ПАО «МОСКОВСКАЯ БИРЖА»

УТВЕРЖДЕН
ВАМБ.00075-02–ЛУ

АППАРАТНО-ПРОГРАММНЫЙ КОМПЛЕКС «КЛИЕНТ МБ» ВЕРСИЯ 2.0

ПРОГРАММНЫЙ КОМПЛЕКС«СПРАВОЧНИК СЕРТИФИКАТОВ»

РУКОВОДСТВО ОПЕРАТОРА

ВАМБ.00075-02 34 01

2015

Аннотация

Данный документ содержит описание эксплуатации программного комплекса (ПК) «Справочник сертификатов» (далее по тексту - ПК «Справочник сертификатов» или Справочник).

Документ предназначен для пользователей как руководство по эксплуатации Справочника.

Содержание

1 ТРЕБОВАНИЯ К ОПЕРАЦИОННОЙ СРЕДЕ И АППАРАТНОМУ ОБЕСПЕЧЕНИЮ 5

2 СОСТАВ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ 6

3 НАЗНАЧЕНИЕ ПРОГРАММНОГО КОМПЛЕКСА 7

4 РЕГИСТРАЦИЯ ПОЛЬЗОВАТЕЛЯ В ЦЕНТРЕ РЕГИСТРАЦИИ 8

5 ЗАПУСК ПК СПРАВОЧНИК СЕРТИФИКАТОВ 9

5.1 Запуск ПК «Справочник сертификатов» . . . 9
5.2 Установка сертификата регистрации и ключа регистрации . . . 9
5.3 Установка резервной копии справочников полученной в Центре Регистрации . . . 9

6 РАБОТА СО СПРАВОЧНИКОМ 10

6.1 Интерфейс и структура Справочника . . . 10
6.2 Настройка Справочника . . . 12
6.3 Формирование личных ключей пользователя . . . 17
6.3.1 Передача созданного запроса в ЦР . . . 18
6.3.2 Печать бланка запроса . . . 20
6.3.3 Формирование резервной копии ключа ЭП . . . 20
6.4 Получение личного сертификата пользователя . . . 20
6.5 Разграничение прав доступа на использование Справочника . . . 20
6.5.1 Установка пароля . . . 21
6.5.2 Изменение пароля . . . 21
6.5.3 Удаление пароля . . . 21
6.6 Добавление сертификатов . . . 21
6.7 Отображение объектов в интерфейсе . . . 23
6.7.1 Общая информация об объекте или списке объектов . . . 23
6.7.2 Информация об объекте в диалоге отображения объекта . . . 23
6.7.3 Диалог отображения сертификата . . . 23
6.7.4 Диалог отображения запроса на сертификат . . . 26
6.7.5 Диалог отображения списка отозванных сертификатов . . . 27
6.7.6 Диалог отображения сообщения о компрометации . . . 29
6.8 Обновление сертификата ЦС . . . 29
6.9 Обновление списка отозванных сертификатов . . . 29
6.10 Запись объектов Справочника на внешний носитель . . . 30
6.11 Компрометация ключа пользователя . . . 30
6.12 Окончание действия объектов Справочника . . . 31
6.13 Печать бланков объектов . . . 32
6.14 Настройка интерфейса Справочника . . . 32
6.14.1 Настройка отображения . . . 32
6.14.2 Сохранение отображения в файл . . . 33
6.15 Журнал Справочника . . . 33
6.16 Резервное копирование и восстановление Справочника . . . 33
6.16.1 Резервное копирование . . . 33

6.16.2 Полное восстановление справочников . . . 34
6.16.3 Ручное восстановление справочников . . . 35
6.16.4 Восстановление базы справочника при использовании ODBC . . . 36
6.17 Сетевые справочники сертификатов . . . 37
6.17.1 Добавление Сетевого справочника . . . 37
6.17.2 Работа с Сетевым справочником сертификатов . . . 38
6.17.3 Обновление Сетевого справочника сертификатов . . . 38
6.17.4 Удаление Сетевого справочника сертификатов . . . 38
6.18 Фильтрация объектов при работе с ODBC хранилищем . . . 39
6.18.1 Фильтрация сертификатов . . . 39
6.18.2 Фильтрация СОС . . . 40
6.18.3 Фильтрация запросов на сертификат . . . 41
6.18.4 Фильтрация запросов на отзыв сертификата . . . 42
6.19 Поиск объектов в Справочнике . . . 43
6.20 Работа с несколькими профилями . . . 46
6.20.1 Добавление нового профиля . . . 47
6.20.2 Изменение профиля . . . 47
6.20.3 Удаление профиля . . . 48
6.21 Настройка распечаток . . . 48

7 РАСШИРЕНИЕ ПРОВОДНИКА 49
7.1 Запуск расширения проводника . . . 49
7.2 Настройка расширения проводника . . . 50
7.2.1 Общие настройки расширения проводника . . . 50
7.2.2 Настройки безопасности расширения проводника . . . 52
7.2.3 Дополнительные настройки расширения проводника . . . 54
7.3 Загрузка и выгрузка ключа . . . 55
7.4 Криптографические операции над файлами . . . 56
7.4.1 Создание ЭП . . . 56
7.4.2 Проверка ЭП . . . 57
7.4.3 Проверка и удаление ЭП . . . 61
7.4.4 Удаление ЭП без проверки . . . 63
7.4.5 Зашифрование . . . 65
7.4.6 Расшифрование . . . 71
7.4.7 Получение криптографической информации . . . 73
7.4.8 Создание отсоединённой ЭП . . . 75
7.4.9 Проверка отсоединённой ЭП . . . 77
7.5 Закодирование в формат Base64 . . . 81
7.6 Раскодирование из формата Base64 . . . 83
7.7 Хэширование файлов . . . 84
7.8 Протоколирование в расширении проводника . . . 85

8 ССЫЛКИ 88

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;
- 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 НАЗНАЧЕНИЕ ПРОГРАММНОГО КОМПЛЕКСА

Программный комплекс «Справочник сертификатов» предназначен для:

– формирования защищенного персонального справочника пользователя, содержащего сертификат главного ЦС;

– формирования личных ключей ЭП и ключей проверки ЭП пользователей системы электронного документооборота (СЭД) МБ с использованием различных ключевых носителей;

– формирования запроса на сертификат в формате PKCS#10 с использованием созданного личного ключа ЭП и ключа проверки ЭП;

– передачи запроса в защищенном виде в ЦР;

– добавления и удаления сертификатов, списков отозванных сертификатов (СОС);

– проверки и отображения состояния сертификатов, связанного с окончанием их сроков действия или их отзыва СОС;

– формирования и передачи в ЦР сообщения и компрометации ключа пользователя;

– отображения содержания и вывода на печать сертификатов, запросов, СОС и сообщений о компрометации;

– обновление СОС с использованием сетевого справочника;

– восстановление персонального и локального справочника с резервной копии (Мобильный справочник пользователя).

4 РЕГИСТРАЦИЯ ПОЛЬЗОВАТЕЛЯ В ЦЕНТРЕ РЕГИСТРАЦИИ

Перед началом работы в системе каждый пользователь должен выполнить процедуру регистрации в ЦР. Для этого пользователь системы или администратор безопасности прибывают в ЦР с документами, необходимыми для регистрации пользователя в прикладной системе. Регистрация может быть осуществлена через Администратора ЦР или Оператора ЦР.

В процессе формирования первичного сертификата в ЦР создается ключ ЭП и/или закрытый ключ шифрования пользователя, а также запрос на получение первичного сертификата пользователя. Далее сформированный запрос передается в ЦС (либо Администратору ЦС, либо оператору ЦС) для выпуска сертификата пользователя.

После выпуска сертификата он передается пользователю. Для получения сертификата личная явка пользователя не требуется, так как сертификат защищен ЭП, выполненной на ключе ЭП Администратора ЦС.

5 ЗАПУСК ПК СПРАВОЧНИК СЕРТИФИКАТОВ

5.1 Запуск ПК «Справочник сертификатов»

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

5.2 Установка сертификата регистрации и ключа регистрации

При каждом запуске Справочник проверяет наличие и целостность персонального справочника пользователя (ПСП). При первом запуске ПО персональный справочник отсутствует, и будет выдано сообщение об ошибке.

Для продолжения процедуры выберите файл, содержащий сертификат регистрации пользователя. После выбора сертификата регистрации производится формирование персонального и локального справочника с использованием сертификатов, находящихся в сертификате регистрации. ПО Справочника попросит загрузить ключ (ключ регистрации) с определенным идентификатором с использованием выбранного устройства считывания, соответствующий сертификату регистрации. Идентификатор ключа представляет собой последовательность цифр от “0” до “9” и букв от “A” до “Z” длиной 16 символов и соответствует идентификатору ключа, содержащемуся в сертификате.

В случае загрузки ключа, не соответствующего сертификату регистрации, диалоговый интерфейс Справочника попросит повторить процедуру загрузки.

После загрузки ключа регистрации создается персональный и локальный справочник. Персональный справочник пользователя защищается ЭП с использованием ключа регистрации.

После завершения процедуры регистрации пользователю выдается сообщение с предложением сформировать запрос на сертификат (новые ключ ЭП и ключ проверки ЭП пользователя). При отказе от его создания пользователь попадает в основной интерфейс Справочника или переходит к процедуре формирования запроса (см. п. 6.3).

5.3 Установка резервной копии справочников полученной в Центре Регистрации

При первом запуске пользователю выдается запрос “Есть ли у Вас резервная копия из Центра Регистрации для установки справочников?”. При ответе “ДА” пользователю необходимо указать каталог, в котором находится резервная копия, полученная в Центре Регистрации. После восстановления справочников, программа завершит свою работу. При следующем запуске программы программа будет работать уже с восстановленными справочниками в нормальном режиме.

6 РАБОТА СО СПРАВОЧНИКОМ

6.1 Интерфейс и структура Справочника

Графический интерфейс и структура Справочника приведена на рисунке (Рисунок 1).

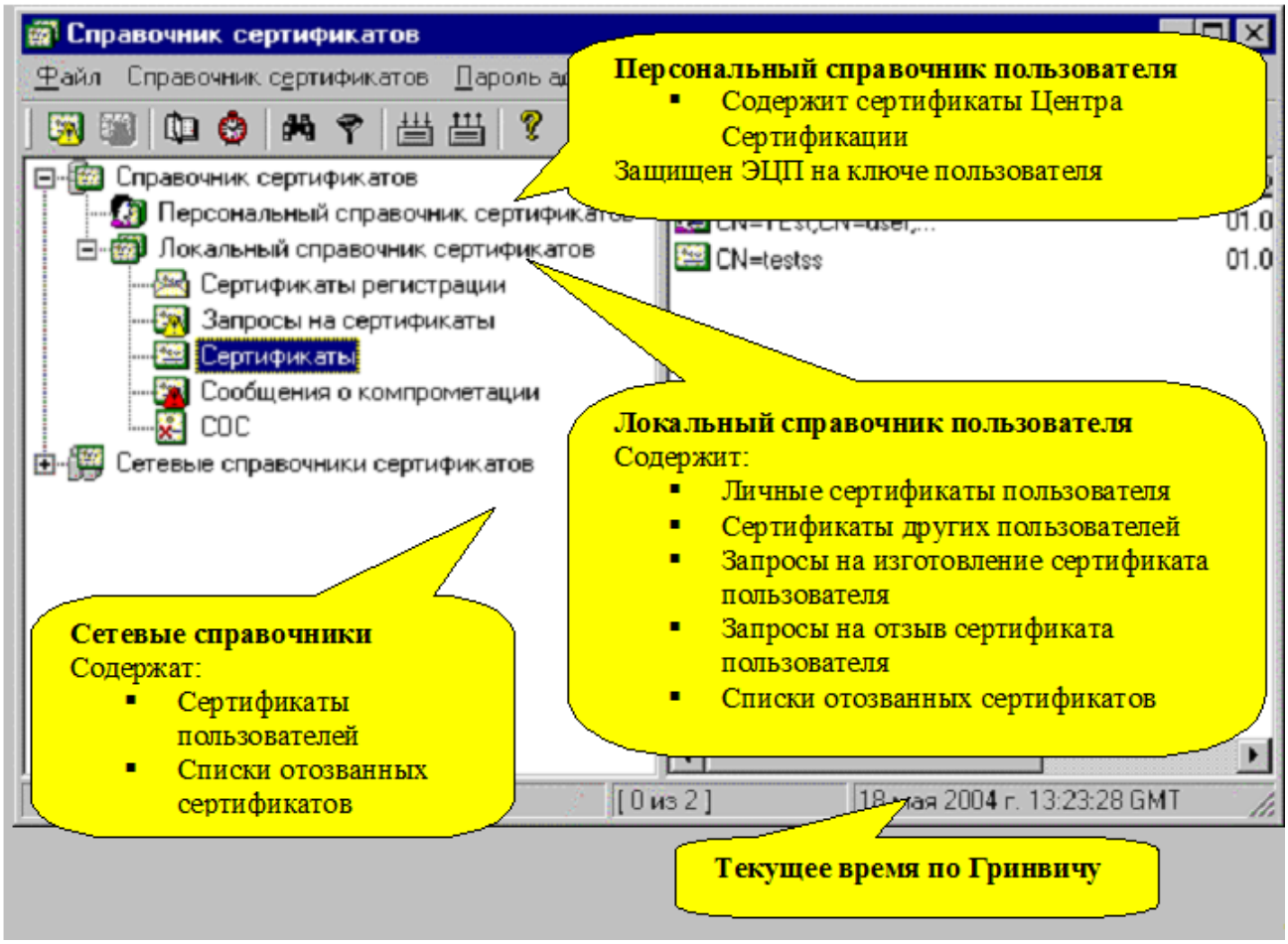

Рисунок 1 – Интерфейс Справочника

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.

6.2 Настройка Справочника

Для настройки Справочника необходимо выбрать из основного меню «Настройки», «Настройка Справочника сертификатов». Появиться диалоговое окно для настройки параметров Справочника (Рисунок 2). 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».

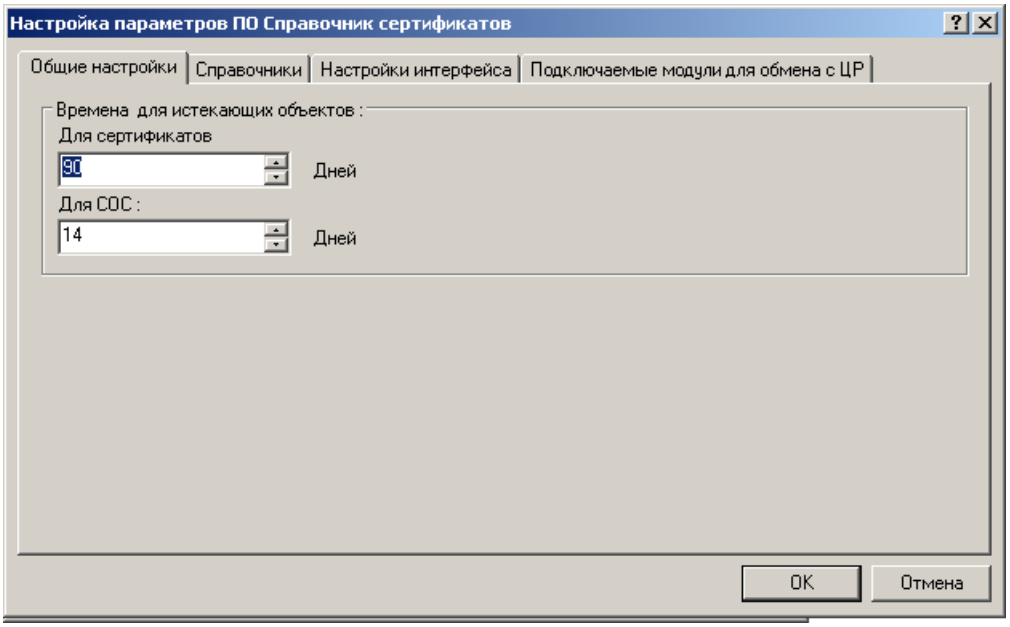

Рисунок 2 – Окно «Общие настройки»

На закладке «Справочники» (Рисунок 3) 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».

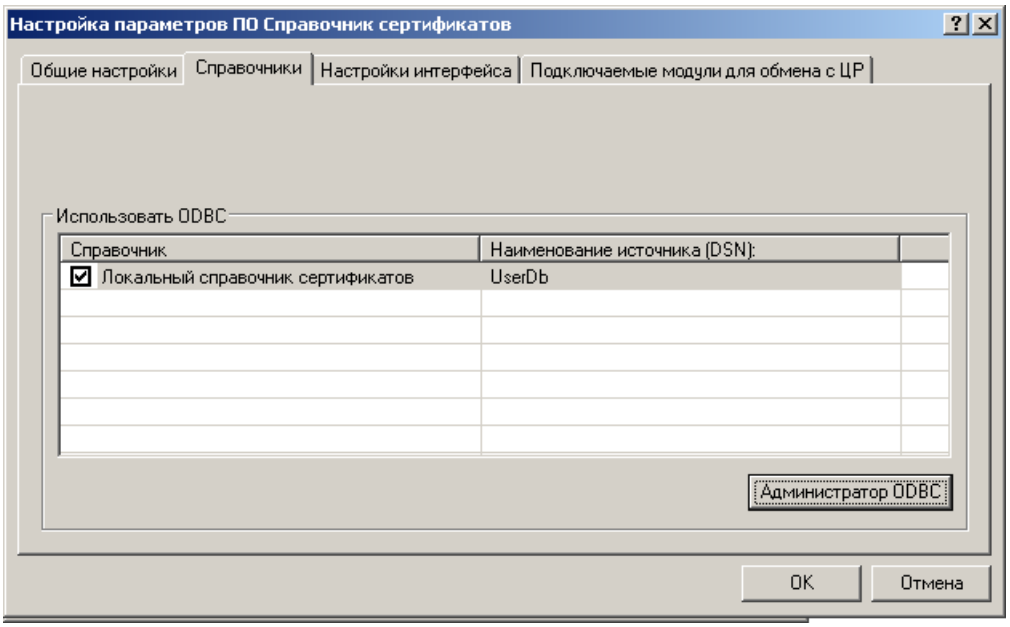

Рисунок 3 – Окно «Настройка Справочника»

На закладке «Настройки интерфейса» (Рисунок 4) 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.

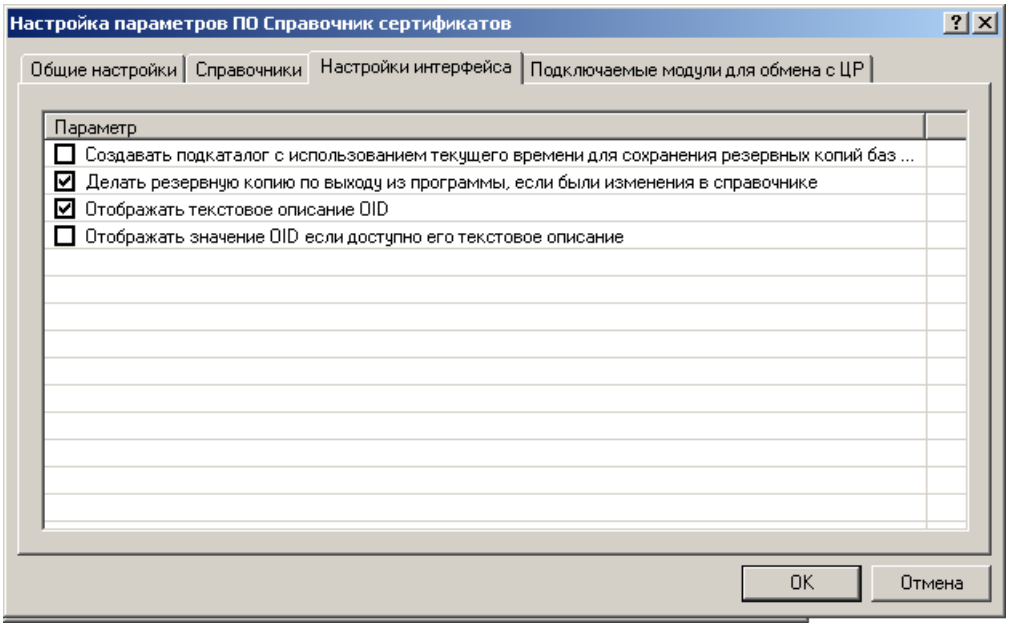

Рисунок 4 – Окно «Настройки интерфейса»

На закладке "Настройки автоматического режима"(Рисунок 5) можно настроить интервал (в секундах) автоматической проверки обновлений справочника.

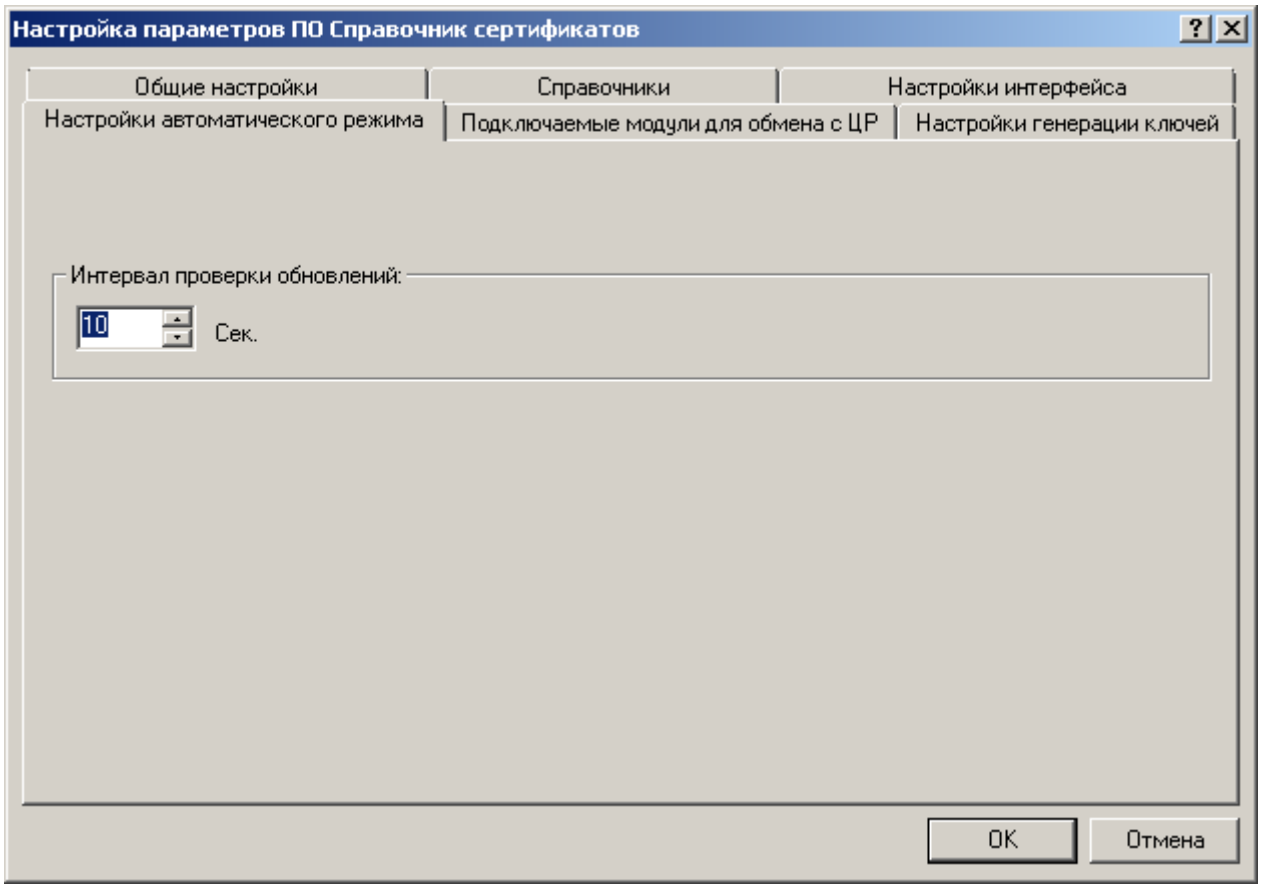

Рисунок 5 – Окно «Настройки автоматического режима»

На закладке "Подключаемый модули для обмена с ЦР"(Рисунок 6) 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 6). 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».

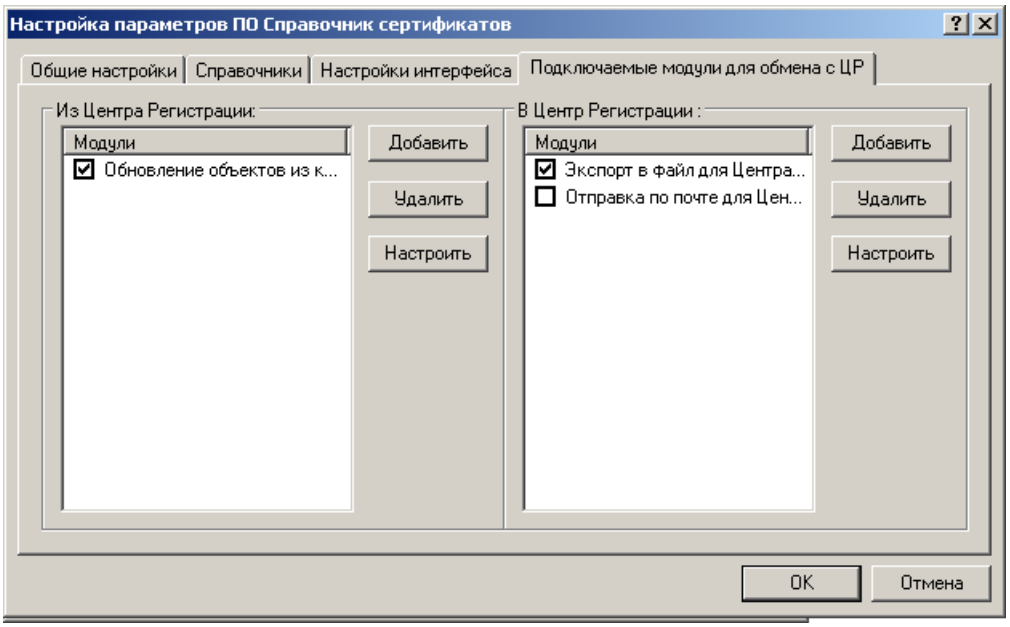

Рисунок 6 – Окно «Подключаемые модули для обмена с ЦР»

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 7). В поле «Адрес ЦР» необходимо указать почтовый адрес Центра Регистрации в формате RFC 822.

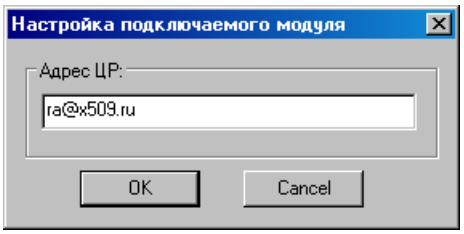

Рисунок 7 – Настройка модуля «Отправка по почте для Центра Регистрации»

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 8). 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.

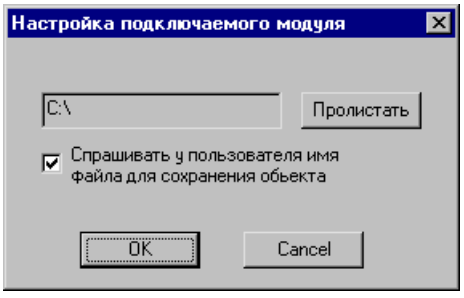

Рисунок 8 – Настройка модуля «Экспорт в файл для Центра Регистрации»

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 9). 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.

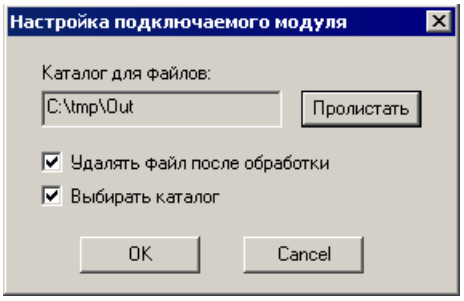

Рисунок 9 – Настройка модуля «Обновление объектов из каталога»

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 10). В поле «Адрес WEB сервера ЦР» необходимо указать URL WEB сервера ЦР.

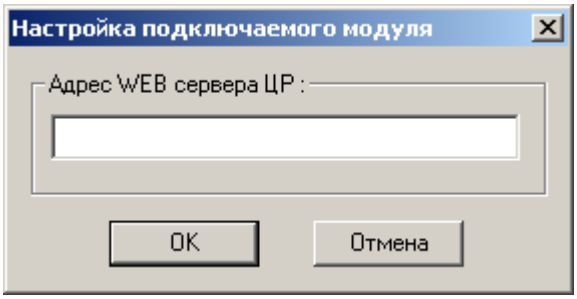

Рисунок 10 – Настройка модуля «Обновление объектов с WEB сервера ЦР»

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

Диалоговое окно настройки модуля аналогично диалоговому окну настройки модуля «Обновление объектов с WEB сервера ЦР» (Рисунок 10).

Для удаления модуля необходимо выбрать необходимый модуль и нажать кнопку «Удалить» (Рисунок 6).

На закладке "Настройки генерации ключей"(Рисунок 11) можно указать алгоритм, по которому будут создаваться ключи (выбрать соответствующий стандарт).

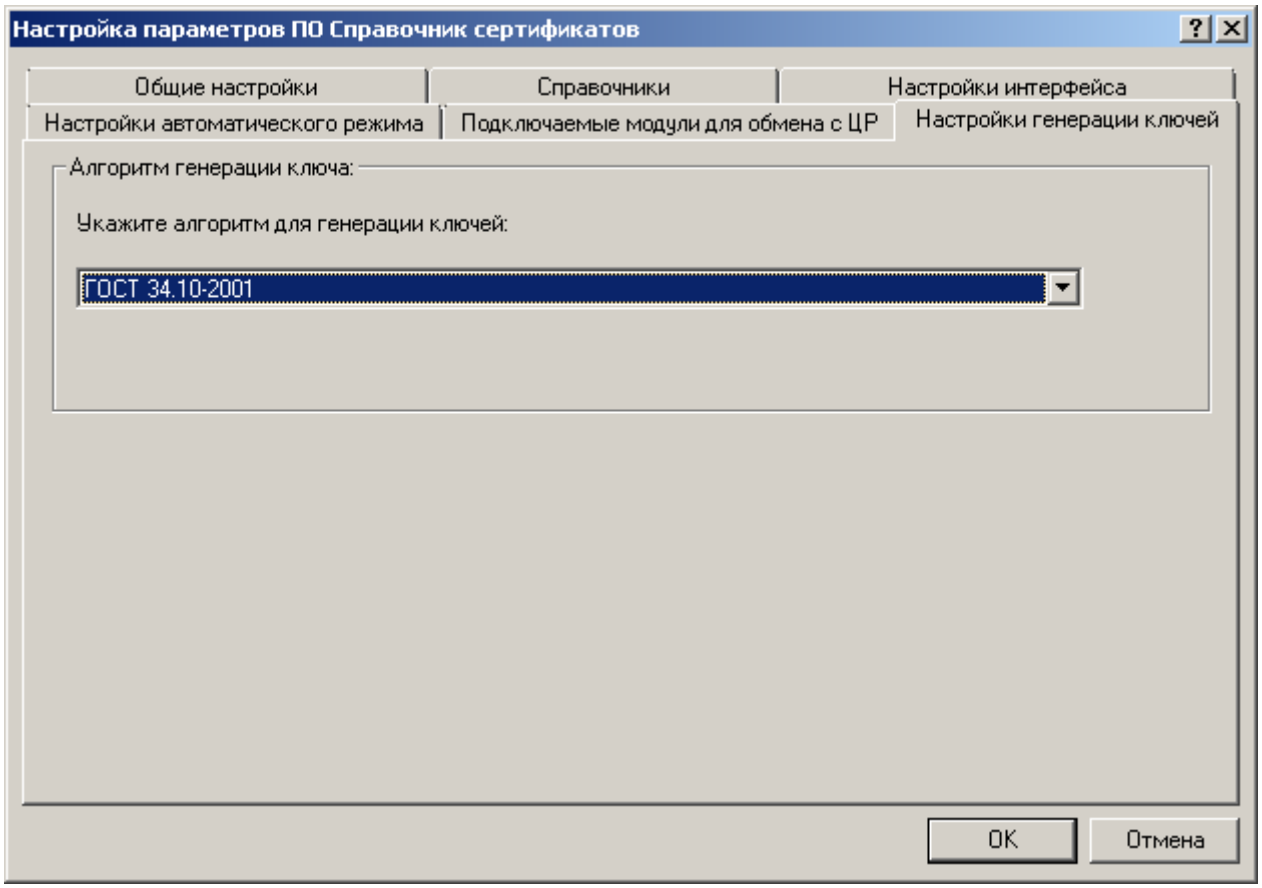

Рисунок 11 – Окно «Настройки генерации ключей»

6.3 Формирование личных ключей пользователя

Для формирования нового ключа ЭП и ключа проверки ЭП пользователя выберите пункт из основного меню «Справочник сертификатов», «Сформировать запрос на получение сертификата» или нажмите кнопку с иконкой Запроса на сертификат или щелкните правой кнопкой «мыши» на разделе «Локальный справочник сертификатов» интерфейса Справочника и выберите аналогичный пункт меню «Сформировать запрос на получение сертификата» (Рисунок 12).

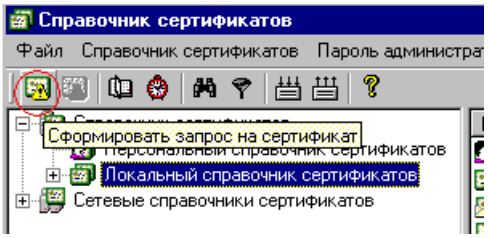

Рисунок 12 – Создание запроса на сертификат

После этого появится диалог, в котором пользователь должен выбрать тип носителя, на который будет записан новый ключ ЭП.

Примечание - Запишите идентификатор ключа ЭП на этикетку ключевого носителя (если пользователь имеет несколько ключей). При запуске Справочника и прикладного ПО, использующего криптографический модуль, данный идентификатор используется для помощи пользователю при определении требуемого ключевого носителя.

После завершения формирования ключа ЭП на носитель производится создание запроса на выпуск сертификата в формате PKCS#10, содержащего созданный ключ проверки ЭП, имя Владельца и некоторые дополнительные атрибуты (Рисунок 13 и Рисунок 14). Запрос будет подписан созданным ключом ЭП.

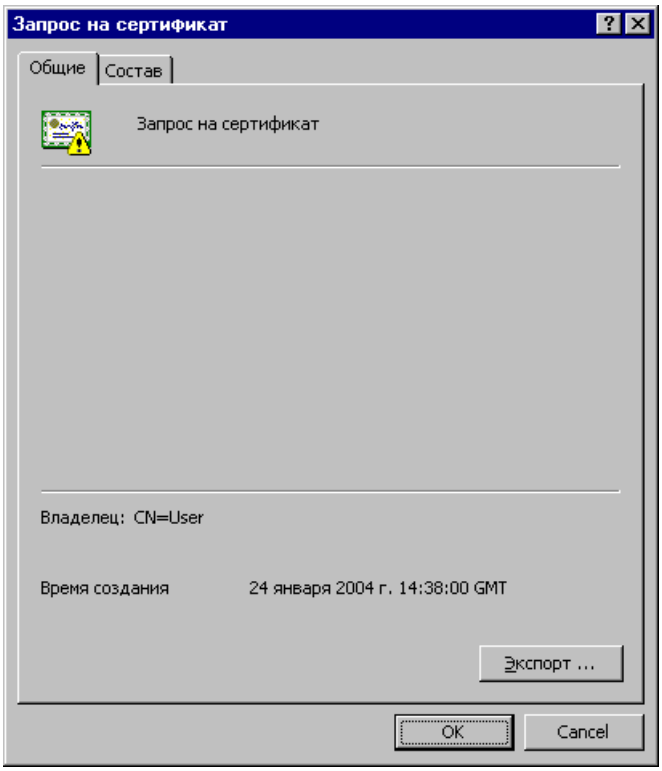

Рисунок 13 – Окно «Сформированный запрос»

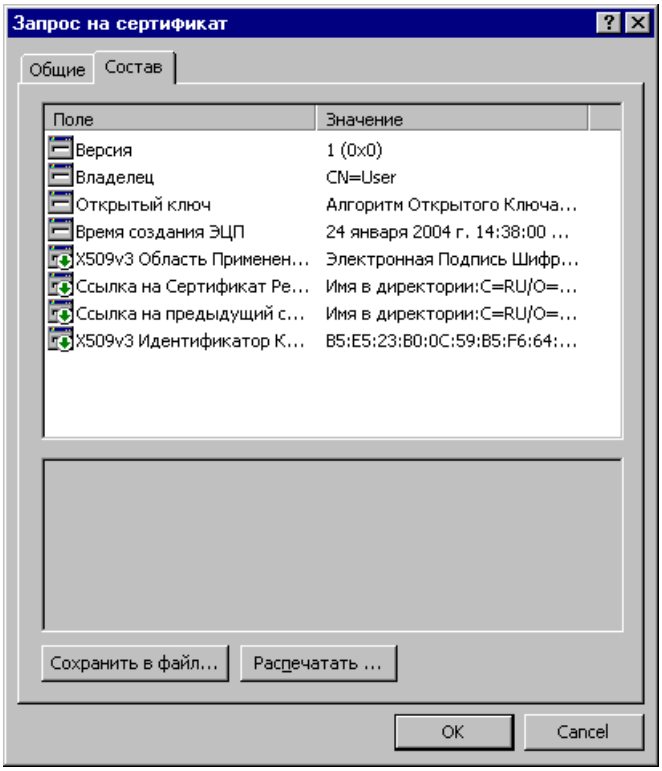

Рисунок 14 – Окно «Сформированный запрос»

6.3.1 Передача созданного запроса в ЦР

Созданный запрос на сертификат пользователь (или администратор безопасности организации) вместе с заверенным бланком запроса должен передать в ЦР для дальнейшей обработки и издания сертификата. Для

подтверждения принадлежности запроса зарегистрированному пользователю системы запрос упаковывается в сообщение в формате PKCS#7 и защищается ЭП пользователя на действующем ключе пользователя (в случае первичного изготовления запроса – на ключе регистрации).

После создания запроса на сертификат (в случае, если установлена опция в настройках интерфейса - Рисунок 4) на экран выдается окно, в котором предлагается сохранить защищенный запрос на магнитном носителе. Укажите носитель и имя файла, в который будет записан защищенный запрос (Рисунок 15).

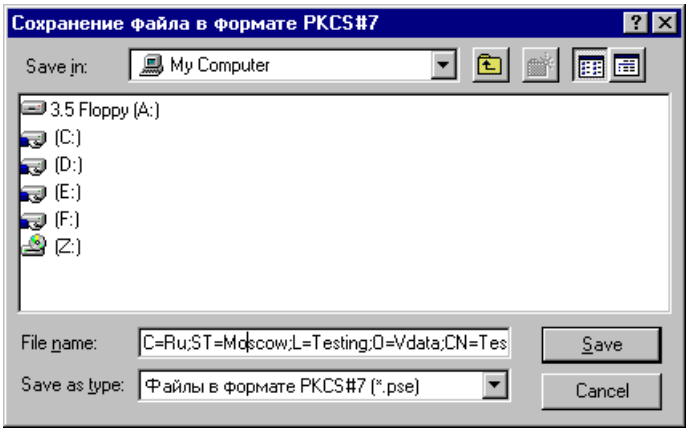

Рисунок 15 – Окно «Сохранения защищенного запроса»

Если пользователь отказался от сохранения запроса в защищенном виде после его создания, то это можно сделать впоследствии, используя интерфейс Справочника (Рисунок 16).

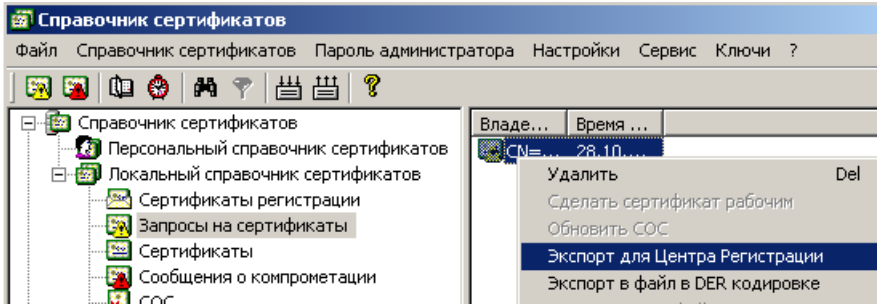

Рисунок 16 – Экспорт запроса для ЦР

Если по какой-либо причине пользователь не может сохранить запрос в защищенном виде (например, истек срок действия его ключа ЭП), то можно сохранить запрос на сертификат в открытом виде, используя пункт меню «Экспорт в файл в DER кодировке» (Рисунок 16).

Если установлена опция отправки запроса по почте, то после создания запроса на сертификат запустится почтовый агент, установленный на компьютере пользователя (Рисунок 17). Если пользователь отказался от отправки по почте, то это можно сделать впоследствии, используя интерфейс Справочника (Рисунок 16).

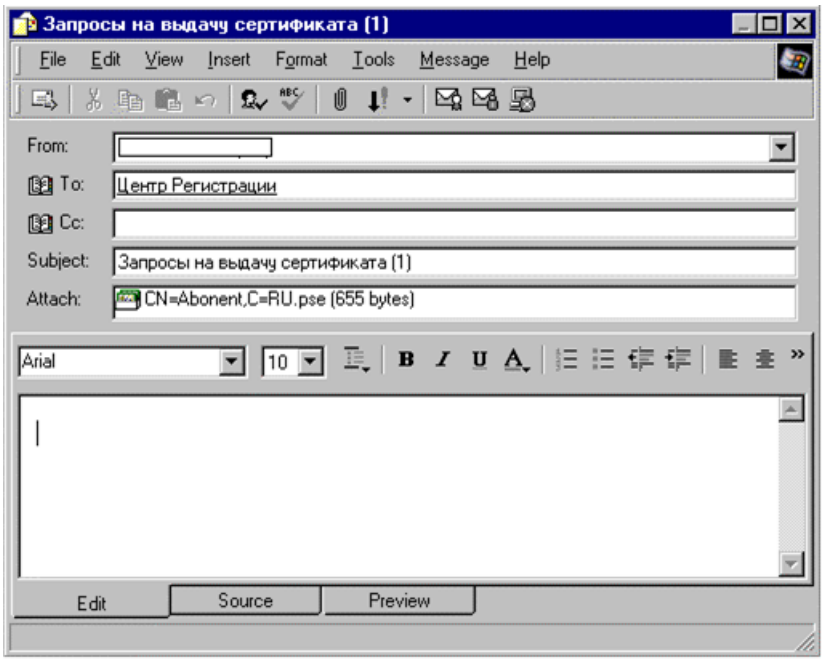

Рисунок 17 – Отправка запроса в ЦР по почте

6.3.2 Печать бланка запроса

Для вывода на печать бланка запроса на сертификат установите курсор на требуемый запрос, щелкните два раза левой клавишей, переключитесь на вкладку «Состав» и нажмите кнопку «Распечатать...» (Рисунок 14).

Примечание - Справочник сертификатов использует принтеры, установленные в операционной системе. Если принтер по умолчанию не установлен, печать будет невозможна.

6.3.3 Формирование резервной копии ключа ЭП

Формирование резервной копии ключа пользователя выполняется средствами «Валидата CSP» (см. документ ВАМБ.00060-05 34 02, раздел «4.1 Операции с ключами»).

6.4 Получение личного сертификата пользователя

После передачи запроса в ЦР производится его обработка ЦР и издание сертификата ЦС.
ЦС при формировании сертификата абонента может:

– изменить срок действия ключей ЭП пользователя;

– изменить срок действия сертификата пользователя;

– изменить поля дополнения «Альтернативное Имя Владельца», за исключением тех, которые не относятся к функционированию сертификата в прикладной системе;

– добавить или удалить значения одного или нескольких идентификаторов в дополнение «Расширенная область применения ключа» (extendedKeyUsage), если это необходимо технологическим процессом обработки системы для разделения полномочий владельцев сертификатов;

– добавить или удалить регламент использования сертификата, если это необходимо технологическим процессом обработки системы для разделения полномочий владельцев сертификатов;

– добавить или удалить дополнения сертификата, если это необходимо технологическим процессом обработки системы для разделения полномочий владельцев сертификатов.

6.5 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.

6.5.1 Установка пароля

Для установки пароля необходимо выбрать пункт «Установить пароль Администратора» основного меню «Пароль Администратора» (Рисунок 18).

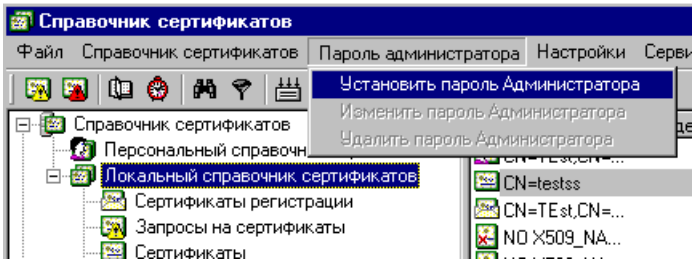

Рисунок 18 – Установка Пароля администратора

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

6.5.2 Изменение пароля

Для изменения пароля администратора необходимо выбрать пункт «Изменить пароль Администратора» главного меню «Пароль Администратора» (Рисунок 18). Далее появится диалоговое окно, предлагающее ввести новый пароль администратора (Рисунок 19).

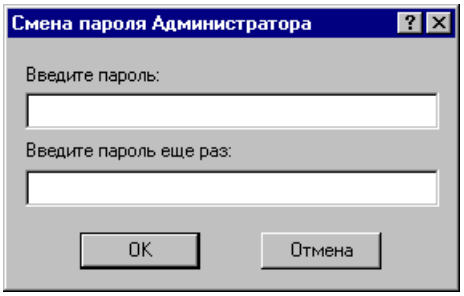

Рисунок 19 – Окно «Смена пароля администратора»

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

6.5.3 Удаление пароля

Для удаления пароля администратора необходимо выбрать пункт «Удалить пароль Администратора» основного меню «Пароль Администратора» (см. Рисунок 18).

Примечание - Удаление пароля возможно только в режиме Администратора.

6.6 Добавление сертификатов

Для добавления личного сертификата щелкните правой кнопкой «мыши» на разделе «Локальный справочник сертификатов» интерфейса Справочника и выберите пункт меню «Импортировать сертификат в локальный справочник» (Рисунок 20). После этого необходимо выбрать файл, содержащий сертификат пользователя.

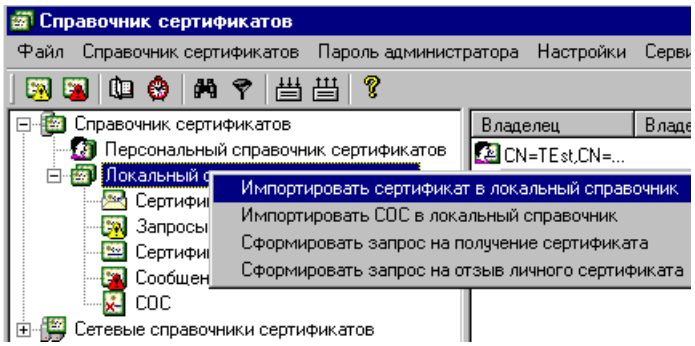

Рисунок 20 – Добавление сертификата

Добавить сертификат в Справочник можно также из Сетевого справочника LDAP. Для этого необходимо выбрать Сетевой справочник, выделить необходимый для добавления сертификат, нажать правую кнопку «мыши» и в появившемся меню выбрать пункт «Экспорт в локальный справочник».

Перед добавлением в Справочник, пользователю будет выдано диалоговое окно с отображением добавляемого сертификата (Рисунок 21).

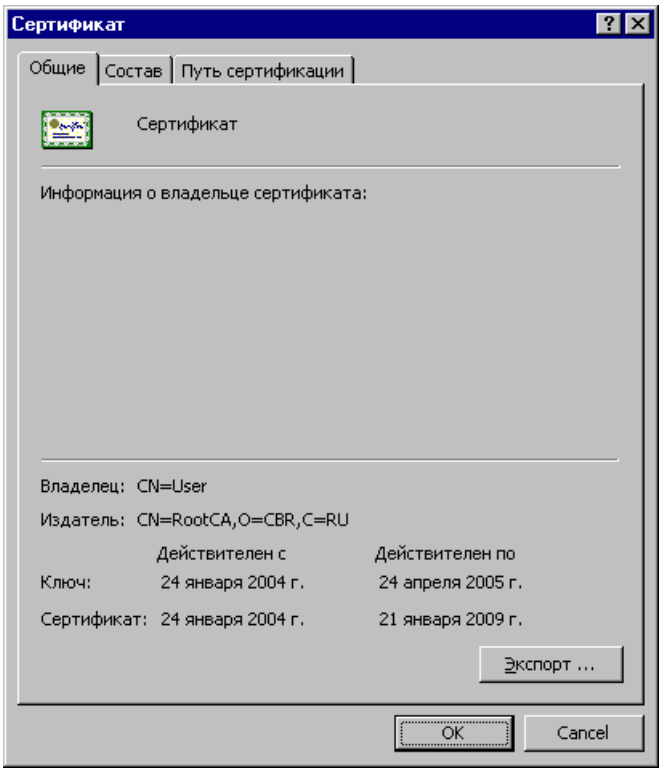

Рисунок 21 – Окно «Диалог отображения сертификата»

Для того чтобы добавить сертификат, необходимо нажать кнопку «ОК». Если проверка сертификата не прошла успешно, то этот сертификат не будет добавлен.

Для того чтобы сделать сертификат рабочим (личным), вам необходимо в интерфейсе Справочника выбрать нужный сертификат, нажать правую клавишу «мыши» и выбрать пункт меню «Сделать сертификат рабочим» (Рисунок 22).

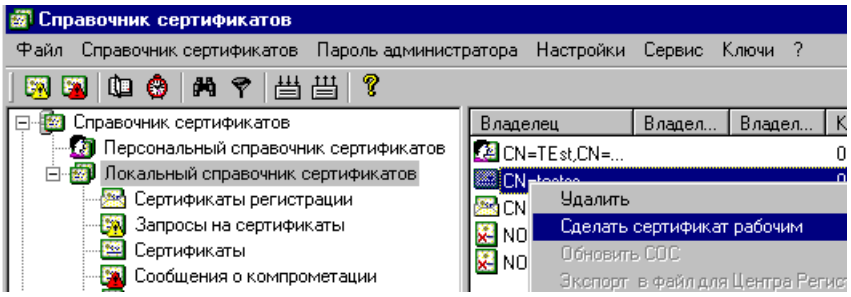

Рисунок 22 – Установка личного сертификата

Перед установкой личного сертификата требуется загрузить ключ ЭП, соответствующий ключу проверки ЭП в сертификате. При этом высвечивается диалог загрузки ключа с идентификатором требуемого ключа. При добавлении личного сертификата в Справочник, Персональный справочник пользователя подписывается на личном сертификате пользователя.

6.7 Отображение объектов в интерфейсе

Интерфейс Справочника отображает информацию об объектах в правом окне интерфейса.

6.7.1 Общая информация об объекте или списке объектов

В данном режиме правое окно выводит общую информацию об объекте или списке объектов, содержащихся в подразделе Справочника. Состав выводимой информации определяется конфигурацией Справочника и настраивается для списка объектов (см. п. 6.14). Вид выводимой информации для списка представлен на рисунке (Рисунок 23).

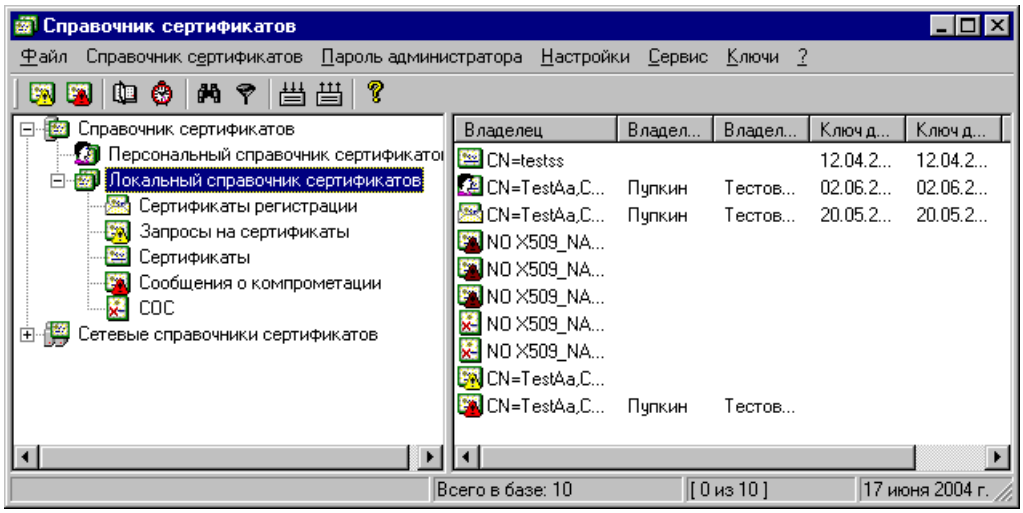

Рисунок 23 – Окно «Информация о списке объектов»

6.7.2 Информация об объекте в диалоге отображения объекта

Для каждого типа объекта, используемого в Справочнике, есть диалог отображения. Для отображения диалога необходимо, установив курсор на объекте в правом окне, дважды щелкнуть левой клавиши «мыши».

6.7.3 Диалог отображения сертификата

Диалог отображения сертификата состоит из нескольких окон, каждое из которых можно отобразить, выбрав соответствующую закладку. Закладка «Общие» выводит окно, содержащее основную информацию о сертификате (Рисунок 24).

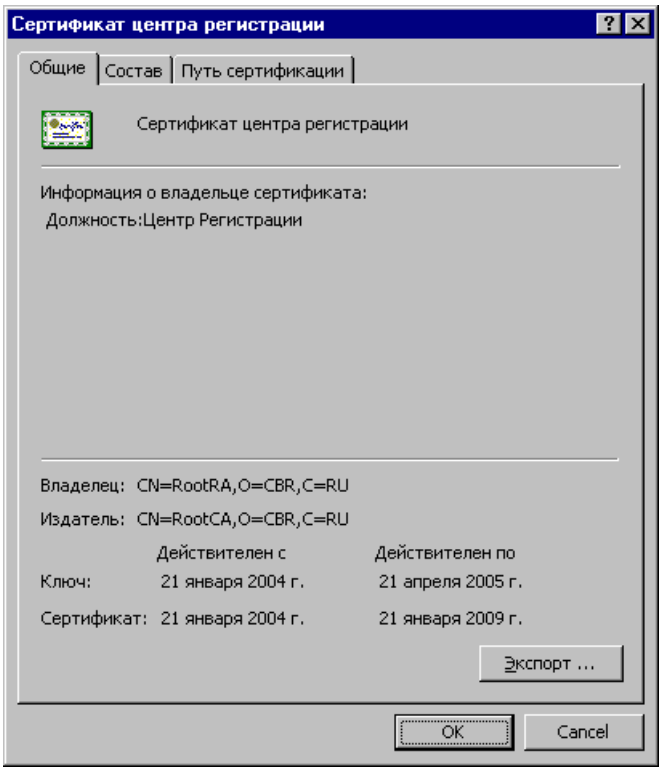

Рисунок 24 – Окно «Диалог отображения сертификата»

Закладка «Состав» выводит окно, отображающее состав сертификата, информацию, которая содержится в сертификате (Рисунок 25).

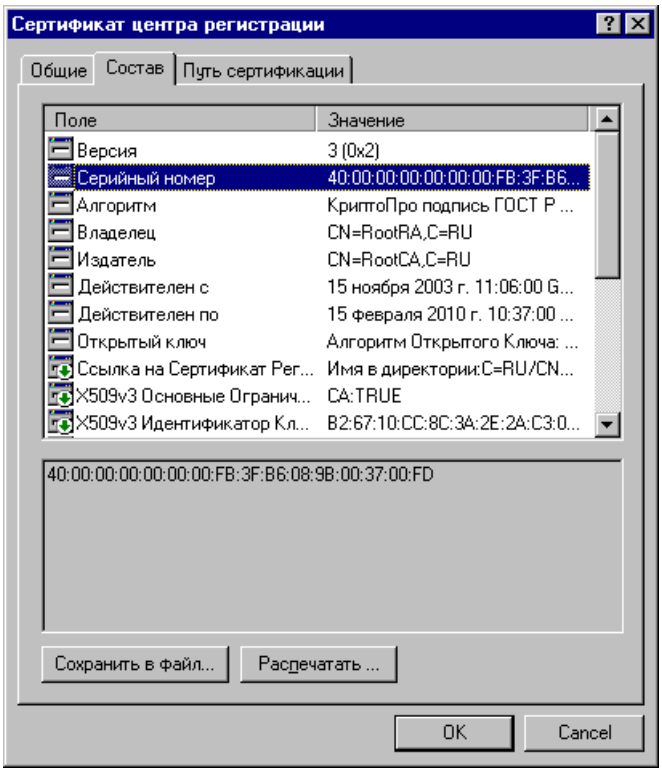

Рисунок 25 – Окно «Отображение состава сертификата»

Закладка «Путь сертификации» выводит окно, отображающее результат полной проверки сертификата.

Полная проверка сертификата включает построение цепочки сертификатов и СОС, проверку ЭП всех сертификатов и СОС в цепочке, проверку сроков их действия. Если в ходе проверки определяется отсутствие или недействительность какого-либо объекта в цепочке, то информация об этом отображается в окне. Обязательным условием проверки является наличие главного сертификата (самоподписанного сертификата ЦС) в ПСП (Рисунок 26).

Примечание - При позиционировании курсора на любой сертификат в цепочке и двойном нажатии левой клавиши «мыши», производится отображение выбранного сертификата в аналогичном диалоге.

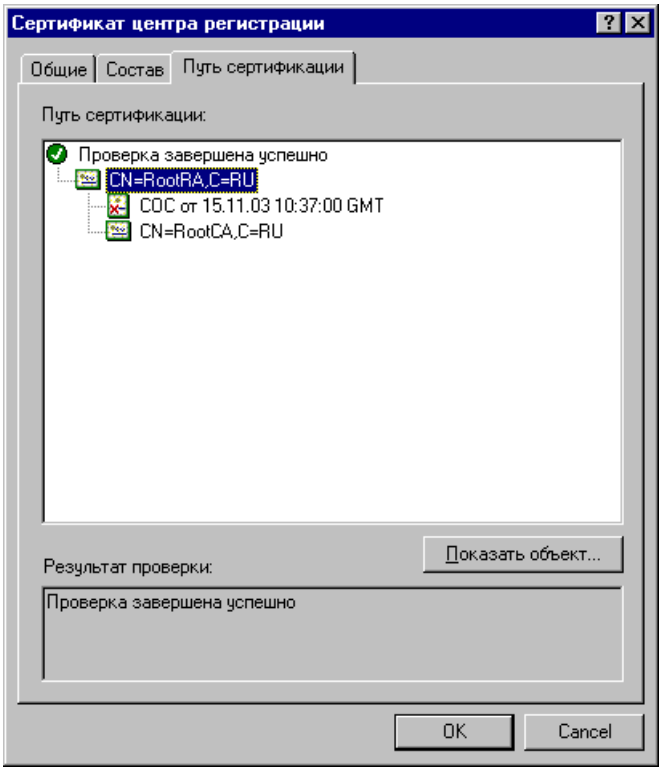

Рисунок 26 – Окно «Отображение пути сертификации»

В случае ошибки при проведении проверки сертификата (отсутствия объекта в цепочке, отсутствия сертификата, на котором подписан СОС) диалог проверки отображает ошибку (Рисунок 27).

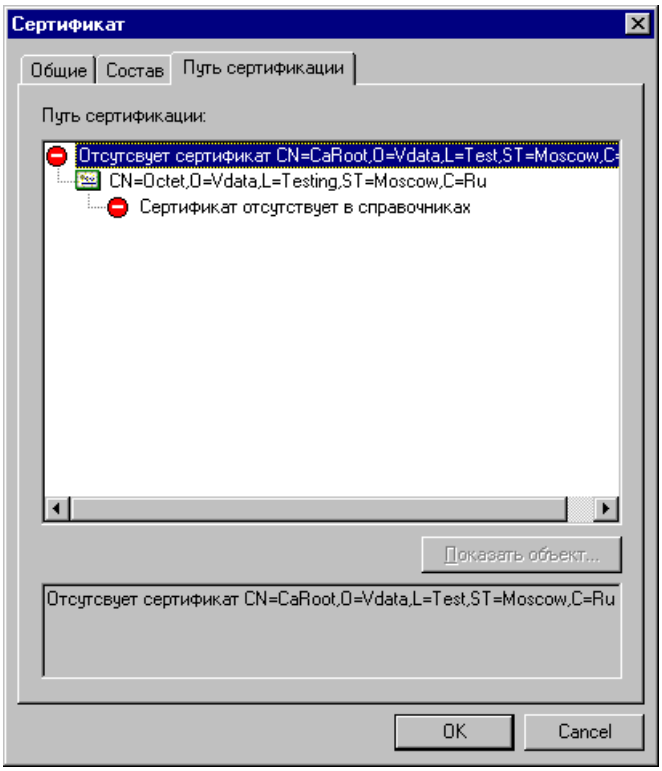

Рисунок 27 – Окно «Отображение ошибок при проверке сертификата»

6.7.4 Диалог отображения запроса на сертификат

Закладка «Общие» диалога отображения запроса на сертификат отображает основную информацию о запросе (Рисунок 28):

- имя владельца ключа проверки ЭП;
- дата создания запроса на сертификат ключа проверки ЭП.

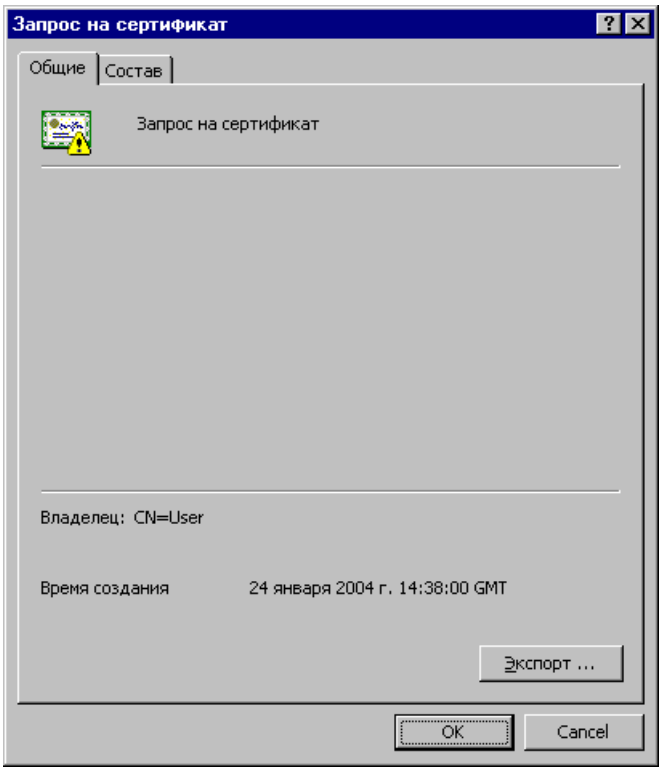

Рисунок 28 – Окно «Диалог отображения запроса»

Закладка «Состав» аналогична закладке, описанной в диалоге отображения сертификата (см. п. 6.7.3).

6.7.5 Диалог отображения списка отозванных сертификатов

Закладка «Общие» диалога отображения списка отозванных сертификатов отображает основную информацию о списке (Рисунок 29):

- имя Издателя списка (ЦС);
- дата издания списка;
- дата обновления списка (может отсутствовать).

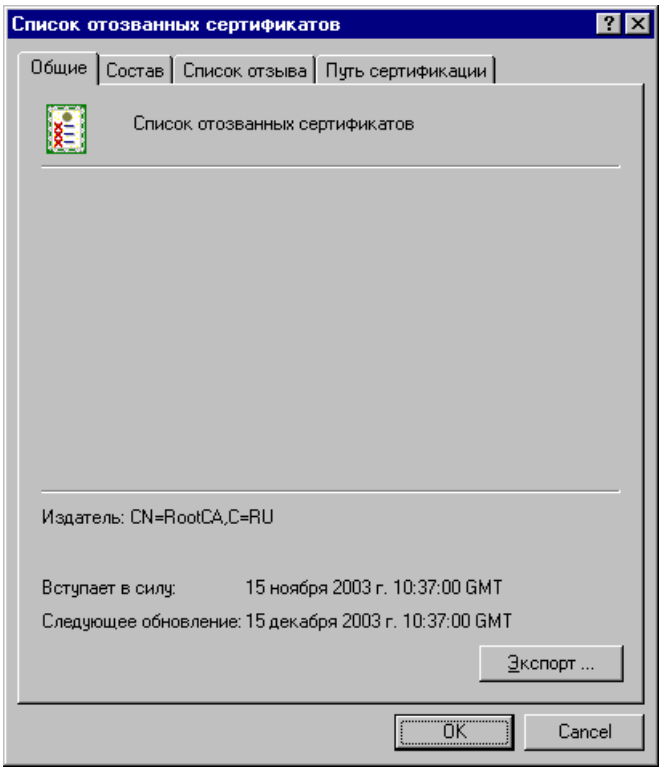

Рисунок 29 – Окно «Диалог отображения списка отозванных сертификатов»

Закладка «Список отзыва» показывает список, в котором присутствуют отозванные сертификаты (серийные номера отозванных сертификатов) (Рисунок 30).

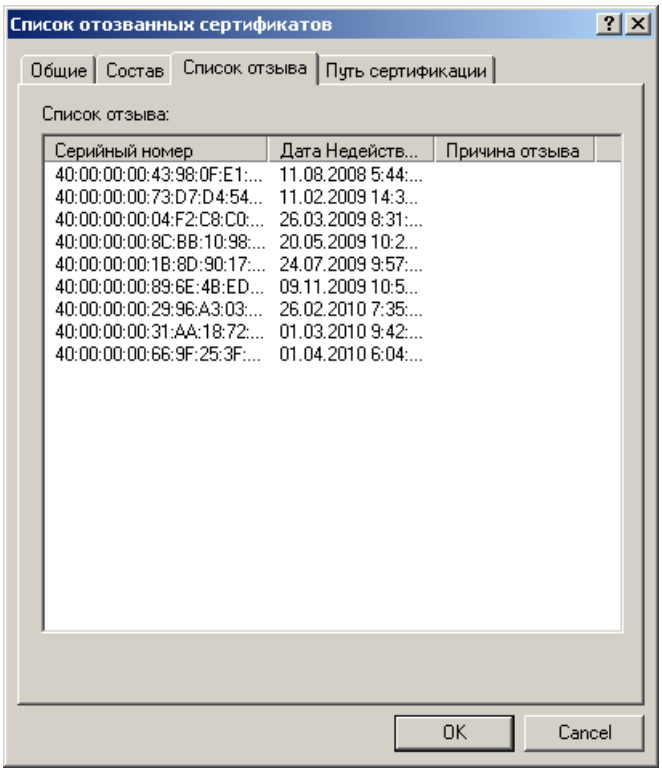

Рисунок 30 – Окно «Отображение списка отзыва»

Закладки «Состав», «Путь сертификации» аналогичны закладкам, описанным в диалоге отображения сертификата (см. п. 6.7.3).

6.7.6 Диалог отображения сообщения о компрометации

Закладка «Общие» диалога отображения сообщения о компрометации отображает основную информацию (Рисунок 31):

– имя Владельца сертификата;

– дата создания сообщения.

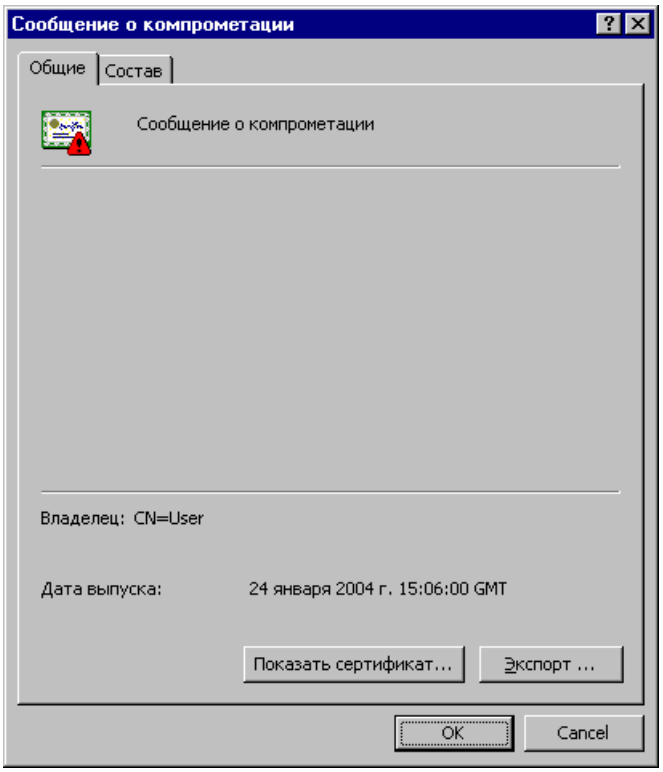

Рисунок 31 – Окно «Диалог отображения сообщения о компрометации»

Закладка «Состав» аналогична закладке, описанной в диалоге отображения сертификата (см. п. 6.7.3).

6.8 Обновление сертификата ЦС

После издания нового сертификата ЦС все пользователи системы должны получить новый сертификат и СОС ЦС в ЦР.

Для добавления объектов из ЦС или ЦР, в основном меню необходимо выбрать пункт меню «Справочник сертификатов» и подпункт «Обновить объекты». Программа предложит выбрать файл с обновлениями.

6.9 Обновление списка отозванных сертификатов

Обновление списка отозванных сертификатов возможно несколькими способами:

– добавление списка из файла, находящегося на внешнем магнитном носителе;

– обновление через файл с обновлениями (из ЦР или ЦС);

– обновление списка отозванных сертификатов по сети с использованием дополнения «Точка распространения СОС».

Для обновления списка отозванных сертификатов из файла необходимо выбрать пункт меню «Справочник сертификатов» и подпункт «Импортировать СОС в локальный справочник» или как показано на рисунке (Рисунок 32).

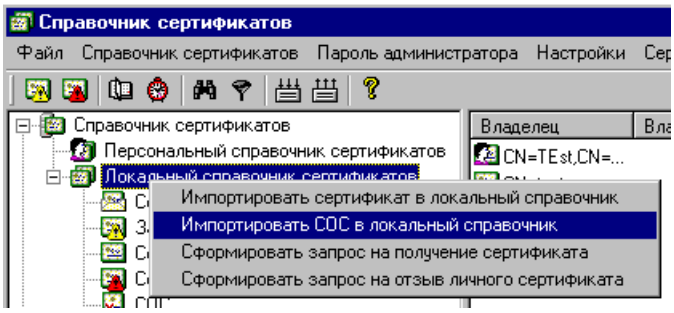

Рисунок 32 – Обновление СОС

При добавлении СОС, изданного с использованием сертификата ЦС, который отсутствует в Справочнике, отображается информация об ошибке. Объекты, не прошедшие проверку, в Справочник добавлены быть не могут.

При наличии сетевого способа распространения СОС в системе возможно их обновление по сети. Для этого в правом окне интерфейса Справочника установите курсор на необходимый СОС, щелкните правой кнопкой «мыши» и выберите пункт меню «Обновить СОС» (Рисунок 33).

Примечание - Если СОС не содержит дополнения «Точка распространения СОС», сетевое обновление невозможно. Если Сетевой справочник недоступен, то выдается сообщение об ошибке.

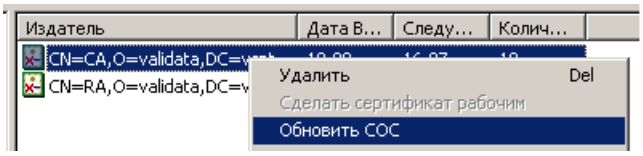

Рисунок 33 – Обновление СОС по сети

6.10 Запись объектов Справочника на внешний носитель

Каждый объект из Справочника (сертификат, запрос, СОС, сообщение о компрометации) можно сохранить на внешний носитель. Объект можно сохранить в DER кодировке (т. е. объект как он есть).

Для этого в правом окне интерфейса Справочника установите курсор на требуемый объект, щелкните правой кнопкой «мыши» и выберите пункт меню «Экспорт в файл в DER кодировке».

6.11 Компрометация ключа пользователя

При компрометации ключа у пользователя он должен немедленно прекратить связь по сети с другими абонентами.

Пользователь (или администратор безопасности организации) должен немедленно известить ЦР о компрометации ключа. Информация о компрометации может передаваться по телефону с сообщением заранее условленного пароля, зарегистрированного в «Карточке оповещения о компрометации». При наличии сетевого взаимодействия пользователя может оповестить ЦР путем формирования сообщения о компрометации.

Для этого необходимо выбрать пункт меню «Справочник сертификатов» и подпункт «Сформировать запрос на отзыв личного сертификата» или как показано на рисунке (Рисунок 34). При этом формируется сообщение о компрометации с вложением личного сертификата пользователя. Для передачи его в ЦР его можно сохранить в виде файла на внешнем носителе или передать по электронной почте аналогично запросу на сертификат.

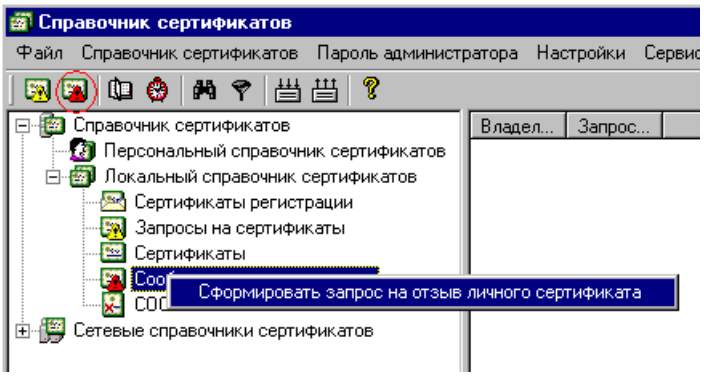

Рисунок 34 – Формирование запроса на отзыв сертификата

После формирования запроса на отзыв сертификата, если пользователь имеет резервный сертификат, необходимо установить его как рабочий (Рисунок 22).

Если пользователь не имеет резервного ключа, он должен прибыть в ЦР для повторной регистрации (см. п. 4).

6.12 Окончание действия объектов Справочника

При каждом запуске Справочник производит проверку:

- сроков действия ключа ЭП и сертификата пользователя;
- сроков действия ключа ЭП и сертификатов, хранящихся в ПСП;
- сроков действия списков отозванных сертификатов.

Если до окончания перечисленных сроков действия осталось меньше времени, чем указано в Настройках (Рисунок 2), интерфейс Справочника при запуске выводит диалог, оповещающий о данном событии (Рисунок 35). Если необходимо посмотреть истекающие объекты еще раз, необходимо выбрать пункт меню «Сервис» и подпункт «Объекты с истекающим сроком действия... » или нажать кнопку на панели инструментов (Рисунок 36).

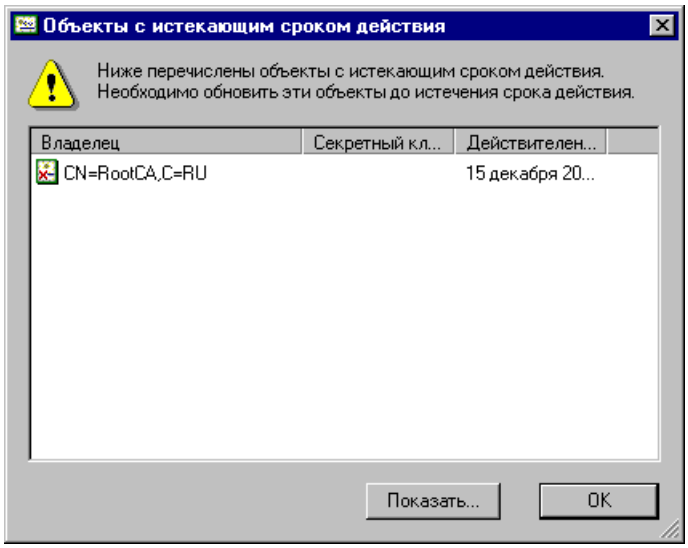

Рисунок 35 – Окно «Окончание сроков действия»

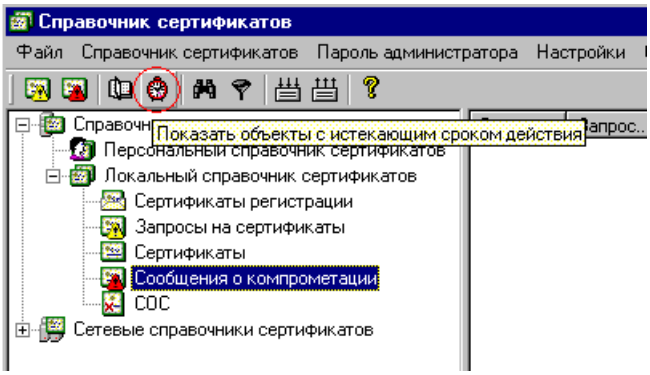

Рисунок 36 – Просмотр объектов с истекающим сроком действия

Данное сообщение служит предупреждением пользователю о необходимости совершить следующие действия:

– сформировать запрос на сертификат или установить текущим сертификат соответствующий новому ключу;

– получить в ЦР новый сертификат ЦС;

– обновить СОС.

Примечание - Окончание действия любого из перечисленных объектов приведет к невозможности работы со Справочником. В данном случае при запуске Справочника будет выдано сообщение об ошибке проверки сертификата. Если пользователь не произвел перечисленные выше действия, он должен прибыть в ЦР для повторной регистрации.

6.13 Печать бланков объектов

Печать бланков объектов осуществляется из диалога просмотра объектов (см. п. 6.7). Для печати бланка необходимо выбрать закладку «Состав» и нажать кнопку «Распечатать».

Примечание - Справочник использует принтеры, установленные в операционной системе. Если принтер по умолчанию не установлен, печать будет невозможна.

6.14 Настройка интерфейса Справочника

6.14.1 Настройка отображения

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 37). 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.

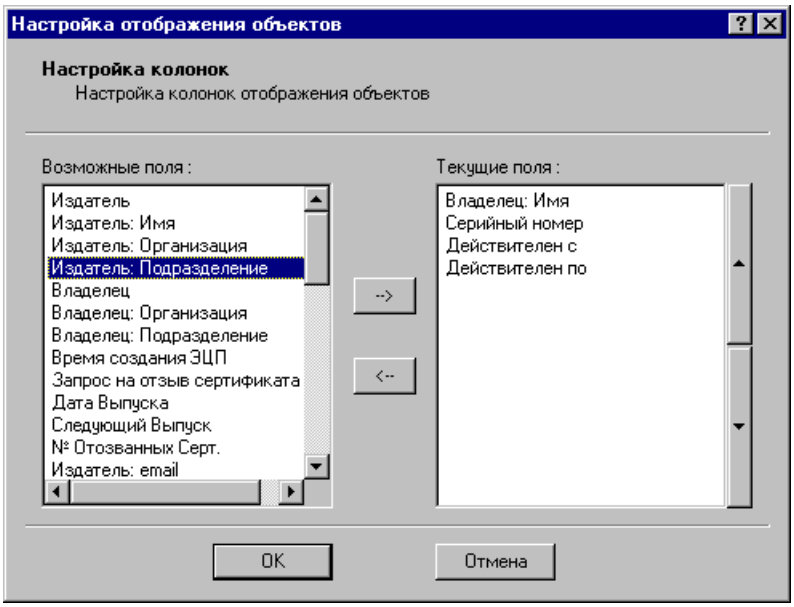

Рисунок 37 – Окно «Настройка отображения объектов»

6.14.2 Сохранение отображения в файл

Справочник позволяет сохранить информацию, выводимую в правой части интерфейса. Информация сохраняется в текстовый файл, разделителем колонок является символ табуляции. Для сохранения отображения списка объектов необходимо нажать правую кнопку «мыши» и выбрать пункт меню «Сохранить отображение в файл». Далее надо указать, в какой файл будет сохранено отображение.

6.15 Журнал Справочника

В процессе работы Справочник ведёт журнальный файл средствами операционной системы. Для просмотра журнального файла выберите пункт главного меню «Сервис», «Журнал работы». Также можно использовать программу «Просмотр событий» ОС Windows.

6.16 Резервное копирование и восстановление Справочника

6.16.1 Резервное копирование

Для обеспечения бесперебойной работы Справочник содержит функции, позволяющие произвести резервное копирование справочников. Для восстановления работоспособности в случае потери данных на жестком диске пользователь должен иметь резервные копии:

- Персонального справочника сертификатов (сертификата ЦС);
- личного сертификата;
- сертификата ЦР;
- всех СОС;
- сертификатов других пользователей, для обеспечения работоспособности в прикладном ПО.

Резервная копия содержит копию всех справочников (сетевые справочники не входят).

Для формирования резервной копии необходимо выбрать пункт меню "Сервис"и подпункт меню "Резервное копирование справочников"или нажать кнопку на панели инструментов (Рисунок 38).

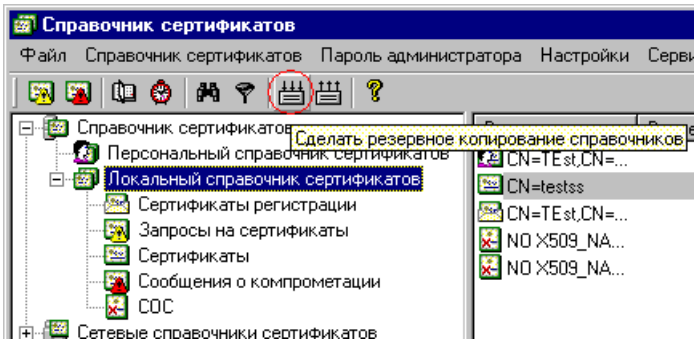

Рисунок 38 – Резервное копирование Справочников

Далее пользователю будет предложено выбрать каталог, в который будут записаны резервные копии справочников (Рисунок 39).

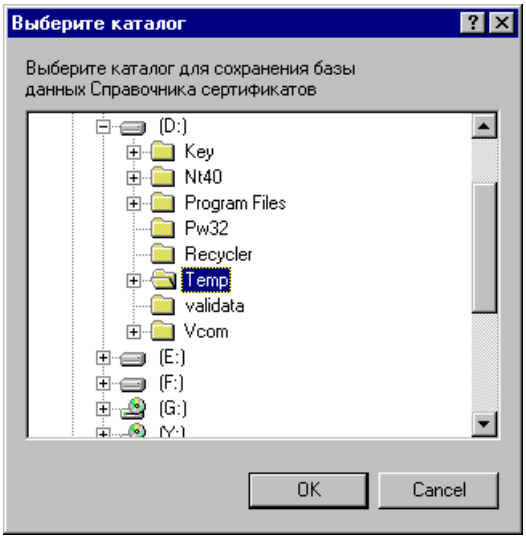

Рисунок 39 – Окно «Выбор каталога резервного копирования»

Если в настройках интерфейса установлена опция «Создавать подкаталог с использованием текущего времени для сохранения резервных копий баз справочника сертификатов», то в указанной поддиректории будет создан каталог с текущем временем в формате «ГГГГ.ММ.ДД ЧЧ.ММ.СС», в который будет сохранена резервная копия. Также имеется возможность включения автоматического создания резервной копии по выходу из программы. Для включения автоматического создания резервной копии по выходу из программы необходимо в настройках интерфейса установить опцию «Делать резервную копию по выходу из программы, если были изменения в справочнике».

6.16.2 Полное восстановление справочников

Восстановление справочников возможно в случае, если при запуске произошла ошибка при проверке целостности Справочника. Пользователю будет предложено выбрать каталог, содержащий резервную копию справочников. После копирования справочников с резервной копии программа завершает свою работу, и Вам необходимо запустить ее еще раз. ПО Справочника запустится уже с восстановленными справочниками. Восстановить Справочник можно также, нажав кнопку на панели инструментов (Рисунок 40) или выбрав в главном меню пункт «Сервис» и подпункт меню «Восстановление справочников».

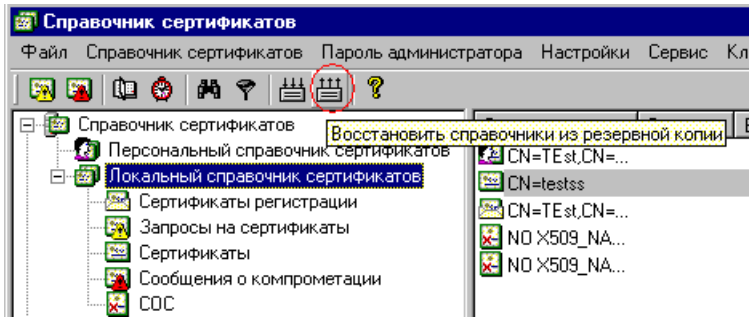

Рисунок 40 – Восстановление справочников

Далее пользователь должен указать каталог, в котором содержится резервная копия справочников, необходимая для восстановления. После копирования справочников с резервной копии программа завершает свою работу, и Вам необходимо запустить ее еще раз. Справочник запустится уже с восстановленными справочниками.

6.16.3 Ручное восстановление справочников

Ручное восстановление справочников необходимо для частичного восстановления справочников. Эта возможность позволяет восстановить функциональность справочников, используя информацию из нескольких резервных копий, сделанных раньше (например, если удален какой-нибудь объект из Справочника). Для ручного восстановления необходимо выбрать пункт меню «Сервис» и подпункт меню «Ручное восстановление справочников» (Рисунок 41).

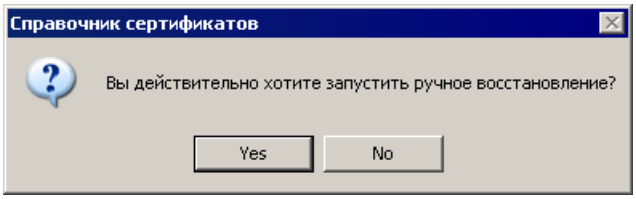

Рисунок 41 – Подтверждение запуска ручного восстановления справочника

Далее необходимо выбрать каталог, в котором находится резервная копия справочников (Рисунок 42).

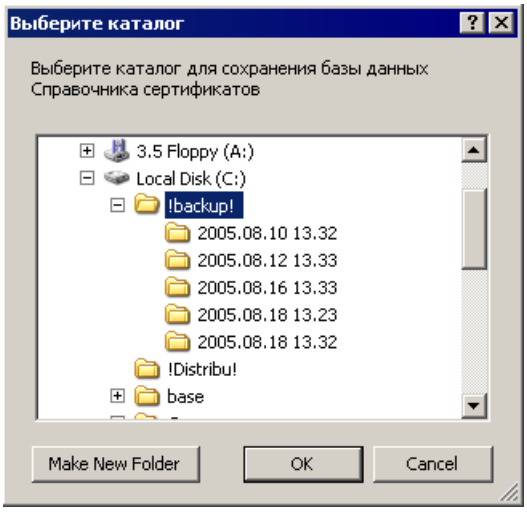

Рисунок 42 – Выбор каталога с резервной копией

Далее необходимо указать справочники для ручного восстановления (Рисунок 43).

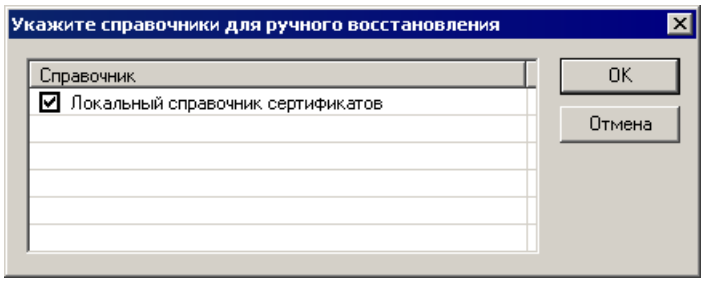

Рисунок 43 – Выбор справочника для восстановления

После нажатия кнопки «OK» откроется окно, которое содержит объекты, находящиеся в справочнике резервной копии (Рисунок 44).

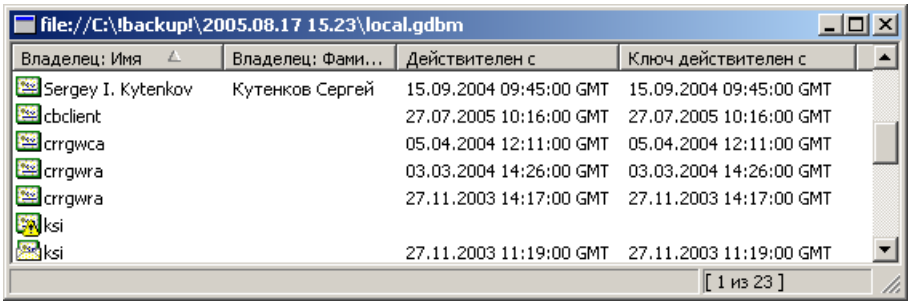

Рисунок 44 – Объекты Справочника для восстановления

Просмотр объектов осуществляется двойным щелчком мыши по нужному объекту. Для импорта объекта в Справочник необходимо выбрать объекты, затем выбрать пункт меню “Импортировать объект в справочник” (Рисунок 44).

6.16.4 Восстановление базы справочника при использовании ODBC

Для восстановления баз при использовании ODBC необходимо применить средства резервирования SQL, в зависимости от используемой базы для хранения объектов. Для ручного восстановления некоторых объектов можно воспользоваться возможностью сохранения объектов в GDBM формате (Рисунок 45).

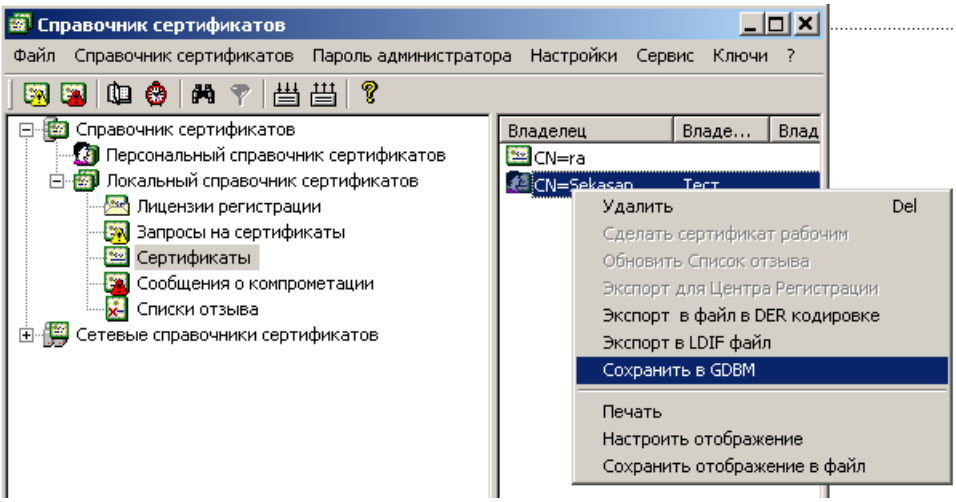

Рисунок 45 – Сохранение в GDBM формате

При сохранении объектов файл GDBM создается с именем, в зависимости от той базы, в которой происходит сохранение (Рисунок 46). Далее необходимо использовать «Ручное восстановление» и при восстановлении указать каталог, в котором был сохранен GDBM файл.

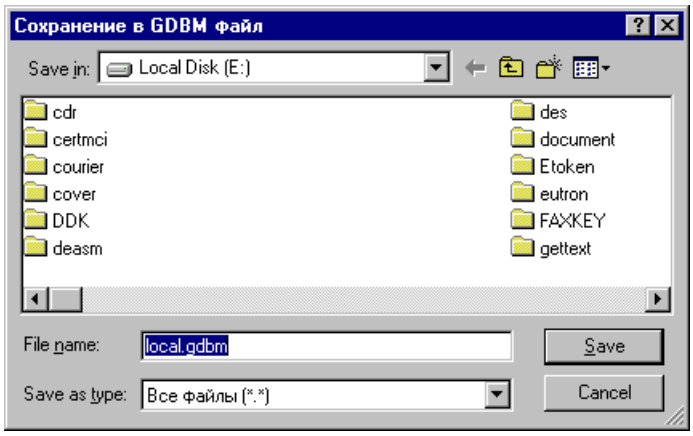

Рисунок 46 – Сохранение в GDBM

6.17 Сетевые справочники сертификатов

6.17.1 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 47).

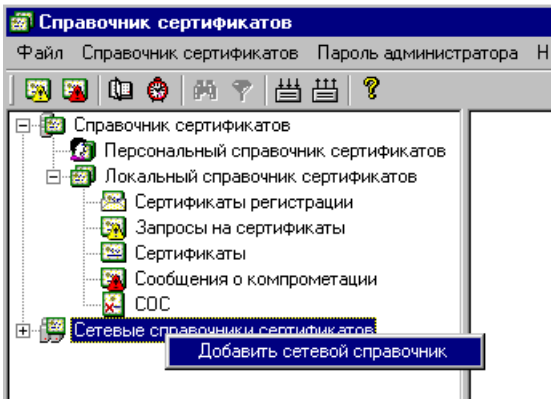

Рисунок 47 – Добавление Сетевого справочника сертификатов

Далее пользователю необходимо настроить параметры Сетевого справочника сертификатов, такие как (Рисунок 48):

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

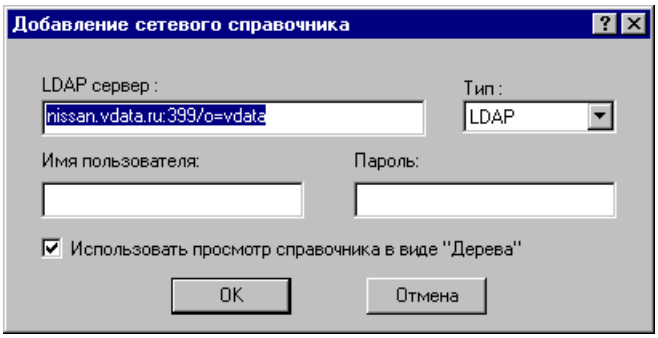

Рисунок 48 – Окно «Настройка параметров Сетевого справочника»

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).

6.17.2 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».

6.17.3 Обновление Сетевого справочника сертификатов

Так как в процессе работы в Сетевом справочнике могут появляться или удалятся объекты, то для того чтобы видеть текущее состояние Сетевого справочника сертификатов, необходимо обновление Сетевого справочника сертификатов. Обновление Сетевого справочника сертификатов делается вручную. Для обновления Сетевого справочника сертификатов необходимо в левом окне интерфейса (Рисунок 49) выбрать Сетевой справочник (необходимый для обновления), нажать клавишу «F5» или правую клавишу «мыши» и выбрать пункт меню «Перечитать справочник».

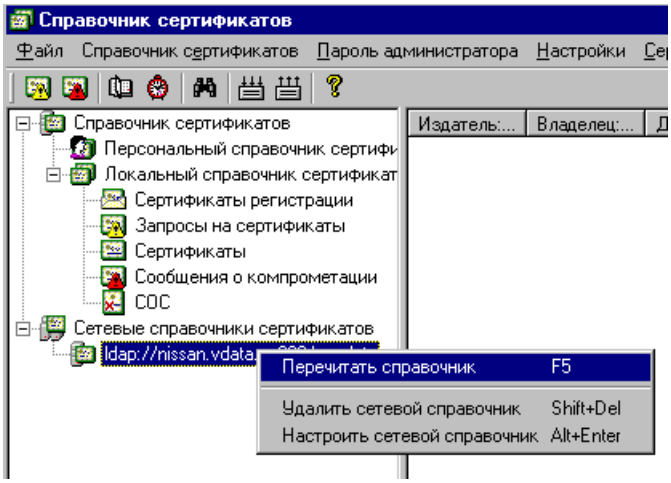

Рисунок 49 – Обновление Сетевого справочника сертификатов

6.17.4 Удаление Сетевого справочника сертификатов

Для удаления из интерфейса Сетевого справочника сертификатов необходимо в левом окне интерфейса выбрать Сетевой справочник (который нужно удалить) и нажать клавишу Shift вместе с клавишей Del или нажать правую клавишу «мыши» и выбрать пункт меню «Удалить сетевой справочник».

6.18 Фильтрация объектов при работе с ODBC хранилищем

Если объекты хранятся в ODBC хранилище, то для того чтобы не получать весь список объектов, находящихся в базе, необходимо установить фильтрацию объектов по определенному признаку. Для включения фильтра необходимо нажать кнопку на панели инструментов (Рисунок 50) или выбрать пункт главного меню «Настройки», «Установить фильтрацию объектов в базе». После фильтрации будут отображаться только отфильтрованные объекты, а количество всех объектов отображается в статусной строке. Далее появится диалог по настройке фильтрации (Рисунок 51). Диалог по настройке фильтрации имеет четыре закладки для настройки фильтрации сертификатов (Рисунок 51), СОС (Рисунок 52), запросов на выдачу сертификатов (Рисунок 53) и запросов на отзыв сертификатов (Рисунок 54).

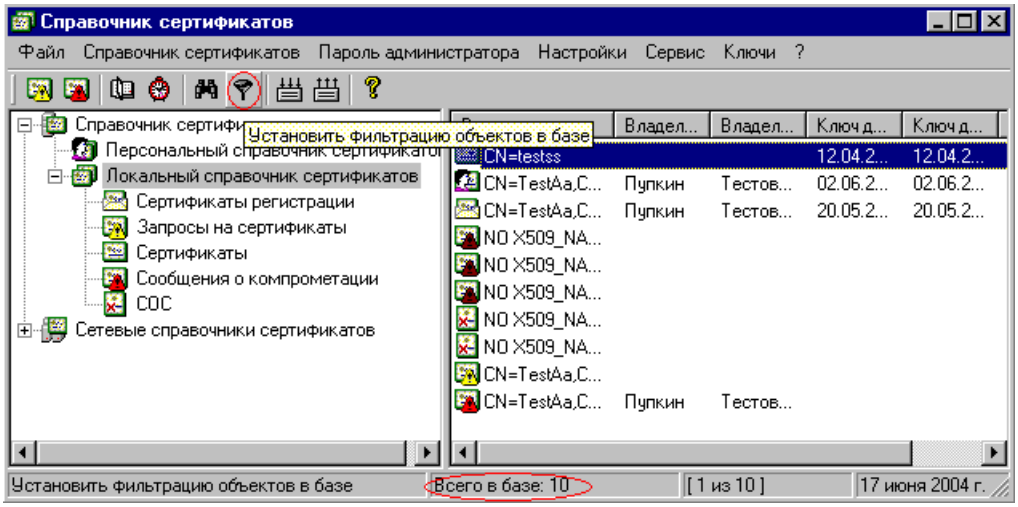

Рисунок 50 – Фильтрация объектов

6.18.1 Фильтрация сертификатов

Если установлена опция «Все записи», «Последние N записей» или «За последние N дней», то ввод дополнительных условий фильтрации невозможен. Если установлена опция «Все записи», то будут отображаться все объекты, если «Последние N записей» - последние N сформированных объектов за последнее время, если «За последние N дней» - объекты, созданные за последние N дней. Для ввода условий фильтрации необходимо установить опцию «Фильтрация по параметрам». При указании условий фильтрации условия складываются по «ИЛИ», то есть если заполнены несколько условий, то результатом фильтрации будут объекты, которые удовлетворяют или первому, или второму условию. Для задания условия поиска подстроки подстроку необходимо указывать в символах «%» (Рисунок 51). Кнопка «Очистить все» очищает все условия (поля) фильтрации.

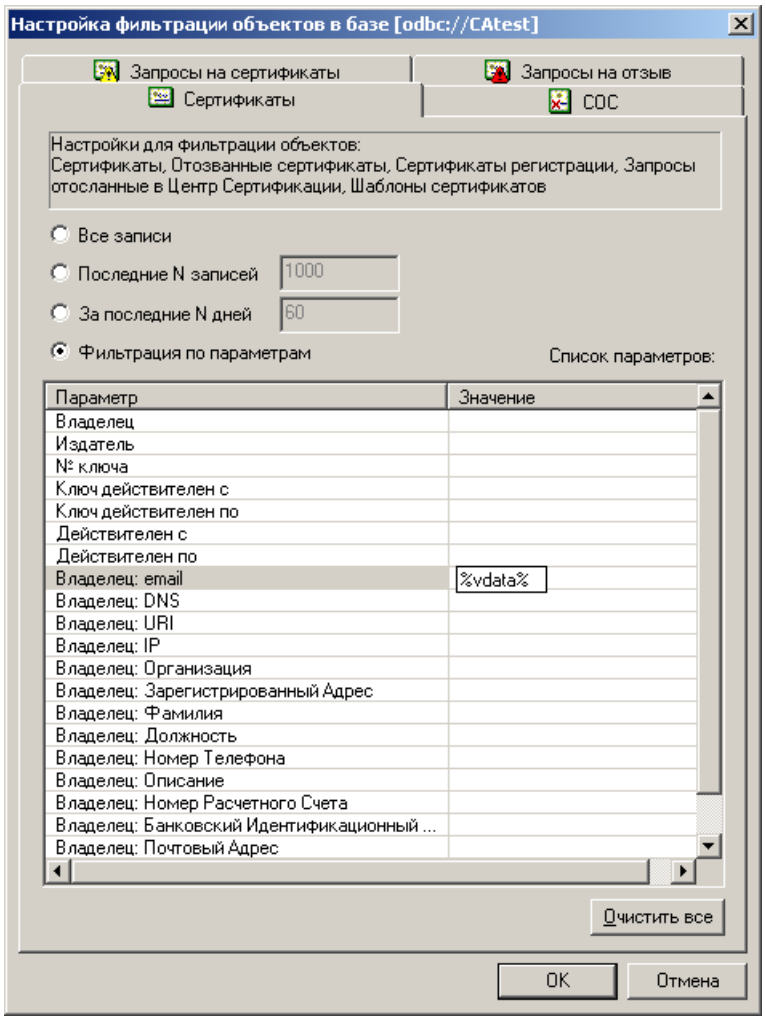

Рисунок 51 – Настройка фильтрации сертификатов

6.18.2 Фильтрация COC

Если установлена опция «Все записи», «Последние N записей» или «За последние N дней», то ввод дополнительных условий фильтрации невозможен. Если установлена опция «Все записи», то будут отображаться все объекты, если «Последние N записей» - последние N сформированных объектов за последнее время, если «За последние N дней» - объекты, созданные за последние N дней. Для ввода условий фильтрации необходимо установить опцию «Фильтрация по параметрам». При указании условий фильтрации условия складываются по «ИЛИ», то есть, если заполнены несколько условий, то результатом фильтрации будут объекты, которые удовлетворяют или первому, или второму условию. Для задания условия поиска подстроки подстроку необходимо указывать в символах «%» (Рисунок 52). Кнопка «Очистить все» очищает все условия (поля) фильтрации.

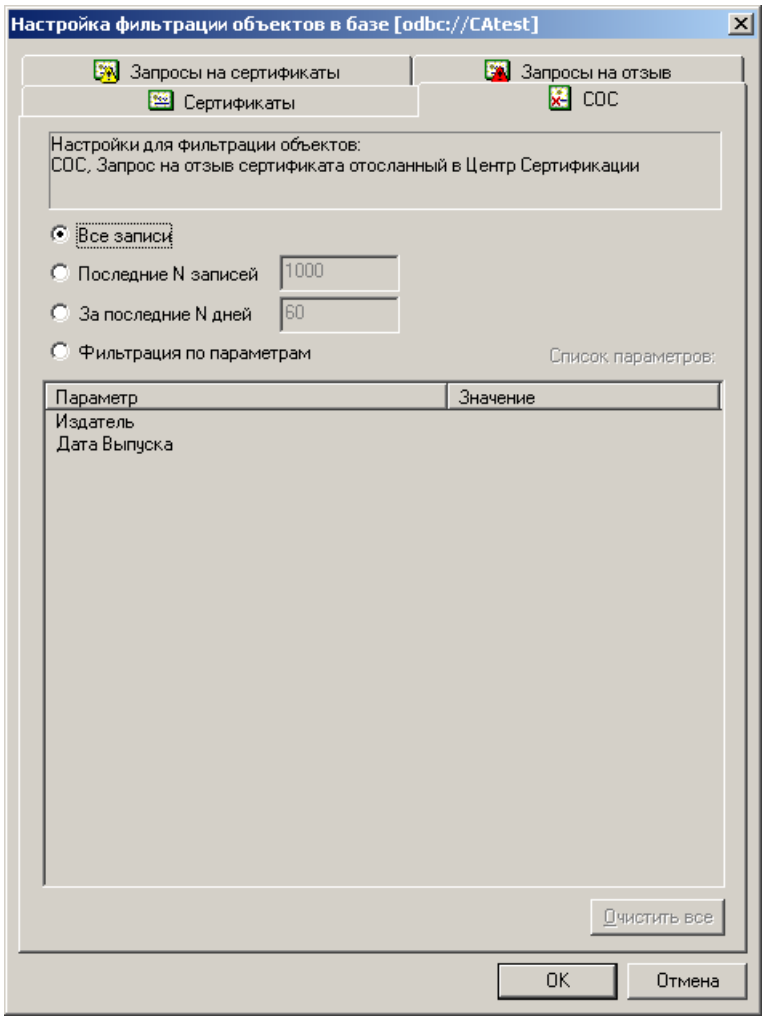

Рисунок 52 – Настройка фильтрации COC

6.18.3 Фильтрация запросов на сертификат

Если установлена опция «Все записи», «Последние N записей» или «За последние N дней», то ввод дополнительных условий фильтрации невозможен. Если установлена опция «Все записи», то будут отображаться все объекты, если «Последние N записей» - последние N сформированных объектов за последнее время, если «За последние N дней» - объекты, созданные за последние N дней. Для ввода условий фильтрации необходимо установить опцию «Фильтрация по параметрам». При указании условий фильтрации условия складываются по «ИЛИ», то есть, если заполнены несколько условий, то результатом фильтрации будут объекты, которые удовлетворяют или первому, или второму условию. Для задания условия поиска подстроки подстроку необходимо указывать в символах «%» (Рисунок 53). Кнопка «Очистить все» очищает все условия (поля) фильтрации.

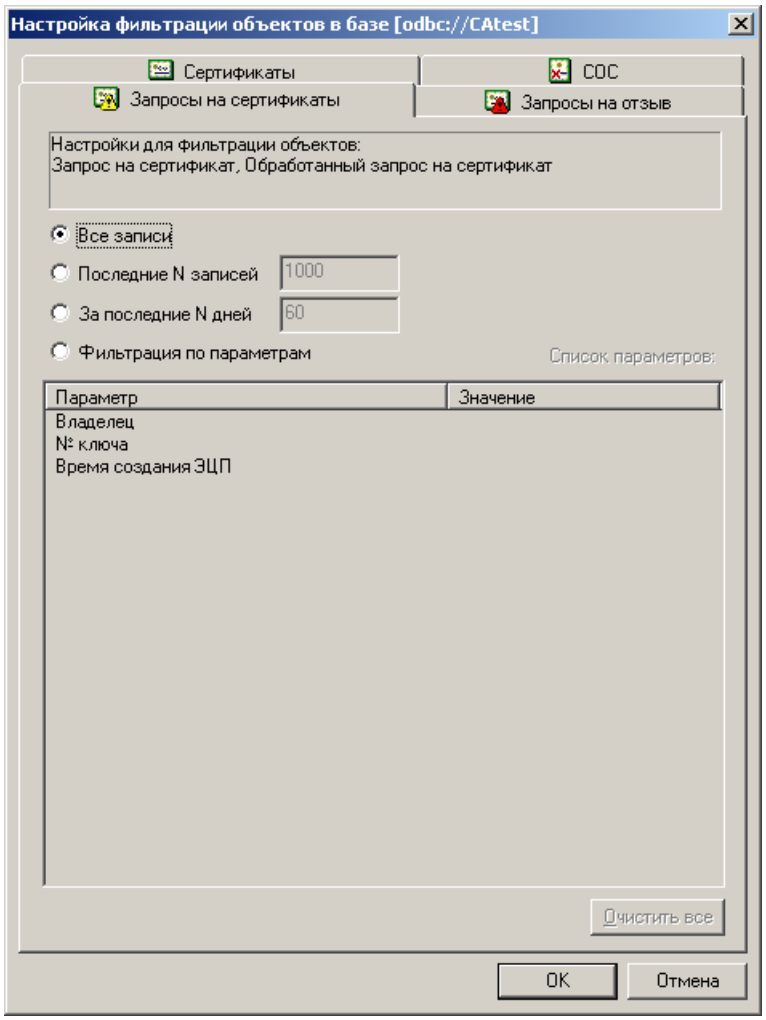

Рисунок 53 – Настройка фильтрации запросов на сертификат

6.18.4 Фильтрация запросов на отзыв сертификата

Если установлена опция «Все записи», «Последние N записей» или «За последние N дней», то ввод дополнительных условий фильтрации невозможен. Если установлена опция «Все записи», то будут отображаться все объекты, если «Последние N записей» - последние N сформированных объектов за последнее время, если «За последние N дней» - объекты, созданные за последние N дней. Для ввода условий фильтрации необходимо установить опцию «Фильтрация по параметрам». При указании условий фильтрации условия складываются по «ИЛИ», то есть, если заполнены несколько условий, то результатом фильтрации будут объекты, которые удовлетворяют или первому, или второму условию. Для задания условия поиска подстроки подстроку необходимо указывать в символах «%» (Рисунок 54). Кнопка «Очистить все» очищает все условия (поля) фильтрации.

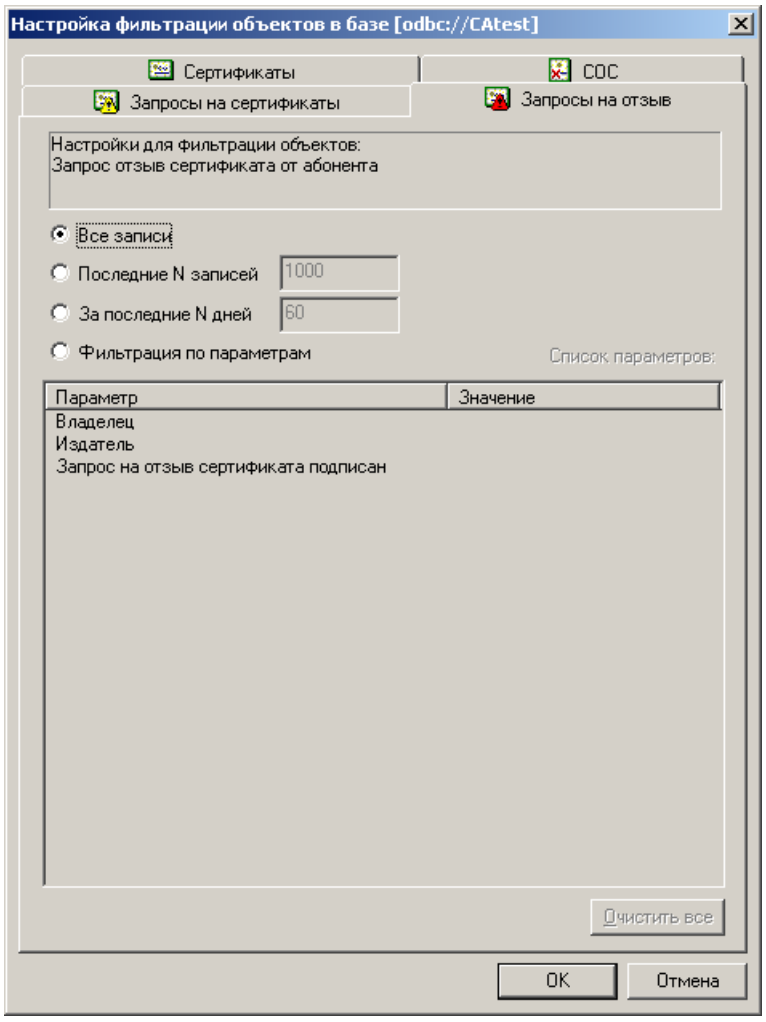

Рисунок 54 – Настройка фильтрации запросов на отзыв сертификата

6.19 Поиск объектов в Справочнике

Для поиска объектов в справочнике сертификатов (таких, как сертификаты, COC, запросы на сертификат) пользователю необходимо нажать кнопку на панели инструментов или выбрать меню «Сервис» –> «Поиск» или нажать CTRL+F. После этого на экран будет выведено диалоговое окно (Рисунок 55), позволяющее заполнить условия поиска. При помощи ниспадающего списка пользователь должен выбрать, по каким полям он будет искать.

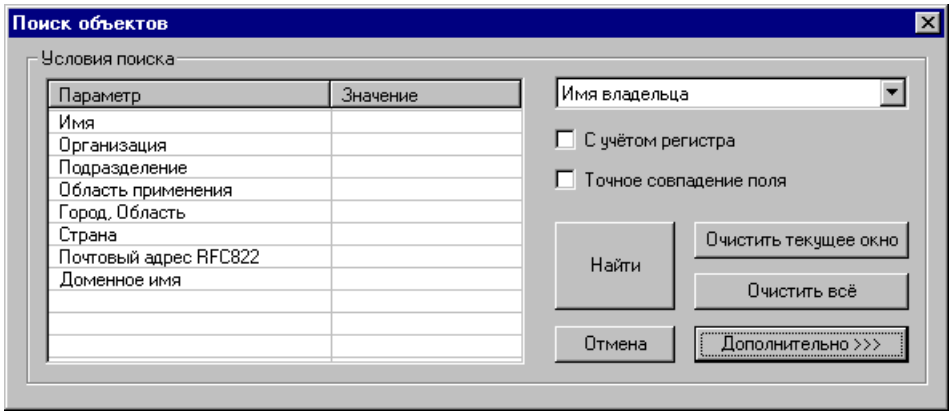

Рисунок 55 – Окно «Поиск объектов»

Для поиска доступны следующие варианты:

1) Имя владельца:

– Имя,
– Организация,
– Подразделение,
– Область применения,
– Город, Область,
– Страна,
– Почтовый адрес RFC822,
– Доменное имя;

2) Альтернативное имя владельца:

– EMAIL,
– DNS,
– URL,
– IP адрес,
– Организация,
– Зарегистрированный адрес,
– Фамилия,
– Должность,
– Номер телефона,
– Описание,
– Номер расчетного счета,
– БИК,
– Почтовый адрес,
– Адрес Exchange;

3) Имя издателя:

– Имя,
– Организация,
– Подразделение,
– Область применения,
– Город,
– Область,
– Страна,
– Почтовый адрес RFC822,
– Доменное имя;

4) Альтернативное имя издателя:

– EMAIL,
– DNS,
– URL,
– IP адрес,
– Организация,

– Зарегистрированный адрес,
– Фамилия,
– Должность,
– Номер телефона,
– Описание,
– Номер расчетного счета,
– БИК,
– Почтовый адрес,
– Адрес Exchange;

5) Прочее:

– N ключа подписи,
– N ключа шифрования,
– Серийный номер,
– Время действия сертификата,
– Время действия ключа.

Также доступен расширенный поиск. Для того чтобы его включить, необходимо нажать кнопку «Дополнительно»» (Рисунок 56). Расширенный поиск позволяет к обычному поиску добавить фильтрацию по:

– расширенному применению ключа;
– регламенту;
– дополнению.

Для того чтобы заполнить список дополнительной фильтрации, необходимо ввести идентификатор объекта вручную (Рисунок 57) или выбрать из списка (Рисунок 58).

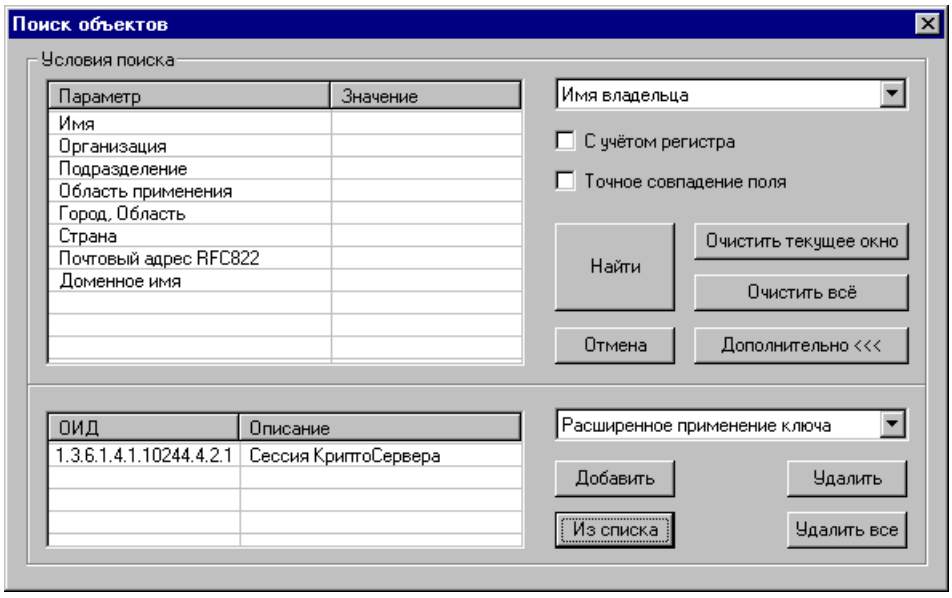

Рисунок 56 – Расширенный поиск

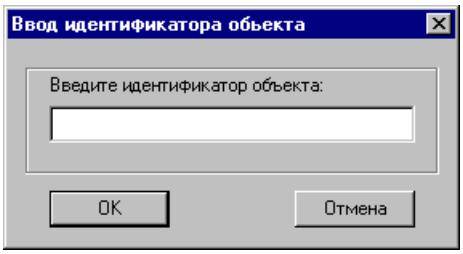

Рисунок 57 – Добавление идентификатора вручную

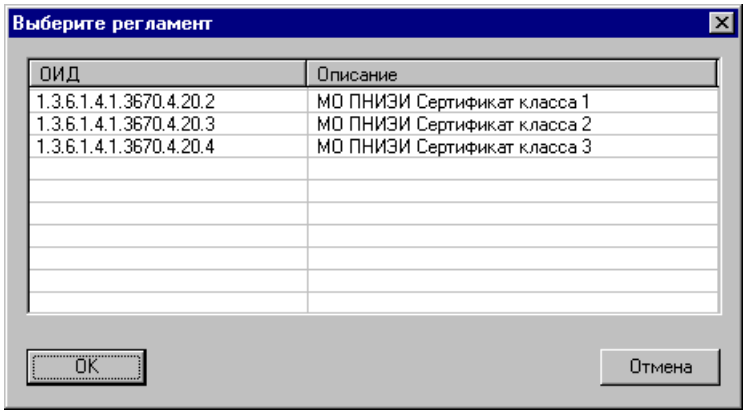

Рисунок 58 – Выбор идентификаторов из списка

После заполнения всех необходимых полей необходимо нажать кнопку «Найти», и на экран будет выведено окно (Рисунок 59) с результатами поиска. Отображение результатов поиска настраивается так же, как и отображение списка объектов.

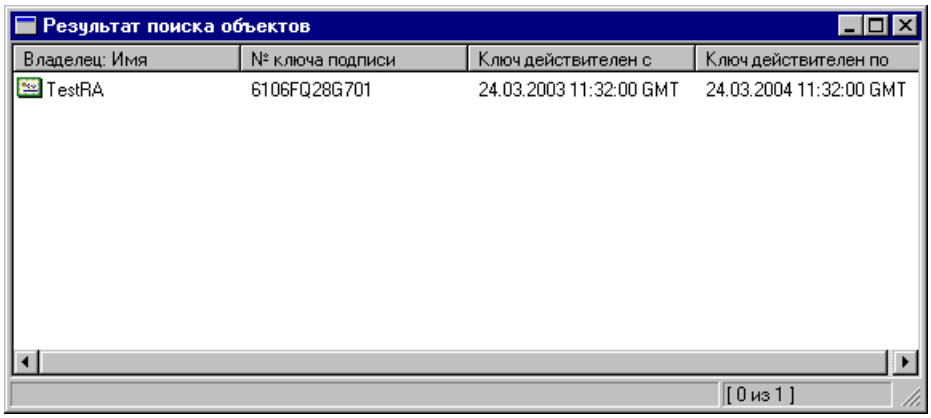

Рисунок 59 – Результат поиска объектов

6.20 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 60).

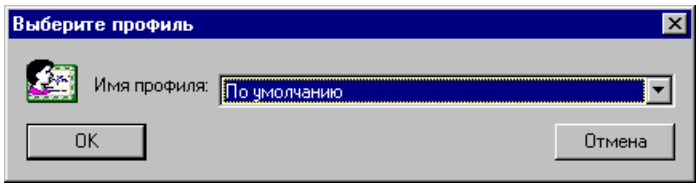

Рисунок 60 – Выбор профиля

Для создания дополнительных профилей в Справочнике, а также модификации уже существующих необходимо выбрать пункт меню «Настройки» и подпункт меню «Настройки профилей» (Рисунок 61).

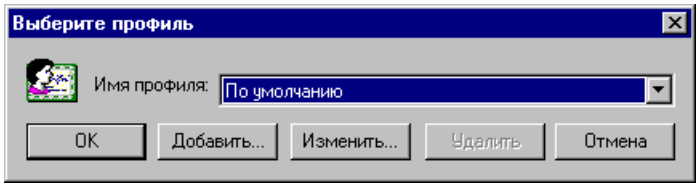

Рисунок 61 – Настройка профилей

6.20.1 Добавление нового профиля

Для добавления профиля необходимо нажать кнопку «Добавить...» (Рисунок 61), после этого отобразится диалоговое окно (Рисунок 62).

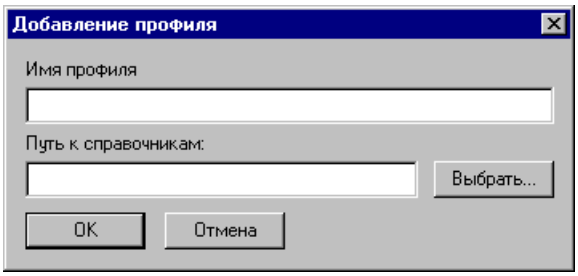

Рисунок 62 – Добавление профиля

– имя профиля – название профиля;

– путь к справочникам – каталог, в котором расположены справочники сертификатов.

Кнопка «Выбрать» служит для интерактивного выбора каталога.

6.20.2 Изменение профиля

Для добавления профиля необходимо выбрать нужный профиль из списка профилей и нажать кнопку «Изменить...» (Рисунок 62), после этого отобразится диалоговое окно (Рисунок 63).

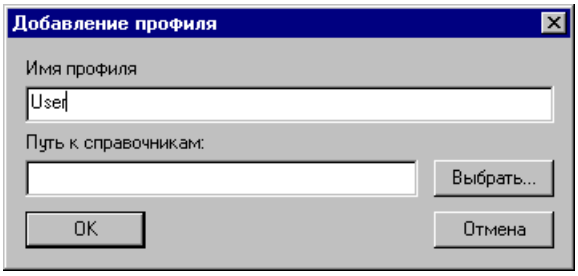

Рисунок 63 – Изменение профиля

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

6.20.3 Удаление профиля

Для добавления профиля необходимо выбрать нужный профиль из списка профилей и нажать кнопку «Удалить...» (Рисунок 62), 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).

6.21 Настройка распечаток

Для того чтобы выполнить настройки текста бланков распечаток, необходимо выбрать пункт меню «Настройки» –> «Настройка распечаток» (Рисунок 64).

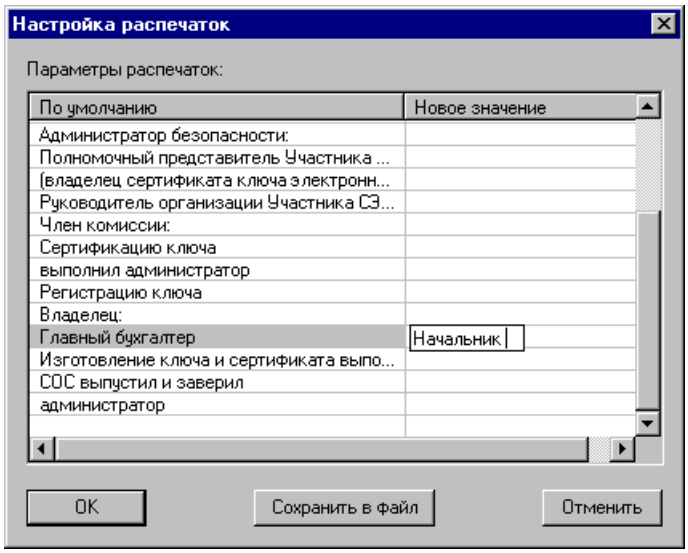

Рисунок 64 – Диалоговое окно настройки распечаток

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.

7 РАСШИРЕНИЕ ПРОВОДНИКА

Расширение проводника – это программный модуль, встраивающийся в контекстное меню Проводника и позволяющий выполнять криптографические операции с группами файлов и каталогами. Для работы расширения проводника требуется установленный и настроенный Справочник сертификатов.

7.1 Запуск расширения проводника

Для запуска расширения проводника запустите Проводник, выберите один или несколько файлов или каталогов и откройте контекстное меню (нажатием правой кнопки мыши). Выберите в контекстном меню пункт «АПК Клиент МБ» - откроется главное меню расширения проводника (Рисунок 65).

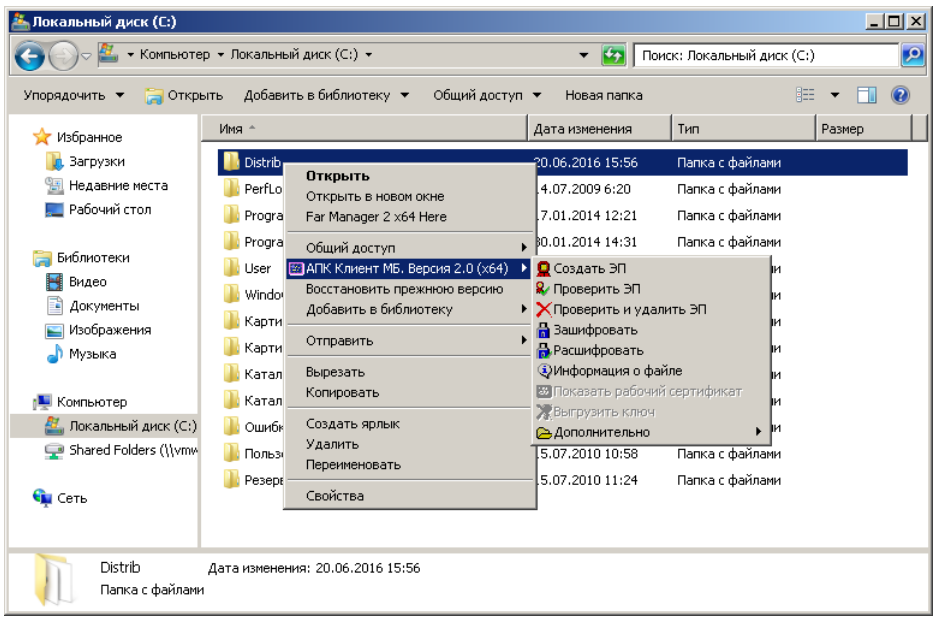

Рисунок 65 – Главное меню расширения проводника

Большинство операций, выполняемых расширением проводника, совершается над всеми выбранными файлами последовательно. В случае, если выбран один или несколько каталогов, операции совершаются над всеми файлами, расположенными в этих каталогах и их подкаталогах. Если вы попытаетесь выполнить какую-либо операцию расширения проводника на ярлыке файла, вы получите сообщение об ошибке (Рисунок 66).

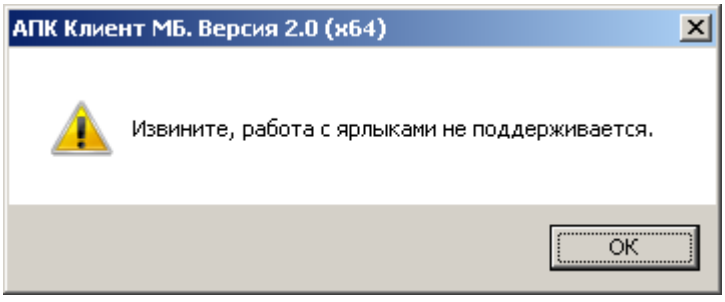

Рисунок 66 – Сообщение о невозможности обработать ярлык файла

Однако если выбрать один или несколько ярлыков в составе группы файлов или каталогов, они будут обработаны как обычные файлы. Часть операций, выполняемых расширением проводника, - «Показать рабочий сертификат», «Выгрузить ключ» и «Настройки пользователя» - выполняется вне зависимости от того, какие файлы выбраны в Проводнике.

7.2 Настройка расширения проводника

Для настройки параметров расширения проводника выберите в главном меню расширения проводника пункт «Дополнительно», подпункт «Настройки пользователя». Выберите одну из трёх закладок, измените настройки и нажмите кнопку «Применить» для сохранения внесённых изменений, кнопку «ОК» для закрытия окна настроек с сохранением внесённых изменений или кнопку «Отмена» для закрытия окна настроек без сохранения внесённых изменений.

7.2.1 Общие настройки расширения проводника

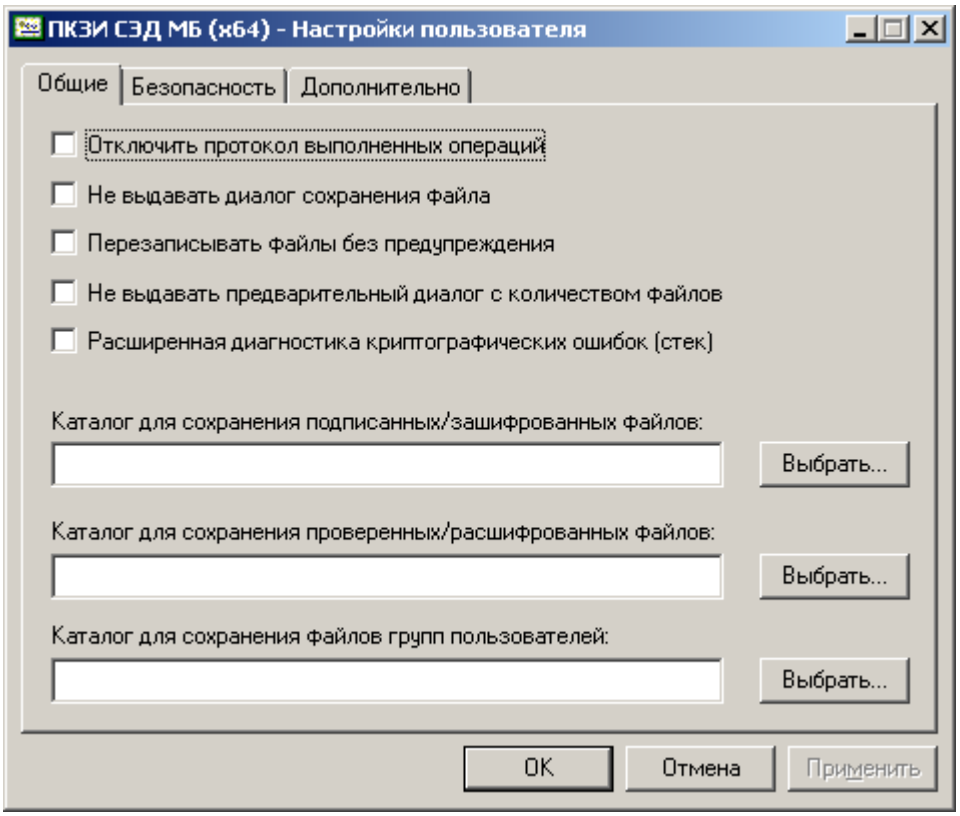

Рисунок 67 – Общие настройки расширения проводника

Таблица 3 – Общие настройки расширения проводника

Название параметра	**Описание**	**Значение по умолчанию (после установки)**
Отключить протокол выполненных операций	Отключает протоколирование всех выполняемых операций в журнал приложений (Event Log) Windows.	Выключено.
Не выдавать диалог сохранения файла	В случае, если при попытке записи файла файл с таким именем уже существует, отключает выдачу на экран стандартного диалога сохранения файла.	Выключено.
Перезаписывать файлы без предупреждения	В случае, если при попытке записи файла файл с таким именем уже существует, отключает выдачу на экран предупреждения.	Выключено.
Не выдавать предварительный диалог с количеством файлов	Отключает выдачу предупреждения о предстоящей операции с указанием количества файлов, к которым эта операция будет применена (если количество файлов более одного).	Выключено.
Расширенная диагностика криптографических ошибок (стек)	Добавляет к сообщению об ошибке криптографических функций содержимое стека ошибок.	Выключено.
Каталог для сохранения подписанных/зашифрованных файлов	Задаёт каталог, в который записываются результаты подписи и зашифрования. Если параметр не задан, результаты записываются в тот же каталог, в котором находится подписываемый или шифруемый файл.	Не задан (пусто)
Каталог для сохранения проверенных/расшифрованных файлов:	Задаёт каталог, в который записываются результаты удаления подписей и расшифрования. Если параметр не задан, результаты записываются в тот же каталог, в котором находится подписанный или зашифрованный файл.	Не задан (пусто)
Каталог для сохранения файлов групп пользователей	Задаёт каталог, в котором предлагается открывать и сохранять файлы групп пользователей – предполагаемых получателей зашифрованных сообщений.	Не задан (пусто)

7.2.2 Настройки безопасности расширения проводника

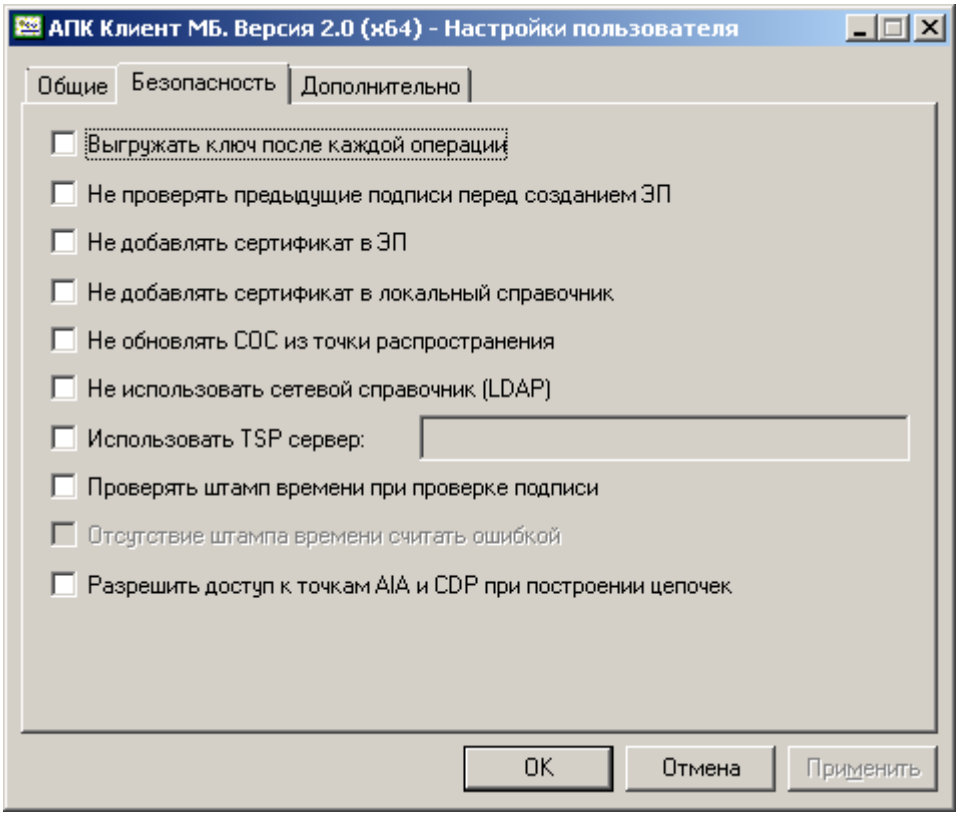

Рисунок 68 – Настройки безопасности расширения проводника

Таблица 4 – Настройки безопасности расширения проводника

Название параметра	**Описание**	**Значение по умолчанию (после установки)**
Выгружать ключ после каждой операции	После завершения любой операции с одним или несколькими файлами выгружать ключ, что потребует его повторной загрузки при выполнении следующей операции.	Выключено.
Не проверять предыдущие подписи перед созданием ЭП	Отключить проверку всех ЭП файла (если они уже есть) перед созданием следующей ЭП.	Выключено.
Не добавлять сертификат в ЭП	Отключить режим включения в ЭП сертификата, на котором создаётся ЭП.	Выключено.
Не добавлять сертификат в локальный справочник	Отключить режим добавления сертификата, найденного в сетевом справочнике в базу сертификатов Справочника сертификатов. (Изменения вступают в силу после загрузки ключа).	Выключено.

Название параметра	**Описание**	**Значение по умолчанию (после установки)**
Не обновлять COC из точки распространения	Отключить режим обязательного обновления COC из точки распространения при инициализации криптоконтекста (загрузке ключа).	Выключено.
Не использовать сетевой справочник (LDAP)	Отключить использование сетевого справочника, указанного в настройках Справочника сертификатов, при операциях проверки подписи и поиска сертификатов для зашифрования. (Изменения вступают в силу после загрузки ключа).	Выключено.
Использовать TSP сервер (выключатель)	При создании подписи добавлять в неё штамп времени с сервера, адрес которого задаётся следующим параметром.	Выключено.
Использовать TSP сервер (строка ввода)	Адрес TSP сервера, доступен для редактирования только при включённом предыдущем параметре.	Пустая строка
Проверять штамп времени при проверке подписи	При проверке каждой подписи пытаться проверить для неё штамп времени. Ошибка проверки штампа времени считается ошибкой проверки подписи.	Выключено.
Отсутствие штампа времени считать ошибкой	Требовать наличие штампа времени. Отсутствие штампа времени хотя бы одной из подписей считается ошибкой проверки подписи. Доступен для изменения только при включённом предыдущем параметре.	Выключено.
Разрешить доступ к точкам AIA и CDP при построении цепочек	Разрешать доступ к точкам распространения сертификатов и COC при построении цепочек проверки сертификатов.	Выключено.

7.2.3 Дополнительные настройки расширения проводника

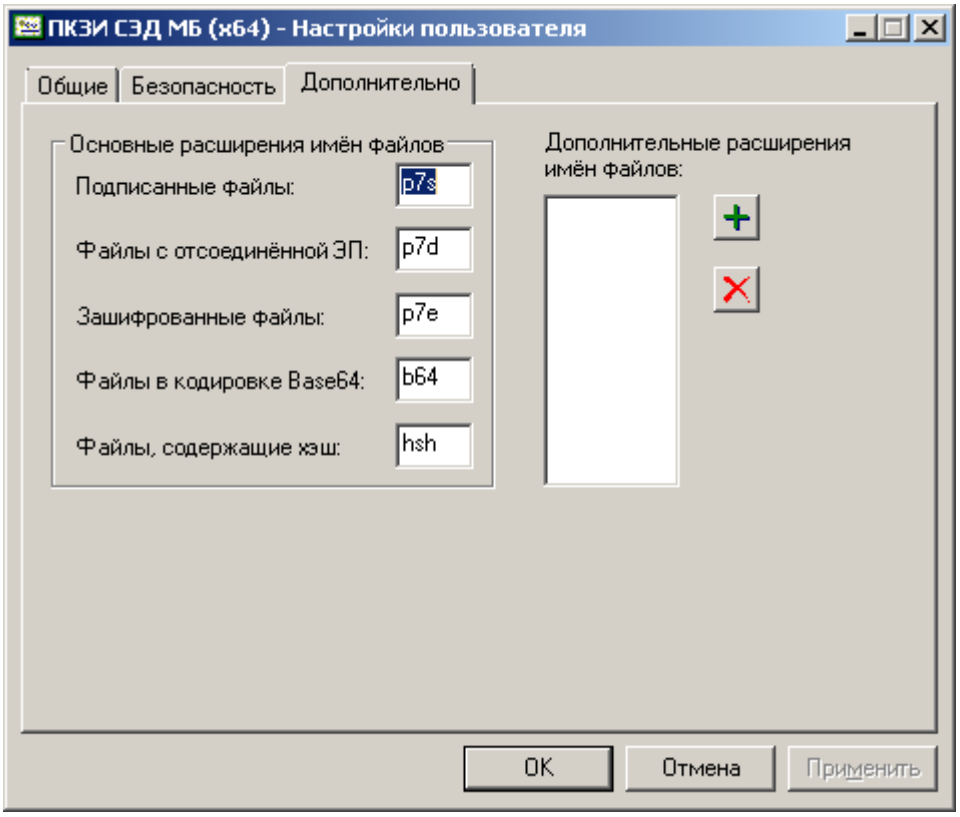

Рисунок 69 – Дополнительные настройки расширения проводника

Таблица 5 – Дополнительные настройки расширения проводника

Название параметра	**Описание**	**Значение по умолчанию (после установки)**
Подписанные файлы	Расширение, которое добавляется к файлу при создании присоединённой ЭП и снимается при удалении ЭП.	p7s
Файлы с отсоединённой ЭП	Расширение, которое добавляется к файлу при создании отсоединённой ЭП.	p7d
Зашифрованные файлы	Расширение, которое добавляется к файлу при зашифровании и снимается при расшифровании.	p7e
Файлы в кодировке Base64	Расширение, которое добавляется к файлу при преобразование в кодировку Base64 зашифровании и снимается при преобразование из кодировки Base64.	b64
Файлы, содержащие хэш	Расширение, которое добавляется к файлу при сохранении хэша.	hsh
Дополнительные расширения имён файлов	Список расширений, которые снимаются с файлов при удалении ЭП и расшифровании.	Пустой список

Для добавления дополнительного расширения в список нажмите кнопку  , введите расширение в диалоге и нажмите кнопку «OK»:

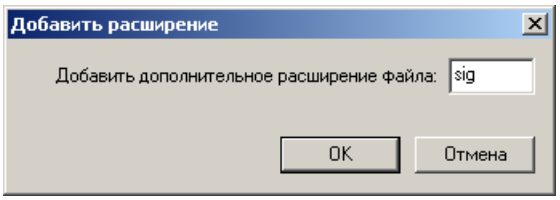

Рисунок 70 – Диалог добавления дополнительного расширения

Для удаления дополнительного расширения выберите его в списке и нажмите кнопку  .

7.3 Загрузка и выгрузка ключа

Для выполнения любой криптографической операции над одним или несколькими файлами необходимо загрузить ключ. Загрузка ключа производится в случае, если он ещё не загружен, после предупреждения о предстоящей операции с указанием количества файлов (если оно появляется) и до начала собственно операции. В процессе загрузки ключа может потребоваться выбор профиля пользователя, ключевого носителя, выбор ключа, задание пароля ключа, инициализация датчика случайных чисел – в зависимости от настроек Справочника сертификатов и криптопровайдера.

В случае, если опция «Выгружать ключ после каждой операции» в настройках расширения проводника выключена, ключ останется загруженным в памяти до закрытия данного экземпляра (окна) Проводника. Принудительно выгрузить ключ, не закрывая Проводник, можно, выбрав в главном меню расширения проводника пункт «Выгрузить ключ». Просмотреть информацию о рабочем сертификате (и загруженном ключе) можно, выбрав в главном меню расширения проводника пункт «Показать рабочий сертификат».

Если опция «Выгружать ключ после каждой операции» включена, ключ будет выгружен сразу после завершения операции над всеми выбранными файлами.

В случае, если одновременно загружено несколько экземпляров Проводника, в них могут быть загружены разные ключи. Сразу после загрузки ключа производится подключение к сетевому справочнику (LDAP), если в настройках пользователя не установлен режим «Не использовать сетевой справочник (LDAP)». В случае, если при подключении к LDAP произошла ошибка, на экран выводится диалог (возможно, после таймаута):

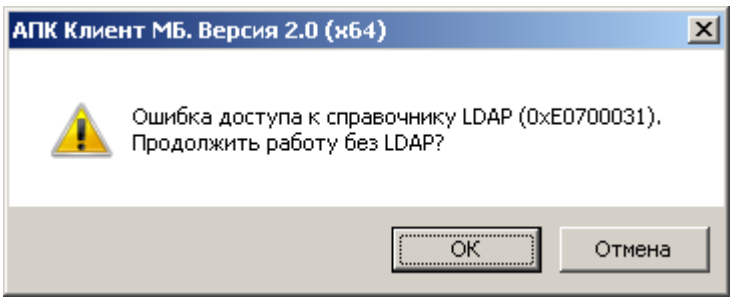

Рисунок 71 – Диалог с сообщением об ошибке подключения к LDAP

Нажатие кнопки «OK» приводит к продолжению работы без сетевого справочника, нажатие кнопки «Отмена» - к выгрузке ключа и отказу от операции.

Если в настройках пользователя не установлен режим «Не обновлять COC из точки распространения», будет произведено обновление COC. В случае ошибки на экран выводится диалог (возможно, после таймаута):

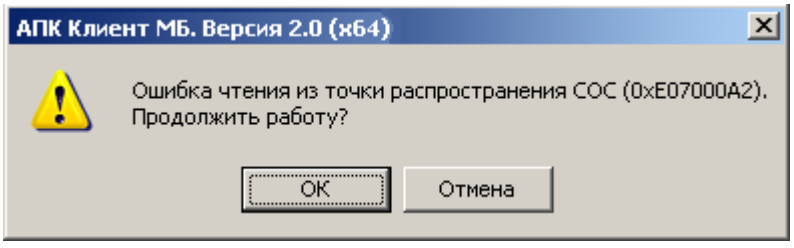

Рисунок 72 – Диалог с сообщением об ошибке при обновлении COC

Нажатие кнопки «ОК» приводит к продолжению работы без обновления СОС из точки распространения, нажатие кнопки «Отмена» - к выгрузке ключа и отказу от операции.

7.4 Криптографические операции над файлами

7.4.1 Создание ЭП

Для того чтобы создать присоединённую ЭП в формате PKCS#7, выделите в Проводнике один или несколько файлов или каталогов и выберите в главном меню расширения проводника пункт «Создать ЭП». Если ранее в этом экземпляре Проводника не был загружен (или был выгружен) ключ, произойдёт загрузка ключа (см. п. 7.3). Перед созданием ЭП будет произведена проверка уже имеющихся в файле присоединённых ЭП в формате PKCS#7 (если они там есть), при условии, что в настройках пользователя не установлен режим «Не проверять предыдущие подписи перед созданием ЭП». Если проверка существующих ЭП не была успешной, создание новой ЭП не происходит. Подписанный файл сохраняется в каталог, заданный в параметре «Каталог для сохранения подписанных/ зашифрованных файлов» в настройках пользователя (или в каталог, где находится подписываемый файл, если этот параметр не задан). При этом к имени файла добавляется расширение, заданное в параметре «Основные расширения имён файлов - Подписанные файлы» в настройках пользователя. В случае, когда файл уже имеет такое расширение, второй раз оно не добавляется. Если при записи подписанного файла оказывается, что файл с таким именем уже существует (за исключением случая, когда происходит добавление подписи в уже подписанный файл), выдаётся стандартный диалог, предлагающий сохранить файл под другим (или тем же самым) именем (если в настройках пользователя не установлен режим «Не выдавать диалог сохранения файла»). Нажатие кнопки «Отмена» прекращает выполнение операции. Кроме того, будет выдан диалог подтверждения перезаписи (если в настройках пользователя не установлен режим «Перезаписывать файлы без предупреждения»):

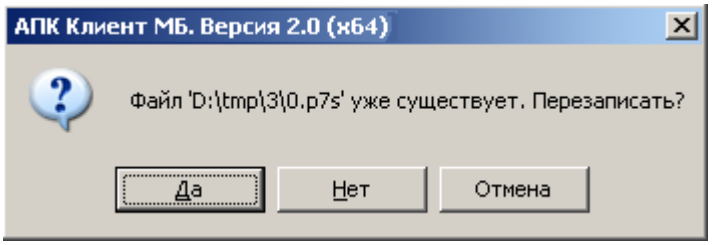

Рисунок 73 – Диалог подтверждения перезаписи файла

Нажатие кнопки «Да» приводит к выполнению операции, кнопки «Нет» - пропуску операции с текущим файлом, кнопки «Отмена» - прекращению операции со всеми оставшимися файлами.

Если операция создания ЭП производится с одним файлом, после создания ЭП на экран выдаётся сообщение об успехе:

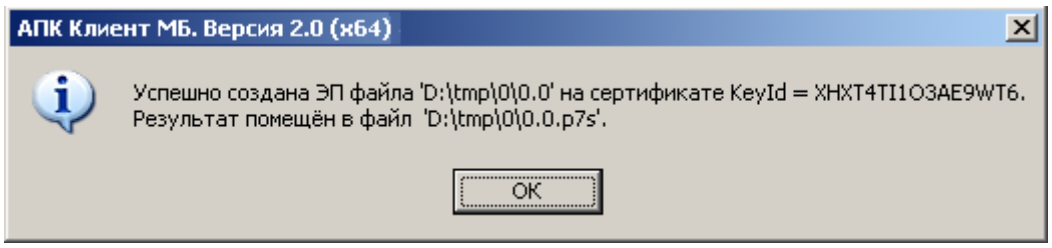

Рисунок 74 – Сообщение об успешном создании ЭП

или сообщение об ошибке:

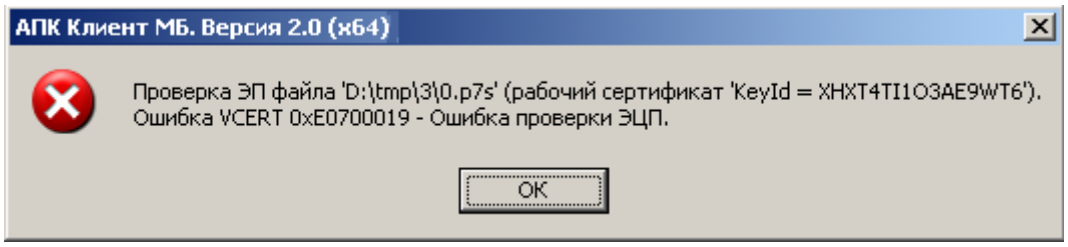

Рисунок 75 – Сообщение об ошибке при создании ЭП

Если в настройках пользователя установлен режим «Использовать TSP сервер» и задан адрес TSP сервера, при создании ЭП в неё будет добавлен штамп времени (TSP). Если при добавлении штампа времени произошла ошибка, вся операция считается неуспешной, подписанный файл не создаётся.

Если операция создания ЭП производится с несколькими файлами, сначала на экран выдаётся запрос на подтверждение, при условии, что в настройках пользователя не установлен режим «Не выдавать предварительный диалог с количеством файлов»:

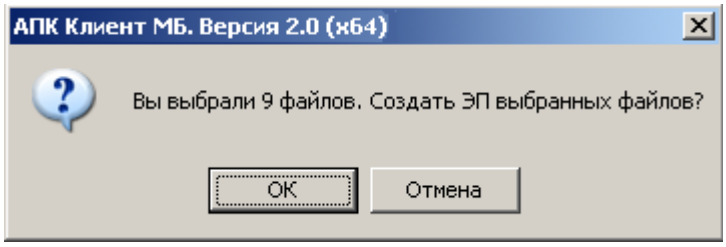

Рисунок 76 – Запрос на создание ЭП

Затем на экран выдаётся диалог создания ЭП файлов:

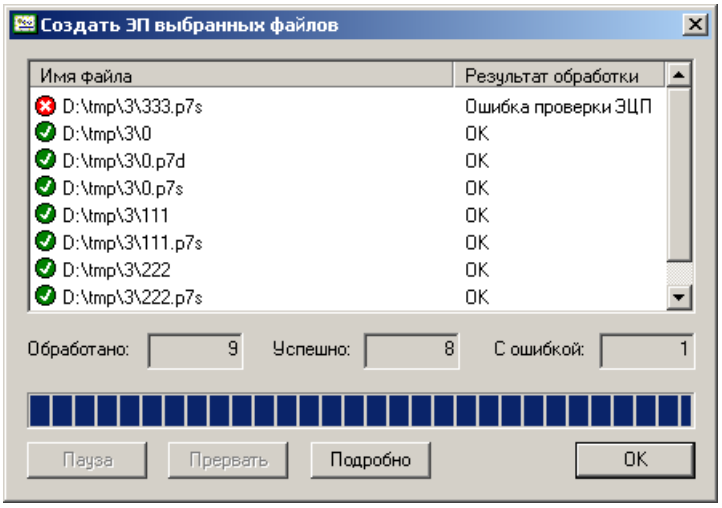

Рисунок 77 – Диалог создания ЭП файлов

Во второй колонке списка выводится краткая информация о результате создания ЭП. Для отображения полной информации выделите строчку с файлом и нажмите кнопку «Подробно» (или сделайте двойной клик мышью).

В процессе обработки вы можете приостановить или прервать создание ЭП нажатием кнопок «Пауза» или «Прервать».

7.4.2 Проверка ЭП

Для того чтобы проверить присоединённую ЭП, выделите в Проводнике один или несколько файлов или каталогов и выберите в главном меню расширения проводника пункт «Проверить ЭП». Если ранее в этом экземпляре Проводника не был загружен (или был выгружен) ключ, произойдёт загрузка ключа (см. п. 7.3).

Если операция проверки ЭП производится с одним файлом, после проверки ЭП на экран выдаётся диалог с информацией о проверенных ЭП:

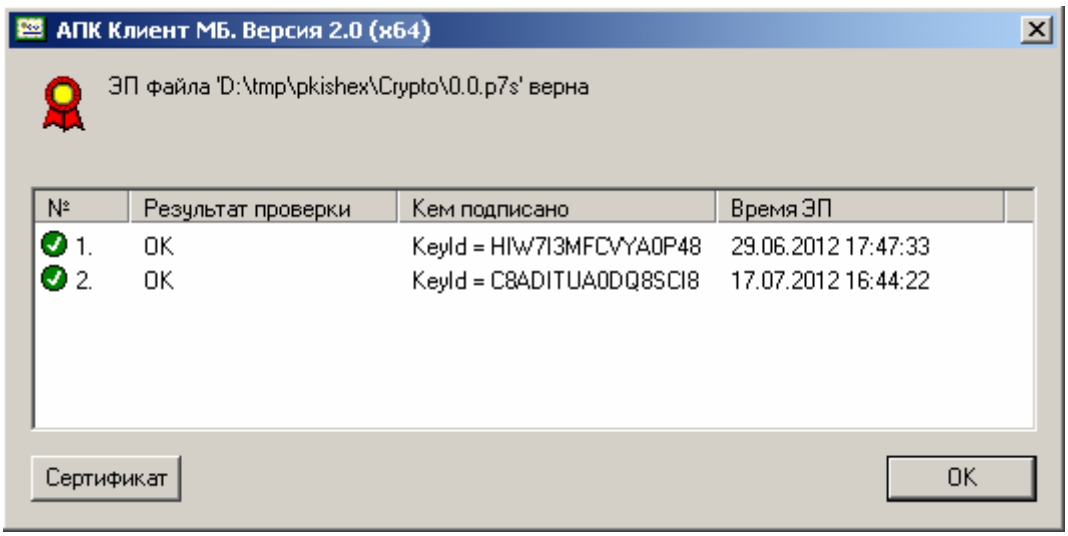

Рисунок 78 – Диалог с информацией о проверке ЭП

Первая колонка содержит номер ЭП и иконку – признак успешной или неуспешной проверки, вторая колонка – описание результата проверки этой подписи, третья – идентификатор сертификата, на котором создана ЭП, и четвёртая – время создания ЭП. Чтобы подробно просмотреть сертификат, выделите подпись и нажмите кнопку «Сертификат» (или сделайте двойной клик мышью):

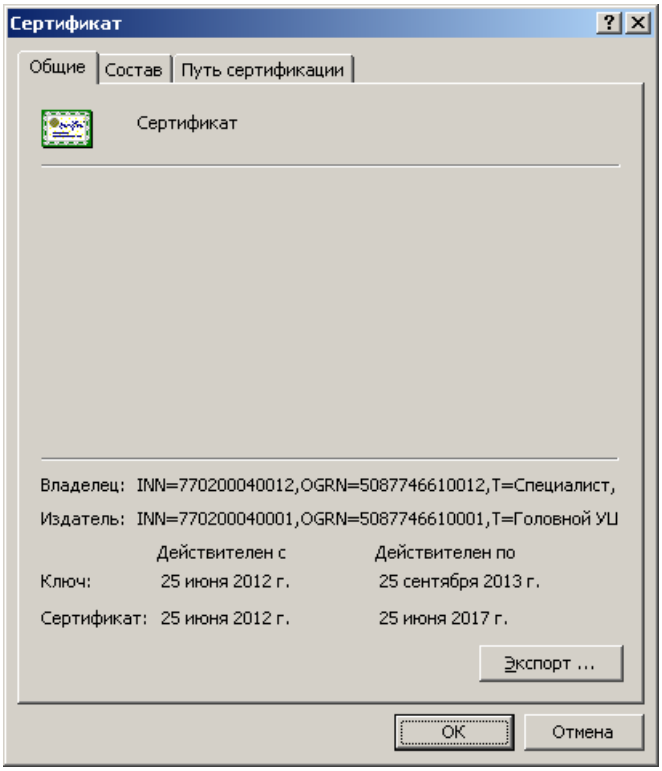

Рисунок 79 – Диалог просмотра сертификата

В случае если хоть одна подпись не была успешно проверена, результат проверки файла является отрицательным:

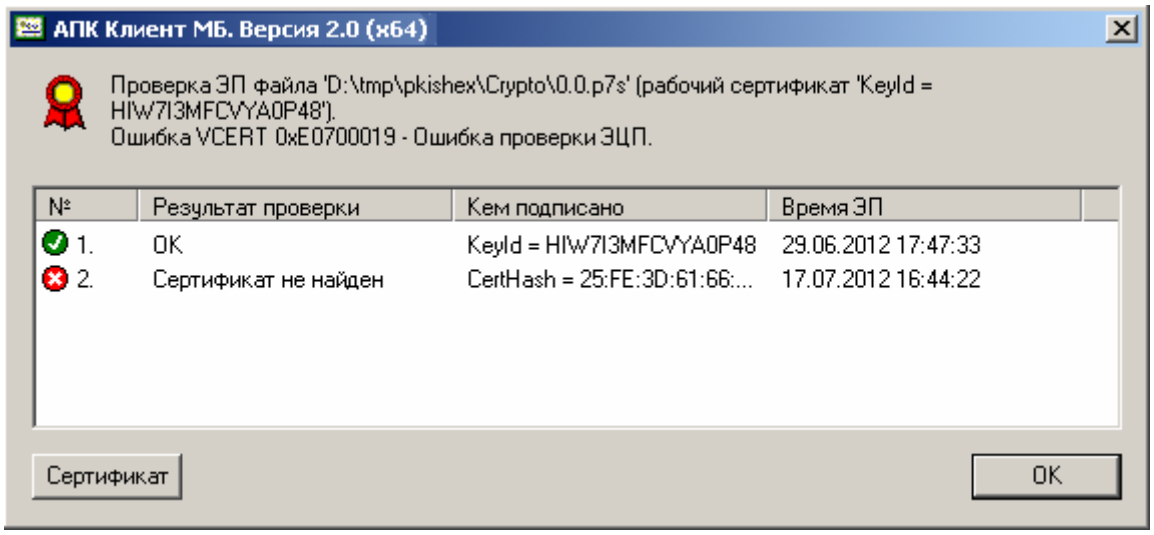

Рисунок 80 – Диалог с информацией об ошибке при проверке ЭП

Если в настройках пользователя установлен режим «Проверять штамп времени при проверке подписи», при проверке каждой ЭП производится поиск штампа времени (TSP) и его проверка (в случае обнаружения). В диалоге с информацией о проверке ЭП информация о проверке штампа времени ЭП содержится под строчкой, содержащей информацию о проверке этой ЭП и содержит аналогичную информацию (если в настройках пользователя не установлен режим «Отсутствие штампа времени считать ошибкой», информация об отсутствии штампа времени не выводится):

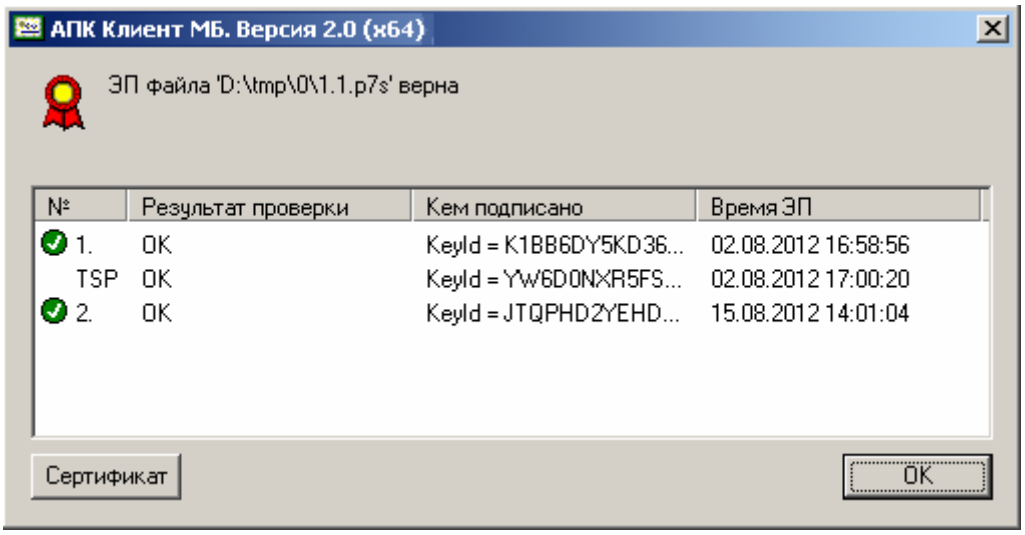

Рисунок 81 – Диалог с информацией о проверке ЭП со штампом времени

В случае возникновения ошибки при проверке штампа времени проверка подписи считается неудачной:

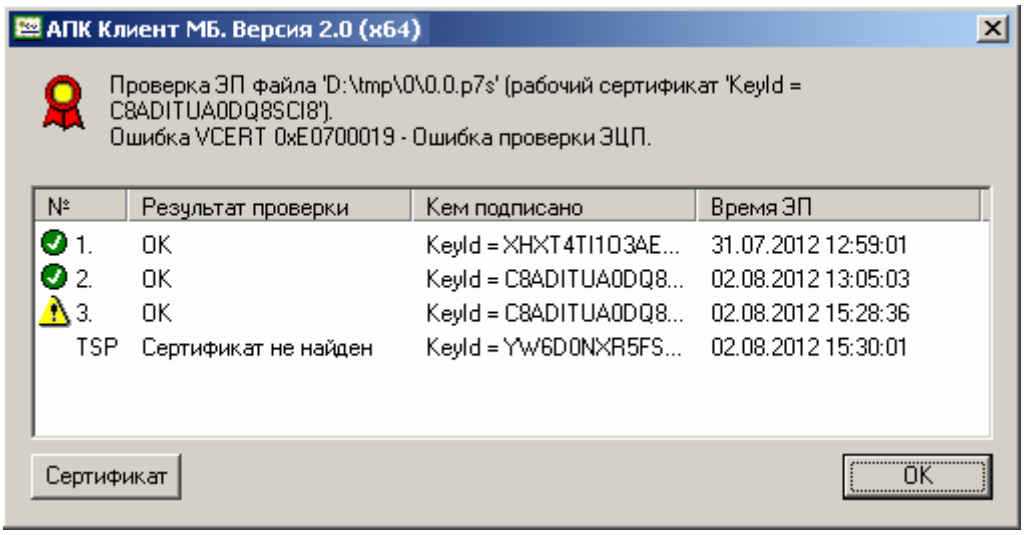

Рисунок 82 – Диалог с информацией об ошибке при проверке штампа времени ЭП

Если в настройках пользователя установлен режим «Отсутствие штампа времени считать ошибкой», отсутствующие штампы времени отображаются отдельной строкой:

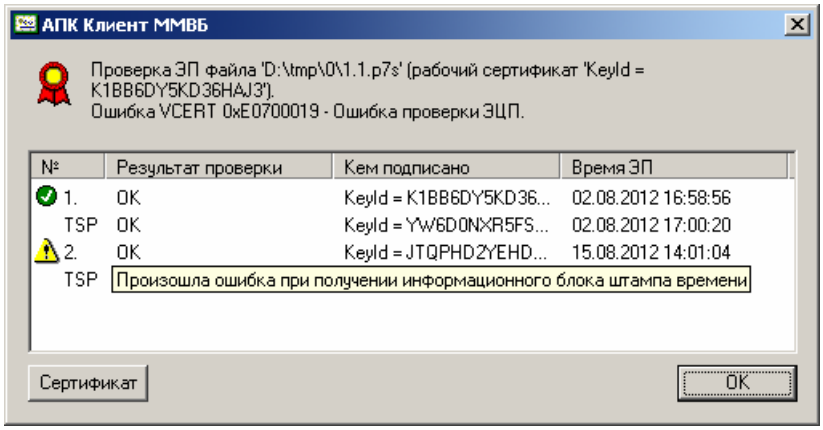

Рисунок 83 – Диалог с информацией об отсутствии штампа времени ЭП

Если операция проверки ЭП производится с несколькими файлами, сначала на экран выдаётся запрос на подтверждение при условии, что в настройках пользователя не установлен режим «Не выдавать предварительный диалог с количеством файлов»:

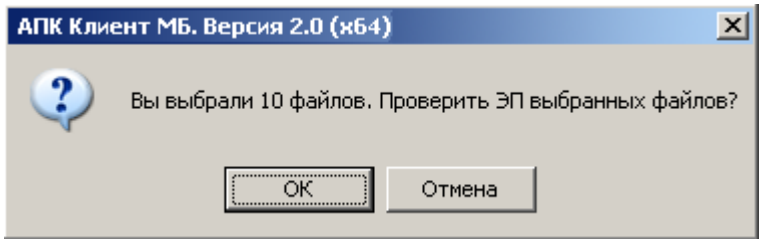

Рисунок 84 – Запрос на проверку ЭП

Затем на экран выдаётся диалог проверки ЭП файлов:

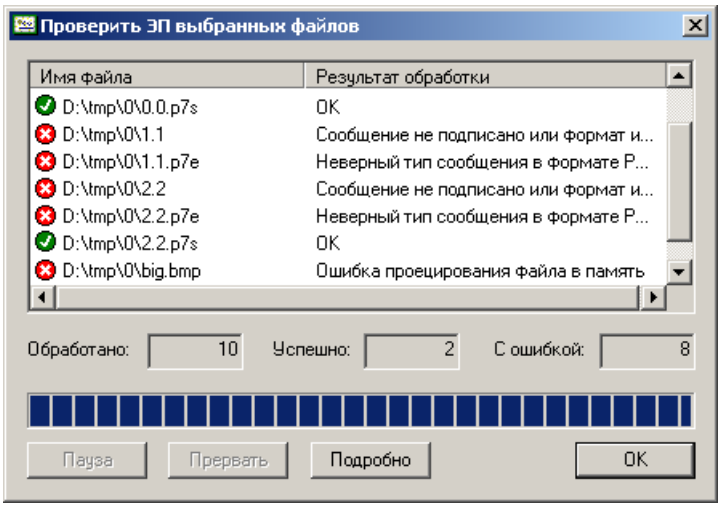

Рисунок 85 – Диалог проверки ЭП файлов

Во второй колонке списка выводится краткая информация о результате проверки ЭП. Для отображения полной информации выделите строчку с файлом и нажмите кнопку «Подробно» (или сделайте двойной клик мышью).

В процессе обработки вы можете приостановить или прервать проверку ЭП нажатием кнопок «Пауза» или «Прервать».

7.4.3 Проверка и удаление ЭП

Для того чтобы проверить присоединённую ЭП и удалить из файла одну или несколько подписей выделите в Проводнике один или несколько файлов или каталогов и выберите в главном меню расширения проводника пункт «Проверить и удалить ЭП». Если ранее в этом экземпляре Проводника не был загружен (или был выгружен) ключ, произойдёт загрузка ключа (см. п. 7.3). Затем на экране появится диалог подтверждения удаления ЭП. Диалог будет выдан независимо от количества выбранных файлов и от выбора режима «Не выдавать предварительный диалог с количеством файлов» в настройках пользователя:

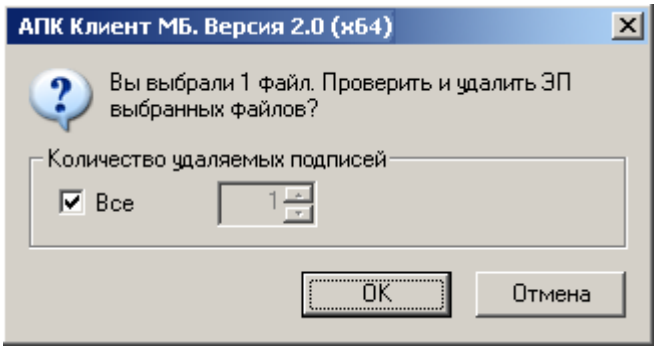

Рисунок 86 – Диалог удаления ЭП

Чтобы удалить не все подписи, а несколько (начиная с конца), снимите опцию «Все» и выберите количество удаляемых подписей:

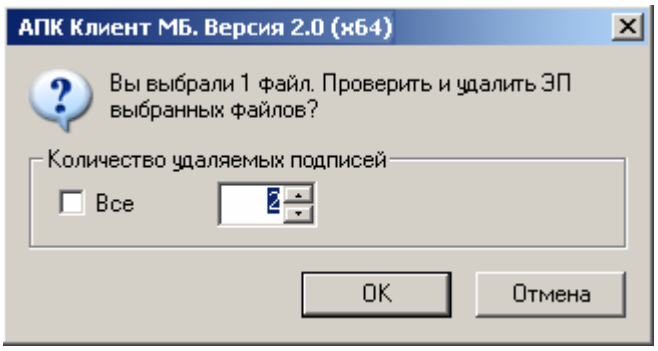

Рисунок 87 – Диалог удаления ЭП без опции «Все»

Удаление ЭП производится только в случае успешной проверки всех подписей файла. Файл, полученный в результате удаления подписей, сохраняется в каталог, заданный в параметре «Каталог для сохранения проверенных/ расшифрованных файлов» в настройках пользователя (или в каталог, где находится проверяемый файл, если этот параметр не задан). При этом, если удаляются все подписи, а файл имеет расширение, заданное в параметре «Основные расширения имён файлов - Подписанные файлы» или в параметре «Дополнительные расширения имён файлов» в настройках пользователя, это расширение будет удалено. В случае, когда файл не имеет такого расширения и в случае, когда удаляются не все подписи, имя файла не меняется. Если при записи файла с удалёнными ЭП оказывается, что файл с таким именем уже существует (за исключением случая, когда происходит удаление не всех ЭП, и результат записывается в исходный файл), выдаётся стандартный диалог, предлагающий сохранить файл под другим (или тем же самым) именем (если в настройках пользователя не установлен режим «Не выдавать диалог сохранения файла»). Нажатие кнопки «Отмена» прекращает выполнение операции. Кроме того, будет выдан диалог подтверждения перезаписи (если в настройках пользователя не установлен режим «Перезаписывать файлы без предупреждения»):

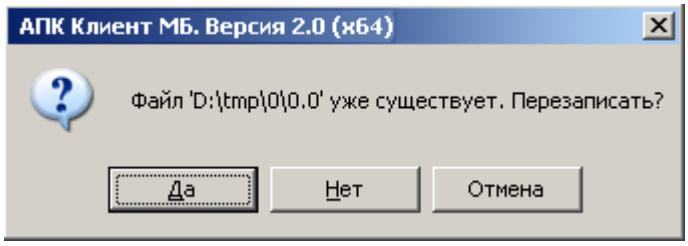

Рисунок 88 – Диалог подтверждения перезаписи файла

Нажатие кнопки «Да» приводит к выполнению операции, кнопки «Нет» - пропуску операции с текущим файлом, кнопки «Отмена» - прекращению операции со всеми оставшимися файлами.

Если операция проверки и удаления ЭП производится с одним файлом, после выполнения операции на экран выдаётся диалог с информацией о проверенных и удалённых ЭП:

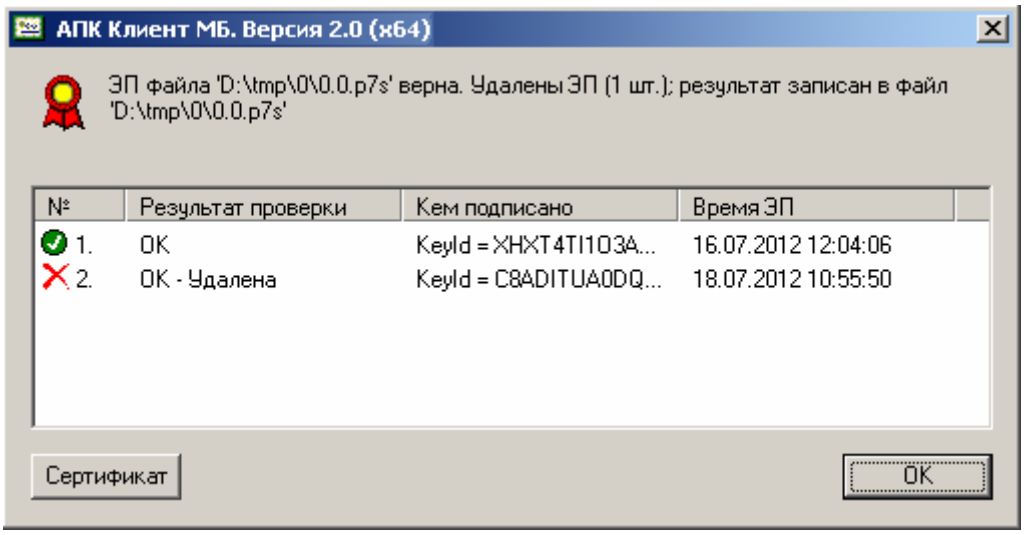

Рисунок 89 – Диалог с информацией о проверке и удалении ЭП

Первая колонка содержит номер ЭП и иконку – признак удаления или успешной (неуспешной) проверки, вторая колонка – описание результата операции, третья – идентификатор сертификата, на котором создана ЭП, и четвёртая – время создания ЭП. Чтобы подробно просмотреть сертификат, выделите подпись и нажмите кнопку «Сертификат» (или сделайте двойной клик мышью).

Если операция проверки ЭП производится с несколькими файлами, на экран выдаётся диалог проверки и удаления ЭП файлов:

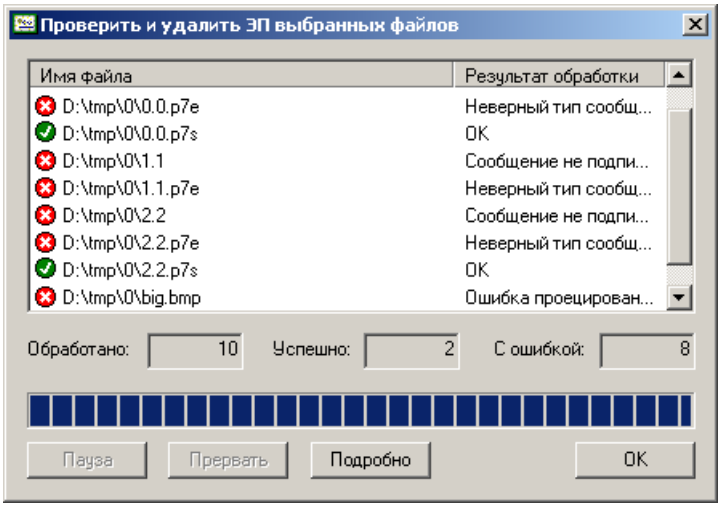

Рисунок 90 – Диалог проверки и удаления ЭП файлов

Во второй колонке списка выводится краткая информация о результате операции. Для отображения полной информации выделите строчку с файлом и нажмите кнопку «Подробно» (или сделайте двойной клик мышью).

В процессе обработки вы можете приостановить или прервать выполнение операции нажатием кнопок «Пауза» или «Прервать».

7.4.4 Удаление ЭП без проверки

Для того чтобы удалить из файлов все ЭП, выделите в Проводнике один или несколько файлов или каталогов и выберите в главном меню расширения проводника «Дополнительно», подпункт «Удалить ЭП без проверки». Если ранее в этом экземпляре Проводника не был загружен (или был выгружен) ключ, произойдёт загрузка ключа (см. п. 7.3).

Файл, полученный в результате удаления всех подписей, сохраняется в каталог, заданный в параметре «Каталог для сохранения проверенных/ расшифрованных файлов» в настройках пользователя (или в каталог, где находится подписанный файл, если этот параметр не задан). При этом, если файл имеет расширение, заданное

в параметре «Основные расширения имён файлов - Подписанные файлы» или в параметре «Дополнительные расширения имён файлов» в настройках пользователя, это расширение будет удалено. В случае, когда файл не имеет такого расширения, имя файла не меняется. Если при записи файла с удалёнными ЭП оказывается, что файл с таким именем уже существует, выдаётся стандартный диалог, предлагающий сохранить файл под другим (или тем же самым) именем (если в настройках пользователя не установлен режим «Не выдавать диалог сохранения файла»). Нажатие кнопки «Отмена» прекращает выполнение операции. Кроме того, будет выдан диалог подтверждения перезаписи (если в настройках пользователя не установлен режим «Перезаписывать файлы без предупреждения»):

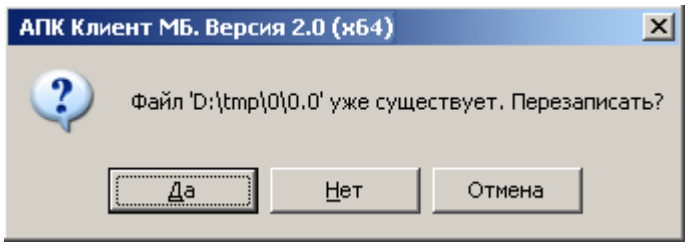

Рисунок 91 – Диалог подтверждения перезаписи файла

Нажатие кнопки «Да» приводит к выполнению операции, кнопки «Нет» - пропуску операции с текущим файлом, кнопки «Отмена» - прекращению операции со всеми оставшимися файлами.

Если операция удаления ЭП производится с одним файлом, после проверки ЭП на экран выдаётся сообщение об успехе:

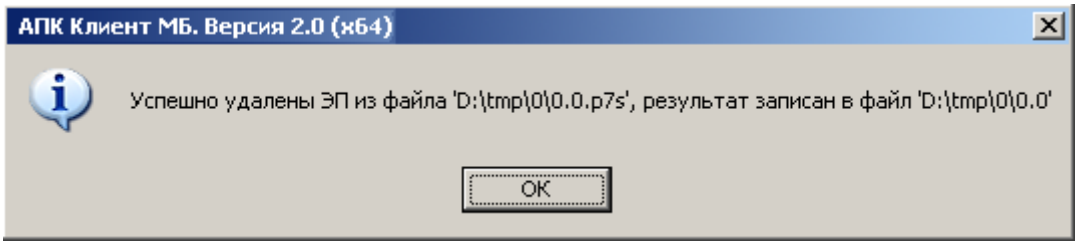

Рисунок 92 – Сообщение об успешном удалении ЭП

или сообщение об ошибке:

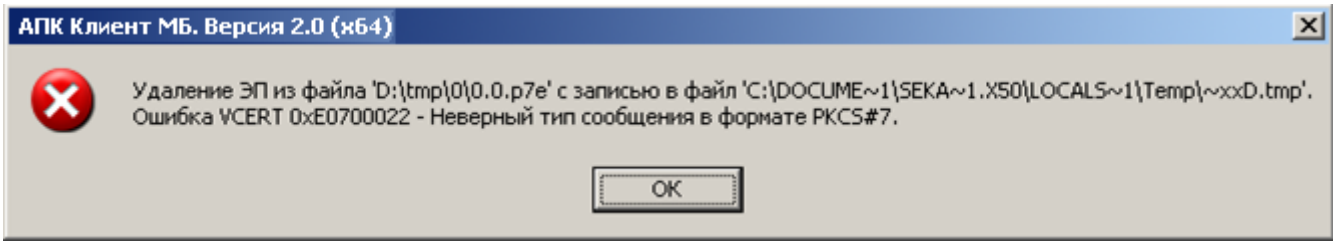

Рисунок 93 – Сообщение об ошибке при удалении ЭП

Если операция удаления ЭП производится с несколькими файлами, сначала на экран выдаётся запрос на подтверждение при условии, что в настройках пользователя не установлен режим «Не выдавать предварительный диалог с количеством файлов»:

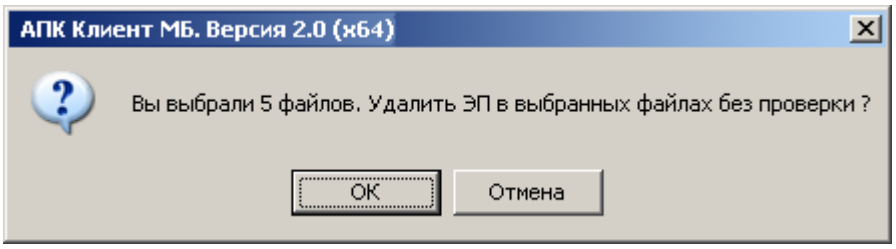

Рисунок 94 – Запрос на удаление ЭП

Затем на экран выдаётся диалог удаления ЭП:

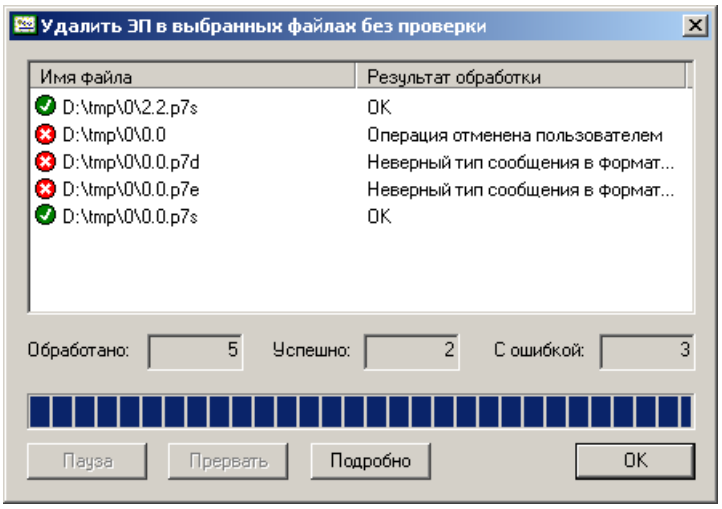

Рисунок 95 – Диалог удаления ЭП

Во второй колонке списка выводится краткая информация о результате операции. Для отображения полной информации выделите строчку с файлом и нажмите кнопку «Подробно» (или сделайте двойной клик мышью).

В процессе обработки вы можете приостановить или прервать выполнение операции нажатием кнопок «Пауза» или «Прервать».

7.4.5 Зашифрование

Для зашифрования файлов размером до 256Мб выделите в Проводнике один или несколько файлов или каталогов и выберите в главном меню расширения проводника пункт «Зашифровать». Для зашифрования файлов размером более 256Мб выберите пункт «Дополнительно», подпункт «Зашифровать большой файл» (при этом зашифрование будет происходить в потоковом режиме). Потоковый режим зашифрования применим к файлам любого (в том числе маленького) размера, однако файлы, зашифрованные таким образом, могут не расшифроваться некоторым другим ПО, поэтому в целях совместимости форматов не рекомендуется использовать режим потокового зашифрования без необходимости. Если ранее в этом экземпляре Проводника не был загружен (или был выгружен) ключ, произойдёт загрузка ключа (см. п. 7.3). Прежде, чем начать зашифрование, необходимо задать список получателей зашифрованного сообщения. Для этого на экран выдаётся диалог выбора получателей зашифрованного сообщения:

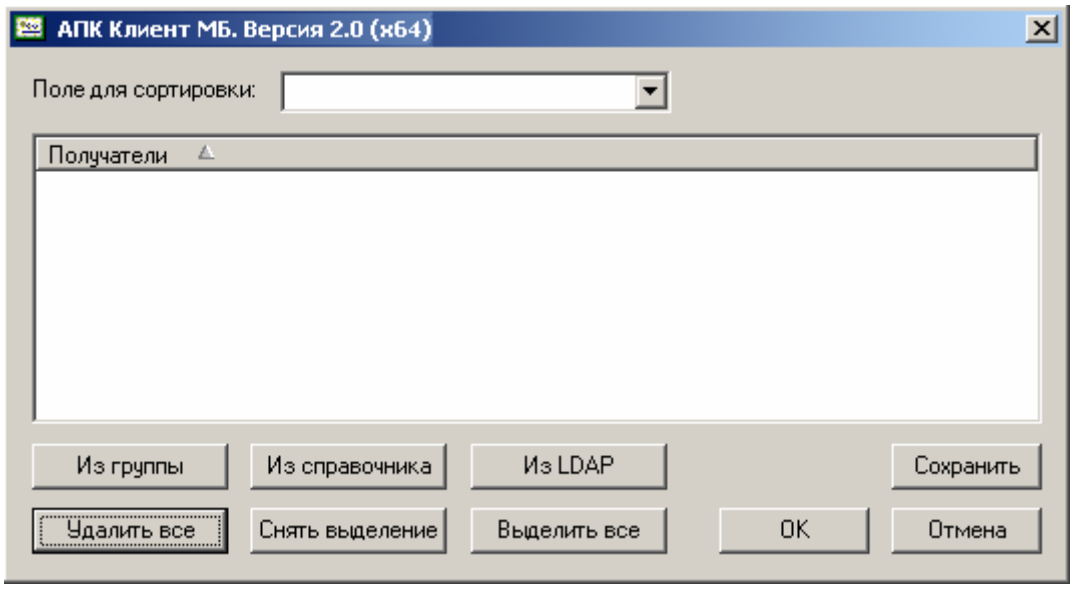

Рисунок 96 – Пустой диалог выбора получателей

Изначально список получателей пуст. Нажмите кнопку «Из справочника», чтобы внести в список всех владельцев сертификатов, предназначенных для шифрования, содержащихся в Справочнике сертификатов. Найденные имена пользователей добавляются к списку получателей и отмечаются «галочками»:

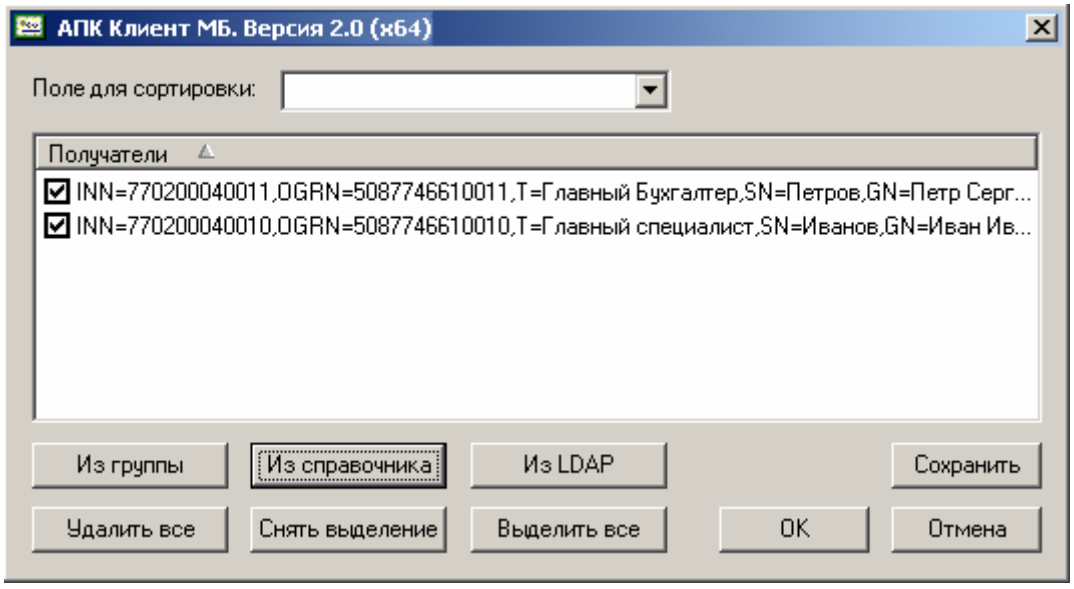

Рисунок 97 – Заполненный диалог выбора получателей

Чтобы просмотреть имя владельца сертификата целиком, сделайте на нём двойной клик мышью:

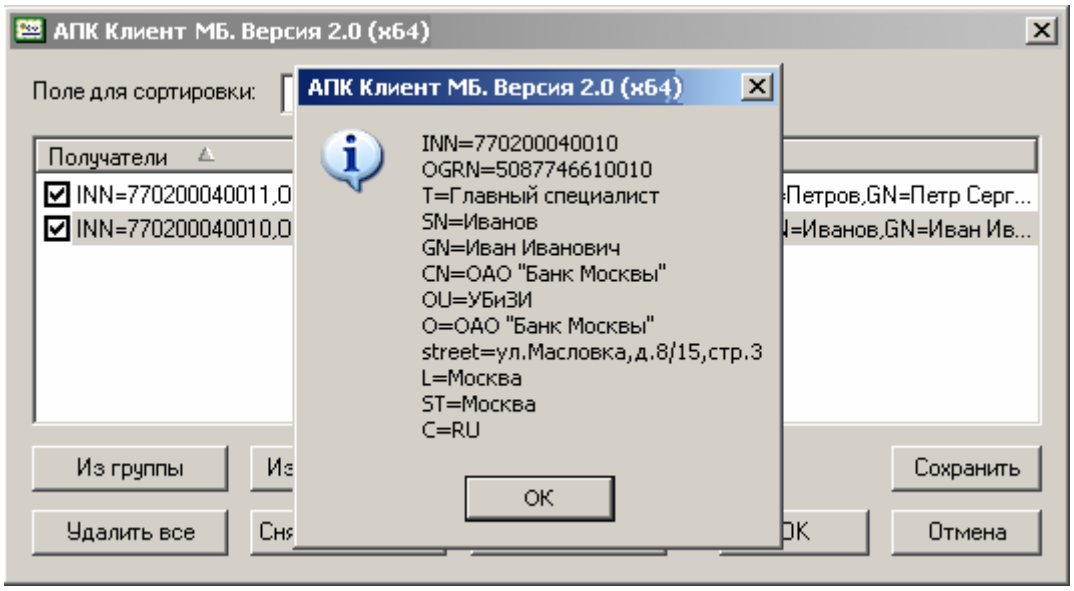

Рисунок 98 – Диалог просмотра имени владельца сертификата

Если в настройках пользователя отключён режим «Не использовать сетевой справочник (LDAP)», будет доступна кнопка «Из LDAP». Для поиска сертификатов в сетевом справочнике нажмите её. На экране появится диалог поиска в LDAP:

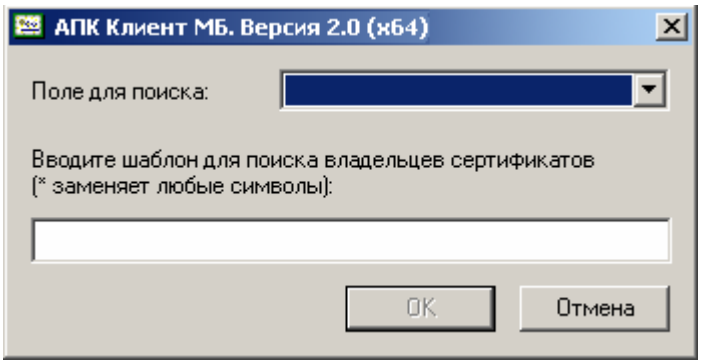

Рисунок 99 – Диалог поиска в LDAP

Задайте поле (часть имени владельца сертификата) для поиска и шаблон поиска – строку, в которой символ * (звёздочка) заменяет любой набор символов (регистр букв при поиске значения не имеет). Например, для поиска всех пользователей с отчеством «Иванович» поиск должен выглядеть следующим образом:

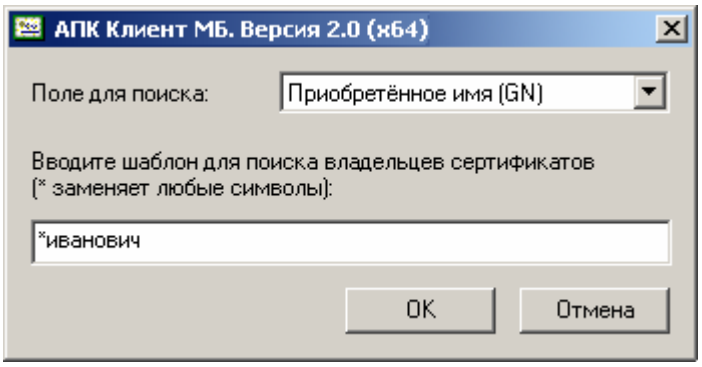

Рисунок 100 – Заполненный диалог поиска в LDAP

В качестве поля для поиска можно выбрать режим <Поиск по всему имени>:

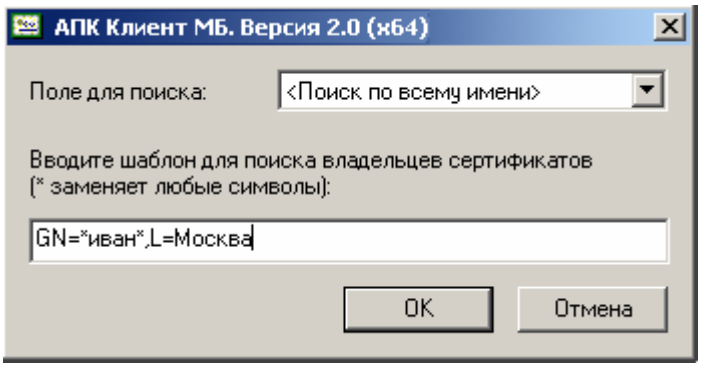

Рисунок 101 – Поиск в LDAP по всему имени

В этом режиме можно задать шаблон для поиска по всему имени владельца (порядок полей имеет значение). К заданному шаблону в начале и в конце добавляется символ * (звёздочка).

Найденные имена пользователей добавляются к списку получателей и отмечаются «галочками». Список получателей может быть отсортирован по любому полю (части имени владельца сертификата). Для сортировки выберите поле в раскрывающемся списке; нажатие на заголовок списка (там, где слово «Получатели») переключает порядок сортировки – по возрастанию / по убыванию:

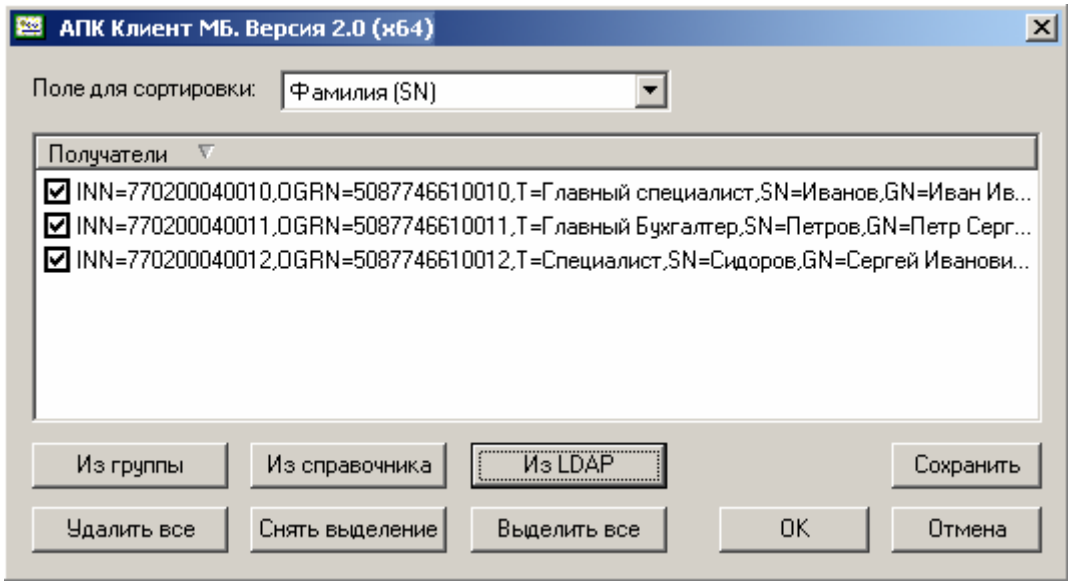

Рисунок 102 – Список, отсортированный по фамилии

Чтобы сохранить группу получателей, отметьте их в списке «галочками» и нажмите кнопку «Сохранить». Выберите имя для файла группы в стандартном диалоге сохранения файла (если в настройках пользователя задан параметр «Каталог для сохранения файлов групп пользователей», этот каталог будет предложен для сохранения файла). Для удобства выделения «галочками» имён пользователей используйте кнопки «Выделить все» и «Снять выделение». Нажатие на кнопку «Удалить все» после подтверждения очищает список.

Чтобы открыть ранее созданную группу, нажмите кнопку «Из группы» и выберите имя файла в стандартном диалоге открытия файла (если в настройках пользователя задан параметр «Каталог для сохранения файлов групп пользователей» этот каталог будет предложен для открытия файла). Имена пользователей, содержащиеся в открытой группе, добавляются к списку получателей и отмечаются «галочками».

После того, как список сформирован, для зашифрования на всех получателей из списка, отмеченных «галочками», нажмите кнопку «OK». При этом будет сформирован список сертификатов для выполнения зашифрования (один пользователь может иметь несколько сертификатов, зашифрование производится на все сертификаты

пользователя предназначенные для шифрования). Если для какого-либо получателя из списка не найдено ни одного сертификата, на экран выдаётся предупреждение:

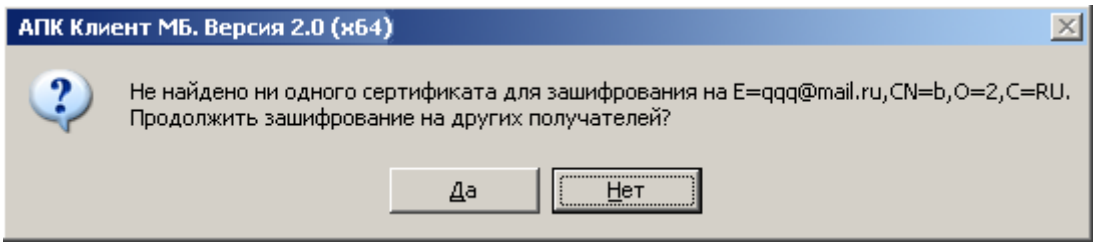

Рисунок 103 – Предупреждение об отсутствии сертификатов для шифрования

Нажатие кнопки «Да» исключает получателя из списка, нажатие кнопки «Нет» прекращает операцию. Список получателей, для которых найден хотя бы один сертификат для шифрования, сохраняется (но не более 256 получателей) и предлагается пользователю при следующем открытии диалога выбора получателей.

Если файл, к которому применяется операция зашифрования, уже зашифрован, на экран выдаётся предупреждение:

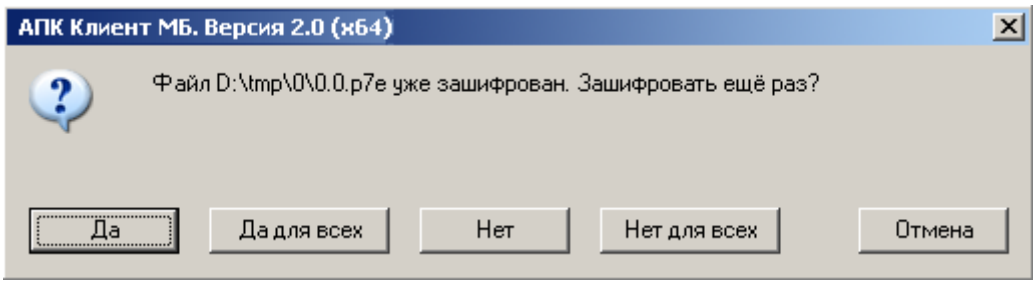

Рисунок 104 – Предупреждение о том, что файл уже зашифрован

Нажмите кнопку «Да», чтобы разрешить повторное зашифрование файла, на кнопку «Да для всех» разрешает повторное зашифрование указанного файла и всех остальных файлов, выбранных для данной операции. Нажатие на кнопку «Нет» приводит к пропуску данного файла, «Нет для всех» - к пропуску всех зашифрованных файлов, выбранных для данной операции. Кнопка «Отмена» прекращает операцию (в случае, если для зашифрования выбран только один файл, в этом диалоге будут только две кнопки – «OK» и «Отмена»).

Зашифрованный файл сохраняется в каталог, заданный в параметре «Каталог для сохранения подписанных/ зашифрованных файлов» в настройках пользователя (или в каталог, где находится шифруемый файл, если этот параметр не задан). При этом к имени файла добавляется расширение, заданное в параметре «Основные расширения имён файлов - Зашифрованные файлы» в настройках пользователя. В случае, когда файл уже имеет такое расширение, второй раз оно не добавляется. Если при записи зашифрованного файла оказывается, что файл с таким именем уже существует (за исключением случая, когда происходит зашифрование уже зашифрованного файла), выдаётся стандартный диалог, предлагающий сохранить файл под другим (или тем же самым) именем (если в настройках пользователя не установлен режим «Не выдавать диалог сохранения файла»). Нажатие кнопки «Отмена» прекращает выполнение операции. Кроме того, будет выдан диалог подтверждения перезаписи (если в настройках пользователя не установлен режим «Перезаписывать файлы без предупреждения»):

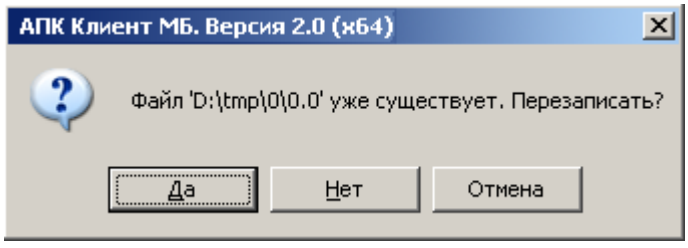

Рисунок 105 – Диалог подтверждения перезаписи файла

Нажатие кнопки «Да» приводит к выполнению операции, кнопки «Нет» - пропуску операции с текущим файлом, кнопки «Отмена» - прекращению операции со всеми оставшимися файлами.

Если операция зашифрования производится с одним файлом, после выполнения операции на экран выдаётся сообщение об успехе:

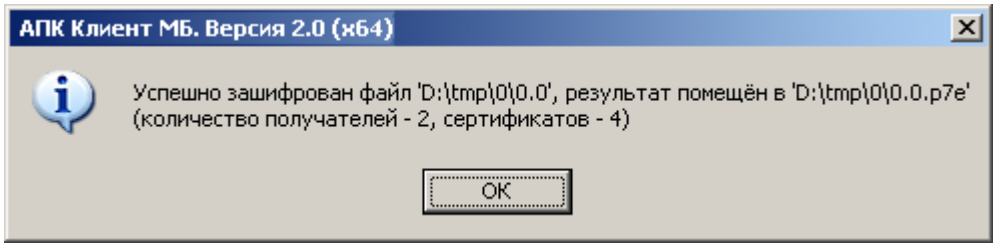

Рисунок 106 – Сообщение об успешном зашифровании файла

либо сообщение об ошибке:

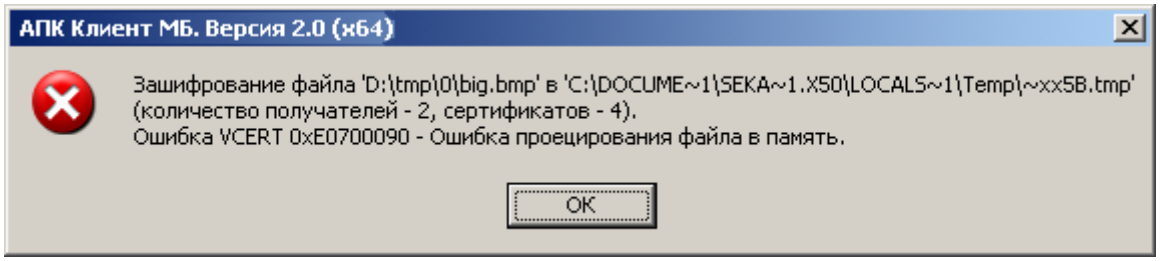

Рисунок 107 – Сообщение об ошибке при зашифровании файла

Если операция зашифрования производится с несколькими файлами, сначала на экран выдаётся запрос на подтверждение при условии, что в настройках пользователя не установлен режим «Не выдавать предварительный диалог с количеством файлов»:

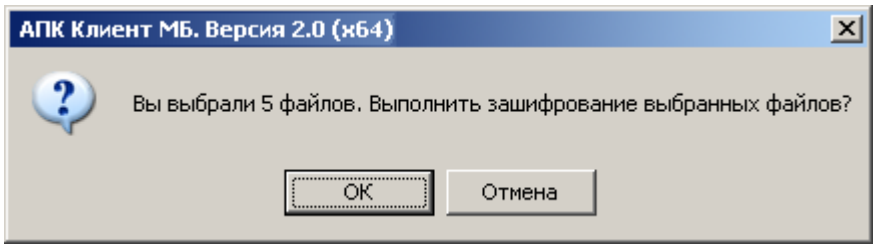

Рисунок 108 – Запрос на зашифрование

Затем на экран выдаётся диалог зашифрования файлов:

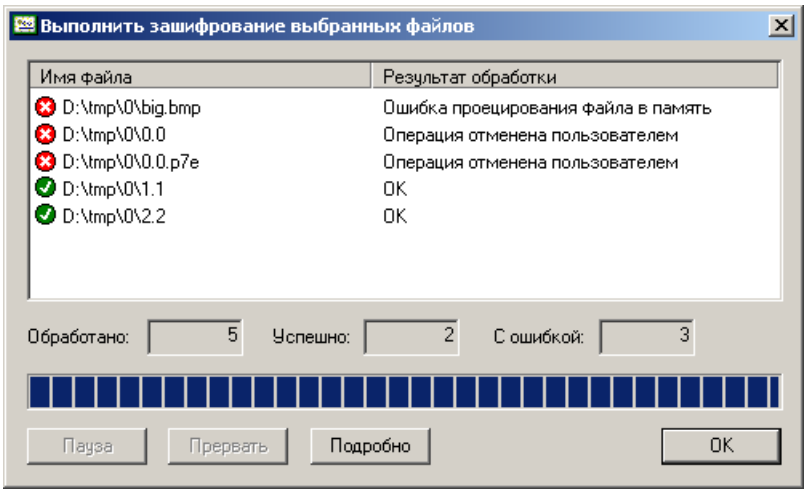

Рисунок 109 – Диалог зашифрования файлов

Во второй колонке списка выводится краткая информация о результате зашифрования. Для отображения полной информации выделите строчку с файлом и нажмите кнопку «Подробно» (или сделайте двойной клик мышью).

В процессе обработки вы можете приостановить или прервать зашифрование нажатием кнопок «Пауза» или «Прервать».

7.4.6 Расшифрование

Для расшифрования файлов размером до 256Мб выделите в Проводнике один или несколько файлов или каталогов и выберите в главном меню расширения проводника пункт «Расшифровать». Для расшифрования файлов размером более 256Мб выберите пункт «Дополнительно», подпункт «Расшифровать большой файл» (при этом расшифрование будет происходить в потоковом режиме). Потоковый режим расшифрования применим к файлам любого (в том числе маленького) размера. Если ранее в этом экземпляре Проводника не был загружен (или был выгружен) ключ, произойдёт загрузка ключа (см. п. 7.3).

Расшифрованный файл сохраняется в каталог, заданный в параметре «Каталог для сохранения проверенных/ расшифрованных файлов» в настройках пользователя (или в каталог, где находится зашифрованный файл, если этот параметр не задан). При этом, если файл имеет расширение, заданное в параметре «Основные расширения имён файлов - Зашифрованные файлы» или в параметре «Дополнительные расширения имён файлов» в настройках пользователя, это расширение будет удалено. В случае, когда файл не имеет такого расширения, имя файла не меняется. Если при записи рашифрованного файла оказывается, что файл с таким именем уже существует, выдаётся стандартный диалог, предлагающий сохранить файл под другим (или тем же самым) именем (если в настройках пользователя не установлен режим «Не выдавать диалог сохранения файла»). Нажатие кнопки «Отмена» прекращает выполнение операции. Кроме того, будет выдан диалог подтверждения перезаписи (если в настройках пользователя не установлен режим «Перезаписывать файлы без предупреждения»):

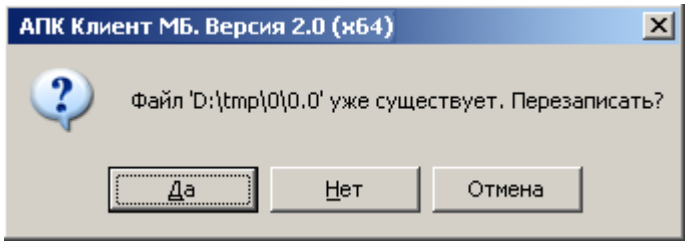

Рисунок 110 – Диалог подтверждения перезаписи файла

Нажатие кнопки «Да» приводит к выполнению операции, кнопки «Нет» - пропуску операции с текущим файлом, кнопки «Отмена» - прекращению операции со всеми оставшимися файлами.

Если операция расшифрования производится с одним файлом, после выполнения операции на экран выдаётся сообщение об успехе:

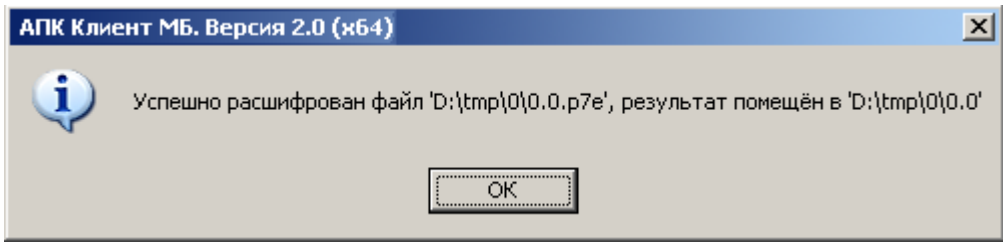

Рисунок 111 – Сообщение об успешном расшифровании файла

или сообщение об ошибке:

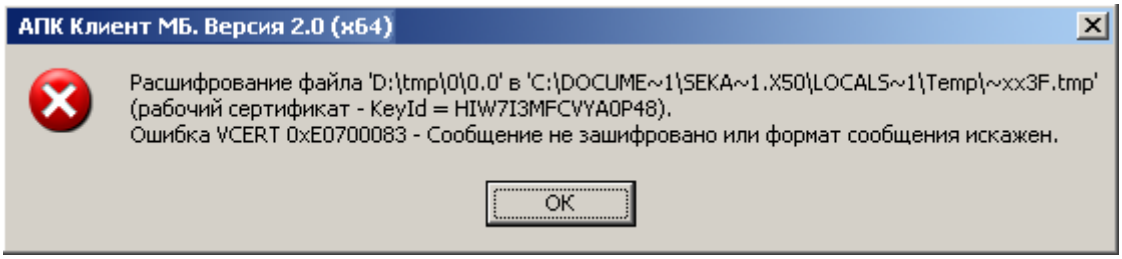

Рисунок 112 – Сообщение об ошибке при расшифровании файла

Если операция расшифрования производится с несколькими файлами, сначала на экран выдаётся запрос на подтверждение, при условии, что в настройках пользователя не установлен режим «Не выдавать предварительный диалог с количеством файлов»:

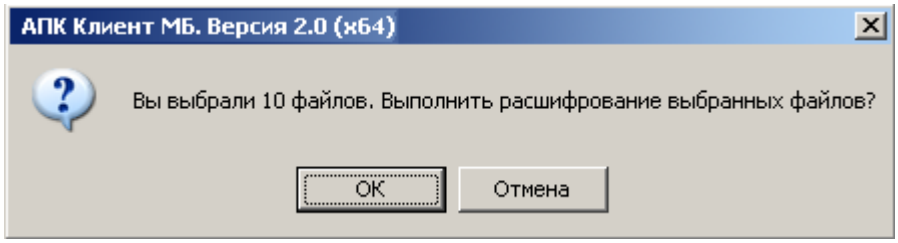

Рисунок 113 – Запрос на расшифрование

Затем на экран выдаётся диалог расшифрования файлов:

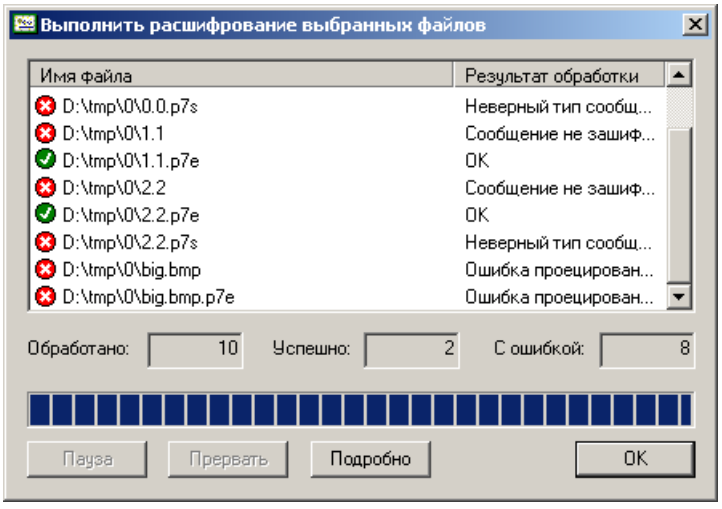

Рисунок 114 – Диалог расшифрования файлов

Во второй колонке списка выводится краткая информация о результате расшифрования. Для отображения полной информации выделите строчку с файлом и нажмите кнопку «Подробно» (или сделайте двойной клик мышью).

В процессе обработки вы можете приостановить или прервать расшифрование нажатием кнопок «Пауза» или «Прервать».

7.4.7 Получение криптографической информации

Для того чтобы получить информацию о зашифрованных или содержащих ЭП файлах, выделите в Проводнике один или несколько файлов или каталогов и выберите в главном меню расширения проводника пункт «Информация о файле». Если ранее в этом экземпляре Проводника не был загружен (или был выгружен) ключ, произойдёт загрузка ключа (см. п. 7.3).

Если операция производится с одним файлом, то для зашифрованного файла на экран будет выдан диалог с информацией о зашифрованном файле, содержащий список получателей (на кого зашифрован файл):

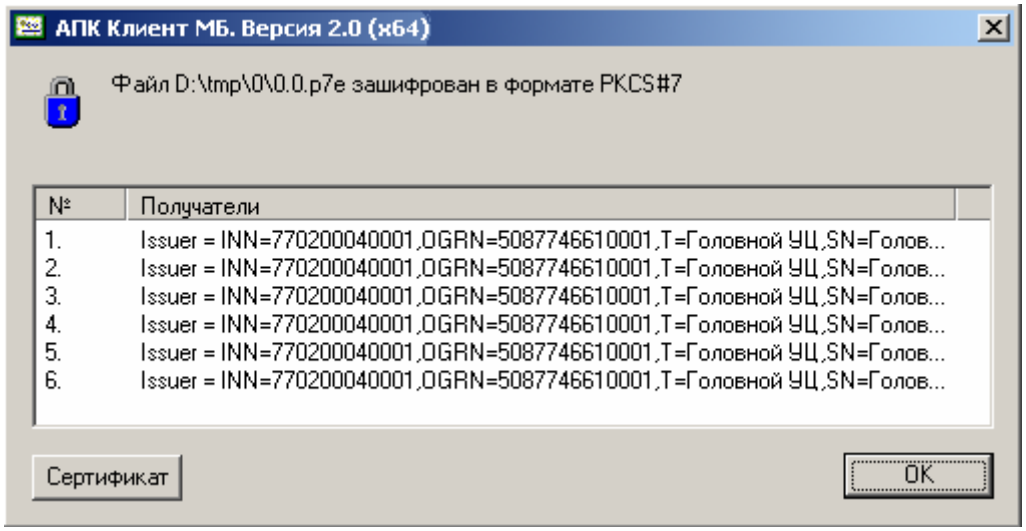

Рисунок 115 – Диалог с информацией о зашифрованном файле

Чтобы подробно просмотреть сертификат получателя, выделите его и нажмите кнопку «Сертификат» (или сделайте двойной клик мышью).

Для файла, содержащего ЭП, будет выдан диалог с информацией об ЭП:

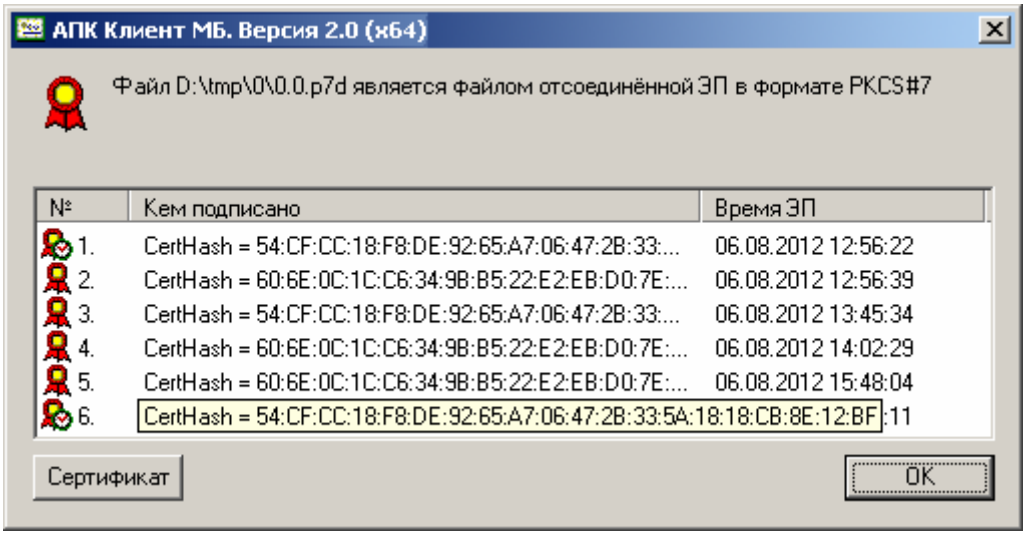

Рисунок 116 – Диалог с информацией об ЭП

В отличие от диалога с информацией о проверке подписи, здесь не отображается информация о сертификате и времени установки штампа времени, а только факт его существования: если подпись содержит штамп времени, он помечается иконкой , а если не содержит - . Чтобы подробно просмотреть сертификат, на котором выполнена подпись, выделите его и нажмите кнопку «Сертификат» (или сделайте двойной клик мышью).

Для файла, не содержащего ЭП и не зашифрованного, будет выдано сообщение:

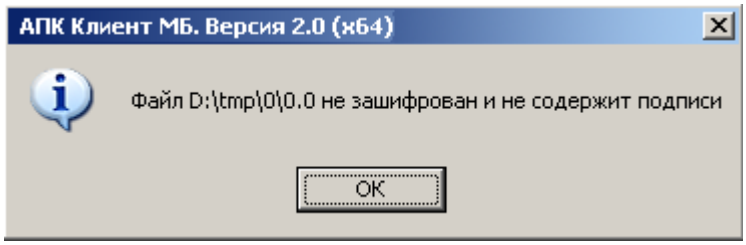

Рисунок 117 – Сообщение о незашифрованном файле, не содержащем ЭП

Если операция производится с несколькими файлами, сначала на экран выдаётся запрос на подтверждение, при условии, что в настройках пользователя не установлен режим «Не выдавать предварительный диалог с количеством файлов»:

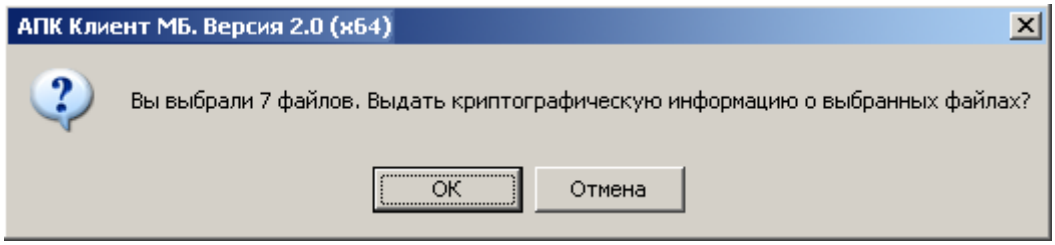

Рисунок 118 – Запрос на отображение криптографической информации о файлах

Затем на экран выдаётся диалог отображения криптографической информации о файлах:

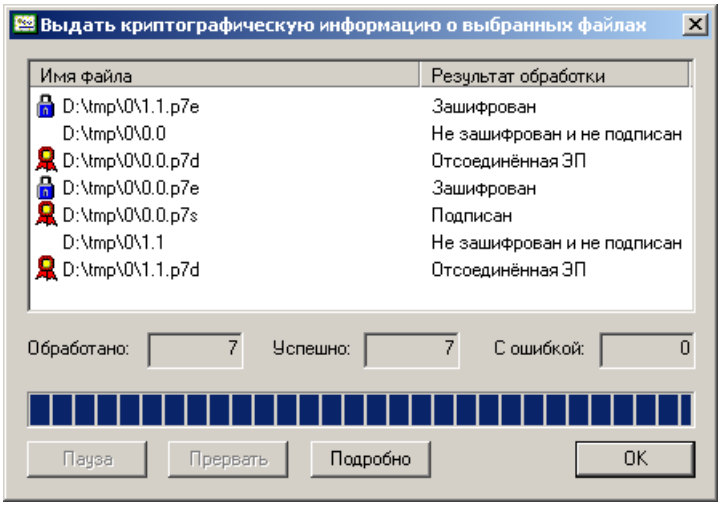

Рисунок 119 – Диалог отображения криптографической информации о файлах

Во второй колонке списка выводится краткая информация о файле. Для отображения полной информации выделите строчку с файлом и нажмите кнопку «Подробно» (или сделайте двойной клик мышью).

В процессе обработки вы можете приостановить или прервать операцию нажатием кнопок «Пауза» или «Прервать».

7.4.8 Создание отсоединённой ЭП

Для того чтобы создать отсоединённую (detached) ЭП в формате PKCS#7, выделите в Проводнике один или несколько файлов или каталогов и выберите в главном меню расширения проводника пункт «Дополнительно», подпункт «Создать отсоединённую ЭП». Если ранее в этом экземпляре Проводника не был загружен (или был выгружен) ключ, произойдёт загрузка ключа (см. п. 7.3). Файл с отсоединённой подписью сохраняется в каталог, заданный в параметре «Каталог для сохранения подписанных/ зашифрованных файлов» в настройках пользователя (или в каталог, где находится подписываемый файл, если этот параметр не задан). При этом к имени файла добавляется расширение, заданное в параметре «Основные расширения имён файлов – Файлы с отсоединённой ЭП» в настройках пользователя. В случае, когда файл уже имеет такое расширение, второй раз оно не добавляется. Если при записи подписанного файла оказывается, что файл с таким именем уже существует (за исключением случая, когда файл содержит отсоединённую ЭП), выдаётся стандартный диалог, предлагающий сохранить файл под другим (или тем же самым) именем (если в настройках пользователя не установлен режим «Не выдавать диалог сохранения файла»). Нажатие кнопки «Отмена» прекращает выполнение операции. Кроме того, будет выдан диалог подтверждения перезаписи (если в настройках пользователя не установлен режим «Перезаписывать файлы без предупреждения»):

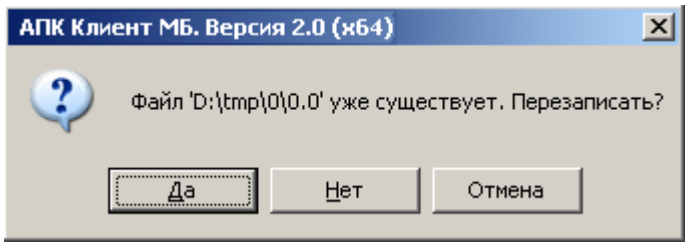

Рисунок 120 – Диалог подтверждения перезаписи файла

Нажатие кнопки «Да» приводит к выполнению операции, кнопки «Нет» - пропуску операции с текущим файлом, кнопки «Отмена» - прекращению операции со всеми оставшимися файлами.

В случае, если параметр «Каталог для сохранения подписанных/ зашифрованных файлов» в настройках пользователя не задан, при попытке создать отсоединённую ЭП для файла, имеющего расширение, заданное в параметре «Основные расширения имён файлов – Файлы с отсоединённой ЭП» в настройках пользователя, будет выдана ошибка:

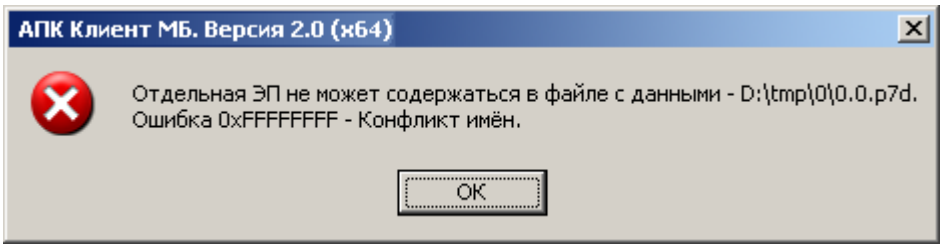

Рисунок 121 – Сообщение о конфликте имён при создании отсоединённой ЭП

В такой ситуации для создания отсоединённой ЭП необходимо изменить расширение подписываемого файла.

Перед созданием отсоединённой ЭП будет произведена проверка уже имеющихся подписей в файле с отсоединённой ЭП (если они там есть), при условии, что в настройках пользователя не установлен режим «Не проверять предыдущие подписи перед созданием ЭП». Если проверка существующих отсоединённых ЭП не была успешной, создание новой отсоединённой ЭП не происходит.

Если операция создания отсоединённой ЭП производится с одним файлом, после создания ЭП на экран выдаётся сообщение об успехе:

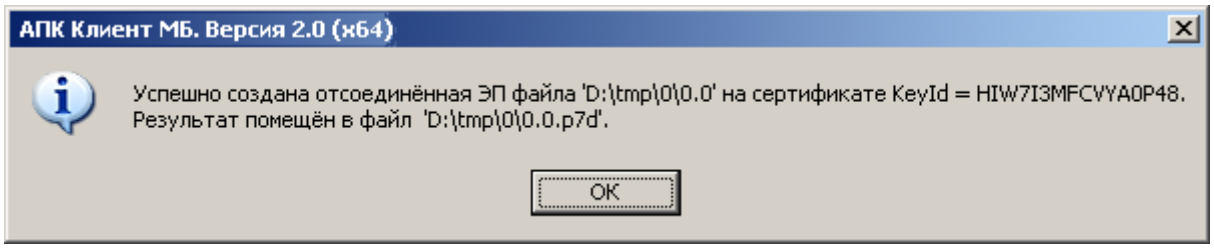

Рисунок 122 – Сообщение об успешном создании отсоединённой ЭП

или сообщение об ошибке:

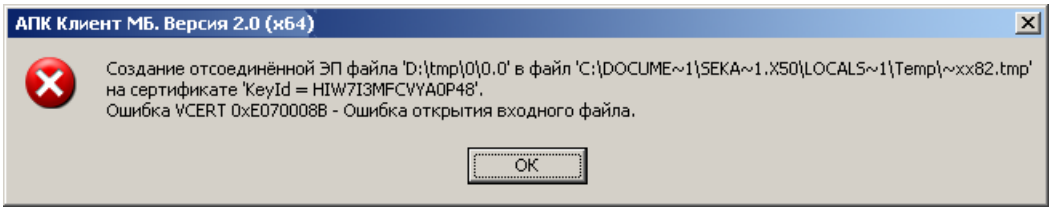

Рисунок 123 – Сообщение об ошибке при создании отсоединённой ЭП

Если в настройках пользователя установлен режим «Использовать TSP сервер» и задан адрес TSP сервера, при создании отсоединённой ЭП в неё будет добавлен штамп времени (TSP). Если при добавлении штампа времени произошла ошибка, вся операция считается неуспешной, файл с отсоединённой ЭП не создаётся.

Если операция создания отсоединённой ЭП производится с несколькими файлами, сначала на экран выдаётся запрос на подтверждение, при условии, что в настройках пользователя не установлен режим «Не выдавать предварительный диалог с количеством файлов»:

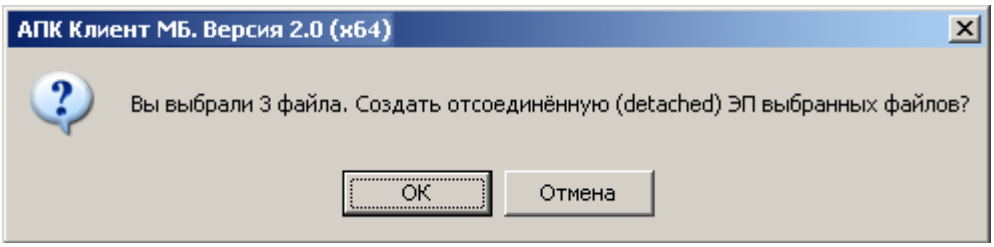

Рисунок 124 – Запрос на создание отсоединённой ЭП

Затем на экран выдаётся диалог создания отсоединённой ЭП файлов:

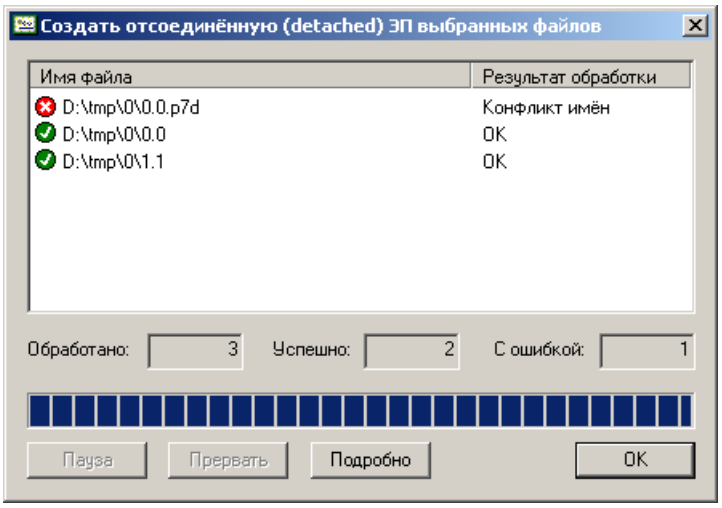

Рисунок 125 – Диалог создания отсоединённой ЭП файлов

Во второй колонке списка выводится краткая информация о результате создания отсоединённой ЭП. Для отображения полной информации выделите строчку с файлом и нажмите кнопку «Подробно» (или сделайте двойной клик мышью).

В процессе обработки вы можете приостановить или прервать создание отсоединённой ЭП нажатием кнопок «Пауза» или «Прервать».

7.4.9 Проверка отсоединённой ЭП

Для того чтобы проверить отсоединённую ЭП выделите в Проводнике один или несколько файлов или каталогов и выберите в главном меню расширения проводника пункт «Дополнительно», подпункт «Проверить отсоединённую ЭП». Если ранее в этом экземпляре Проводника не был загружен (или был выгружен) ключ, произойдёт загрузка ключа (см. п. 7.3).

Внимание: для проверки отсоединённой ЭП надо выбирать в Проводнике файлы с подписанными данными, а не файлы отсоединённых подписей. Для каждого файла с данными файл с отсоединённой подписью ищется в каталоге, заданном в параметре «Каталог для сохранения подписанных/ зашифрованных файлов» в настройках пользователя (или в каталоге, где находится подписанный файл, если этот параметр не задан). При этом к имени файла с данными добавляется расширение, заданное в параметре «Основные расширения имён файлов – Файлы с отсоединённой ЭП» в настройках пользователя (в случае, когда файл уже имеет такое расширение, второй раз оно не добавляется).

В случае, если параметр «Каталог для сохранения подписанных/ зашифрованных файлов» в настройках пользователя не задан, при попытке проверить отсоединённую ЭП для файла, имеющего расширение, заданное в параметре «Основные расширения имён файлов – Файлы с отсоединённой ЭП» в настройках пользователя, будет выдана ошибка:

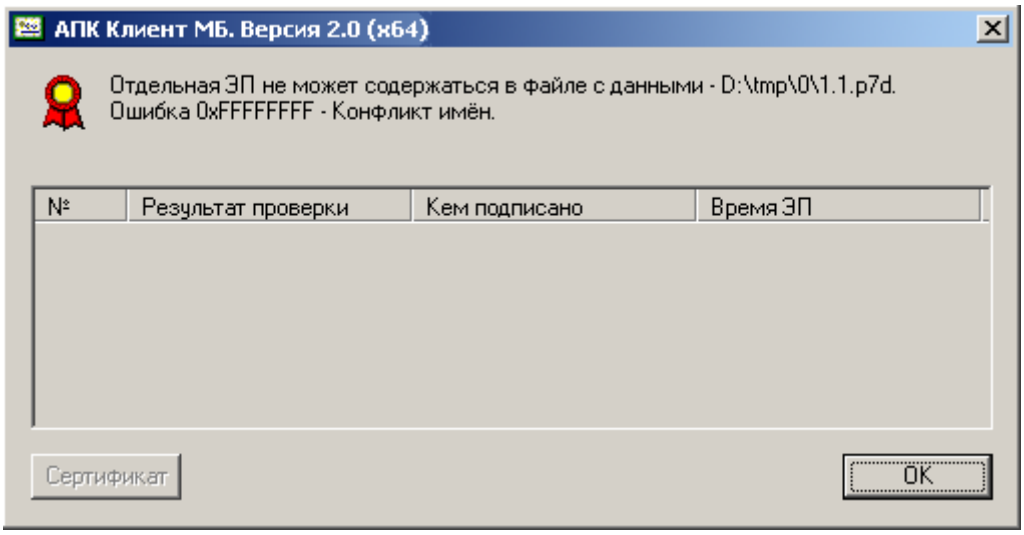

Рисунок 126 – Сообщение о конфликте имён при проверке отсоединённой ЭП

Если операция проверки отсоединённой ЭП производится с одним файлом, после проверки ЭП на экран выдаётся диалог с информацией о проверенных ЭП:

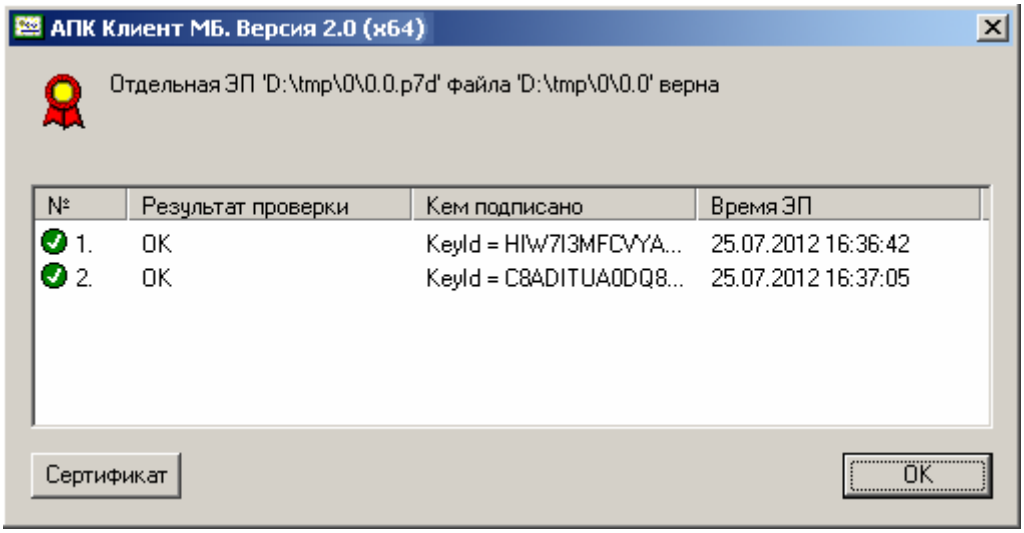

Рисунок 127 – Диалог с информацией о проверке отсоединённой ЭП

Первая колонка содержит номер ЭП и иконку – признак успешной или неуспешной проверки, вторая колонка – описание результата проверки этой подписи, третья – идентификатор сертификата, на котором создана ЭП, и четвёртая – время создания ЭП. Чтобы подробно просмотреть сертификат, выделите подпись и нажмите кнопку «Сертификат» (или сделайте двойной клик мышью):

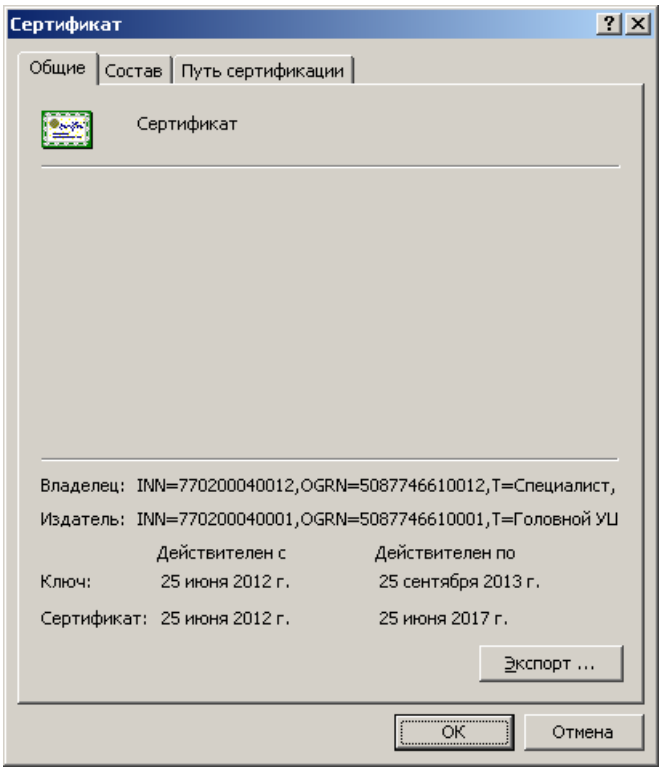

Рисунок 128 – Диалог просмотра сертификата

В случае если хоть одна подпись не была успешно проверена, результат проверки файла является отрицательным:

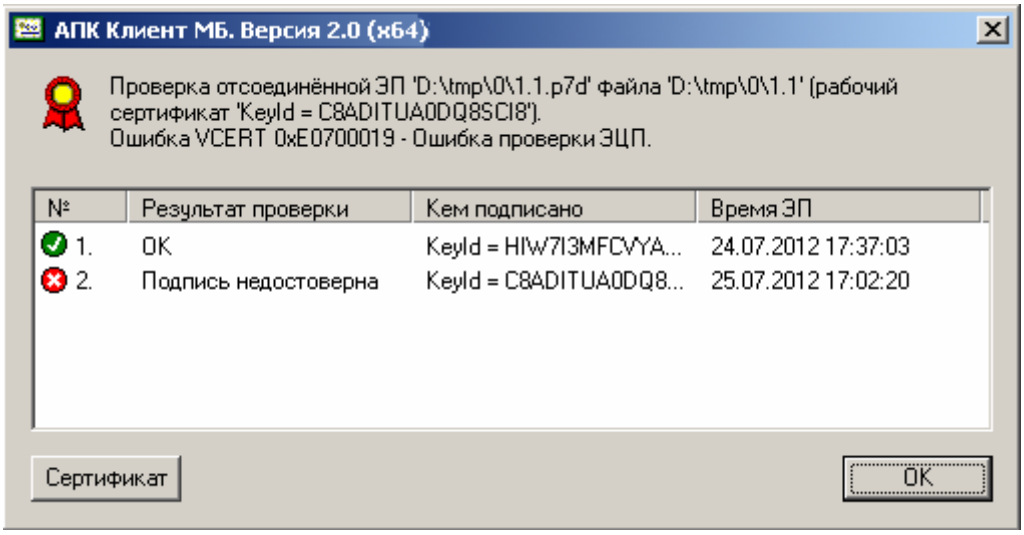

Рисунок 129 – Диалог с информацией об ошибке при проверке отсоединённой ЭП

Если в настройках пользователя установлен режим «Проверять штамп времени при проверке подписи», при проверке каждой отсоединённой ЭП производится поиск штампа времени (TSP) и его проверка (в случае обнаружения). В диалоге с информацией о проверке отсоединённой ЭП информация о проверке штампа времени ЭП содержится под строчкой, содержащей информацию о проверке этой ЭП и содержит аналогичную информацию (если в настройках пользователя не установлен режим «Отсутствие штампа времени считать ошибкой», информация об отсутствии штампа времени не выводится):

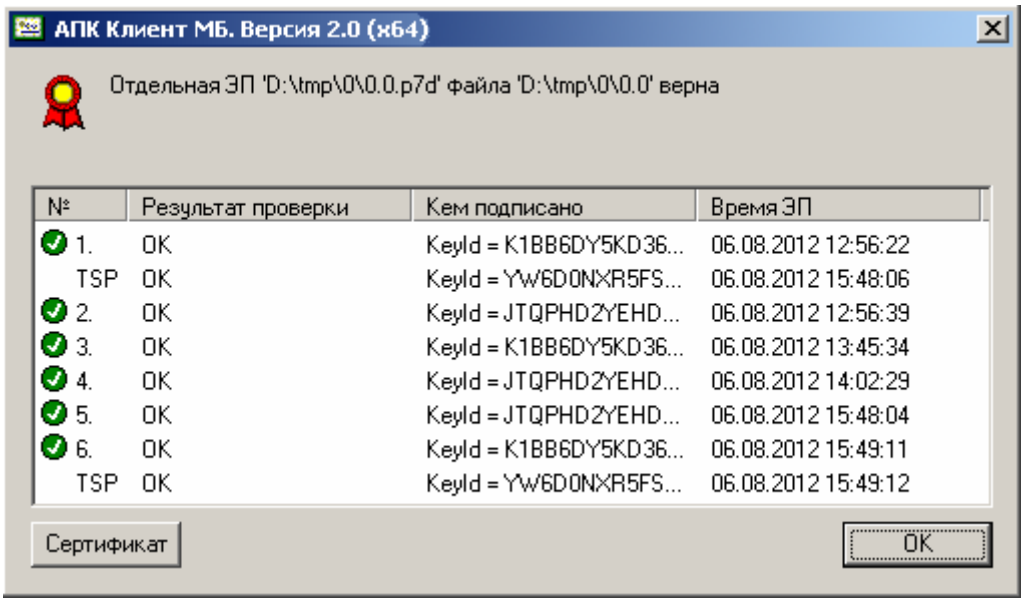

Рисунок 130 – Диалог с информацией о проверке отсоединённой ЭП со штампом времени

В случае возникновения ошибки при проверке штампа времени, проверка подписи считается неудачной. Если в настройках пользователя установлен режим «Отсутствие штампа времени считать ошибкой», отсутствующие штампы времени отображаются отдельной строкой:

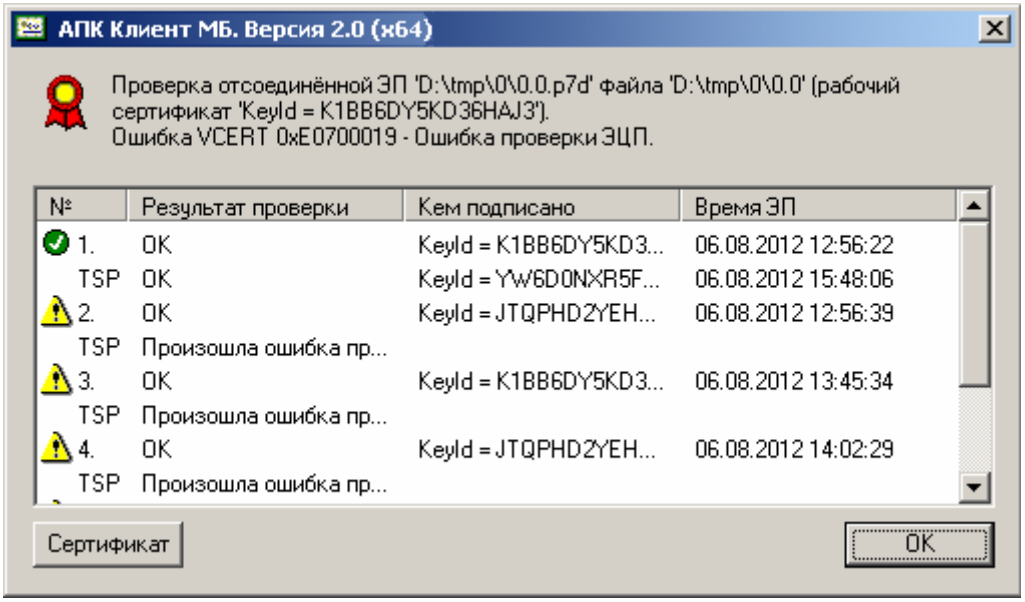

Рисунок 131 – Диалог с информацией об отсутствии штампа времени отсоединённой ЭП

Если операция проверки отсоединённой ЭП производится с несколькими файлами, сначала на экран выдаётся запрос на подтверждение, при условии, что в настройках пользователя не установлен режим «Не выдавать предварительный диалог с количеством файлов»:

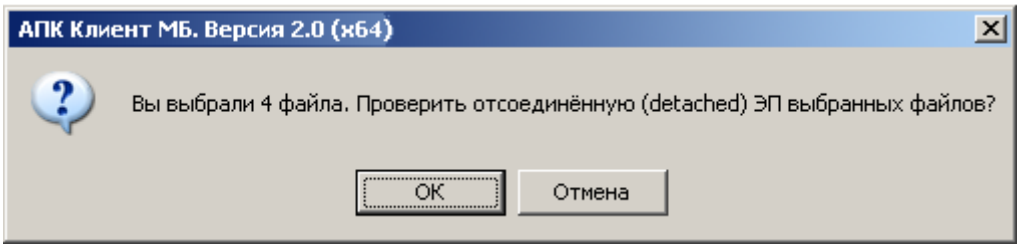

Рисунок 132 – Запрос на проверку отсоединённой ЭП

Затем на экран выдаётся диалог проверки отсоединённой ЭП файлов:

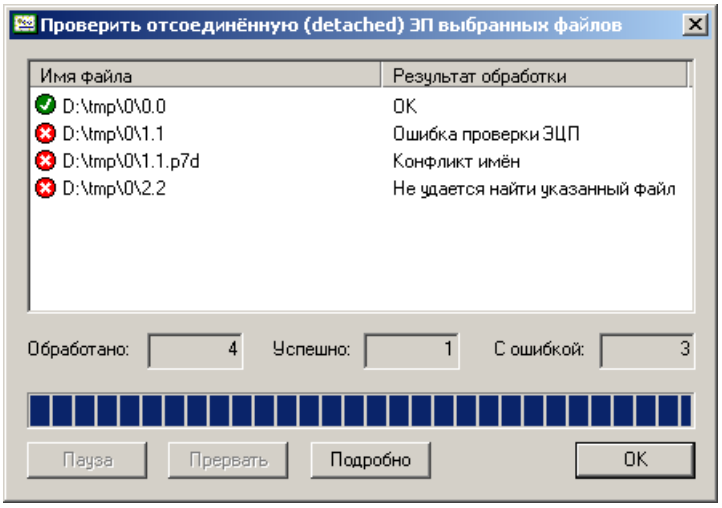

Рисунок 133 – Диалог проверки отсоединённой ЭП файлов

Во второй колонке списка выводится краткая информация о результате проверки ЭП. Для отображения полной информации выделите строчку с файлом и нажмите кнопку «Подробно» (или сделайте двойной клик мышью).

В процессе обработки вы можете приостановить или прервать проверку отсоединённой ЭП нажатием кнопок «Пауза» или «Прервать».

7.5 Закодирование в формат Base64

Для того чтобы закодировать в формат Base64, выделите в Проводнике один или несколько файлов или каталогов и выберите в главном меню расширения проводника «Дополнительно», подпункт «Закодировать в Base64». Для выполнения этой операции загрузка ключа не требуется.

Файл, полученный в результате закодирования в формат Base64, сохраняется в каталог, где находится кодируемый файл. При этом к имени файла добавляется расширение, заданное в параметре «Основные расширения имён файлов - Файлы в кодировке Base64» в настройках пользователя. В случае, когда файл уже имеет такое расширение, второй раз оно не добавляется.

Если операция закодирования в формат Base64 производится с одним файлом, после после её на экран выдаётся сообщение об успехе или сообщение об ошибке:

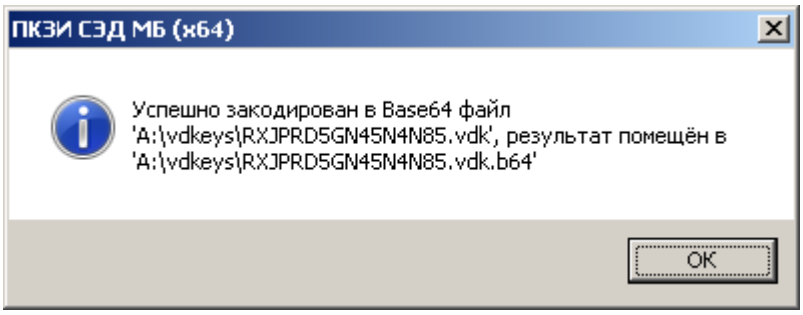

Рисунок 134 – Сообщение об успешном кодировании файла

Если операция закодирования в формат Base64 производится с несколькими файлами, сначала на экран выдаётся запрос на подтверждение при условии, что в настройках пользователя не установлен режим «Не выдавать предварительный диалог с количеством файлов»:

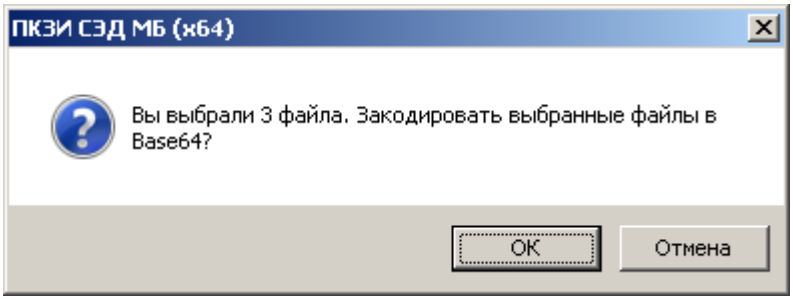

Рисунок 135 – Запрос на закодирование в формат Base64

Затем на экран выдаётся диалог закодирования в формат Base64:

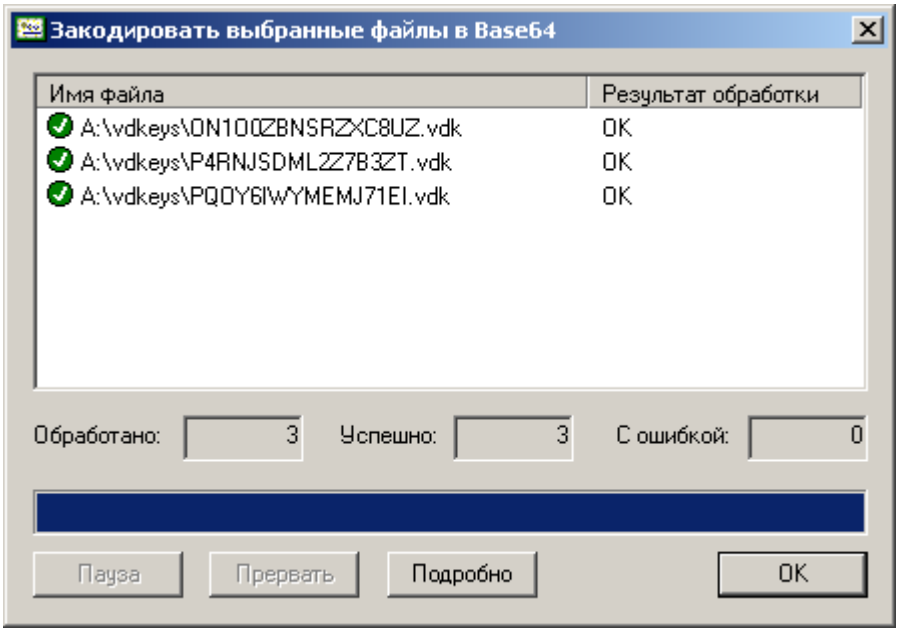

Рисунок 136 – Диалог закодирования в формат Base64

Во второй колонке списка выводится краткая информация о результате операции. Для отображения полной информации выделите строчку с файлом и нажмите кнопку «Подробно» (или сделайте двойной клик мышью).

В процессе обработки вы можете приостановить или прервать выполнение операции нажатием кнопок «Пауза» или «Прервать».

7.6 Раскодирование из формата Base64

Для того чтобы раскодировать из формата Base64, выделите в Проводнике один или несколько файлов или каталогов и выберите в главном меню расширения проводника «Дополнительно», подпункт «Раскодировать из Base64». Для выполнения этой операции загрузка ключа не требуется.

Файл, полученный в результате раскодирования из формата Base64, сохраняется в каталог, где находится закодированный файл. При этом, если файл имеет расширение, заданное в параметре «Основные расширения имён файлов - Файлы в кодировке Base64». В случае, когда файл не имеет такого расширения, имя файла не меняется.

Если при записи раскодированного файла оказывается, что файл с таким именем уже существует, выдаётся стандартный диалог, предлагающий сохранить файл под другим (или тем же самым) именем (если в настройках пользователя не установлен режим «Не выдавать диалог сохранения файла»). Нажатие кнопки «Отмена» прекращает выполнение операции. Кроме того, будет выдан диалог подтверждения перезаписи (если в настройках пользователя не установлен режим «Перезаписывать файлы без предупреждения»).

Нажатие кнопки «Да» приводит к выполнению операции, кнопки «Нет» - пропуску операции с текущим файлом, кнопки «Отмена» - прекращению операции со всеми оставшимися файлами.

Если операция раскодирования из формата Base64 производится с одним файлом, после неё на экран выдаётся сообщение об успехе или сообщение об ошибке:

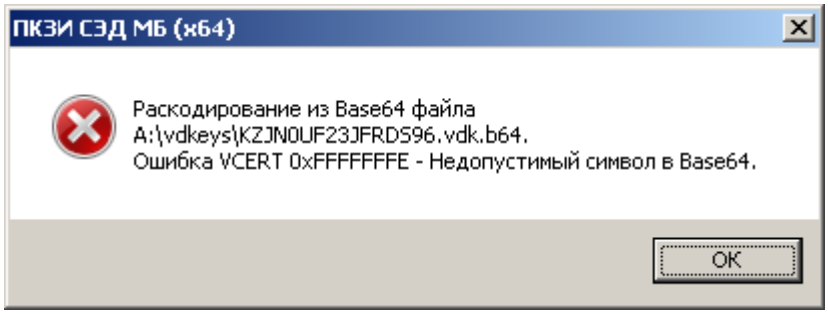

Рисунок 137 – Сообщение об ошибке при раскодировании файла

Если операция раскодирования из формата Base64 производится с несколькими файлами, сначала на экран выдаётся запрос на подтверждение при условии, что в настройках пользователя не установлен режим «Не выдавать предварительный диалог с количеством файлов»:

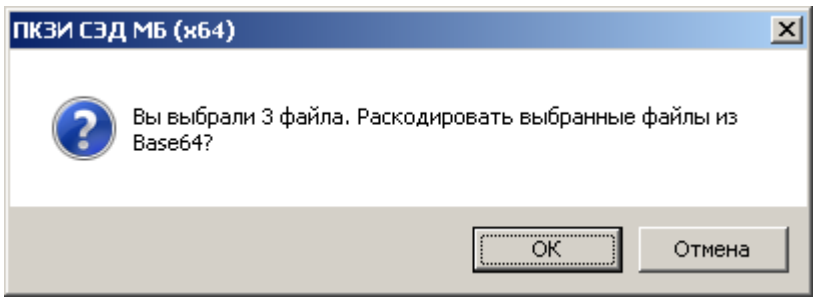

Рисунок 138 – Запрос на раскодирование из формата Base64

Затем на экран выдаётся диалог раскодирования из формата Base64:

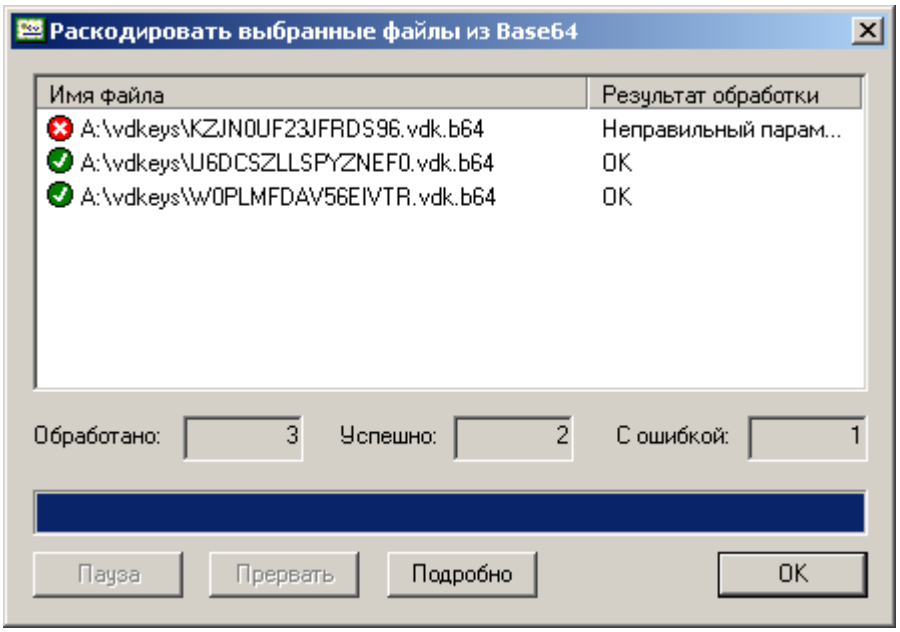

Рисунок 139 – Диалог раскодирования из формата Base64

Во второй колонке списка выводится краткая информация о результате операции. Для отображения полной информации выделите строчку с файлом и нажмите кнопку «Подробно» (или сделайте двойной клик мышью).

В процессе обработки вы можете приостановить или прервать выполнение операции нажатием кнопок «Пауза» или «Прервать».

7.7 Хэширование файлов

Для того чтобы вычислить хэш по ГОСТ 34.11-2012 (256 бит), выделите в Проводнике один или несколько файлов или каталогов и выберите в главном меню расширения проводника «Дополнительно», подпункт «Вычислить хэш». Для выполнения этой операции загрузка ключа не требуется.

Если операция хэширования производится с одним файлом, на экран выдаётся диалоговое окно с результатом или сообщение об ошибке:

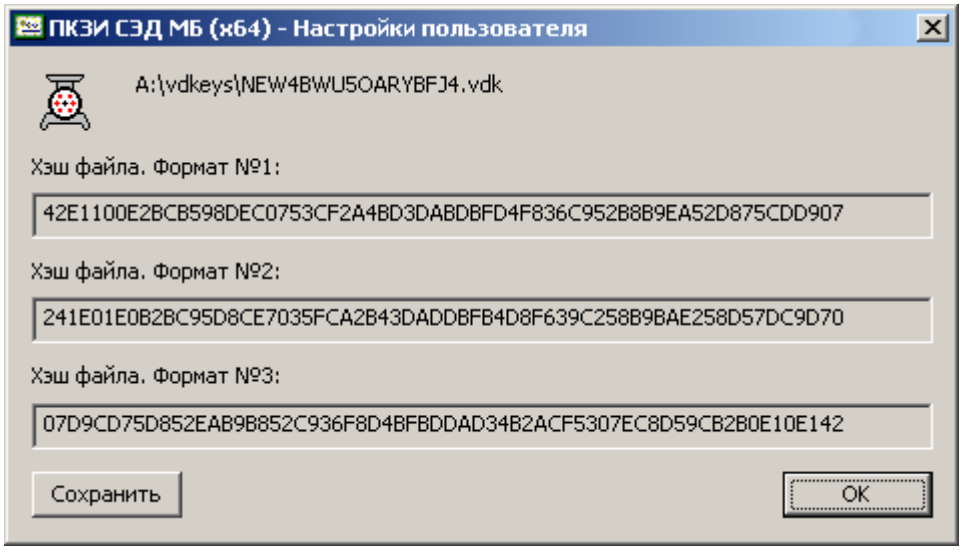

Рисунок 140 – Диалог с результатом хэширования

Хэш представлен в трёх форматах. Формат 1 является простым побайтовым шестнадцатиричным представлением. Формат 2 отличается от него только порядком полубайт (ниббллов) в байте и отображается для

совместимости с другими средствами хэширования. Формат 3 отличается от Формата 1 обратным порядком байт и соответствует требованиям ГОСТ 34.11-2012.

Для сохранения вычисленного значения хэша в файл нажмите кнопку «Сохранить» и укажите имя файла в стандартном диалоге сохранения.

Если операция хэширования производится с несколькими файлами, сначала на экран выдаётся запрос на подтверждение при условии, что в настройках пользователя не установлен режим «Не выдавать предварительный диалог с количеством файлов»:

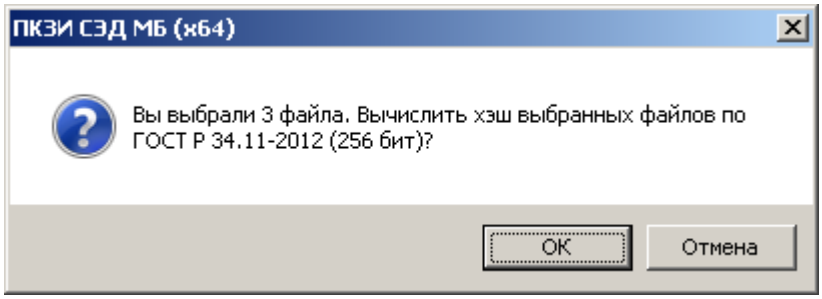

Рисунок 141 – Запрос на хэширование

Затем на экран выдаётся диалог вычисления хэша:

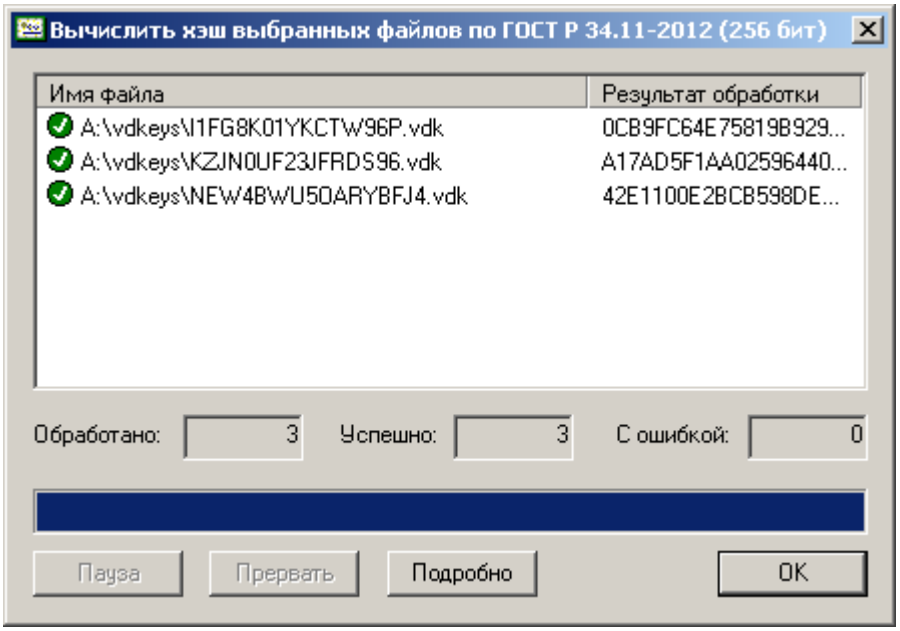

Рисунок 142 – Диалог вычисления хэша

Во второй колонке списка выводится результат операции. Для отображения полной информации выделите строчку с файлом и нажмите кнопку «Подробно» (или сделайте двойной клик мышью).

В процессе обработки вы можете приостановить или прервать выполнение операции нажатием кнопок «Пауза» или «Прервать».

7.8 Протоколирование в расширении проводника

В случае, если в настройках пользователя не включён режим «Отключить протокол выполненных операций», расширение проводника протоколирует в журнал приложений (Event Log) Windows все криптографические операции и все ошибки, возникшие в процессе их выполнения. В качестве кода события всегда указывается 1, источника события – xPKISHXX, а категория отсутствует. В описании события указывается программный модуль (xpkishxx.dll), идентификаторы процесса и потока и текстовое описание события или ошибки, совпадающее с сообщениями, выдаваемыми в экранных диалогах (однако длинные сообщения обрезаются до длины

16 Кб). В случае, если в настройках включён режим «Расширенная диагностика криптографических ошибок (стек)», текстовое описание может содержать стек ошибок.

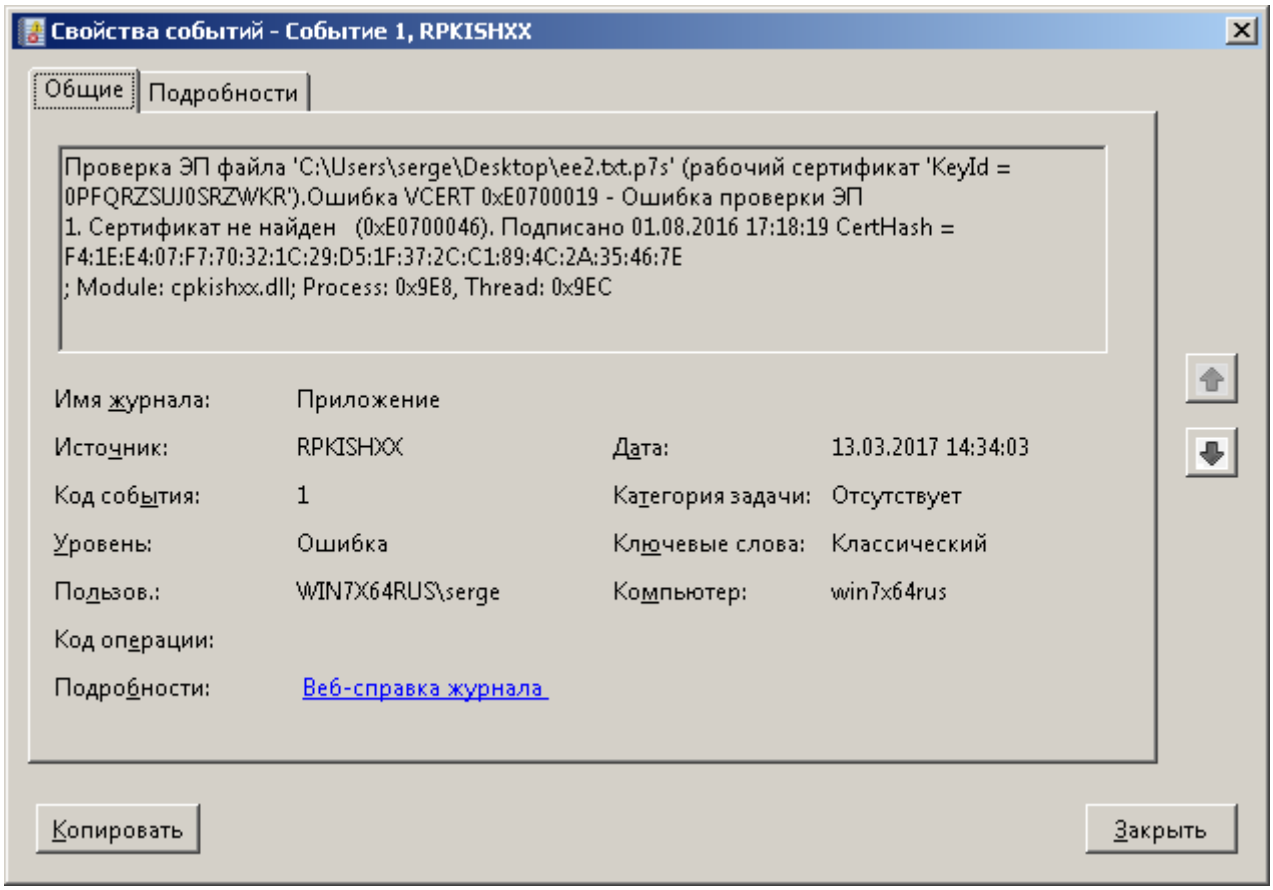

Рисунок 143 – Описание ошибки проверки подписи без стека ошибок

Такое же сообщение, но при включённом режиме «Расширенная диагностика криптографических ошибок (стек)» будет выглядеть так:

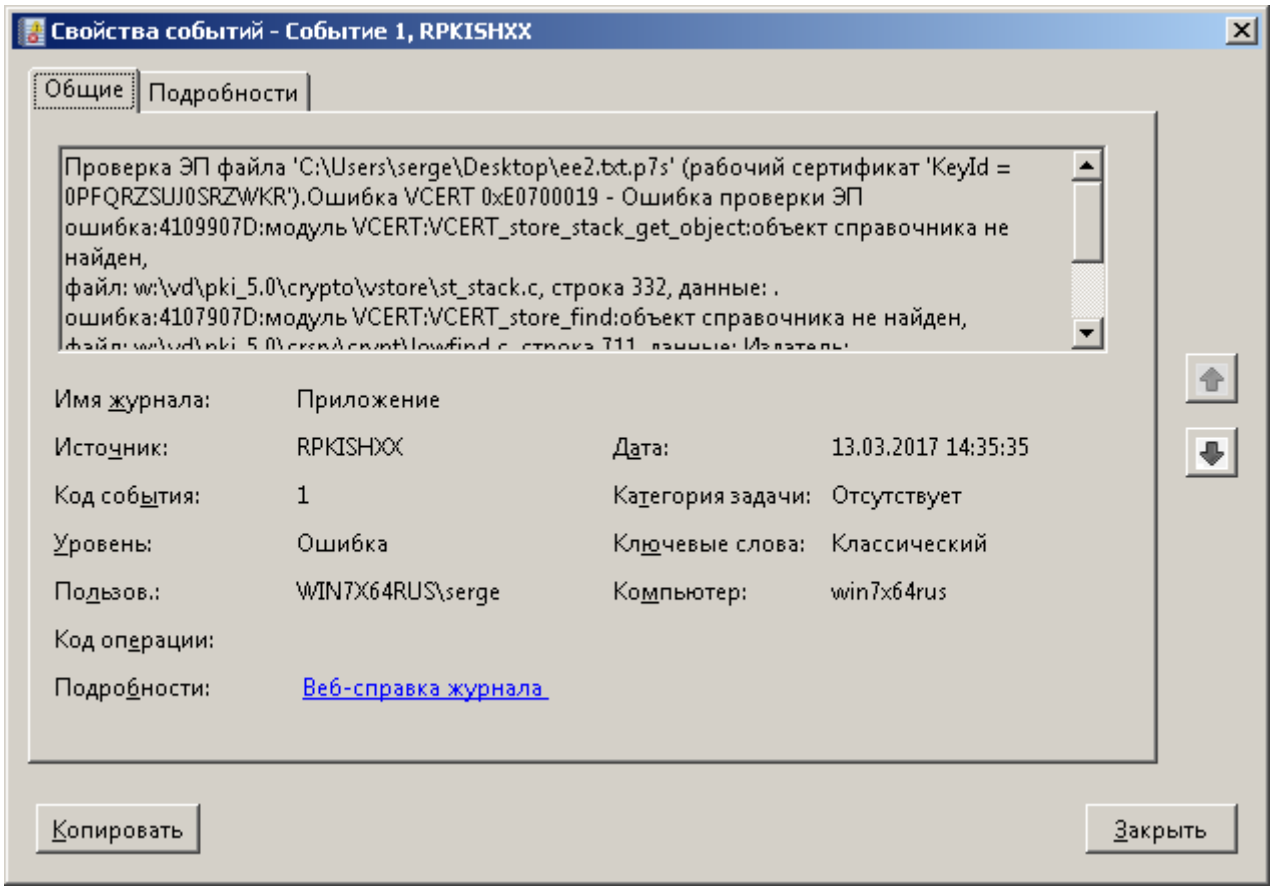

Рисунок 144 – Описание ошибки проверки подписи со стеком ошибок

8 ССЫЛКИ

ВАМБ.00074-02 31 01	ВАМБ.00074-02 31 01 «АПК «УЦ МБ» версия 2.0. Описание применения»
ВАМБ.00074-02 91 01	ВАМБ.00074-02 91 01 «АПК «УЦ МБ» версия 2.0. Программный комплекс «Центр Сертификации». Руководство по установке и настройке»
ВАМБ.00060-05 34 02	ВАМБ.00060-05 34 02 «Провайдер криптографического сервиса «Валидата CSP» версия 5.0». Руководство пользователя

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			