

ООО «ВАЛИДАТА»

УТВЕРЖДЕН  
ВАМБ.00096-06-ЛУ

**СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ  
«ВАЛИДАТА КРИПТОСЕРВЕР» ВЕРСИЯ 4**

Руководство по установке и настройке

ВАМБ.00096-06 91 01

2020

## **Аннотация**

Данный документ содержит описание установки и настройки библиотеки прикладного программного интерфейса (ППИ) криптосервера, работающей под управлением операционной системы (ОС) Microsoft Windows; программного обеспечения (ПО) криптографического сервера (далее по тексту — криптосервер или КС), работающего под управлением ОС Microsoft Windows; ПО автоматизированного рабочего места управления криптосервером (АРМ УКС) и автоматизированного рабочего места формирования отчетов (АРМ ФО), работающих под управлением ОС Microsoft Windows, входящих в состав ПК ВАМБ.00096-06 «Средство криптографической защиты информации «Валидата Криптосервер» версия 4» (далее по тексту — СКЗИ «Валидата Криптосервер»), а также описание настройки Сетевого справочника сертификатов (далее по тексту — ССС), реализованного на базе технологии Microsoft Active Directory.

Документ предназначен для администратора ОС Microsoft Windows как руководство по установке и настройке СКЗИ «Валидата Криптосервер».

## Содержание

<b>1 ОБЩИЕ СВЕДЕНИЯ</b>	<b>5</b>
<b>2 БИБЛИОТЕКА ПРИКЛАДНОГО ПРОГРАММНОГО ИНТЕРФЕЙСА ДЛЯ С/С++</b>	<b>6</b>
2.1 Назначение и условия функционирования	6
2.2 Состав	6
2.3 Установка	6
2.4 Удаление	7
2.5 Конфигурирование	7
<b>3 БИБЛИОТЕКА ПРИКЛАДНОГО ПРОГРАММНОГО ИНТЕРФЕЙСА ДЛЯ ПЛАТФОРМ JAVA/IBM WEBSPPHERE APPLICATION SERVER</b>	<b>8</b>
3.1 Назначение	8
3.2 Состав	8
3.3 Установка	8
3.4 Конфигурирование	9
3.5 Удаление	9
<b>4 КРИПТОСЕРВЕР</b>	<b>11</b>
4.1 Назначение и условия использования	11
4.2 Состав	11
4.3 Установка	11
4.4 Удаление	18
4.5 Настройка	18
4.5.1 Создание справочников сессий криптосервера	19
4.5.2 Конфигурация криптосервера	19
4.5.3 Настройка сессии администрирования	20
4.5.4 Настройки сессий криптосервера	22
4.5.5 Добавление сессии	22
4.5.6 Настройка авторизации при работе с сессией	25
4.5.7 Удаление сессии	27
4.5.8 Изменение параметров сессии	27
4.6 Настройка параметров криптографии	28
4.7 Настройка параметров DCE-RPC	29
4.8 Настройка журнала работы криптосервера	30
4.9 Организация удаленного доступа к файлу протокола	32
4.10 Формат журнала работы криптосервера	32
4.11 Завершение конфигурации криптосервера	36
4.12 Настройки операционной системы	36
4.12.1 Настройки параметров ОС Microsoft Windows	36
4.12.2 Настройки параметров СКЗИ «Валидата Криптосервер»	36
4.13 Установка и настройка базы данных	37
4.14 Настройка кластера криптосерверов	37
4.14.1 Общее описание	37
4.14.2 Описание механизма распределения нагрузки	37

4.14.3	Установка и настройка службы "Балансировка сетевой нагрузки" . . . . .	37
4.15	Настройка узла кластера криптосерверов . . . . .	38
4.16	Работа с узлами кластера криптосерверов . . . . .	45
4.17	Настройка службы синхронизации времени . . . . .	46
4.18	Работа КС . . . . .	47
4.18.1	Инициализация криптографического модуля . . . . .	47
4.18.2	Инициализация обработки входящих запросов . . . . .	48
<b>5</b>	<b>АВТОМАТИЗИРОВАННОЕ РАБОЧЕЕ МЕСТО УПРАВЛЕНИЯ КРИПТОСЕРВЕРОМ</b>	<b>49</b>
5.1	Назначение и условия использования . . . . .	49
5.2	Установка АРМ УКС и АРМ ФО . . . . .	49
5.3	Настройка АРМ УКС . . . . .	50
5.4	Настройка АРМ ФО . . . . .	50
<b>6</b>	<b>СЕТЕВОЙ СПРАВОЧНИК СЕРТИФИКАТОВ</b>	<b>52</b>
6.1	Назначение . . . . .	52
6.2	Описание технологии . . . . .	52
6.3	Установка . . . . .	54
6.3.1	Установка Active Directory . . . . .	54
6.3.2	Установка Active Directory - Lightweight Directory Services . . . . .	54
6.4	Настройка . . . . .	54
6.4.1	Настройка схемы . . . . .	54
6.4.2	Настройка схемы Active Directory . . . . .	55
6.4.3	Настройка схемы Active Directory - Lightweight Directory Services . . . . .	60
6.4.4	Настройка доступа . . . . .	61
6.4.5	Настройка доступа к ActiveDirectory и ActiveDirectory - Lightweight Directory Services . . . . .	62
6.5	Взаимодействие CCC . . . . .	63
6.5.1	CCC КС . . . . .	63
6.5.2	CCC пользователей . . . . .	63
6.5.3	Репликация CCC . . . . .	64
	<b>ПЕРЕЧЕНЬ СОКРАЩЕНИЙ</b>	<b>64</b>
	<b>ПЕРЕЧЕНЬ РИСУНКОВ</b>	<b>66</b>
	<b>ПЕРЕЧЕНЬ ТАБЛИЦ</b>	<b>67</b>

# 1 ОБЩИЕ СВЕДЕНИЯ

Перед установкой СКЗИ «Валидата Криптосервер» необходимо проверить целостность установочного комплекта с помощью программы контроля целостности **hashfile.exe**, находящейся на передаточном носителе.

Описание работы с программой контроля целостности, требования и порядок проведения процедуры контроля целостности описаны в документах ВАМБ.00060-06 93 02 «СКЗИ «Валидата CSP» версия 6. Контроль целостности. Руководство администратора информационной безопасности» и ВАМБ.00060-06 92 01 «СКЗИ «Валидата CSP» версия 6. Программа контроля целостности. Руководство пользователя».

## 2 БИБЛИОТЕКА ПРИКЛАДНОГО ПРОГРАММНОГО ИНТЕРФЕЙСА ДЛЯ С/С++

### 2.1 Назначение и условия функционирования

«Библиотека прикладного программного интерфейса криптографического сервера для С/С++» (далее — библиотека ППИ для С/С++) предназначена для предоставления программного интерфейса вызовов функций криптосервера. Библиотека ППИ для С/С++ предназначена для функционирования как под управлением 32-разрядных ОС Microsoft Windows (x86), так и под управлением 64-разрядных ОС Microsoft Windows (x64).

Список файлов, входящих в библиотеку ППИ и требующих обеспечения контроля целостности, приведён в документе ВАМБ.00096-06 93 01 «СКЗИ «Валидата Криптосервер» версия 4. Руководство администратора информационной безопасности».

### 2.2 Состав

В состав установочного комплекта библиотеки ППИ для С/С++ входят два файла - *libpki1\_x86.msi* и *libpki1\_x64.msi* (установочные комплекты для 32-битных ОС Microsoft Windows и для 64-битных ОС Microsoft Windows соответственно).

### 2.3 Установка

Установка должна производиться пользователем, имеющим права локального администратора.

Установка библиотеки ППИ для С/С++ выполняется стандартной установочной процедурой *msiexec.exe*, входящей в комплект поставки ОС.

Для установки библиотеки ППИ для С/С++ необходимо:

- зарегистрироваться в системе с правами локального администратора;
- смонтировать передаточный носитель на соответствующее устройство;
- сменить текущий каталог на каталог, в котором находятся файлы установочного комплекта;
- запустить программу Установщика *msiexec.exe /i libpki1\_x86.msi* (или *msiexec.exe /i libpki1\_x64.msi*);
- выбрать каталог и компоненты продукта для установки;
- следовать инструкциям программы Установщика Windows.

После инсталляции в каталог *%ProgramFiles%\VALIDATA\CrSrvSdk* (или *%ProgramFiles(x86)%\VALIDATA\CrSrvSdk*) будут записаны следующие файлы:

- *inc\vcert1.h* - файл описания констант, структур и функций;
- *inc\vcerterr.h* - файл с описаниями ошибок;
- *lib\libpki1.lib* - файл библиотеки для выполнения компоновки;
- *%WINDIR%\system32\libpki1.dll* (или *%WINDIR%\sysWOW64\libpki1.dll*) - файл разделяемой библиотеки интерфейса;

- *bin\pki1utl.exe* - исполняемый модуль тестовой утилиты;
- *bin\pki1.conf* - пример файла конфигурации тестовой утилиты;
- *bin\asn1.exe* - утилита для получения содержимого сертификата в текстовом виде;
- *src\\*.\** - исходные тексты тестовой утилиты.

## 2.4 Удаление

Удаление библиотеки ППИ для C/C++ выполняется стандартной установочной процедурой *msiexec.exe*, входящей в комплект поставки ОС.

Для удаления библиотеки ППИ для C/C++ необходимо:

- зарегистрироваться в системе с правами локального администратора;
- смонтировать передаточный носитель на соответствующее устройство;
- сменить текущий каталог на каталог, в котором находятся файлы установочного комплекта;
- запустить процедуру удаления с помощью программы Установщика *msiexec.exe /x libpki1\_x86.msi* (или *msiexec.exe /x libpki1\_x64.msi*);
- выбрать компоненты продукта для удаления;
- следовать инструкциям программы Установщика Windows.

При отсутствии передаточного носителя библиотеки ППИ для C/C++ для ее удаления можно воспользоваться Мастером установки и удаления программ, который находится в Панели управления ОС Microsoft Windows.

## 2.5 Конфигурирование

Библиотека ППИ для C/C++ использует стандартные клиентские библиотеки ОС, реализующие протокол DCE-RPC. Никаких дополнительных настроек для ОС Microsoft Windows не требуется. При работе с криптосервером используется встроенный контроль целостности протокола DCE-RPC.

## 3 БИБЛИОТЕКА ПРИКЛАДНОГО ПРОГРАММНОГО ИНТЕРФЕЙСА ДЛЯ ПЛАТФОРМ JAVA/IBM WEBSHERE APPLICATION SERVER

### 3.1 Назначение

Библиотека прикладного программного интерфейса криптографического сервера для платформ Java/IBM WebSphere Application Server (ППИ Java) предназначена для предоставления программного интерфейса, выполняемого с помощью Java JRE (среда выполнения) версия 1.6.0 или выше и/или IBM WebSphere Application Server (сервер приложений) версия 8.0, 8.5, 8.5.5 или выше, к функциям КС.

### 3.2 Состав

В состав установочного комплекта библиотеки ППИ для платформ Java/IBM WebSphere Application Server входит файл **CryptoServerInstall.jar**, упакованный с помощью утилиты **Jar**, входящей в состав Java SDK (среда разработки) версия 1.6.0 или выше.

### 3.3 Установка

Установка библиотеки ППИ для платформ Java/IBM WebSphere Application Server выполняется посредством распаковки файла установочного комплекта **CryptoServerInstall.jar** утилитой **Jar**, входящей в состав Java SDK версия 1.6.0 или выше.

Для установки библиотеки ППИ Java необходимо выполнить следующие действия:

- зарегистрироваться в системе с правами локального администратора;
- смонтировать носитель установочного комплекта на соответствующее устройство;
- создать каталог (далее называемый каталогом установки программного интерфейса), в который будет произведена установка библиотеки ППИ Java;
- скопировать, пользуясь стандартными средствами ОС, файл установочного комплекта **CryptoServerInstall.jar** в каталог установки библиотеки ППИ Java;
- распаковать файл дистрибутива с помощью команды **jar -xvf CryptoServerInstall.jar**, выполненной в каталоге установки библиотеки ППИ Java;
- после распаковки необходимо убедиться, что в каталоге установки были созданы следующие файлы:
  - CryptoServerLibrary.jar;
  - jarapac/jarapac.jar;
  - jarapac/ncacn\_ip\_tcp.jar;
  - jarapac/lib/jcifs-1.1.2.jar;
  - CRSRVTest/CryptoServerTest.class;



- CRSSRVTest/CryptoServerTest\$CryptoServerTestThread.class;
- CRSSRVTest/CryptoServerTestBean.class;
- CRSSRVTest/CryptoServerTestHome.class;
- CRSSRVTest/CryptoServerTestInterface.class;
- CRSSRVTest/CryptoServerTestServlet.class;
- CRSSRVTest/CryptoServerTestJSP.jsp;
- CRSSRVTest/CryptoServerTestPage.html;
- CRSSRVTest/CryptoServerUtil.class;
- CRSSRVTest/CryptoServerUtil\$1.class;
- CRSSRVTest/CryptoServerUtil\$execute\_test\_t\$break\_exception\_t.class;
- CRSSRVTest/CryptoServerUtil\$execute\_test\_t.class;
- CRSSRVTest/CryptoServerUtil\$test\_param\_t.class;
- run.cmd;
- run.sh.

### 3.4 Конфигурирование

Библиотека ППИ для платформ Java/IBM WebSphere Application Server не требует никакого дополнительного конфигурирования и готова к использованию сразу после успешного проведения установки.

### 3.5 Удаление

Удаление библиотеки ППИ для платформ Java/IBM WebSphere Application Server выполняется стандартными утилитами удаления, входящими в комплект ОС.

Для удаления библиотеки ППИ Java необходимо выполнить следующие действия:

- зарегистрироваться в системе с правами локального администратора;
- перейти в каталог установки библиотеки ППИ Java;
- удалить следующие файлы:
  - CryptoServerLibrary.jar;
  - jarapac/jarapac.jar;
  - jarapac/ncacn\_ip\_tcp.jar;
  - jarapac/lib/jcifs-1.1.2.jar;
  - CRSSRVTest/CryptoServerTest.class;
  - CRSSRVTest/CryptoServerTest\$CryptoServerTestThread.class;
  - CRSSRVTest/CryptoServerTestBean.class;
  - CRSSRVTest/CryptoServerTestHome.class;
  - CRSSRVTest/CryptoServerTestInterface.class;
  - CRSSRVTest/CryptoServerTestServlet.class;

- CRSRVTest/CryptoServerTestJSP.jsp;
  - CRSRVTest/CryptoServerTestPage.html;
  - CRSRVTest/CryptoServerUtil.class;
  - CRSRVTest/CryptoServerUtil\$1.class;
  - CRSRVTest/CryptoServerUtil\$execute\_test\_t\$break\_exception\_t.class;
  - CRSRVTest/CryptoServerUtil\$execute\_test\_t.class;
  - CRSRVTest/CryptoServerUtil\$test\_param\_t.class;
  - run.cmd;
  - run.sh.
- удалить следующие каталоги:
- CRSRVTest
  - jarapac/lib
  - jarapac
- при необходимости, перейдя в корневой каталог, удалить каталог установки библиотеки ППИ Java.

## 4 КРИПТОСЕРВЕР

### 4.1 Назначение и условия использования

ПК ВАМБ.00096-06 12 01 «Криптографический сервер» (далее - КС) предназначен для выполнения функций электронной подписи (ЭП), хэширования, шифрования и др. Для обеспечения безопасности ключевой информации и целостности ПО КС доступ прикладных программ ко всем функциям КС осуществляется по локальной сети с помощью протокола DCE-RPC (Remote Procedure Call).

КС устанавливается на одной или нескольких ЭВМ. Перед началом установки КС необходимо установить и настроить криптографическое ядро - ПК ВАМБ.00060-06 «СКЗИ «Валидата CSP» версия 6» (далее - СКЗИ «Валидата CSP») - и ПК ВАМБ.00077-06 ««Валидата Клиент» версия 4» (далее - ПК «Валидата Клиент»). Установка указанных ПК осуществляется в соответствии с документами ВАМБ.00060-06 91 01 «СКЗИ «Валидата CSP» версия 6. Руководство по установке и настройке» и ВАМБ.00077-06 91 01 ««Валидата Клиент» версия 4. Руководство по установке и настройке».

*Примечание - 32-битный вариант СКЗИ «Валидата Криптосервер» может работать как в среде 32-битных ОС Microsoft Windows, так и в среде 64-битных ОС Microsoft Windows (естественно, в 32-битном режиме). При этом, "битность" используемого ПК «Валидата Клиент» должна совпадать с "битностью" КС, а "битность" СКЗИ «Валидата CSP» должна совпадать с "битностью" ОС Microsoft Windows.*

### 4.2 Состав

В состав ПО КС входят следующие файлы:

- *zcssvc.exe* - исполняемый модуль сервиса КС;
- *cslogsvc.exe* - исполняемый модуль сервиса протоколирования КС;
- *zcsmom.exe* - исполняемый модуль локального монитора КС;
- *csmgmt.dll* - модуль динамической библиотеки настройки КС;
- *vcertmsg.dll* - модуль динамической библиотеки сообщений КС.

Кроме того, используются модули, входящие в состав ПК «Валидата Клиент» и криптографического ядра СКЗИ «Валидата CSP».

При использовании КС должен быть обеспечен контроль целостности файлов ПО КС, СКЗИ «Валидата CSP», ПК «Валидата Клиент» и файлов системного ПО в соответствии с требованиями документа ВАМБ.00096-06 93 01 «СКЗИ «Валидата Криптосервер» версия 4. Руководство администратора информационной безопасности».

### 4.3 Установка

Установка должна производиться пользователем, имеющим права локального администратора.

В состав установочного комплекта КС для ОС Microsoft Windows входят, в том числе, два файла - *zcrsrv\_x86.msi* и *zcrsrv\_x64.msi* (установочные комплекты для

32-битных ОС Microsoft Windows и для 64-битных ОС Microsoft Windows, соответственно).

Установка КС для ОС Microsoft Windows выполняется стандартной установочной процедурой *msiexec.exe*, входящей в комплект поставки ОС.

Для установки КС необходимо:

- зарегистрироваться в системе с правами локального администратора;
- смонтировать передаточный носитель на соответствующее устройство;
- сменить текущий каталог на каталог, в котором находятся файлы установочного комплекта;
- запустить программу Установщика *msiexec.exe /i zcrsrv\_x86.msi* (или *msiexec.exe /i zcrsrv\_x64.msi*).

После запуска программы установки на экране появляется стартовый диалог мастера установки (Рисунок 1).

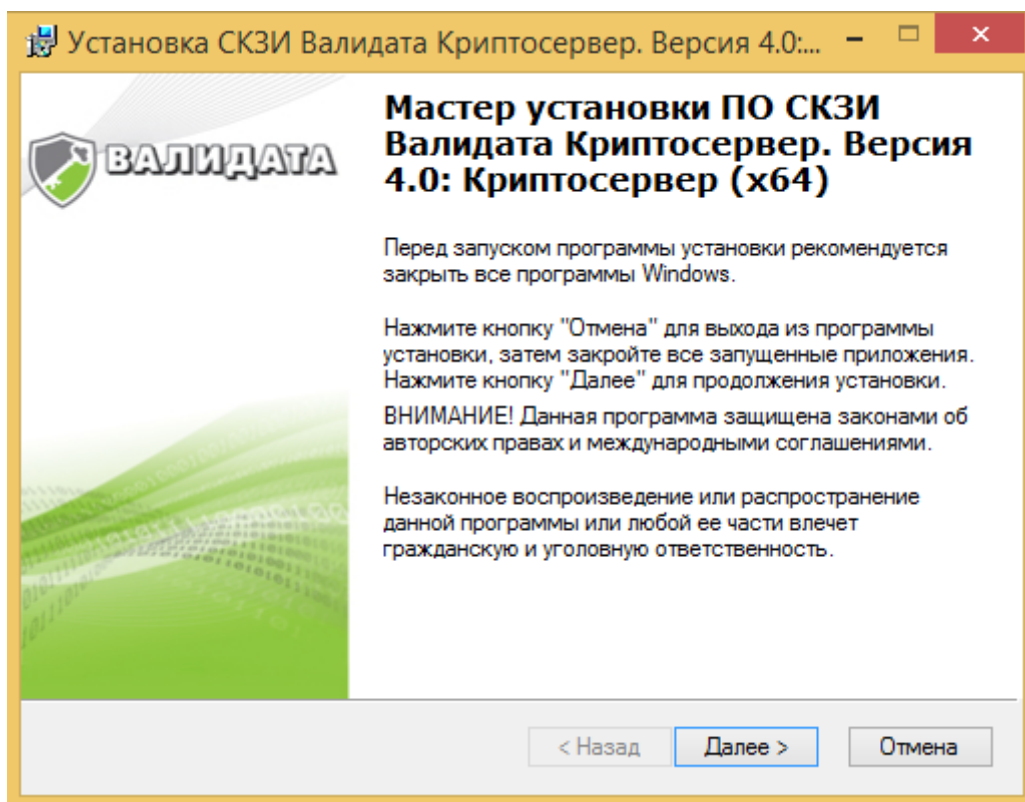


Рисунок 1 – Запуск программы установки

Нажмите кнопку «**Далее**». В следующем диалоге (Рисунок 2) укажите имя пользователя и наименование эксплуатирующей организации.

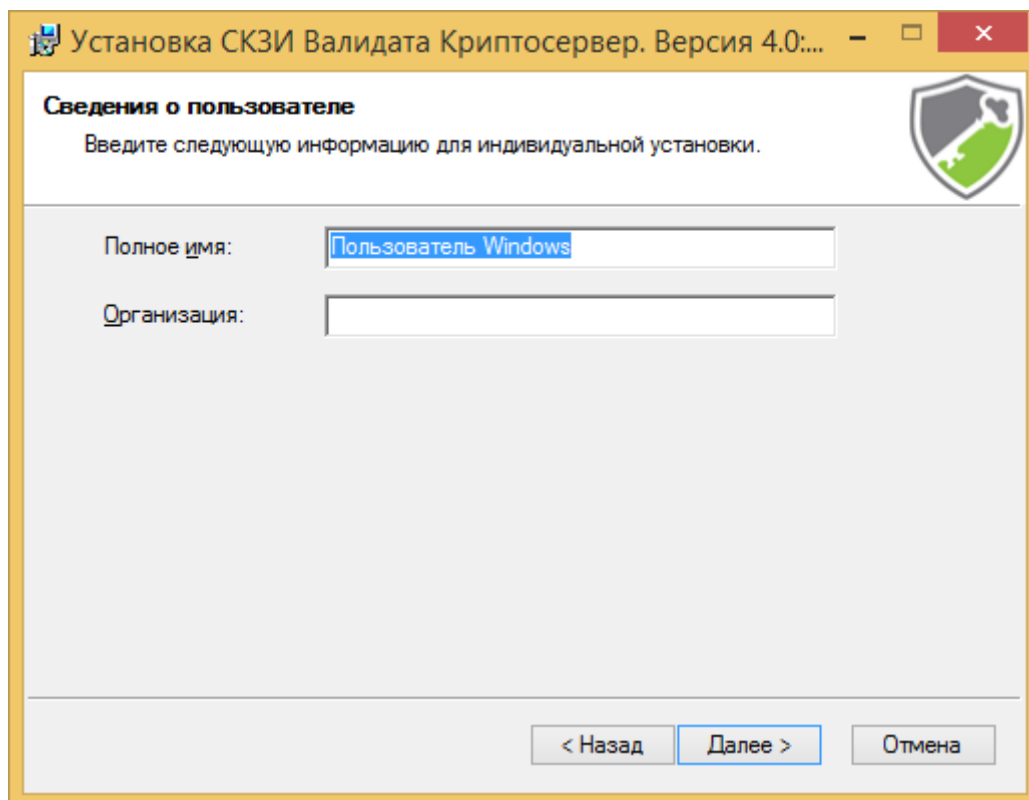


Рисунок 2 – Ввод имени пользователя

Нажмите кнопку «**Далее**». При необходимости измените папку установки по умолчанию (Рисунок 3).

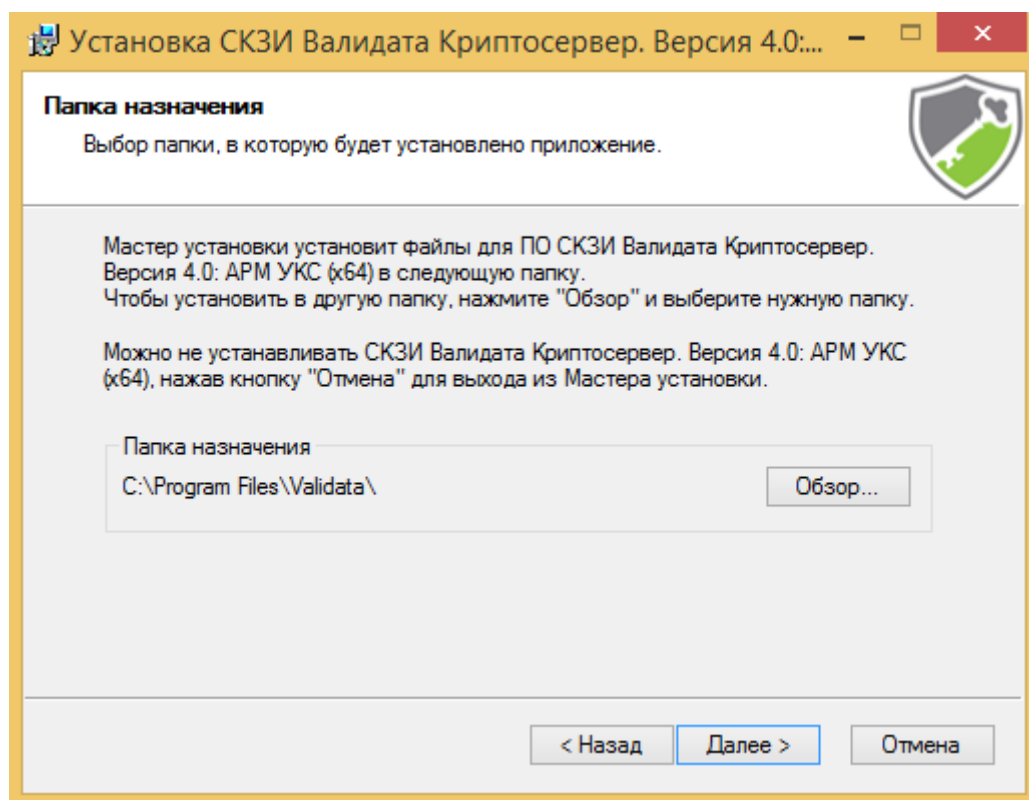


Рисунок 3 – Выбор папки установки

Нажмите кнопку «**Далее**». Выберите тип установки (Рисунок 4). «Обычная» установка устанавливает набор компонентов, необходимых для работы КС. «Полная» установка устанавливает все имеющиеся компоненты СКЗИ «Валидата Криптосервер». «Выборочная» установка позволяет пользователю вручную выбрать требуемые компоненты для установки (Рисунок 5).

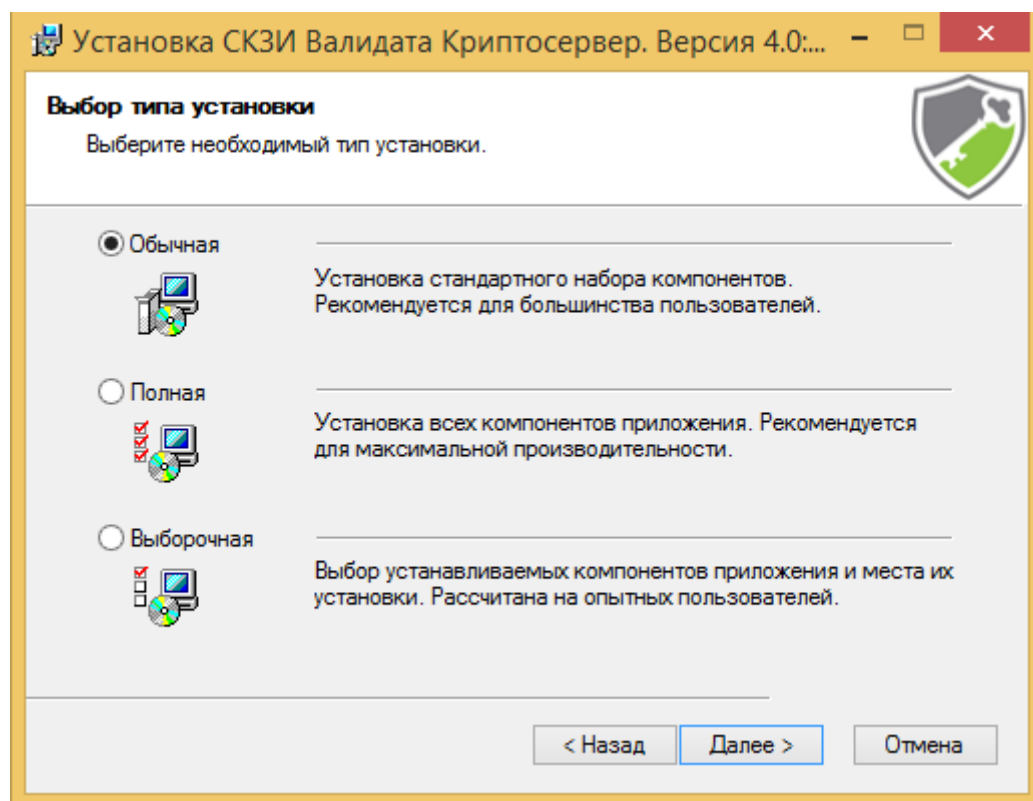


Рисунок 4 – Выбор типа установки

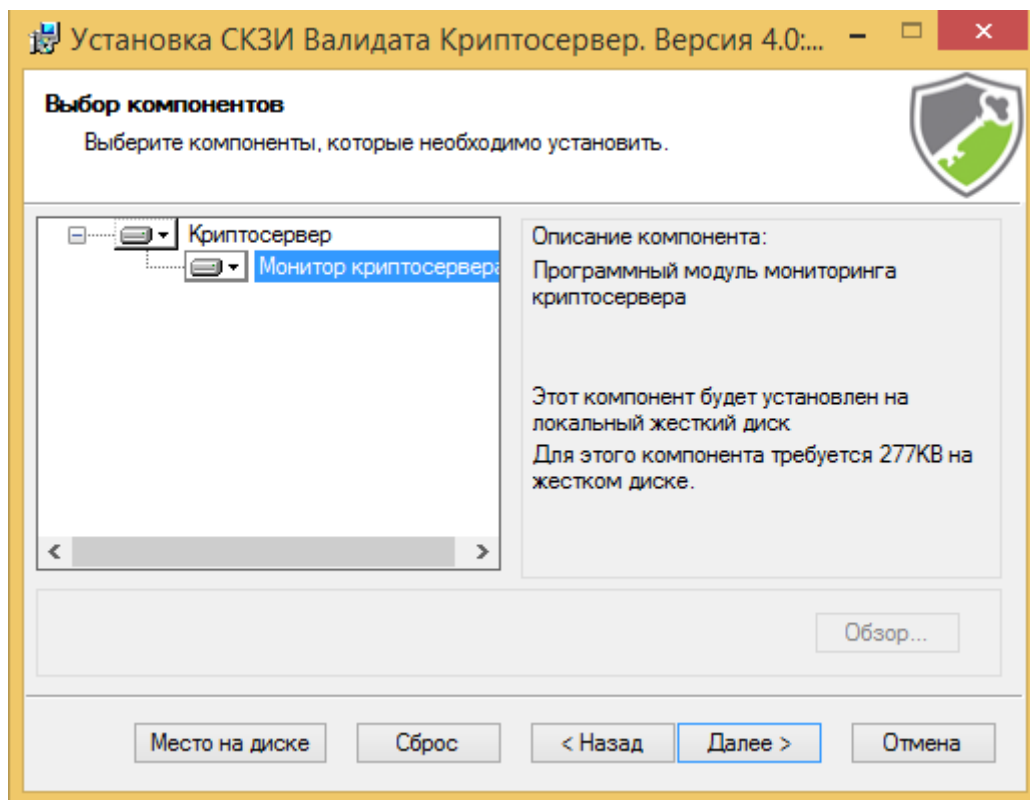


Рисунок 5 – «Выборочная» установка

Нажмите кнопку «**Далее**». Отображается диалог готовности к установке (Рисунок 6).

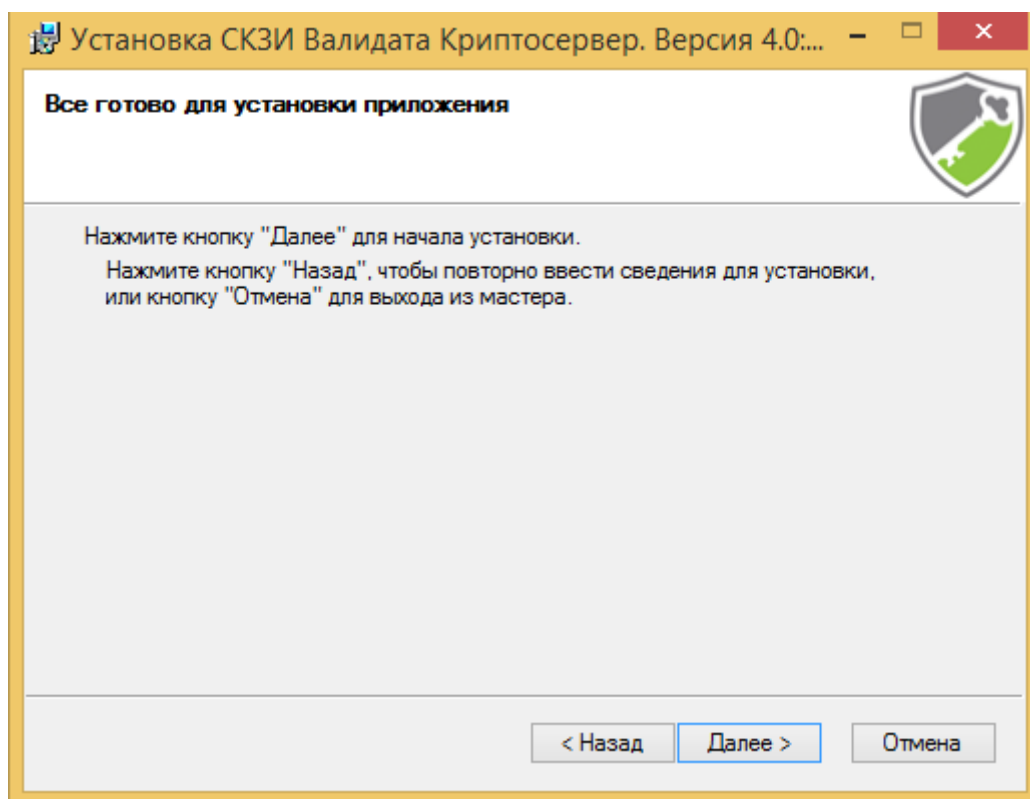


Рисунок 6 – Диалог готовности к установке

Нажмите кнопку «**Далее**». По окончании установки отображается финальный диалог мастера установки (Рисунок 7).

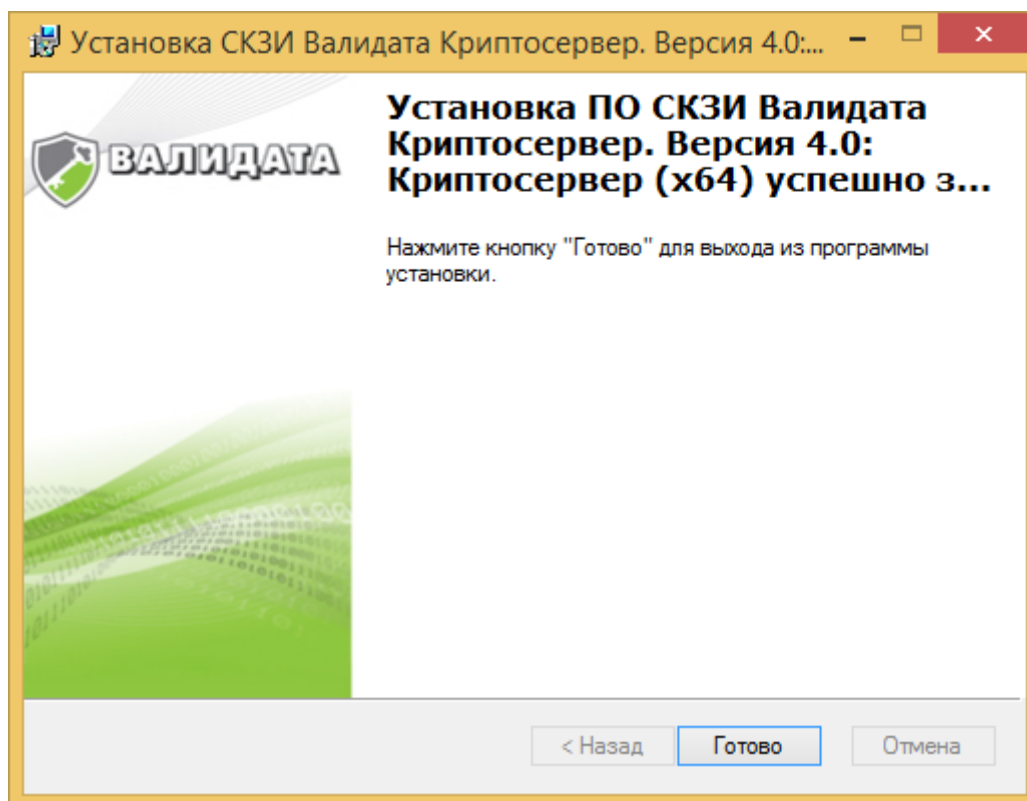


Рисунок 7 – Установка завершена

Нажмите кнопку «**Готово**» для завершения работы мастера установки.

Установка производит добавление двух сервисов ОС Microsoft Windows в режиме ручного запуска:

- *CryptoServer Logger - СКЗИ Валидата Криптосервер* - сервис сервера протоколов;
- *CryptoServer Service - СКЗИ Валидата Криптосервер* - сервис криптосервера.

Так как сервис криптосервера может отображать пользовательский интерфейс СКЗИ «Валидата CSP» для загрузки ключевой информации, то он должен выполняться под учетной записью локальной системы (SYSTEM) с включенной опцией, позволяющей работать в интерактивном режиме (Рисунок 8).



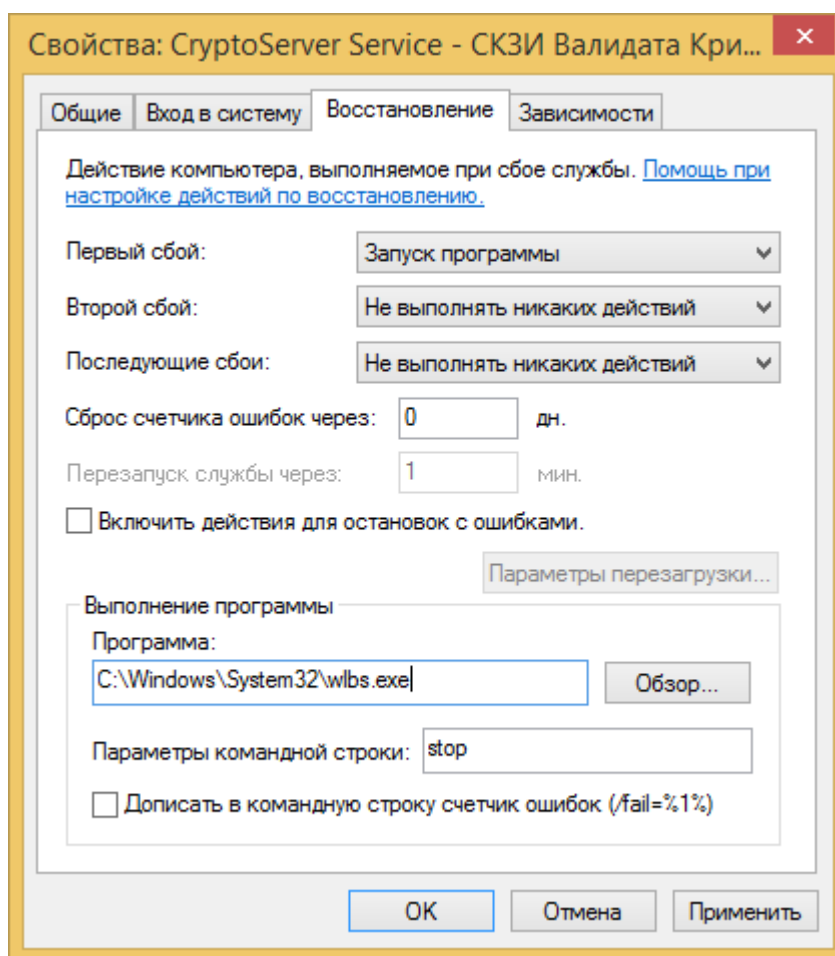


Рисунок 8 – Настройки учетной записи сервиса криптосервера

При необходимости запуска сервиса криптосервера в "тихом" режиме следует выключить опцию "Разрешить взаимодействие с рабочим столом" в настройках сервиса. При этом ключ ЭП должен быть смонтирован до запуска сервиса криптосервера, и загрузка данного ключа не должна требовать ввода пароля и/или ПИН-кода.

Сервис криптосервера зависит от сервиса сервера протоколов и сервиса "Удаленный вызов процедур" (Рисунок 9).

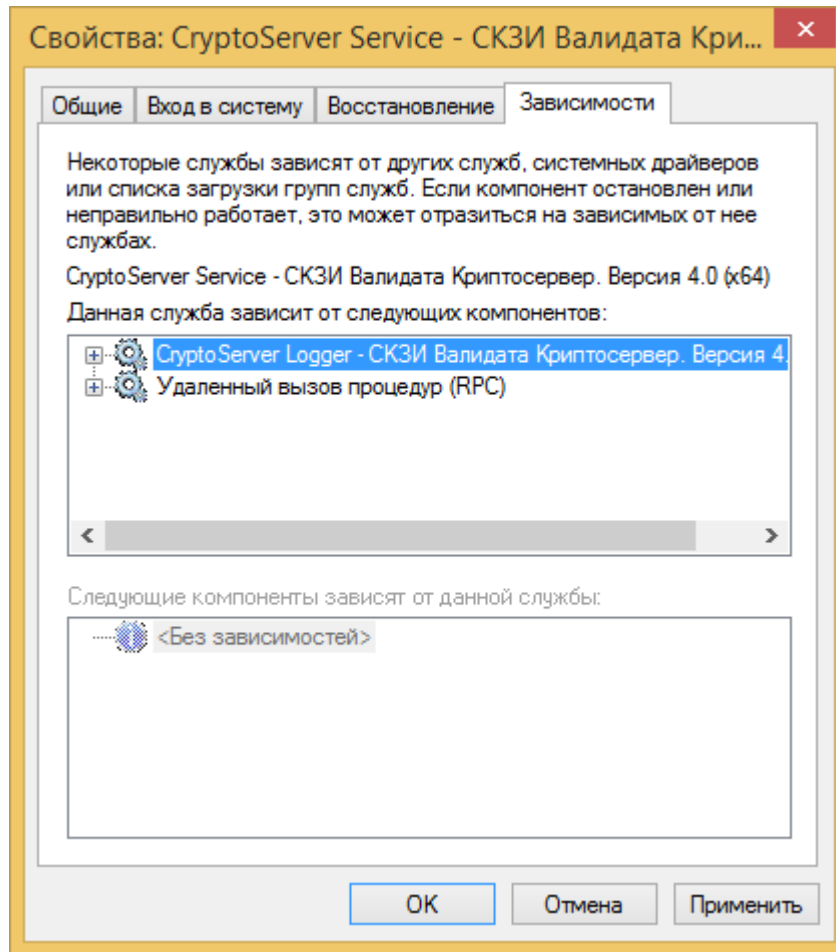


Рисунок 9 – Зависимости сервиса криптосервера

После установки, если это необходимо, можно удалить сервис криптосервера и сервис сервера протоколов из таблицы сервисов ОС Microsoft Windows, запустив исполняемые модули *cslogsvc.exe* и *zcssvc.exe* с параметром *-unregserver*, а добавить их заново можно, запустив те же модули с параметром *-regserver*.

#### 4.4 Удаление

Для удаления КС выберите пункт меню ОС Windows «Пуск» – «Панель управления» – «Удаление программ», выберите в списке пункт «**СКЗИ Валидата Криптосервер. Версия 4.0: Криптосервер**» и нажмите кнопку «Удалить».

Подтвердите действие в появившемся диалоге подтверждения удаления СКЗИ «Валидата Криптосервер».

#### 4.5 Настройка

Администратор КС осуществляет настройку СКЗИ «Валидата Криптосервер», используя права локального администратора ОС, временно предоставленные ему для этого системным администратором.

Перед настройкой криптосервера администратору КС необходимо создать рабочие справочники сессий КС.

#### **4.5.1 Создание справочников сессий криптосервера**

Администратору КС необходимо получить рабочий сертификат пользователя (сессии администрирования) в соответствии с процедурой, описанной в документе ВАМБ.00077-06 92 01 «Валидата Клиент» версия 4. Справочник сертификатов. Руководство пользователя». В сертификате сессии администрирования КС, которая будет использоваться для взаимодействия с АРМ УКС, должно присутствовать расширенное применение ключа "Сессия администрирования криптосервера" (1.3.6.1.4.1.10244.4.2.3). В локальный справочник этой сессии необходимо добавить сертификаты всех администраторов КС.

Также необходимо получить как минимум один рабочий сертификат пользователя (сессии) с расширенным применением ключа "Сессия криптосервера" (1.3.6.1.4.1.10244.4.2.1) для сессии КС, которая будет использоваться для выполнения криптографических функций.

*Примечание — Если создание локального и персонального справочника выполняется на ЭВМ, отличной от ЭВМ с установленным ПО КС, необходимо средствами ПК «Справочник сертификатов» из состава ПК «Валидата Клиент» выполнить резервное копирование персонального и локального справочников сессии, перенести копии на компьютер КС и скопировать объекты из резервной копии локального справочника в локальный справочник, расположенный в хранилище ODBC.*

#### **4.5.2 Конфигурация криптосервера**

Для запуска программы конфигурации криптосервера необходимо выбрать пункт системного меню Windows Программы -> СКЗИ Валидата Криптосервер. Версия 4.0 -> Конфигурация криптосервера.

На экране появится главное диалоговое окно программы конфигурации КС (Рисунок 10).

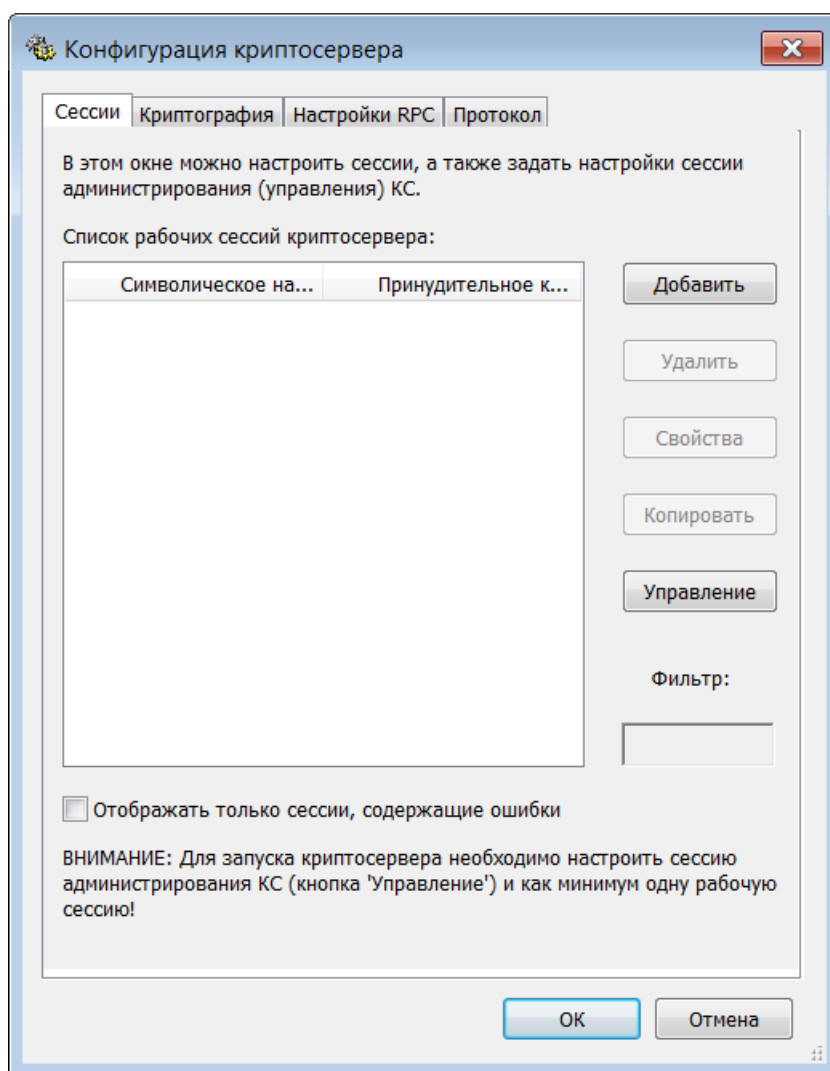


Рисунок 10 – Главное окно программы конфигурации

#### 4.5.3 Настройка сессии администрирования

Администратор криптосервера должен настроить сессию администрирования КС для взаимодействия с АРМ УКС. Для этого необходимо в главном окне программы конфигурации (Рисунок 10) нажать кнопку "Управление...". После этого появится диалоговое окно настройки сессии администрирования (Рисунок 11).

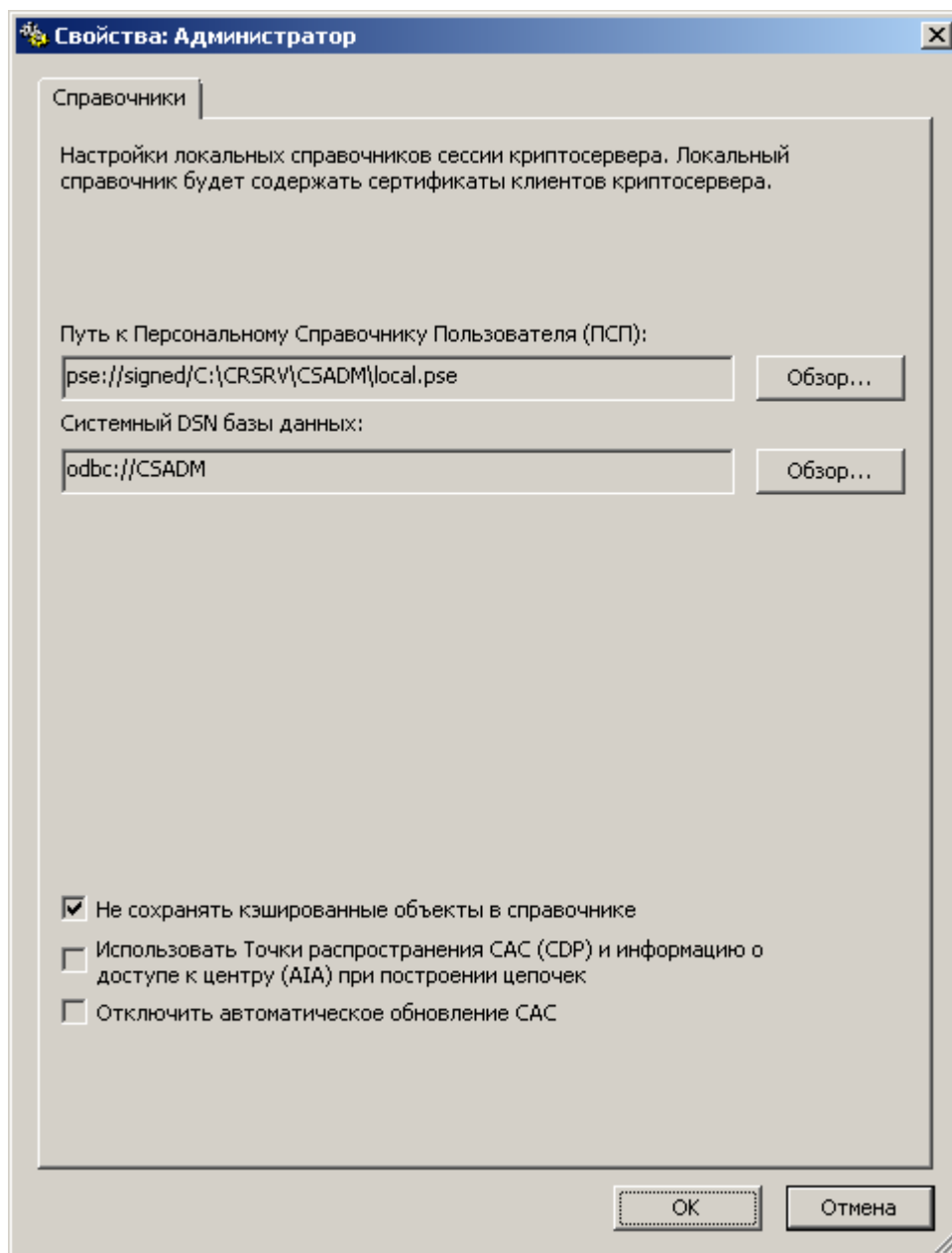


Рисунок 11 – Настройки сессии администрирования

Необходимо задать путь к персональному справочнику пользователя (ПСП) local.pse для сессии администрирования КС, а также путь к системному ODBC DSN для сессии администрирования КС. Для повышения отказоустойчивости и производительности КС рекомендуется использовать БД с интерфейсом ODBC.

#### *Примечания*

1 При использовании БД с интерфейсом ODBC в настройках КС необходимо задавать именно системное ODBC DSN, а также настроить авторизацию сервиса компьютера в БД, если используются разные серверы для КС и для БД.

2 При использовании БД с интерфейсом ODBC необходимо предварительно скопировать в эту БД объекты с помощью ПК "Справочник сертификатов".

Остальные настройки можно оставить "по умолчанию".

При взаимодействии с АРМ УКС расшифрование и проверка ЭП команд, поступающих с АРМ УКС, будут выполняться на сертификатах, находящихся в ЛСП сессии администрирования, поэтому необходимо добавить в ЛСП сертификаты всех администраторов КС.

#### **4.5.4 Настройки сессий криптосервера**

Криптосервер может поддерживать не более 16384 сессий. При этом две любые попарно различные криптографические сессии не должны иметь рабочие сертификаты с совпадающими ключами ЭП. Для работы КС необходимо настроить одну административную сессию и как минимум одну рабочую сессию.

#### **4.5.5 Добавление сессии**

Для добавления новой сессии нажмите кнопку «**Добавить**» в главном окне программы конфигурации (Рисунок 10). На экране появится диалоговое окно настройки параметров сессии КС (Рисунок 12).

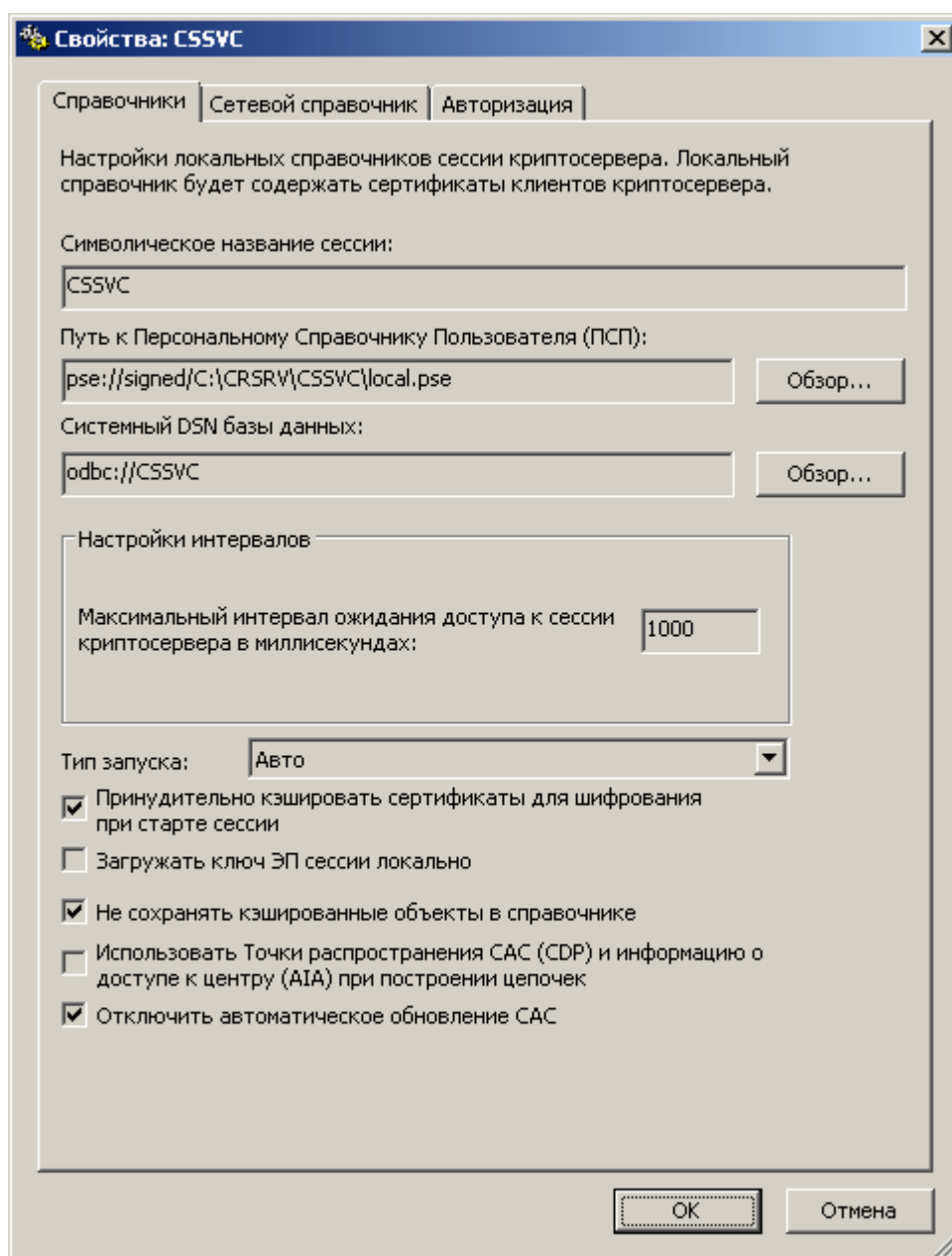


Рисунок 12 – Настройка новой сессии

Нужно ввести символическое название сессии, а также указать путь к ПСП local.pse для сессии КС и выбрать системный DSN базы данных ODBC для сессии КС.

#### Примечания

1 В настройках КС необходимо задавать системный ODBC DSN, а также настроить авторизацию сервиса компьютера в БД, если используются разные серверы для КС и для БД.

2 Необходимо предварительно скопировать в указанную БД объекты с помощью ПК "Справочник сертификатов".

Опция "**Максимальный интервал ожидания доступа к сессии криптосервера в миллисекундах**" позволяет задать время ожидания доступа к сессии криптосервера. Если заданный интервал истёк, это означает, что данная

сессия криптосервера заблокирована и не готова обрабатывать поступающие запросы. В этом случае выдаётся соответствующее сообщение об ошибке. Опция **"Принудительно кэшировать сертификаты для шифрования при старте сессии"** используется для увеличения скорости поиска сертификатов для шифрования (при этом, однако, может увеличиться время, необходимое для запуска КС). Опцию **"Загружать ключ ЭП сессии локально"** следует включить, если ключ ЭП необходимо загружать с консоли, а не через АРМ УКС. Опция **"Не сохранять кэшированные объекты в справочнике"** позволяет не добавлять в ЛСП кэшированные в сессии объекты при ее остановке. Опция **"Использовать Точки распространения САС (CDP) и информацию о доступе к центру (AIA) при построении цепочек"** разрешает доступ к точкам AIA и CDP при построении и проверке цепочек сертификатов. Опция **"Отключить автоматическое обновление САС"** позволяет отключить автоматическое обновление списков аннулированных сертификатов (САС) для сессии КС — т.е. обновление САС, выполняющееся при запуске сессии КС, а также периодическое обновление САС сессии КС. Данная опция не отключает возможность обновления САС по команде с АРМ УКС. Изменение вышеописанных опций вступает в силу только после перезагрузки сессии КС или перезапуска КС целиком.

Остальные настройки можно оставить по умолчанию.

*Примечание — В связи с тем, что при включенной опции **"Принудительно кэшировать сертификаты для шифрования при старте сессии"** процесс кэширования сертификатов протекает в многопоточном режиме, необходимо включить многопоточную обработку для локальных справочников, расположенных в хранилище ODBC (см. пункт 4.12.2). Для локальных справочников, расположенных в хранилищах других типов, данная опция не поддерживается.*

Если для работы данной сессии необходимо использование сетевого справочника сертификатов, находящегося на LDAP-сервере, то следует выбрать закладку **"Сетевой справочник"** (Рисунок 13), включить опцию **"Использовать сетевой справочник сертификатов"** и заполнить следующие параметры:

- адрес LDAP-сервера (доменное имя или IP-адрес) и порт (по умолчанию используется 389 TCP-порт);
- базовый DN для подключения к LDAP-серверу (например, `cn=users,dc=x509,dc=ru`);
- параметры аутентификации (метод аутентификации, имя и пароль). При выборе метода аутентификации Negotiate или NTLM при работе с Microsoft Active Directory (AD) может использоваться встроенная аутентификация ОС Windows и, следовательно, возможно не задавать имя и пароль.



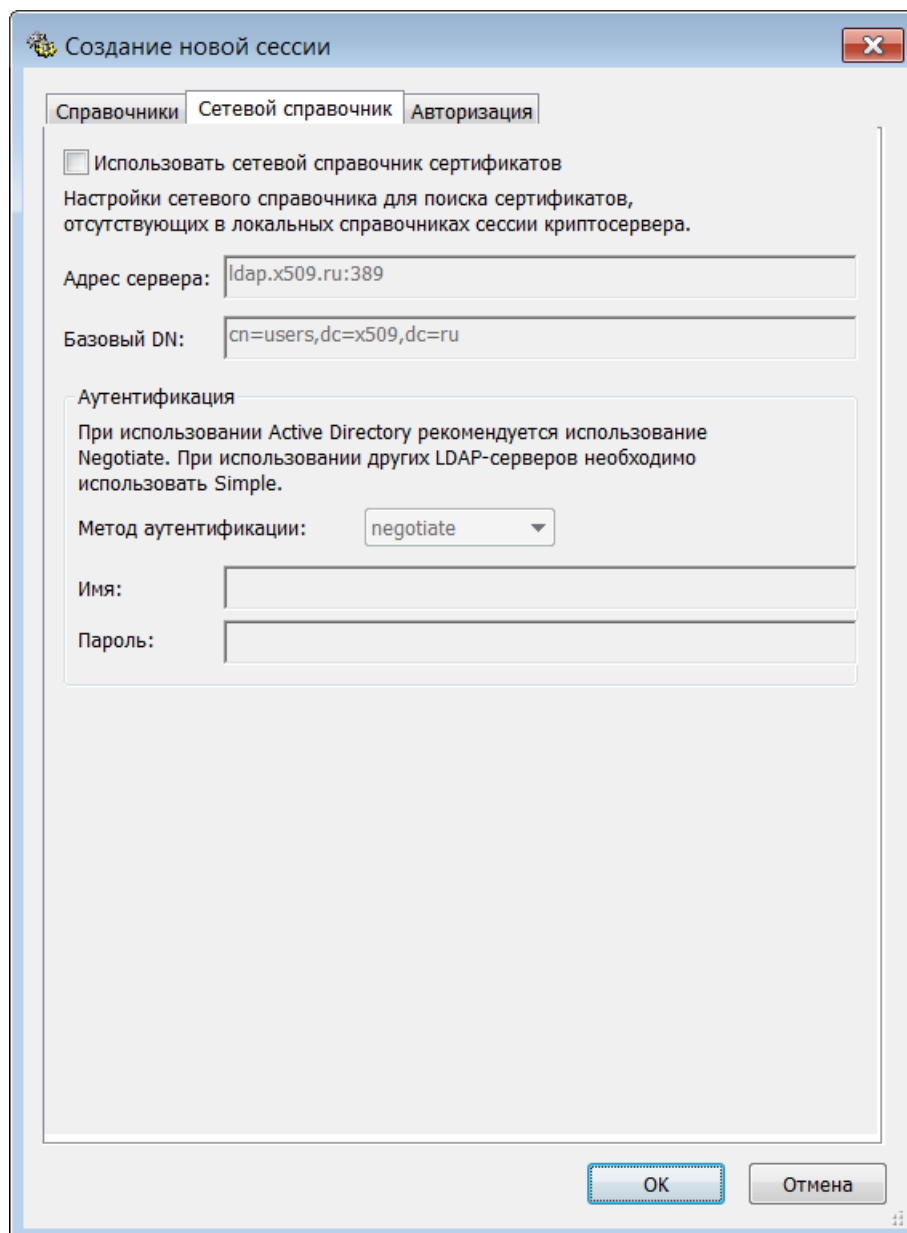


Рисунок 13 – Настройка сетевого справочника сессии

#### 4.5.6 Настройка авторизации при работе с сессией

Для настройки авторизации при работе с сессией криптосервера на вкладке "Авторизация" (Рисунок 14) необходимо включить опцию **"Использовать авторизацию при работе с сессией криптосервера"** и настроить список авторизованных подключений для данной сессии.

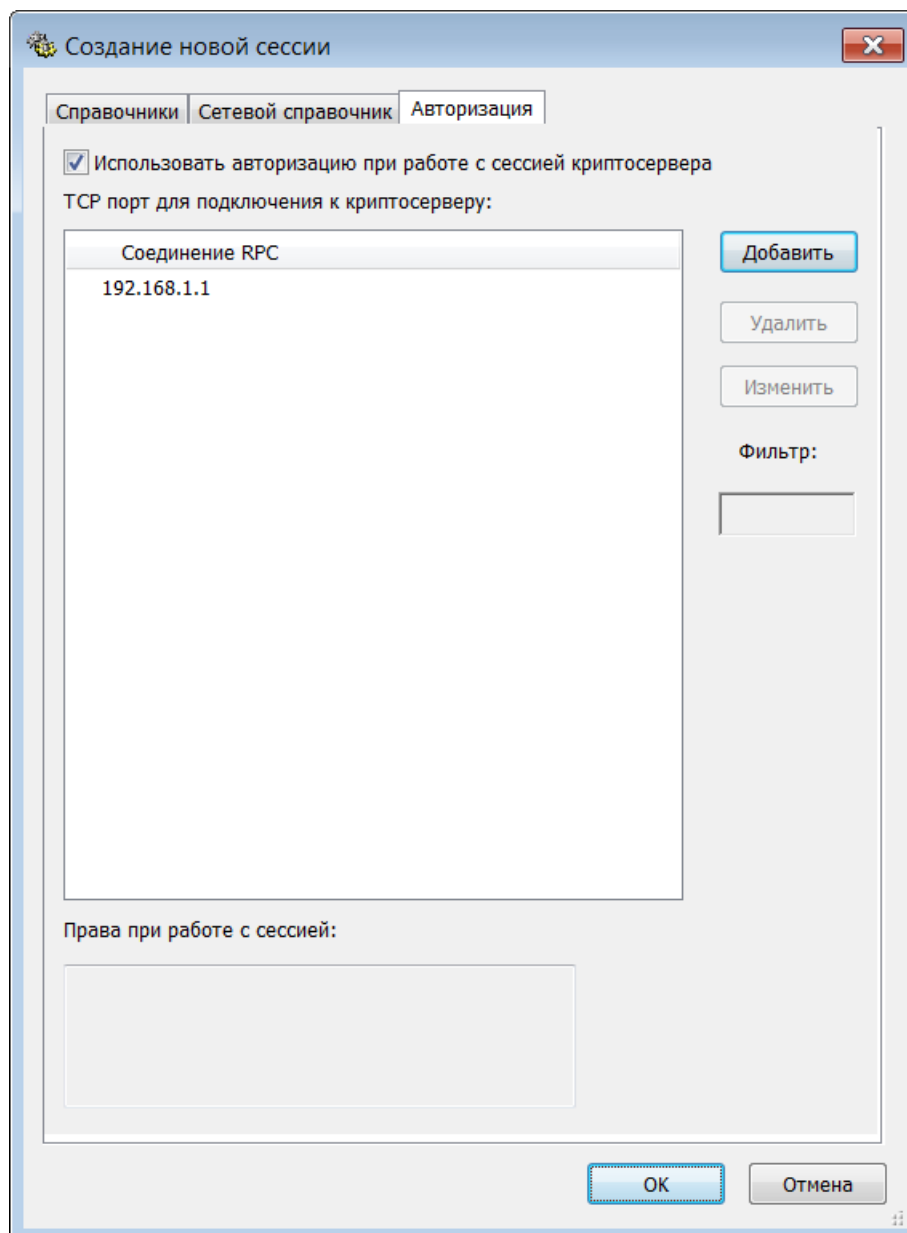


Рисунок 14 – Настройка авторизации сессии

Для добавления нового авторизованного подключения к сессии необходимо нажать кнопку **"Добавить"** и заполнить данные авторизации в диалоговом окне (Рисунок 15).

Необходимо указать IP-адрес компьютера, с которого будет производиться работа с сессией, ввести данные аутентификации (длиной не менее 8-и символов), и отметить разрешенные для данного авторизованного подключения операции (**"Разрешить выполнение зашифрования"**, **"Разрешить выполнение расшифрования"**, **"Разрешить вычисление ЭП"**, **"Разрешить добавление сертификата"**, **"Разрешить добавление САС"**). После этого необходимо нажать кнопку **"ОК"** для сохранения настроек.

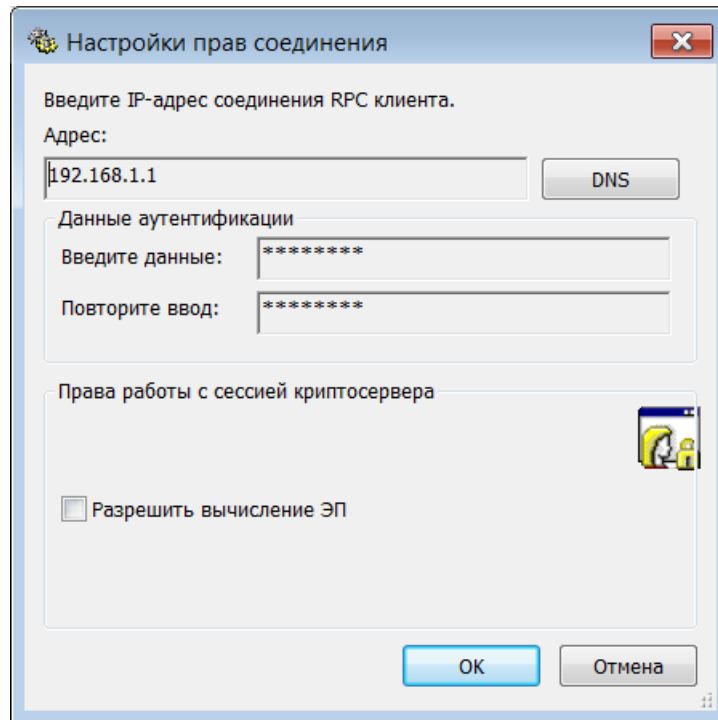


Рисунок 15 – Настройка авторизованного подключения

*Примечание – Рекомендуется, чтобы данные аутентификации не хранились в конфигурации прикладного процесса, а вводились администратором информационной безопасности при его запуске и сразу после использования в функции установки аутентификационных данных ППИ криптосервера уничтожались или маскировались в памяти.*

Для удаления авторизованного подключения необходимо нажать кнопку **"Удалить"** (Рисунок 14). Для изменения настроек авторизованного подключения или изменения данных аутентификации необходимо нажать кнопку **"Изменить"** (Рисунок 14) и выполнить редактирование данных в диалоговом окне (Рисунок 15).

Работающий криптосервер автоматически определит, что были внесены изменения в настройки авторизации сессии, и перечитает измененные настройки.

#### **4.5.7 Удаление сессии**

Для удаления сессии КС необходимо указать в списке (Рисунок 10) удаляемую сессию и нажать кнопку **"Удалить"**.

#### **4.5.8 Изменение параметров сессии**

Для изменения параметров сессии КС необходимо выделить в списке (Рисунок 10) сессию и нажать кнопку **"Свойства"**. После этого в диалоговом окне установки параметров сессии следует внести все необходимые изменения и нажать кнопку **"ОК"**.

## 4.6 Настройка параметров криптографии

Для настройки параметров криптографии в главном диалоговом окне конфигурационной программы (Рисунок 10) выберите закладку "**Криптография**" (Рисунок 16):

- **период обновления списка аннулированных сертификатов** – указывается в минутах;
- **использовать многопоточную обработку** – включение многопоточной (параллельной) обработки;
- **включить индексирование идентификаторов ключей владельцев** – при включенном индексировании поиск по идентификатору ключа владельца будет выполняться исключительно по индексу;
- **включить индексирование идентификаторов ключей ЭП** – при включенном индексировании поиск по идентификатору ключа ЭП будет выполняться исключительно по индексу;
- **включить индексирование частей OU RDN имён владельцев** – при включенном индексировании поиск по части типа OU имени владельца будет выполняться исключительно по индексу;
- **количество корзин для хранения объектов** – кэш представляет собой упорядоченный список корзин, каждая из которых в свою очередь представляет собой упорядоченный список объектов системы управления сертификатами (СУС). Для повышения производительности рекомендуется наличие в корзине в среднем не более 1024 объектов СУС. Увеличение количества корзин приводит к повышению производительности, однако при этом увеличиваются требования к используемым ресурсам.

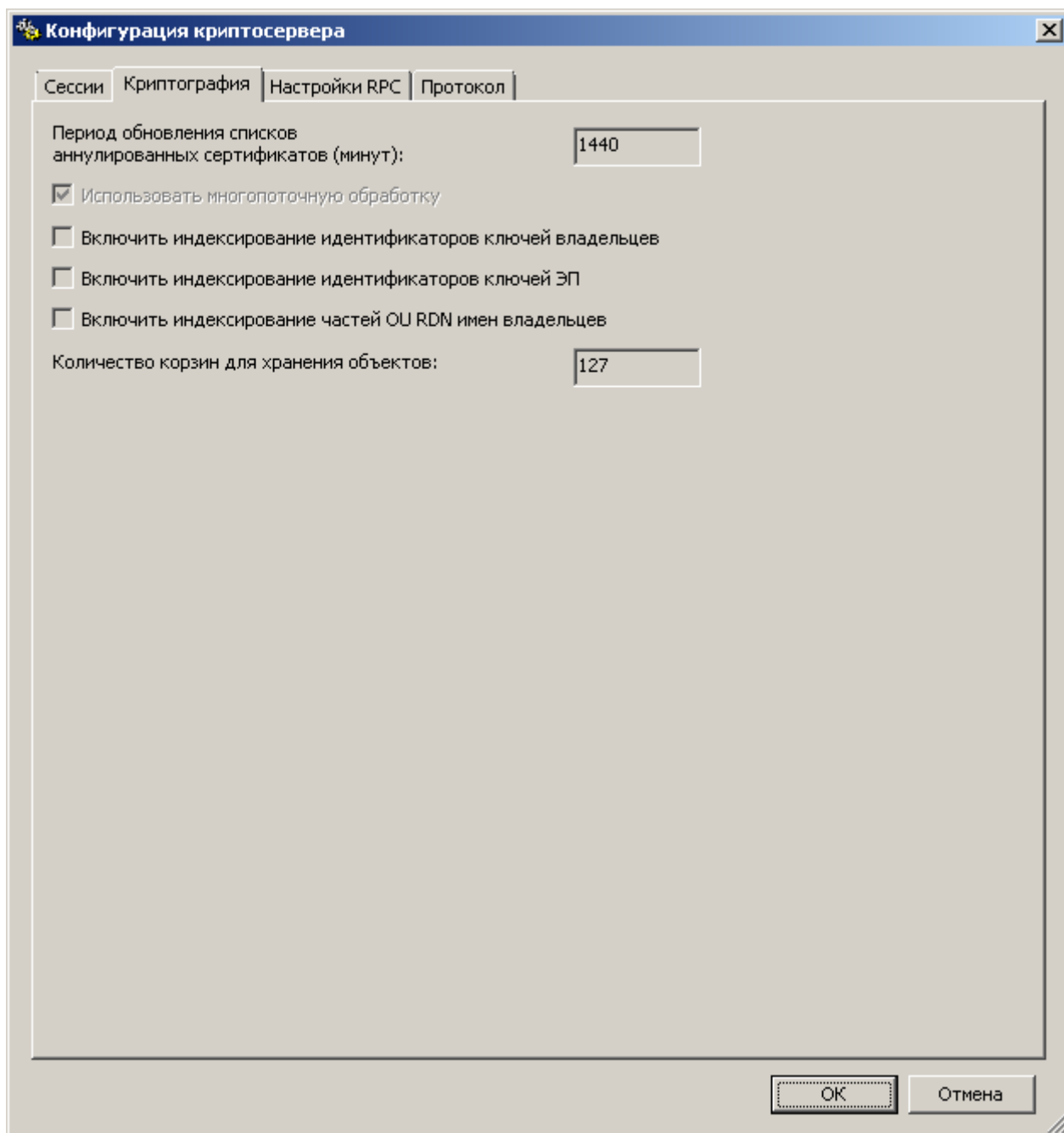


Рисунок 16 – Настройка параметров криптографии

*Примечание - Команда обновления САС может быть также подана с АРМ УКС.*

#### 4.7 Настройка параметров DCE-RPC

Криптосервер отвечает на все запросы прикладного ПО по протоколу DCE-RPC. Для настройки параметров DCE-RPC в главном диалоговом окне конфигурационной программы (Рисунок 10) выберите закладку **"Настройки RPC"** (Рисунок 17).

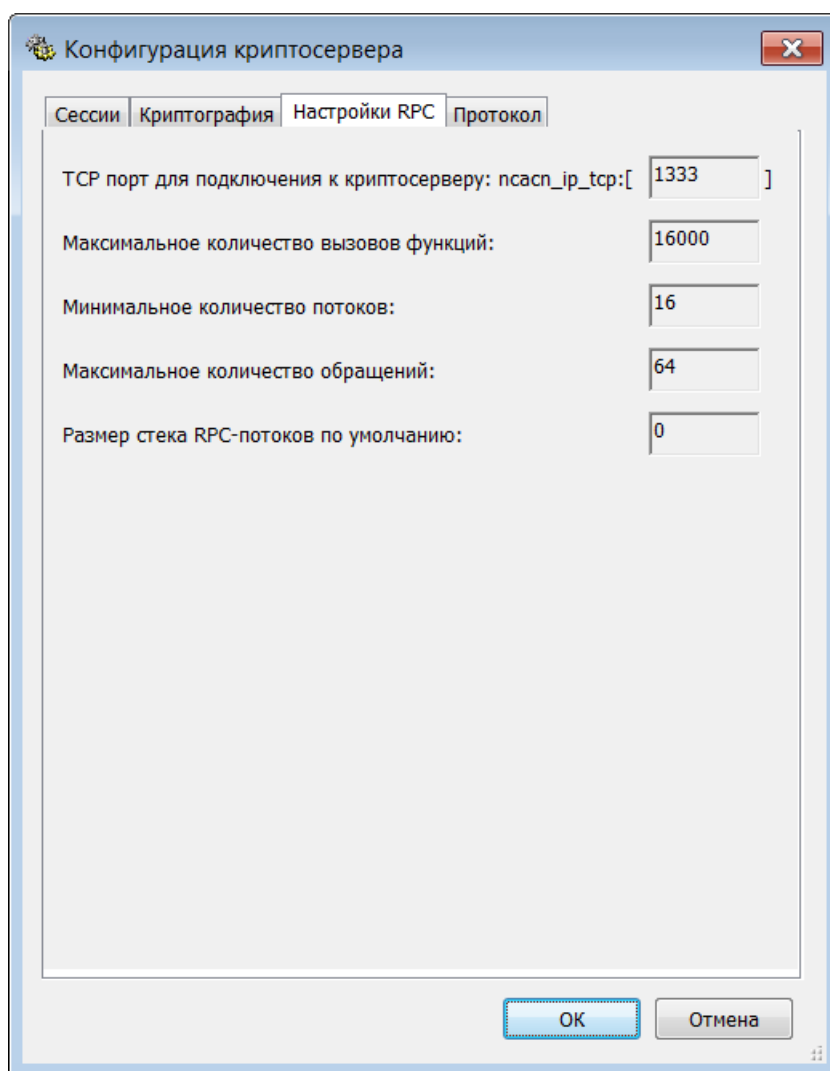


Рисунок 17 – Настройка параметров DCE-RPC

Параметры протокола DCE-RPC рекомендуется оставить по умолчанию (при большом количестве запросов от прикладного ПО рекомендуется увеличить минимальное количество потоков и максимальное количество обращений к КС).

#### 4.8 Настройка журнала работы криптосервера

КС ведет журнал событий и ошибок в виде файлов протоколов. Для настройки журнала в главном диалоговом окне конфигурационной программы (Рисунок 10) выберите закладку **"Протокол"** (Рисунок 18).

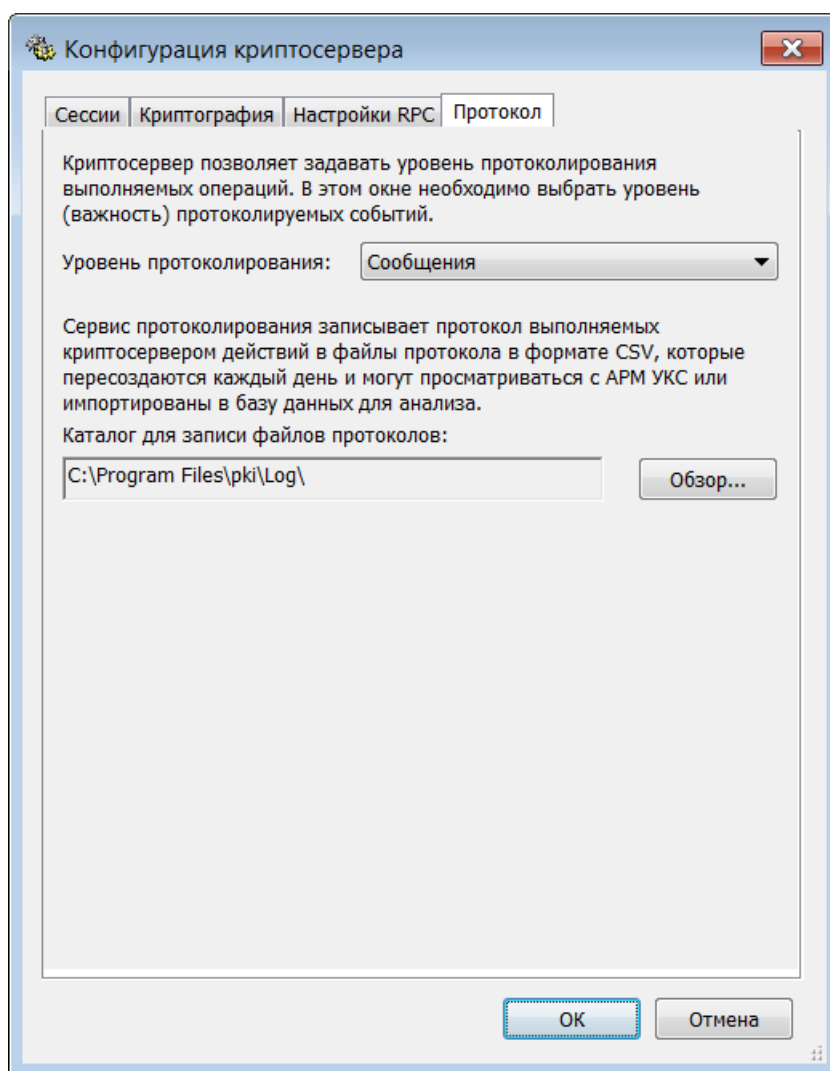


Рисунок 18 – Настройка журнала работы криптосервера

Необходимо задать уровень протоколируемых событий:

- *Ошибки* - протоколировать только ошибки;
- *Сообщения* - протоколировать сообщения и ошибки;
- *Аудит отказов* - протоколировать ошибки при авторизации, подключения, сообщения и ошибки;
- *Аудит успехов* - протоколировать успешные авторизации, ошибки при авторизации, подключения, сообщения и ошибки;
- *Отладочную информацию* - протоколировать отладочную информацию, успешные авторизации, ошибки при авторизации, подключения, сообщения и ошибки подключения, сообщения и ошибки;
- *Выполнение функций (трассировка)* - протоколировать этапы выполнения функций криптосервера.

Дополнительно необходимо указать каталог, в котором будут создаваться файлы протоколов в формате CSV с именами YYYYMMDD.CSV (где YYYY - год, MM - месяц, DD - день).

Для возможности получения файлов протоколов по сети на APM UKS админи-

стратором криптосервера необходимо разрешить доступ на чтение к каталогу, в котором создаются эти файлы. Правом на запись в данный каталог должна обладать лишь учетная запись локальной системы (SYSTEM).

Работающий криптосервер автоматически определит, что были внесены изменения в настройки уровня протоколирования, и перечитывает измененные настройки.

## 4.9 Организация удаленного доступа к файлу протокола

Для организации доступа к файлам протоколов с АРМ УКС на КС необходимо предоставить возможность удаленного доступа к этим файлам. Для этого администратор информационной безопасности должен запустить в ОС Windows проводник и, щелкнув правой кнопкой мыши на каталоге, в котором будут создаваться файлы протоколов, выбрать пункт меню для предоставления общего доступа к файлам **«Поделиться»** – **«Расширенная настройка общего доступа»**. Далее необходимо нажать кнопку **«Расширенная настройка»** и в появившемся диалоговом окне установить параметр **«Открыть общий доступ к этой папке»**, задать **«Имя общего ресурса»**, число одновременных подключений оставить по умолчанию и нажать **«ОК»**.

## 4.10 Формат журнала работы криптосервера

Журнал работы КС, в который записывается информация об ошибках и других событиях, ведется в текстовом формате в файлах протоколов, имеющих расширение **.csv** и содержащих в своем имени дату наступления протоколируемых событий в формате **YYYYMMDD**, где **YYYY** – год (например, 2019), **MM** – месяц (от 01 до 12), **YY** – день (от 01 до 31).

Информация об ошибках всегда протоколируется параллельно в двух файлах протоколов – общем файле и файле ошибок, причем файл ошибок имеет в своем имени префикс **Err**. Информация обо всех остальных событиях протоколируется исключительно в общем файле протоколов.

Информация об ошибках и событиях протоколируется в виде строк (записей), разделенных запятыми на одиннадцать полей. Информация о конкретной ошибке или событии может содержать одну или несколько таких строк (записей).

Описание полей строк (записей) приведено ниже (Таблица 1).



Таблица 1 - Описание полей строк (записей) протоколов

<b>Поле</b>	<b>Описание содержимого поля</b>	<b>Пример содержимого поля (численные значения приведены в шестнадцатеричной системе счисления)</b>
№1	Время и дата создания записи, с точностью до миллисекунд	01/01/2019 01:01:01:001
№2	Имя узла КС	CRSRV2016
№3	Идентификатор процесса КС	000012AB
№4	Идентификатор потока КС	000089EF
№5	Идентификатор источника записи	Подсистема протоколирования -- 30 Сервисный процесс КС — 40 Прикладной программный интерфейс -- 70 Подсистема конфигурирования — 71 Подсистема администрирования -- 72 Подсистема библиотеки СУС — 80
№6	Идентификатор важности записи	Критическая ошибка -- 20 Некритическая ошибка — 30 Сообщение предупреждения — 40 Информационное сообщение — 60 Аудит отказа — 66 Аудит успеха — 67 Отладочная информация — 70 Данные трассировки — 80
№7	Функция, инициировавшая протоколирование записи	Добавление сертификата — 0008 Добавление САС — 0009 Команда управления с АРМ УКС -- 0030 Присоединение ЭП к CMS сообщению - 0025 Получение информации о CMS сообщении - 0041 Расшифрование CMS сообщения - 0006 Удаление сертификата или САС — 0020 Отсоединение ЭП от CMS сообщения - 0024 Зашифрование CMS сообщения - 0005 Перебор сертификатов или САС справочников - 0042

Поле	Описание содержимого поля	Пример содержимого поля (численные значения приведены в шестнадцатеричной системе счисления)
		<p>Формирование запроса PKCS#10/на аннулирование/прекращение действия или добавление сертификата/CAC в системное хранилище — 0023</p> <p>Поиск сертификата по заданному шаблону — 0019</p> <p>Проверка соответствия сертификата заданному шаблону -- 001A</p> <p>Вычисление хэш-значения данных - 0002</p> <p>Импорт сертификата или CAC, в том числе из обновления -- 0022</p> <p>Базовая инициализация КС -- 0016</p> <p>Получение OCSP статуса для сертификата - 0043</p> <p>Проверка OCSP статуса для сертификата - 0044</p> <p>Изменение или обновление настроек КС - 0021</p> <p>Формирование случайной последовательности — 000E</p> <p>Инициализация сессии КС -- 0011</p> <p>Вычисление ЭП CMS сообщения -- 0003</p> <p>Вычисление ЭП хэш-значения -- 0026</p> <p>Простановка штампа времени -- 0045</p> <p>Проверка штампа времени — 0046</p> <p>Обновление CAC сессии КС — 000F</p> <p>Проверка ЭП CMS сообщения — 0004</p> <p>Построение и проверка цепочки сертификата — 001D</p> <p>Проверка ЭП хэш-значения — 0027</p> <p>Построение и проверка цепочки сертификата или CAC -- 0037</p>

Поле	Описание содержимого поля	Пример содержимого поля (численные значения приведены в шестнадцатеричной системе счисления)
№8	Результат выполнения функции	00000000
№9	Идентификатор удаленного клиента	ncasn_ip_tcp:192.168.0.1
№10	Идентификатор сессии КС с идентификатором ключа ЭП или именем владельца рабочего сертификата	CONTROL[2254MFPPQA01]
№11	Дополнительная информация	<p>Построение и проверка цепочки сертификата [флаги: 000000CF]  (w:\vd\pki\crsrv\crypt\apiinfo.c:1100)  Поля сертификата.....: 4000E067  Серийный номер.....:  40:50:15:90:DB:10:65:1D:7E:48:64:6F:59:F6:E6:61  Издатель.....: CN=17svc-CA-test,OU=PKI,OU=Vladimir,DC=region,DC=x509,DC=ru  Владелец.....: CN=17AdmUKS,CN=CS,OU=ТЕСТ СУС,OU=PKI,OU=Vladimir,DC=region,DC=x509,DC=ru  Действителен с.....: Mon Oct 30 11:44:20 2017  Действителен по.....: Thu Jan 31 02:59:00 2019  Ключ ЭП действителен с.....:  Mon Oct 30 11:44:20 2017  Ключ ЭП действителен по.....:  Thu Jan 31 02:59:00 2019  Идентификатор ключа ЭП.....: 8909QQBQWU01</p>

## 4.11 Завершение конфигурации криптосервера

Для завершения конфигурации криптосервера и сохранения всех внесенных изменений нажмите кнопку "ОК" (Рисунок 18).

## 4.12 Настройки операционной системы

### 4.12.1 Настройки параметров ОС Microsoft Windows

Для возможности подключения к криптосерверу необходимо разрешить анонимный доступ клиентов по протоколу DCE-RPC, а также получение портов опубликованных DCE-RPC интерфейсов. Дополнительно необходимо разрешить системным сервисам отображать пользовательский интерфейс (диалоговые окна). Данные настройки выполняются посредством редактирования Реестра ОС (после выполнения настроек необходима перезагрузка ОС).

Разрешение анонимного доступа по протоколу DCE-RPC:

- ключ реестра: *HKLM\SOFTWARE\Policies\Microsoft\Windows NT\RPC*;
- параметр: *RestrictRemoteClients*;
- тип: *REG\_DWORD*;
- значение: *0* (по умолчанию используется *1*).

Разрешение анонимного получения порта опубликованного DCE-RPC интерфейса (если порт не задаётся в точке подключения):

- ключ реестра: *HKLM\SOFTWARE\Policies\Microsoft\Windows NT\RPC*;
- параметр: *EnableAuthEpResolution*;
- тип: *REG\_DWORD*;
- значение: *1* (по умолчанию используется *0*).

Разрешение отображения пользовательского интерфейса (диалоговых окон) системными сервисами:

- ключ реестра: *HKLM\SYSTEM\CurrentControlSet\Control\Windows*;
- параметр: *NoInteractiveServices*;
- тип: *REG\_DWORD*;
- значение: *0* (по умолчанию используется *1*).

### 4.12.2 Настройки параметров СКЗИ «Валидата Криптосервер»

Для обеспечения высокопроизводительной криптографической обработки с большим количеством (до 1000000 и более) сертификатов пользователей, криптосервер СКЗИ «Валидата Криптосервер» поддерживает дополнительные настройки. Данные настройки выполняются посредством редактирования Реестра ОС (после выполнения настроек необходима перезагрузка криптосервера).

Описание конфигурационных параметров приведено в разделе 1.3.5 документа ВАМБ.00077-06 33 01 «Валидата Клиент» версия 4. Руководство программиста».

### 4.13 Установка и настройка базы данных

Описание процедуры установки и настройки базы данных приведено в документе ВАМБ.00077-06 91 01 «“Валидата Клиент” версия 4. Руководство по установке и настройке». Для СКЗИ «Валидата Криптосервер» использование базы данных является обязательным.

### 4.14 Настройка кластера криптосерверов

Кластер криптосерверов СКЗИ «Валидата Криптосервер» обеспечивает возможность масштабирования, то есть возможность работы криптосерверов на нескольких ЭВМ, обеспечивая распределение запросов, поступающих от прикладного программного обеспечения (ППО); и увеличение пропускной способности криптографической подсистемы, а также повышение ее отказоустойчивости.

#### 4.14.1 Общее описание

Криптосервер представляет собой приложение, использующее интерфейс удалённого вызова процедур (Remote Procedure Call, RPC). Интерфейс взаимодействия не зависит от используемого сетевого протокола и типа ОС, а также от языка программирования, на котором написано ППО. Системный сервис RPC, обеспечивающий возможность использования RPC, входит в поставку ОС Microsoft Windows.

#### 4.14.2 Описание механизма распределения нагрузки

Обеспечение масштабирования требует эффективной технологии кластеризации на базе стандартных аппаратных компонентов и коммуникационных протоколов. В качестве решения, реализующего кластер криптосерверов, выбрана служба “Балансировка сетевой нагрузки” (Network Load Balancing, NLB), входящая в поставку серверных ОС Microsoft Windows и расширяющая масштабируемость и отказоустойчивость TCP/IP приложений на платформе ОС Microsoft Windows.

#### 4.14.3 Установка и настройка службы “Балансировка сетевой нагрузки”

Службу “Балансировка сетевой нагрузки” следует устанавливать как компонент ОС Microsoft Windows Server с аналогичным названием, используя процедуру установки компонент ОС из состава **Диспетчера сервера**.

Служба работает как дополнительный сервис для подключений по локальной сети (Local Area Network, LAN) через выделенный сетевой адаптер (кластерный адаптер), при этом не предъявляются специальные требования к аппаратуре (могут использоваться почти все сетевые адаптеры Ethernet и FDDI).

После включения службы “Балансировка сетевой нагрузки” следует выполнить ее настройку:

- кластеру присваивается единый виртуальный IP-адрес, который используется для идентификации всего кластера. Каждому узлу кластера должен быть присвоен выделенный IP-адрес для передачи трафика данному конкретному узлу (например, для управления узлом). Сетевой трафик, предназначенный для

данного адреса, не обрабатывается службой;

- каждому узлу кластера присваивается его вес (приоритет). Узел с наивысшим весом (наименьшим по значению) называется основным узлом, и отвечает, в том числе, за распределение нагрузки между узлами кластера;

- назначаются правила балансировки сетевого трафика для указанного диапазона TCP/UDP портов. При использовании многоузловой балансировки нагрузки, входящие клиентские запросы распределяются по всем узлам кластера, в зависимости от их веса и загруженности. При использовании одноузловой балансировки, входящие клиентские запросы направляются на узел с наивысшим весом для обработки. Если требуется, чтобы клиентские запросы от конкретного IP-адреса или подсети обрабатывались на конкретном узле кластера, следует использовать настройку сродства клиента.

В состав службы "Балансировка сетевой нагрузки" входит программа удаленного управления (*wlbs.exe*), которая позволяет администратору опрашивать состояние и управлять узлами кластера (например, удалять узел из кластера). Эта программа может быть использована для автоматизации управления кластером. Все удалённые команды защищаются на пароле.

При использовании службы "Балансировка сетевой нагрузки" все криптосерверы должны быть настроены одинаково (они должны использовать одинаковые справочники сертификатов и сетевые справочники, и иметь одинаковые настройки сессий) и запущены на всех узлах кластера. Для выполнения обслуживания и/или обновления ПО на криптосервере необходимо придерживаться следующей процедуры:

- вывести криптосервер из состава кластера;
- остановить процесс криптосервера;
- выполнить обслуживание криптосервера и/или обновить ПО;
- запустить процесс криптосервера и (при необходимости) загрузить ключи ЭП;
- ввести криптосервер в состав кластера.

При использовании службы "Балансировка сетевой нагрузки" каждый узел кластера получает каждый входящий IP-пакет, но обрабатывает его только один из узлов. Узлы кластера одновременно обрабатывают запросы разных клиентов, что позволяет уменьшить время отклика. Узлы кластера обмениваются тактовыми сообщениями для управления составом кластера и, в случае выключения одного из узлов, другие узлы перераспределяют сетевой трафик, одновременно предоставляя постоянный сервис клиентам. Для сохранения сведений о состоянии соединения для каждой сессии может использоваться настройка сродства клиента.

#### **4.15 Настройка узла кластера криптосерверов**

Для того, чтобы выполнить настройку службы "Балансировка сетевой нагрузки", необходимо открыть диалог настроек выделенного сетевого адаптера и включить службу "Балансировка сетевой нагрузки" (Рисунок 19).

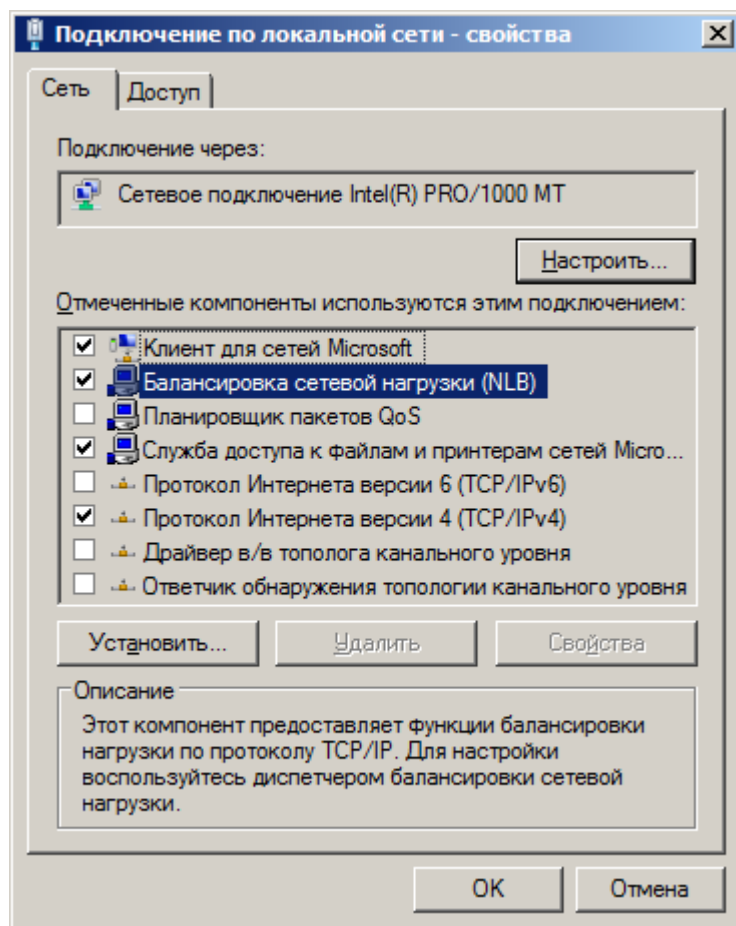


Рисунок 19 – Включение службы балансировки сетевой нагрузки

Далее следует перейти к настройкам кластера криптосерверов, запустив **Диспетчер балансировки сетевой нагрузки** (последующие настройки следует выполнить на всех узлах кластера). Вначале необходимо назначить виртуальный IP-адрес кластера (Рисунок 20).

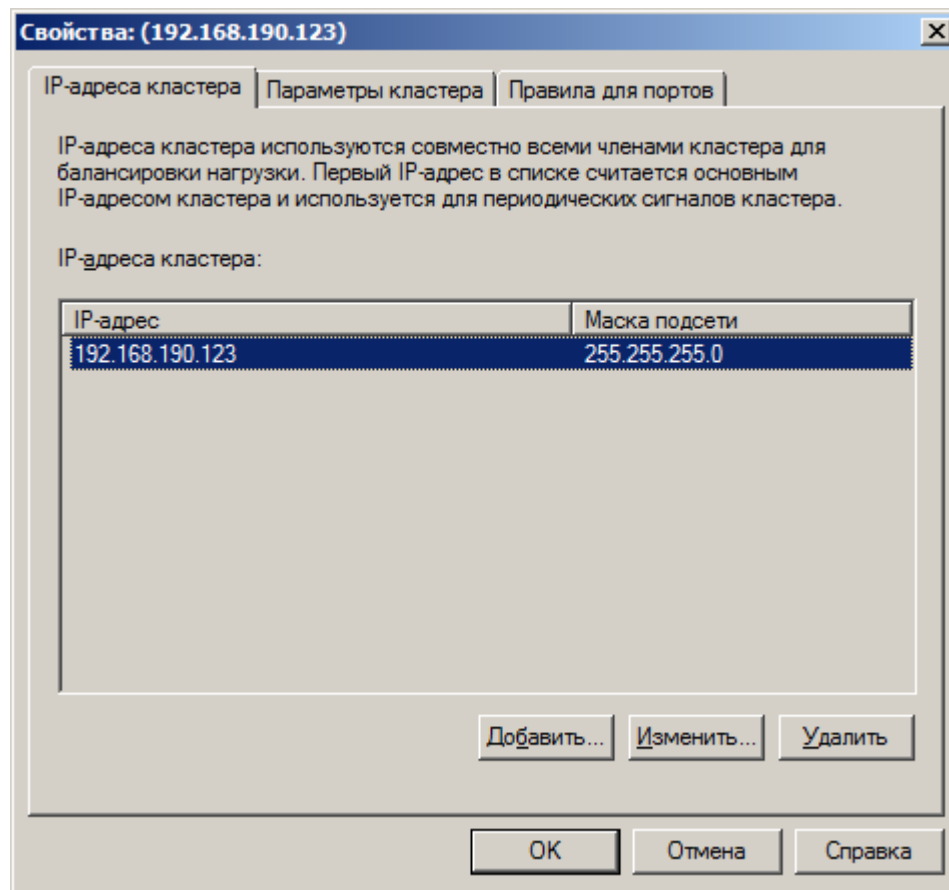


Рисунок 20 – Настройка виртуального IP-адреса кластера

Далее следует задать Полное Интернет-имя (FQDN) кластера и указать режим работы кластера (одноадресный или многоадресный) (Рисунок 21).



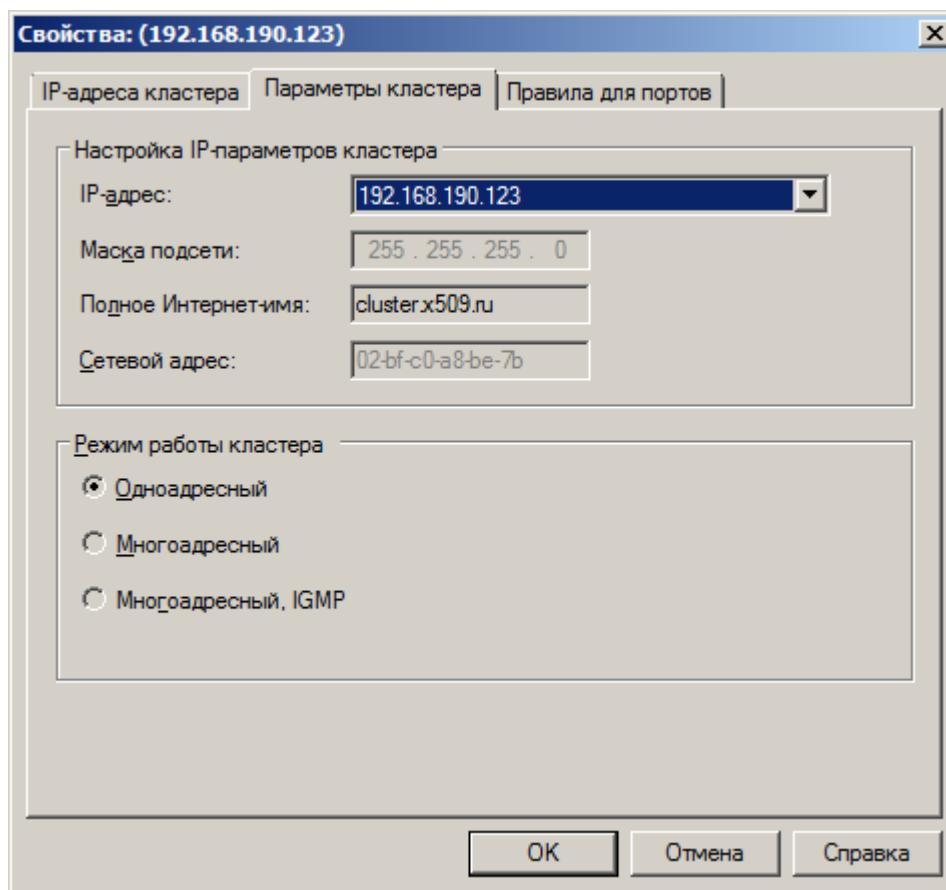


Рисунок 21 – Настройка режима работы кластера

Если будет использоваться многоадресный режим работы кластера с использованием группового MAC-адреса, этот режим должен быть установлен на всех узлах кластера (аналогично при использовании одноадресного режима с изменением MAC-адреса кластерного адаптера узла). Про ограничения и особенности использования режимов (в частности одноадресного режима с коммутаторами фирмы Cisco) подробнее описано в документации по службе "Балансировка сетевой нагрузки".

Если управление узлами кластера будет выполняться удаленно, то необходимо задать имя пользователя и пароль, используя пункт меню **Параметры | Изменить....** После этого можно переходить к настройкам узла кластера (Рисунок 22).

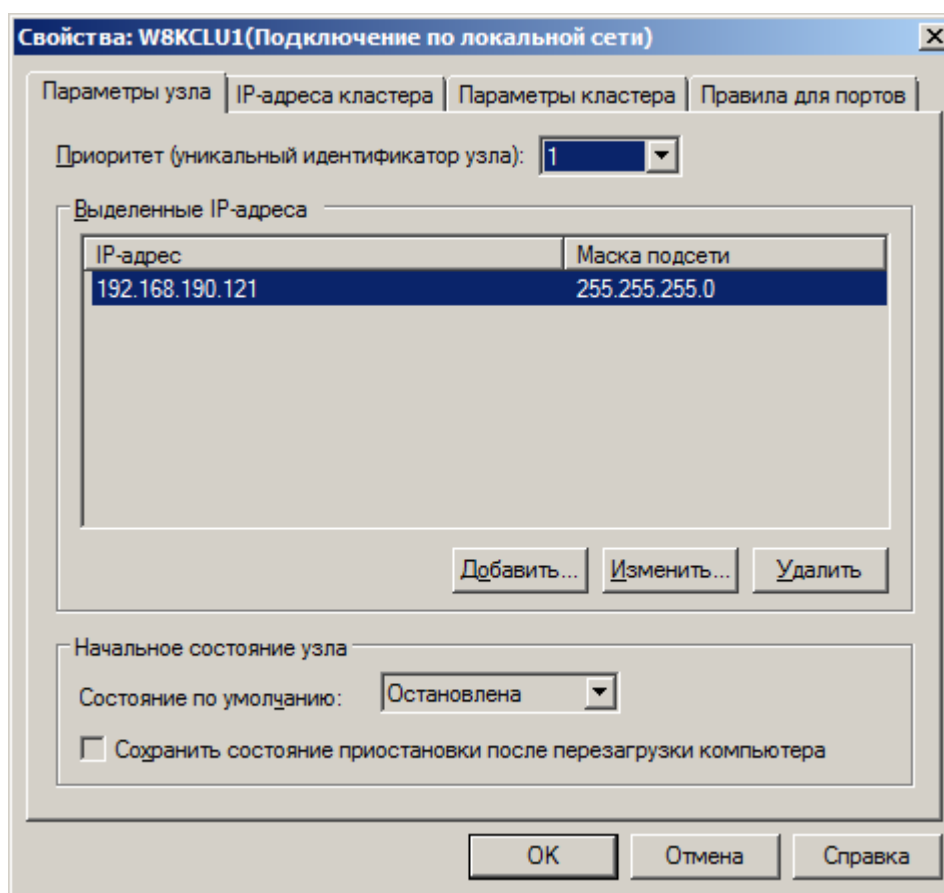


Рисунок 22 – Настройки узла кластера

Необходимо назначить уникальный для каждого узла вес (приоритет) узла кластера (чем меньше число, тем больше приоритет). Также необходимо назначить выделенный IP-адрес узла кластера, который используется для передачи сетевого трафика, не связанного с кластерными операциями. При этом для трафика, непосредственно предназначенного узлу кластера (например, команд АРМ УКС), рекомендуется использовать сетевой адаптер, не задействованный в службе "Балансировка сетевой нагрузки".

Так как для полноценной работы криптосервера необходима загрузка ключей ЭП с АРМ УКС, то начальное состояние (состояние по умолчанию) службы "Балансировка сетевой нагрузки" должно быть **Остановлена**.

В заключение необходимо настроить правила для портов кластера (Рисунок 23).

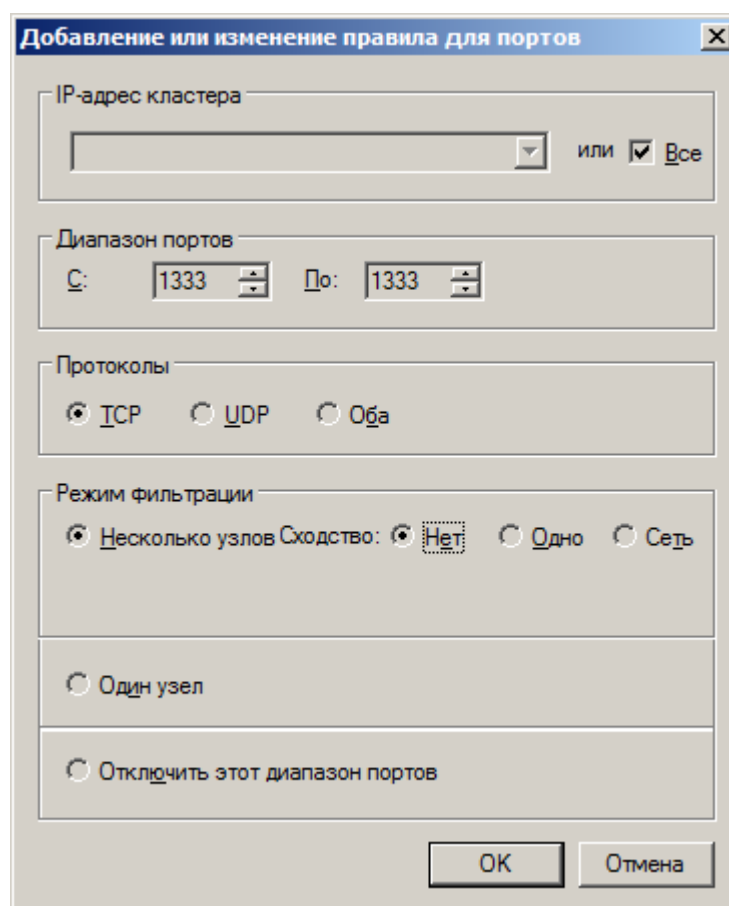


Рисунок 23 – Настройка правил для портов

В данном примере настраивается правило для порта 1333 (порта криптосервера "по умолчанию") и протокола TCP (транспорт ncasp\_ip\_tcp протокола DCE-RPC в настройках КС).

Для обеспечения распределения запросов, поступающих от прикладного ПО, необходимо использовать режим фильтрации **Несколько узлов**, определяющий балансировку нагрузки между всеми узлами кластера. Также необходимо переключатель **Сходство** (средство клиента) установить в положение *Нет*, чтобы запросы с одного клиентского места могли распределяться между всеми узлами кластера.

Для завершения настройки узла кластера необходимо добавить виртуальный (первичный) IP-адрес кластера в настройках выбранного для использования в службе "Балансировка сетевой нагрузки" сетевого адаптера (Рисунок 24).

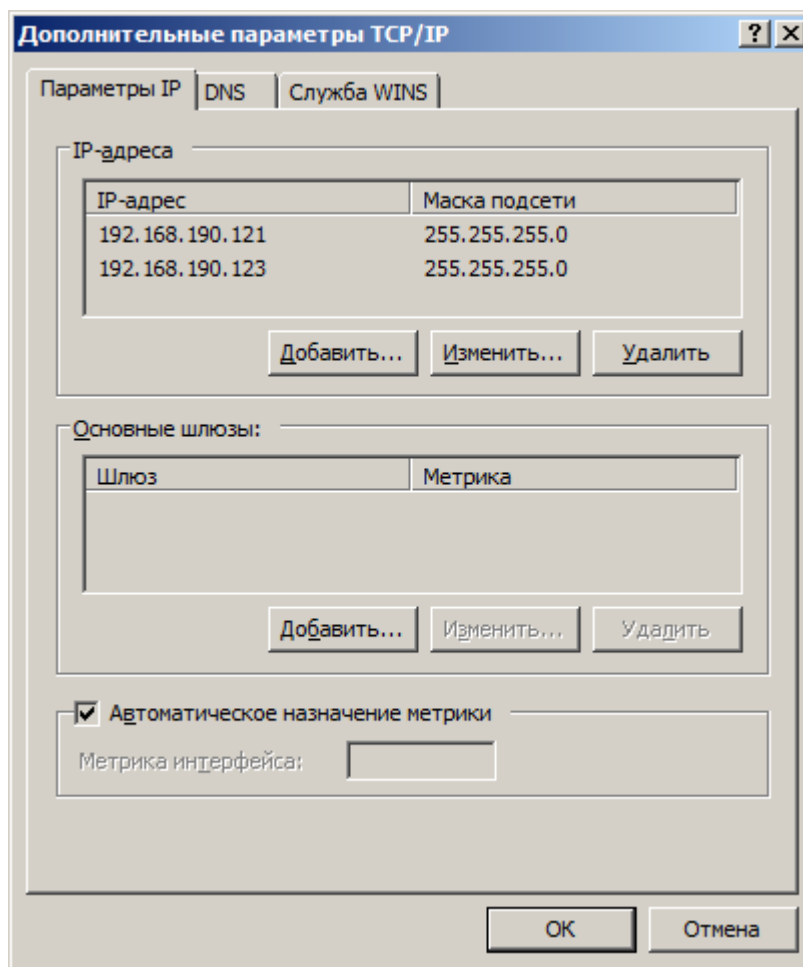


Рисунок 24 – Добавление виртуального IP-адреса кластера

После выполнения всех вышеописанных настроек необходимо проверить работу службы "Балансировка сетевой нагрузки". Для этого необходимо на любом из узлов кластера выполнить в режиме командной строки следующую команду: *wlbs.exe query*. Если все настройки узлов совпадают и успешно завершился процесс конвергенции (схождения), то появится строка следующего содержания:

WLBS Программа управления кластером, версия V2.5 (C) Корпорация Майкрософт (Microsoft Corporation), 1997-2007.

Кластер 192.168.190.123

Узел 1 входил в состояние схождения 1 раз после присоединения к кластеру, и последнее схождение завершено приблизительно:  
22.08.2012 20:48:42

Выполнено схождение узла 1 как узла DEFAULT со следующими узлами в качестве части кластера:

1, 2

Если процесс конвергенции продолжается, то появится строка следующего содержания:

WLBS Программа управления кластером, версия V2.5 (C) Корпорация Майкрософт (Microsoft Corporation), 1997-2007.

Кластер 192.168.190.123

Узел 1 входил в состояние схождения 1 раз после присоединения к кластеру и по-прежнему находится в состоянии схождения. Выполняется схождение узла 1 со следующими узлами в качестве части кластера:

1

Необходимо подождать несколько секунд и повторить команду. Если процесс конвергенции не завершается, то для детального анализа проблемы следует обратиться к документации по службе "Балансировка сетевой нагрузки".

#### **4.16 Работа с узлами кластера криптосерверов**

Для работы с узлами кластеров КС используется программа удаленного управления (*wlbs.exe*).

Так как для полноценной работы криптосервера необходима загрузка ключей ЭП с АРМ УКС, то изначально криптосервер не входит в кластер. После завершения загрузки закрытых ключей администратор должен добавить узел в кластер КС. Это можно сделать, либо послав соответствующую команду с АРМ УКС, либо выполнив следующую команду: *wlbs.exe start*. Состояние узла кластера (процесс конвергенции) можно проверить либо в строке состояния узла в АРМ УКС, либо с помощью следующей команды: *wlbs.exe query*.

На случай аварийной остановки службы КС на узле кластера необходимо выполнить настройку автоматического вывода КС из состава кластера (Рисунок 25).

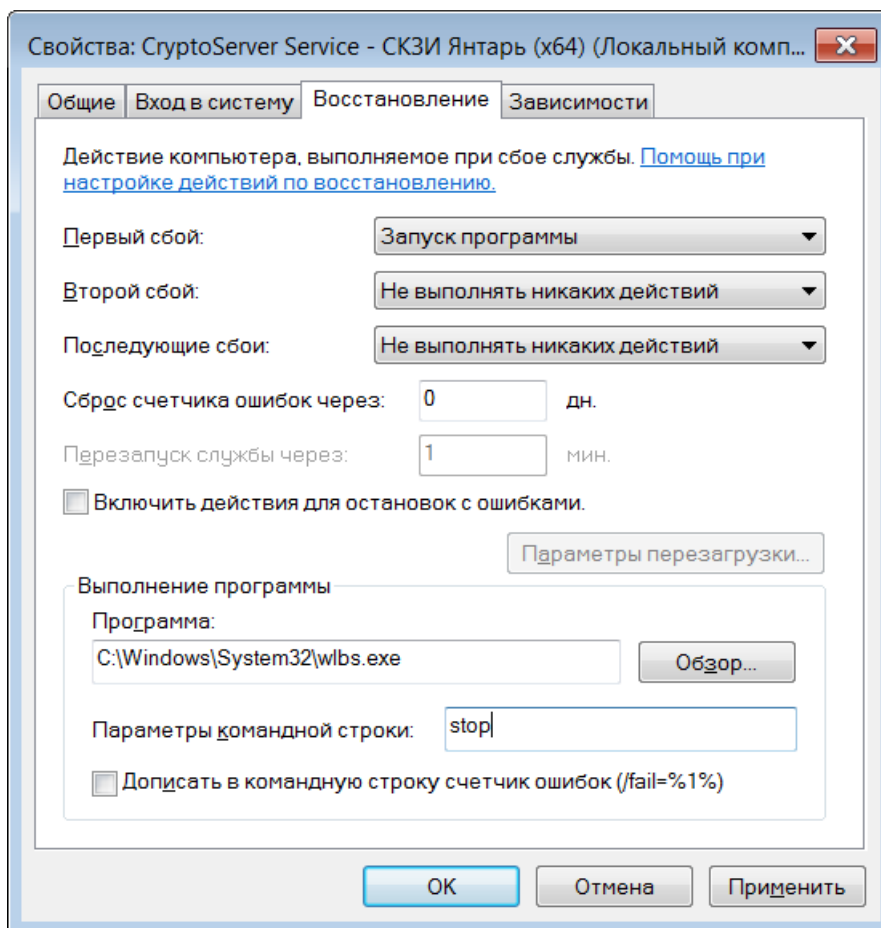


Рисунок 25 – Настройка аварийного завершения сервиса криптографического сервера

Таким образом, в случае аварийного завершения службы КС, узел будет выведен из состава кластера автоматически.

При необходимости выполнения обслуживания и/или обновления ПО на узле кластера для обеспечения бесперебойного функционирования кластера данный узел должен быть плавно выведен из состава кластера, для чего необходимо выполнить следующую команду: *wlbs.exe drainstop*.

#### 4.17 Настройка службы синхронизации времени

Для корректной работы КС или кластера криптосерверов, а также прикладного ПО, важным вопросом является синхронизация времени на всех компонентах СКЗИ «Валидата Криптосервер». Для выполнения синхронизации времени рекомендуется использовать службу синхронизации времени W32Time. Эта служба входит в состав ОС Microsoft Windows.

В качестве эталонного сервера времени может использоваться сервер, поддерживающий протокол Network Time Protocol (NTP). Рекомендуется использовать доверенный сервер, устанавливаемый в пределах закрытого сегмента корпоративной сети.

По умолчанию, первичный контроллер домена (Primary Domain Controller, PDC) является эталонным сервером времени для домена. Для того, чтобы настроить сервер времени как эталонный для домена с синхронизацией времени с

доверенным NTP сервером времени, локальному администратору ОС необходимо выполнить указанные ниже команды, которые произведут настройку и перезапуск службы синхронизации времени (<NTP Server> - IP-адрес или DNS-имя доверенного NTP сервера времени):

```
w32tm.exe /config /manualpeerlist:"<NTP Server>" /syncfromflags:MANUAL  
/reliable:yes  
w32tm.exe /config /update  
net stop W32Time  
net start W32Time  
w32tm.exe /resync /rediscover
```

При необходимости использовать для синхронизации времени доверенный NTP сервер времени непосредственно (а не использовать первичный контроллер домена), локальному администратору ОС следует выполнить команду *net time /setsntp:<NTP Server>*".

## 4.18 Работа КС

### 4.18.1 Инициализация криптографического модуля

Инициализация криптографического модуля (СКЗИ «Валидата CSP» и датчика случайных чисел) и загрузка закрытого ключа сессии администрирования должны выполняться при локальном входе пользователя в ОС Microsoft Windows (это связано с необходимостью использования графического интерфейса ОС). Следует отметить, что графический интерфейс ОС будет использоваться, только если КС не настроен на работу в "тихом" режиме (см. Рисунок 8).

При первой инициализации криптографического модуля выполняется инициализация датчика случайных чисел (ДСЧ). Для инициализации ДСЧ (если используется Биологический ДСЧ) необходимо двигать курсор "мыши" в окне инициализации ДСЧ (Рисунок 26) в соответствии с правилами, изложенными в документе ВАМБ.00060-06 95 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора».

*Примечание — При использовании аппаратного ДСЧ, входящего в состав сертифицированных ФСБ России средств защиты информации от несанкционированного доступа (см. документ ВАМБ.00060-06 30 01 «СКЗИ «Валидата CSP» версия 6. Формуляр»), манипуляций «мышью» для инициализации программного ДСЧ не требуется.*

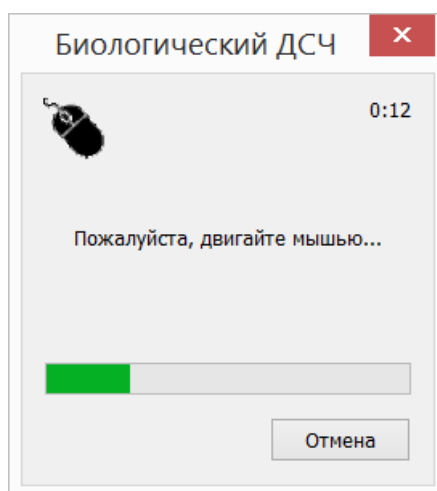


Рисунок 26 – Инициализация Биологического ДСЧ

#### 4.18.2 Инициализация обработки входящих запросов

По завершении инициализации криптографического модуля ПО КС проверяет наличие и целостность ПСП для каждой из сессий КС, начиная с сессии администрирования. Для этого производится проверка ЭП ПСП и, для сессии администрирования, загрузка ключа ЭП с идентификатором, соответствующим рабочему сертификату сессии администрирования.

После проверки ЭП ПСП и проверки рабочего сертификата для каждой из сессий КС завершается инициализация ПО КС. Для всех сессий КС (кроме сессии администрирования) ключи ЭП можно загружать удаленно с АРМ УКС.

В заключение, криптосервер запускает потоки (Threads) ожидания и обработки входящих запросов, поступающих по протоколу DCE-RPC. Процесс криптосервера может быть завершен либо по команде с АРМ УКС, либо при завершении работы ЭВМ, либо непосредственной остановкой сервиса КС с помощью команды: *net stop ZCSSVC*.



## 5 АВТОМАТИЗИРОВАННОЕ РАБОЧЕЕ МЕСТО УПРАВЛЕНИЯ КРИПТОСЕРВЕРОМ

### 5.1 Назначение и условия использования

ПК ВАМБ.00096-06 12 02 «Автоматизированное рабочее место управления криптографическим сервером» предназначен для управления КС, мониторинга текущего состояния КС, удаленной загрузки ключей на КС, а также для просмотра журналов сообщений и ошибок на всех КС. Взаимодействие между АРМ УКС и КС осуществляется по локальной сети по протоколу DCE-RPC (Distributed Computing Environment - Remote Procedure Call).

*Примечание – Загрузку ключей может осуществлять как Администратор, так и Оператор АРМ УКС.*

Перед началом установки АРМ УКС и ПК ВАМБ.00096-06 12 03 «Автоматизированное рабочее место формирования отчётов» необходимо установить и настроить криптографическое ядро СКЗИ «Валидата CSP» и ПК «Справочник сертификатов» (см. документы ВАМБ.00060-06 91 01 «СКЗИ «Валидата CSP» версия 6. Руководство по установке и настройке» и ВАМБ.00077-06 91 01 «“Валидата Клиент” версия 4. Руководство по установке и настройке»).

При использовании АРМ УКС и АРМ ФО должен быть обеспечен контроль целостности файлов АРМ УКС и ПО АРМ ФО, СКЗИ «Валидата CSP», ПК «Справочник сертификатов» и файлов системного ПО в соответствии с требованиями документа ВАМБ.00096-06 93 01 «СКЗИ «Валидата Криптосервер» версия 4. Руководство администратора информационной безопасности».

### 5.2 Установка АРМ УКС и АРМ ФО

Установка должна производиться пользователем, имеющим права локального администратора.

В состав установочного комплекта КС для ОС Microsoft Windows входят, в том числе, два файла - *zcsadm\_x86.msi* и *zcsadm\_x64.msi* (установочные комплекты для 32-битных ОС Microsoft Windows и для 64-битных ОС Microsoft Windows, соответственно).

Установка АРМ УКС и АРМ ФО для ОС Microsoft Windows выполняется стандартной инсталляционной процедурой *msiexec.exe*, входящей в комплект поставки ОС.

Для установки АРМ УКС и АРМ ФО необходимо:

- зарегистрироваться в системе с правами локального администратора;
- смонтировать передаточный носитель на соответствующее устройство;
- сменить текущий каталог на каталог, в котором находятся файлы установочного комплекта;
- запустить программу Установщика *msiexec.exe /i zcsadm\_x86.msi* (или *msiexec.exe /i zcsadm\_x64.msi*);
- выбрать каталог и компоненты продукта для установки;
- следовать инструкциям программы Установщика Windows. Для установки ПО АРМ ФО следует выбрать этот компонент в диалоге выбора компонентов для установки (Рисунок 27).

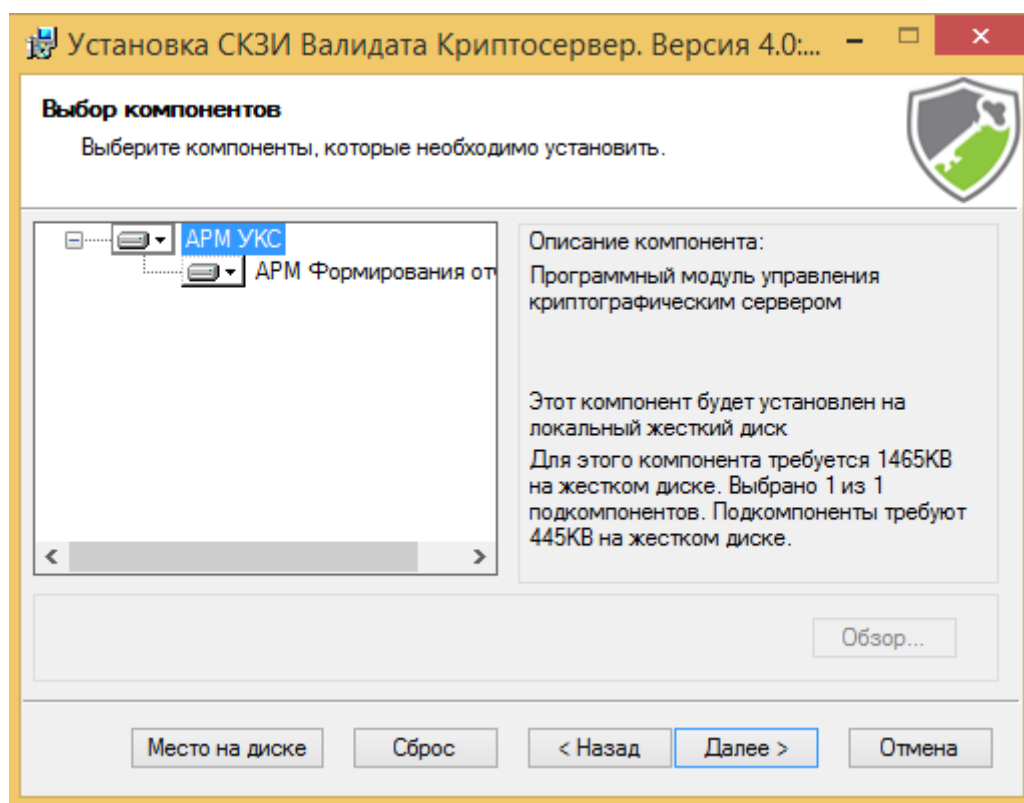


Рисунок 27 – Окно выборочного режима установки

Инсталляционная программа выполнит копирование файлов ПО АРМ УКС и ПО АРМ ФО и выдаст на экран сообщение об успешном завершении процедуры установки ПО.

### 5.3 Настройка АРМ УКС

Настройка АРМ УКС включает в себя добавление КС или кластера крипто-серверов, а также другие действия. Описание процедуры настройки АРМ УКС приведено в документе ВАМБ.00096-06 95 01 «СКЗИ «Валидата Криптосервер» версия 4. АРМ УКС. АРМ ФО. Руководство администратора».

### 5.4 Настройка АРМ ФО

Настройка АРМ ФО включает в себя настройку источника протоколов и настройку соединения с БД, которые осуществляются непосредственно из программы АРМ ФО.

Предварительно должны быть выполнены два условия:

1. Должен быть обеспечен файловый доступ с АРМ ФО к каталогу, содержащему протоколы КС. Пользователи, работающие с АРМ ФО, должны иметь права на чтение файлов протоколов КС (это обеспечивается средствами ОС Microsoft Windows);
2. На сервере БД (Microsoft SQL Server) уже должна быть создана БД, причём пользователи, работающие с АРМ ФО, должны иметь права на чтение и запись в эту БД (это обеспечивается, например, с помощью **Среды SQL Server Management Studio**).

Для создания новой базы данных в **Среде SQL Server Management Studio** следует выбрать папку **Базы данных** и пункт меню **Создать базу данных...** Далее необходимо задать имя БД, а все параметры, предлагаемые по умолчанию, можно оставить без изменения.

*Примечание - АРМ ФО не требует отдельной БД, т.е. если БД уже создана, то можно настроить АРМ ФО на работу с этой БД.*

Для обеспечения пользователям АРМ ФО прав на чтение и запись в уже созданной БД, следует создать для пользователя новое **Имя входа** в разделе **Безопасность**. Далее, для уже созданной БД, следует выбрать последовательно папку **Безопасность** и папку **Пользователи**. После этого следует выбрать раздел **Создать пользователя**, найти созданное ранее **Имя входа** пользователя и предоставить ему права *db\_datareader* и *db\_datawriter*.

## 6 СЕТЕВОЙ СПРАВОЧНИК СЕРТИФИКАТОВ

### 6.1 Назначение

Сетевой справочник сертификатов предназначен для управления и распределения ключевой информации СУС СКЗИ «Валидата Криптосервер». ССС обеспечивает централизованное хранение выпущенных сертификатов и САС, и предоставляет доступ к хранимым объектам по протоколу LDAP версии 3.

ССС СУС СКЗИ «Валидата Криптосервер» состоит из следующих компонент:

- эталонный ССС для КС (или кластера криптосерверов);
- один или более ССС для пользователей, которые обеспечивают обновление локальных справочников клиентов СКЗИ «Валидата Криптосервер» в установленном порядке. Между ССС должна осуществляться репликация для обеспечения актуальности и целостности хранимых данных.

В качестве ССС можно использовать LDAP-сервер, обеспечивающий работу по протоколу LDAP версии 3 и поддерживающий возможность расширения схемы объектов. В данном документе описаны настройки следующих рекомендованных к использованию LDAP-серверов:

- Microsoft Active Directory;
- Microsoft Active Directory - Lightweight Directory Services.

Кроме того, в качестве ССС также могут использоваться продукты других производителей, такие как: OpenLDAP Server версии 2.1.2 или выше, iPlanet/Sun Directory Server версии 5.0 или выше, Novell NDS, и т.д.

### 6.2 Описание технологии

ССС использует технологию каталогов LDAP для хранения информации об объектах и пользователях системы управления сертификатами СКЗИ «Валидата Криптосервер». В общем случае, каталоги LDAP призваны решить задачу хранения данных о реальных объектах в относительно простой, надежной и распределенной системе. Технология каталогов опирается на стандарты рабочей группы ITU X.500 (первая версия стандарта X.500 вышла в 1988 году), которые содержат в себе ключевые элементы, перечисленные ниже:

– *Порядок именования данных* — объекты в каталоге упорядочиваются в логическое "дерево": корень дерева не имеет имени, а остальные вершины характеризуются парами "атрибут-значение". Полное наименование вершины получается путем составления таких пар на пути от корня дерева к самой вершине. К примеру, объект может иметь следующий уникальный идентификатор: *cn=User,ou=Department,o=x509,c=ru*. Здесь *cn*, *ou*, *o* и *c* — зафиксированные наименования атрибутов;

– *Порядок представления данных* — каждая вершина дерева, помимо уникального наименования, содержит информацию о соответствующем реальном объекте, представленную в виде набора пар в том же формате "атрибут-значение". Так, с указанной выше вершиной могут быть связаны пары *mail: user@x509.ru*, *phone: +7-495-2320687*, и т.д;

- *Клиентский протокол DAP (Directory Access Protocol)* — описывает порядок посылки запросов от клиентской программы к каталогу и формат ответа;

- *Протокол для создания "теневого" копия DISP (Directory Information Shadowing Protocol)* — для повышения эффективности каталогов иногда имеет смысл создать резервную копию, доступную только для чтения (т.е. "тенью"), поблизости от потребителей информации. При помощи DISP один каталог может передать данные другому каталогу для использования в качестве теневой копии;

- *Протокол для передачи запросов DSP (Directory System Protocol)* — при помощи протокола DSP один каталог может запросить у другого информацию, которая отсутствует у него самого. Таким образом, клиент, связываясь всегда с одним и тем же каталогом, сможет получать данные из всей системы каталогов.

Полная поддержка стандартов X.500 сложна, а конкретные реализации ненадежны и мало совместимы между собой, поэтому был разработан протокол LDAP (Lightweight Directory Access Protocol), работающий непосредственно с TCP/IP, для упрощения работы с каталогами. Каталоги LDAP сохраняют логические стандарты X.500 (организация объектов в логическое дерево, хранение данных в виде "атрибут-значение" и т.д.), но обладают независимостью от X.500 на уровне протоколов и обеспечивают упрощенное управление и использование (RFC 1487).

Технически современные серверы LDAP сконструированы так, чтобы минимизировать время обработки запросов на чтение данных; соответственно, изменение данных происходит относительно медленно. Это означает, что каталоги лучше всего подходят для хранения информации, которая часто считывается и редко меняется — например, данные об именах, адресах и телефонных номерах реальных людей. Но использование каталогов LDAP не ограничивается одними только адресными книгами. Дело в том, что потребителем информации из каталога вполне может быть не человек, а другая программа. Соответственно, каталоги LDAP могут использоваться как хранилище пользовательских профилей (имен, паролей, прав доступа и т.п.). Наиболее распространенные способы использования каталогов:

- хранение данных о ресурсах компьютерной сети (пользователях, группах, компьютерах). У каталогов Microsoft Active Directory и Novell NDS/eDirectory это предназначение является главным;

- хранение контактных данных сотрудников организации (внутренняя адресная книга);

- хранение контактных данных клиентов или партнеров организации (внешняя адресная книга);

- хранение пользовательских профилей для многопользовательских программ. К примеру, сервер электронной почты Exchange поставляется вообще без своего хранилища профилей; предполагается, что профили будут размещены в Active Directory;

- хранение профилей пользователей сайтов Internet/extranet/intranet. При помощи таких профилей можно контролировать степень доступа пользователя и персонализировать содержание самих страниц;

- хранение сертификатов в криптографических системах с открытым ключом;

чом (Public Key Infrastructure - PKI). Доступность любого сертификата для быстрого считывания является важным условием для качественной работы систем PKI, и каталоги LDAP представляются естественным решением. Интересно, что такое предназначение каталогов предусматривалось с самого начала — самым широко используемым сегодня стандартом PKI является X.509, разработанный параллельно с X.500.

Все эти применения совершенно не исключают друг друга; более того, имеется тенденция придать как можно больше функций одному и тому же каталогу с тем, чтобы избежать возникновения множества каталогов, требующих независимой поддержки.

## 6.3 Установка

Установка должна производиться пользователем, имеющим права локального администратора.

При установке LDAP-сервера необходимо задать основу структуры каталогов (директории), которая соответствует корню иерархии системы управления сертификатами СКЗИ «Валидата Криптосервер» (например, DC=x509, DC=ru) для того, чтобы обеспечить связь между объектами директории и объектами СКЗИ «Валидата Криптосервер». Перед установкой ССС необходимо продумать иерархическое дерево директории для размещения объектов: использование контейнеров организации (О) и подразделений организации (ОУ), а также возможность передачи прав на управление ветвями дерева директории.

### 6.3.1 Установка Active Directory

Установка Microsoft Active Directory выполняется в соответствии с документацией на ОС Microsoft Windows с передаточного носителя ОС Microsoft Windows. Для запуска программы установки необходимо запустить в командной строке команду *dcprmo.exe* и далее следовать указаниям мастера установки.

### 6.3.2 Установка Active Directory - Lightweight Directory Services

Установка Microsoft Active Directory - Lightweight Directory Services выполняется в соответствии с документацией на ОС Microsoft Windows с передаточного носителя ОС Microsoft Windows. Для запуска программы установки необходимо запустить **Диспетчер сервера**, добавить роль сервера *Службы Active Directory облегченного доступа к каталогам* и далее следовать указаниям мастера установки.

## 6.4 Настройка

### 6.4.1 Настройка схемы

Схема директории каталогов LDAP описывает объекты и атрибуты объектов, которые могут храниться в директории. Для хранения сертификатов и САС, а также поиска по каталогам LDAP-сервера используется схема, основанная на RFC 2587.

Для обеспечения поиска сертификатов и САС в СКЗИ «Валидата Криптосервер» необходимо в схему директории каталогов LDAP ввести пять дополнительных атрибутов: *vdKeyId*, *vdIASHash*, *vdSubjKeyId*, *vdAuthKeyId* и *vdSubjName*:

```

vdKeyId      ATTRIBUTE ::= {
    WITH SYNTAX          IA5String
    EQUALITY MATCHING RULE  caseIgnoreIA5Match
    ID iso(1) org(3) dod(6) internet(1) private(4) enterprise(1)
    validata(10244) extensions(4) keyid(3) }

vdIASHash     ATTRIBUTE ::= {
    WITH SYNTAX          IA5String
    EQUALITY MATCHING RULE  exactIA5Match
    ID iso(1) org(3) dod(6) internet(1) private(4) enterprise(1)
    validata(10244) extensions(4) iashash(4) }

vdSubjKeyId    ATTRIBUTE ::= {
    WITH SYNTAX          IA5String
    EQUALITY MATCHING RULE  exactIA5Match
    ID joint-iso-itu-t(2) ds(5) certificateExtension(29)
    subjectKeyIdentifier(14) }

vdAuthKeyId    ATTRIBUTE ::= {
    WITH SYNTAX          IA5String
    EQUALITY MATCHING RULE  exactIA5Match
    ID joint-iso-itu-t(2) ds(5) certificateExtension(29)
    authorityKeyIdentifier(35) }

vdSubjName     ATTRIBUTE ::= {
    WITH SYNTAX          UTF8String
    EQUALITY MATCHING RULE  caseIgnoreMatch
    ID iso(1) org(3) dod(6) internet(1) private(4) enterprise(1)
    validata(10244) ldapAttributes(1002) subjname(1) }

```

#### 6.4.2 Настройка схемы Active Directory

Модифицировать схему домена рекомендуется на том контроллере домена, который является мастером схемы домена (Domain Schema Master). Для модификации схемы администратор, который будет выполнять модификацию, должен входить в группу Schema Administrator (по умолчанию в неё входит только администратор домена).

Схему Active Directory следует изменить таким образом, чтобы в контейнере типа *person* (*CN=Person,CN=Schema,CN=Configuration*) можно было хранить сертификаты пользователей, сертификаты ЦС и САС. Для этого необходимо сохранить в файлы (в формате LDIF, см. RFC 2849) нижеследующие процедуры для утилиты *ldifde.exe*:

- Файл *person-update.ldf*:

```

dn: CN=Person,CN=Schema,CN=Configuration
changetype: modify
add: mayContain
mayContain: userCertificate
-

```

```
dn: CN=Person,CN=Schema,CN=Configuration
changetype: modify
add: mayContain
mayContain: caCertificate
-
```

```
dn: CN=Person,CN=Schema,CN=Configuration
changetype: modify
add: mayContain
mayContain: certificateRevocationList
-
```

```
dn:
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
-
```

– Файл *vdiashash.ldf*:

```
dn: CN=vdIASHash,CN=Schema,CN=Configuration
changetype: add
objectClass: attributeSchema
ldapDisplayName: vdIASHash
adminDisplayName: vdIASHash
adminDescription: vdIASHash
attributeId: 1.3.6.1.4.1.10244.4.4
attributeSyntax: 2.5.5.5
omSyntax: 22
isSingleValued: FALSE
systemOnly: FALSE
searchFlags: 1
showInAdvancedViewOnly: TRUE
```

```
dn:
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
-
```

```
dn: CN=Person,CN=Schema,CN=Configuration
changetype: modify
add: mayContain
mayContain: vdIASHash
-
```

```
dn:
```



```
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
-
```

– Файл *vdkeyid.ldf*:

```
dn: CN=vdKeyId,CN=Schema,CN=Configuration
changetype: add
objectClass: attributeSchema
ldapDisplayName: vdKeyId
adminDisplayName: vdKeyId
adminDescription: vdKeyId
attributeId: 1.3.6.1.4.1.10244.4.3
attributeSyntax: 2.5.5.5
omSyntax: 22
isSingleValued: FALSE
systemOnly: FALSE
searchFlags: 1
showInAdvancedViewOnly: TRUE
```

```
dn:
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
-
```

```
dn: CN=Person,CN=Schema,CN=Configuration
changetype: modify
add: mayContain
mayContain: vdKeyId
-
```

```
dn:
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
-
```

– Файл *vdsubjkeyid.ldf*:

```
dn: CN=vdSubjKeyId,CN=Schema,CN=Configuration
changetype: add
objectClass: attributeSchema
ldapDisplayName: vdSubjKeyId
adminDisplayName: vdSubjKeyId
adminDescription: vdSubjKeyId
attributeId: 2.5.29.14
attributeSyntax: 2.5.5.5
```

```
omSyntax: 22
isSingleValued: FALSE
systemOnly: FALSE
searchFlags: 1
showInAdvancedViewOnly: TRUE
```

```
dn:
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
-
```

```
dn: CN=Person,CN=Schema,CN=Configuration
changetype: modify
add: mayContain
mayContain: vdSubjKeyId
-
```

```
dn:
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
-
```

– Файл *vdauthkeyid.ldf*:

```
dn: CN=vdAuthKeyId,CN=Schema,CN=Configuration
changetype: add
objectClass: attributeSchema
ldapDisplayName: vdAuthKeyId
adminDisplayName: vdAuthKeyId
adminDescription: vdAuthKeyId
attributeId: 2.5.29.35
attributeSyntax: 2.5.5.5
omSyntax: 22
isSingleValued: FALSE
systemOnly: FALSE
searchFlags: 1
showInAdvancedViewOnly: TRUE
```

```
dn:
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
-
```

```
dn: CN=Person,CN=Schema,CN=Configuration
```

```
changetype: modify
add: mayContain
mayContain: vdAuthKeyId
-
```

```
dn:
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
-
```

– Файл *vdsubjname.ldf*:

```
dn: CN=vdSubjName,CN=Schema,CN=Configuration
changetype: add
objectClass: attributeSchema
ldapDisplayName: vdSubjName
adminDisplayName: vdSubjName
adminDescription: vdSubjName
attributeId: 1.3.6.1.4.1.10244.1002.1
attributeSyntax: 2.5.5.12
omSyntax: 64
isSingleValued: TRUE
systemOnly: FALSE
searchFlags: 1
showInAdvancedViewOnly: TRUE
```

```
dn:
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
-
```

```
dn: CN=Person,CN=Schema,CN=Configuration
changetype: modify
add: mayContain
mayContain: vdSubjName
-
```

```
dn:
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
-
```

После сохранения вышеописанных файлов во временный каталог, в командной строке следует выполнить следующие команды (считается, что текущим рабочим каталогом является временный каталог):

```
ldifde.exe -i -f person-update.ldf -s localhost -c "CN=Schema,CN=
  Configuration" #schemaNamingContext
ldifde.exe -i -f vdkeyid.ldf -s localhost -c "CN=Schema,CN=
  Configuration" #schemaNamingContext
ldifde.exe -i -f vdiashash.ldf -s localhost -c "CN=Schema,CN=
  Configuration" #schemaNamingContext
ldifde.exe -i -f vdsbjkeyid.ldf -s localhost -c "CN=Schema,CN=
  Configuration" #schemaNamingContext
ldifde.exe -i -f vdauthkeyid.ldf -s localhost -c "CN=Schema,CN=
  Configuration" #schemaNamingContext
ldifde.exe -i -f vdsbjname.ldf -s localhost -c "CN=Schema,CN=
  Configuration" #schemaNamingContext
```

### 6.4.3 Настройка схемы Active Directory - Lightweight Directory Services

Для модификации схемы необходимы права локального администратора.

Схему Active Directory - Lightweight Directory Services следует изменить таким образом, чтобы в контейнере типа *person* (*CN=Person,CN=Schema,CN=Configuration*) можно было хранить сертификаты пользователей, сертификаты ЦС и САС. Для этого необходимо сохранить в файлы (в формате LDIF, см. RFC 2849) нижеследующие процедуры для утилиты *ldifde.exe*:

– Файл *ca-certificate.ldf*:

```
dn: CN=CA-Certificate,CN=Schema,CN=Configuration
changetype: add
objectClass: attributeSchema
ldapDisplayName: caCertificate
adminDisplayName: CA-Certificate
adminDescription: CA-Certificate
attributeId: 2.5.4.37
attributeSyntax: 2.5.5.10
omSyntax: 4
rangeLower: 1
rangeUpper: 32768
isSingleValued: FALSE
systemOnly: FALSE
searchFlags: 0
showInAdvancedViewOnly: TRUE

dn:
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
-
```

– Файл *certificate-revocation-list.ldf*:

```
dn: CN=Certificate-Revocation-List,CN=Schema,CN=Configuration
```

```

changetype: add
objectClass: attributeSchema
ldapDisplayName: certificateRevocationList
adminDisplayName: Certificate-Revocation-List
adminDescription: Certificate-Revocation-List
attributeId: 2.5.4.39
attributeSyntax: 2.5.5.10
omSyntax: 4
rangeUpper: 10485760
isSingleValued: TRUE
systemOnly: FALSE
searchFlags: 0
showInAdvancedViewOnly: TRUE

dn:
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
-

```

После сохранения вышеописанных файлов во временный каталог, в командной строке следует выполнить следующие команды (считается, что текущим рабочим каталогом является временный каталог):

```

ldifde.exe -i -f ca-certificate.ldf -s localhost -c "CN=
Schema,CN=Configuration" #schemaNamingContext
ldifde.exe -i -f certificate-revocation-list.ldf -s localhost -c "CN=
Schema,CN=Configuration" #schemaNamingContext

```

После выполнения вышеприведенных операций, следует выполнить все те изменения схемы, которые описаны в процедуре изменения схемы Active Directory (см. пункт 6.4.2).

#### 6.4.4 Настройка доступа

После установки и настройки LDAP-сервера необходимо завести учётную запись ответственного за администрирование ССС (далее — администратор ССС), использующую аутентификацию (для защищенной подсети можно использовать Simple Authentication по имени пользователя и паролю). Учетной записи администратора ССС необходимо дать права на модификацию записей объектов СКЗИ «Валидата Криптосервер» для изменения и добавления сертификатов и САС (то есть права на чтение/запись атрибутов объектов *person*, а также право на создание объектов в контейнерах, которые будут содержать эти объекты).

Можно также завести учётные записи для криптосервера и пользователей и задать им необходимые права на доступ. Учётная запись криптосервера должна обладать правами на чтение всех контейнеров, содержащих объекты СКЗИ «Валидата Криптосервер». Учетные записи пользователей должны обладать правами на чтение записей других пользователей и САС (можно ограничить права пользователей на чтение в рамках своей организации, задав соответствующие

права или другой базовый DN, например, O=validata,DC=x509,DC=ru) и, возможно, модификацию некоторых полей своей записи (например, телефона или адреса).

Желательно, чтобы обеспечивался доступ без аутентификации к объектам, содержащим САС, для обеспечения возможности автоматического обновления САС на клиентских местах.

#### **6.4.5 Настройка доступа к ActiveDirectory и ActiveDirectory - Lightweight Directory Services**

ОС Microsoft Windows хранят в Active Directory все настройки домена и пользователей, поэтому необходимо максимально ограничивать доступ пользователей СКЗИ «Валидата Криптосервер» к объектам Active Directory. Такая интеграция имеет как свои плюсы (единая точка хранения учётных данных, данных почтовых ящиков Exchange и других приложений), так и свои минусы (необходимость детальной настройки прав доступа к атрибутам и контроля обращений).

Можно не совмещать хранение сертификатов и глобальный каталог AD (то есть использовать для хранения сертификатов и САС отдельный ССС). Для этого возможно организовать двухуровневую схему, в которой мастером репликации выступает Active Directory, информация из которого реплицируется (средствами метадиректории или встроенным механизмом репликации) в другой LDAP-сервер (OpenLDAP, iPlanet Directory или Active Directory - Lightweight Directory Services).

Администраторам ССС следует предоставить необходимые полномочия для управления объектами СКЗИ «Валидата Криптосервер» (*person*) и контейнерами, которые будут их содержать (*organization, organizationUnit*).

Настройки контейнеров:

- create organization Objects (если администратор ССС создает контейнеры пользователей);
- delete organization Objects (если администратор ССС создает контейнеры пользователей);
- list contents.

Создание объектов СКЗИ «Валидата Криптосервер»:

- create person Objects;
- delete person Objects.

Управление объектами СКЗИ «Валидата Криптосервер»:

- person Objects;
- List Contents;
- Read All Properties;
- Write All Properties;
- Delete.

Обеспечение свободного доступа всех пользователей к сертификатам и САС, хранящимся в контейнерах LDAP, просмотр контейнеров объектов СКЗИ «Валидата Криптосервер» (*organization, organizationUnit*, и т.д.):

- organization Objects;

- list contents.

Обеспечение доступа всех пользователей к сертификатам пользователей, сертификатам ЦС и САС:

- person Objects;
- read cACertificate;
- read certificateRevocationList;
- read userCertificate;
- read vdIASHash;
- read vdKeyId.

Дополнительно рекомендуется разрешить доступ анонимным пользователям к сертификатам пользователей, сертификатам ЦС и САС. Для этого следует установить седьмой бит в 1 (0000002) для атрибута *dSHeuristic* записи *CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration* (или создать этот атрибут, если он не существует).

## 6.5 Взаимодействие ССС

### 6.5.1 ССС КС

ССС КС СКЗИ «Валидата Криптосервер» обеспечивает централизованное хранение выпущенных сертификатов открытых ключей и САС для использования в КС (например, при поиске сертификатов получателей и обновлении САС). Данный ССС служит эталоном для ССС пользователей. Добавлять сертификаты и САС в ССС КС может администратор ССС, используя, например, средства LDAP-сервера для добавления сертификатов и САС в виде файлов. Структура директории LDAP-сервера должна соответствовать иерархии системы управления сертификатами СКЗИ «Валидата Криптосервер». При настройке прав доступа право на запись в директорию должен иметь только администратор ССС, при подключении которого должна производиться обязательная аутентификация.

### 6.5.2 ССС пользователей

ССС пользователей СКЗИ «Валидата Криптосервер» обеспечивают хранение выпущенных сертификатов открытых ключей и САС для пользователей системы управления сертификатами СКЗИ «Валидата Криптосервер». Они могут содержать полную копию эталонного ССС или только ту часть, которая относится к группе пользователей СКЗИ «Валидата Криптосервер». ССС пользователей могут применяться также для хранения другой информации. ССС обеспечивают доступ пользователей по протоколу LDAP версии 3 для ПК «Справочник сертификатов» из состава ВАМБ.00077-06 ««Валидата Клиент» версия 4» (см. документ ВАМБ.00077-06 92 01 ««Валидата Клиент» версия 4. Справочник сертификатов. Руководство пользователя»), а также для Библиотеки ППИ работы с сертификатами для С/С++ и для платформы Microsoft .Net Framework (см. документ ВАМБ.00077-06 33 01 ««Валидата Клиент» версия 4. Руководство программиста»).

### **6.5.3 Репликация ССС**

Репликация между ССС может осуществляться как в online-режиме, так и в offline-режиме.

В online-режиме репликация от эталонного ССС в пользовательские ССС осуществляется стандартными механизмами копирования данных между серверами LDAP (с использованием схемы single-master replication), при этом эталонный ССС КС выступает как поставщик данных, доступных только для чтения, а ССС пользователей — как получатели данных.

При использовании offline-режима (без прямого подключения ССС КС к внешним ССС пользователей) репликация осуществляется через текстовые файлы в стандартном формате LDIF (см. RFC 2849). Этот способ репликации обеспечивает лучшую защиту передаваемых данных и передачу данных больших объемов. При этом, данные ССС КС экспортируются в файл в формате LDIF на внешний носитель, а потом импортируются в ССС пользователей.



## **ПЕРЕЧЕНЬ СОКРАЩЕНИЙ**

АРМ	Автоматизированное рабочее место
АРМ УКС	АРМ управления КС
АРМ ФО	АРМ формирования отчетов
АС	Автоматизированная система
БД	База данных (Database)
ДСЧ	Датчик случайных чисел
КЗИ	Криптографическая защита информации
КС	Криптографический сервер
ЛСП	Локальный справочник пользователя
ОС	Операционная система (Operating System)
ПК	Программный комплекс
ПО	Программное обеспечение
ППИ	Прикладной программный интерфейс
ПСП	Персональный справочник пользователя
САС	Список аннулированных сертификатов (Certificate Revocation List)
СКЗИ	Средство КЗИ
ССС	Сетевой справочник сертификатов
ЦР	Центр регистрации (Registration Authority)
ЦС	Центр сертификации (Certification Authority)
ЭП	Электронная подпись (Digital Signature)

## ПЕРЕЧЕНЬ РИСУНКОВ

1	Запуск программы установки . . . . .	12
2	Ввод имени пользователя . . . . .	13
3	Выбор папки установки . . . . .	13
4	Выбор типа установки . . . . .	14
5	«Выборочная» установка . . . . .	15
6	Диалог готовности к установке . . . . .	15
7	Установка завершена . . . . .	16
8	Настройки учетной записи сервиса криптосервера . . . . .	17
9	Зависимости сервиса криптосервера . . . . .	18
10	Главное окно программы конфигурации . . . . .	20
11	Настройки сессии администрирования . . . . .	21
12	Настройка новой сессии . . . . .	23
13	Настройка сетевого справочника сессии . . . . .	25
14	Настройка авторизации сессии . . . . .	26
15	Настройка авторизованного подключения . . . . .	27
16	Настройка параметров криптографии . . . . .	29
17	Настройка параметров DCE-RPC . . . . .	30
18	Настройка журнала работы криптосервера . . . . .	31
19	Включение службы балансировки сетевой нагрузки . . . . .	39
20	Настройка виртуального IP-адреса кластера . . . . .	40
21	Настройка режима работы кластера . . . . .	41
22	Настройки узла кластера . . . . .	42
23	Настройка правил для портов . . . . .	43
24	Добавление виртуального IP-адреса кластера . . . . .	44
25	Настройка аварийного завершения сервиса криптографического сервера . . . . .	46
26	Инициализация Биологического ДСЧ . . . . .	48
27	Окно выборочного режима установки . . . . .	50

**ПЕРЕЧЕНЬ ТАБЛИЦ**

1	Описание полей строк (записей) протоколов . . . . .	33
---	---	----

[illegible][illegible]