и сервером централизованного управления;
- изменять параметры протокола сетевого взаимодействия;
- удалить компьютер из списка зарегистрированных ПКО.

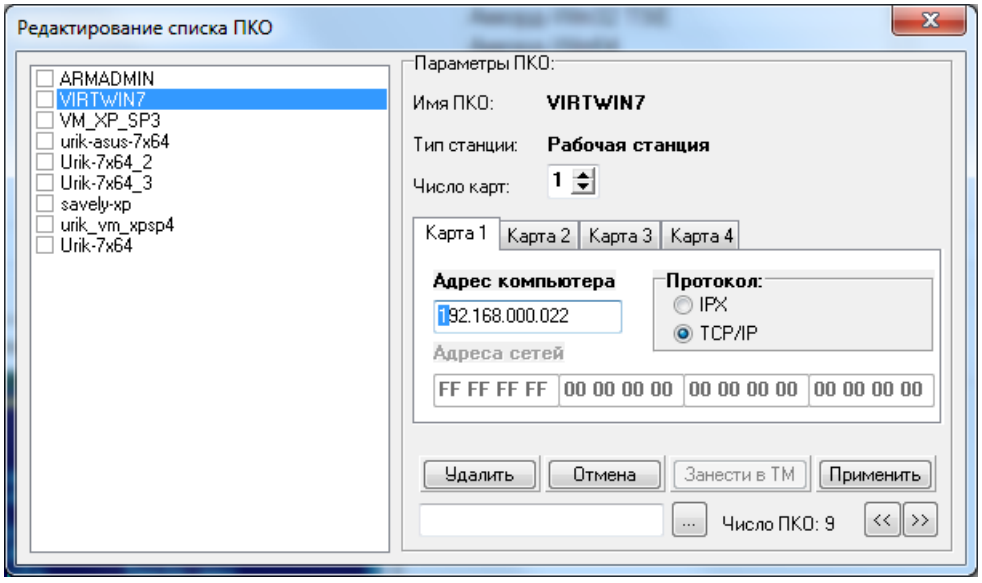

Рисунок 17 - Окно редактирования списка ПКО

3.9 Установка обновлений ПО СУЦУ

3.9.1 Обновление ПО сервера централизованного управления

Порядок обновления ПО СУЦУ (сервера централизованного управления и клиента СУЦУ) следующий:

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

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

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

4) удалить предыдущую версию ПО СУЦУ;

5) запустить обновленное ПО СУЦУ: программу SUCU-SERVER-A.B.C.D.exe на сервере централизованного управления или SUCU-CLIENT-A.B.C.D.exe, на ПКО (A, B, C и D – десятичные числа);

6) перезагрузить компьютер после завершения работы программы установки обновления.

3.9.2 Обновление ПО клиентов СУЦУ СЗИ от НСД

Выполнять обновление ПО клиентов СУЦУ СЗИ от НСД следует каждый раз после обновления ПО сервера централизованного управления.

Обновление установленного на подконтрольные объекты программного обеспечения клиентов СУЦУ СЗИ от НСД осуществляется удалённо с сервера централизованного управления при помощи приложения «UpdateManager.exe». Данное приложение находится в папке, в которую установлено ПО сервера централизованного управления (по умолчанию C:\ASM).

После запуска данной утилиты на экран выводится окно, приведённое на рисунке 18.

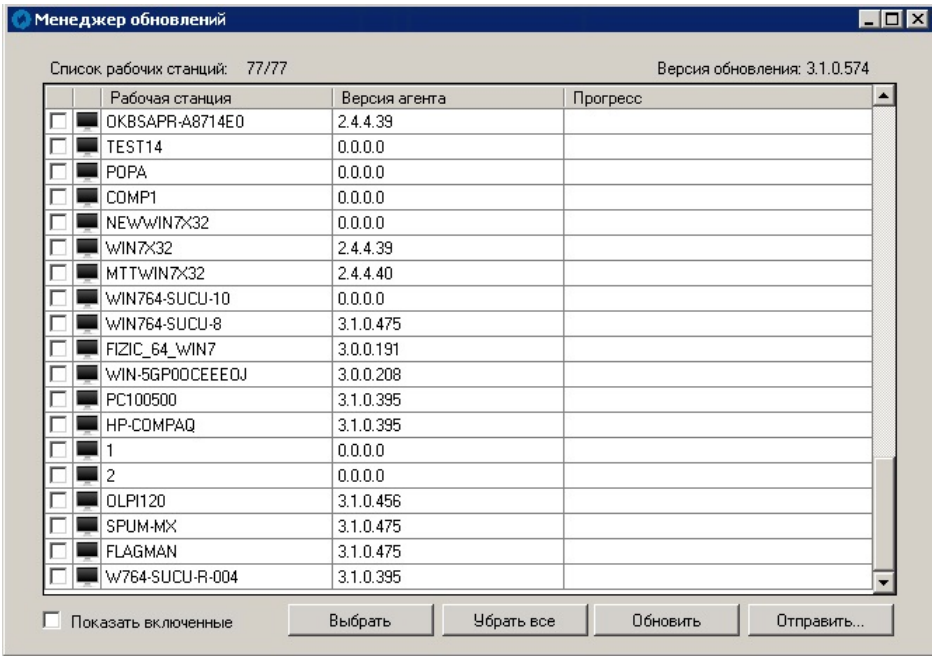

Рисунок 18 – Менеджер обновлений

Данное окно содержит список зарегистрированных на сервере централизованного управления подконтрольных объектов с указанием в столбце «версия агента» версии клиентского ПО СУЦУ СЗИ от НСД. 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 СУЦУ СЗИ от НСД 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 клиентского ПО СУЦУ СЗИ от НСД на нём будет выполнено сразу после его включения и загрузки. После завершения обновления ПО клиентов СУЦУ СЗИ от НСД на всех выбранных ПКО на экран будет выведено сообщение о завершении обновления, приведённое на рисунке 19. В столбец «Прогресс» будет записана информация о результатах выполнения обновления ПО клиентов СУЦУ СЗИ от НСД на ПКО.

Примечания:

1 Новые версии файлов обновления ПО клиентов СУЦУ СЗИ от НСД копируются на сервер централизованного управления при выполнении процедуры обновления ПО сервера централизованного управления. Данные файлы находятся в папке C:\Asm\ACCONNET\Client.Upd\.

2 Помимо удалённого централизованного обновления ПО клиентов СУЦУ СЗИ от НСД на ПКО приложение «UpdateManager.exe» обеспечивает передачу файлов на выбранные ПКО.

Для передачи файлов с помощью данного приложения нужно в окне, приведённом на рисунке 18 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 СУЦУ СЗИ от НСД на ПКО.

После передачи на экран 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.

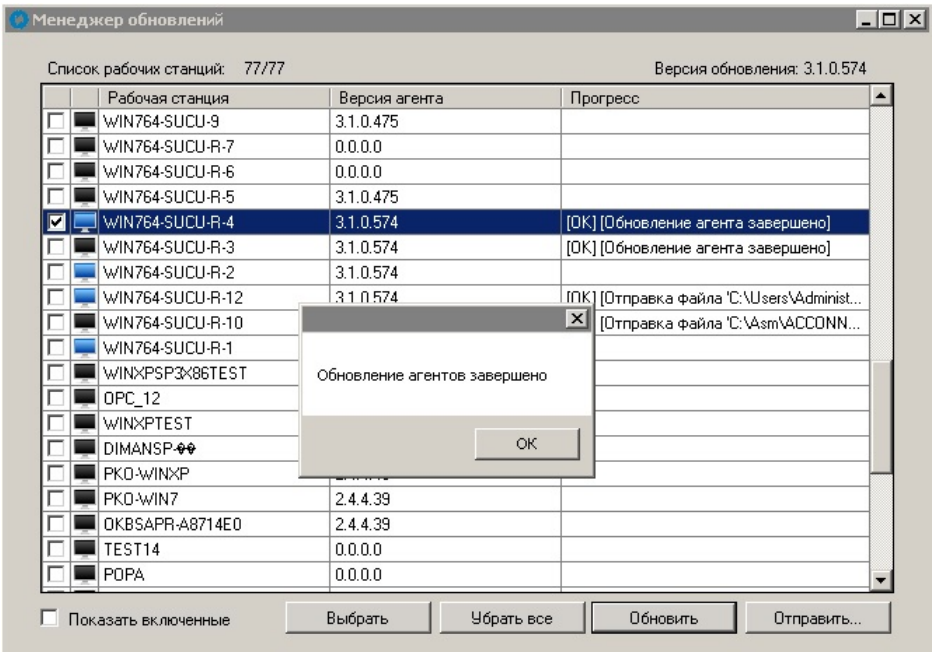

Рисунок 19 - Менеджер обновлений. Завершение обновления ПО клиентов СУЦУ

4 Работа с сервером централизованного управления

4.1 Общие принципы управления

Пользовательский интерфейс ПО сервера централизованного управления подчиняется следующим правилам:

- кнопка <Добавить> предназначены для добавления той или иной сущности;
- кнопка <Удалить> предназначены 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 сервера централизованного управления, доступный администратору для выполнения его обязанностей.

4.2 Вкладка «Пользователи системы»

4.2.1 Общие сведения

Внешний вид вкладки «Пользователи системы» приведён на рисунке 20.

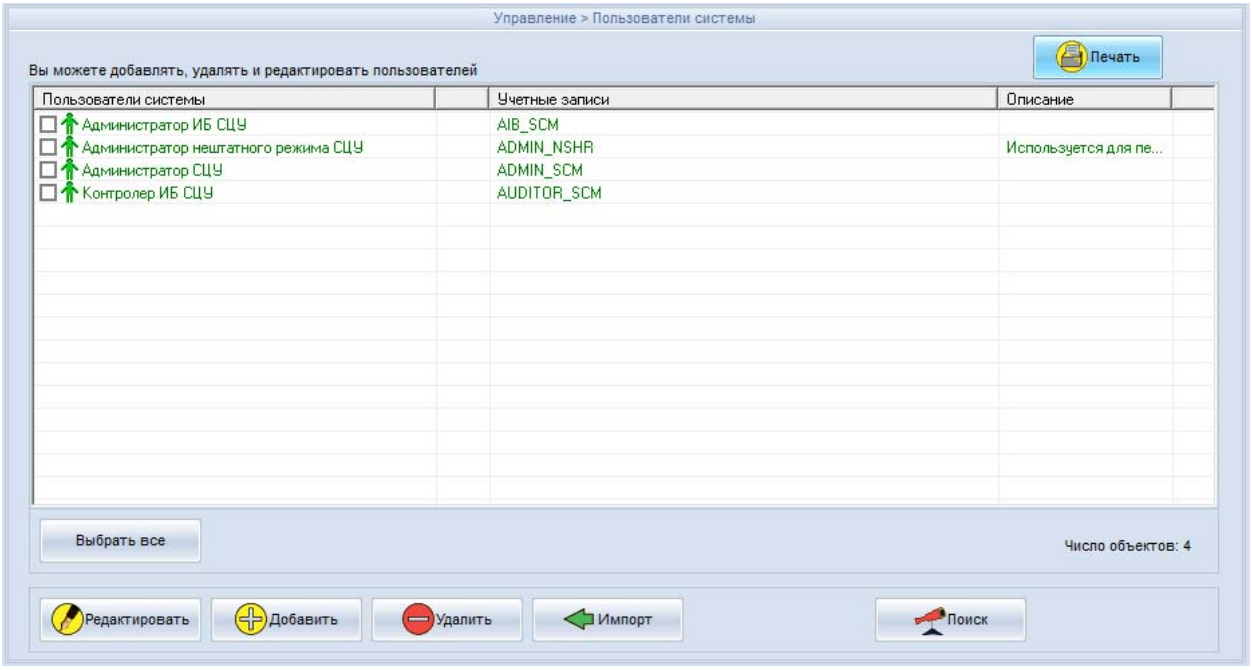

Рисунок 20 - Вкладка «Пользователи системы»

Используя элементы управления данной вкладки, Администратор СУЦУ СЗИ от НСД может выполнять следующие функции:

- добавлять новых пользователей в систему. Данная функция описана в пункте 4.2.2;
- импортировать в систему пользователей из ПАК СЗИ от НСД «Аккорд-Win32», ПАК СЗИ от НСД «Аккорд-Win64» и пользователей из ОС Windows. Данная функция описана в пункте 4.2.3;
- изменять параметры пользователей системы. Данная функция описана в пункте 4.2.4;
- удалять пользователей системы. Данная функция описана в пункте 4.2.5;
- осуществлять поиск пользователя по идентификатору. Данная функция описана в пункте 4.2.6;
- выводить на печать выбранную информацию о пользователях. Данная 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 20, нажать кнопку <Добавить>. На экран будет выведено окно, приведённое на рисунке 21.

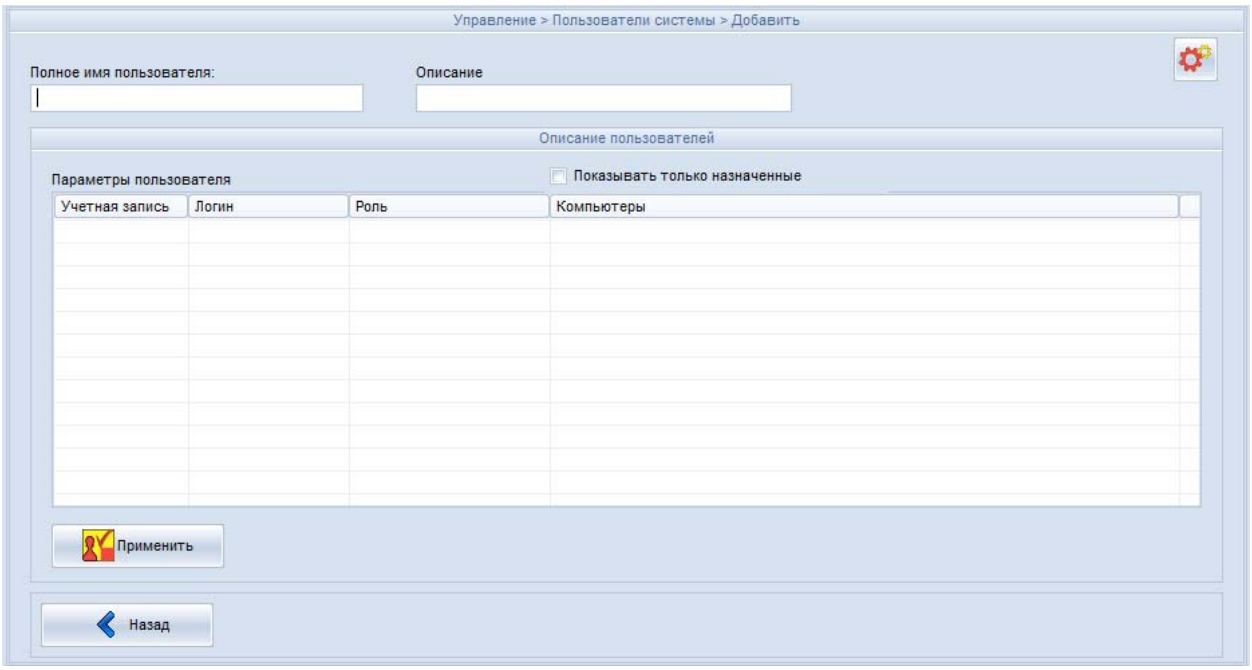

Рисунок 21 - Добавление нового пользователя

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 сервера централизованного управления позволяет импортировать в систему пользователей из ПАК СЗИ от НСД «Аккорд-Win32», ПАК СЗИ от НСД «Аккорд-Win64» и пользователей из ОС Windows. Импортирование в систему пользователей из ПАК СЗИ от НСД «Аккорд-Win32» и ПАК СЗИ от НСД «Аккорд-Win64» 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 ПАК СЗИ от НСД «Аккорд-Win32» и ПАК СЗИ от НСД «Аккорд-Win64»

Данная функция позволяет добавлять в систему пользователей, зарегистрированных в ПАК СЗИ от НСД «Аккорд-Win32» и ПАК СЗИ от НСД «Аккорд-

Win64», установленных на подконтрольных объектах. Подробная информация о пользователях ПАК СЗИ от НСД «Аккорд-Win32» и порядок их регистрации приведены в документе 11443195.4012-036 97 «Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-Win32» (версия 4.0). Установка правил разграничения доступа. Программа ACED32». Подробная информация о пользователях ПАК СЗИ от НСД «Аккорд-Win64» и порядок их регистрации приведены в документе 11443195.4012-037 97 «Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-Win64» (версия 5.0). Установка правил разграничения доступа. Программа ACED32».

Необходимая для выполнения импортирования информация о пользователях ПАК СЗИ от НСД «Аккорд-Win32» и ПАК СЗИ от НСД «Аккорд-Win64» передаётся подконтрольными объектами и хранится на сервере централизованного управления в так называемых базах пользователей – файлах с расширением *.amz. Имена этих файлов совпадают с именами ПКО, от которых они были получены.

Для импортирования в систему пользователей из ПАК СЗИ от НСД «Аккорд-Win32» и ПАК СЗИ от НСД «Аккорд-Win64» следует в окне, приведённом на рисунке 20, нажать кнопку <Импорт>. В появившемся окне импорта пользователей, приведённом на рисунке 21, установить переключатель «Вы можете импортировать пользователей из:» в положение «базы Accord».

Для импортирования пользователей следует в окне импорта пользователей, приведённом на рисунке 21, нажать кнопку <Импортировать>. На экран будет выведено стандартное диалоговое окно открытия файла, в котором Администратору СУЦУ СЗИ от НСД следует выбрать файл с расширением *.amz (базу пользователей), содержащий информацию о пользователях, которых следует импортировать в систему. На сервере централизованного управления файлы с расширением *.amz хранятся в папке C:\Asm\ACCONNET\IN\, имена этих файлов совпадают с именами ПКО, от которых они были получены.

Рисунок 22 - Окно импорта пользователей. Импортирование пользователей из ПАК СЗИ от НСД «Аккорд-Win32» и ПАК СЗИ от НСД «Аккорд-Win64»

После выбора и открытия файла базы пользователей окно импорта пользователей примет вид, приведённый на рисунке 23.

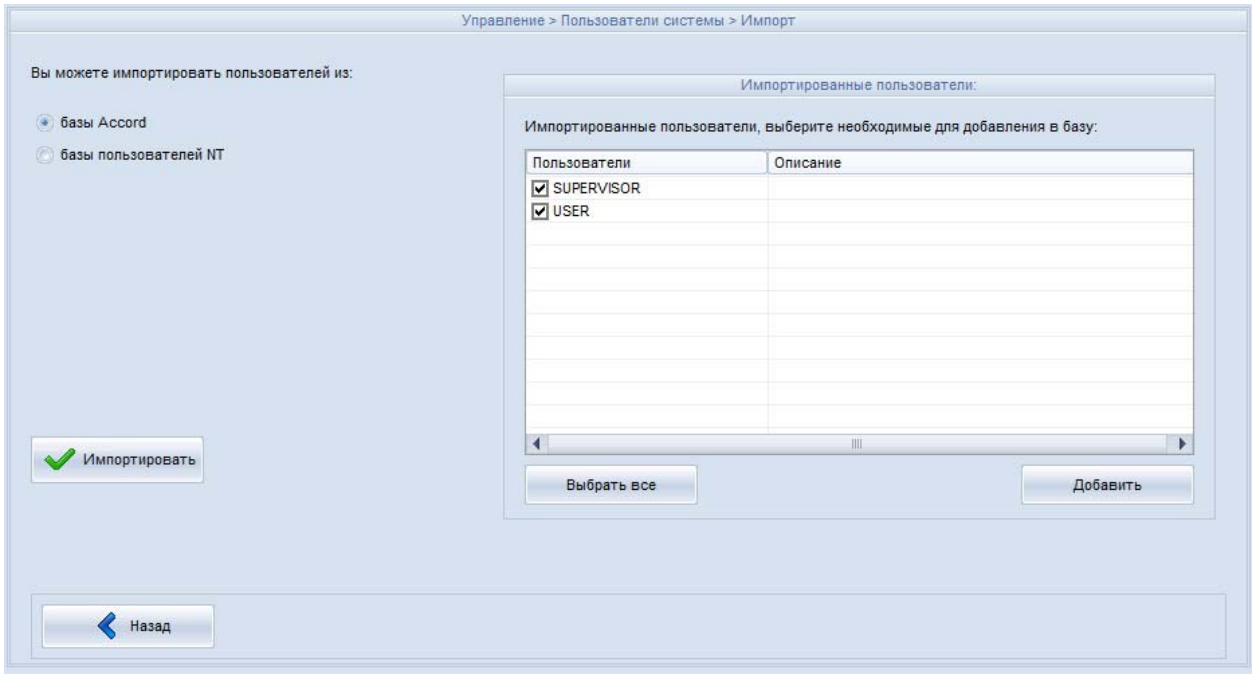

Рисунок 23 - Окно импорта пользователей. Импортирование пользователей из ПАК СЗИ от НСД «Аккорд-Win32» и ПАК СЗИ от НСД «Аккорд-Win64». Выбор пользователей для импорта

В правой части окна импорта пользователей, приведённого на рисунке 23, будет отображаться список пользователей, информация о которых содержится в выбранной базе пользователей. Администратору СУЦУ СЗИ от НСД следует ус-

тановить 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 20, нажать кнопку <Импорт>. В появившемся окне импорта пользователей, приведённом на рисунке 24, установить переключатель «Вы можете импортировать пользователей из:» в положение «базы пользователей NT».

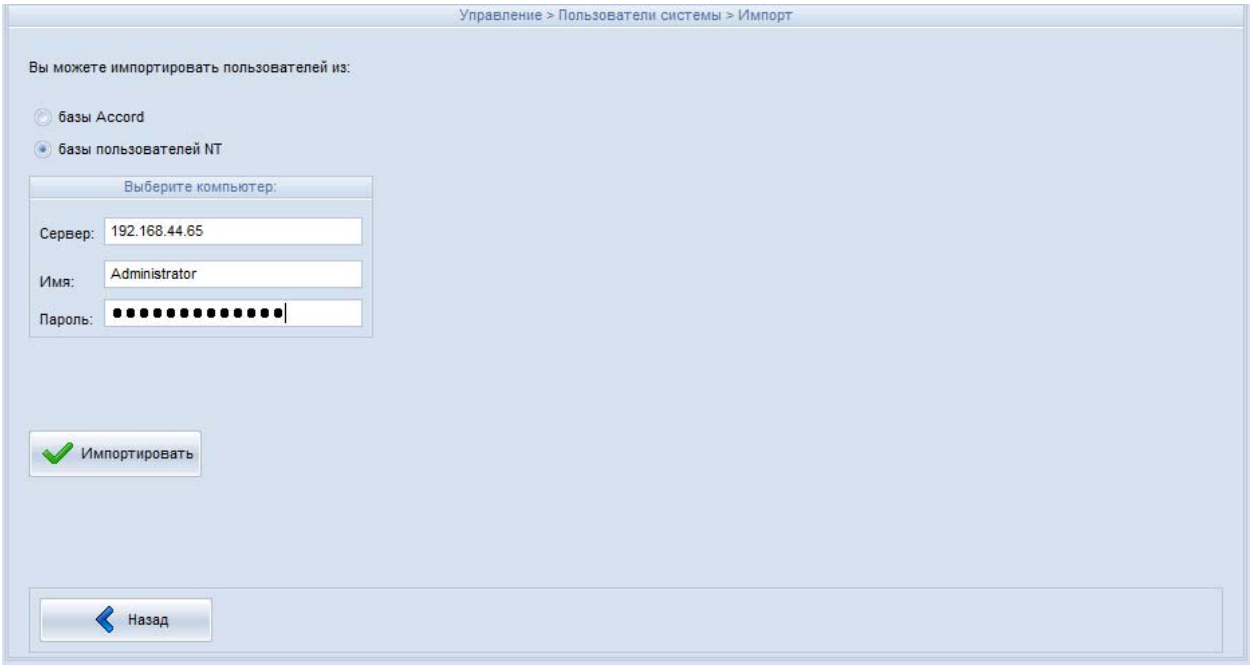

Рисунок 24 - Окно импорта пользователей. Импортирование пользователей ОС Windows

В окне импорта пользователей, приведённом на рисунке 24, 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 25.

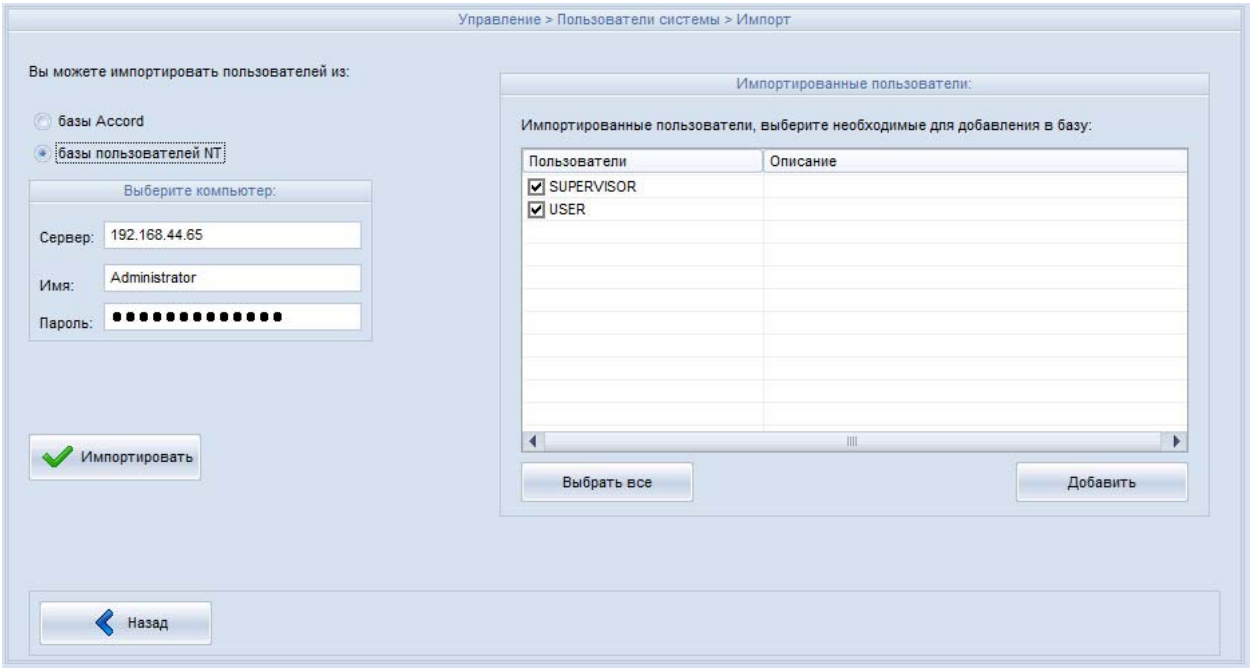

Рисунок 25 - Окно импорта пользователей. Импортирование пользователей ОС Windows. Выбор пользователей для импорта

В правой части окна импорта пользователей, приведённого на рисунке 25, будет отображаться список пользователей ОС выбранного подконтрольного объекта. Администратору СУЦУ СЗИ от НСД 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 20, дважды щелкнуть по записи данного пользователя или, установив флажок напротив данного пользователя, нажать кнопку <Редактировать>. На экран будет выведено окно, приведённое на рисунке 26.

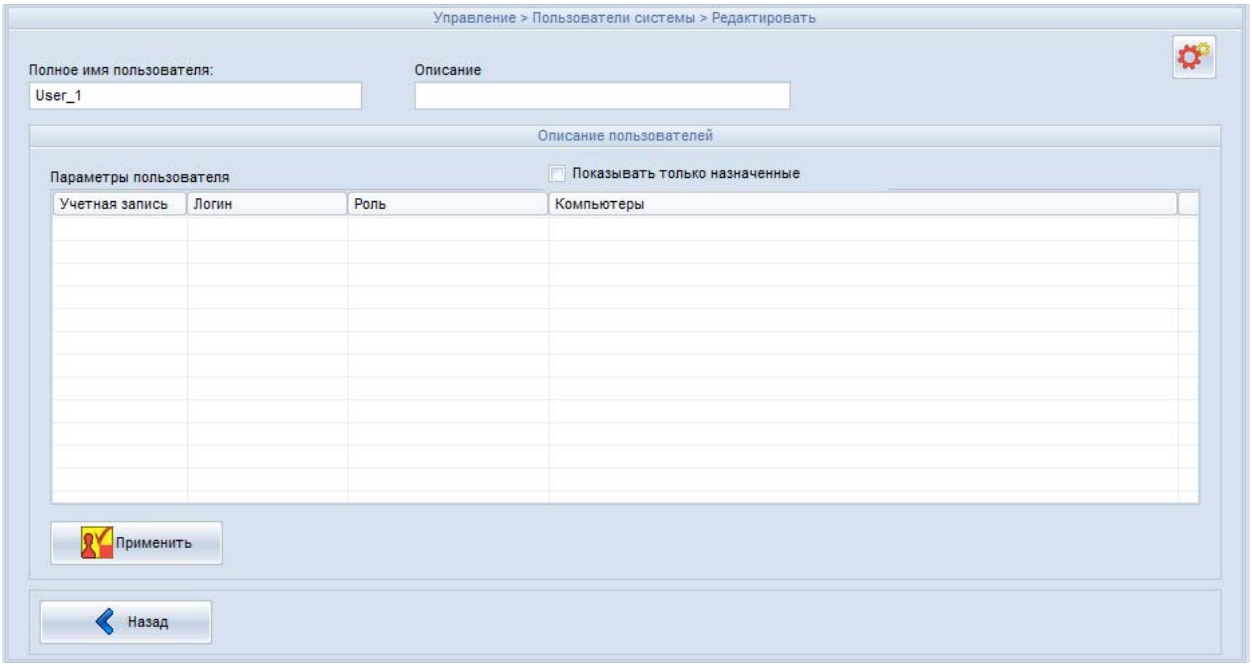

Рисунок 26 - Изменение параметров пользователя

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 26) поля «Учётная запись» или «Роль» пусты, то это означает, что выполнены процедуры удаления учётной записи, которая принадлежала данному пользователю СУЦУ, или удаления роли, назначенной данному пользователю, соответственно (выполняет Администратор ИБ в соответствии с документом «11443195.4012-053 91. Руководство Администратора ИБ СУЦУ СЗИ от НСД»).

Кнопка <Настройка отображения информации> позволяет в окне, приведённом на рисунке 26, 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, управляется ли от СВМиКД ПКО, на котором зарегистрирован данный пользователь. После нажатия на кнопку <Настройка отображения информации> на экран выводится окно, приведённое на рисунке 27. 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 за-

дач, литеры «С» – определен список стартовых задач, У – ПКО, на котором зарегистрирован данный пользователь, управляется от СВМиКД.

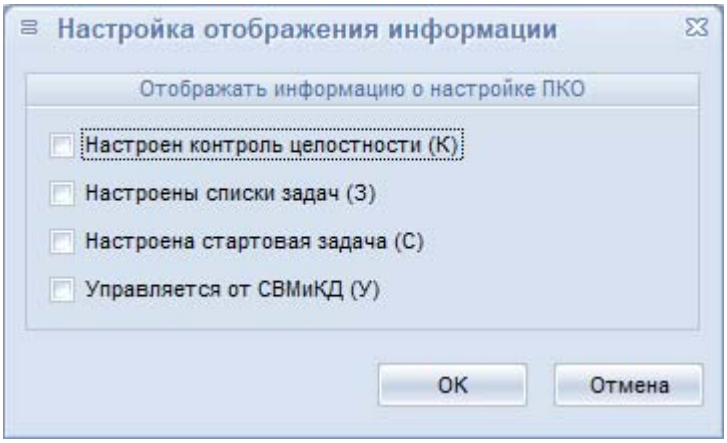

Рисунок 27 – Настройка отображения информации

4.2.5 Удаление пользователя

Данная функция позволяет удалять пользователей системы.

Для удаления пользователей следует в окне, приведённом на рисунке 20, установить флажки напротив пользователей, которых нужно удалить, нажать кнопку <Удалить> и утвердительно ответить на сообщение, запрашивающее подтверждение удаления пользователей.

В ПО СУЦУ СЗИ от НСД при выполнении процедуры удаления пользователя системы предусмотрена возможность автоматического редактирования параметров учётной записи пользователя СУЦУ. По выполнении процедуры удаления пользователя системы в параметрах учётных записей, сопоставленных 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 20, нажать кнопку <Поиск>. На экран будет выведено сообщение «Введите идентификатор!». Администратору СУЦУ СЗИ от НСД следует приложить идентификатор разыскиваемого пользователя к считывателю.

Если приложенный идентификатор назначен какому-либо пользователю системы, то в окне, приведённом на рисунке 20, будет выделена строка, содержащая информацию о данном пользователе.

Если приложенный идентификатор никакому пользователю системы не назначен, то в строке состояния окна, приведённого на рисунке 20, 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 20, установить флажок напротив пользователей, информацию о которых нужно вывести, и нажать кнопку <Печать>. На экран будет выведено окно, приведённое на рисунке 28.

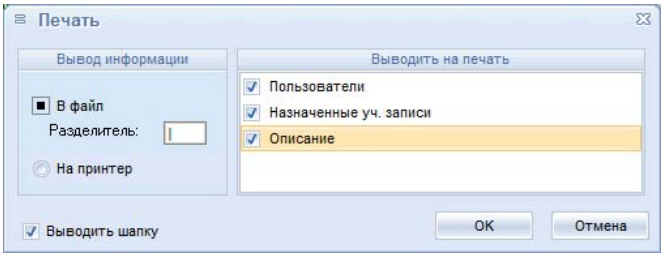

Рисунок 28 - Печать информации о пользователе

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 29.

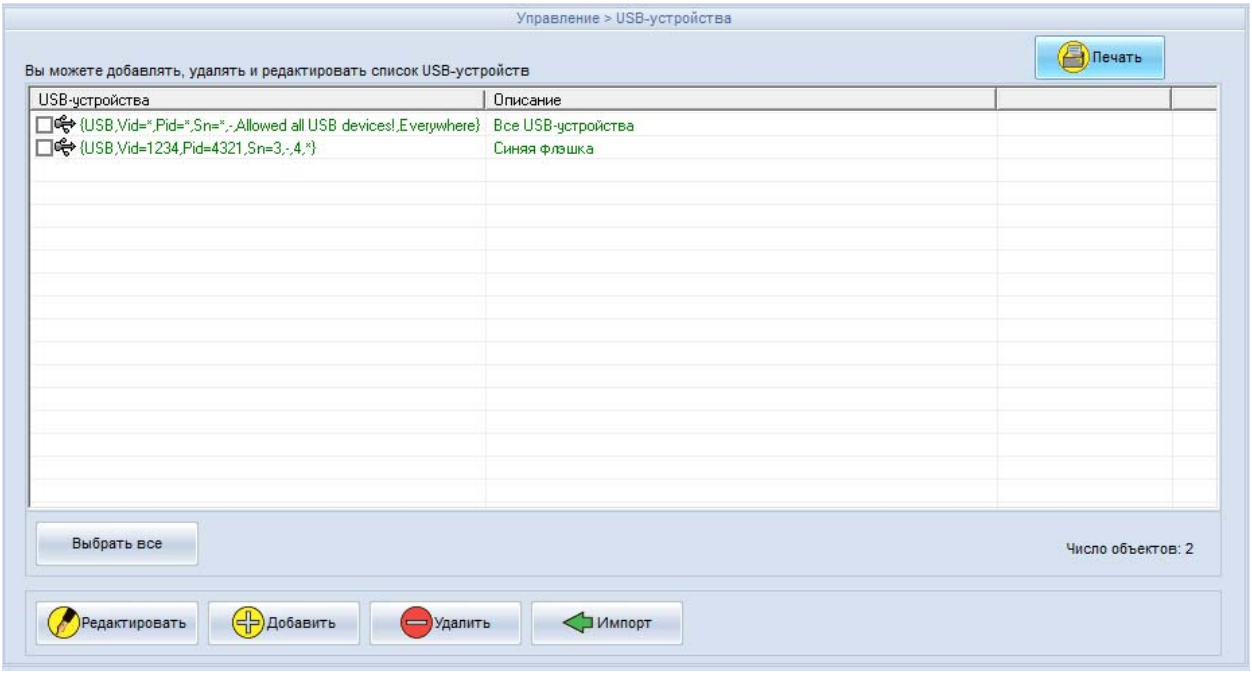

Рисунок 29 - Вкладка «USB-устройства»

Используя элементы управления данной вкладки, Администратор СУЦУ СЗИ от НСД 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 СУЦУ СЗИ от НСД использует следующие функции ПО сервера централизованного управления:

- 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:

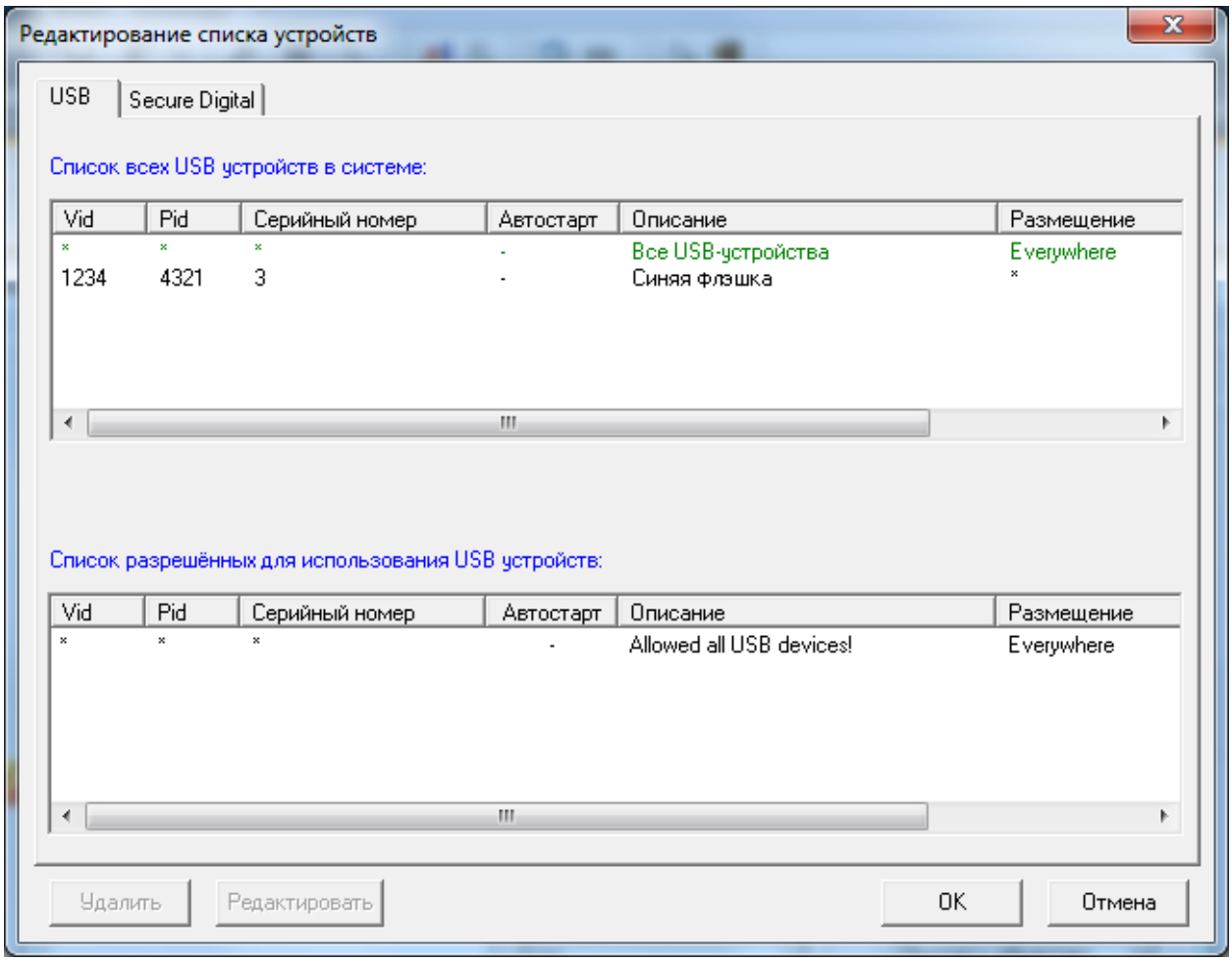

Рисунок 30 - Информация из поля «Описание» во вкладке Управление\USB-устройства совпадает с информацией в графе «Описание» программы ACED32.EXE

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 29, нажать кнопку <Добавить>. На экран будет выведено окно, приведённое на рисунке 31.

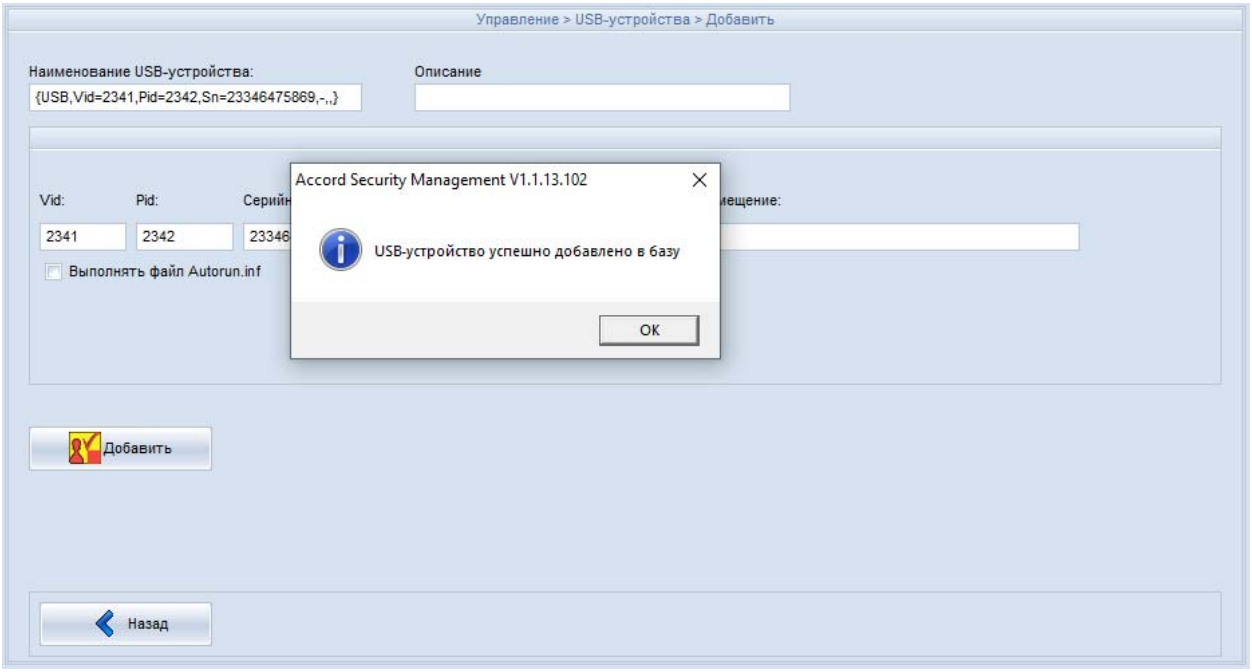

Рисунок 31 - Добавление USB-устройства в список разрешённых USB-устройств системы

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 сервера централизованного управления позволяет импортировать в список разрешённых USB-устройств системы информацию о следующих USB-устройствах:

- USB-устройствах, подключенных к подконтрольным объектам в настоящий момент либо подключаемых к ним когда-нибудь ранее. Импортирование данных USB-устройств описано в подпункте 4.3.3.2;
- USB-устройствах, которые ПАК СЗИ от НСД «Аккорд-Win32» или ПАК СЗИ от НСД «Аккорд-Win64» 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 подконтрольным объектам в настоящий момент либо подключаемых к ним когда-нибудь ранее.

Для выполнения данной операции следует в окне, приведённом на рисунке 29, нажать кнопку <Импорт>. В появившемся окне импорта USB-устройств, приведённом на рисунке 32, установить переключатель «Вы можете импортировать USB-устройства из:» в положение «включенных ПКО».

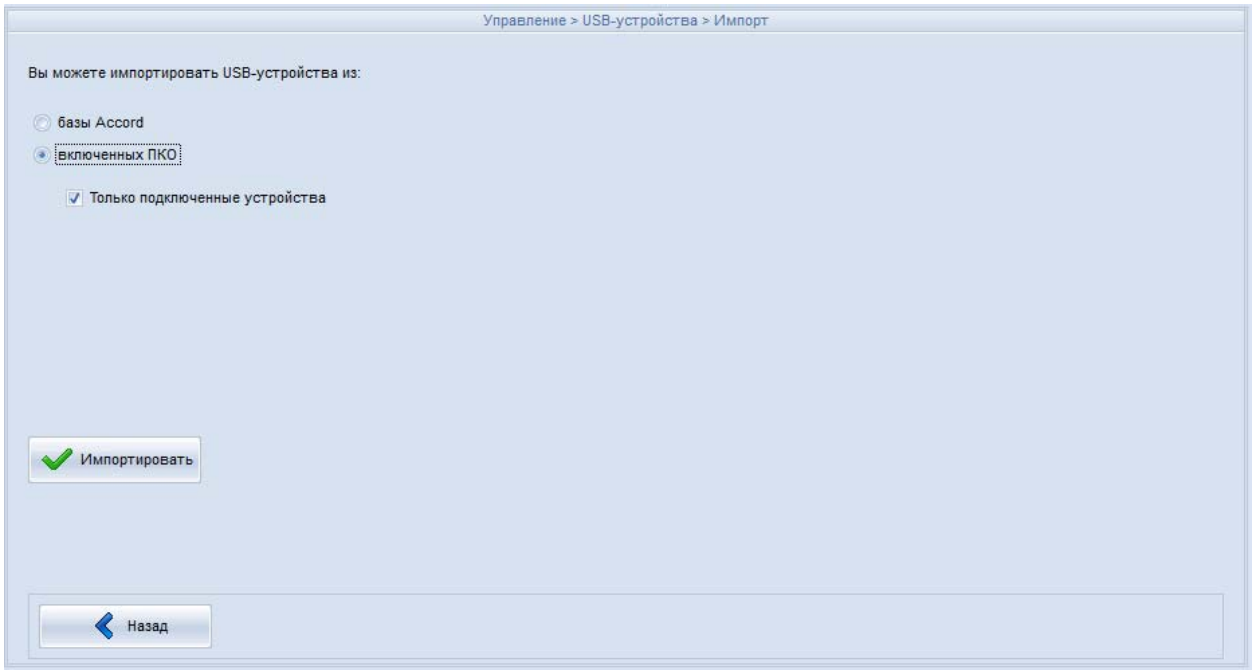

Рисунок 32 – Окно импорта USB-устройств. Импортирование информации о подключаемых к ПКО USB-устройствах

Если флажок «Только подключенные устройства» в окне импорта USB-устройств, приведённом на рисунке 32, 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 32, 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> на экран будет выведено окно, приведённое на рисунке 33.

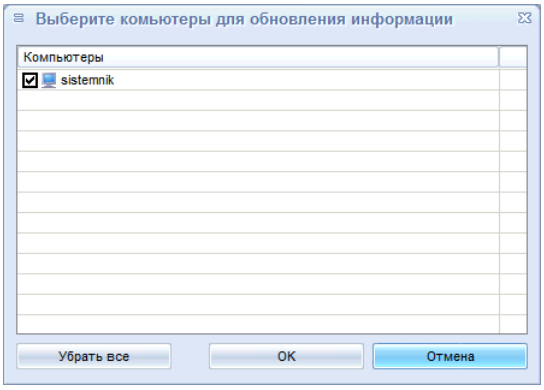

Рисунок 33 – Выбор ПКО, от которых будет получена информация о подключаемых USB-устройствах

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 ПАК СЗИ от НСД «Аккорд-Win32» или ПАК СЗИ от НСД «Аккорд-Win64» разрешают использовать на ПКО

Данная функция позволяет импортировать в список разрешённых USB-устройств системы информацию о USB-устройствах, которые ПАК СЗИ от НСД «Аккорд-Win32» и ПАК СЗИ от НСД «Аккорд-Win64» разрешают использовать на ПКО. Информация о формировании списка разрешенных USB-устройств на ПКО с помощью ПАК СЗИ от НСД «Аккорд-Win32» приведена в документе 11443195.4012-036 97 «Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-Win32» (версия 4.0). Установка правил разграничения доступа. Программа ACED32». Информация о формировании списка разрешенных USB-устройств на ПКО с помощью ПАК СЗИ от НСД «Аккорд-Win64» приведена в документе 11443195.4012-037 97 «Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-Win64» (версия 5.0). Установка правил разграничения доступа. Программа ACED32».

Необходимая для выполнения импортирования информация о разрешённых для использования на ПКО USB-устройствах передаётся подконтрольными объектами и хранится на сервере централизованного управления в так называемых ба-

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

Для импортирования в список разрешённых USB-устройств системы информации о USB-устройствах, которые ПАК СЗИ от НСД «Аккорд-Win32» или ПАК СЗИ от НСД «Аккорд-Win64» разрешают использовать на ПКО, следует в окне, приведённом на рисунке 29, нажать кнопку <Импорт>. В появившемся окне импорта USB-устройств, приведённом на рисунке 34, установить переключатель «Вы можете импортировать USB-устройства из:» в положение «базы Accord».

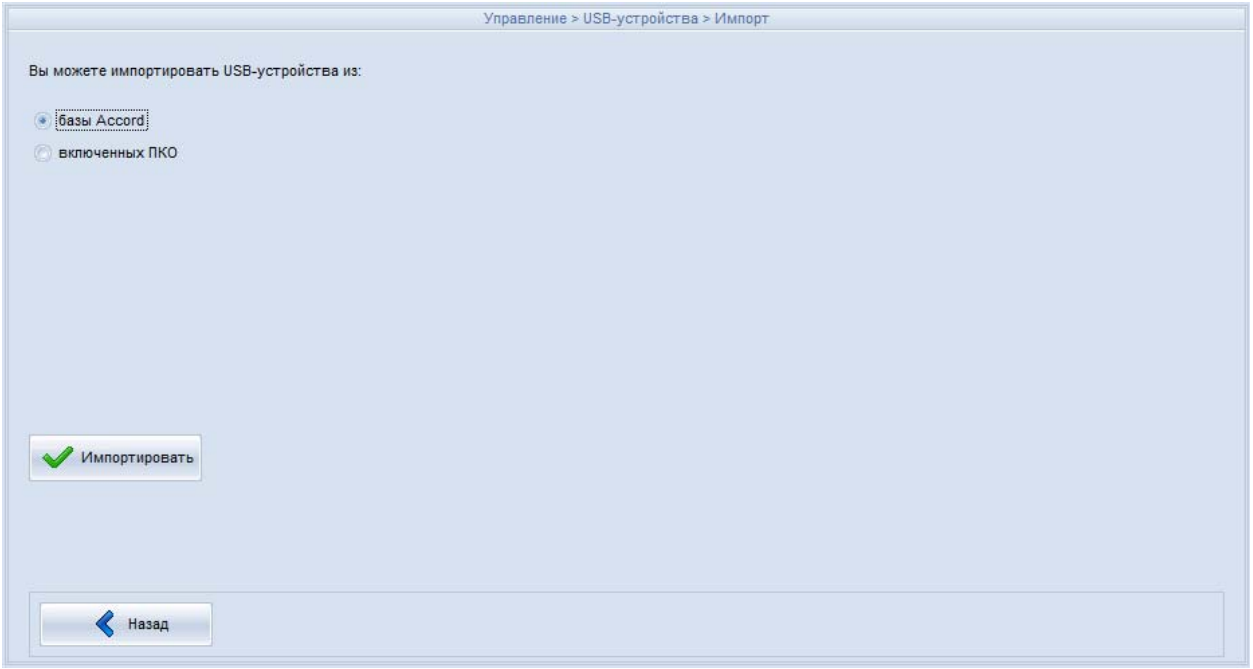

Рисунок 34 - Окно импорта USB-устройств. Импортирование информации о USB-устройствах, которые ПАК СЗИ от НСД «Аккорд-Win32» или ПАК СЗИ от НСД «Аккорд-Win64» разрешают использовать на ПКО

Для импортирования информации о USB-устройствах следует в окне импорта USB-устройств, приведённом на рисунке 34, нажать кнопку <Импортировать>. На экран будет выведено стандартное диалоговое окно открытия файла, в котором Администратору СУЦУ СЗИ от НСД следует выбрать файл с расширением *.amz (базу пользователей), содержащий информацию о USB-устройствах, которые следует импортировать в список разрешённых USB-устройств системы. На сервере централизованного управления 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 35.

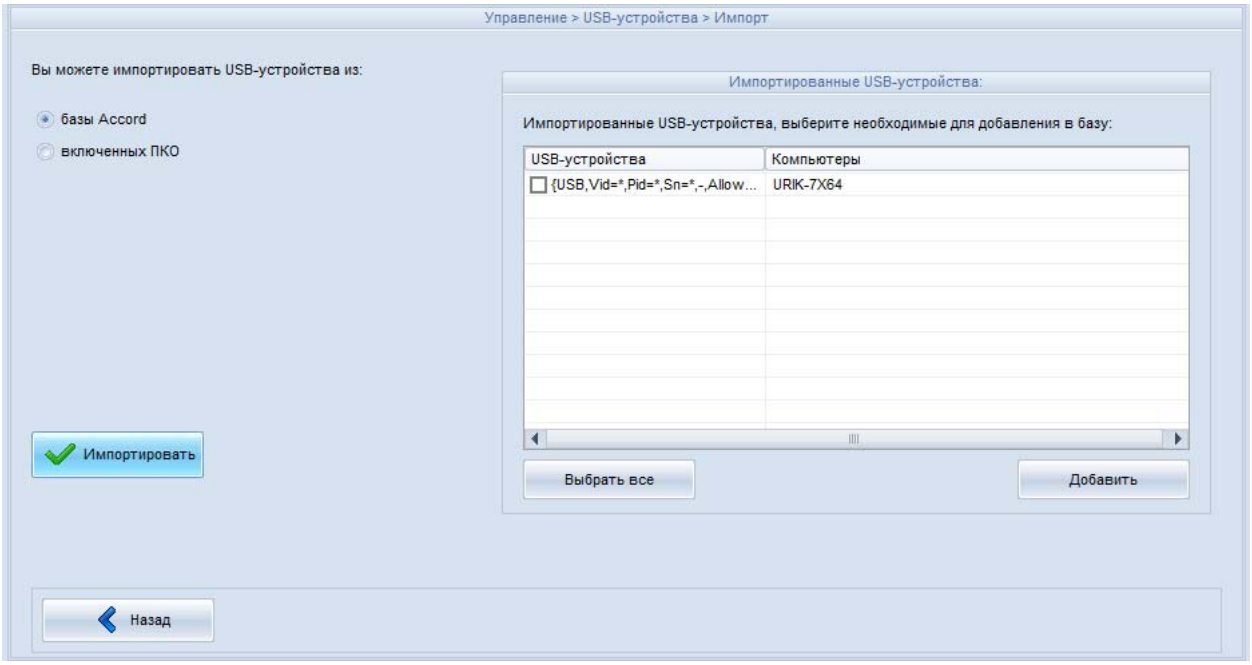

Рисунок 35 - Окно импорта USB-устройств. Импортирование информации о USB-устройствах, которые ПАК СЗИ от НСД «Аккорд-Win32» или ПАК СЗИ от НСД «Аккорд-Win64» разрешают использовать на ПКО. Выбор USB-устройств для импорта

В правой части окна импорта USB-устройств, приведённого на рисунке 35, будет отображаться список USB-устройств, информация о которых содержится в выбранной базе пользователей. Администратору СУЦУ СЗИ от НСД следует установить флажки напротив тех USB-устройств, которые нужно импортировать в список разрешённых USB-устройств системы и нажать кнопку <Добавить>.

Как показано на рисунке 36, список импортированных USB-устройств будет совпадать со списком разрешённых для использования USB-устройств, сформированным на ПКО средствами ПАК СЗИ от НСД «Аккорд-Win32» или ПАК СЗИ от НСД «Аккорд-Win64».

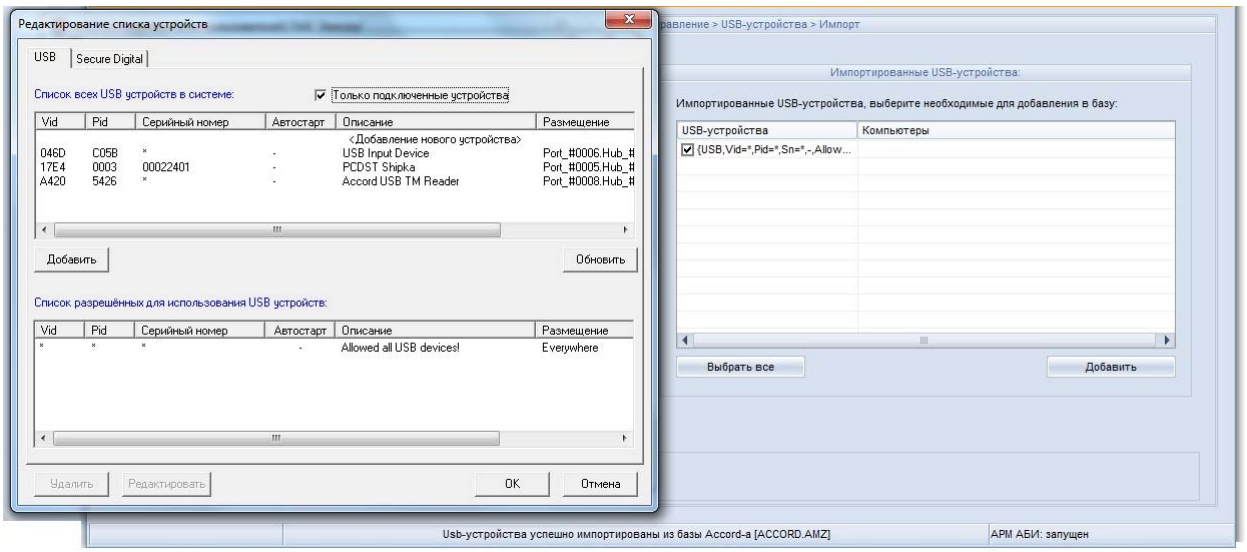

Рисунок 36 - Совпадение списка импортированных USB-устройств со списком разрешённых для использования на ПКО USB-устройств

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 29, дважды щелкнуть по записи, соответствующей данному USB-устройству или, установив флажок напротив данного USB-устройства, нажать кнопку <Редактировать>. На экран будет выведено окно, приведённое на рисунке 37.

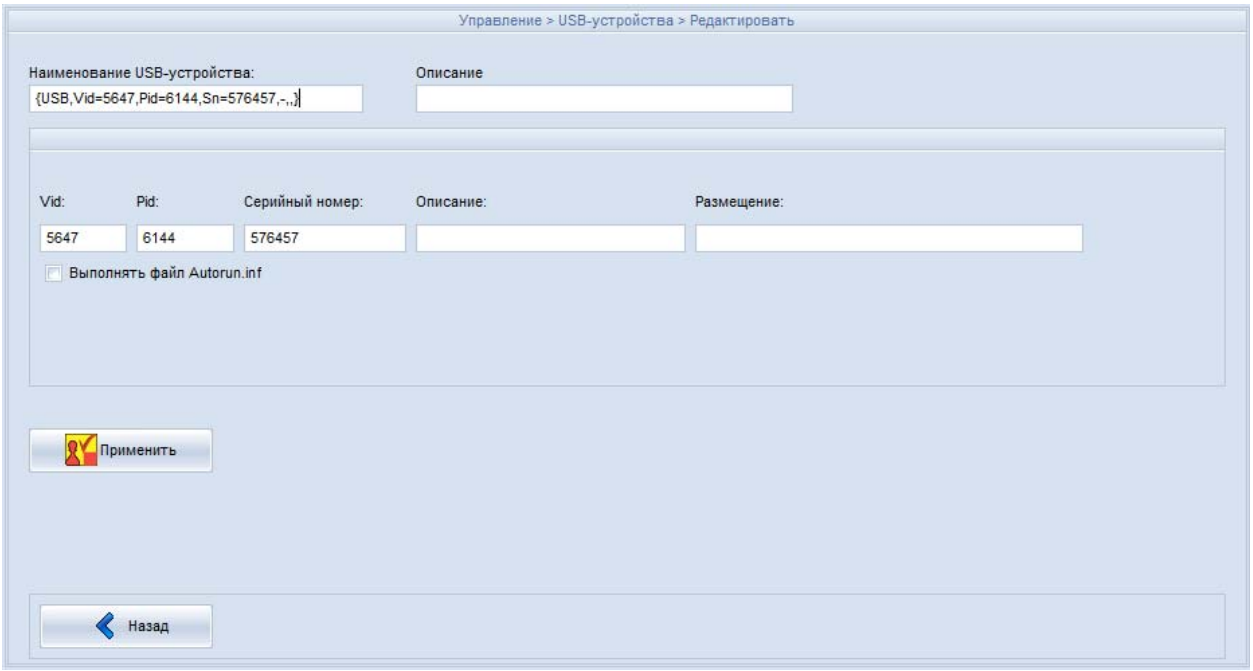

Рисунок 37 - Изменение информации о USB-устройстве

В данном окне следует внести необходимые изменения в информацию о USB-устройстве. Для сохранения внесённых изменений нужно 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 29, 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 38, Администратор СУЦУ 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.

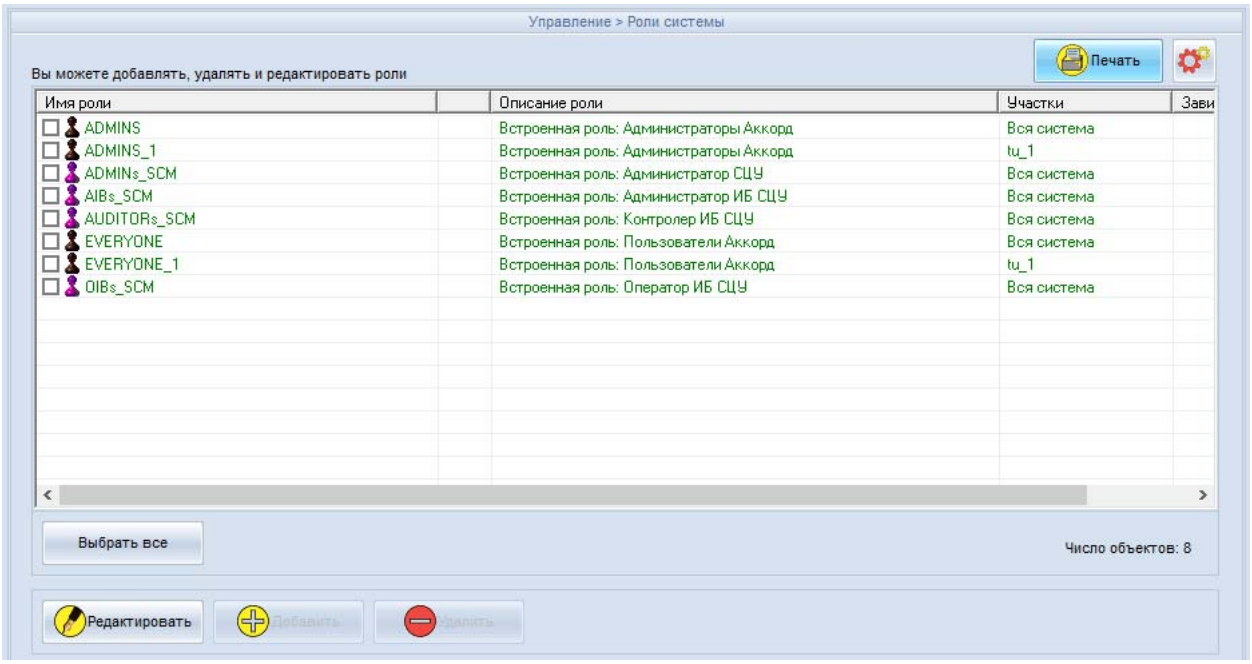

Рисунок 38 - Вкладка Управление > Роли системы

Для отображения в списке ролей вкладки Управление > Роли системы, приведённой на рисунке 38, информации о наличии списков файлов контроля целостности, списков задач и стартовых задачах нужно нажать кнопку <Настройка ото-

бражения информации>. После нажатия данной кнопки на экране появляется окно, приведённое на рисунке 39, в котором устанавливаются флаги напротив той информации о настройках ПКО, которую нужно отображать.

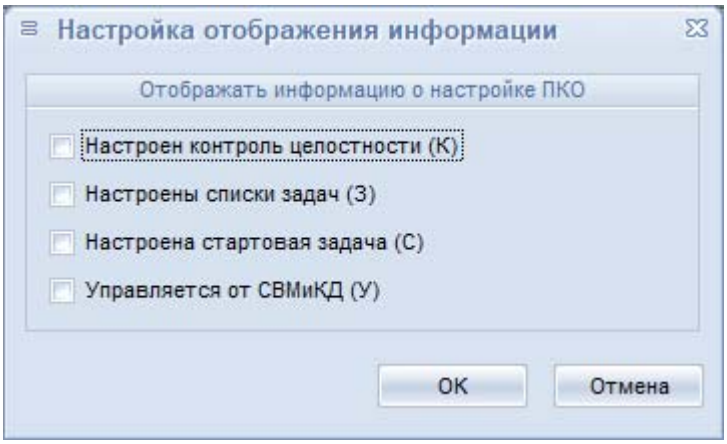

Рисунок 39 - Настройка отображения информации

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). После нажатия на данную кнопку на экран выводится окно, приведённое на рисунке 40, 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.

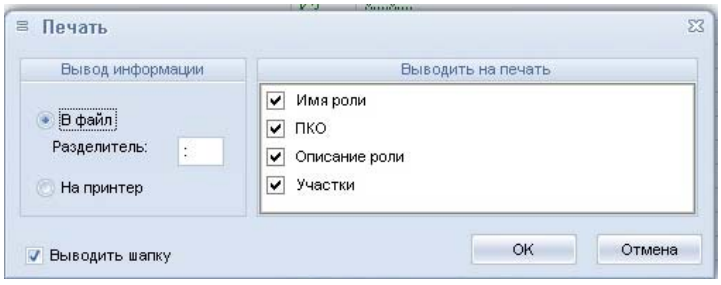

Рисунок 40 - Печать информации о ролях

Нажатие кнопки <Редактировать> выводит на экран окно, приведённое на рисунке 41.

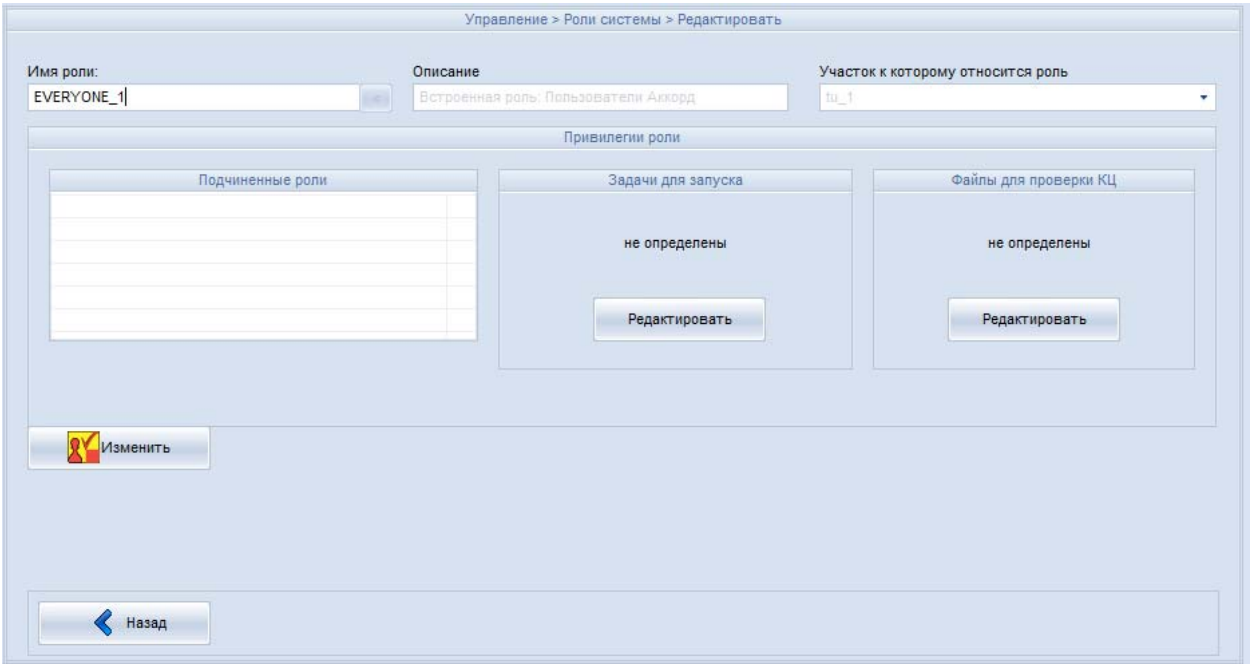

Рисунок 41 - Просмотр характеристик роли

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 42, Администратор СУЦУ СЗИ от НСД выполняет процедуры просмотра списка зарегистрированных в системе идентификаторов, печати информации об идентификаторах, поиска идентификаторов в базе.

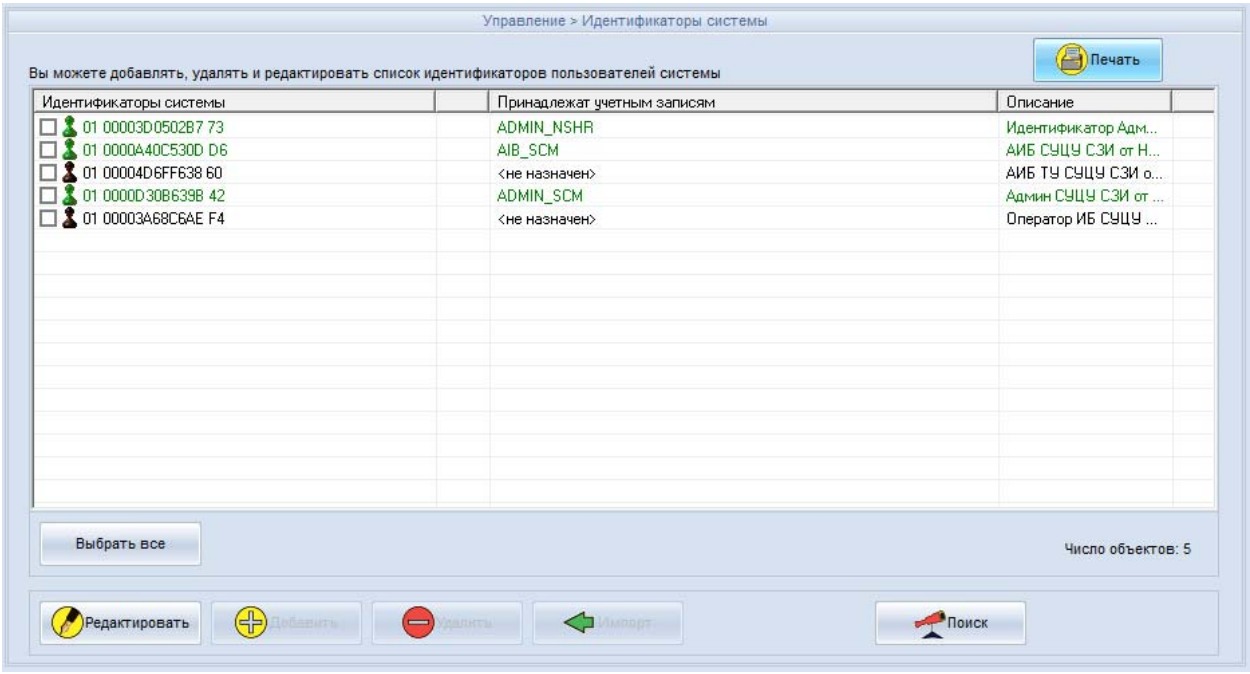

Рисунок 42 - Идентификаторы системы

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 43, 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.

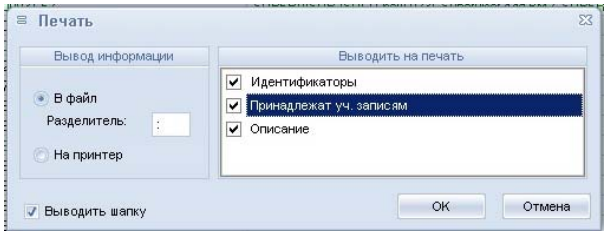

Рисунок 43 - Печать информации об идентификаторах

Если необходимо определить, добавлен ли идентификатор в базу СУЦУ СЗИ от НСД, следует нажать кнопку <Поиск> во вкладке Управление > Идентификаторы системы. Появится окно с сообщением «Введите идентификатор», приведённое на рисунке 44.

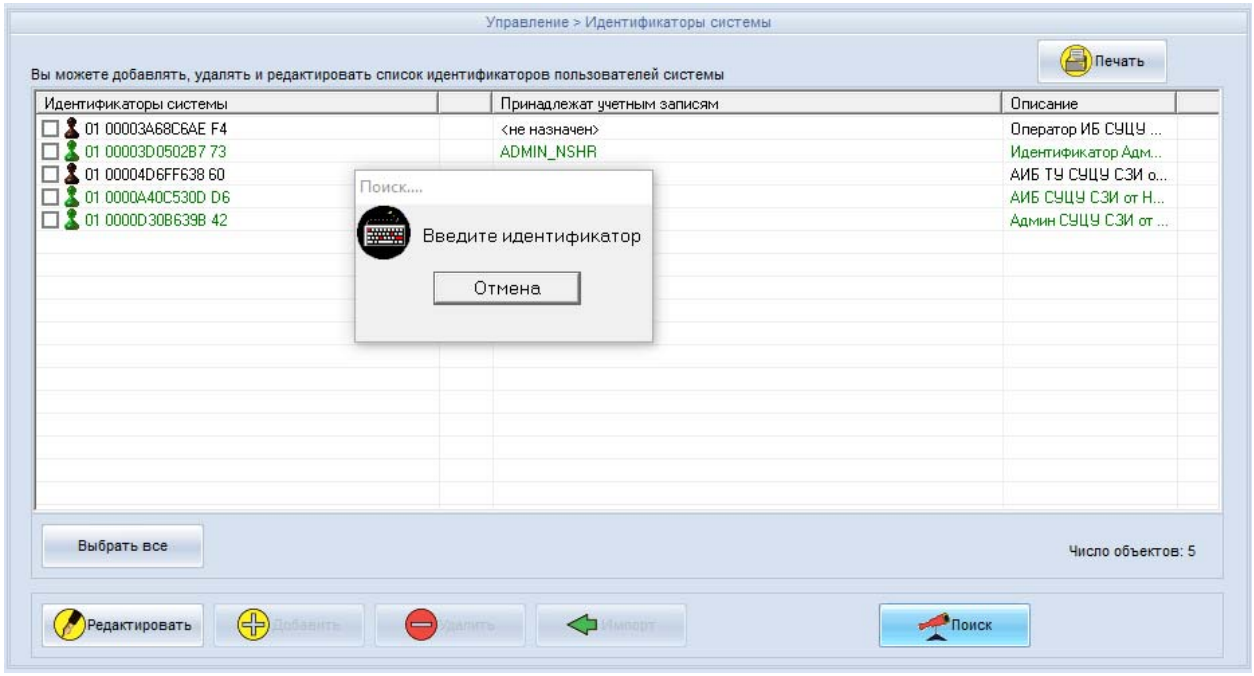

Рисунок 44 - Сообщение «Введите идентификатор»

Если приложенный идентификатор имеется в базе, то этот идентификатор будет выделен, как показано на рисунке 45.

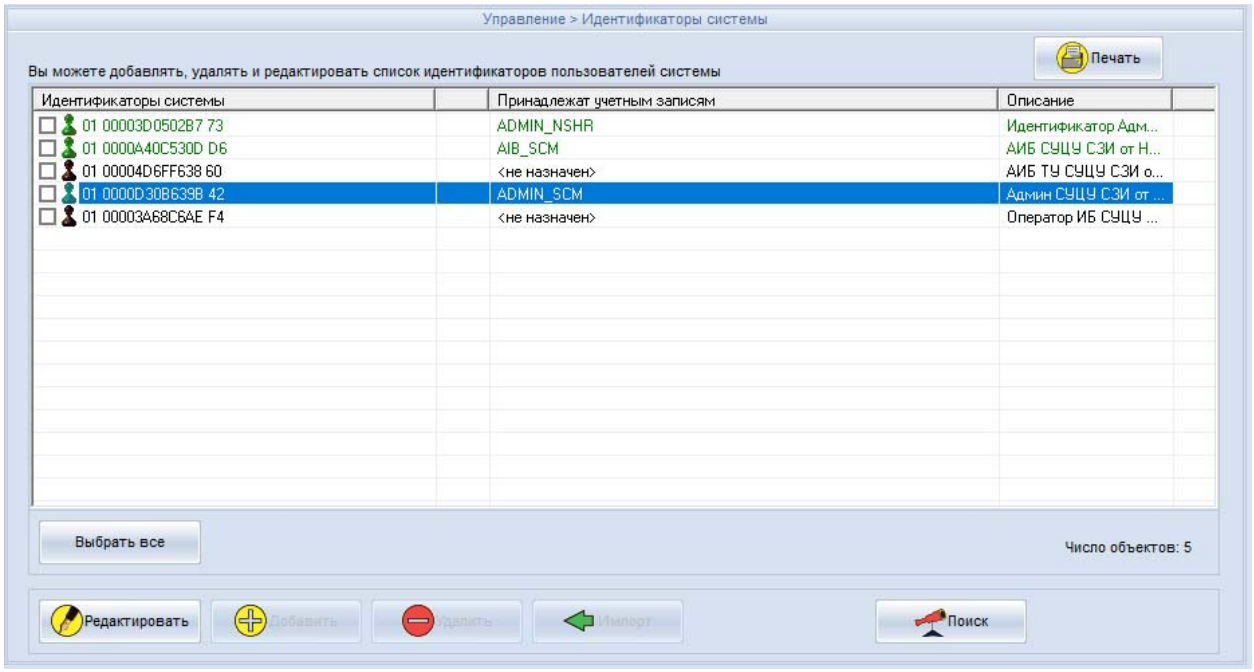

Рисунок 45 - Найдена учетная запись, которой назначен идентификатор

Если приложенный идентификатор отсутствует в базе, то в нижней части окна появится сообщение «Идентификатор не зарегистрирован!», как показано на рисунке 46.

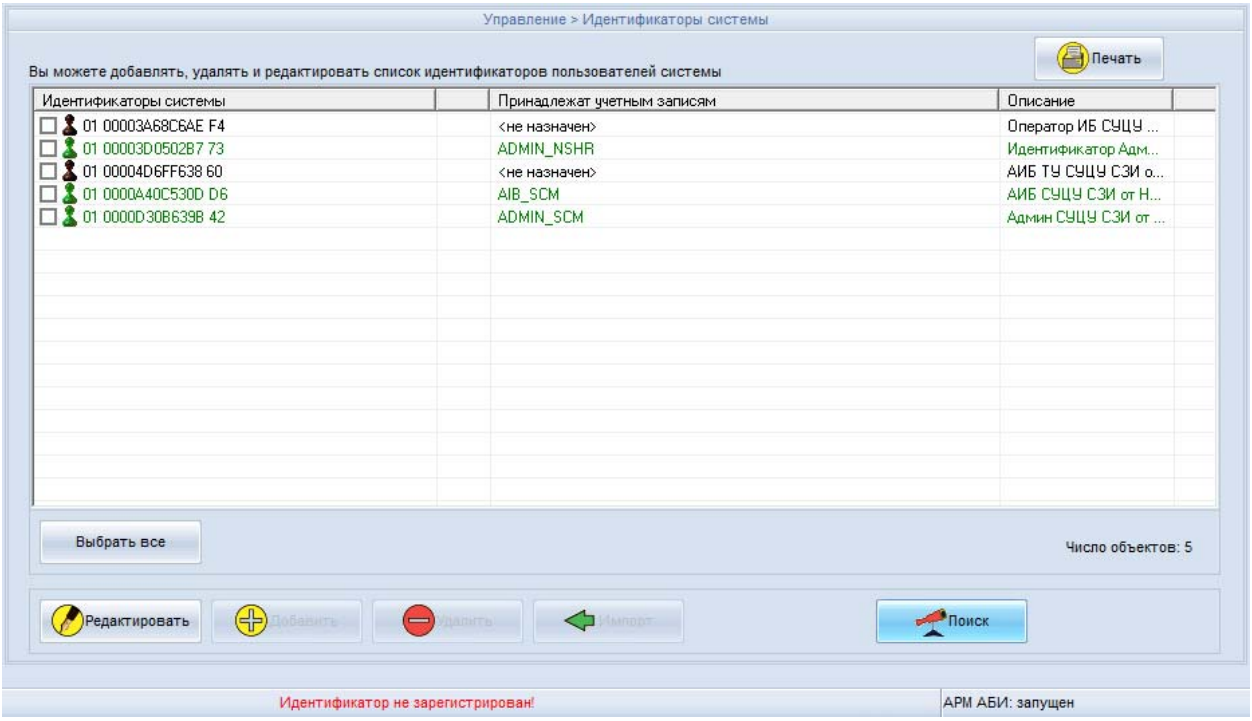

Рисунок 46 - Сообщение о том, что идентификатор не зарегистрирован

Нажатие кнопки <Редактировать> выводит на экран окно, приведённое на рисунке 47.

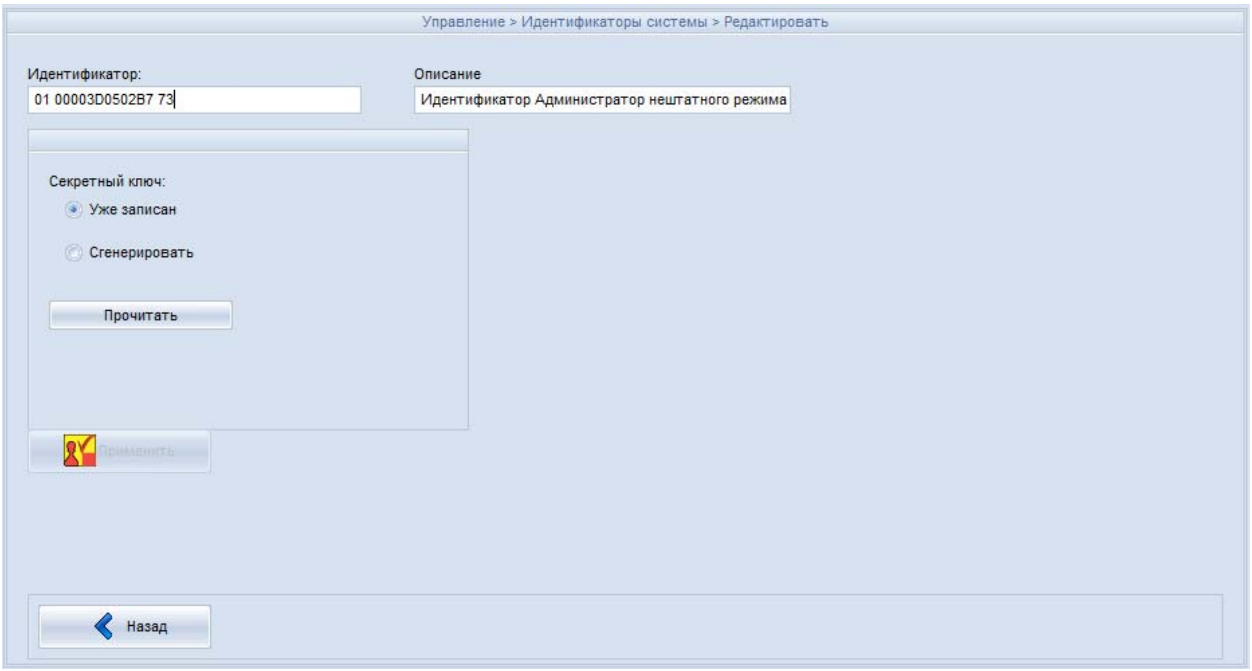

Рисунок 47 - Просмотр характеристик идентификатора

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

4.6 Вкладка «Компьютеры»

Во вкладке Управление > Компьютеры системы, приведённой на рисунке 48, Администратор СУЦУ может выполнять просмотр параметров ПКО, параметров ПАК СЗИ от НСД «Аккорд» и мандатные метки.

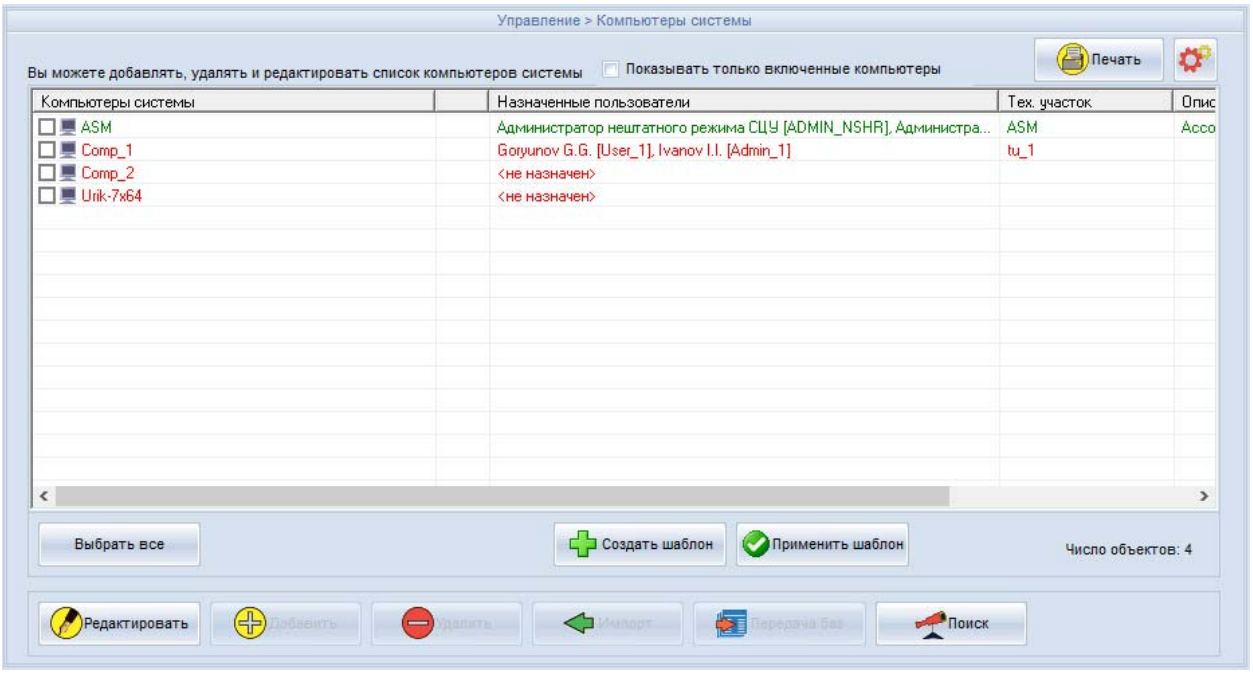

Рисунок 48 - Компьютеры системы

Для отображения в списке компьютеров информации о наличии списков файлов контроля целостности, списков задач (*.act файлов) и стартовых задачах нужно в окне, приведенном на рисунке 48, нажать кнопку <Настройка отображения информации>. После нажатия данной кнопки на экране появляется окно, приведённое на рисунке 27, 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). После нажатия на данную кнопку на экран выводится окно, приведённое на рисунке 49, в котором нужно выбрать способ печати: в файл или на принтер, тип выводимой информа-

ции (имя компьютера, описание компьютера, технологический участок, которому принадлежит данный компьютер, 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.

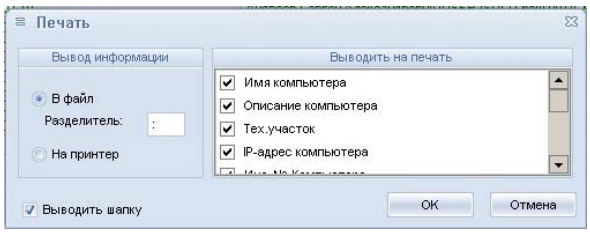

Рисунок 49 - Печать информации о компьютерах

Если необходимо определить, зарегистрирован ли компьютер в системе, следует нажать кнопку <Поиск> во вкладке Управление > Компьютеры системы (рисунок 48). На экран будет выведено окно, приведённое на рисунке 50.

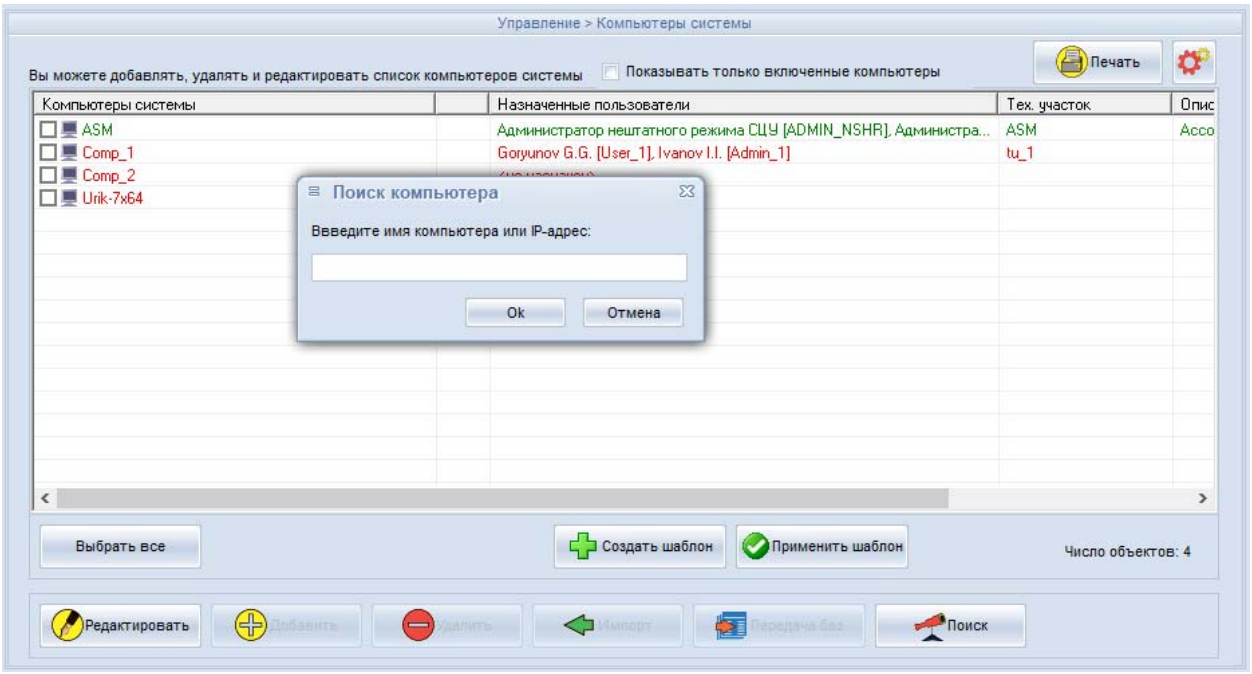

Рисунок 50 – Поиск компьютера по имени или IP-адресу

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 51.

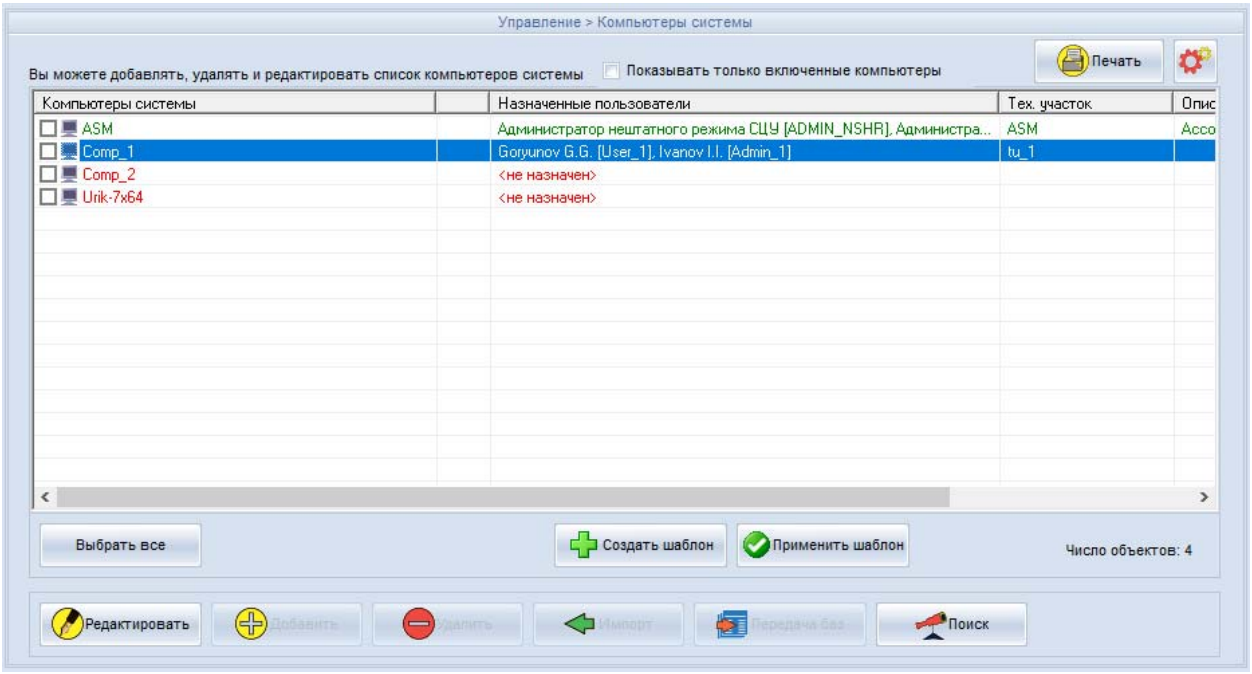

Рисунок 51 – Компьютер найден

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 52.

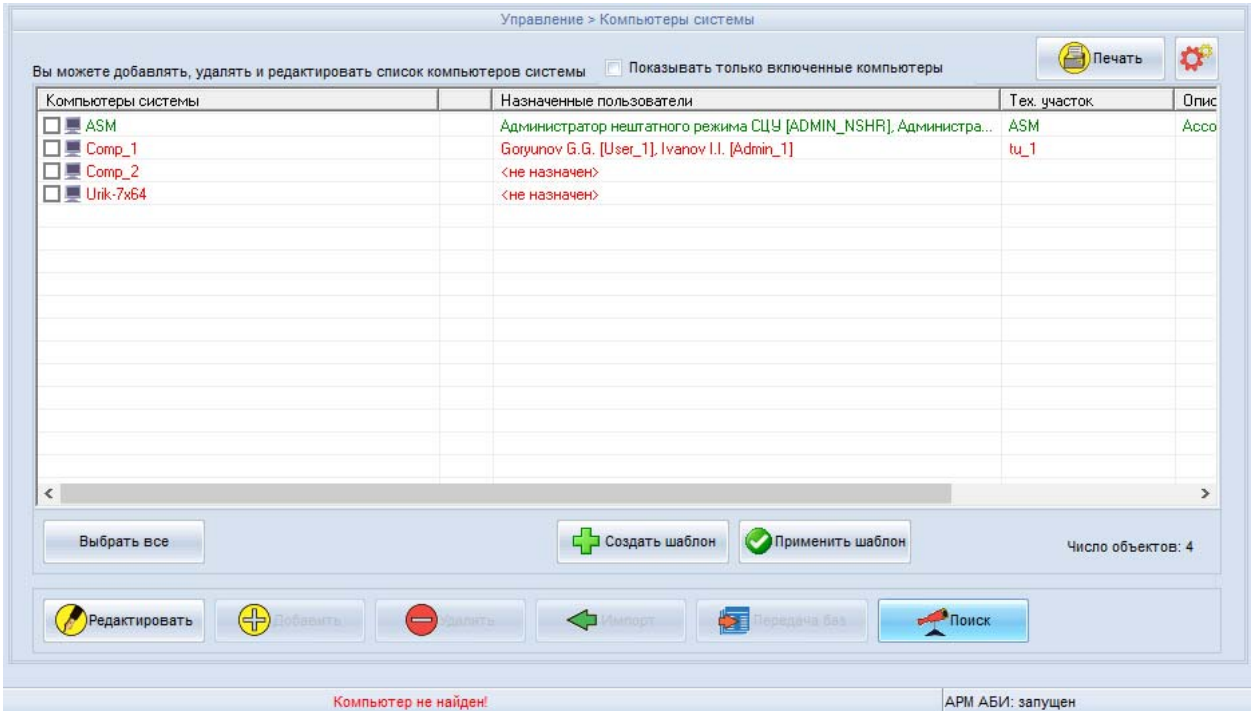

Рисунок 52 - Сообщение о том, что компьютер не найден

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

Нажатие кнопки <Редактировать> выводит на экран окно, приведённое на рисунке 53.

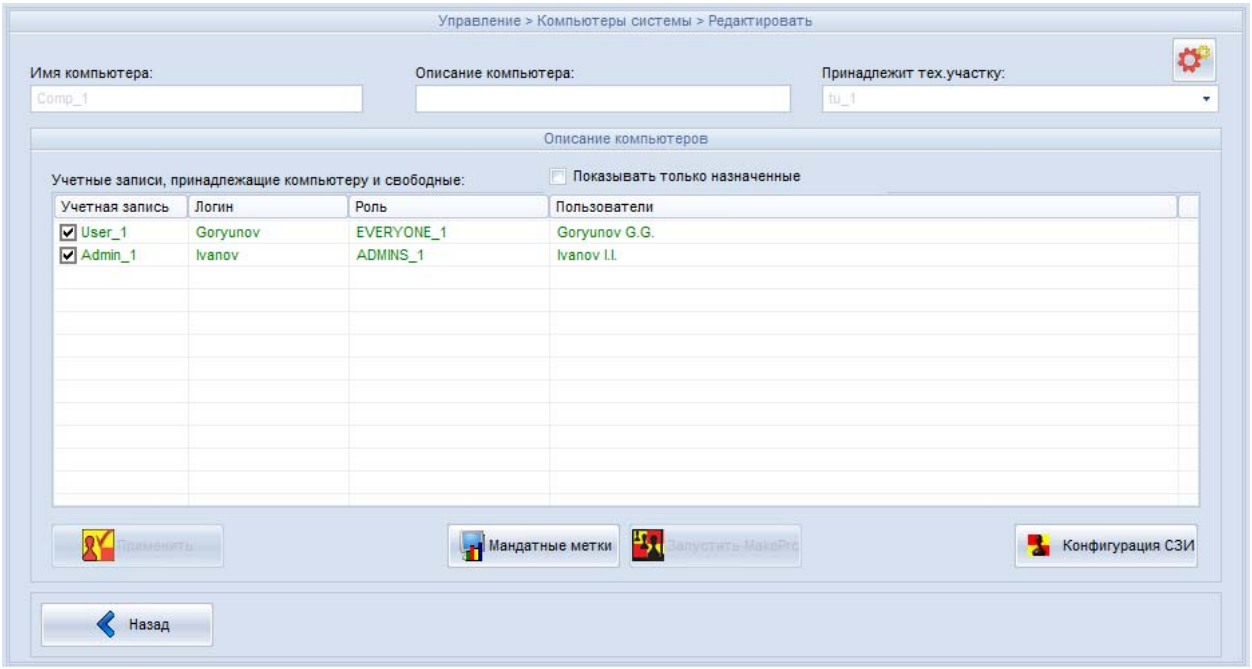

Рисунок 53 - Просмотр свойств подконтрольного объекта

Нажатие кнопки <Мандатные метки> выводит на экран окно, приведённое на рисунке 54.

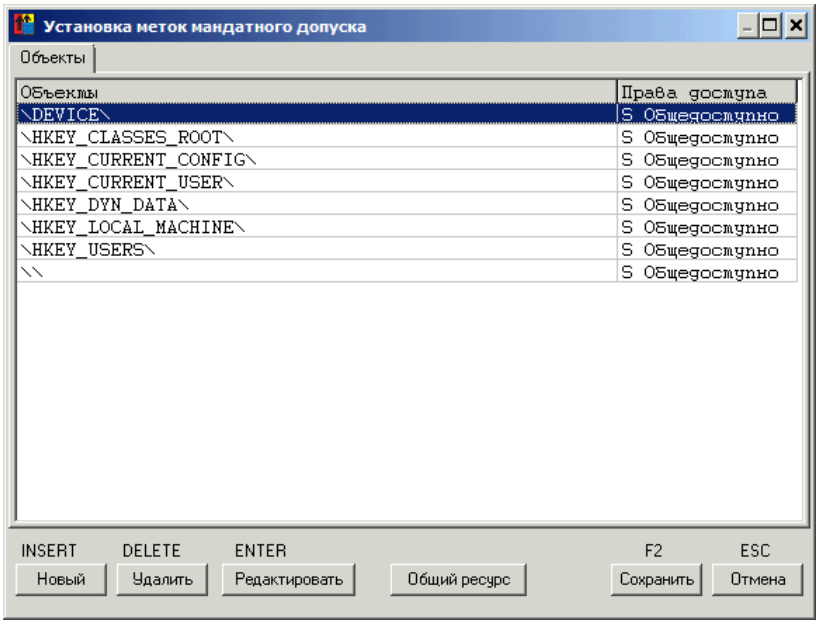

Рисунок 54 – Установка меток мандатного допуска

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

Нажатие кнопки <Конфигурация СЗИ> выводит на экран окно, приведённое на рисунке 55, 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». Администратор может просматривать установленные для данного ПКО настройки, но изменять их информацию он не может.

Рисунок 55 – Конфигурация СЗИ на подконтрольном объекте

4.7 Вкладка «Технологические участки»

Во вкладке Управление > Технологические участки системы, приведённой на рисунке 56, Администратор СУЦУ может просматривать технологические участки.

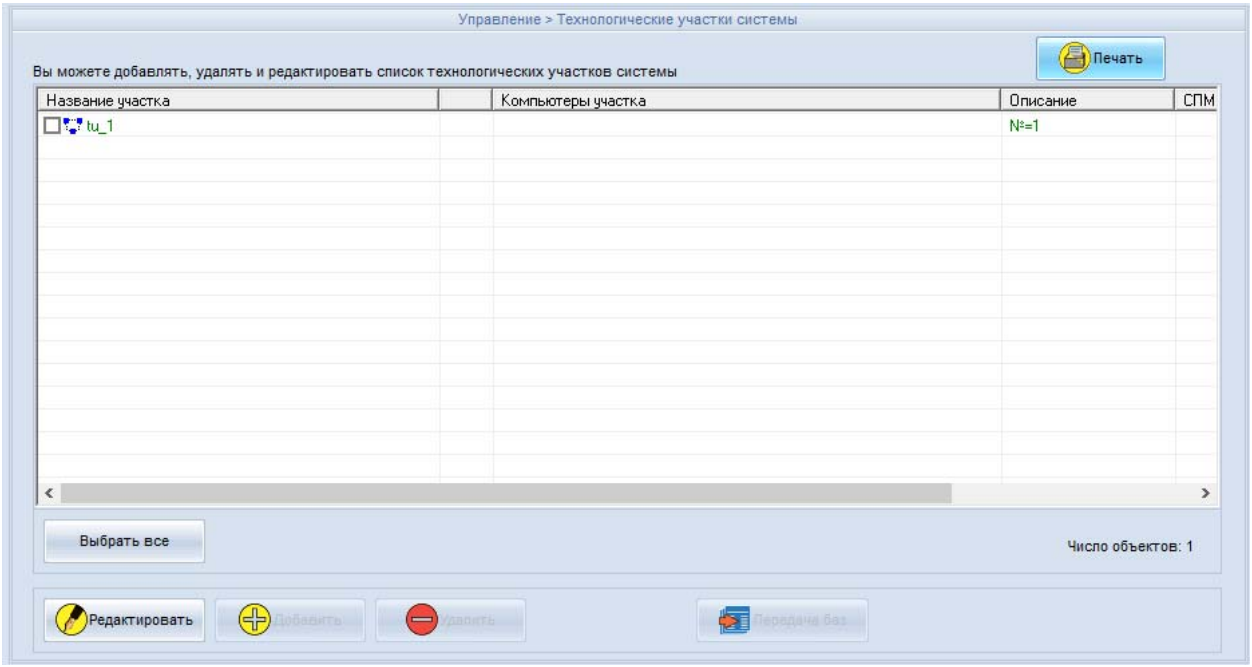

Рисунок 56 - Технологические участки системы

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 40, в котором нужно выбрать способ печати: в файл или на принтер, тип выводимой информации (имя участка, компьютеры, принадлежащие данному участку, описание технологического участка, значение параметра синхронизации паролей доменных пользователей в технологическом участке (СПМТ)); при печати в файл следует также указать разделитель.

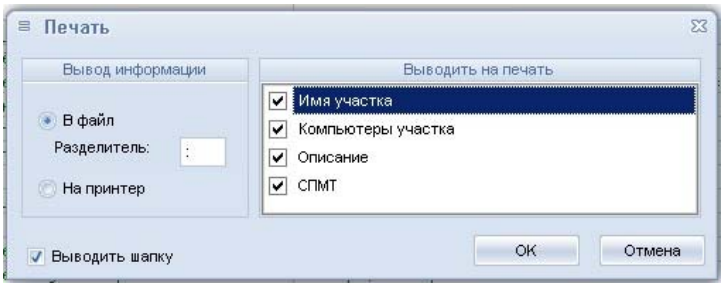

Рисунок 57 - Печать информации о технологических участках

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

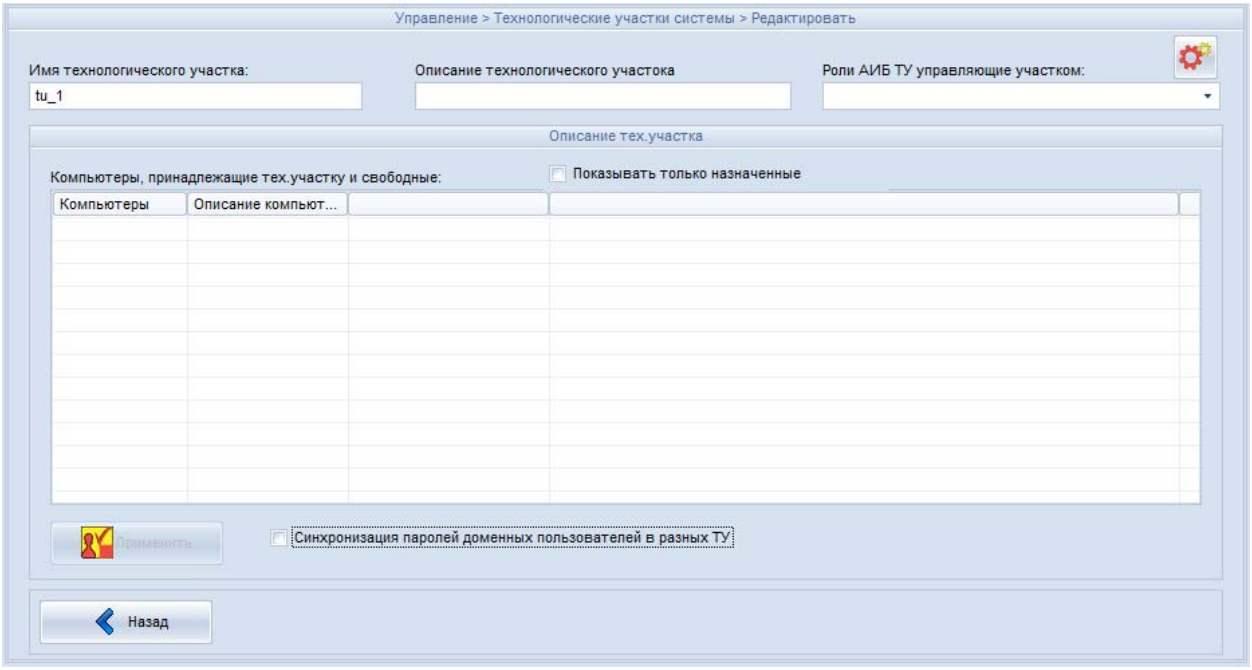

Рисунок 58 - Просмотр свойств технологического участка

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 59, Администратор СУЦУ может просматривать учетные записи, печатать информацию об учетных записях и осуществлять поиск учетных записей по идентификатору.

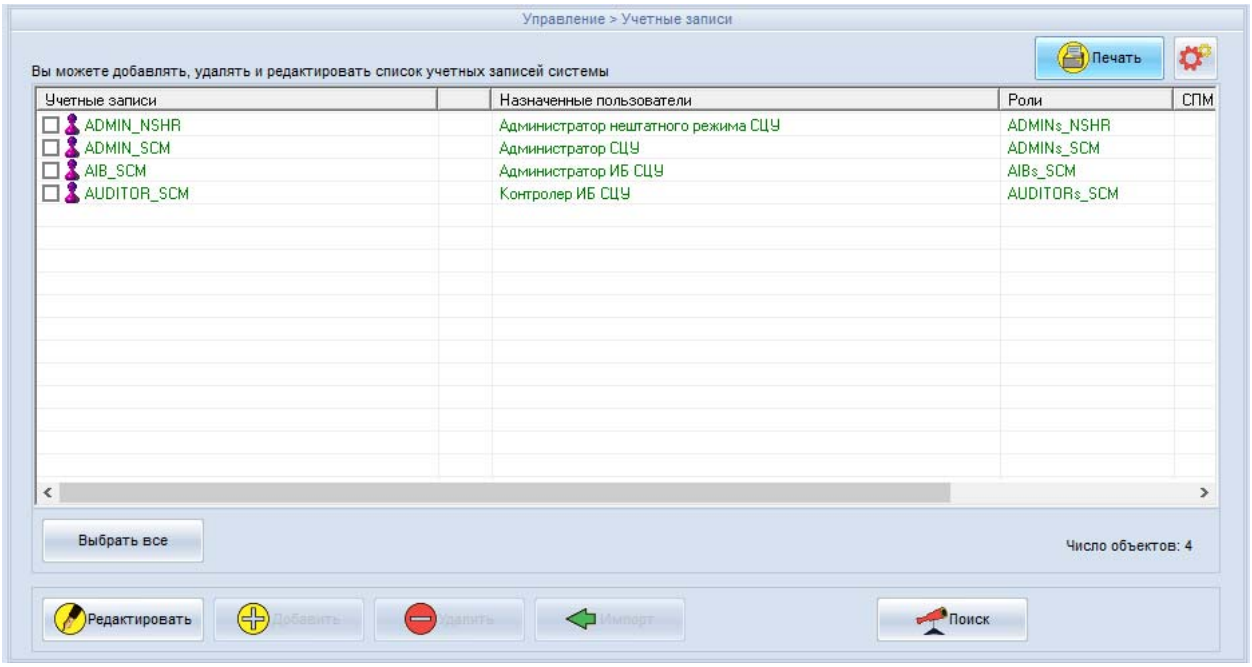

Рисунок 59 - Учётные записи

Для отображения в списке учётных записей информации о наличии списков файлов контроля целостности, списков задач и стартовых задачах нужно в окне, приведенном на рисунке 59, нажать кнопку <Настройка отображения информации>. После нажатия данной кнопки на экране появляется окно, приведённое на рисунке 27, 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). После нажатия на данную кнопку на экран выводится окно, приведённое на рисунке 60, 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.

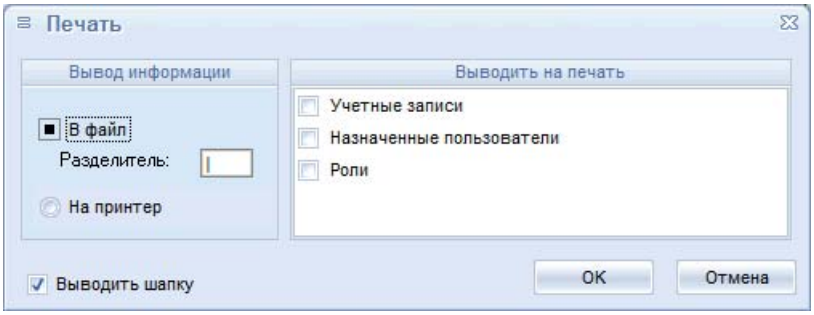

Рисунок 60 - Печать информации об учетных записях

Если необходимо определить, какой учётной записи принадлежит некоторый идентификатор, следует нажать кнопку <Поиск> на вкладке «Учётные записи». Появится сообщение «Введите идентификатор», приведённое на рисунке 61.

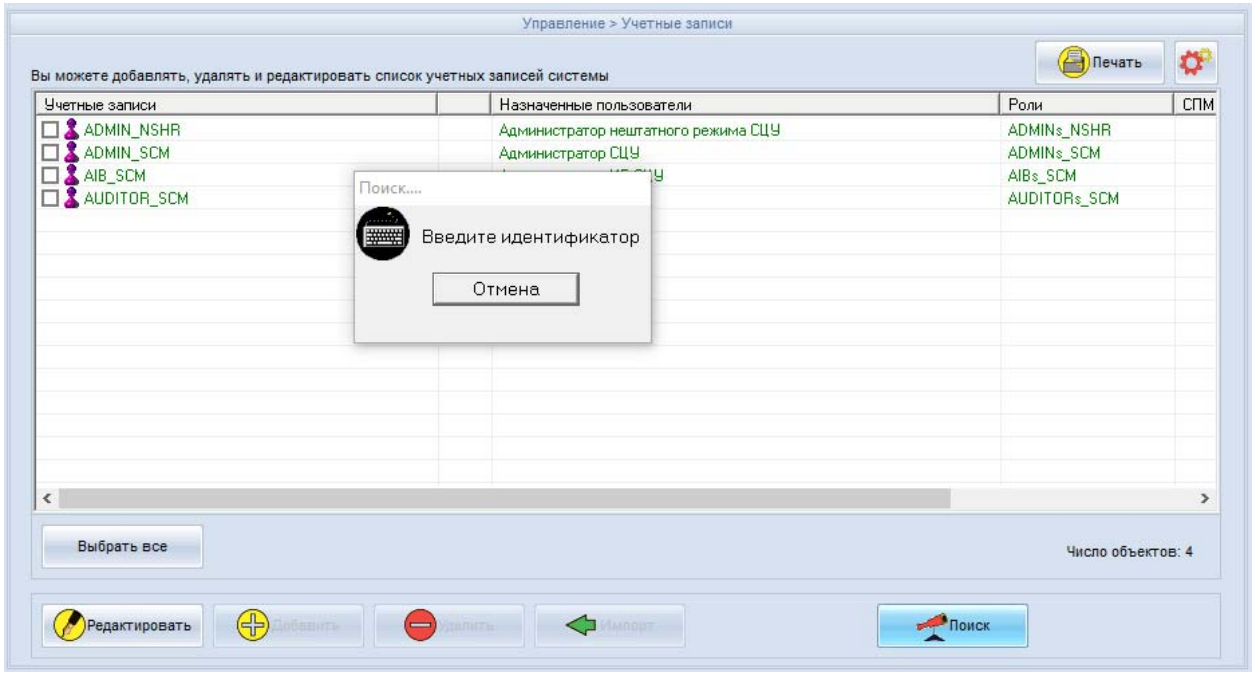

Рисунок 61 - Окно с сообщением «Введите идентификатор»

Если предъявленный идентификатор назначен какой-либо учётной записи, то эта учетная запись будет выделена, как показано на рисунке 62.

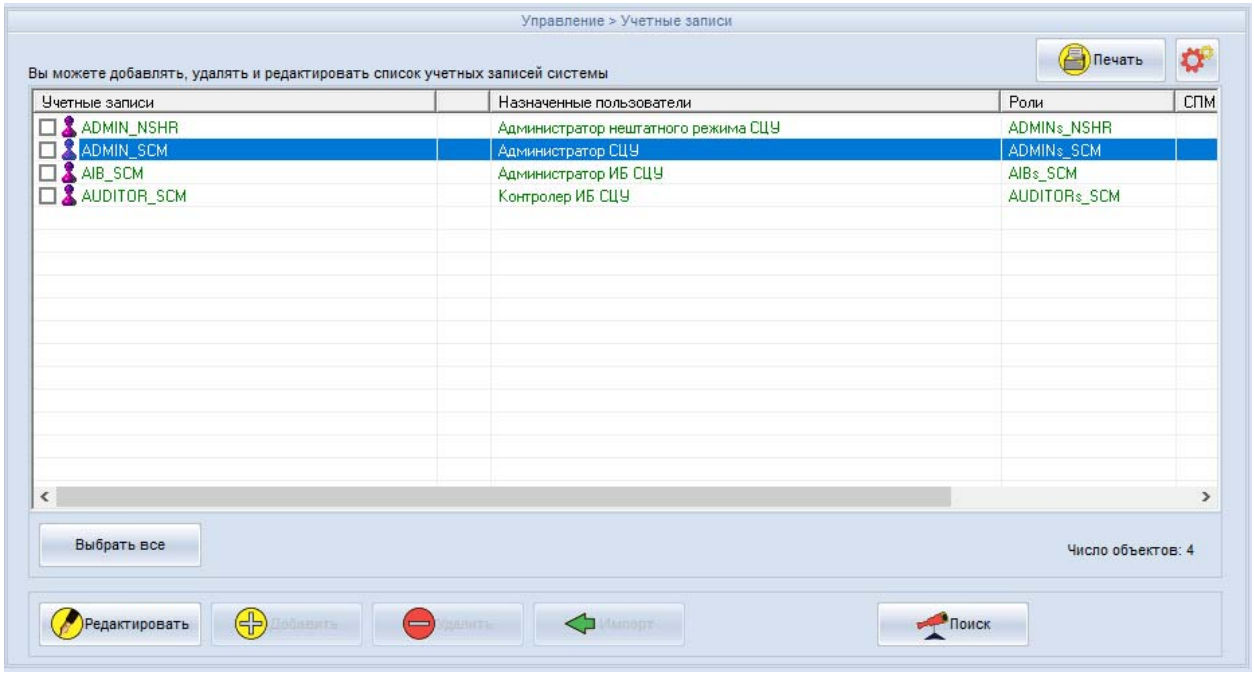

Рисунок 62 - Учетная запись, которой назначен идентификатор

Если предъявленный идентификатор не назначен никакой учётной записи, то в нижней части окна появится сообщение «Идентификатор не зарегистрирован!», как показано на рисунке 63.

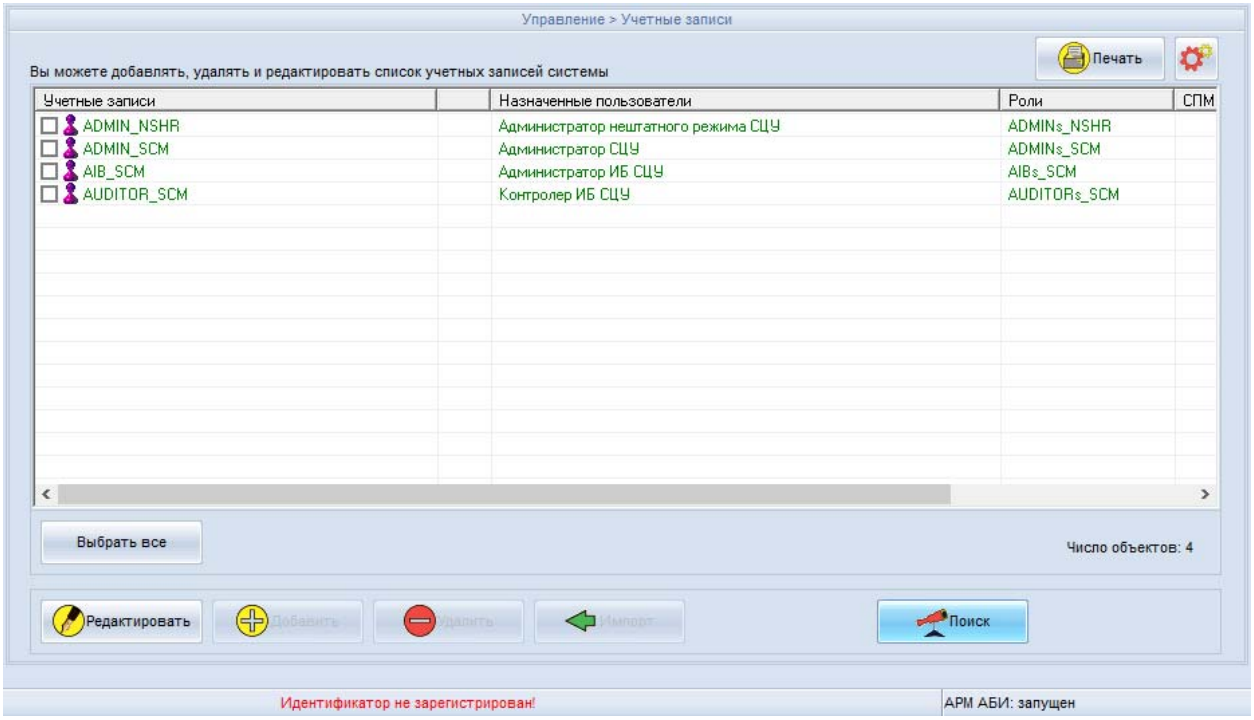

Рисунок 63 - Сообщение о том, что идентификатор не зарегистрирован

Нажатие кнопки <Редактировать> выводит на экран окно, приведённое на рисунке 64.

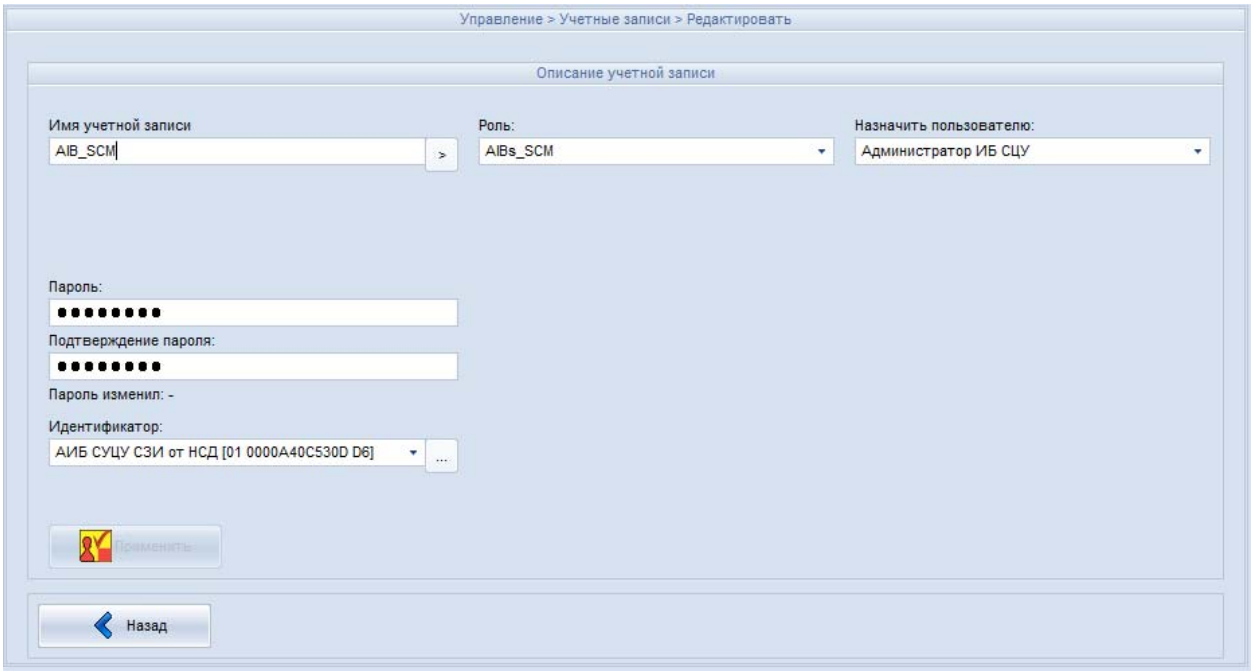

Рисунок 64 - Просмотр параметров учётной записи

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

4.9 Настройки сервера централизованного управления

4.9.1 Общие сведения

Администратор СУЦУ СЗИ от НСД осуществляет настройку основных параметров ПО сервера централизованного управления.

Для сохранения сделанных настроек необходимо нажать кнопку <Применить>.

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

Для экспорта настоек нужно во вкладке Настройка > Основные настройки, приведённой на рисунке 65, нажать кнопку <Экспорт>. После нажатия данной кнопки на экран будет выведено стандартное диалоговое окно выбора папки, в которую будет записан файл ASM.CFG.

Для импорта сохранённых в файле экспорта настроек нужно во вкладке Настройка > Основные настройки, приведённой на рисунке 65, нажать кнопку <Импорт>. После нажатия данной кнопки на экран будет выведено стандартное диалоговое окно выбора папки. Нужно указать папку, в которой находится файл экспорта ASM.CFG.

4.9.2 Основные настройки

Для настройки сервера централизованного управления администратором СУЦУ необходимо открыть вкладку Настройка > Основные настройки. После этого на экран будет выведено окно, приведённое на рисунке 65. С помощью данного окна у администратора СУЦУ имеется возможность:

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

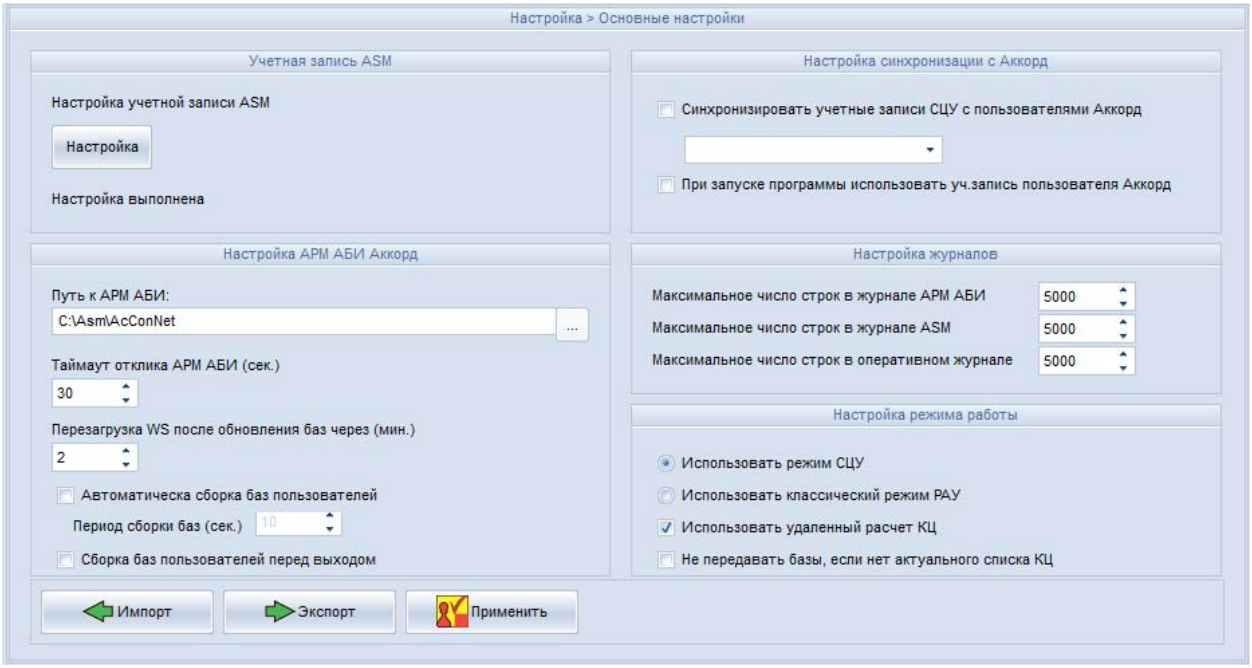

Рисунок 65 – Основные настройки сервера централизованного управления

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>. После её нажатия на экран 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>. После этого на экране 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 СУЦУ:
  - C:\Asm\asm.ini;
  - C:\Asm\asm.log;
  - базы СУЦУ:
  - 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 сервера централизованного управления 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 сервера централизованного управления 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 СУЦУ 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 СУЦУ

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 СУЦУ) 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 каталоге %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.

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
СВТ	Средства вычислительной техники
СЗИ	Средство защиты информации
СУЦУ	Система удалённого централизованного управления
СУ	Система управления
ASM	Accord Security Management

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

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

СОГЛАСОВАНО

Наименование организации, предприятия	Должность ис-полнителя	Фамилия, имя, отчество	Подпись	Дата