ПАО «МОСКОВСКАЯ БИРЖА»

УТВЕРЖДЕН
ВАМБ.00075-02 91 01–ЛУ

# АППАРАТНО-ПРОГРАММНЫЙ КОМПЛЕКС «КЛИЕНТ МБ» ВЕРСИЯ 2.0

# ПРОГРАММНЫЙ КОМПЛЕКС «СПРАВОЧНИК СЕРТИФИКАТОВ»

РУКОВОДСТВО ПО УСТАНОВКЕ И НАСТРОЙКЕ

ВАМБ.00075-02 91 01

2015

# Аннотация

Данный документ содержит описание процесса установки и настройки программного комплекса (ПК) «Справочник сертификатов» (далее Справочник сертификатов или Справочник), входящего в состав аппаратно-программного комплекса «Клиент МБ» версия 2.0 (далее по тексту - АПК «Клиент МБ»).

Документ предназначен для администраторов и пользователей как руководство по установке и настройке Справочника.

# Содержание

# 1 ТРЕБОВАНИЯ К ОПЕРАЦИОННОЙ СРЕДЕ И АППАРАТНОМУ ОБЕСПЕЧЕНИЮ

ПК «Справочник сертификатов» предназначен для использования в следующих операционных системах:

– Microsoft Windows Vista с пакетом обновлений 1 и выше;

– Microsoft Windows Server 2008 с пакетом обновлений 1 и выше;

– Microsoft Windows 7;

– Microsoft Windows Server 2008 R2;

– Microsoft Windows 8/8.1;

– Microsoft Windows Server 2012/2012 R2;

– Microsoft Windows 10.

В состав дополнительных аппаратных средств могут входить:

– программно-аппаратный комплекс (ПАК) защиты от НСД «Аккорд - АМДЗ» или ПАК «Соболь»;

– лазерный принтер;

– сетевая карта для обеспечения сетевого взаимодействия.

# 2 СОСТАВ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Справочник реализован в виде исполняемого модуля xCS.EXE (Certificate Store). В состав ПО Справочника входят следующие основные модули динамической компоновки:

– модуль **XPKI.DLL**, реализующий функции работы с сертификатами и другими объектами системы, формирования и проверки ЭП;

– модуль **GDBM.DLL**, реализующий функции базы Справочника;

– модуль **INTL.DLL**, реализующий поддержку различных кодировок языка;

– модуль **XCERTUI.DLL**, реализующий функции пользовательского интерфейса.

Модуль xPKI.DLL использует динамическую библиотеку WLDAP32.DLL для обеспечения взаимодействия с сетевым справочником LDAP. Данная библиотека входит в состав ПО Microsoft и устанавливается вместе с ПО Microsoft Internet Explorer или Outlook Express.

# 3 УСТАНОВКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Перед установкой Справочника на ПЭВМ необходимо предварительно установить СКЗИ «Валидата CSP», руководствуясь инструкцией по его установке. АПК «Клиент МБ» «Справочник сертификатов» работает с СКЗИ «Валидата CSP» версии 5.0 в варианте исполнения 1 или 2.

Перед непосредственной установкой Справочника необходимо проверить целостность дистрибутива. Это осуществляется с помощью программы hashfile.exe, находящейся на инсталляционной дискете.

## 3.1 Контроль целостности эталонной копии ПО

Программа hashfile.exe входит в инсталляционную программу АПК «Клиент МБ» «Справочник сертификатов» и предназначена для контроля целостности инсталляционных программ и контроля легальности использования этих продуктов. Она находится в корневом каталоге инсталляционной дискеты.

*Примечание - Указанная выше программа hashfile.exe является средством проверки целостности установочного комплекта. Для проведения текущего и периодического контроля используется программа hashfile.exe, входящая в состав СКЗИ «Валидата CSP» версия 5.0.*

Описание программы контроля целостности смотри документ ВАМБ.00060-05 92 03 «СКЗИ «ВАЛИДАТА CSP» версия 5.0. Программа контроля целостности. Руководство пользователя».

## 3.2 Инсталляция

Инсталляция должна производиться пользователем, имеющим права администратора.

Перед инсталляцией удалите все ранее существующие версии устанавливаемого ПО и модуля криптографической поддержки. Если модуль криптографической поддержки не удален, новая версия не будет установлена. Для этого используйте пункты основного меню Windows «Пуск», «Настройка», «Панель управления», «Установка и удаление программ».

Затем установите СКЗИ «Валидата CSP». После этого можно продолжить установку АПК «Клиент МБ» «Справочник сертификатов».

Установка программного обеспечения производится путем запуска дистрибутива xCS_-xXX.msi, находящегося на инсталляционном диске. Для запуска необходимо запустить процесс установки из проводника двойным щелчком мыши по файлу xcs_x86.msi (для ОС Microsoft Windows x86) или по файлу xcs_x64.msi (для ОС Microsoft Windows x64). После запуска процесса установки будет отображен начальный диалог (Рисунок 1).

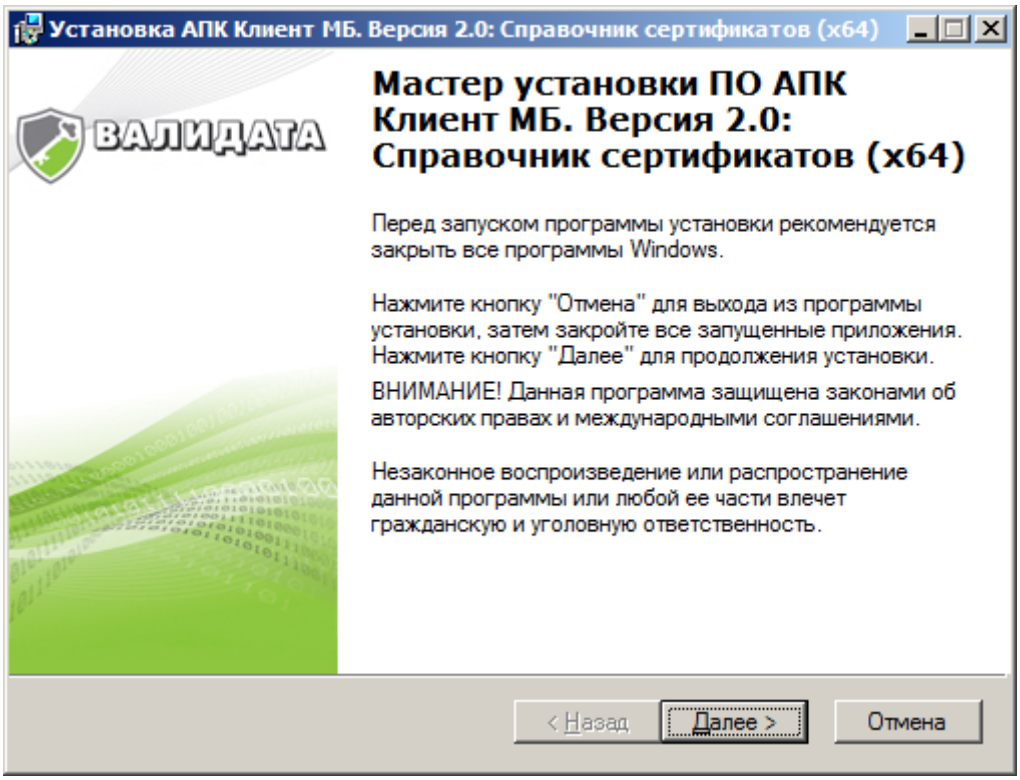


Рисунок 1 – Начальный диалог установки

Дальнейшая установка производится в соответствии с сообщениями, выдаваемыми ПО установки.

ПК «Справочник сертификатов» рекомендуется устанавливать в режиме «Обычной» установки.

При необходимости изменения компонентов установки нужно выбрать режим установки «Выборочная» (Рисунок 2).

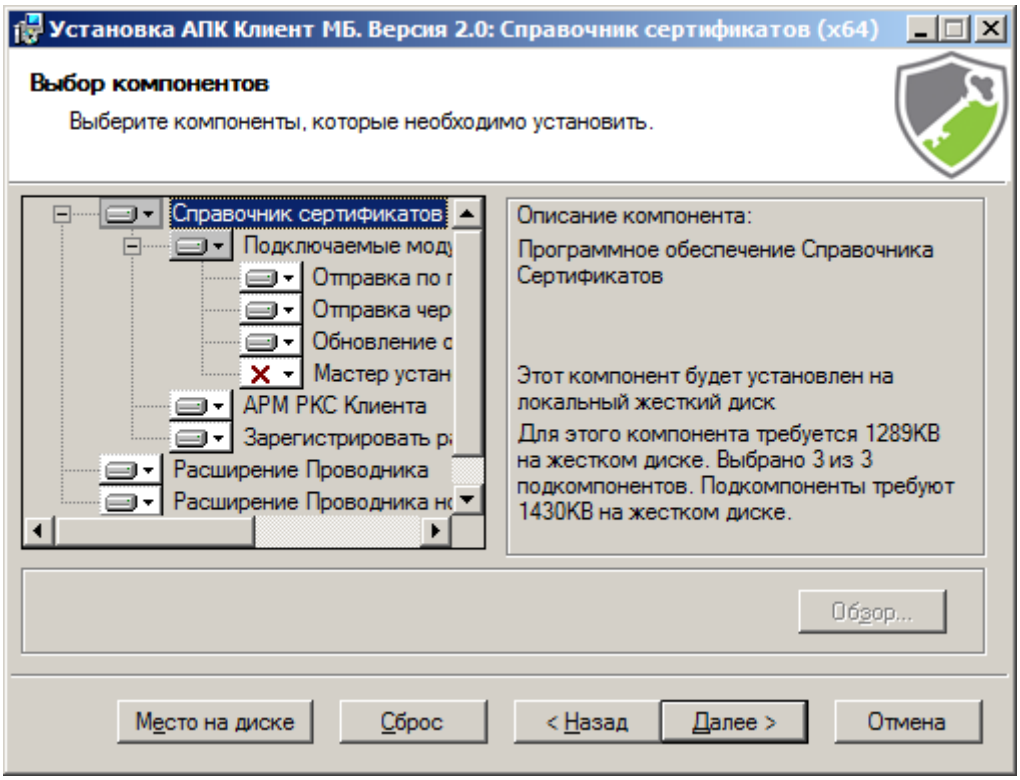


Рисунок 2 – Выбор компонентов установки

При использовании этого режима возможен выбор отдельных компонентов АПК «Клиент МБ» «Справочник сертификатов» и каталогов, в которые будет производиться установка.

После завершения процесса установки АПК «Клиент МБ» «Справочник сертификатов» должны быть выполнены действия, необходимые для осуществления регулярного контроля установленного программного обеспечения с помощью ПО контроля целостности, входящего в состав АПК «Клиент МБ», и/или ПАК «Аккорд – АМДЗ».

Инсталляция обеспечивает все необходимые настройки для функционирования Справочника.

# 4 ЗАПУСК ПК «СПРАВОЧНИК СЕРТИФИКАТОВ»

## 4.1 Запуск ПК «Справочник сертификатов»

ПК «Справочник сертификатов» запускается из основного меню Windows «Программы», «Клиент МБ», «Справочник сертификатов».

## 4.2 Запуск Справочника с использованием ODBC

ПК «Справочник сертификатов» может быть запущен с использованием одного из подключений к базе данных (DSN), но для этого необходимо выполнить следующие действия:

а) настроить подключение к базе данных (см. п. 6.5);

б) скопировать в каталог хранения баз Справочника файл local.pse (по умолчанию это каталог C:\Users\<имя пользователя>\AppData\Roaming\Validata\ xcs\);

в) создать в каталоге хранения баз Справочника файл cfg.ini, следующего вида:

ODBC ;

- local.gdbm=xcscert;
- local.gdbm_type=2

где параметр local.gdbm задает имя DNS, а параметр local.gdbm_type – тип хранилища базы сертификатов, если 2 – то база данных, если 1 – то локальный gdbm.

После этого можно запускать Справочник из основного меню ОС Windows.

# 5 РАБОТА СО СПРАВОЧНИКОМ

## 5.1 Интерфейс и структура Справочника

Графический интерфейс и структура Справочника приведена на рисунке (Рисунок 3).

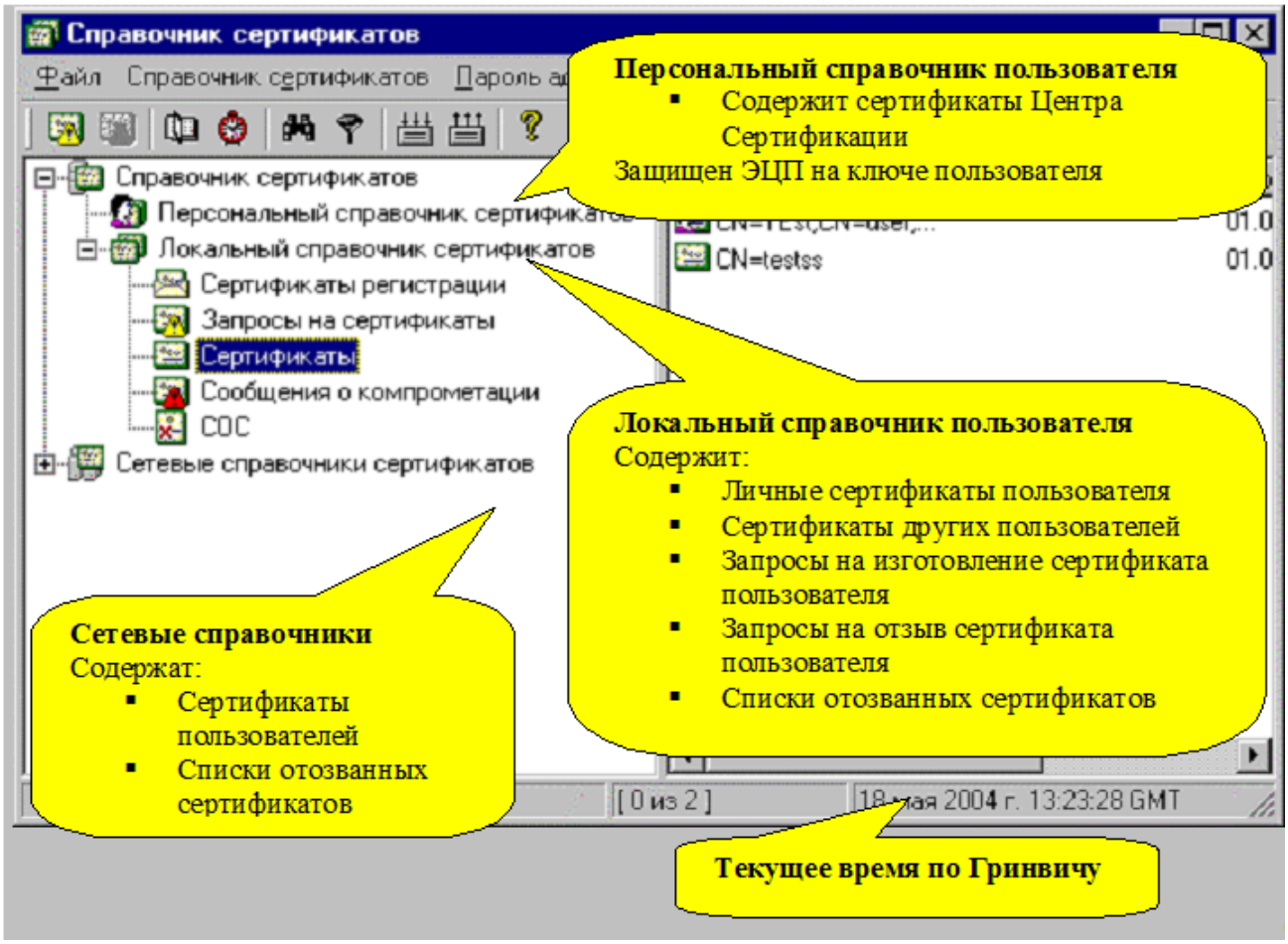


Рисунок 3 – Интерфейс Справочника

Интерфейс Справочника отображает следующие типы справочников (Таблица 1) , типы объектов (Таблица 2) и их состояния.

*Примечание - Рисунки в таблице приведены в соответствии со структурой Справочника.*

Таблица 1 – Отображение структуры Справочника

| **Рисунок и название в интерфейсе** | **Примечание** |
|---|---|
|  Справочник сертификатов | Справочник сертификатов пользователя |
|  Персональный справочник сертификатов | Персональный справочник пользователя. Содержит сертификаты ЦС. Защищен ЭП на ключе пользователя |
|  Локальный справочник сертификатов | Локальный справочник пользователя. Отображает все объекты, находящиеся в локальном справочнике. |
|  Сертификаты регистрации | Отображает сертификаты регистрации пользователя, находящиеся в локальном справочнике пользователя. |
|  Запросы на сертификаты | Отображает запросы на сертификаты пользователя, находящиеся в локальном справочнике пользователя. |
|  Сертификаты | Отображает сертификат пользователя (  ) и другие сертификаты, находящиеся в локальном справочнике пользователя. |
|  Сообщения о компрометации | Отображает сообщения о компрометации сертификата пользователя, находящиеся в локальном справочнике пользователя. |
|  СОС | Отображает списки отозванных сертификатов, находящиеся в локальном справочнике пользователя. |
|  Сетевые справочники сертификатов | Сетевые справочники сертификатов. Содержит список сетевых справочников. |
|  Название сетевого справочника | Сетевой справочник. Содержит сертификаты пользователей и СОС ЦС и ЦР |

Таблица 2 – Отображение объектов Справочника

| **Пиктограмма** | **Описание** |
|---|---|
|  | Действующий сертификат. |
|  | Отозванный сертификат. Сертификат был отозван и находится в СОС |
|  | Недействующий сертификат. Сертификат не удовлетворяет тем временным границам, которые для него установлены. |
|  | Список отозванных сертификатов. Содержит серийные номера сертификатов, которые были отозваны ЦС. |
|  | Недействующий СОС. СОС не удовлетворяет тем временным границам, которые для него установлены. |
|  | Сертификат регистрации пользователя. Сертификат, который получает пользователь в ЦР. На основании этого сертификата пользователь формирует запрос в ЦР на выпуск своего сертификата. |
|  | Недействующий Сертификат регистрации. Сертификат регистрации не удовлетворяет тем временным границам, которые для него установлены. |
|  | Личный сертификат пользователя. Сертификат пользователя, на котором защищен Персональный справочник пользователя. |
|  | Отозванный Личный сертификат пользователя. Сертификат был отозван и находится в СОС. |
|  | Недействующий Личный сертификат пользователя. Сертификат не удовлетворяет тем временным границам, которые для него установлены. |
|  | Запрос на выпуск нового сертификата пользователя. |
|  | Запрос на отзыв личного сертификата пользователя. |

## 5.2 Настройка Справочника

Для настройки Справочника необходимо выбрать из основного меню «Настройки», «Настройка Справочника сертификатов». Появится диалоговое окно для настройки параметров Справочника (Рисунок 4). На закладке «Общие настройки» можно указать время в днях, по истечении которого Справочник будет предупреждать пользователя об окончании времени действия таких объектов как «Сертификаты» и «СОС».

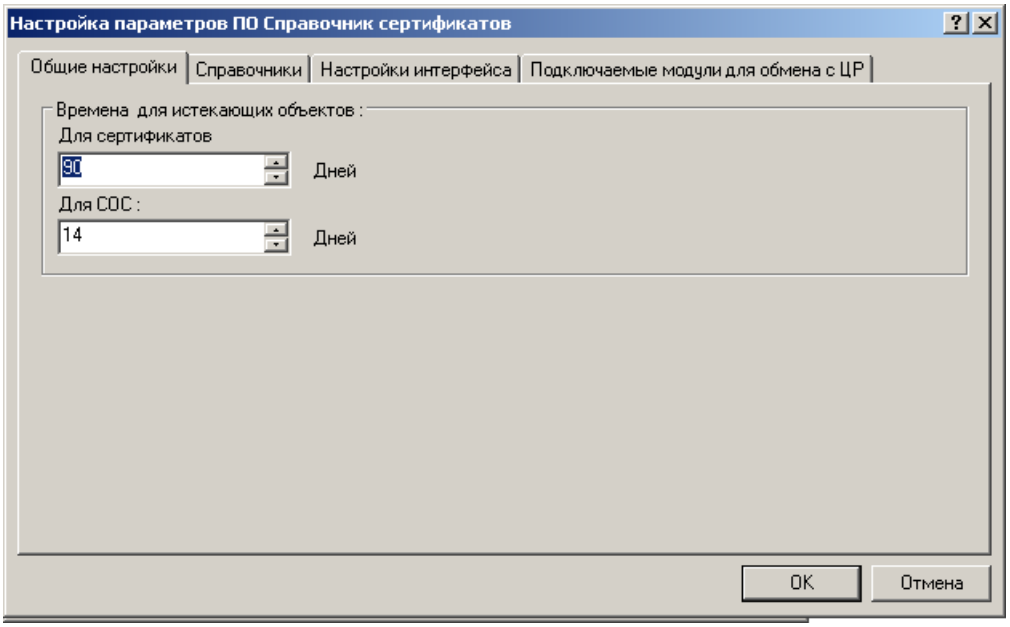


Рисунок 4 – Окно «Общие настройки»

На закладке «Справочники» (Рисунок 5) можно настроить Справочник для работы с ODBC хранилищем. Для этого необходимо указать Источник (DSN), в котором будут храниться объекты справочника. Если источник не существует, его необходимо настроить через «Администратор ODBC».

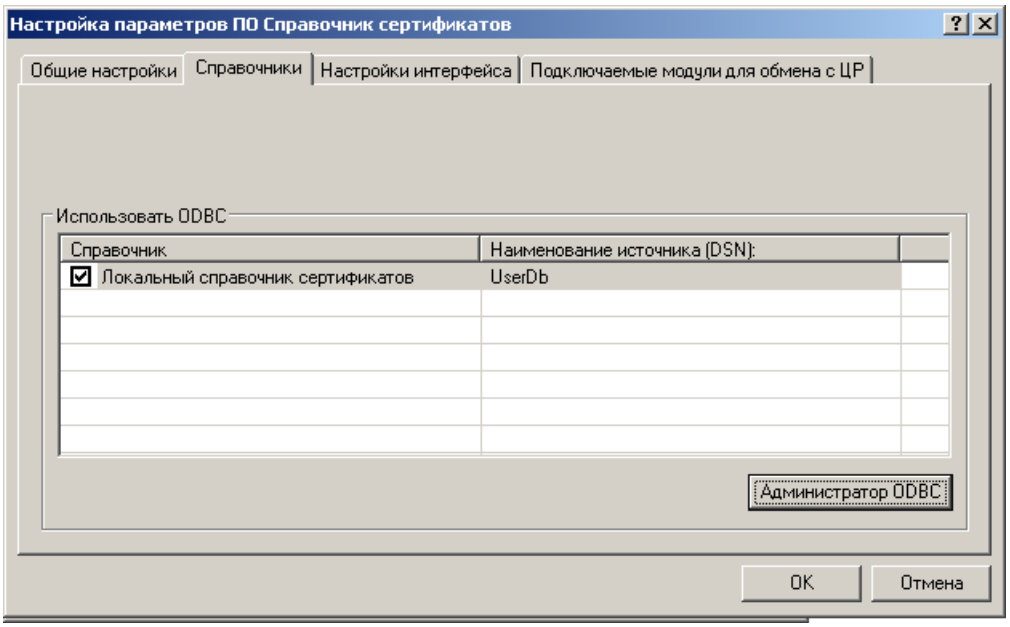


Рисунок 5 – Окно «Настройка Справочника»

На закладке «Настройки интерфейса» (Рисунок 6) можно выбрать определенные настройки для пользовательского интерфейса:

– отсылать запросы по электронной почте – если отмечена эта опция, и на компьютере пользователя установлен почтовый клиент, то после генерации запроса на выдачу сертификата или формировании запроса на отзыв сертификата, будет вызван почтовый клиент для отправки запросов в ЦР. Все нужное для отправки в ЦР будет уже заполнено, пользователю останется только отправить сообщение;

– создавать подкаталог с использованием текущего времени для сохранения резервных копий баз Справочника – при создании резервной копии пользователь должен будет указать каталог, в котором будет создан подкаталог с резервными копиями. Имя подкаталога соответствует времени создания копии.

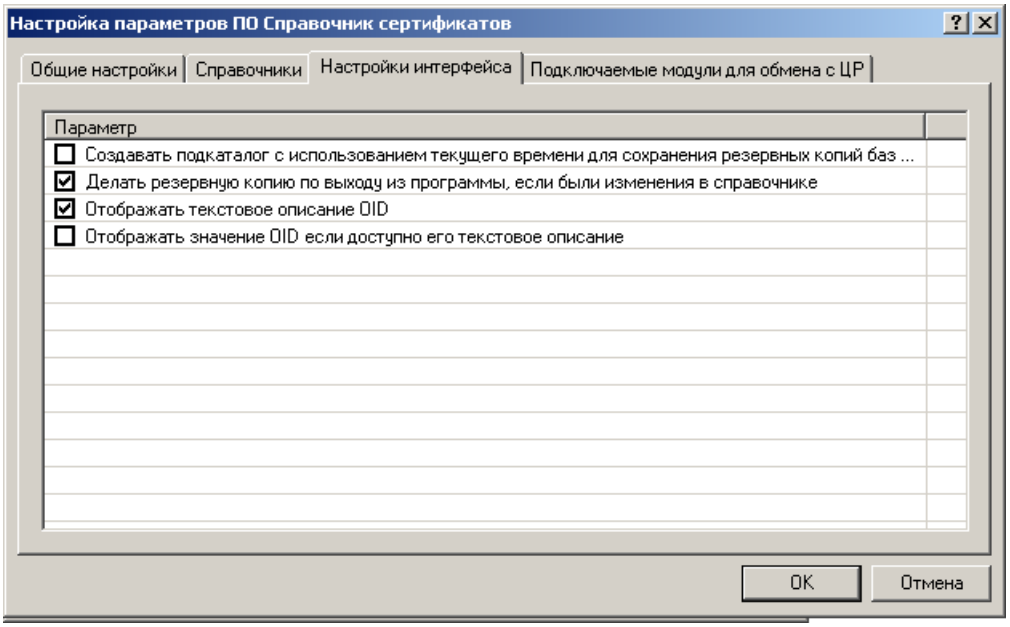


Рисунок 6 – Окно «Настройки интерфейса»

На закладке "Настройки автоматического режима"(Рисунок 7) можно настроить интервал (в секундах) автоматической проверки обновлений справочника.

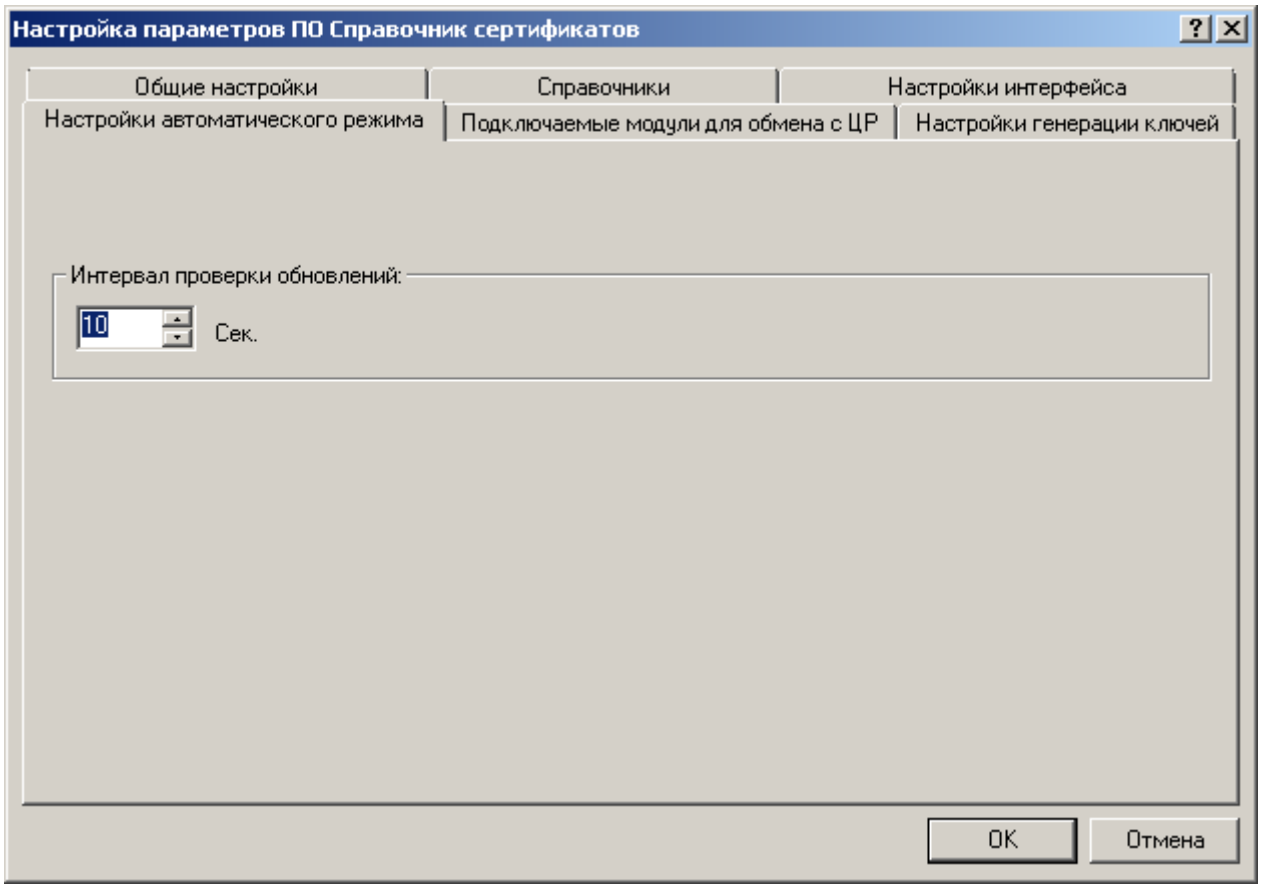


Рисунок 7 – Окно «Настройки автоматического режима»

На закладке "Подключаемый модули для обмена с ЦР"(Рисунок 8) можно выбрать определенные модули для получения и отправки информации в ЦР.

Модули для получения информации из Центра Регистрации служат для получения обновлений, выпускаемых ЦР. Модули для отправки в Центр Регистрации служат для отправки в ЦР таких объектов, как запрос на новый сертификат и запрос на отзыв сертификата. Для настройки модуля необходимо выбрать модуль и нажать кнопку «Настроить». Для того чтобы активировать модуль, необходимо напротив него поставить галочку, для деактивации, наоборот, убрать галочку.

Для добавления модуля необходимо нажать кнопку «Добавить» в зависимости от того, какой тип модуля необходимо добавить: модуль для обновлений из ЦР или для отправки в ЦР (Рисунок 8). Далее появится диалог, предлагающий выбрать подключаемый модуль. Подключаемый модуль является динамической библиотекой, файловое расширение модуля – DLL. После выбора модуля его наименование появится в соответствующем окне.

Для настройки модуля необходимо выбрать необходимый модуль и нажать кнопку «Настроить».

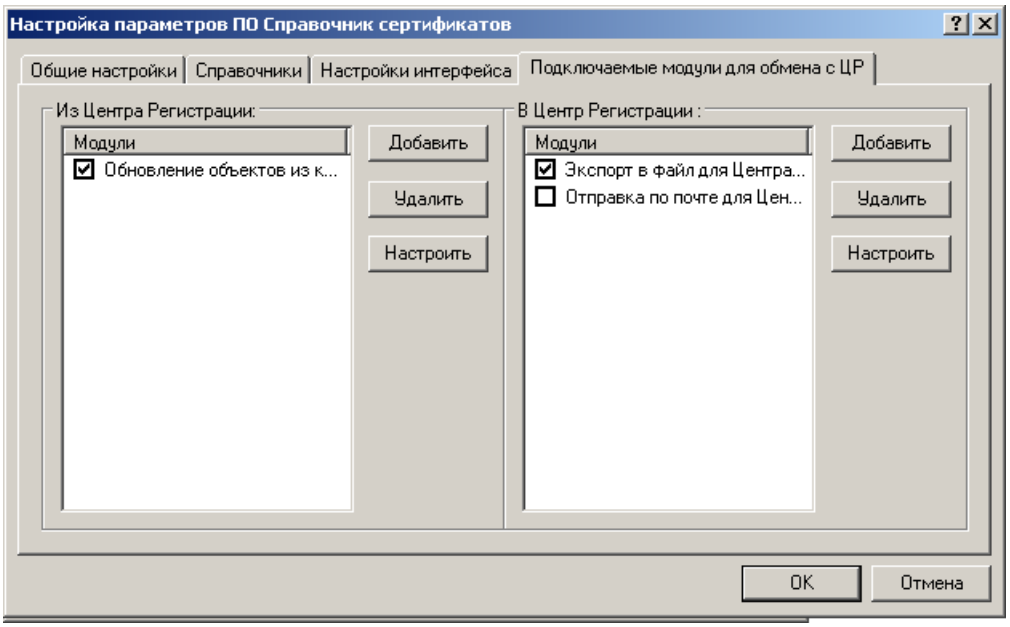


Рисунок 8 – Окно «Подключаемые модули для обмена с ЦР»

Модуль «Отправка по почте для Центра Регистрации» предназначен для отправки файлов в ЦР по электронной почте. Модуль представляет собой динамическую библиотеку xuserpost2ra.dll, расположенную в каталоге C:\Program Files\Validata\xpki\. При настройке модуля появится диалоговое окно настройки модуля (Рисунок 9). В поле «Адрес ЦР» необходимо указать почтовый адрес Центра Регистрации в формате RFC 822.

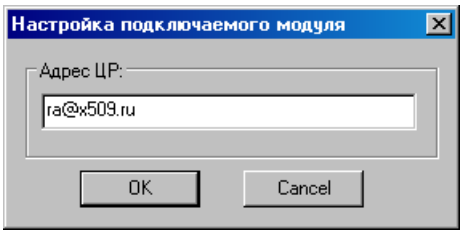


Рисунок 9 – Настройка модуля «Отправка по почте для Центра Регистрации»

Модуль «Экспорт в файл для Центра Регистрации» предназначен для записи файлов на носитель для последующей передачи в ЦР. Модуль представляет собой динамическую библиотеку xuserdisk2ra.dll, расположенную в каталоге C:\Program Files\Validata\xpki\.

При настройке модуля появится диалоговое окно настройки модуля (Рисунок 10). Окно содержит поле для настройки каталога, в который будут записываться экспортируемые объекты, и флаг для интерактивной работы модуля. Если этот флаг установлен, то при экспорте объекта у пользователя будет каждый раз спрашиваться имя файла.

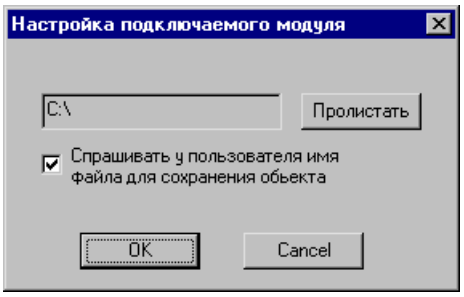


Рисунок 10 – Настройка модуля «Экспорт в файл для Центра Регистрации»

Модуль «Обновление объектов из каталога» предназначен для получения обновлений из Центра Регистрации. Модуль представляет собой динамическую библиотеку xupdatefromdisk.dll, расположенную в каталоге C:\Program Files\Validata\xpki\. При настройке модуля появится диалоговое окно настройки модуля (Рисунок 11). Для настройки необходимо указать каталог, в котором модуль будет искать файлы с расширением «pse». Если установить флаг «Удалять файл после обработки», то файл будет удален. Для случая, если нужно выбрать каталог, отличный от установленного по умолчанию, предусмотрен флаг «Выбирать каталог». Если он будет установлен, то при запуске обновления объектов будет выдано диалоговое окно для выбора каталога, из которого будет производиться обновление.

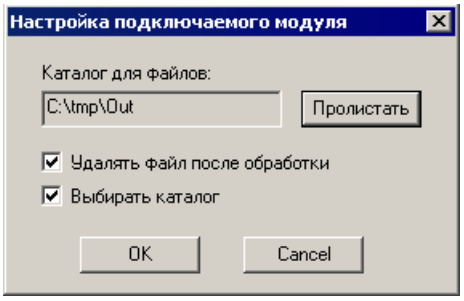


Рисунок 11 – Настройка модуля «Обновление объектов из каталога»

Модуль «Обновление объектов с WEB сервера ЦР» предназначен для получения обновлений из Центра Регистрации через WEB-сервер Центра Регистрации.

При настройке модуля появится диалоговое окно настройки модуля (Рисунок 12). В поле «Адрес WEB сервера ЦР» необходимо указать URL WEB сервера ЦР.

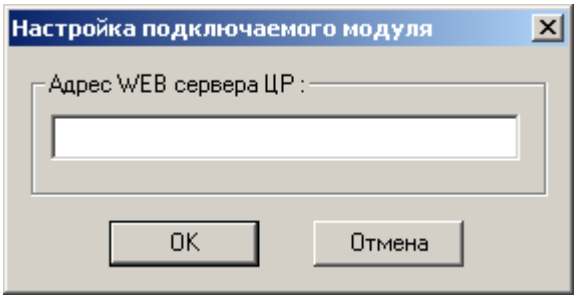


Рисунок 12 – Настройка модуля «Обновление объектов с WEB сервера ЦР»

Модуль «Отправка через HHTP Центра Регистрации» предназначен отправки файлов на сервер Центра Регистрации.

Диалоговое окно настройки модуля аналогично диалоговому окну настройки модуля «Обновление объектов с WEB сервера ЦР» (Рисунок 12).

Для удаления модуля необходимо выбрать необходимый модуль и нажать кнопку «Удалить» (Рисунок 8).

На закладке "Настройки генерации ключей"(Рисунок 13) можно указать алгоритм, по которому будут создаваться ключи (выбрать соответствующий стандарт).

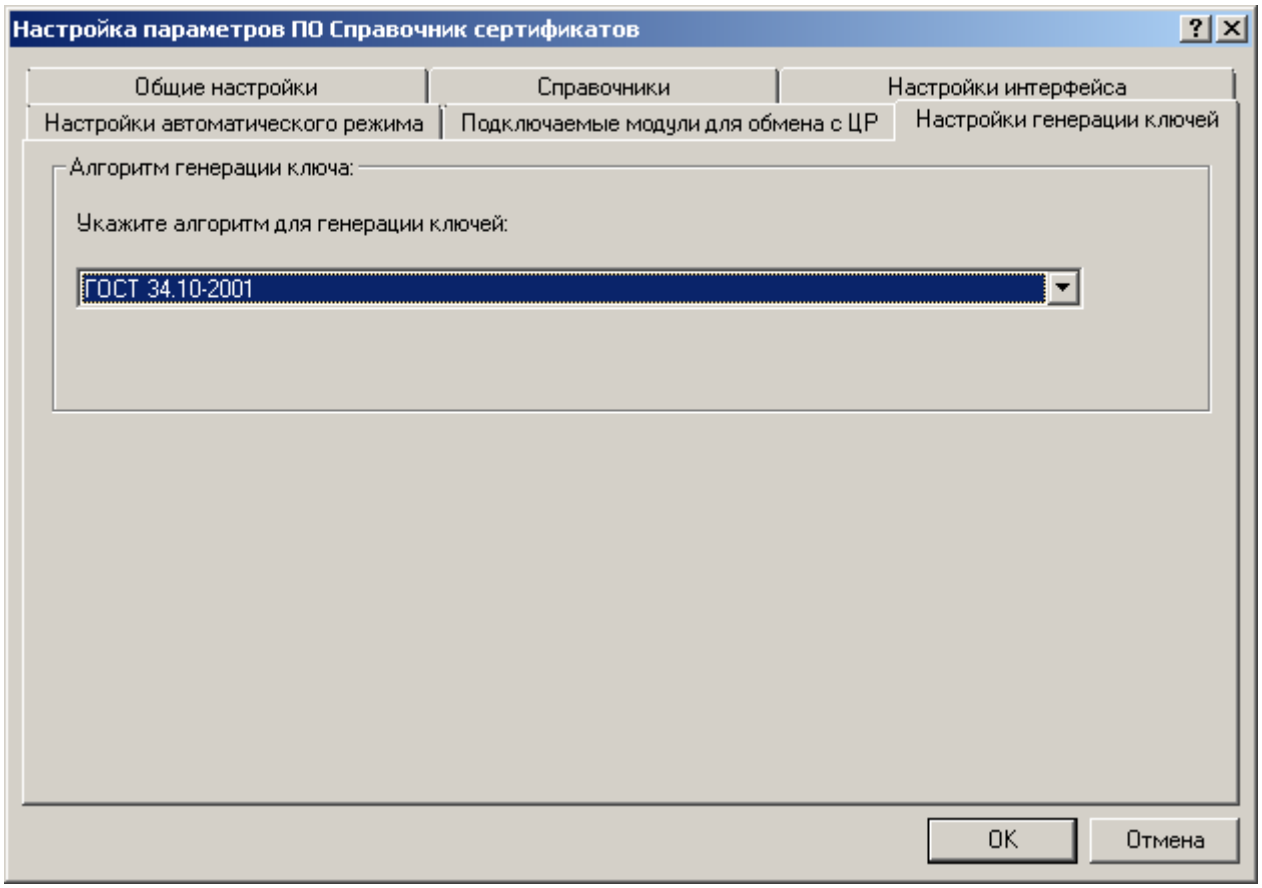


Рисунок 13 – Окно «Настройки генерации ключей»

## 5.3 Разграничение прав доступа на использование Справочника

Для разграничения прав доступа на использование Справочника используется механизм парольной защиты Справочника. Пароль действует до его изменения или отмены. После установки пароля, Справочник может работать в двух режимах:

а) Режим администратора;

б) Режим пользователя.

В режиме пользователя невозможно удаление ни одного из объектов Справочника. В режиме администратора Справочник работает полнофункционально.

### 5.3.1 Установка пароля

Для установки пароля необходимо выбрать пункт «Установить пароль Администратора» основного меню «Пароль Администратора» (Рисунок 14).

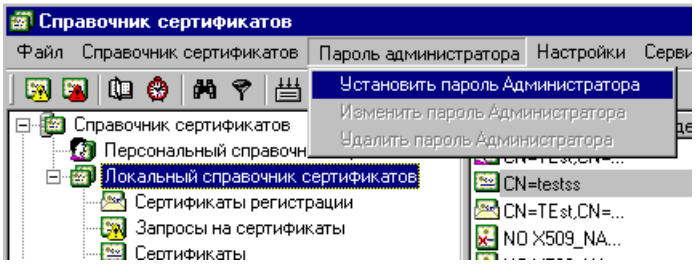


Рисунок 14 – Установка Пароля администратора

После установки пароля при каждом запуске Справочника будет запрашиваться пароль. Если пароль не введен или введен неправильно, Справочник автоматически переключается в режим пользователя.

### 5.3.2 Изменение пароля

Для изменения пароля администратора необходимо выбрать пункт «Изменить пароль Администратора» главного меню «Пароль Администратора» (Рисунок 14). Далее появится диалоговое окно, предлагающее ввести новый пароль администратора (Рисунок 15).

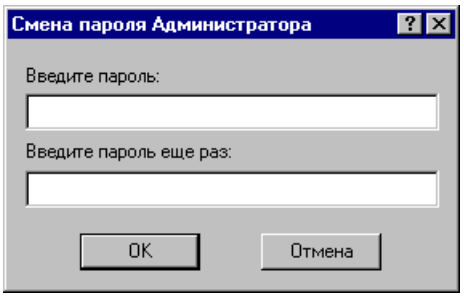


Рисунок 15 – Окно «Смена пароля администратора»

*Примечание - Смена пароля возможна только в режиме Администратора. Минимальная длина пароля 8 символов.*

### 5.3.3 Удаление пароля

Для удаления пароля администратора необходимо выбрать пункт «Удалить пароль Администратора» основного меню «Пароль Администратора» (см. Рисунок 14).

*Примечание - Удаление пароля возможно только в режиме Администратора.*

## 5.4 Настройка интерфейса Справочника

Справочник позволяют определить состав информации, выводимой в правой части интерфейса Справочника для списков объектов. Настройка отображения списка объектов осуществляется выбором необходимого списка в левом окне интерфейса Справочника, далее необходимо переключиться на отображаемый список объектов (правое окно интерфейса Справочника), нажать правую кнопку «мыши» и выбрать пункт меню «Настроить отображение». Для настройки отображения пользователю предлагается выбрать поля (колонки в интерфейсе Справочника), которые необходимо отображать (Рисунок 16). Окно содержит два списка - «Возможные поля» и «Текущие поля». «Возможные поля» – это поля, которые можно выбрать для отображения. «Текущие поля» – это поля, которые отображаются в данный момент. Для добавления списка полей к текущим необходимо выделить все требуемые поля в списке «Возможные поля» и нажать кнопку «$->$». Выбранные поля появятся в списке «Текущие поля». Для удаления полей из списка «Текущие поля», необходимо выделить все требуемые поля в списке «Текущие поля» и нажать кнопку «$<-$». Для изменения порядка отображения используются кнопки, расположенные справа от списка «Текущие поля». Для изменения позиции поля в списке необходимо выбрать поле и нажать кнопку «▲» (вверх) или кнопку «▼» (вниз). Самое верхнее поле в списке «Текущие поля» отображается в интерфейсе Справочника как самая левая колонка, самое нижнее поле – как самая правая колонка.

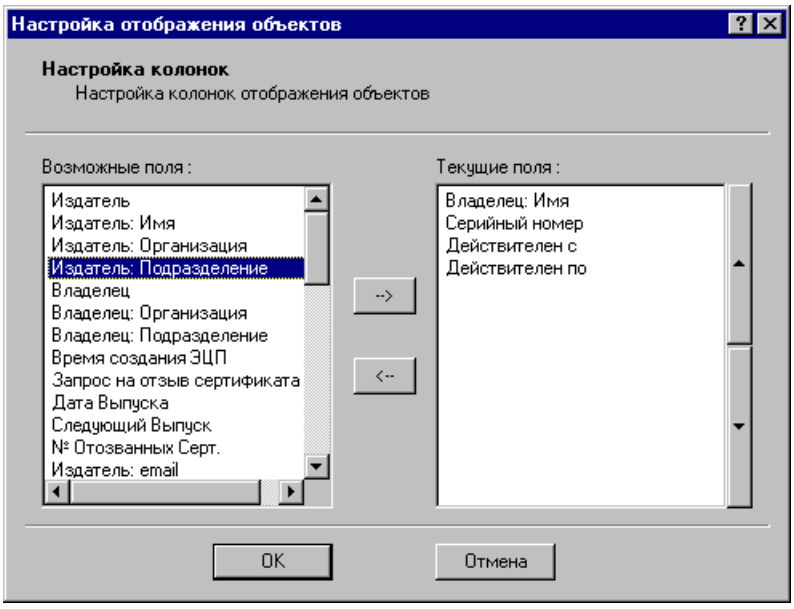


Рисунок 16 – Окно «Настройка отображения объектов»

## 5.5 Сетевые справочники сертификатов

### 5.5.1 Добавление Сетевого справочника

Справочник позволяет пользователю работать с сетевыми справочниками сертификатов по протоколу LDAP. Одновременно пользователь может работать с несколькими справочниками. Для добавления нового Сетевого справочника пользователю необходимо выбрать в левом окне Справочника пункт «Сетевые справочники сертификатов», нажать правую кнопку «мыши» и выбрать пункт меню «Добавить сетевой справочник» (Рисунок 17).

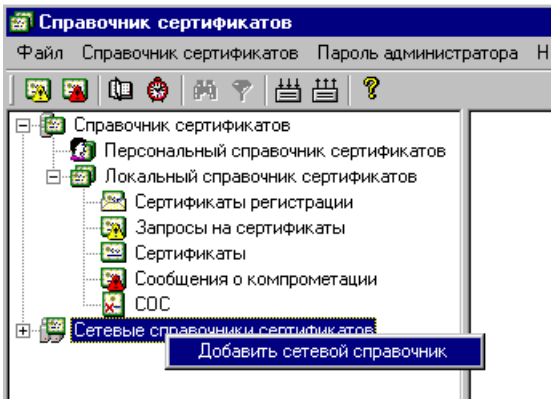


Рисунок 17 – Добавление Сетевого справочника сертификатов

Далее пользователю необходимо настроить параметры Сетевого справочника сертификатов, такие как (Рисунок 18):

- сетевой путь к Справочнику;
- имя пользователя для подключения к Справочнику;
- пароль для подключения к Справочнику;
- режим отображения Сетевого справочника в виде дерева.

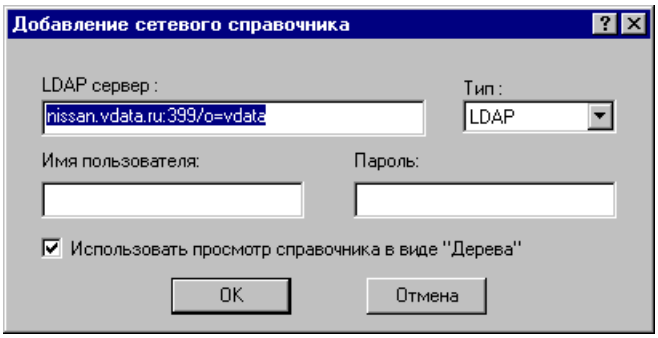


Рисунок 18 – Окно «Настройка параметров Сетевого справочника»

Сетевой путь к Справочнику должен содержать IP адрес Справочника или доменное имя. В путь к Справочнику также может быть включен порт, к которому будет осуществляться подсоединение к LDAP-серверу (порт указывается через «:» после имени). В путь к Справочнику также может быть включен базовый каталог LDAP-сервера (указывается после порта подсоединения).

### 5.5.2 Работа с Сетевым справочником сертификатов

В Сетевом справочнике находятся сертификаты пользователей и СОС, которые помещаются туда ЦР. Пользователь может добавить себе в Локальный справочник объекты, которые находятся в Сетевом справочнике. Для этого необходимо выбрать требуемые объекты в правом окне интерфейса, нажать правую клавишу «мыши» и выбрать пункт меню «Экспорт в локальный справочник».

## 5.6 Работа с несколькими профилями

При работе пользователя с несколькими базами сертификатов или одновременной работе нескольких пользователей с ПК «Справочник сертификатов» необходимо использовать профили. После установки программа работает с профилем по умолчанию, и не просит пользователя выбирать профиль. При наличии нескольких профилей ПК «Справочник сертификатов» будет запрашивать профиль (Рисунок 19).

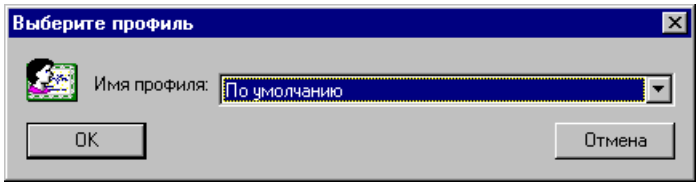


Рисунок 19 – Выбор профиля

Для создания дополнительных профилей в Справочнике, а также модификации уже существующих необходимо выбрать пункт меню «Настройки» и подпункт меню «Настройки профилей» (Рисунок 20).

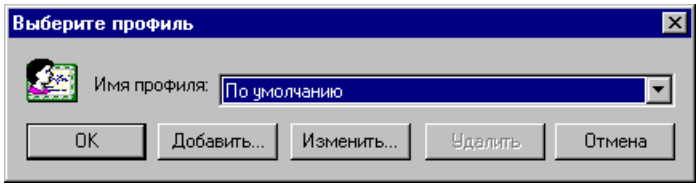


Рисунок 20 – Настройка профилей

### 5.6.1 Добавление нового профиля

Для добавления профиля необходимо нажать кнопку «Добавить...» (Рисунок 20), после этого отобразится диалоговое окно (Рисунок 21).

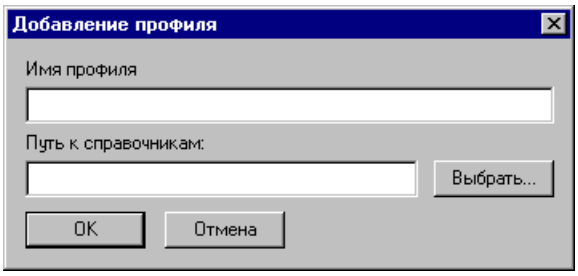


Рисунок 21 – Добавление профиля

– имя профиля – название профиля;
– путь к справочникам – каталог, в котором расположены справочники сертификатов.

Кнопка «Выбрать» служит для интерактивного выбора каталога.

### 5.6.2 Изменение профиля

Для добавления профиля необходимо выбрать нужный профиль из списка профилей и нажать кнопку «Изменить...» (Рисунок 21), после этого отобразится диалоговое окно (Рисунок 22).

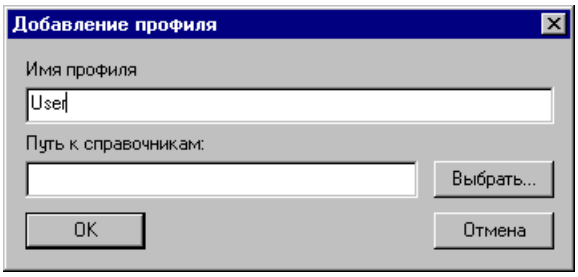


Рисунок 22 – Изменение профиля

Здесь можно изменить имя профиля и путь к справочникам данного профиля.

### 5.6.3 Удаление профиля

Для добавления профиля необходимо выбрать нужный профиль из списка профилей и нажать кнопку «Удалить...» (Рисунок 21), после этого пользователю будет задан запрос на подтверждение удаления, и, в случае положительного ответа, профиль будет удален (файлы со справочниками сертификатов и каталоги во избежание потери информации не удаляются).

## 5.7 Настройка распечаток

Для того чтобы выполнить настройки текста бланков распечаток, необходимо выбрать пункт меню «Настройки» –> «Настройка распечаток» (Рисунок 23).

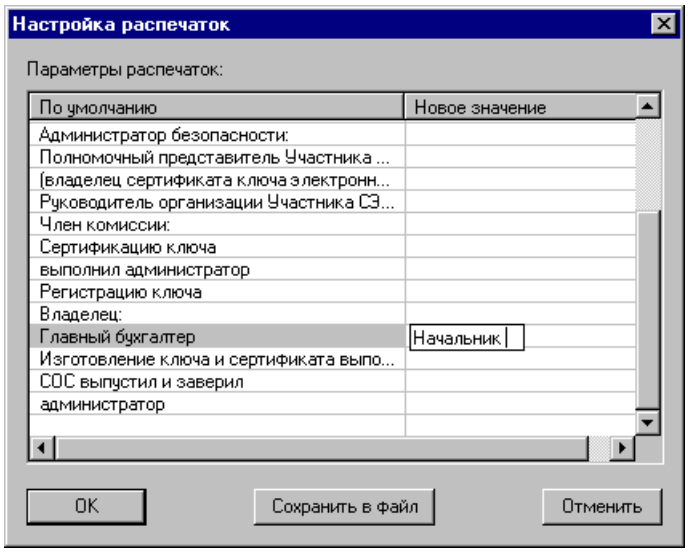


Рисунок 23 – Диалоговое окно настройки распечаток

В левой колонке диалога приведены настройки подписей распечаток «по умолчанию». Для изменения текста распечаток необходимо в правой колонке ввести новые значения и нажать кнопку «Сохранить в файл» для сохранения настроек в текстовом формата редактора реестра. На компьютере, на котором выполняется импорт параметров, необходимо выполнить команду regedit.exe <имя .reg файла> или дважды нажать левую кнопку мышки на файле с расширением .reg.

# 6 УСТАНОВКА И НАСТРОЙКА БАЗЫ ДАННЫХ

## 6.1 Требования к программному обеспечению базы данных

ПК «Справочник сертификатов» может использовать следующие базы данных (далее по тексту БД):

- Microsoft SQL Server 2008;
- Microsoft SQL Server 2008 Express;
- Microsoft SQL Server 2005 SP3;
- Microsoft SQL Server 2005 Express SP3;
- Microsoft SQL Server 2000 SP4 (далее по тексту SQL Server);
- Microsoft Desktop Engine 2000 SP4 (далее по тексту MSDE);
- Microsoft Office Access (далее по тексту Jet).

Для использования в качестве базы регистрации ПК «Справочник сертификатов» рекомендуется использовать Microsoft SQL Server 2008/2005 Express или MSDE, так как эти БД обеспечивает необходимый функционал и не требует дополнительных финансовых затрат. По соображения обеспечения безопасности при работе с БД рекомендуется установить новейший доступный пакет исправлений SP3a и использовать встроенную аутентификацию Windows.

## 6.2 Установка БД

### 6.2.1 Установка БД

Для установки необходимо запустить setup.exe из каталога дистрибутива ПО и следовать указаниям программы установки. Для работы с БД достаточно запустить сервис SQL Server.

### 6.2.2 Настройка сетевого доступа к БД

Если для доступа к БД необходим сетевой доступ (например, для удаленного управления), то необходимо добавить возможность сетевого доступа.

Для этого необходимо следовать инструкциям, описанным в MSDN:

`http://msdn.microsoft.com/ru-ru/library/ms165718(v=SQL.90).aspx.`

После выполнения необходимых настроек следует перезапустить сервис SQL Server (например, с помощью SQL Server Service Manager – sqlmangr.exe) (Рисунок 24).

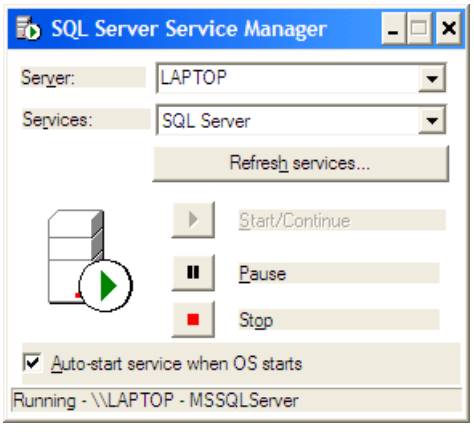


Рисунок 24 – Диалоговое окно управления сервисами SQL Server

Если же нет необходимости в сетевом доступе к БД, то по соображениям безопасности рекомендуется отключить сетевой доступ к БД (например, после завершения удаленного администрирования).

## 6.3 Настройка БД

Для настройки MSDE можно использовать утилиту командной строки osql.exe, для более новых версий ПО SQL Server рекомендуется использовать SQL Server Management Studio или Console.

### 6.3.1 Установка консоли управления

Для установки консоли управления необходимо запустить ПО установки SQL Server и выбрать установку только клиентских компонентов (Рисунок 25).

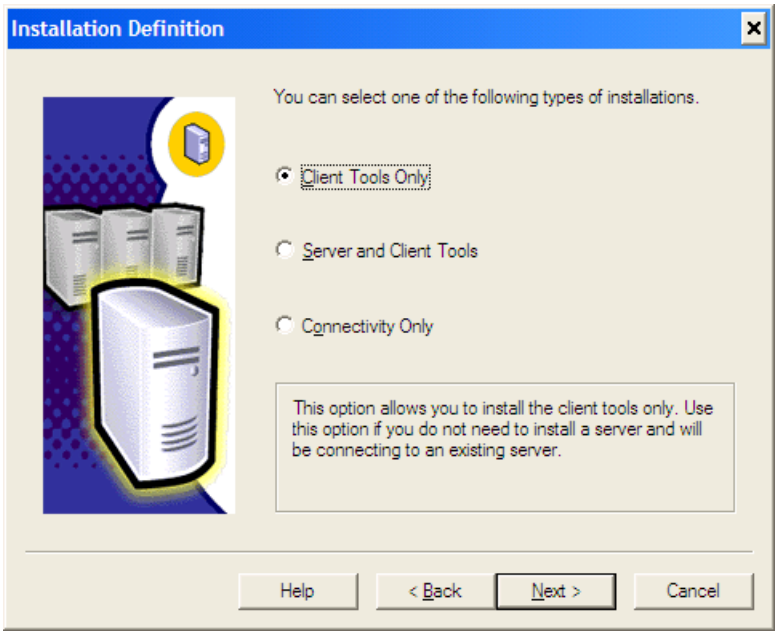


Рисунок 25 – Выбор типа установки

Для выполнения функций управления БД достаточно установить компоненты Client Connectivity и Enterprise Manager (Рисунок 26).

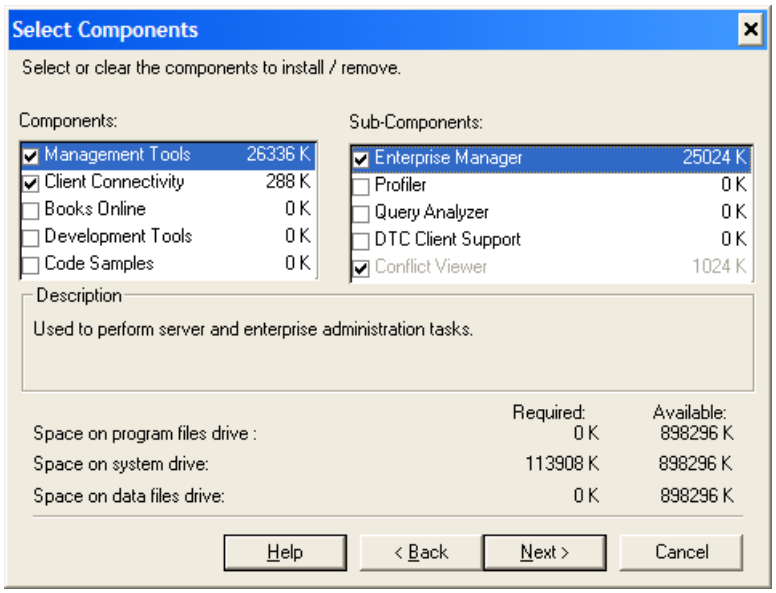


Рисунок 26 – Выбор компонентов установки

Для запуска консоли управление необходимо выбрать пункт системного меню Microsoft SQL Server | Enterprise Manager.

### 6.3.2 Создание БД

БД рекомендуется создавать от имени пользователя, который в дальнейшем будет работать с ЦР. Если этот пользователь не имеет административных прав, надо сначала запустить Enterprise Manager с правами администратора и создать для пользователя новый login (в разделе Security) (Рисунок 27).

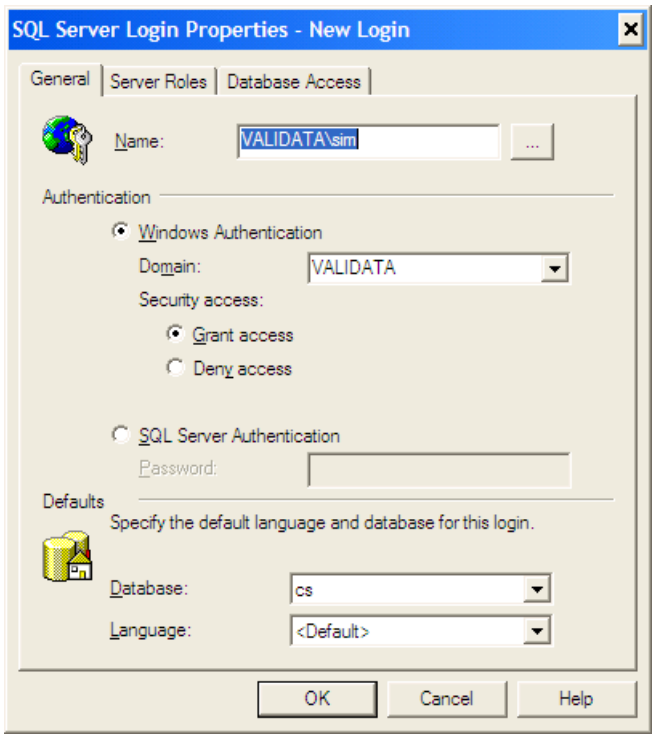


Рисунок 27 – Окно создания учетной записи

С точки зрения безопасности настоятельно рекомендуем использовать аутентификацию ОС Windows при работе с БД.

На вкладке Server Roles дайте ему роль DatabaseCreator.

Затем надо войти в Enterprise Manager под именем пользователя, выбрать папку Databases и пункт меню New Database... В диалоговом окне необходимо задать имя БД, которая будет использоваться в дальнейшем при настройке Data Source Name (далее DSN) в клиентском ПО.

Если необходимо, то можно задать другие имена для файла БД и файла протокола транзакций (вкладки Data Files и Transaction Log соответственно) (Рисунок 28).

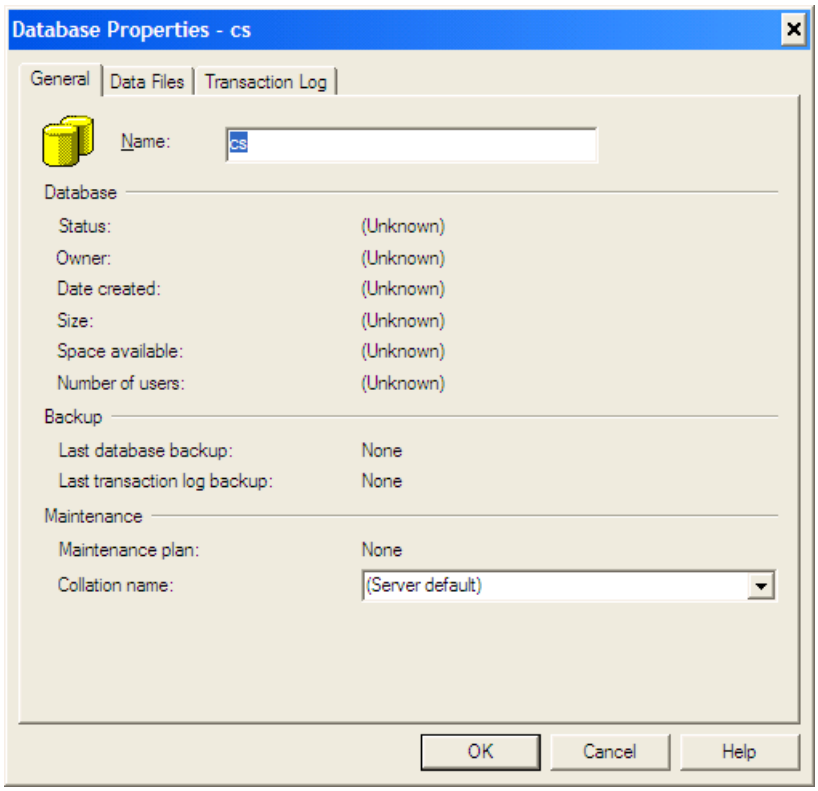


Рисунок 28 – Создание БД

В случае, если Вы (вопреки рекомендациям) создали базу, владелец которой не совпадает с пользователем, который будет работать с ЦР, Вы можете изменить владельца БД, выполнив процедуру sp_changedbowner с единственным параметром – login'ом пользователя в одинарных кавычках. Естественно, к этому моменту этот login уже должен быть создан. Если Вы решительно не хотите делать пользователя владельцем (owner'ом) БД, задайте БД «по умолчанию» для этой учетной записи и дайте ему право CreateTable в этой базе (Рисунок 29).

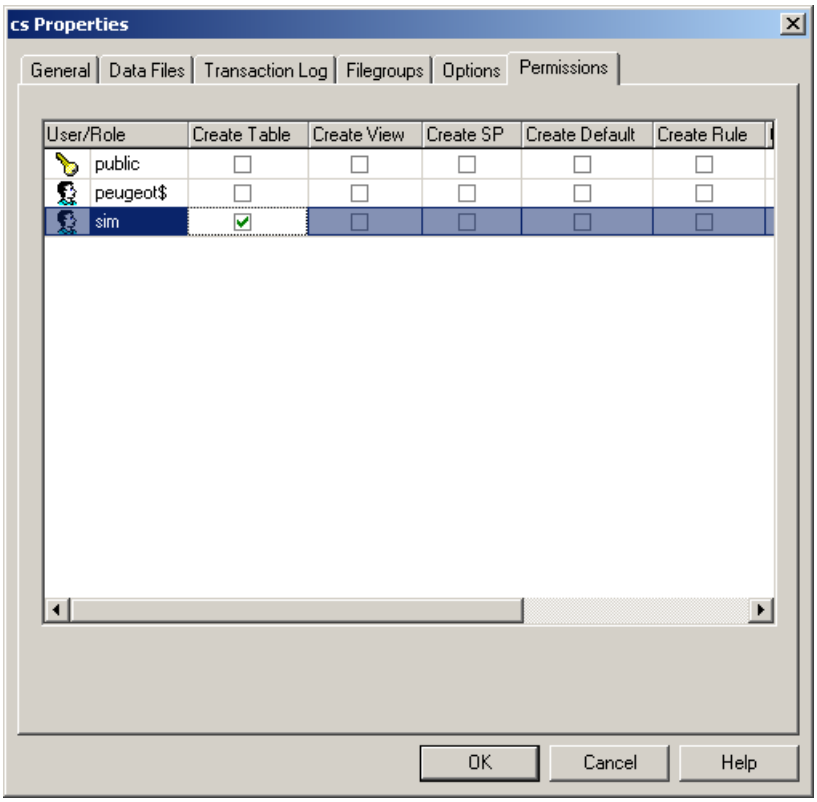


Рисунок 29 – Задание права на создание таблиц в БД

Однако, в этом случае у Вас могут возникнуть проблемы при переносе БД на другую машину методом резервного копирования/восстановления.

## 6.4 Резервное копирование БД

Для выполнения резервного копирования БД средствами SQL Server необходимо выбрать папку Management | Backup и пункт меню «Backup a database. . . » (Рисунок 30).

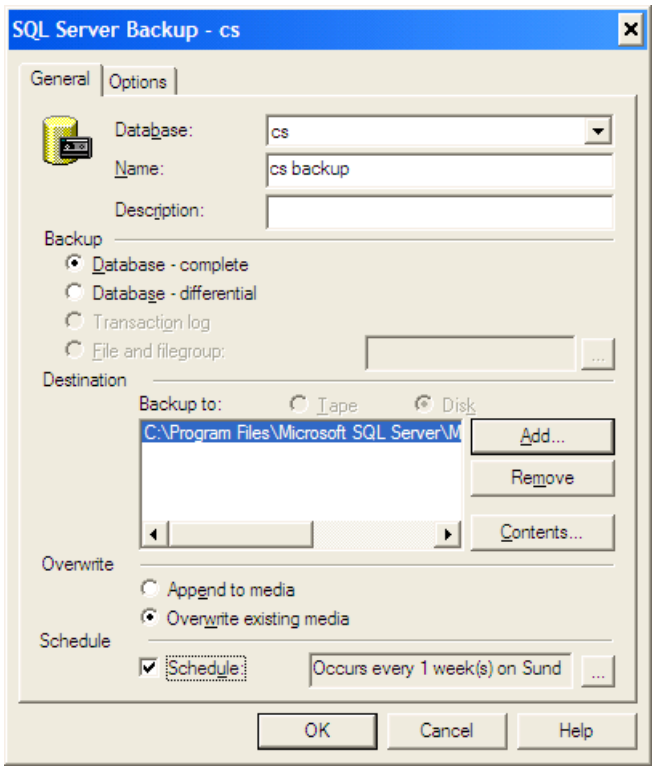


Рисунок 30 – Окно создания резервной копии

Необходимо выбрать режим резервного копирования (полный или инкрементный) в соответствии с планом резервного копирования и каталог, в который будет выполняться копирование БД (можно выбрать ленточный накопитель).

Если необходимо выполнять резервирование БД периодически, то можно задать период выполнения резервного копирования (галочка Schedule). Для этого должен быть запущен сервис SQL Server Agent.

## 6.5 Настройка подключения к базе данных

Для выполнения настройки подключения к базе данных - источнику (Data Source Name, далее DSN) необходимо нажать кнопку «Администратор ODBC» в настройках справочников или выбрать в Панели управления Windows пункт «Администрирование | Источники данных (ODBC)» или запустив апплет ODBCCP32.CPL.

В появившемся диалоговом окне (Рисунок 31) необходимо перейти на вкладку «Пользовательский DSN» (если создается DSN только для текущего пользователя) или «Системный DSN» (если создается DSN для всех пользователей этого компьютера и есть необходимые права) и необходимо нажать кнопку «Добавить...»:

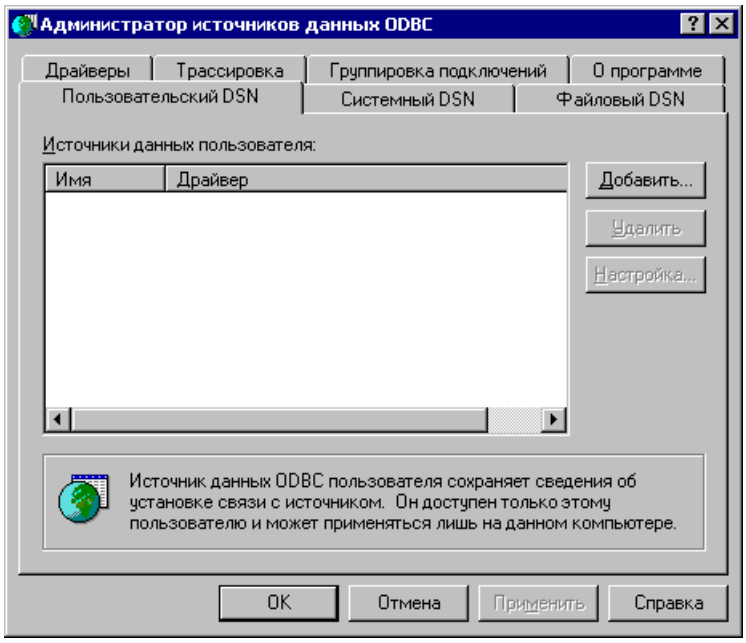


Рисунок 31 – Диалоговое окно администратора источников данных

После этого необходимо выбрать драйвер ODBC (SQL Server или Microsoft Access Driver), который будет использоваться для доступа к БД (Рисунок 32).

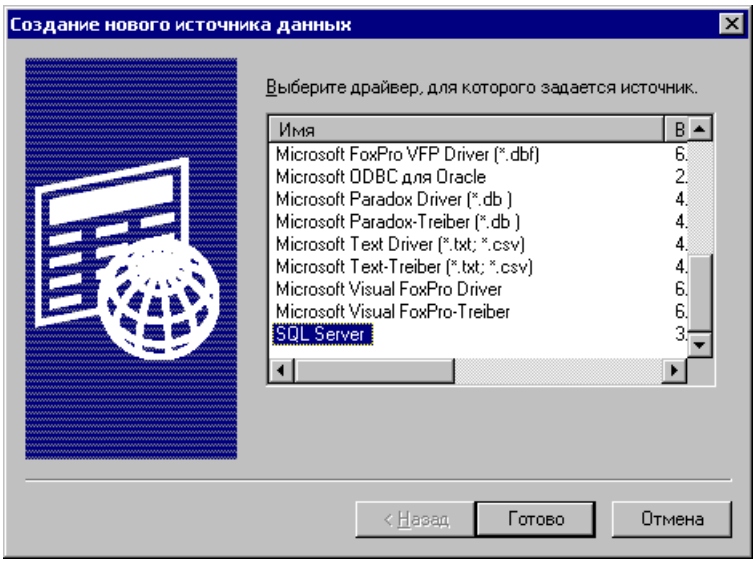


Рисунок 32 – Выбор драйвера БД

И нажать кнопку «Готово». После этого появится мастер создания источника данных (в данном случае SQL-сервера) (Рисунок 33).

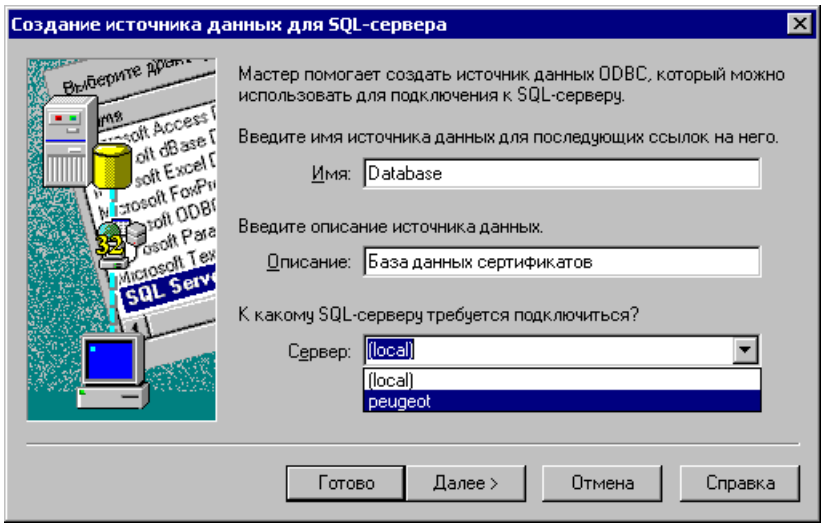


Рисунок 33 – Ввод имени источника данных

Необходимо выбрать имя источника (DSN, который в дальнейшем будет использоваться в ПК) и можно ввести описание источника данных.

Если используется сетевая БД, то необходимо выбрать доступный сервер, к которому необходимо подключиться.

После этого необходимо выбрать способ аутентификации с БД. С точки зрения безопасности рекомендуется использовать проверку подлинности учетной записи ОС Windows (Рисунок 34).

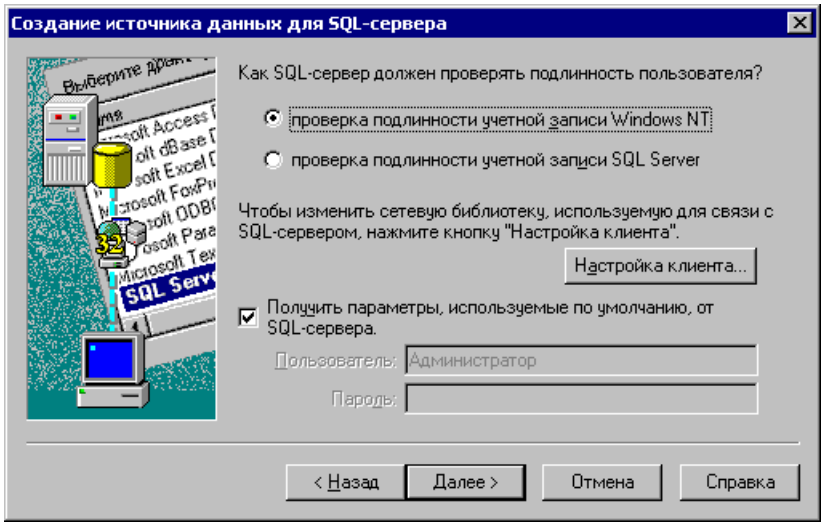


Рисунок 34 – Выбор типа аутентификации с БД

После этого необходимо выбрать базу данных «по умолчанию» для создаваемого источника (Рисунок 35).

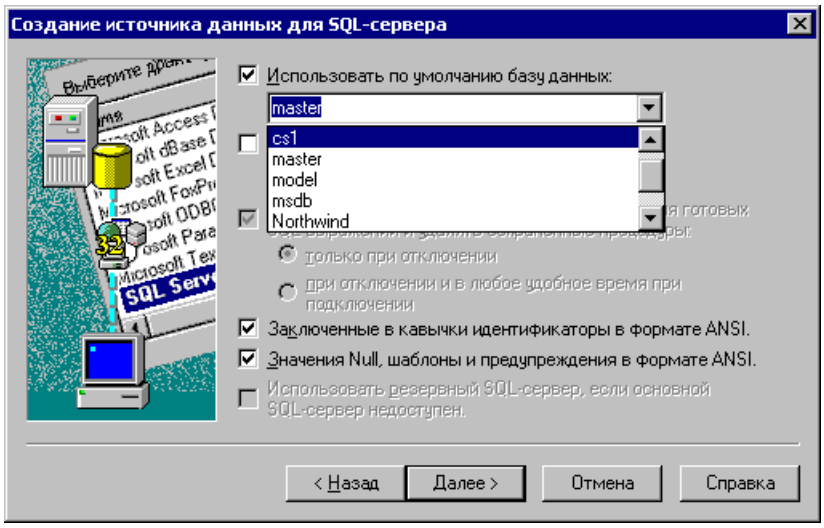


Рисунок 35 – Выбор базы данных

Необходимо, чтобы пользователь обладал достаточными правами для создания таблицы при первом подключении и для добавления/удаления записей в БД. В следующем диалоге рекомендуется оставить настройки «по умолчанию» (Рисунок 36).

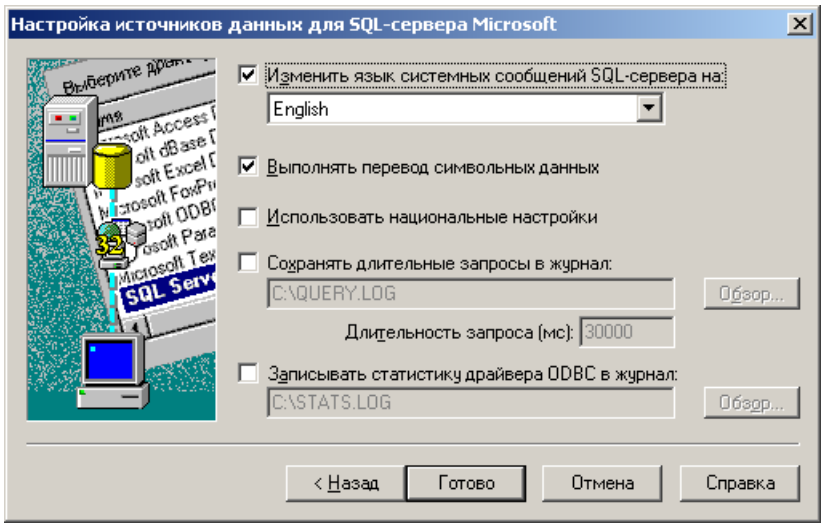


Рисунок 36 – Выбор языка

Здесь надо обратить внимание на язык системных сообщений. Он обязательно должен быть установлен в English, в противном случае возможны проблемы с преобразованием полей БД, содержащих информацию типа Дата.

При успешном подключении к БД появится диалоговое окно (Рисунок 37) с информацией об источнике (DSN).

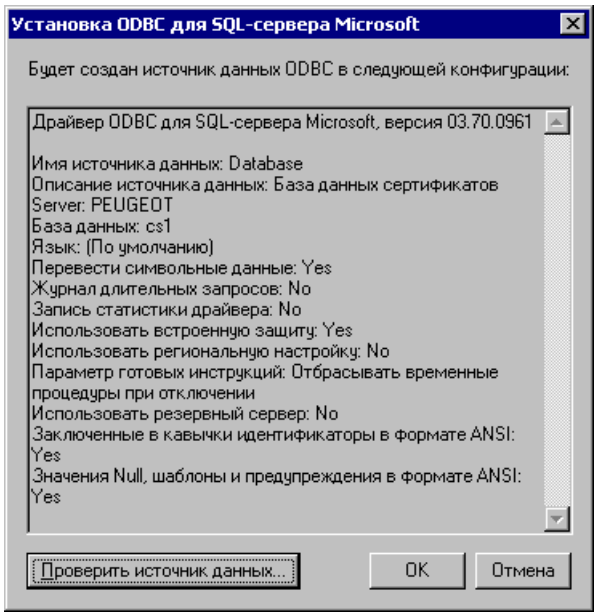


Рисунок 37 – Завершение создания источника данных

Рекомендуется нажать кнопку «Проверить источник данных...» для выполнения дополнительной проверки и после этого нажать кнопку «OK».

Если же при подключении произошла ошибка, то появится диалоговое окно с сообщением об ошибке (Рисунок 38).

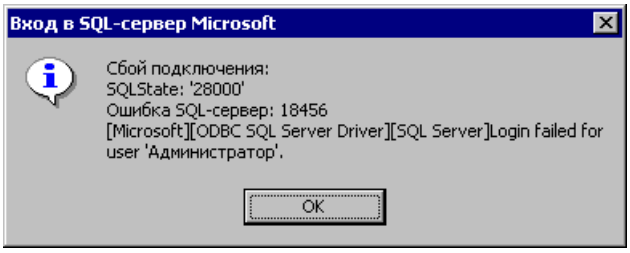


Рисунок 38 – Сообщение об ошибке

В этом случае необходимо проверить доступность сервера БД и настройки сервера (в данном примере проверить пароль и имя пользователя для подключения к БД).

После этого имя источника данных появится в списке DSN «Администратора источников данных ODBC», и его можно использовать для доступа к БД в ПК. Для изменения настроек источника необходимо нажать кнопку «Настройка...» (см. Рисунок 34).

# 7 УДАЛЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

## 7.1 Удаление программного обеспечения

Перед запуском процедуры удаления программного обеспечения необходимо зарегистрироваться на ПЭВМ с правами локального администратора.

Для удаления используйте пункт системного меню ОС Windows «Пуск», «Настройка», «Панель управления», «Установка и удаление программ».

Выберите пункт «АПК Клиент МБ: Справочник Сертификатов» и нажмите кнопку «Удалить». После этого появится диалоговое окно подтверждения удаления.

Необходимо нажать кнопку «Да». После этого будет выполнено удаление программного обеспечения. После завершения удаления рекомендуется выполнить перезагрузку операционной системы.

## 7.2 Удаление настроек программного обеспечения для пользователя

Так как ПК использует для хранения некоторых своих настроек каталоги и ключи реестра, которые доступны только пользователю, который выполнил интерактивный вход на данный компьютер (в каталоге профиля пользователя и ключе HKEY_CURRENT_USER), то для полного удаления программного обеспечения необходимо выполнить следующие действия для каждого пользователя, который запускал ПК:

а) Удалить ключ реестра HKCU\Software\VALIDATA\XCS.

б) Удалить файл из каталога данных с профилем пользователя каталог Validata\XCS.

# 8 УСТАНОВКА, УДАЛЕНИЕ И НАСТРОЙКА ПРОГРАММЫ STUNNEL

## 8.1 Установка и удаление

Программа STunnel, представляющая собой исполняемый модуль **stunnel.exe**, входит в состав ПК "Справочник сертификатов" и программного исполняемого модуля командной строки для ОС Windows, соответственно и установка/удаление программы STunnel выполняется при установке/удалении данных комплексов.

Программа STunnel предназначена для защиты данных, передаваемых по TCP соединениям, посредством оборачивания (инкапсуляции) этих данных протоколом TLS.

По умолчанию, установка программы STunnel не производится. Для установки программы STunnel следует произвести либо полную установку выбранного комплекса, либо выборочную установку с включенным компонентом "Программный модуль обеспечивающий создание защищенных соединений STunnel".

## 8.2 Настройка

Настройка программы STunnel заключается в редактировании текстового конфигурационного файла программы *stunnel.conf*, находящегося в каталоге установки ПК "Справочник сертификатов" и/или программного исполняемого модуля командной строки для ОС Windows.

*Конфигурационный файл stunnel.conf:*

```
; Debugging stuff (may useful for troubleshooting)
;debug = 7
;output = stunnel.log

; Authentication stuff needs to be configured to prevent MITM attacks
; It is not enabled by default!
verify = 2

options = NO_TICKET

socket = l:TCP_NODELAY=1
socket = r:TCP_NODELAY=1

; ************************************************************
; * Service definitions (at least one service has to be defined) *
; ************************************************************

; Example SSL server mode services

[tls1-http-server]
accept = 0.0.0.0:4433
connect = 127.0.0.1:80
TIMEOUTclose = 0

; Example SSL client mode services

[tls1-http-client]
client = yes
accept = 0.0.0.0:8080
connect = 127.0.0.1:4433
TIMEOUTclose = 0
```

Конфигурационный файл *stunnel.conf* состоит из основной секции и секций настроек клиента или сервера. Основная секция начинается с начала (т.е. с первой строки) конфигурационного файла, и продолжается до начала первой секции клиента или сервера. Секция клиента или сервера всегда начинается с идентификатора секции, заключенного в квадратные скобки, т.е. с выражения вида *[Секция]*.

Каждой секции принадлежит список параметров с присвоенными им значениями (Таблица 3, Таблица 4). Для присвоения заданного значения определенному параметру используется выражение вида *Параметр = Значение*. Символ *';'* используется для обозначения комментария.

Таблица 3 – Основная секция

| **Параметр** | **Возможные значения и описание применения** |
|---|---|
| debug | Принимает значения от 0 до 7 и указывает используемый уровнь протоколирования. При установленном значении 0 протоколируются только критические ошибки, при установленном значении 7 протоколируются все (в т.ч. и отладочные) сообщения (т.е. большее значение уровня протоколирования соответствует большему количеству выводимых сообщений). |
| output | Имя файла для записи протоколируемых сообщений. При отсутствии значения сообщения записываются в поток стандартного вывода. |
| verify | Принимает значения от 0 до 3 и указывает тип проверки цепочки сертификата противоположной стороны:<br>— Значение 0 - не проверять цепочку сертификата противоположной стороны;<br>— Значение 1 - проверять цепочку сертификата противоположной стороны только при наличии этого сертификата;<br>— Значение 2 - обязательно проверять цепочку сертификата противоположной стороны. Для клиента обязательно будет проверяться соответствие имени владельца сертификата сервера и DNS имени удаленного узла. Для сервера обязательно будет проверяться наличие сертификата у клиента;<br>— Значение 3 - выполнять те же проверки, что и в предыдущем пункте, используя исключительно сертификаты и COC из локального справочника (т.е. не используя точки AIA и CDP). |
| CRLinterval | Принимает целые неотрицательные (>= 0) значения и задает период автоматического обновления COC в минутах. При значении равном 0 автоматическое обновление COC не производится. |
| options | Позволяет настраивать параметры протокола TLS (допускается наличие нескольких значений):<br>— NO_SESSION_RESUMPTION_ON_RENEGOTIATION - отключает возможность повторного использования ранее установленного сеанса связи при выполнении переподключения (применим только к серверной стороне);<br>— ALLOW_UNSAFE_LEGACY_RENEGOTIATION - отключает требование безопасного переподключения по RFC 5746. |
| socket | Позволяет настраивать параметры TCP подключения (допускается наличие нескольких значений):<br>— l:SO_KEEPALIVE=1 - включает возможность использования TCP пакетов Keep-Alive для локального TCP сокета;<br>— r:SO_KEEPALIVE=1 - включает возможность использования TCP пакетов Keep-Alive для удаленного TCP сокета;<br>— l:TCP_NODELAY=1 - отключает возможность использования задержки передачи данных (алгоритм Нейгла, RFC 896) для локального TCP сокета;<br>— r:TCP_NODELAY=1 - отключает возможность использования задержки передачи данных (алгоритм Нейгла, RFC 896) для удаленного TCP сокета. |

Таблица 4 – Секция клиента или сервера

| **Параметр** | **Возможные значения и описание применения** |
|---|---|
| client | Принимает значения *yes* и *no*. Значение *yes* следует устанавливать для секции клиента, значение *no* (или отсутствие параметра) следует устанавливать для секции сервера. |
| accept | DNS имя (или IP адрес) и TCP порт для входящих подключений, разделенные символом *':'*. Для секции клиента по входящему подключению передаются открытые данные, для секции сервера - данные, защищенные протоколом TLS. |
| connect | DNS имя (или IP адрес) и TCP порт для исходящих подключений, разделенные символом *':'*. Для секции клиента по исходящему подключению передаются данные, защищенные протоколом TLS, для секции сервера - открытые данные. |
| TIMEOUTbusy | Максимальное количество секунд (>= 0), которое следует ожидать до получения необходимых данных при установлении сеанса связи. |
| TIMEOUTclose | Максимальное количество секунд (>= 0), которое следует ожидать до получения предупреждения TLS close_notify, сигнализарующего о завершении сеанса связи, до выполнения принудительного завершения сеанса. |

| Параметр | Возможные значения и описание применения |
|---|---|
| TIMEOUTconnect | Максимальное количество секунд (>= 0), которое следует ожидать при выполнении TCP подключения к удаленному узлу. |
| TIMEOUTidle | Максимальное количество секунд (>= 0), которое следует ожидать перед завершением неактивного сеанса связи (т.е. при условии отсутствия передаваемых данных). |

*Примечание - Для возможности совместной работы программы STunnel и Средства КЗИ по протоколу TLS необходимо в диалоговом окне конфигурации TLS монитора, входящего в состав Средства КЗИ, включить опцию "Игнорировать список владельцев сертификатов ЦС". Такая настройка необходима при конфигурации, в которой с одной стороны используется модуль поддержки TLS СКЗИ, а с другой - STunnel (т.е. клиент и сервер используют различные реализации протокола TLS). Программа STunnel намеренно не использует список владельцев сертификатов ЦС, поскольку она изначально была рассчитана на совместную работу с ССС, в котором хранятся сертификаты ЦС второго уровня (т.е. STunnel рассчитана на динамический список сертификатов ЦС).*

# ПРИЛОЖЕНИЕ А АДМИНИСТРАТИВНАЯ УСТАНОВКА

Программа установки, созданная с помощью Windows Installer, позволяет применять при запуске некоторые параметры командной строки, контролирующие ее выполнение. В данном приложении приводится список данных параметров и описывается назначение каждого из них.

Программа установки поддерживает так называемую «административную» установку, которая помогает администратору при внедрении ПО в корпоративной сети.

ВАЖНО:

– параметры командной строки нечувствительны к регистру символов, например, параметр «/V» имеет то же значение, что и «/v»;

– при одновременном использовании нескольких параметров командной строки необходимо разделять их пробелом.

Ниже приведен список параметров командной строки:

| **Параметр** | **Описание** | **Пример использования** |
|---|---|---|
| /a | Запускает административную установку | msiexec.exe /a |
| /j [u\|m] <msi-файл> | Создает ярлык приложения. При использовании данного параметра игнорируются некоторые введенные свойства и параметры | msiexec.exe /j xpki.msi |
| /i | Позволяет задать msi-файл для установки. При отсутствии данного параметра программа установки использует файл, заданный в setup.ini. | msiexec.exe /i cpki.msi /t ProgramMgmt.mst |
| /o<property=value> | Устанавливает свойства для msi-файла. Программа установки применяет их при работе MSIEXEC. | msiexec.exe /o PIDKEY=12345-12345-12345-12345-12345 |
| /q | Определяет интерфейс программы установки. “/q” - интерфейс отсутствует (“/qn” - для MSIEXEC) | msiexec.exe /q |
| /qb | Базовый интерфейс | msiexec.exe /qb |
| /qr | Сокращенный интерфейс | msiexec.exe /qr |
| /qn | Без пользовательского интерфейса | msiexec.exe /qn |
| /L | Задает путь и уровень протоколирования | msiexec.exe /L[i\|w\|e\|a\|r\|u\|c\|m\|o\|] Logfile |

## Лист регистрации изменений

| Номера листов (страниц) | | | | | Всего листов (страниц) в докум | № документа | Входящий № сопроводительного докум и дата | Подп | Дата |
|---|---|---|---|---|---|---|---|---|---|
| Изм | изменённых | заменённых | новых | аннулированных | | | | | |
| 1 | | Все | | | | ВАМБ.00075-02.001 | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |