УТВЕРЖДЕН

РБ.СЮИК.00364-03 34 01-ЛУ

ПОДСИСТЕМА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

КОМПЛЕКС ПРОГРАММНЫЙ

СРЕДСТВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Руководство оператора

РБ.СЮИК.00364-03 34 01

Листов 187

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

2016

№ изм.	Подп.	Дата

Литера

АННОТАЦИЯ

Настоящий документ предназначен для пользователей, имеющих навыки работы с приложениями в операционных системах Microsoft Windows™.

Документ содержит сведения, необходимые пользователю для применения «Подсистемы криптографической защиты информации. Комплекса программного Средств обеспечения безопасности» РБ.СЮИК.00364-03 (далее – КП СОБ), описание характеристик программы ее назначение, условия применения, входные и выходные параметры, коды возврата и способы настройки программы на различные режимы работы

КП СОБ и входящие в его состав компоненты позволяют выполнять следующие криптографические операции над данными, размещенными в файлах, полный путь к которым передается во входных параметрах:

- управления доступом пользователей к подсистеме криптографической защиты информации (далее – ПС КЗИ);
- шифрование, вычисление значения функции хэширования, выработка имитовставки и преобразование ключа согласно СТБ 34.101.31 (Belt):
    1) Belt-шифрование в режиме простой замены с 256-битным ключом (belt-ecb256 = «1.2.112.0.2.0.34.101.31.13»);
    2) Belt-шифрование в режиме сцепления блоков с 256-битным ключом (belt-cbc256 = «1.2.112.0.2.0.34.101.31.23»);
    3) Belt-шифрование в режиме гаммирования с обратной связью с 256-битным ключом (belt-cfb256 = «1.2.112.0.2.0.34.101.31.33»);
    4) Belt-шифрование в режиме счётчика с 256-битным ключом (belt-ctr256 = «1.2.112.0.2.0.34.101.31.43»);
    5) Belt-алгоритм выработки имитовставки на 256-битном ключе (belt-mac256 = «1.2.112.0.2.0.34.101.31.53»);
    6) Belt-алгоритм одновременного шифрования и имитозащиты данных на 256-битном ключе (belt-datawrap256 = «1.2.112.0.2.0.34.101.31.63»);
    7) Belt-алгоритм одновременного шифрования и имитозащиты ключа на 256-битном ключе (belt-keywrap256 = «1.2.112.0.2.0.34.101.31.73»);
    8) Belt-хэширование (belt-hash256 = «1.2.112.0.2.0.34.101.31.81»);
- выработка имитовставки и генерация псевдослучайных чисел согласно СТБ 34.101.47 (Brng):
    1) выработка имитовставки по алгоритму HMAC с функцией хэширования

СТБ 34.101.31 (hmac-hbelt = «1.2.112.0.2.0.34.101.47.12»);

2) генерация псевдослучайных чисел в режиме счётчика с функцией хэширования СТБ 34.101.31 (brng-ctr-hbelt = «1.2.112.0.2.0.34.101.47.22»);

– выработка и проверка электронной цифровой подписи (ЭЦП), генерация и проверка параметров эллиптической кривой, генерация пары ключей и транспорта ключа согласно СТБ 34.101.45 (Bign):

1) алгоритм ЭЦП с функцией хэширования, определяемой долговременными параметрами (bign-with-hspec = «1.2.112.0.2.0.34.101.45.11»);
2) алгоритм ЭЦП с функцией хэширования СТБ 34.101.31 (bign-with-hbelt = «1.2.112.0.2.0.34.101.45.12»);
3) алгоритм проверки параметров эллиптической кривой (bign-valec = «1.2.112.0.2.0.34.101.45.22»);
4) алгоритм генерации пары ключей (bign-genkeypair = «1.2.112.0.2.0.34.101.45.31»);
5) алгоритм транспорта ключа (bign-keytransport = «1.2.112.0.2.0.34.101.45.41»);

– выработка общих ключей по протоколам формирования общих ключей согласно СТБ 34.101.66 (Bake):

1) протокол формирования общего ключа на эллиптических кривых BMQV (bake-bmqv = «1.2.112.0.2.0.34.101.66.11»);
2) протокол формирования общего ключа на эллиптических кривых BSTS (bake-bsts = «1.2.112.0.2.0.34.101.66.12»);
3) протокол формирования общего ключа на эллиптических кривых BPACE (bake-bpace = «1.2.112.0.2.0.34.101.66.21»);

– шифрование данных и выработка имитовставки согласно ГОСТ 28147-89 (на 256-битном ключе):

1) шифрование в режиме простой замены (gost28147-ecb = «1.2.112.0.2.1.28147.11»);
2) шифрование в режиме гаммирования с обратной связью (gost28147-cfb = «1.2.112.0.2.1.28147.12»);
3) шифрование в режиме гаммирования (gost28147-ctr = «1.2.112.0.2.1.28147.13»);
4) выработка имитовставки (gost28147-mac = «1.2.112.0.2.1.28147.14»);

– вычисление значения функции хэширования с задаваемым начальным вектором согласно СТБ 1176.1 (stb11761-hash = «1.2.112.0.2.0.1176.1.11»);

– выработка и проверка ЭЦП согласно СТБ 1176.2:
    1) алгоритм ЭЦП под данными (stb11762-sign = «1.2.112.0.2.0.1176.2.11»);
    2) алгоритм ЭЦП под хэш-значением от данных, полученным с помощью алгоритма СТБ 34.101.31 (stb11762pre-sign = «1.2.112.0.2.0.1176.2.12»);
– выработка общих ключей по протоколам формирования общих ключей согласно РД РБ «Банковские технологии. Протоколы формирования общего ключа»:
    1) протокол без аутентификации сторон (bdh-noauth = «1.2.112.0.2.0.1176.2.31»);
    2) протокол с аутентификацией сторон (bdh-auth = «1.2.112.0.2.0.1176.2.32»);
    3) односторонний протокол (bdh-oneside = «1.2.112.0.2.0.1176.2.33»);
– разделение и восстановление секрета (ключа) между пользователями, генерацию параметров, необходимых при разделении и восстановлении секрета в соответствии с СТБ 34.101.60.

Все криптографические операции выполняются с использованием сертификатов открытых ключей.

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ ПРОГРАММЫ

КП СОБ предназначен для организации работы конечных пользователей и поддерживает следующие роли операторов:

– «Администратор» (Role.Admin);

– «Пользователь» (Role.User);

– «Гость» (Role.Guest).

Роль «Администратор» должна выполняться оператором, наделенным правами выполнять сервисы, доступные роли «Пользователь» и обладающим правами администратора ОС. В обязанности «Администратора» входит инсталляция КП СОБ на ПЭВМ, настройка среды функционирования, первичный запуск и тестирование КП СОБ.

Роль «Пользователь» выполняет оператор КП СОБ имеющий уникально поименованный криптоконтейнер на НКИ с личным ключом, а также СОК, содержащий парный ему открытый ключ. В роли «Пользователь» для выполнения криптографических операций необходимо предъявление пароля для доступа к криптоконтейнеру на НКИ. Роли «Пользователь» доступны все сервисы.

Роль «Гость» доступна оператору, не имеющему уникально поименованного криптоконтейнера на НКИ с личным ключом. «Гостю» доступны операции самотестирования, получения номера версии, запроса СОК и СОС, формирования запроса на выпуск СОК, просмотр локального хранилища.

КП СОБ обеспечивает реализацию функций:

1) отображения номера версии (номера релиза) программных модулей КП СОБ;

2) идентификации и аутентификации пользователя;

3) управления авторизированным доступом к ресурсам носителя;

4) выполнения криптографических преобразований и использования ключевой информации для следующих целей:

а) шифрование в соответствии с алгоритмами, определенными в ГОСТ 28147 и СТБ 34.101.31;

б) выработка имитовставки в соответствии с алгоритмами, определенными в ГОСТ 28147, СТБ 34.101.31 и СТБ 34.101.47;

в) хэширование в соответствии с алгоритмами, определенными в СТБ 1176.1 и СТБ 34.101.31;

г) генерация пар ключей электронной цифровой подписи (ЭЦП) в соответствии с алгоритмами, определенными в СТБ 1176.2, СТБ 34.101.45;

д) выработка и проверка ЭЦП в соответствии с алгоритмами, определенными в СТБ 1176.2, СТБ 34.101.45;

е) выработка общего секретного ключа шифрования в соответствии с алгоритмами, определенными в СТБ 34.101.66 и РД РБ «Банковские технологии. Протоколы формирования общего ключа»;

ж) генерация псевдослучайных данных с секретным параметром в соответствии с алгоритмами, определенными в СТБ 34.101.47;

и) разделение и восстановление секрета согласно СТБ 34.101.60;

к) поддержка протокола защиты транспортного уровня (протокол TLS), согласно СТБ 34.101.65;

5) формирования запроса на выпуск новых сертификатов открытых ключей (СОК) в соответствии с СТБ 34.101.17;

6) формирования запроса на отзыв (приостановку действия) СОК;

7) формирования запроса на выдачу существующего СОК;

8) формирования OCSP запроса о статусе СОК по СТБ 34.101.26;

9) формирования карточки открытого ключа в соответствии с СТБ 34.101.49;

10) обработки СОК и СОС, удовлетворяющих требованиям СТБ 34.101.19;

11) доступа к журналу аудита;

12) архивного копирования и восстановления данных после сбоя системы;

13) изменения параметров безопасности системы;

14) выполнения процедуры самотестирования.

Скорость выполнения криптографических операций зависит от производительности ПЭВМ.

КП СОБ устанавливается на ПЭВМ, работающей в операционной системе Microsoft Windows™ XP (x86), Server 2003 (x86), 7 (x86, x64), 10.

Для работы КП СОБ необходима ПЭВМ, имеющая эксплуатационные параметры не хуже, чем:

- процессор совместимый с Intel Pentium с тактовой частотой 900 МГц;
- оперативное запоминающее устройство (ОЗУ) с объемом памяти 256 Мбайт;
- накопитель на жестких магнитных дисках (НЖМД) с объемом свободного адресного пространства 10 Гбайт,

а также следующие аппаратные средства:

- средство подключения ПЭВМ к сети передачи данных (сетевая карта или модем);
- источник бесперебойного питания.

Минимальный состав программных средств, необходимых для функционирования КП СОБ включает в себя:

- любую из ОС Microsoft Windows™ XP (x86), Server 2003 (x86), 7 (x86, x64), 10;
- файловую систему FAT12, FAT16, FAT32, NTFS;
- текстовый редактор Angel Writer, установленный в рабочую директорию КП СОБ;
- установленную СУБД Firebird.

Для функционирования КП СОБ необходимо наличие почтового ящика, зарегистрированного на используемом почтовом сервере При работе с электронной почтой необходимо определить следующие элементы:

- адреса TCP/IP;
- номера портов ввода/вывода;
- имя почтового ящика;
- пароль доступа к почтовому ящику.

Внимание: Для обеспечения выполнения функций КП СОБ необходимо загрузить корневой СОК в соответствии с п. 6.6. Без загруженного корневого СОК работа КП СОБ невозможна.

2. ХАРАКТЕРИСТИКИ ПРОГРАММЫ

2.1 КП СОБ написан в средах разработки Visual Studio .NET 2003, Visual Studio 2008, Visual Studio 2013 на языках Ассемблер, C и C++ с использованием MFC.

2.2 КП СОБ обеспечивает выполнение операции проверки подписи по СТБ 34.101.45 за время, не превышающее 50 мс и по СТБ 1176.2 за время, не превышающее 60 мс, при условии, что сертификат открытого ключа находится в хранилище КП СОБ.

2.3 Количество сертификатов, хранимых в локальном хранилище не менее 128 тыс.

2.4 Время доступа к сертификату, находящемуся в хранилище не превышает 10 мс.

3. УСТАНОВКА ПРОГРАММЫ

3.1 Установка программы производится оператором в роли «Администратор».

3.2 Установка программы производится копированием рабочей директории КП СОБ (папки с именем «CryptoService») с поставляемого производителем диска на жесткий диск.

3.3 Установка программы завершается созданием на жестком диске папки «CryptoService», содержащей следующий набор папок, необходимых для работы программы. Перечень папок представлен в таблице 1.

Таблица 1 – Перечень папок, необходимых для корректной работы программы

Наименование папки	Наименование папки, входящей в исходную папку	Описание применения
CertificateStorage	ForCertificatesLoading	Папка для пользователей. В данную папку помещаются СОК, которые впоследствии загружаются во внутреннее локальное хранилище.
	ForCRLsLoading	Папка для пользователей. В данную папку помещаются СОС, которые впоследствии обрабатываются КП СОБ.
	CertificateOriginals	Папка для внутреннего использования. В данной папке содержатся СОК, подгруженные в локальное хранилище, и разобранные СОК в виде xml-файла.
DebugLogging	–	Папка для внутреннего использования. Если включен режим отладки, тогда в данную папку сохраняются все запросы и ответы.
PrivateKeys	–	Папка для внутреннего использования. В данной папке по умолчанию сохраняются личные ключи.

Окончание таблицы 1

Наименование папки	Наименование папки, входящей в исходную папку	Описание применения
PublicKeyCards	–	Папка для внутреннего использования. По умолчанию в данную папку сохраняются карточки открытого ключа.
	Templates	Папка для внутреннего использования. В данной папке находятся шаблоны для выпуска карточек открытого ключа.
ReferenceBooks	–	Папка для внутреннего использования. Справочная информация для формирования заявок на выпуск СОК (название городов, улиц и т.д.)
Requests	–	Папка для внутреннего использования. В данной папке содержатся файлы запросов к КПА УЦ или КП РЦ.
Responses	–	Папка для внутреннего использования. В данной папке содержатся файлы ответов от КПА УЦ или КП РЦ. После анализа ответов файлы могут быть удалены.
ShareSecret	–	Папка для внутреннего использования. В данной папке размещается приложение для разделения и восстановления секретов.
	PrivateSecrets	Папка для внутреннего использования. В данную папку по умолчанию сохраняются вычисленные частичные секреты и восстановленные общие секреты.
PrivateKeysManager	–	Папка для внутреннего использования. В данной папке размещается приложение для управления личными ключами, которое работает с различными носителями ключевой информации.

Примечания:

1. В папке CertificateStorage находится файл внутреннего локального хранилища СОК CertificateStorage.v10.
2. В папке CertificateStorage должен находиться файл долговременных параметров StdLTPs.ber.
3. В папке ReferenceBooks должен находиться файл объектных идентификаторов Object Identifiers.xml.
4. Личные ключи могут храниться в любом удобном для пользователя месте на НКИ.

3.4 Типы файлов, создаваемых при работе КП СОБ, представлены в таблице 2.

Таблица 2 – Типы файлов, создаваемых при работе КП

Расширение файла	Тип файла
.log, .txt	файл журнала аудита
.v10	файл внутреннего локального хранилища СОК
.rbf, .pri	файлы справочников и политик
.der, .iap	файлы заявок на выпуск СОК
.der, .sap, .rap	файлы заявок на приостановку и отзыв СОК
.cer	файлы СОК
.eml	файлы почтовых сообщений
.rtf, .xml	файлы карточек открытых ключей

3.5 Структуры файлов различных типов, создаваемых при работе КП СОБ, представлены в приложении 1.

3.6 Для корректной работы КП СОБ могут понадобиться некоторые из нижеперечисленных системных библиотек, которые необходимо скопировать с поставляемого производителем диска из папки «Вспомогательное окружение\system_dlls» в системную папку system32 по пути C:\WINDOWS\system32:

– mfc71.dll;
– mfc71d.dll;
– mfc100.dll;
– mfc100d.dll;
– mfc120.dll;
– mfc120d.dll;
– mfc140.dll;
– mfc140d.dll;
– msvcp71.dll;
– msvcp71d.dll;
– msvcp100.dll;
– msvcp100d.dll;
– msvcp120.dll;
– msvcp120d.dll;
– msvcp140.dll;
– msvcp140d.dll;
– msvcr71.dll;
– msvcr71d.dll;
– msvcr100.dll;
– msvcr100d.dll;
– msvcr120.dll;
– msvcr120d.dll;
– libeay32.dll (23.03.2007);
– ssleay32.dll (23.03.2007);
– vsinit.dll (15.12.2003).

3.7 Для корректного просмотра или редактирования карточки открытого ключа может понадобиться текстовый редактор Angel Writer. Его установка производится копированием папки «Angel Writer» с поставляемого производителем диска из папки «Вспомогательное окружение» в папку «CryptoService» на жестком диске ПЭВМ.

4. НАСТРОЙКА СРЕДЫ

Настройкой среды занимается оператор в роли «Администратор».

Если используется операционная система Microsoft Windows™ XP или Microsoft Windows™ Server 2003, то Администратор должен создать учетную запись пользователя ОС. В случае, когда используется операционная система Microsoft Windows™ 7 или Microsoft Windows™ 10, то необходимо включить встроенную учетную запись администратора. Далее произвести инсталляцию и настройку КП СОБ, ограничить доступ к файлу настроек и файлу журнала для учетной записи пользователя, произвести первоначальный запуск КП СОБ в учетной записи пользователя от своего имени, т.о. разрешая работу оператору в роли Пользователь и Гость. На момент установки ограничений доступа файл настроек и файл журнала должны существовать.

Настройка среды производится следующим образом:

1. Настроить соответствующую учетную запись:

– для операционной системы Microsoft Windows™ XP:

а) создать учетную запись пользователя (Пуск – Панель управления – Учетные записи пользователей – Создание учетной записи);

б) под учетной записью, имеющей права администратора, открыть окно программы Проводник, после чего выбрать меню Сервис – Свойства папки. Затем на вкладке «Вид» снять флажок «Использовать простой общий доступ к файлам (рекомендуется)» и сохранить изменения (рис. 1).

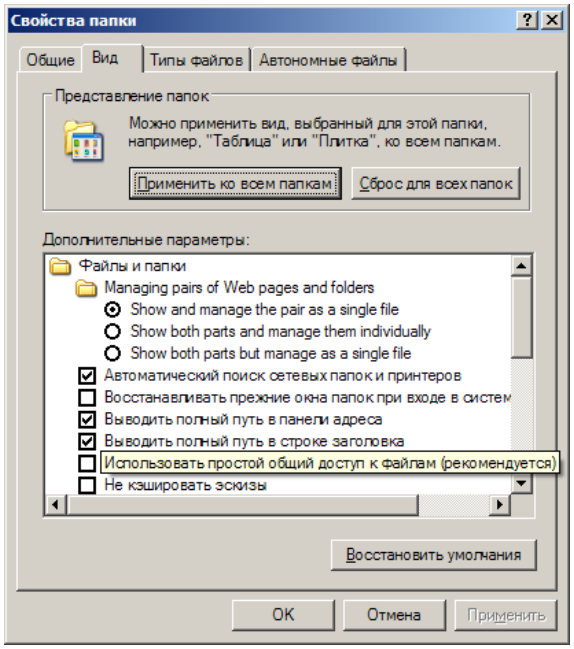

Рис. 1

– для операционной системы Microsoft Windows™ Server 2003:

а) создать учетную запись пользователя (Пуск – Панель управления – Учетные записи пользователей – Создание учетной записи);

– для операционной системы Microsoft Windows™ 7 или Microsoft Windows™ 10:

а) запустить приложение «Командная строка» от имени администратора (нажать правой кнопкой мыши по ярлыку приложения, из контекстного меню выбрать пункт «Запуск от имени администратора»);

б) ввести команду: net user **имя_администратора_компьютера** /active:yes;

в) установить пароль для учетной записи администратора («Панель управления» – «Учетные записи пользователей и семейная безопасность» – «Учетные записи пользователей» – «Управление другой учетной записью» – учетная запись администратора – «Создать пароль»).

2. Чтобы настроить права доступа к файлу настроек CryptoServiceSettings.xml и файлу журнала CryptoServiceLocalLog.txt, которые находятся в рабочей директории CryptoService, необходимо перейти в учетную запись администратора и щелкнуть правой кнопкой мыши на значке соответствующего файла и выбрать команду «Свойства». В открывшемся окне перейти на вкладку «Безопасность» (рис. 2).

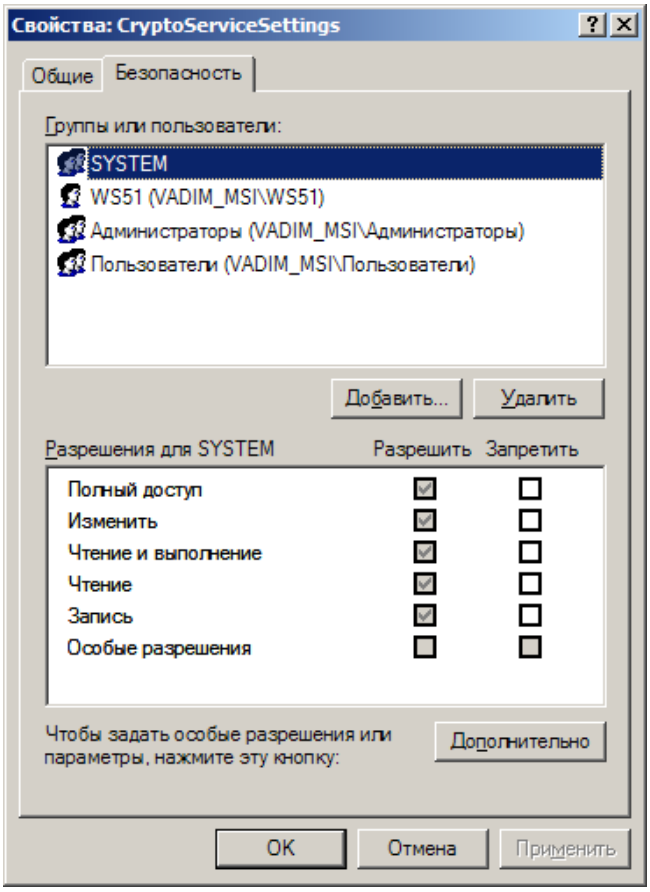

Рис. 2

3. Чтобы установить права доступа к файлу для конкретного пользователя, нужно нажать кнопку «Добавить».

4. В появившемся окне «Выбор: Пользователи или Группы» (рис. 3) нажать кнопку «Дополнительно». В окне «Выбор: Пользователи или Группы» (рис. 4) нажать кнопку «Поиск» и из появившегося списка всех групп и пользователей, выбрать нужного пользователя и дважды нажать кнопку «ОК».

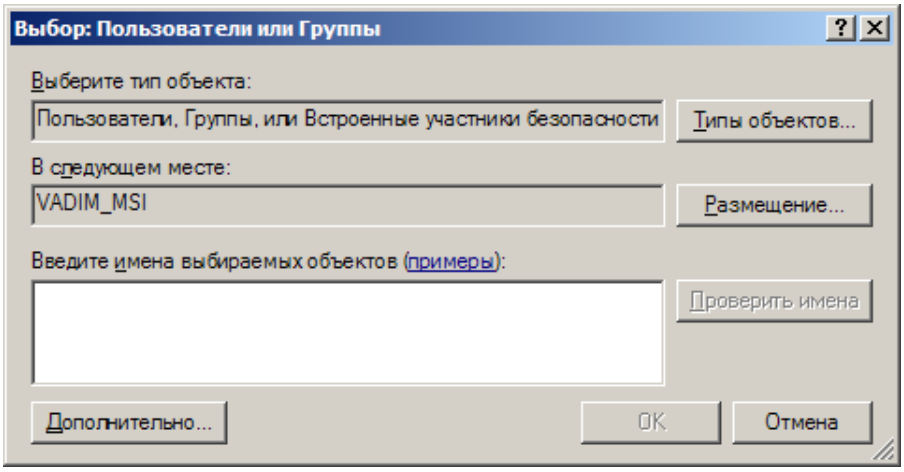

Рис. 3

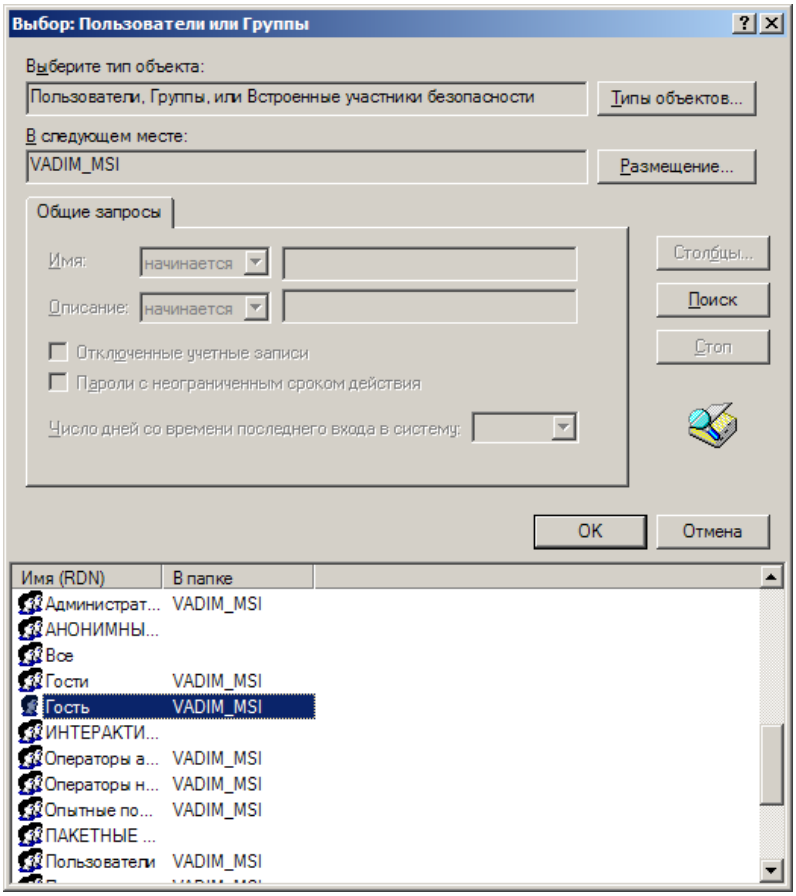

Рис. 4

5. В окне свойств файла на вкладке «Безопасность» в поле «Группы или Пользователи» нужно выбрать имя пользователя или группы, а в нижней части окна следует установить соответствующие флажки «Разрешить» или «Запретить». Сохранить изменения (рис. 5).

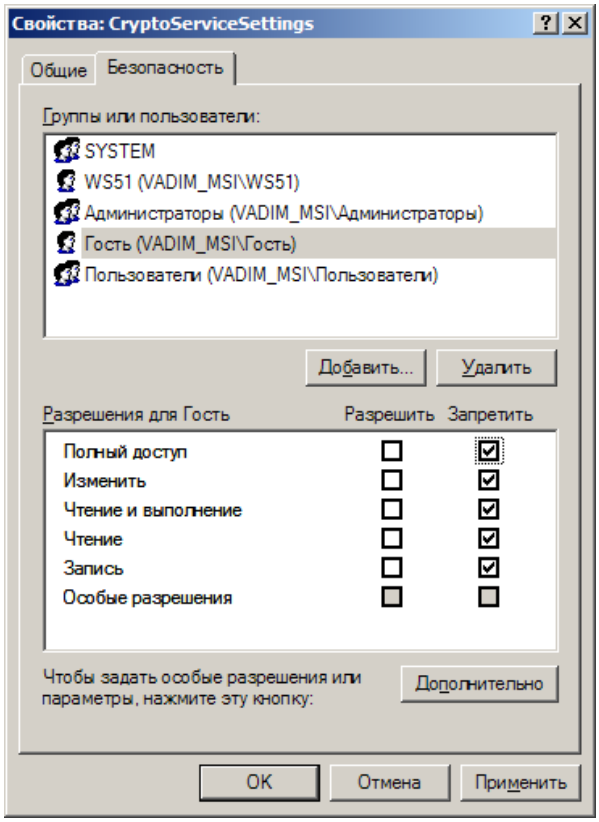

Рис. 5

6. В связи с тем, что для работы КП СОБ необходим доступ к файлу настроек и файлу журнала, запуск КП СОБ должен осуществляться от имени администратора. Это можно сделать с помощью сторонних прикладных программ (например, AdmiLink - http://admilink.narod.ru).

6.1. Запуск КП СОБ от имени администратора с помощью AdmiLink.

6.1.1. Перейти по ссылке http://admilink.narod.ru, скачать инсталляционный файл «installadmilink.exe».

6.1.2. Под учетной записью администратора запустить файл installadmilink.exe, установить программу AdmiLink и создать ярлык CryptoService_41.exe в соответствии с представленной на сайте документацией.

5. ЗАПУСК ПРОГРАММЫ

Запуск программы осуществляется путем запуска ярлыка CryptoService_41.exe, созданного согласно п. 4.

После загрузки программы в правом нижнем углу должна появиться иконка .

В процессе загрузки программы проверяется целостность криптографических библиотек и осуществляется самотестирование криптографических алгоритмов. Если проверка или самотестирование не увенчались успехом, то запуск программы блокируется и выдаются сообщения об ошибках (рис. 6, 7).

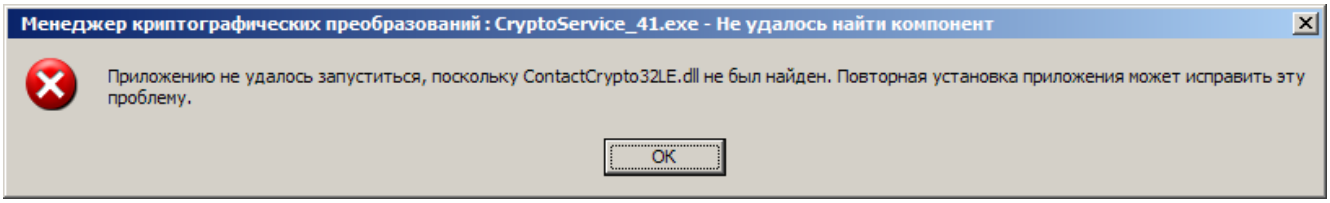

Рис. 6

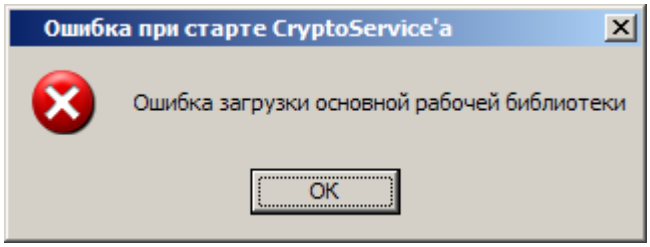

Рис. 7

Для возобновления работы с КП СОБ необходимо произвести повторную установку ПО согласно п. 3.

Если при запуске программы файл локального хранилища отсутствует или произошла ошибка загрузки данного файла, или файл имеет неверный формат, то будет выдано сообщение с указанием соответствующей ошибки загрузки файла локального хранилища и предложением о продолжении работы КП СОБ с пустым хранилищем сертификатов или завершении работы КП СОБ (рис. 8). Если в данном окне нажать кнопку «Да», то работа КП СОБ будет продолжена и файл локального хранилища будет создан и сохранен в рабочей директории в папке CertificateStorage при завершении работы КП СОБ (см. п. 6.13). Если нажать кнопку «Нет», то будет выдано сообщение об ошибке открытия файла с локальным хранилищем сертификатов (рис. 9) и работа КП СОБ будет завершена.

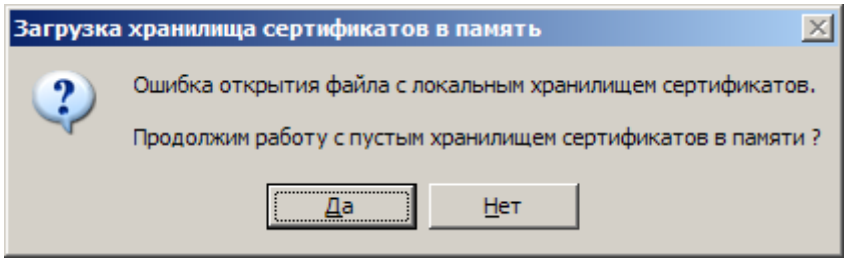

Рис. 8

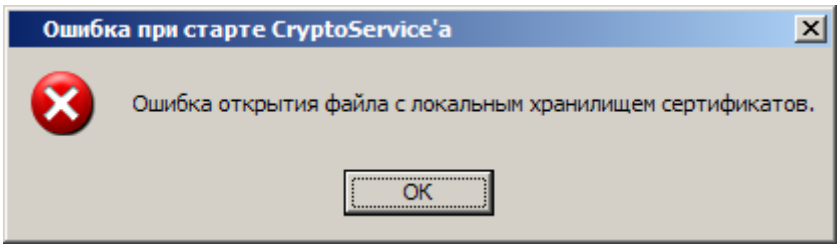

Рис. 9

Внимание: перед запуском любого модуля КП СОБ необходимо убедиться, что запущена программа CryptoService_41. Если программа CryptoService_41 уже некоторое время выполняется до запуска любого модуля КП СОБ, то необходимо сначала провести проверку целостности и тестирование криптобиблиотек (см. п. 6.11).

6. РАБОТА С ПРОГРАММОЙ

Работа с программой в основном не требует вмешательства пользователя.

Исключением являются операции, связанные с генерацией ключей, формирования заявок на выпуск сертификатов, выполнения процедуры его отзыва или приостановки и некоторые другие.

Проведение аутентификации пользователей в системе производится путем обработки введенного пароля к личному ключу пользователя.

Вызов компоненты протоколирования производится отдельными модулями комплекса с передачей ему регистрируемых данных. Отказ любого модуля, за исключением компоненты протоколирования не может привести к нарушению записи данных в журнал и их потерю.

Выполнение криптоопераций осуществляется в ответ на запросы внешних приложений. Обмен входными и выходными данными осуществляется через сокеты. В приложении существует один прослушивающий сокет. В ответ на внешний запрос создаётся индивидуальный поток со своим сокетом обмена. В этом потоке осуществляется выполнение запрошенной криптооперации, результаты которой отправляются внешнему приложению, сделавшему запрос, а поток закрывается.

6.1. Выпуск сертификата открытого ключа

6.1.1. Для формирования заявки на выпуск СОК необходимо щелкнуть правой кнопкой мыши в трее по иконке CryptoService  , что приведет к высвечиванию меню в правом нижнем углу экрана, форма которого представлена на рис.10. Процедура формирования и выполнения заявки на выпуск СОК требует выбрать пункт меню «Выпустить заявку на сертификат / Issue a request for a certificate» (рис.10).

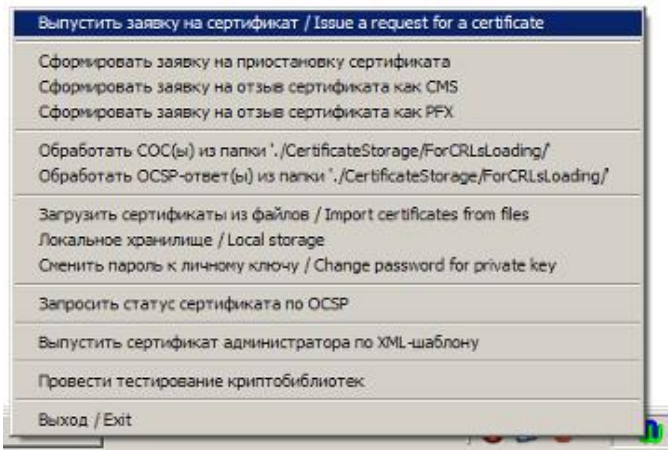

Рис. 10

После этого откроется главное окно диалога формирования заявки на выпуск СОК, в котором следует ввести требуемую информацию в соответствующие поля для каждой из закладок (рис. 11).

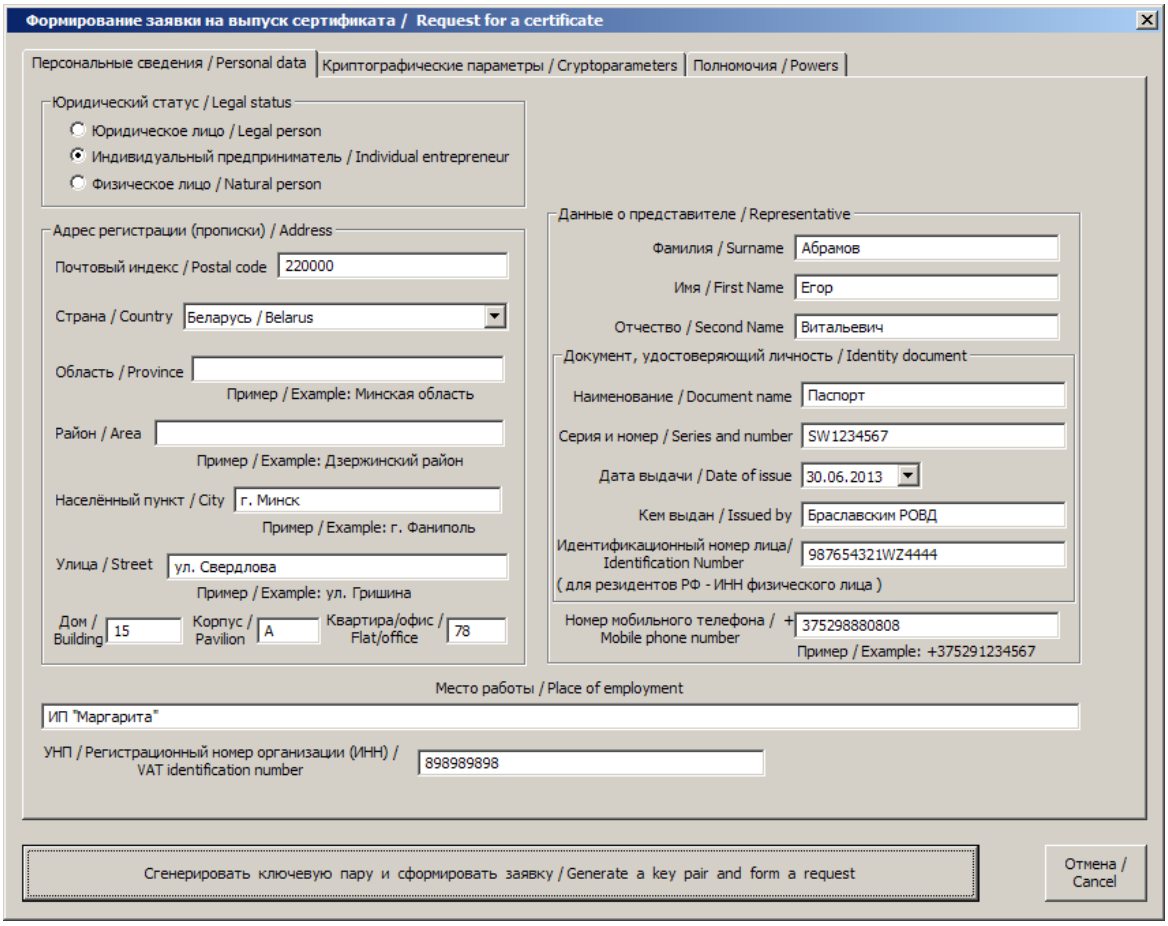

Рис. 11

С помощью закладок в главном окне осуществляется вызов следующих функций:

– «Персональные сведения / Personal data» – вывод персональных данных о владельце СОК;

– «Криптографические параметры» – задание криптографических параметров открытого ключа;

– «Полномочия / Powers» – описание документа, подтверждающего полномочия пользователя.

6.1.2. При выборе закладки «Персональные сведения / Personal data» выдается экранная форма для вывода персональных данных о владельце СОК (рис. 12).

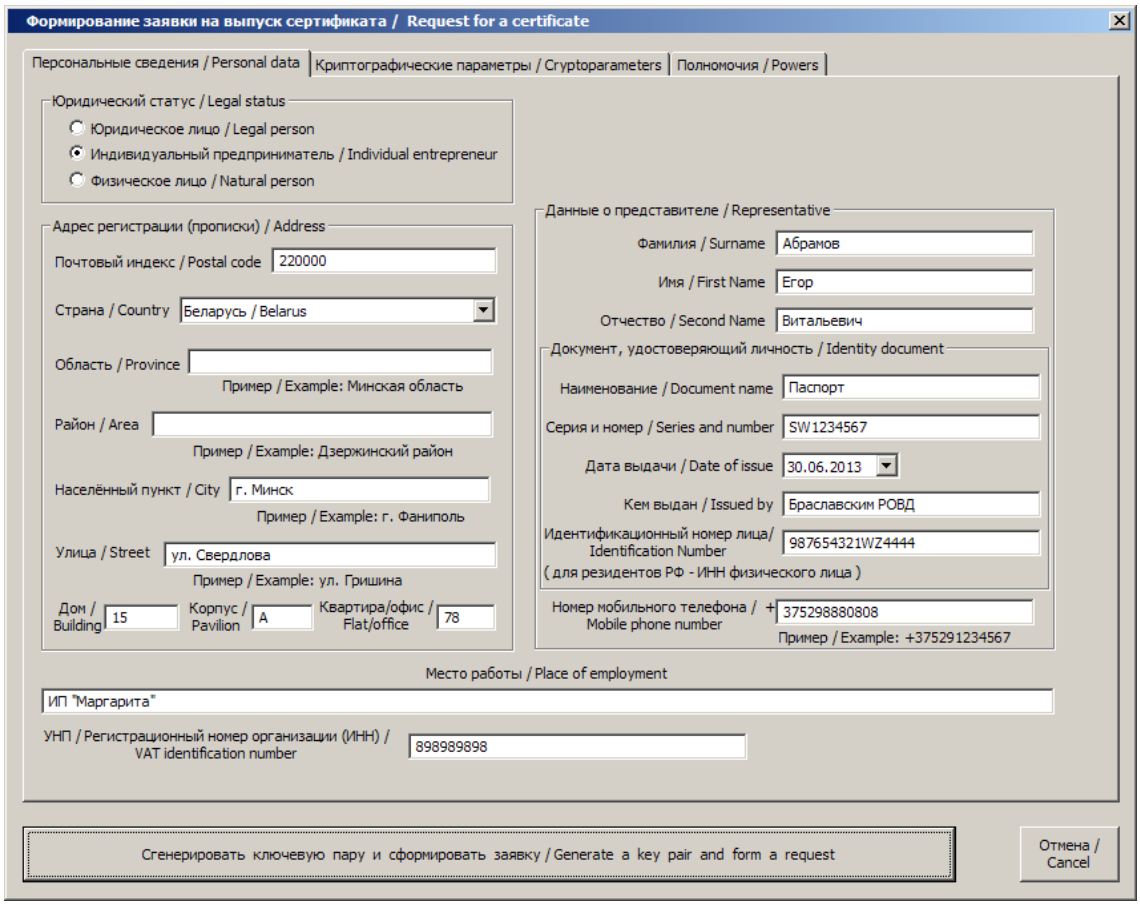

Рис. 12

6.1.3. При заполнении полей следует учитывать, что ввод возможен только в поле, окрашенное в белый цвет. Поле со значком  позволяет выбрать из значений, открывающихся при нажатии на кнопку в правой части поля.

6.1.4. В зависимости от выбранного юридического статуса («Юридический статус / Legal status») происходит изменение внешнего вида формы. Так, при выбранном юридическом статусе «Юридическое лицо / Legal person» или «Индивидуальный предприниматель / Individual entrepreneur» необходимо ввести информацию об УНП (ИНН) организации в текстовое поле «УНП / Регистрационный номер организации (ИНН) / VAT identification number» (рис. 13).

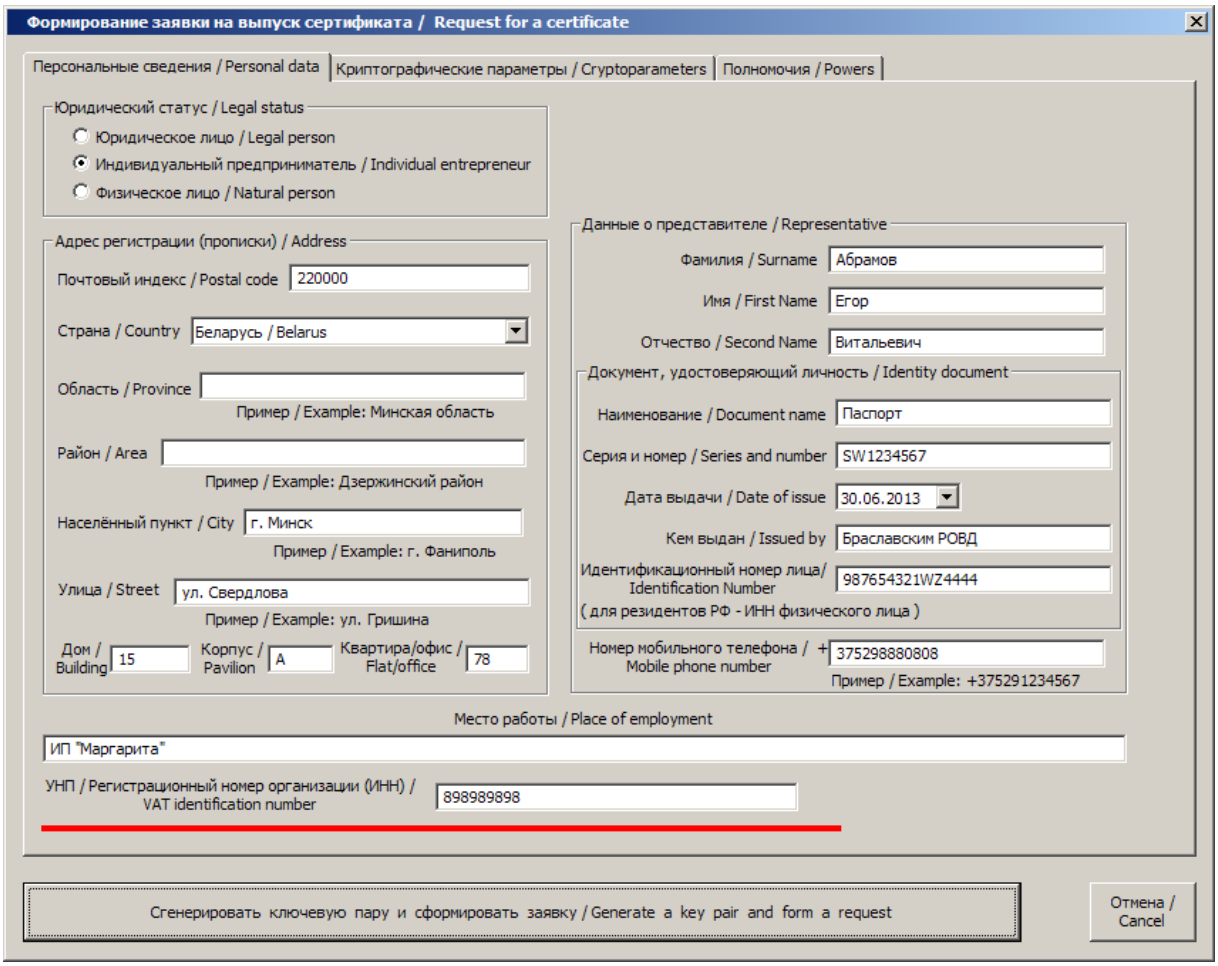

Рис. 13

6.1.5. При выбранном юридическом статусе «Физическое лицо / Natural person» вместо регистрационного номера организации необходимо заполнить текстовое поле «Должность / Position» (рис. 14).

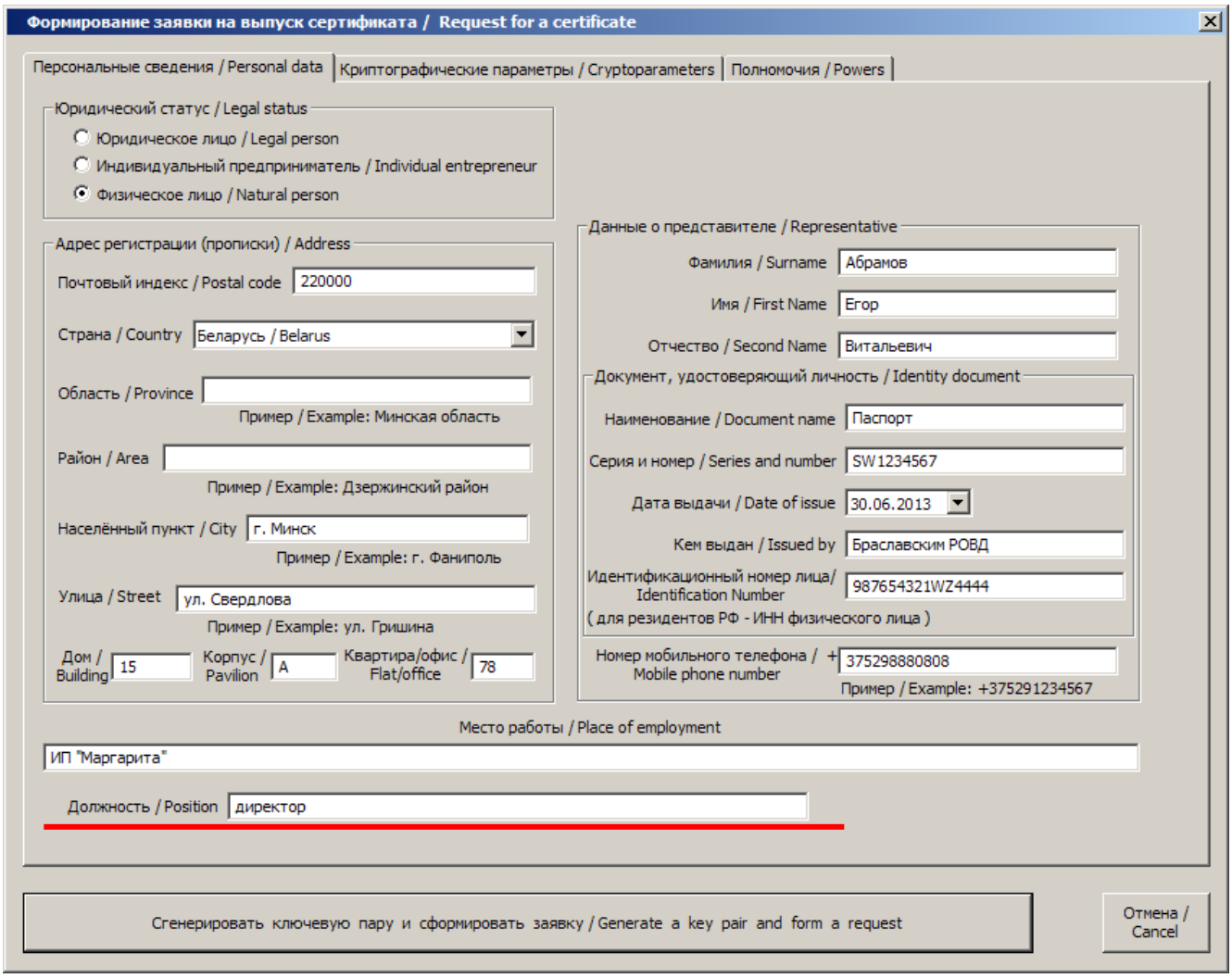

Рис. 14

6.1.6. Если из списка в поле «Страна / Country» выбрана «Беларусь / Belarus», то в текстовое поле «Почтовый индекс / Postal code» предусмотрена возможность ввести только 6 цифр, а в текстовое поле «Идентификационный номер налогоплательщика / VAT identification number» – только 9 цифр (рис. 13).

6.1.7. Аналогичным образом осуществляется заполнение правой стороны формы главного окна диалога формирования заявки на выпуск СОК (рис. 14). При этом в текстовые поля «Серия и номер / Series and number» и «Идентификационный номер лица / Identification Number» допускается вводить только заглавные буквы латинского алфавита и цифры (рис. 14). При вводе других символов будут выведены сообщения-подсказки (рис. 15, 16).

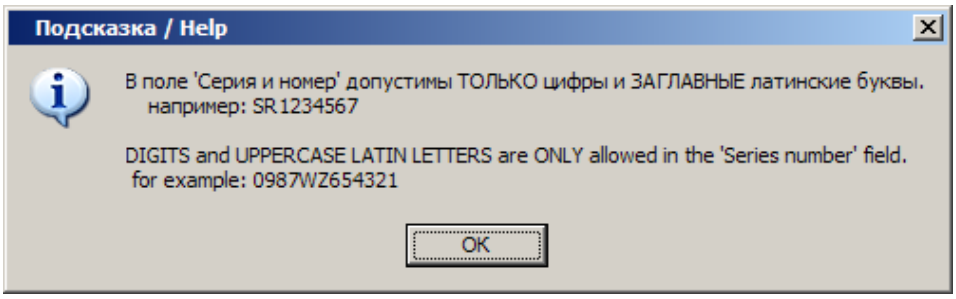

Рис. 15

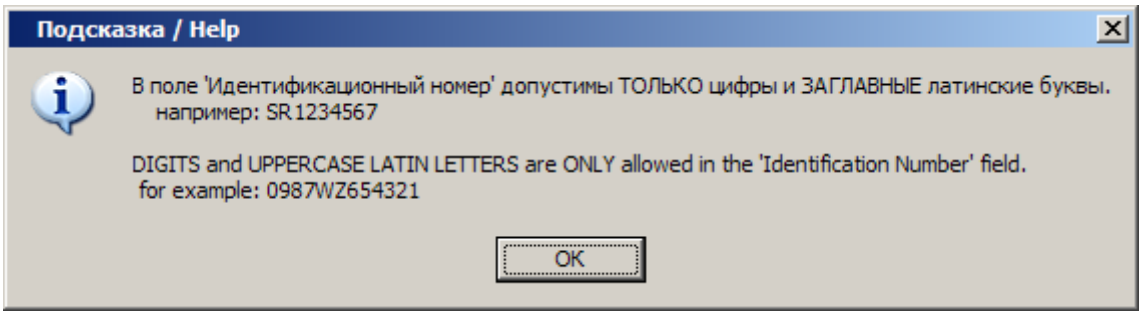

Рис. 16

6.1.8. При выборе закладки «Криптографические параметры» выдается экранная форма, для задания криптографических параметров открытого ключа (рис. 17).

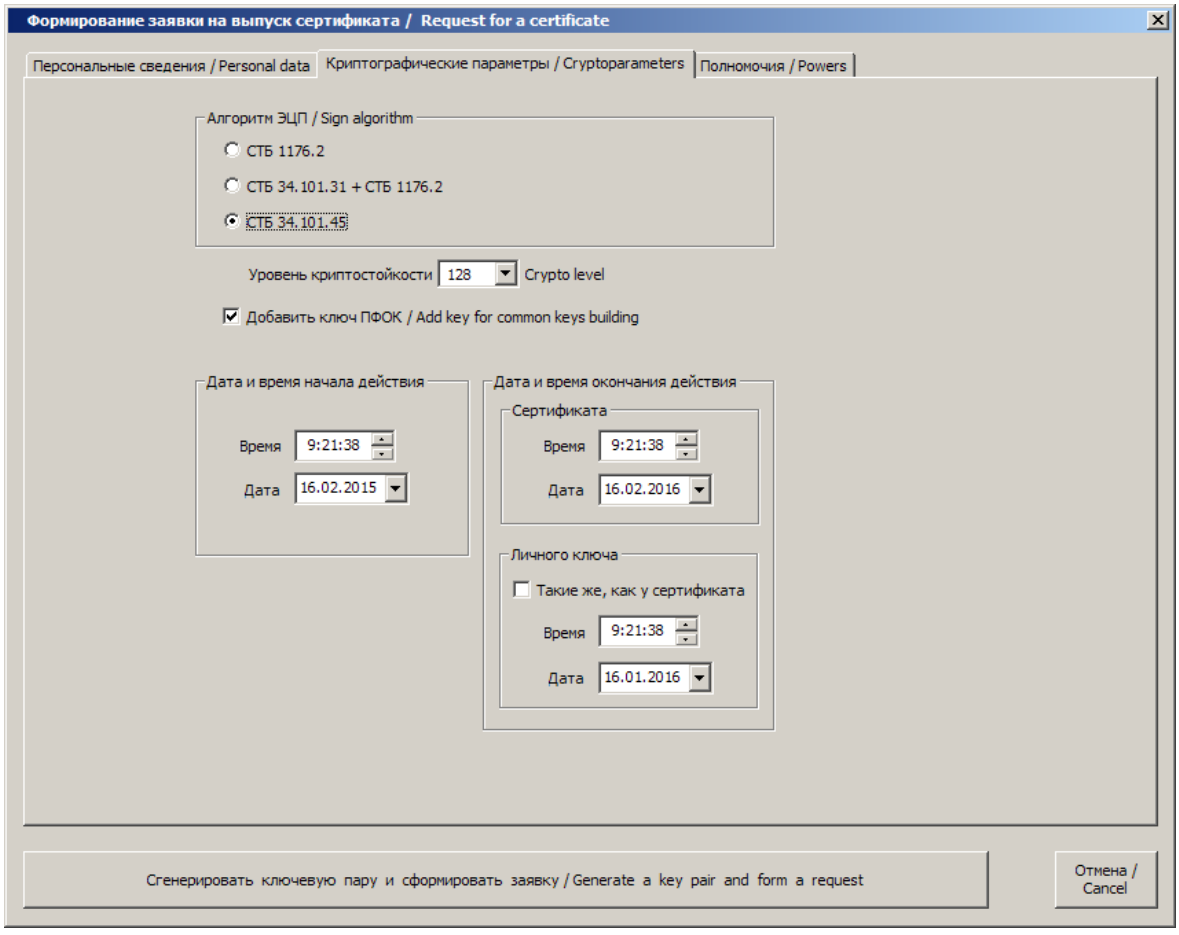

Рис. 17

Для алгоритма ЭЦП СТБ 34.101.45 следует выбирать только уровень криптостойкости 128, в связи с отсутствием стандартов хэш-функций с длинами хэш-значений 384 и 512 бит.

Для установки даты и времени окончания действия личного ключа такими же, как у сертификата, нужно выбрать переключатель «Такие же, как у сертификата».

6.1.9. При выборе закладки «Полномочия / Powers» выдается экранная форма для описания документа, подтверждающего полномочия юридического лица (индивидуального предпринимателя) (рис. 18).

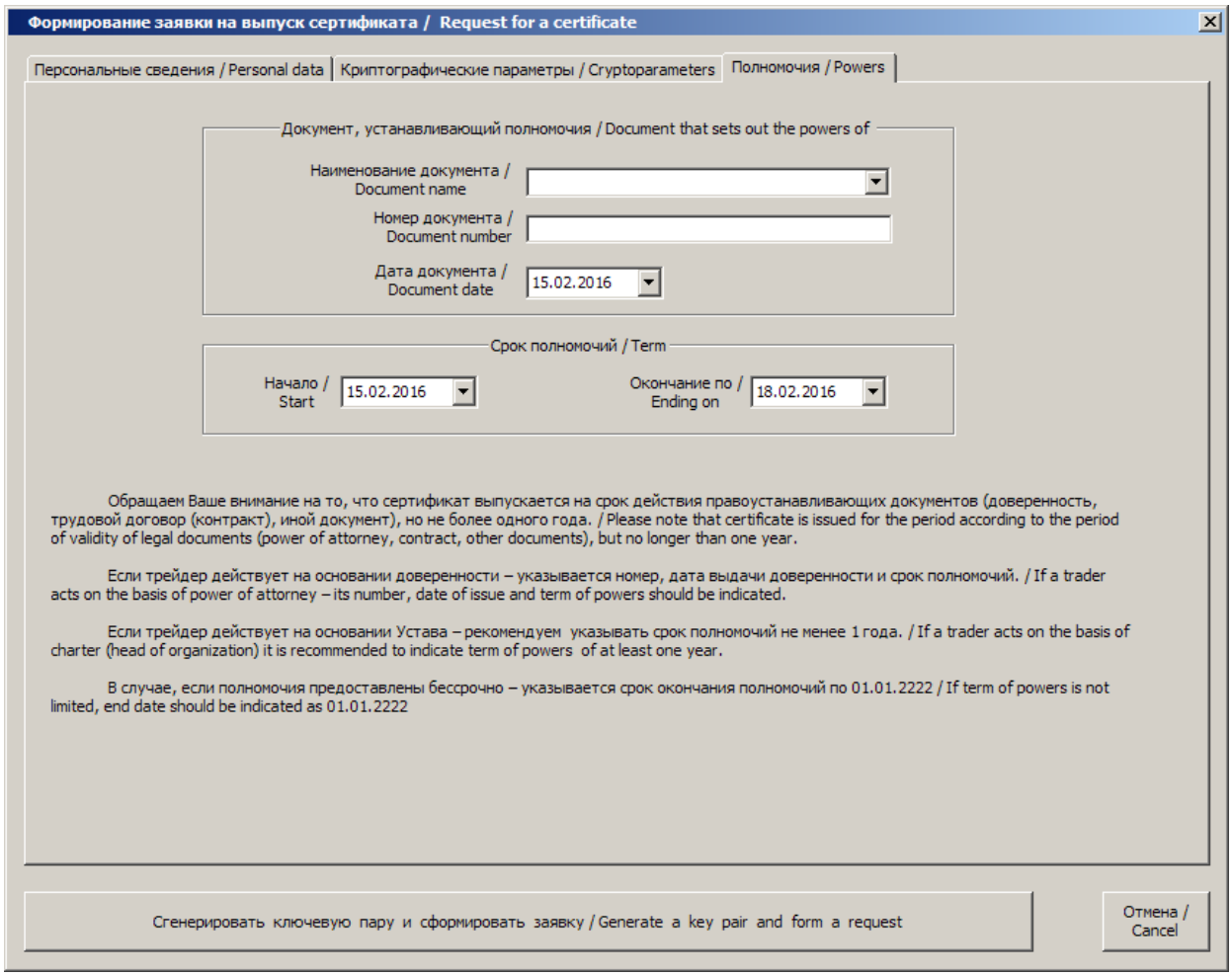

Рис. 18

6.1.10. Если первоначально на закладке «Персональные сведения / Personal data» выбран статус «Юридическое лицо / Legal person» или «Индивидуальный предприниматель / Individual entrepreneur», а далее на закладке «Полномочия / Powers» в поле «Наименование документа / Document name» выбрано «Доверенность», то необходимо ввести номер и дату документа, устанавливающего полномочия, в поля «Номер документа / Document number» и «Дата документа / Document date» соответственно (рис. 18). Если же в качестве наименования документа, устанавливающего полномочия, выбрано другое значение, а не «Доверенность», то

номер и дата документа, устанавливающего полномочия, становятся недоступными для ввода (рис. 19).

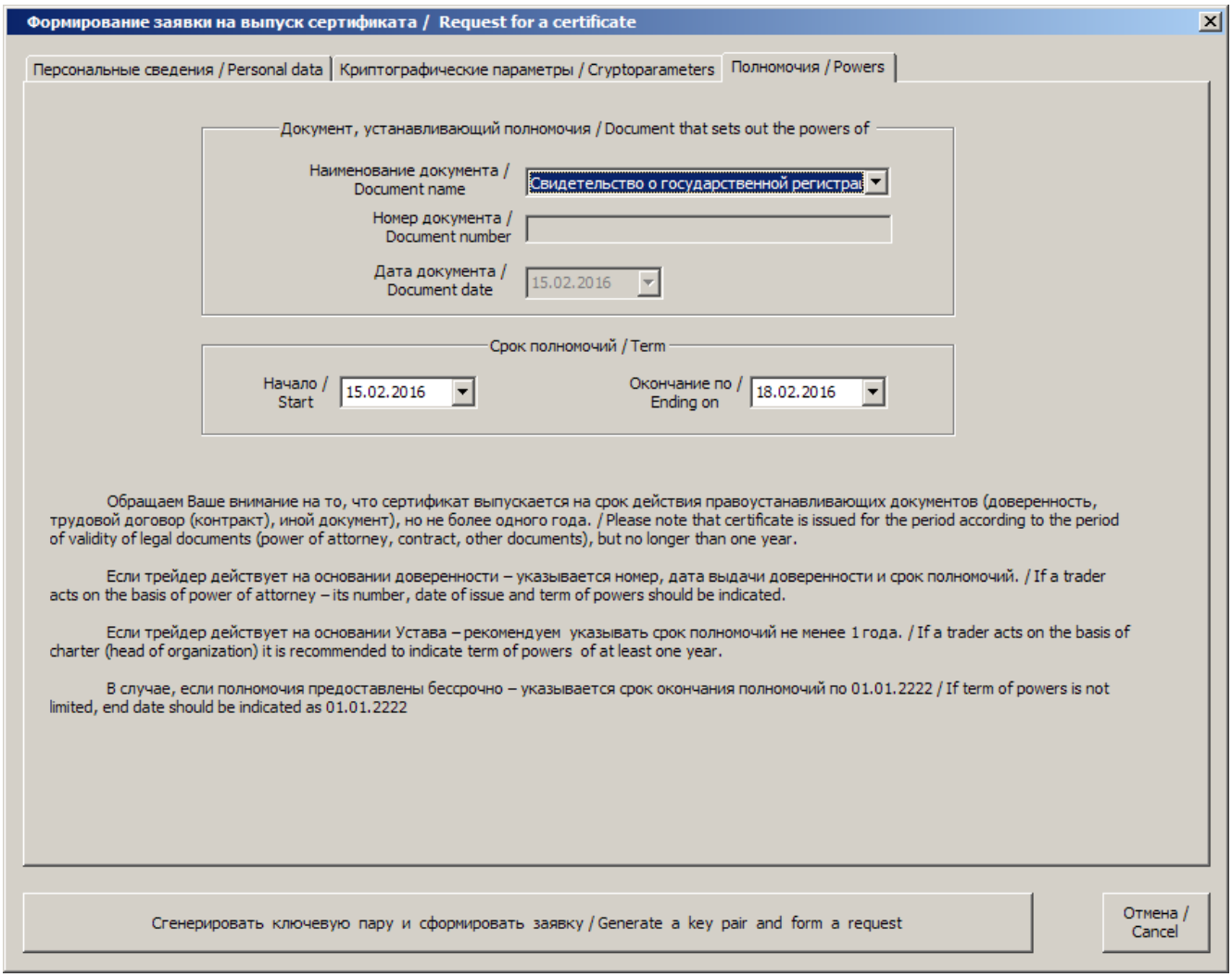

Рис. 19

6.1.11. При первоначальном выборе на закладке «Персональные сведения / Personal data» статуса «Физическое лицо / Natural person» на закладке «Полномочия / Powers» скрываются все поля для указания документа, устанавливающего полномочия, и срока действия полномочий (рис. 20).

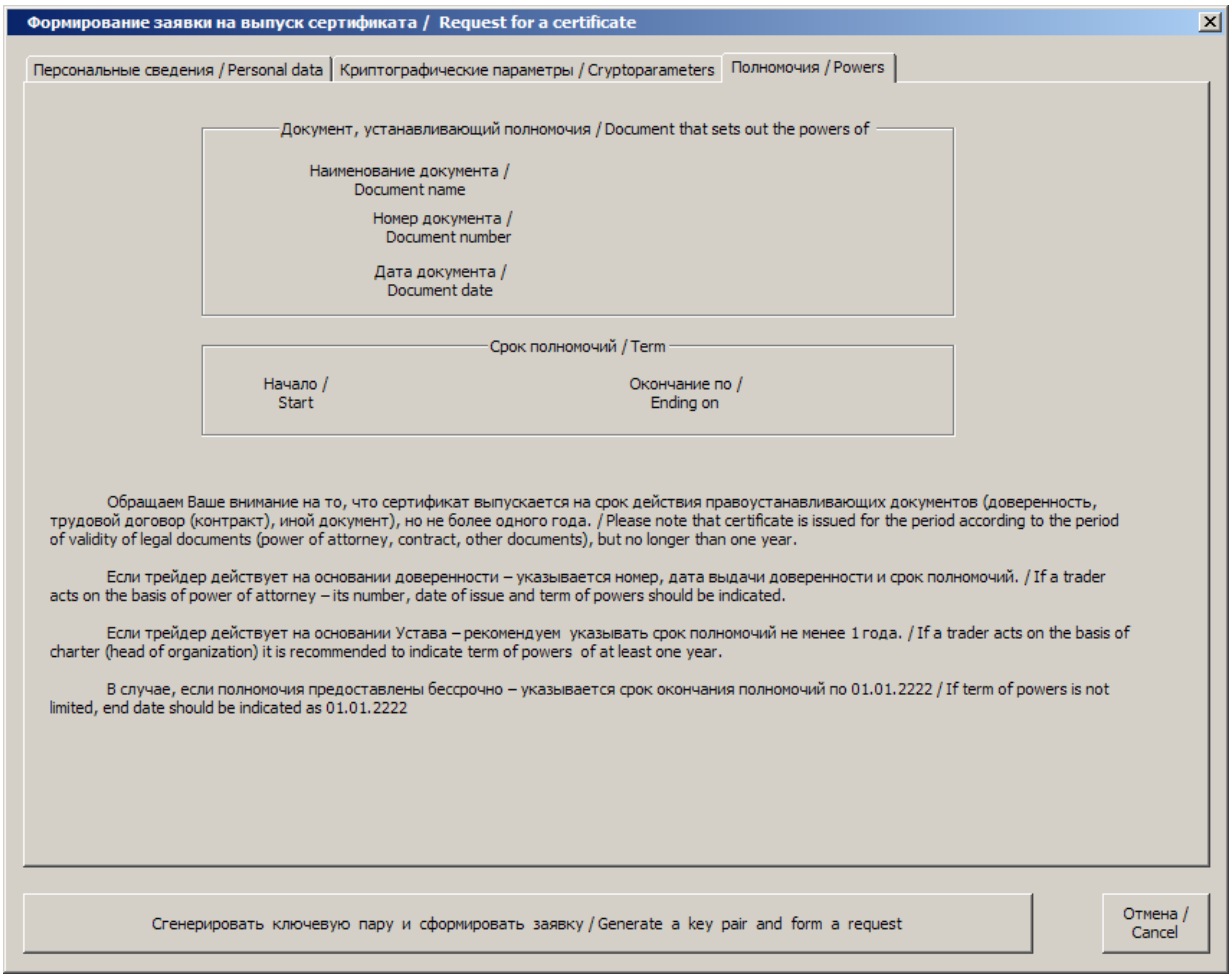

Рис. 20

6.1.12. Для отмены формирования заявки на выпуск СОК необходимо нажать кнопку «Отмена», при этом будет выведено сообщение как на рис. 21. При этом процедура формирования заявки на выпуск СОК будет прекращена.

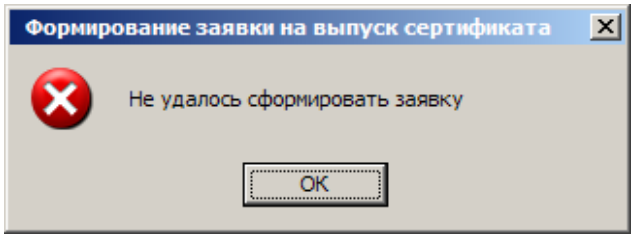

Рис. 21

6.1.13. Для формирования заявки на выпуск СОК и карточки открытого ключа необходимо нажать кнопку «Сгенерировать ключевую пару и сформировать заявку / Generate a key pair and form a request». При этом при нажатии на данную кнопку будет проверено заполнение полей на всех закладках.

6.1.14. Если на закладке «Персональные сведения / Personal data» не заполнены какие-либо обязательные поля, то будет выведено соответствующие сообщение с наименованием незаполненного поля (рис. 22).

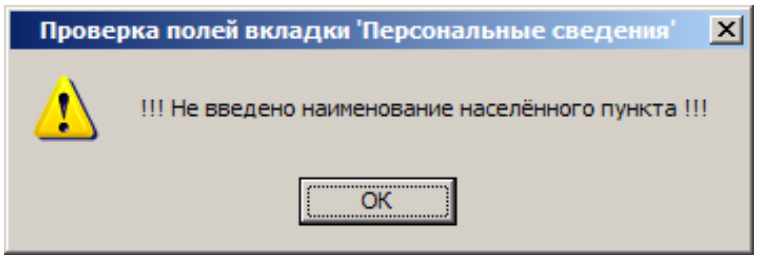

Рис. 22

6.1.15. Также, если на закладке «Полномочия / Powers» в качестве наименования документа, устанавливающего полномочия, выбрана «Доверенность», а номер документа не введен, то будет выведено сообщение, представленное на рис. 23.

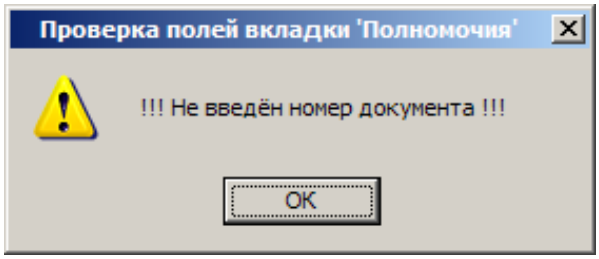

Рис. 23

Если дата начала срока полномочий меньше даты документа, устанавливающего полномочия, то будет выведено сообщение, представленное на рис. 24.

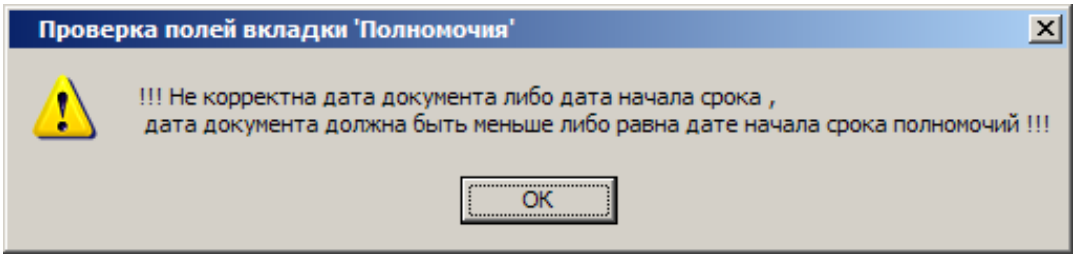

Рис. 24

Если дата начала срока полномочий больше даты окончания срока полномочий, то будет выведено сообщение, представленное на рис. 25.

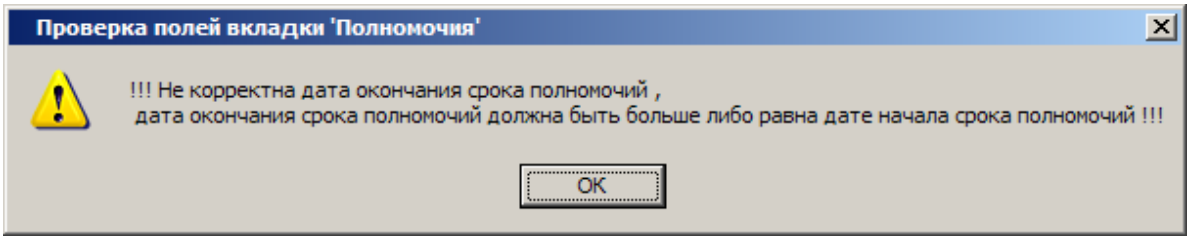

Рис. 25

6.1.16. В случае, если все требуемые поля заполнены корректно, то появится окно для ввода пароля к личному ключу и подтверждения пароля (рис. 26). Минимальная длина пароля составляет 8 символов. Если пароль состоит менее чем из 8 символов, то после ввода пароля и нажатия кнопки «Enter» будет выдано предупреждении (рис. 27).

Количество попыток ввода пароля неограниченно.

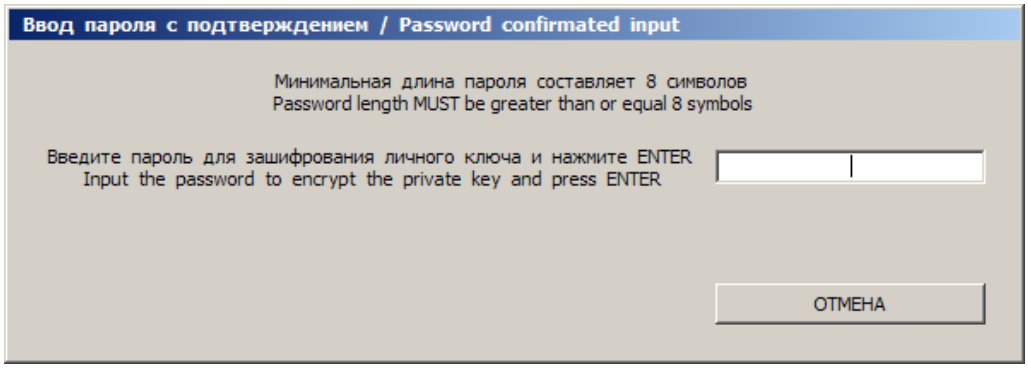

Рис. 26

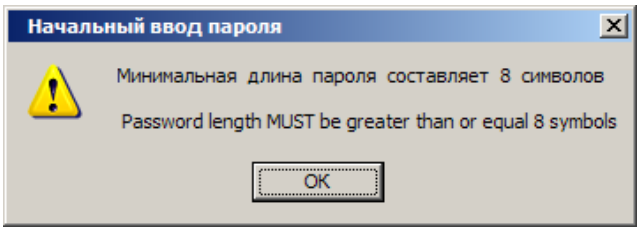

Рис. 27

Если подтверждение пароля не совпало с введенным паролем, то будет выдано предупреждение как на рис. 28.

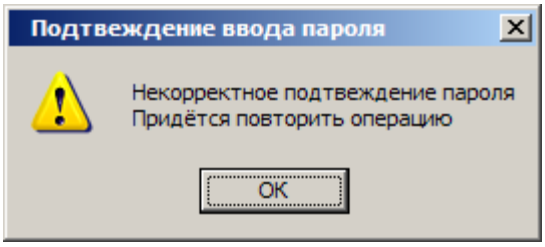

Рис. 28

Для отмены процедуры ввода пароля необходимо нажать кнопку «Отмена», при этом будет выведено сообщение как на рис. 29 и процедура формирования заявки на выпуск СОК будет прекращена.

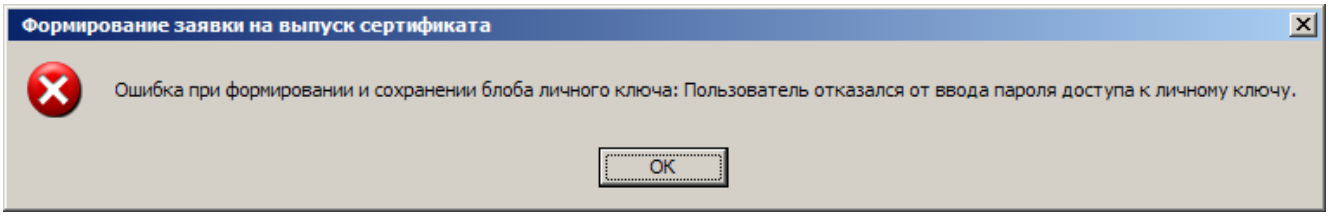

Рис. 29

Если пароль и подтверждение пароля совпали, будет выведено диалоговое окно «Выбор имени файла для сохранения личного ключа», где возможно указать путь, по которому будет сохранен файл с личным ключом, и по необходимости изменить имя файла, содержащего личный ключ (рис. 30).

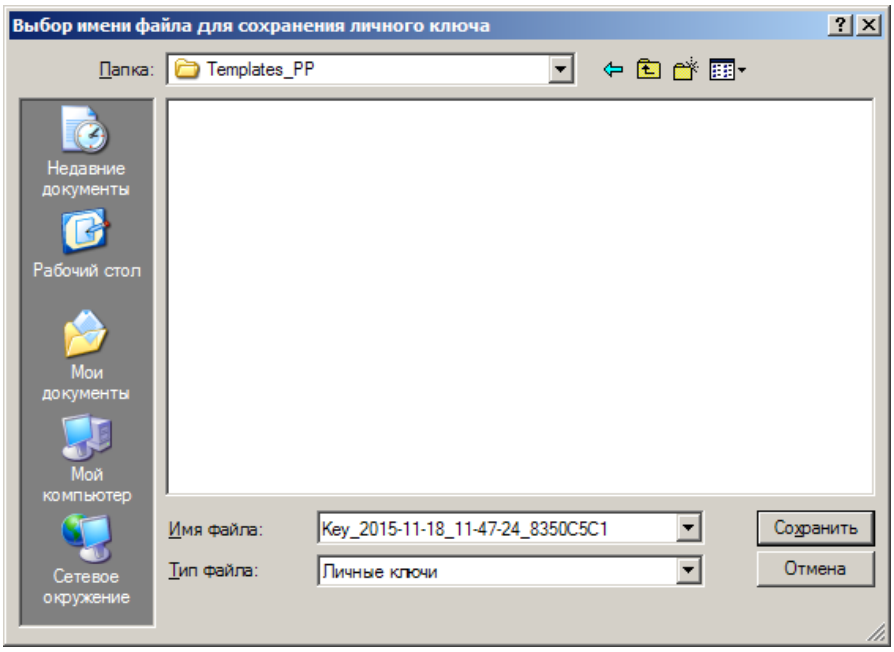

Рис. 30

6.1.17. После сохранения файла с личным ключом будут сформированы ASN1-заявка, SOAP-заявка и выданы соответствующие сообщения (рис. 31, 32).

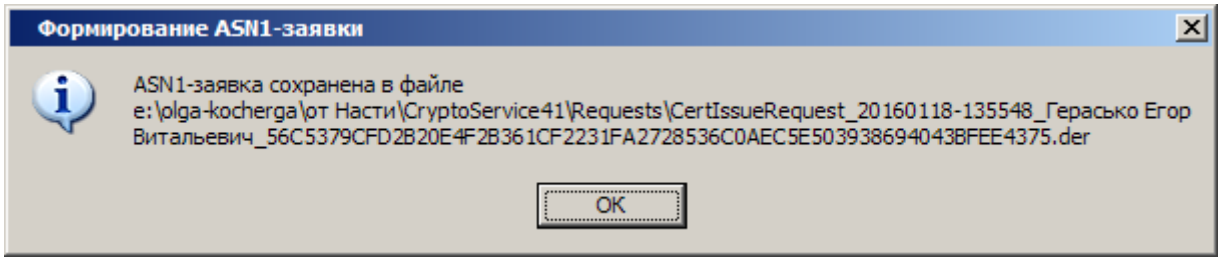

Рис. 31

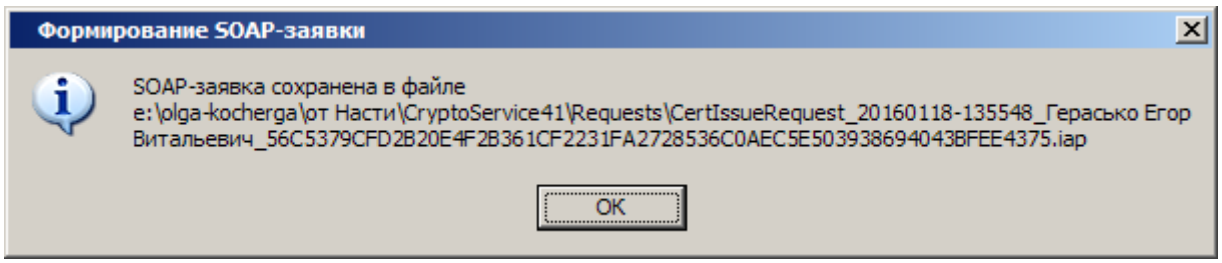

Рис. 32

Структуры SOAP-заявки и ответа приведены в приложении 1.

В случае, если в настроечном файле CryptoServiceSettings.xml указаны неверные почтовые настройки в собственной транспортной секции (секция Transport – секция RA – EMail (см. п. 7.1)) или нет доступа к почтовому серверу, то будет выдано сообщение с ошибкой отправки заявки в КП РЦ (рис. 33). Если соединение с КП РЦ установлено и сформированная заявка была отправлена в КП РЦ, будет показано сообщение как на рис. 34.

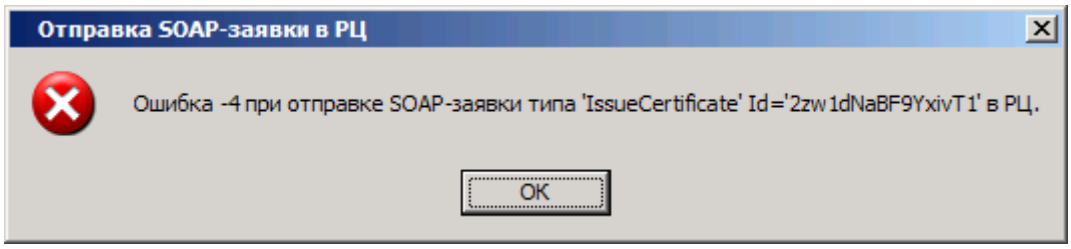

Рис. 33

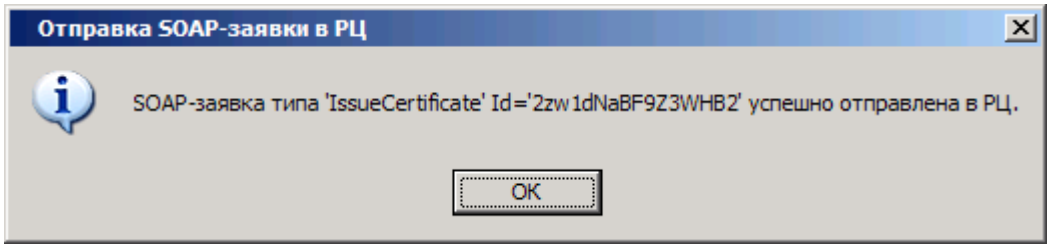

Рис. 34

6.1.18. Так же будет сформирована карточка открытого ключа и выведено сообщение с именем карточки и предложением о ее редактировании (рис. 35). Карточка открытого ключа сохраняется в рабочей директории в папке PublicKeyCards и имеет расширение .rtf.

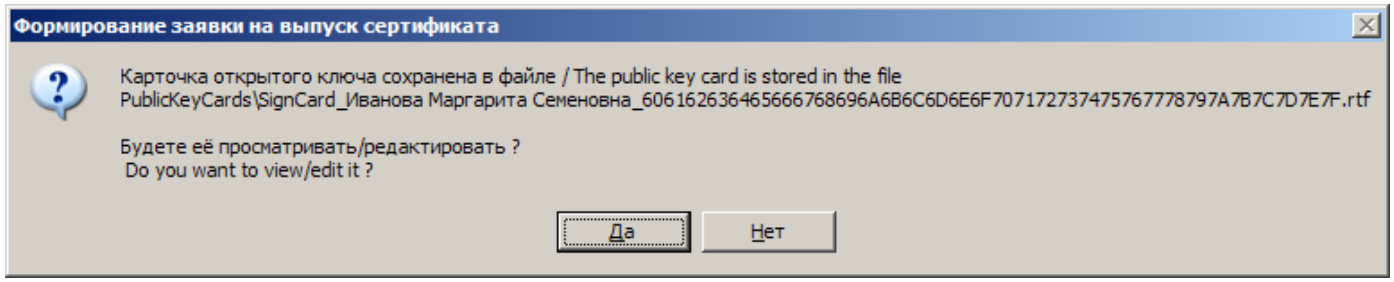

Рис. 35

Чтобы просмотреть и/или редактировать карточку открытого ключа, необходимо нажать кнопку «Да», в результате чего карточка открытого ключа будет выведена на экран монитора (рис. 36).

Для корректного просмотра или редактирования карточки открытого ключа может понадобиться текстовый редактор Angel Writer (см. п. 3.7).

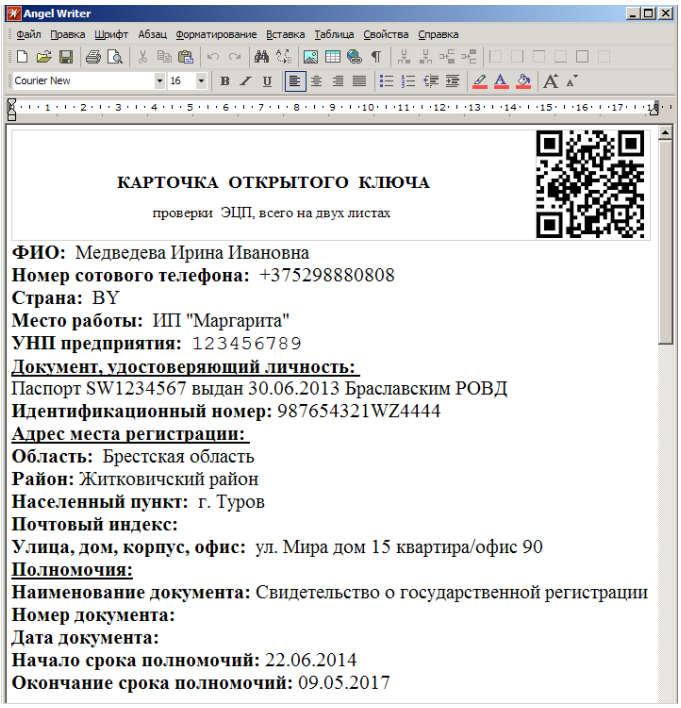

Рис. 36

Когда в рабочей директории КП СОБ по пути PublicKeyCards\Templates не найден соответствующий шаблон для карточки открытого ключа, будут выданы сообщения об ошибках (рис. 37-39) и карточка открытого ключа не будет сформирована.

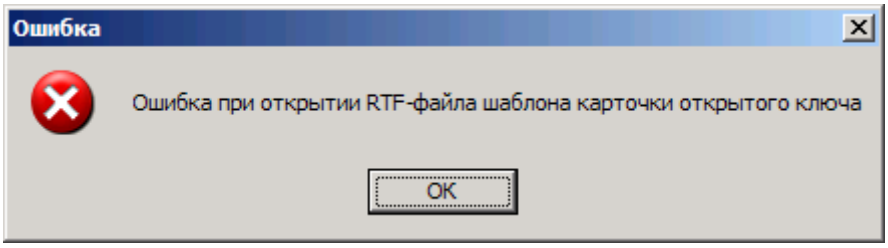

Рис. 37

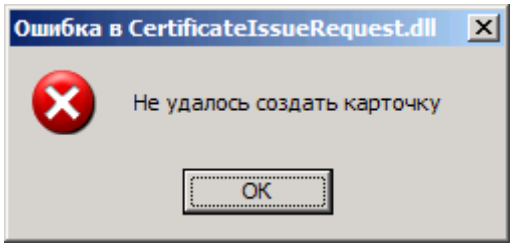

Рис. 38

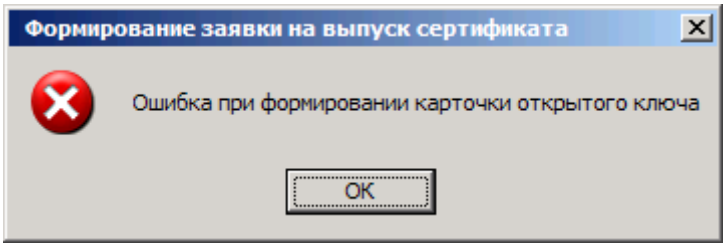

Рис. 39

6.1.19. При успешном формировании заявки на выпуск сертификата будет выдано сообщение как на рис. 40.

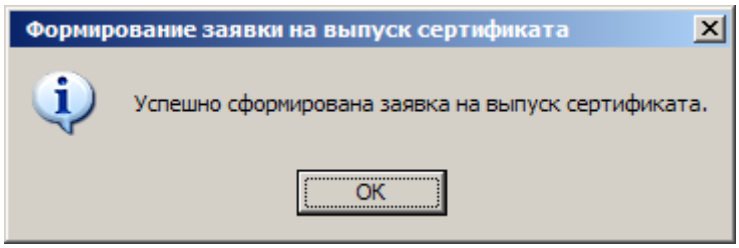

Рис. 40

6.2. Отзыв сертификата открытого ключа

6.2.1. При создании заявки на отзыв СОК следует подвести курсор к иконке  и нажать на правую кнопку мыши. В правом нижнем углу появится меню как это показано на рис. 41.

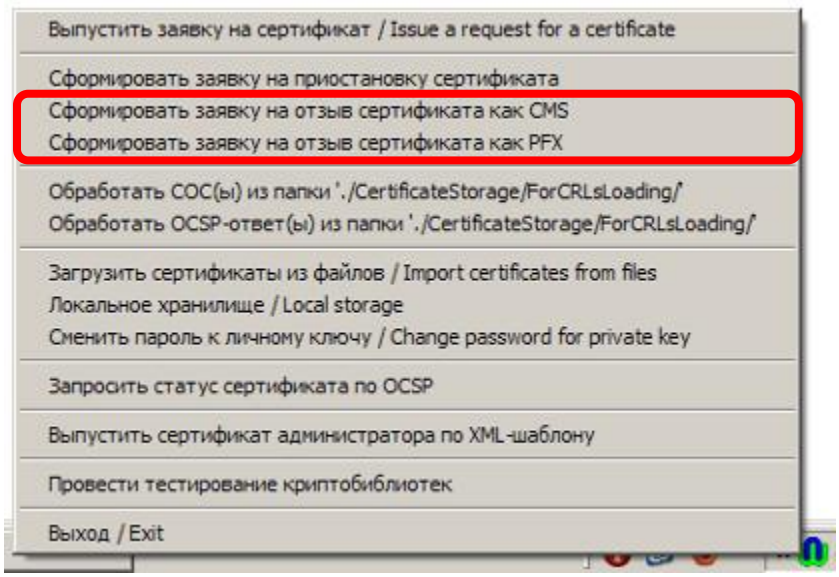

Рис. 41

Для формирования заявки на отзыв СОК можно использовать два пункта меню: «Сформировать заявку на отзыв сертификата как CMS» и «Сформировать заявку на отзыв сертификата как PFX». При выборе пункта меню «Сформировать заявку на отзыв сертификата как CMS» формат заявки на отзыв будет сформирован в соответствии с СТБ 34.101.23, а при выборе пункта меню «Сформировать заявку на отзыв сертификата как PFX» — в соответствии с СТБ 34.101.18.

6.2.2. После выбора одного из пунктов меню для формирования заявки на отзыв СОК, на экран будет выведено окно «Выпуск заявки на отзыв сертификата», как это показано на рис. 42. В данном окне в области «Введите серийный номер или идентификатор открытого ключа

отзываемого сертификата» в соответствующих полях необходимо указать серийный номер или идентификатор открытого ключа отзываемого сертификата.

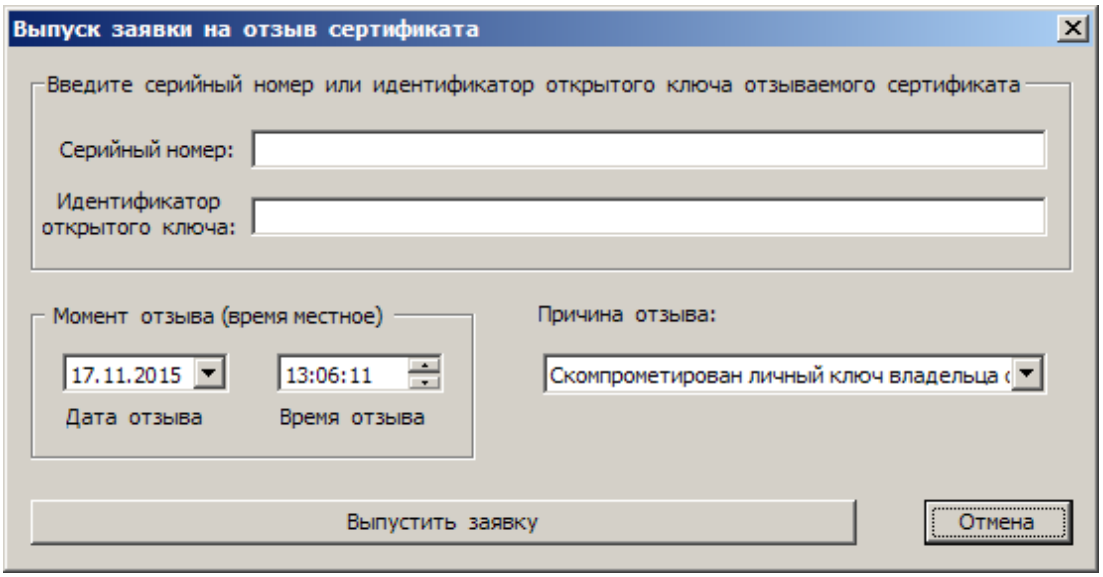

Рис. 42

6.2.3. Серийный номер и идентификатор открытого ключа можно скопировать из локального хранилища (п. 6.7 настоящего документа).

6.2.4. Так же серийный номер и идентификатор открытого ключа можно получить следующим образом.

Поскольку сертификаты размещены в рабочей директории в папке CertificateStorage\CertificateOriginals\, необходимо открыть данную папку, найти в ней сертификат, который требуется отозвать, и дважды щелкнуть по нему левой кнопкой мыши. В результате осуществления данных действий откроется окно «Сертификат» (рис. 43).

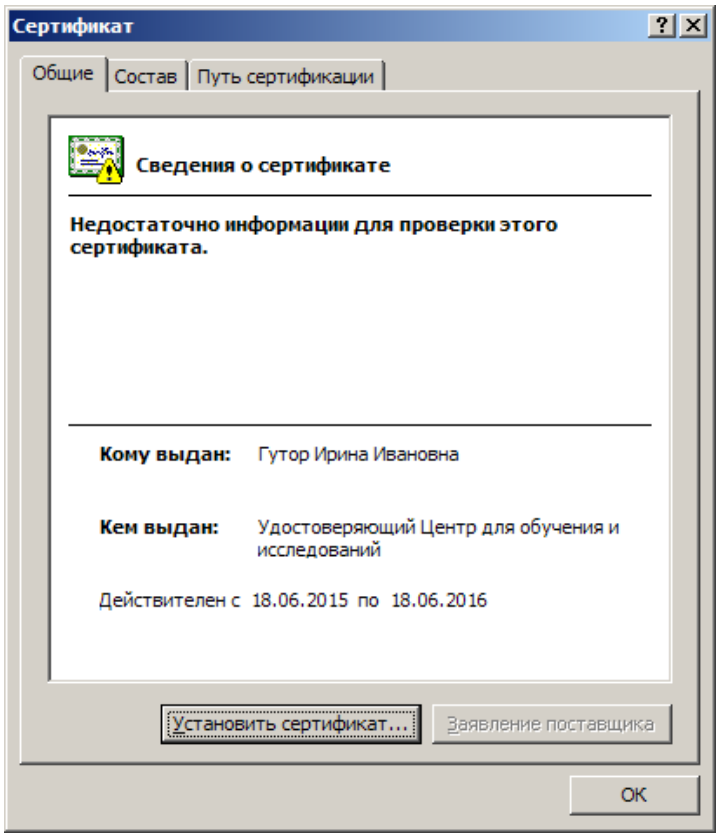

Рис. 43

6.2.4.1. В появившемся окне «Сертификат» имеется три вкладки: «Общие», «Состав» и «Путь сертификации». Вкладка «Общие» предоставляет информацию об общих сведениях о сертификате – имя владельца сертификата, наименование организации, выдавшей сертификат, и срок действия сертификата (рис. 43). Вкладка «Состав» позволяет получить информацию о значениях всех полей выбранного сертификата, а вкладка «Путь сертификации» – показывает цепочку сертификатов от корневого СОК КПА УЦ.

6.2.4.2. Для того, чтобы идентифицировать серийный номер выбранного сертификата, необходимо открыть вкладку «Состав» и нажать левой кнопкой мыши на поле «Серийный номер». В результате данных действий в нижнем окне данной вкладки отобразится серийный номер выбранного сертификата, как это показано на рис. 44.

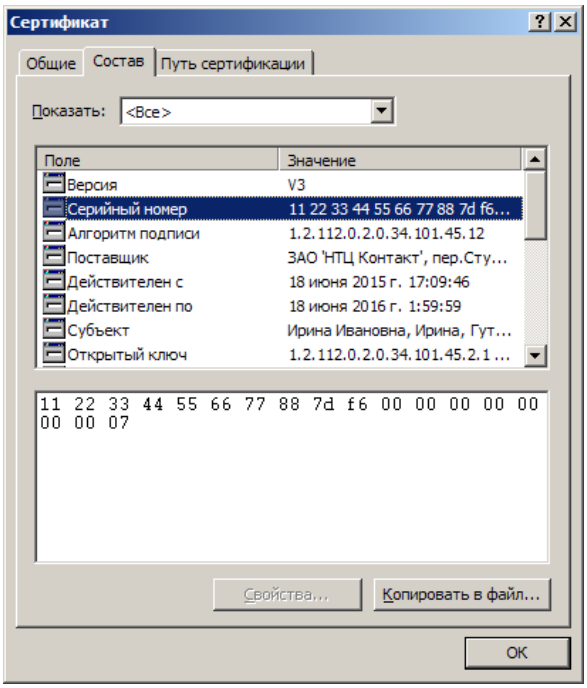

Рис. 44

6.2.4.3. Необходимо выделить с помощью левой кнопки мыши данный серийный номер и нажать комбинацию клавиш «Ctrl + C» на клавиатуре, скопировав его таким образом (рис. 45).

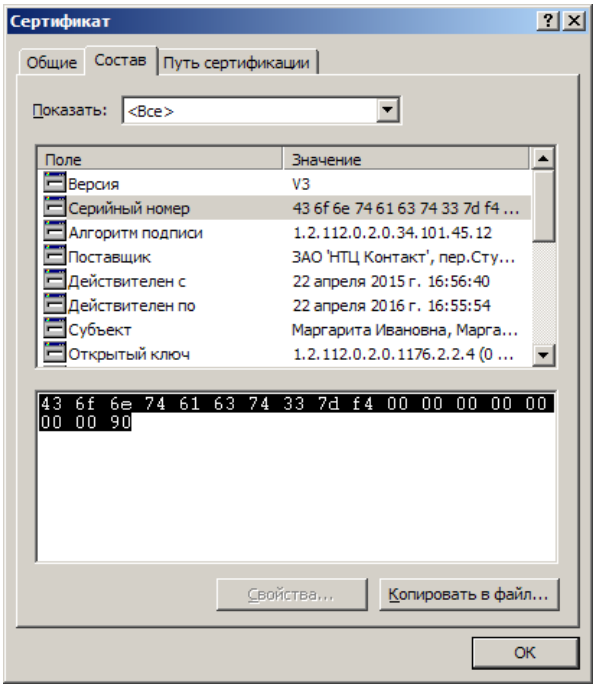

Рис. 45

6.2.5. Далее следует вернуться к окну «Выпуск заявки на отзыв сертификата» (рис. 42), поместить курсор в поле верхней строчки «Введите серийный номер отзываемого сертификата» и нажать комбинацию клавиш «Ctrl + V» на клавиатуре. В результате номер сертификата отобразиться в данной строчке (рис. 46).

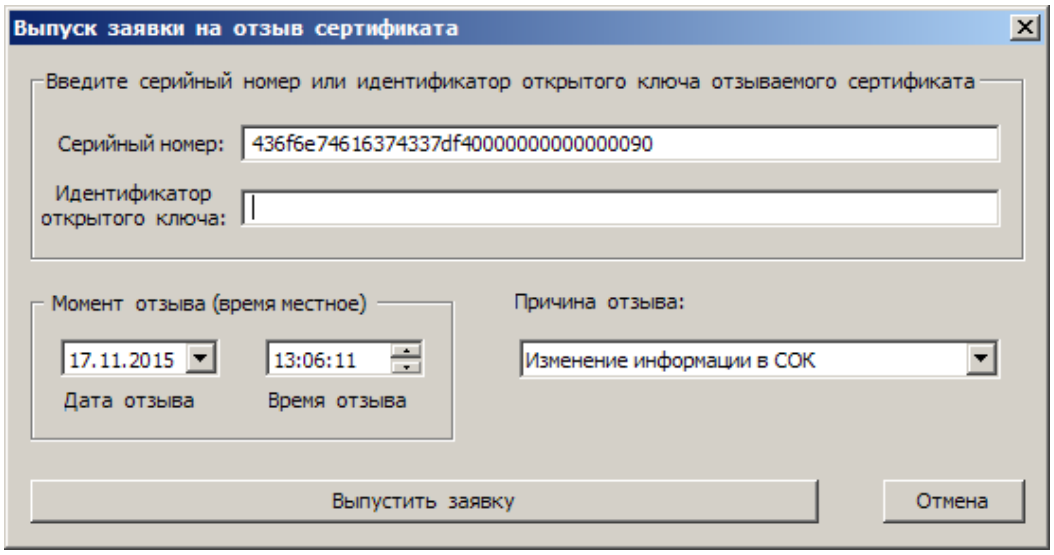

Рис. 46

6.2.6. После ввода серийного номера сертификата и нажатия клавиши «Enter» на клавиатуре в поле «Выбрать причину отзыва сертификата» необходимо выбрать соответствующую формулировку причины отзыва (рис. 47).

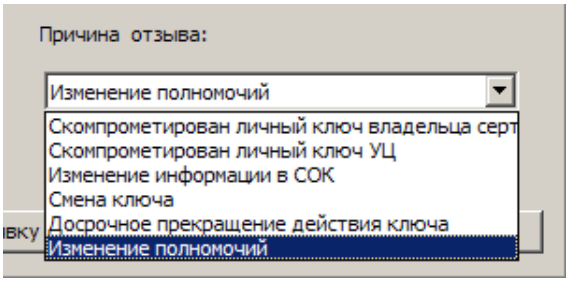

Рис. 47

6.2.7. Затем следует ввести в соответствующие поля значения времени отзыва и дату отзыва сертификата (по умолчанию используется текущие значения времени и даты) (рис. 48).

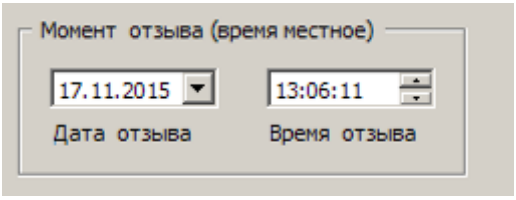

Рис. 48

6.2.8. Для выпуска заявки на отзыв СОК после ввода серийного номера сертификата, причины, времени и даты отзыва следует нажать кнопку «Выпустить заявку».

Если была нажата кнопка «Выпустить заявку» при пустых полях «Серийный номер» и «Идентификатор открытого ключа», то будет выдано сообщение-предупреждение (рис. 49).

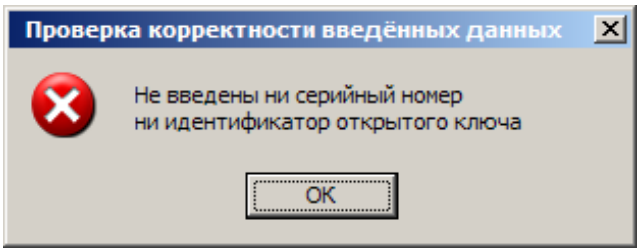

Рис. 49

При необходимости отмены формирования заявки на отзыв СОК, следует нажать кнопку «Отмена», при этом будет выведено сообщение как на рис. 50 и процедура формирования заявки на отзыв СОК будет прекращена.

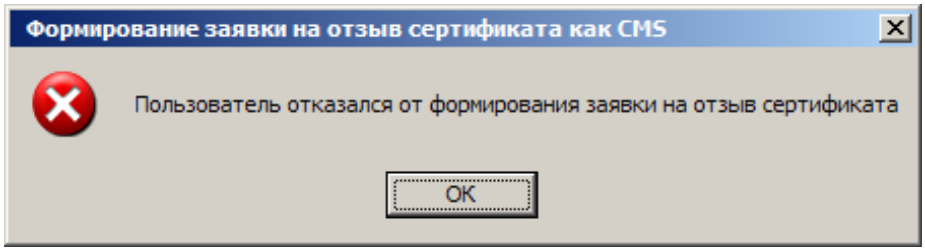

Рис. 50

6.2.9. После нажатия кнопки «Выпустить заявку», на экран будет выведена форма выбора личного ключа для подписи заявки (рис. 51).

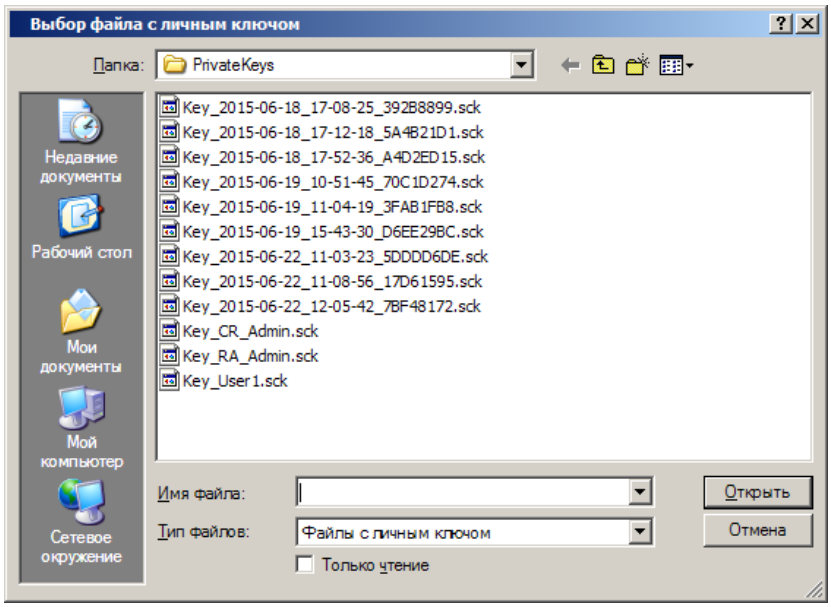

Рис. 51

Если в окне «Выбор файла с личным ключом» нажата кнопка «Отмена», то будет выведено сообщение как на рис. 52 и процедура выпуска заявки на отзыв СОК будет прекращена.

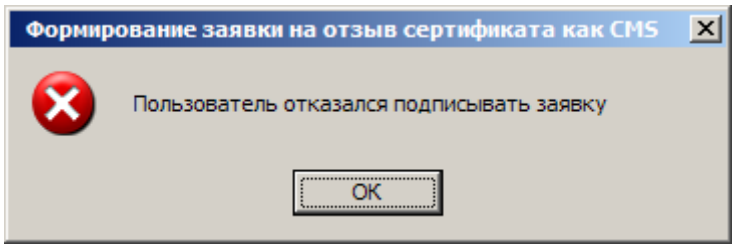

Рис. 52

После выбора личного ключа и нажатия кнопки «Открыть» необходимо ввести пароль к личному ключу (рис. 53).

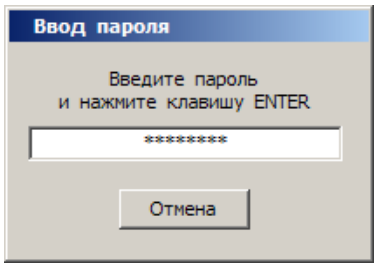

Рис. 53

При вводе неправильного пароля, будет выведено сообщение об ошибке (рис. 54) и процедура отзыва сертификата открытого ключа будет завершена.

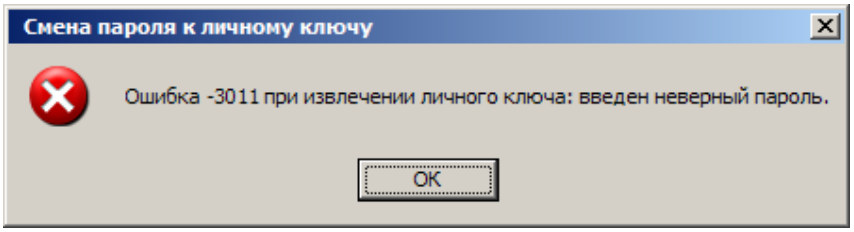

Рис. 54

6.2.10. После ввода правильного пароля будут выведены сообщения-подтверждения (рис. 55-58) и подписанная заявка будет сохранена на локальном диске.

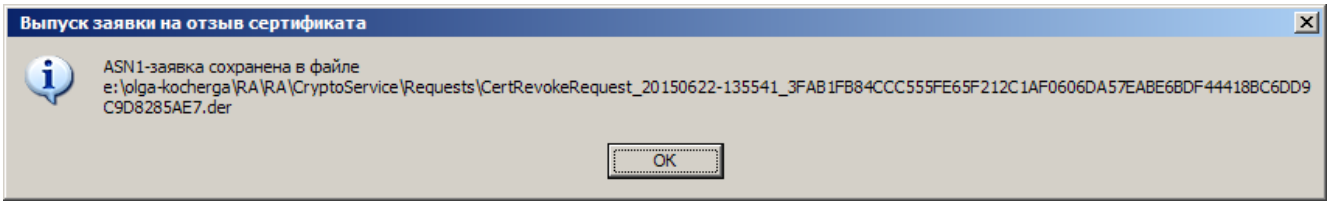

Рис. 55

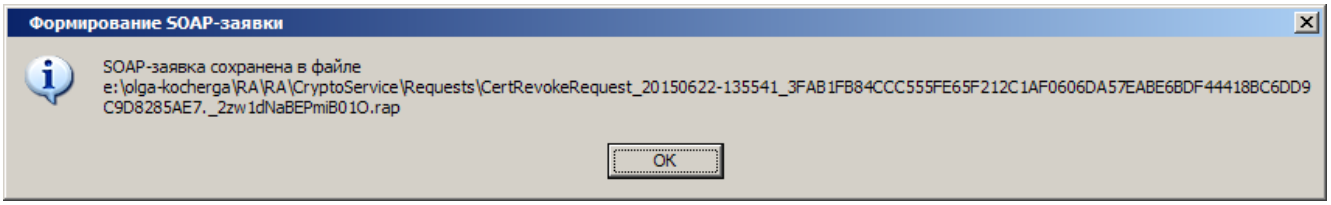

Рис. 56

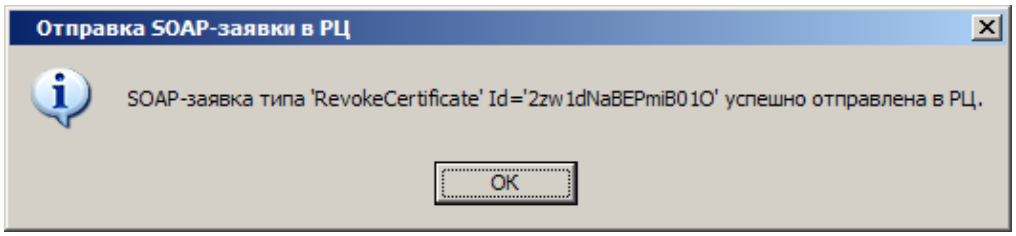

Рис. 57

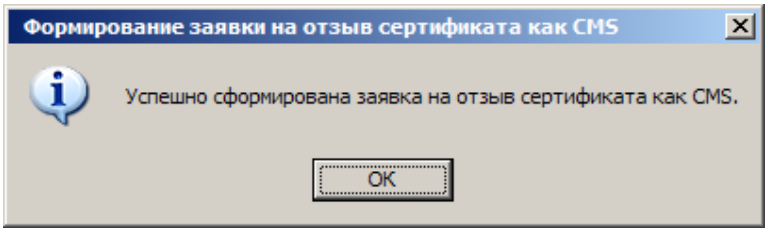

Рис. 58

Структуры SOAP-заявки и ответа приведены в приложении 1.

6.3. Приостановка действия сертификата открытого ключа

6.3.1. При создании заявки на приостановку СОК следует подвести курсор к иконке  и нажать на правую кнопку мыши. В правом нижнем углу будет высвечено меню как на рис. 59.

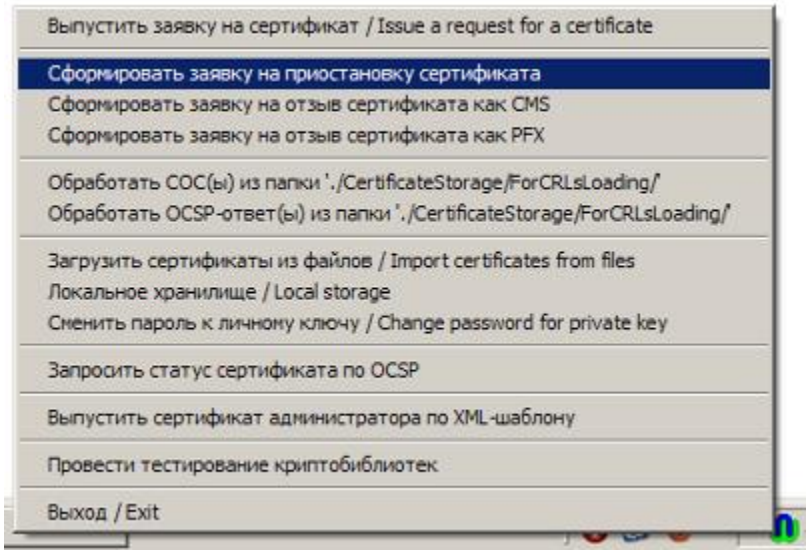

Рис. 59

6.3.2. После выбора пункта меню «Сформировать заявку на приостановку сертификата», на экран будет выведено окно «Выпуск заявки на приостановку сертификата», как это показано на рис. 60.

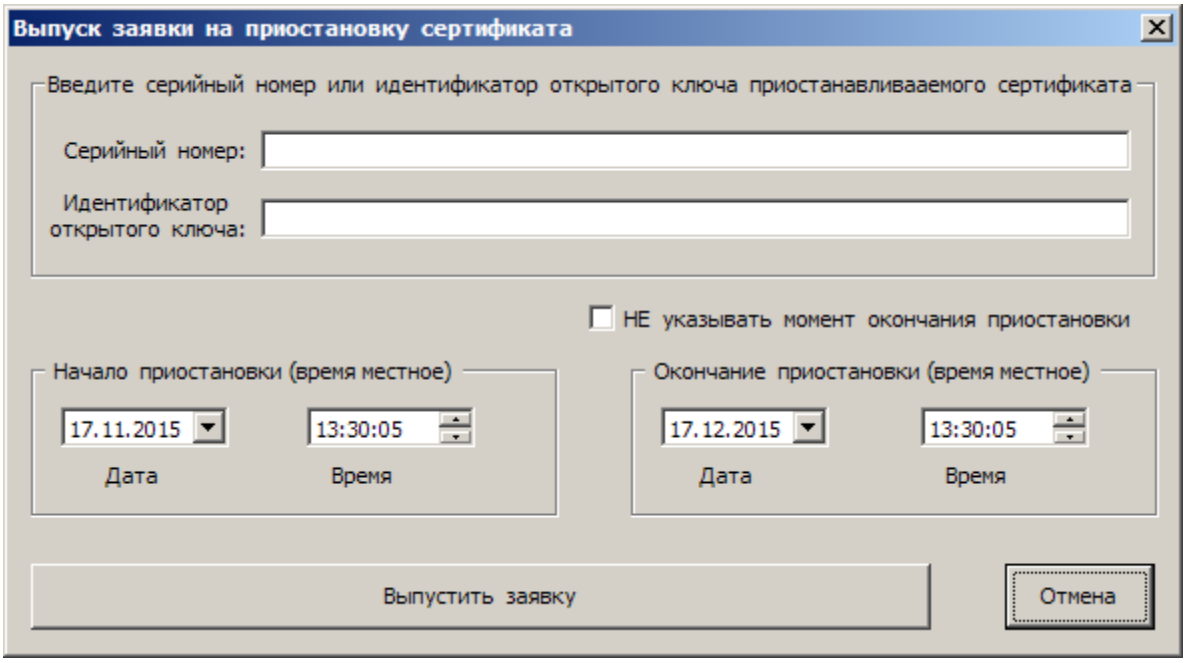

Рис. 60

6.3.3. Действия по формированию запроса на приостановку СОК полностью соответствуют действиям при его отзыве (п.п. 6.2.2 – 6.2.10 настоящего документа), за исключением того, что при приостановке не требуется вводить причину данного действия, но следует ввести время и дату начала и конца действия времени приостановки (рис. 60).

6.3.4. При необходимости отмены формирования заявки на приостановку сертификата, следует нажать кнопку «Отмена», при этом будет выведено сообщение как на рис. 61 и процедура формирования заявки на приостановку сертификата будет прекращена.

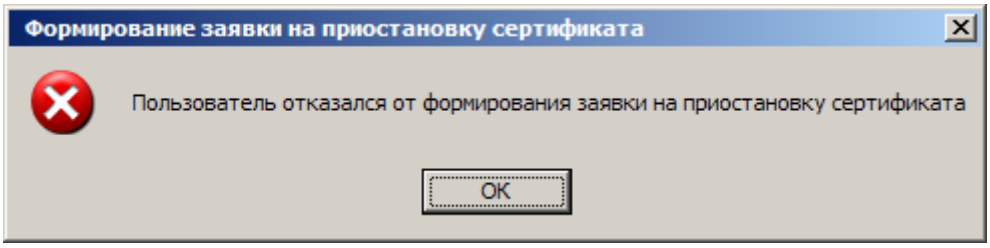

Рис. 61

Структуры SOAP-заявки и ответа приведены в приложении 1.

6.4. Ручная операция обработки списка отозванных сертификатов из файла

6.4.1. При ручной обработке списка отозванных сертификатов из файла, следует поместить файл списка отозванных сертификатов в рабочую директорию в папку CertificateStorage\ForCRLsLoading\, подвести курсор к иконке  и нажать на правую кнопку мыши. В правом нижнем углу будет высвечено меню как на рис. 62. После выбора пункта меню «Обработать СОС(ы) из папки './CertificatesStorage/ForCRLsLoading/'» файл списка отозванных

сертификатов будет обработан автоматически и будет выдано сообщение о результате обработки (рис. 63, 64).

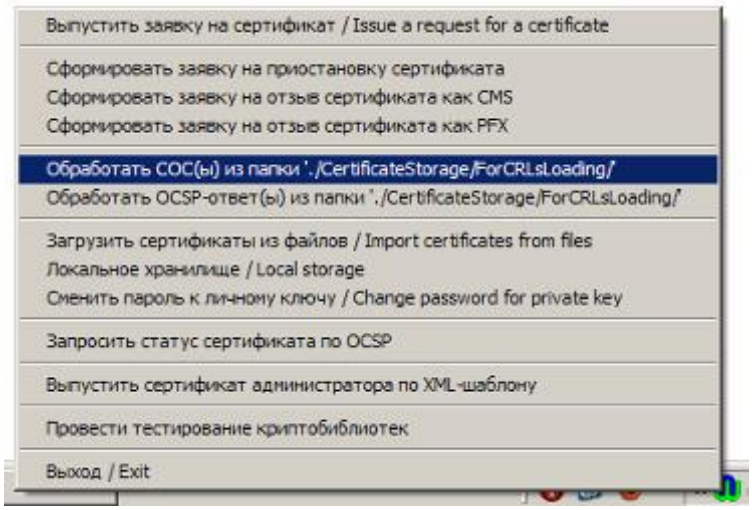

Рис. 62

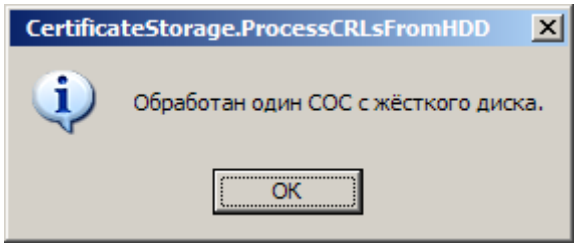

Рис. 63

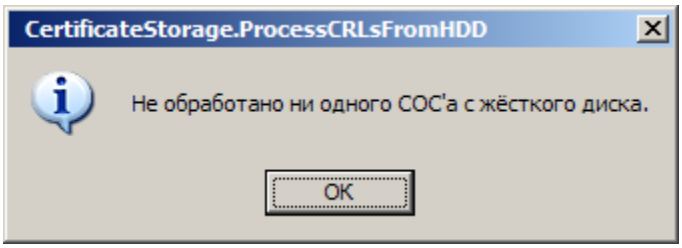

Рис. 64

6.5. Ручная операция обработки OCSP-ответов из файлов

6.5.1. При ручной обработке OCSP-ответов из файла, следует поместить файлы OCSP-ответов в рабочую директорию в папку CertificateStorage\ForCRLsLoading\, подвести курсор к иконке  и нажать на правую кнопку мыши. В правом нижнем углу будет высвечено меню как на рис. 65.

После выбора пункта меню «Обработать OCSP-ответ(ы) из папки './CertificatesStorage/ForCRLsLoading/'» файл OCSP-ответа будет обработан автоматически и будет выдано сообщение о результате обработки (рис. 66, 67).

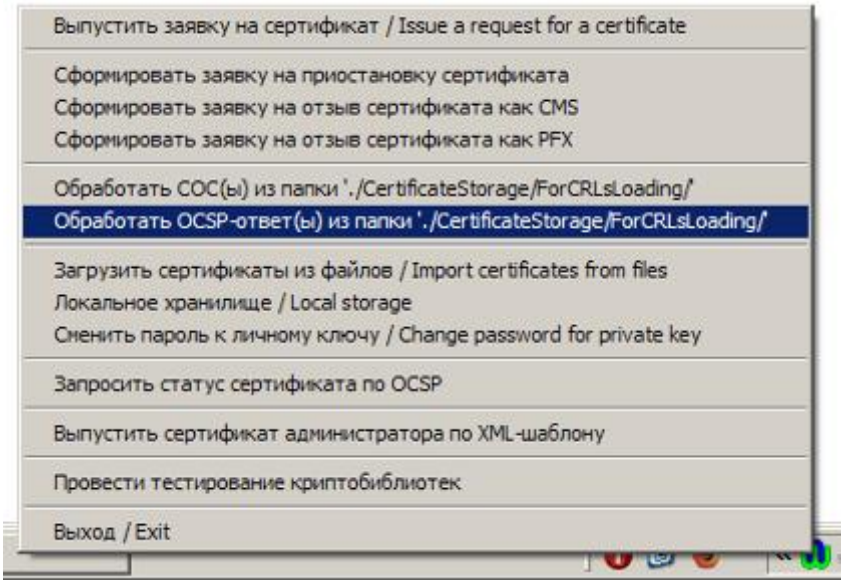

Рис. 65

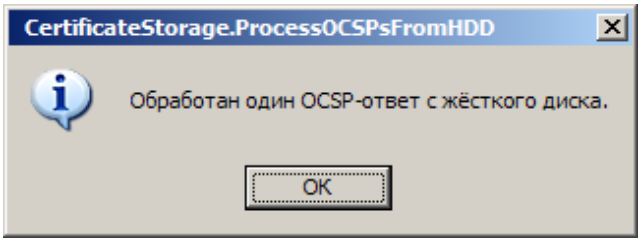

Рис. 66

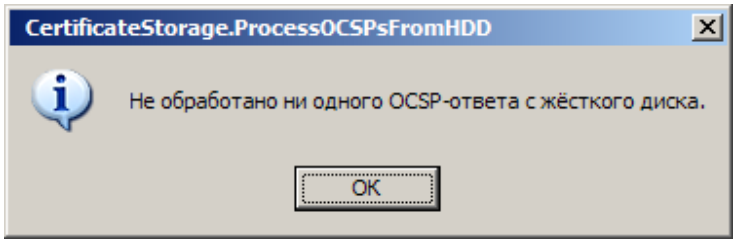

Рис. 67

6.6. Ручная операция загрузки сертификатов из файлов

6.6.1. При ручной загрузке сертификатов из файлов следует подвести курсор к иконке  и нажать на правую кнопку мыши. В правом нижнем углу будет высвечено меню как на рис. 68. Предварительно необходимо поместить сертификаты, которые будут подгружены в локальное хранилище, в рабочую директорию в папку CertificateStorage\ForCertificatesLoading.

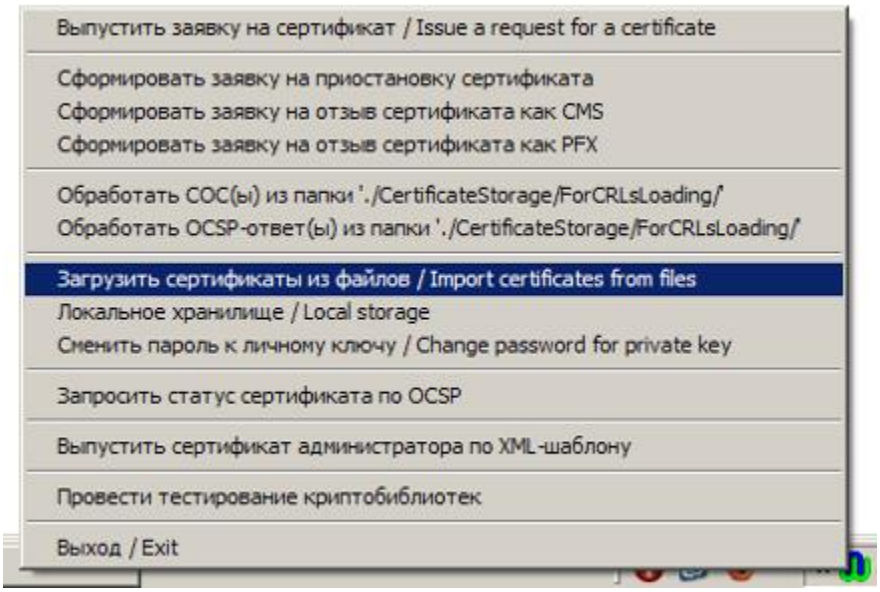

Рис. 66

6.6.2. После выбора пункта меню «Загрузить сертификаты / Import certificates from files» подгрузка сертификатов с жесткого диска будет произведена автоматически и будет выдано сообщение-подтверждение о количестве подгруженных сертификатов (рис. 69, 70).

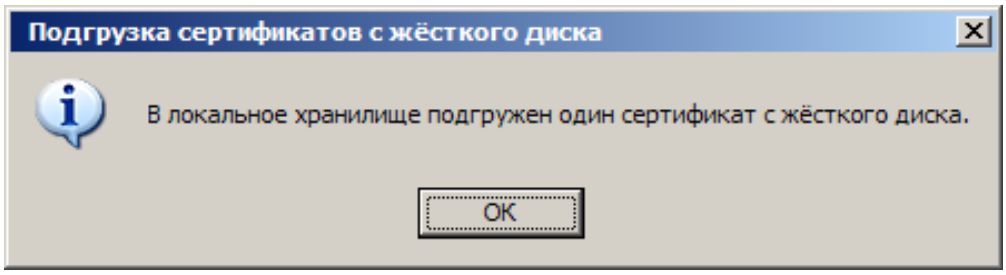

Рис. 69

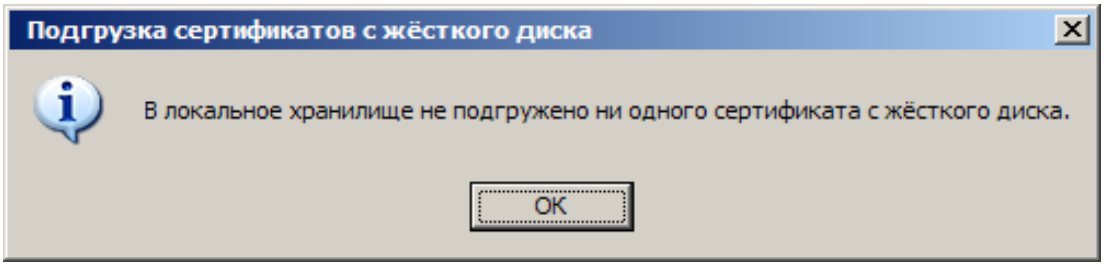

Рис. 70

6.7. Просмотр локального хранилища

6.7.1. Для просмотра локального хранилища сертификатов следует подвести курсор к иконке  и нажать на правую кнопку мыши. В правом нижнем углу будет высвечено меню как на рис. 71.

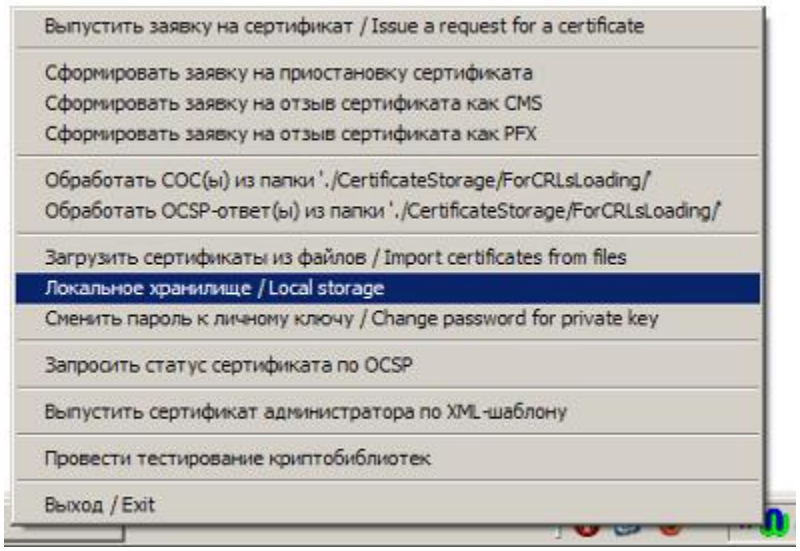

Рис. 71

6.7.2. После выбора пункта меню «Локальное хранилище / Local storage», на экран будет выведен перечень сертификатов, как это показано на рис. 72.

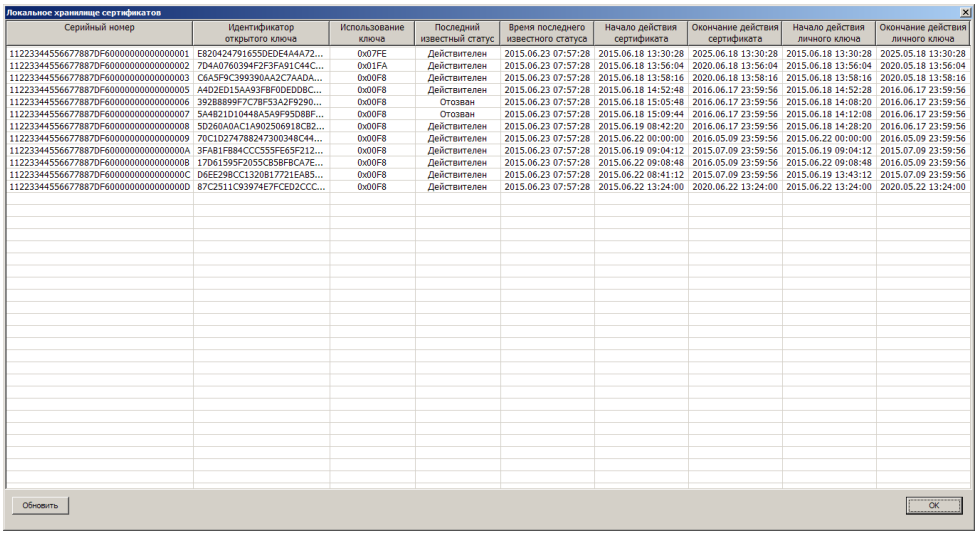

Рис. 72

6.7.3. Чтобы обновить локальное хранилище, необходимо нажать кнопку «Обновить». При нажатии на кнопку «ОК» локальное хранилище будет закрыто.

6.7.4. Если щелкнуть правой кнопкой мыши по интересующей записи, то появится контекстное меню (рис. 73). При желании, пользователь может просмотреть сертификат, копировать значение того поля, по которому щелкнул правой кнопкой мыши, или удалить выбранный сертификат из локального хранилища.

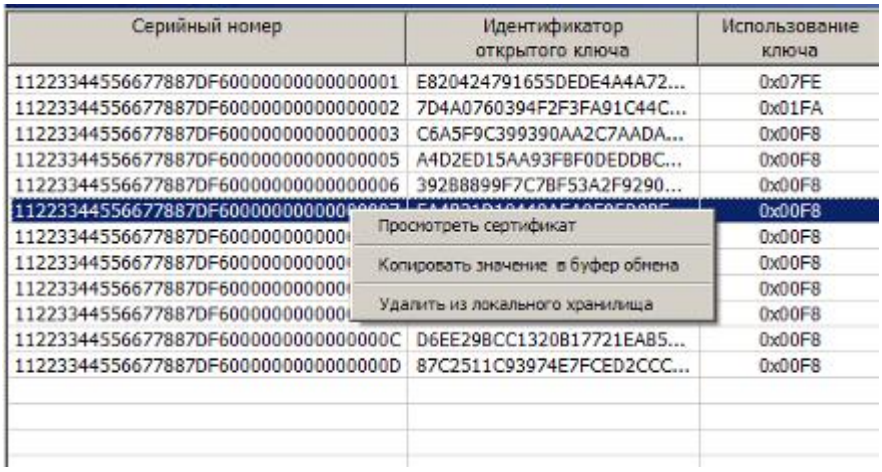

Рис. 73

6.7.5. После выбора пункта меню «Просмотреть сертификат», на экран будет выведено окно «Просмотр сертификата», как это показано на рис. 74.

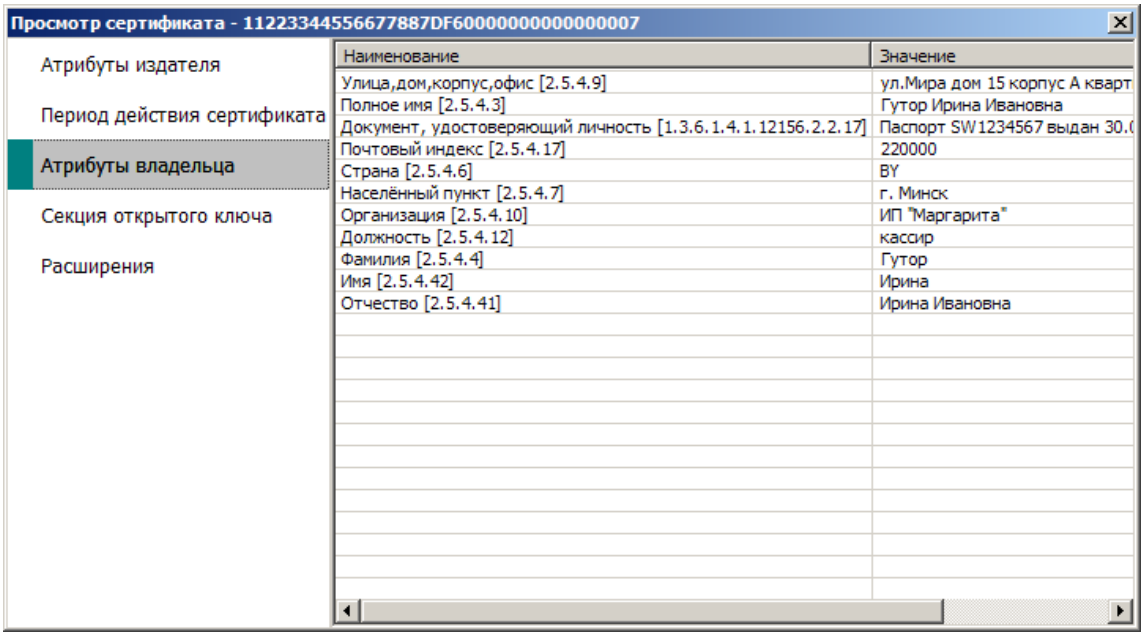

Рис. 74

6.7.6. В появившемся окне «Просмотр сертификата» имеется пять вкладок: «Атрибуты издателя», «Период действия сертификата», «Атрибуты владельца», «Секция открытого ключа» и «Расширения».

Вкладка «Атрибуты издателя» предоставляет информацию об общих сведениях об издателе сертификата – имя издателя, страна, населенный пункт, адрес, наименование организации (рис. 75).

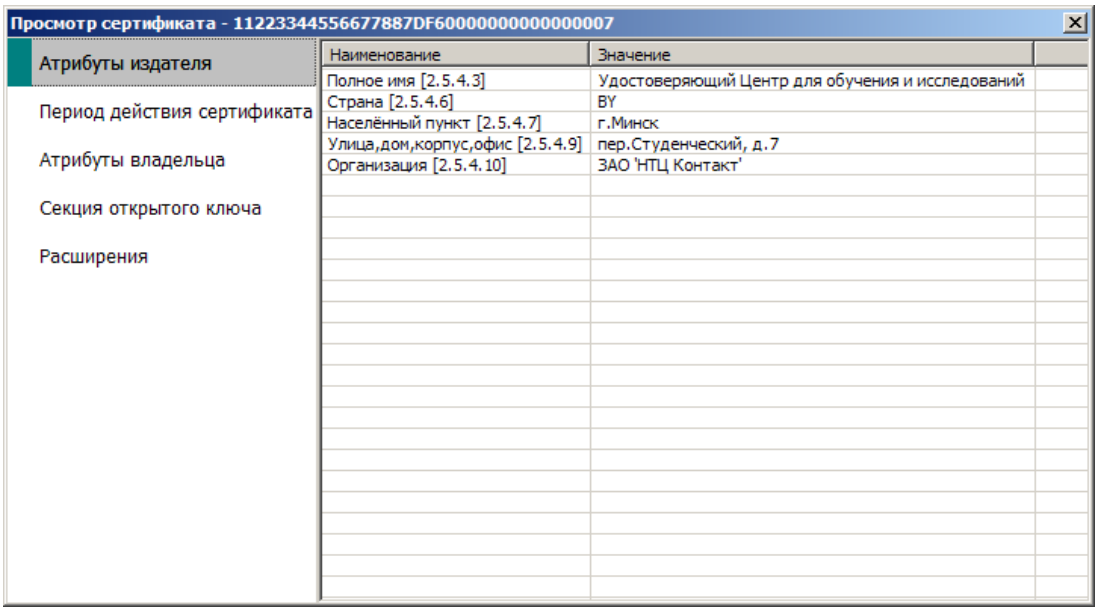

Рис. 75

Вкладка «Период действия сертификата» предоставляет информацию о времени начала и окончания действия сертификата (рис. 76).

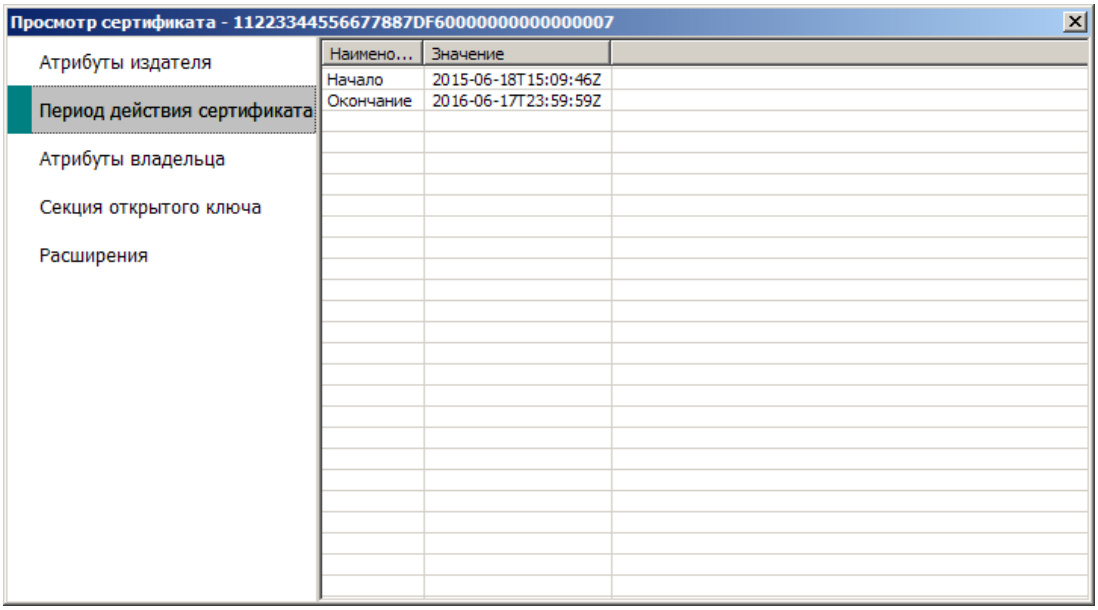

Рис. 76

Вкладка «Атрибуты владельца» предоставляет информацию об общих сведениях о владельце сертификата – имя владельца сертификата страна, населенный пункт, адрес и др. (рис. 77).

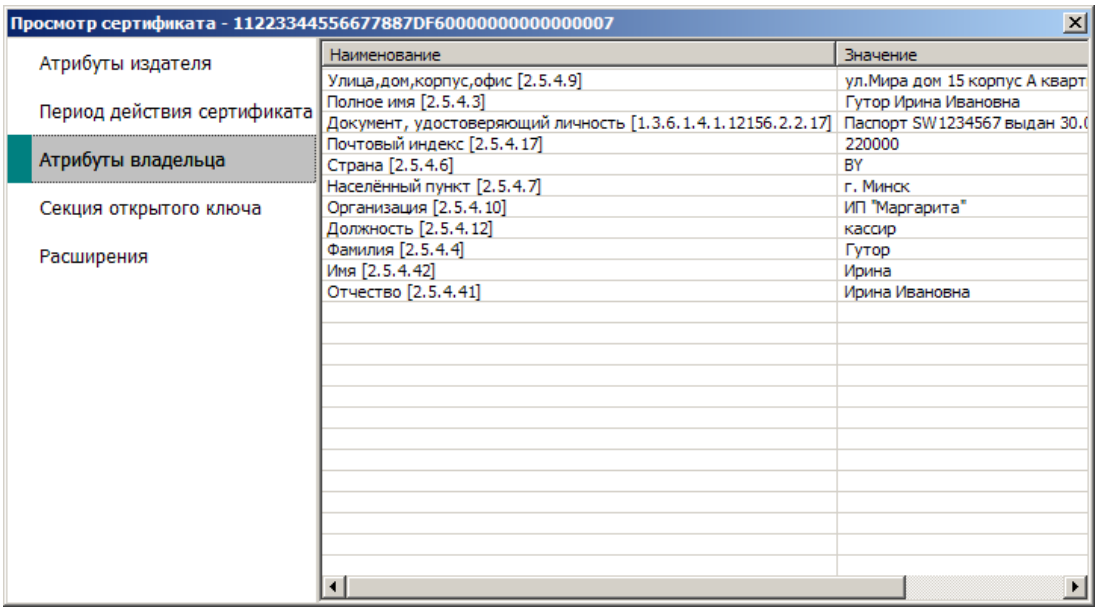

Рис. 77

Вкладка «Секция открытого ключа» предоставляет информацию об алгоритме, длине и значении открытого ключа (рис. 78).

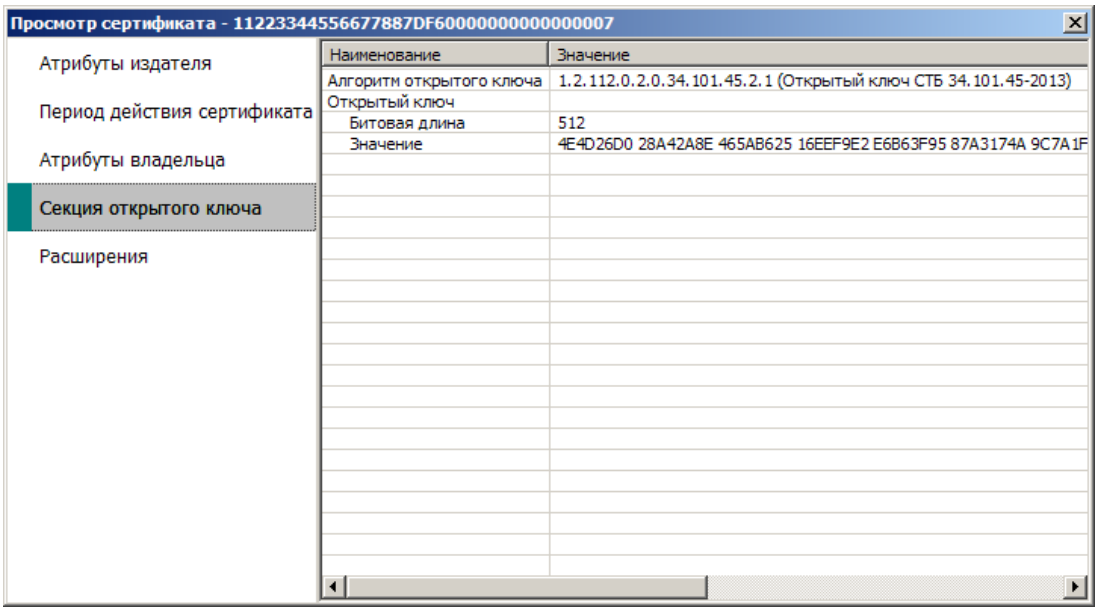

Рис. 78

Вкладка «Расширения» отображает дополнительную информацию (рис. 79).

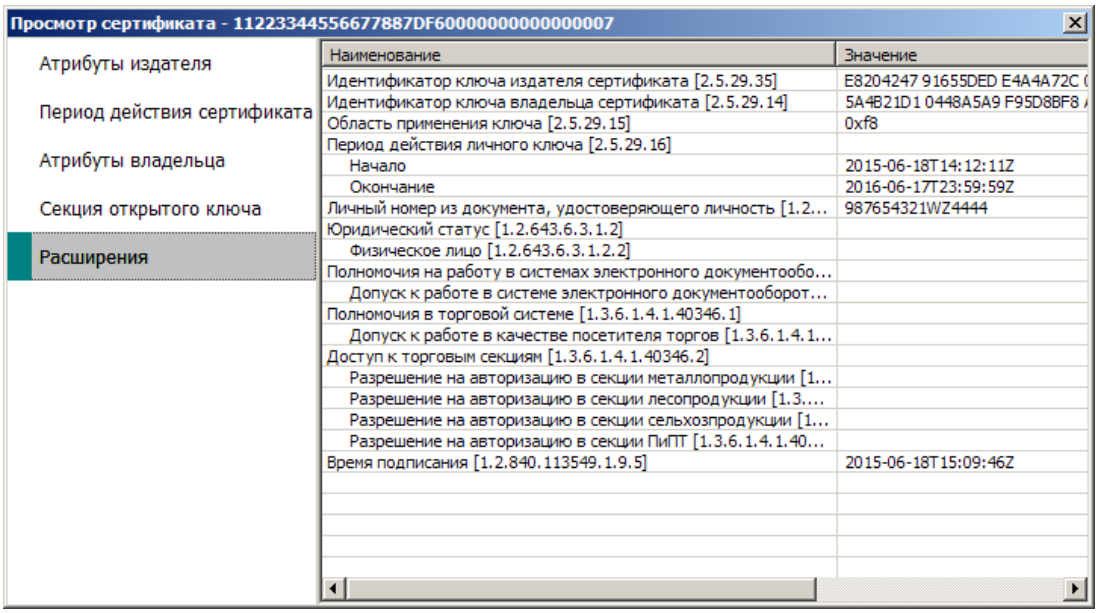

Рис. 79

6.8. Смена пароля к личному ключу

6.8.1. При смене пароля к личному ключу следует подвести курсор к иконке  и нажать на правую кнопку мыши. В правом нижнем углу будет высвечено меню как на рис. 80.

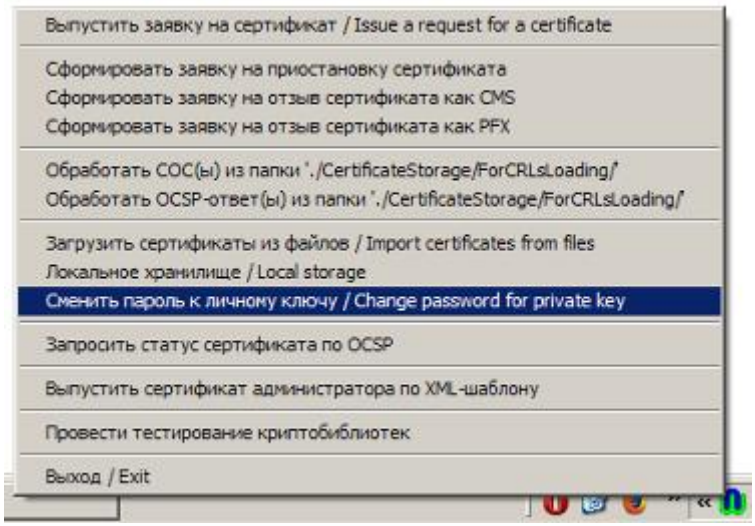

Рис. 80

6.8.2. После выбора пункта меню «Сменить пароль к личному ключу», на экран будет выведено окно «Выбор файла с личным ключом», как это показано на рис. 81, где необходимо выбрать файл с личным ключом, к которому требуется поменять пароль, и нажать кнопку «Открыть».

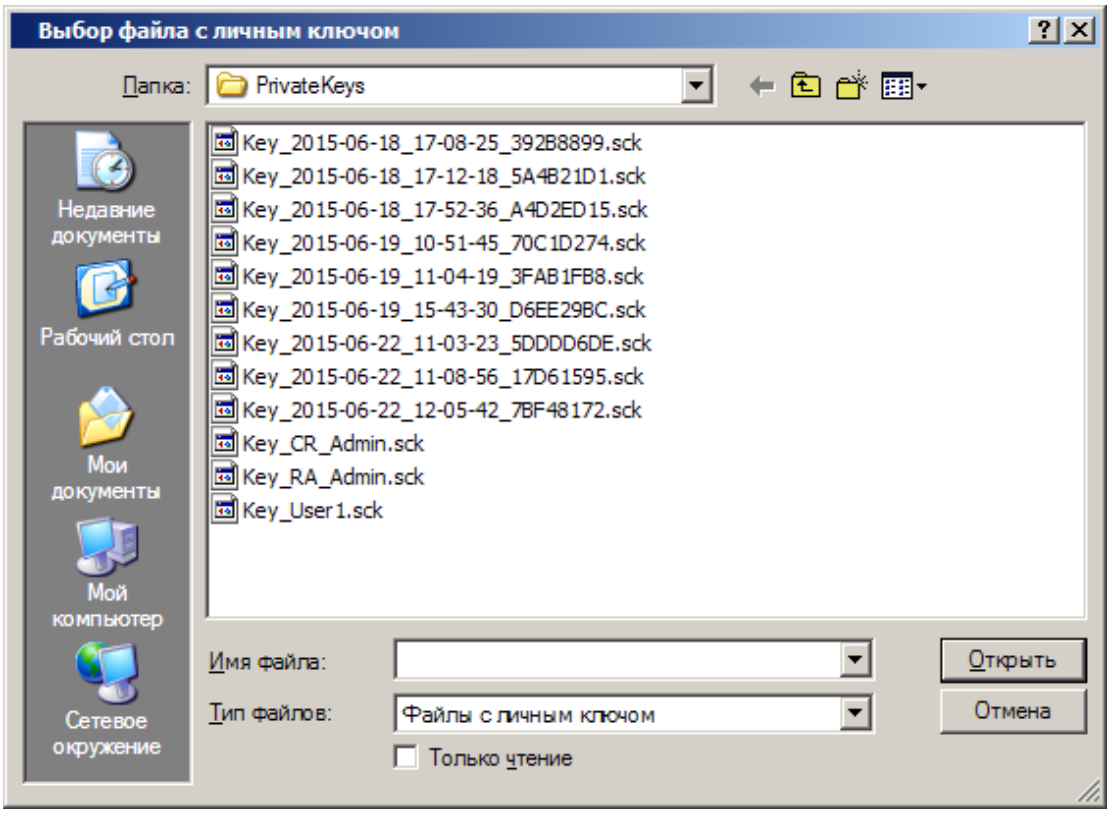

Рис. 81

Если на этапе выбора личного ключа была нажата кнопка «Отмена», то будет выдано сообщение как на рис. 82 и процедура смены пароля к личному ключу будет прекращена.

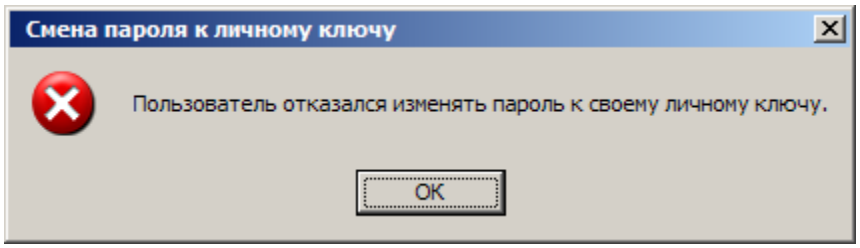

Рис. 82

6.8.3. После того как файл с личным ключом выбран и нажата кнопка «Открыть», на экран будет выведено окно для ввода пароля к личному ключу как на рис. 83.

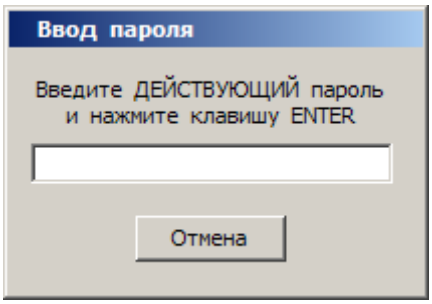

Рис. 83

При вводе неправильного пароля, будет выведено сообщение об ошибке (рис. 84) и процедура смены пароля к личному ключу будет завершена.

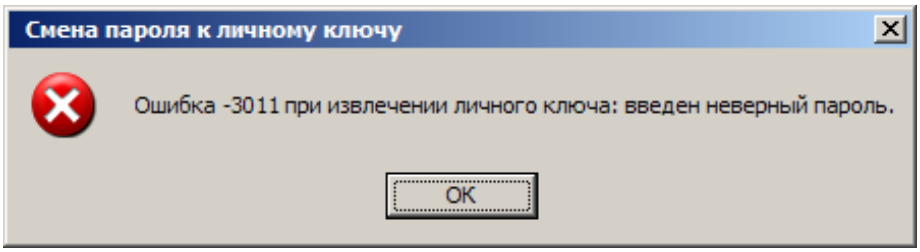

Рис. 84

Если на этапе ввода пароля к личному ключу была нажата кнопка «Отмена», то будет выдано сообщение как на рис. 85 и процедура смены пароля к личному ключу будет завершена.

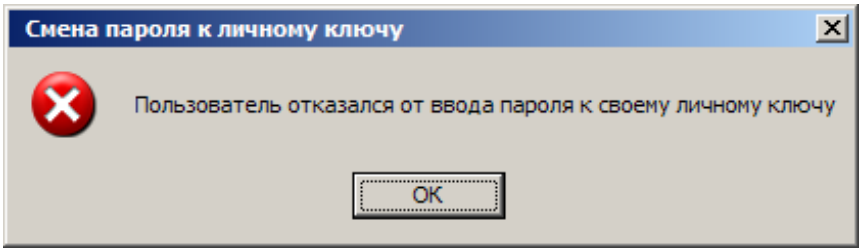

Рис. 85

6.8.4. Если пароль к личному ключу введен правильно, на экран будет выведено окно для ввода нового пароля к личному ключу с подтверждением (рис. 86). Минимальная длина нового пароля составляет 8 символов. Если пароль состоит менее чем из 8 символов, то после ввода пароля и нажатия кнопки «Enter» будет выдано предупреждении (рис. 87). Количество попыток ввода пароля неограниченно.

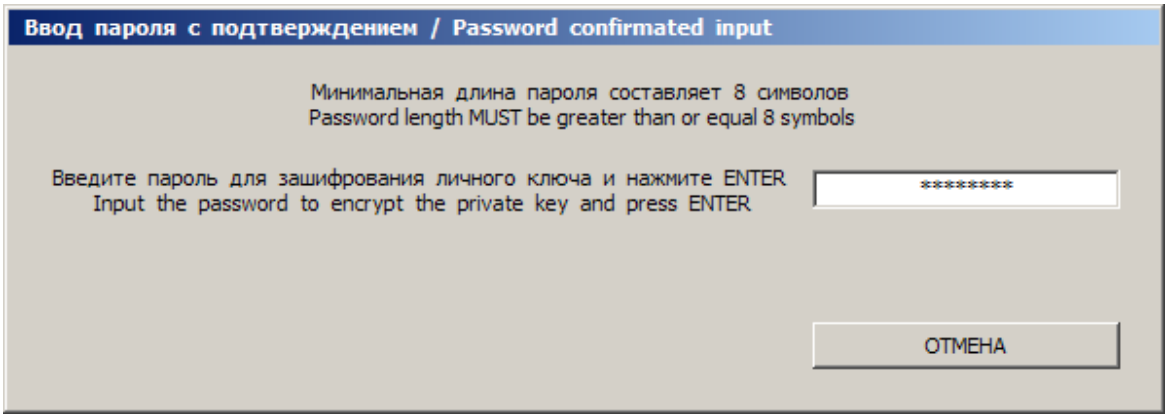

Рис. 86

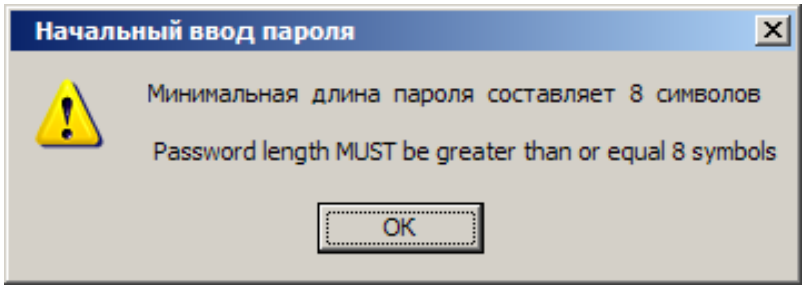

Рис. 87

Если подтверждение пароля не совпало с введенным паролем, то будет выдано предупреждение как на рис. 88.

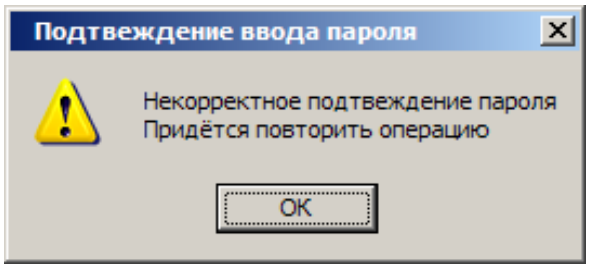

Рис. 88

Если на этапе ввода нового пароля с подтверждением была нажата кнопка «Отмена», то будет выдано сообщение как на рис. 89 и процедура смены пароля к личному ключу будет завершена.

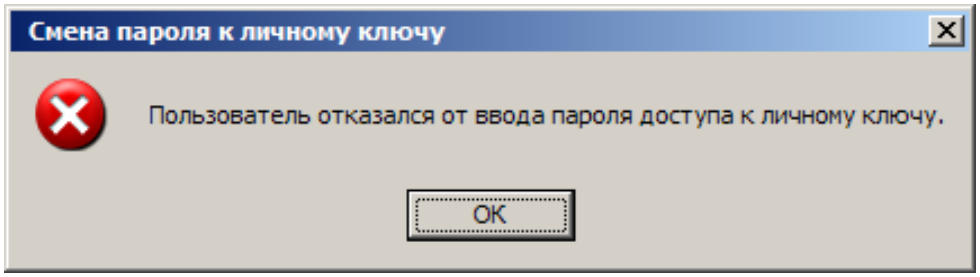

Рис. 89

6.8.5. В случае корректного ввода нового пароля с подтверждением будет выведено сообщение о смене пароля к личному ключу (рис. 90).

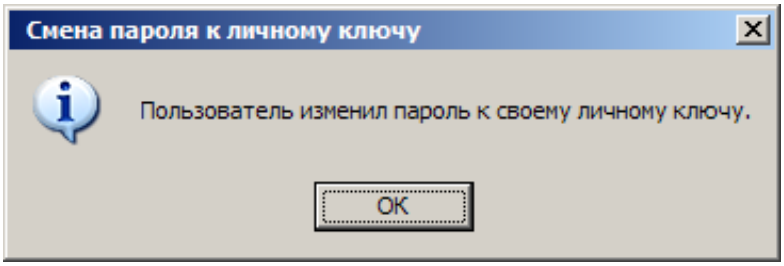

Рис. 90

6.9. Запрос статуса сертификата по OCSP

6.9.1. При запросе статуса сертификата по OSCP следует подвести курсор к иконке  и нажать на правую кнопку мыши. В правом нижнем углу будет высвечено меню как на рис. 91.

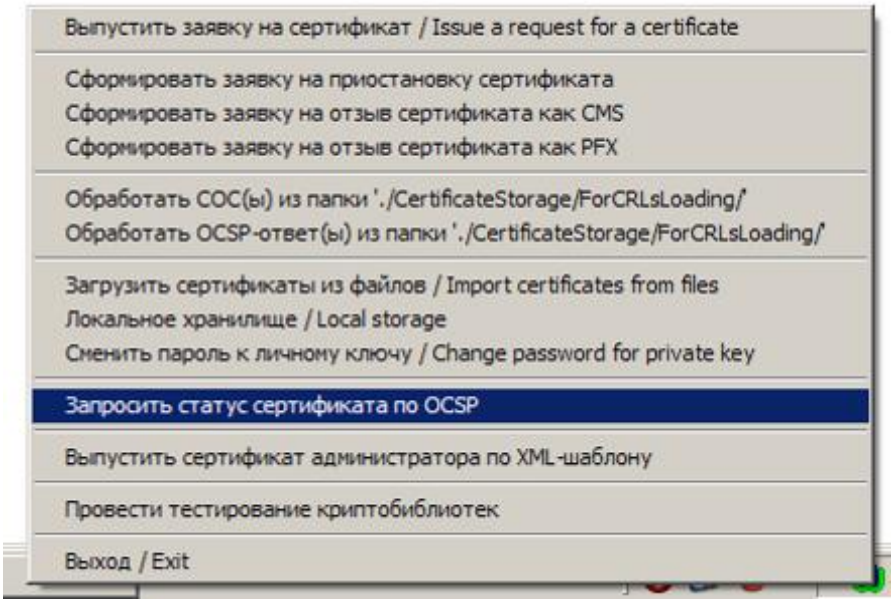

Рис. 91

6.9.2. После выбора пункта меню «Запросить статус сертификата по OCSP», на экран будет выведено окно «Запрос статуса сертификата(ов) по OCSP», как это показано на рис. 92.

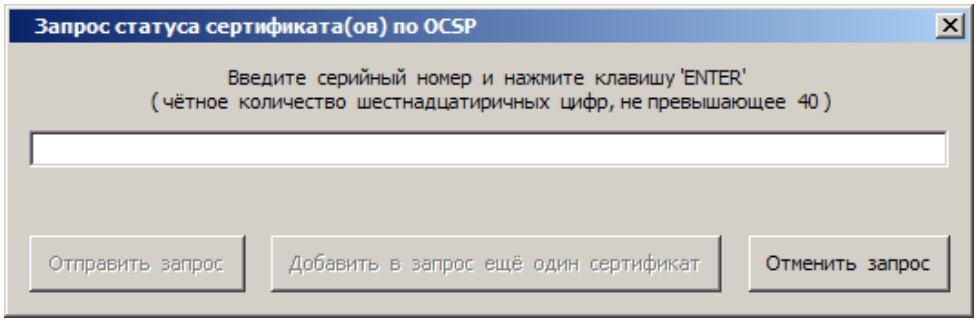

Рис. 92

В окне «Запросить статус сертификата(ов) по OCSP» в текстовое поле необходимо ввести серийный номер сертификата, статус которого требуется узнать, и нажать клавишу «Enter». Получение серийного номера соответствует действиям, описанным в п.п. 6.2.3 – 6.2.4 настоящего документа.

При нажатии на кнопку «Отменить запрос» диалоговое окно «Запросить статус сертификата(ов) по OCSP « будет закрыто и процедура запроса статуса СОК по OCSP будет завершена.

6.9.3. После ввода серийного номера сертификата и нажатия клавиши «Enter», становятся доступны кнопки «Оправить запрос», «Добавить в запрос ещё один сертификат» (рис. 93).

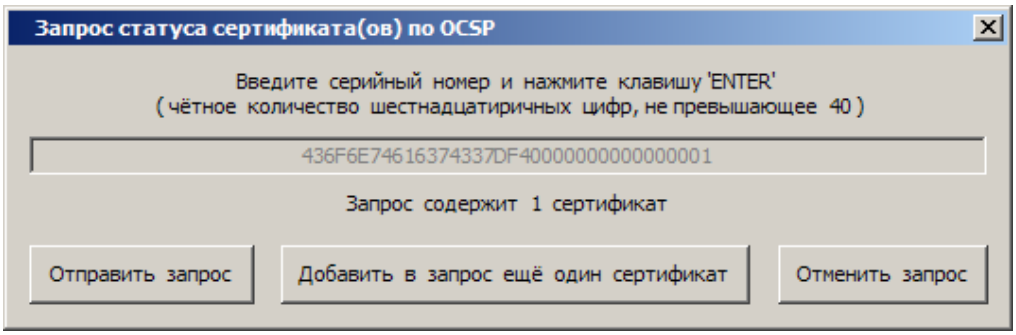

Рис. 93

6.9.3.1. Для добавления в запрос еще одного сертификата нужно нажать на кнопку «Добавить в запрос ещё один сертификат» (рис. 93), в текстовое поле ввести серийный номер и нажать клавишу «Enter» (рис. 94, 95).

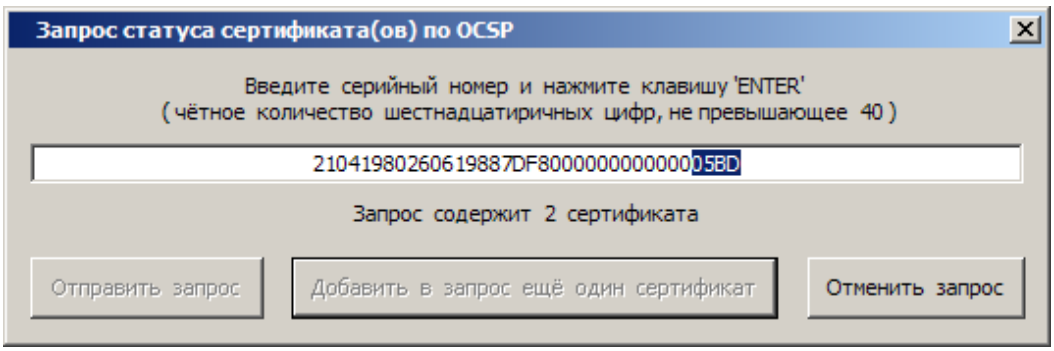

Рис. 94

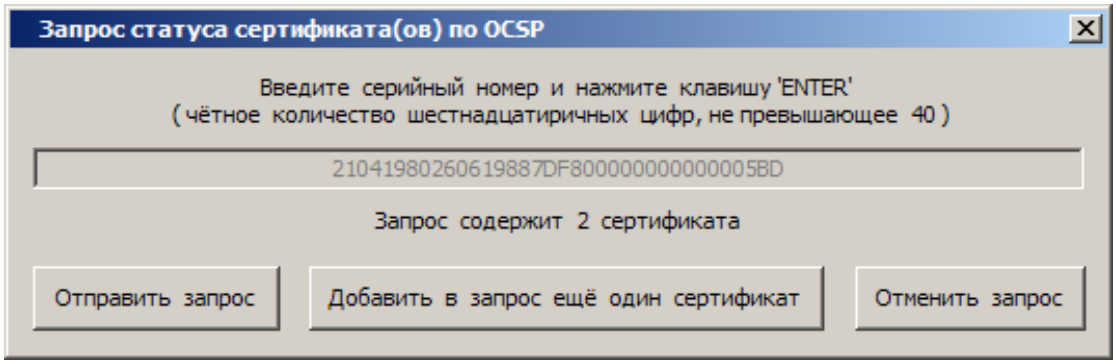

Рис. 95

Если в текстовое поле был введен серийный номер сертификата, который отсутствует в локальном хранилище, то будет выдано сообщение как на рис. 96.

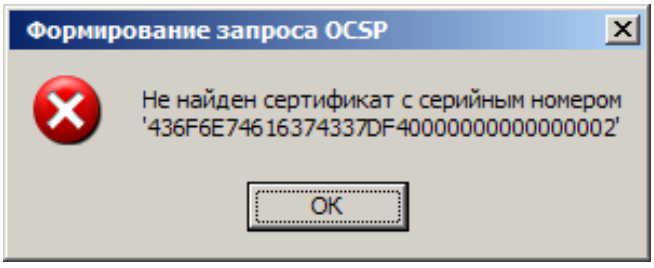

Рис. 96

Если в текстовое поле был введен серийный номер сертификата, который уже добавлен в запрос, то будет выдано сообщение-предупреждение как на рис. 97.

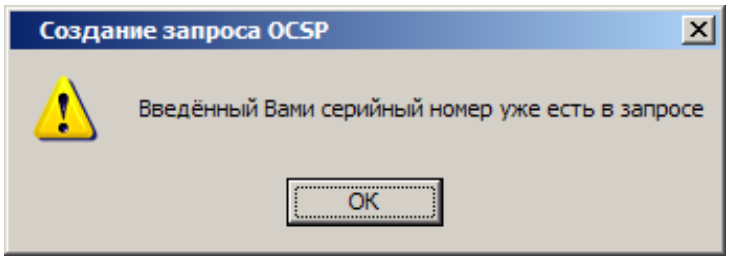

Рис. 97

6.9.3.2. Для отправки запроса необходимо нажать кнопку «Отправить запрос» (рис. 91), после чего будет выдано сообщение о формировании OCSP-запроса с указанием пути, где сохранен файл OCSP-запрос (рис. 98).

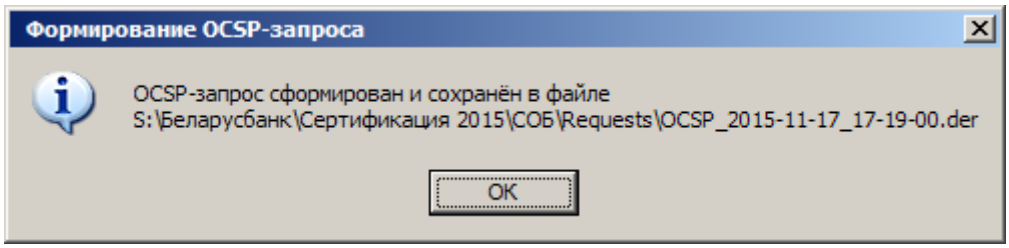

Рис. 98

6.10. Выпуск сертификата открытого ключа для администратора по XML-шаблону

6.10.1. Процедура позволяет выпустить СОК администратора КП РЦ или КПА УЦ.

6.10.2. Перед началом процедуры выпуска сертификата открытого ключа для администратора необходимо настроить шаблон, содержащий информацию о выпускаемом СОК. Настройка XML-шаблона осуществляется путем внесения изменений в текстовый файл с расширением *.xml. Внесение изменений в файл может быть произведено любым тестовым редактором. Пример структуры XML-шаблона для выпуска СОК для администратора указан в приложении 3.

Основными параметрами XML-шаблона для выпуска СОК для администратора являются следующие параметры:

1) В секции Subject XML-шаблона для выпуска СОК для администратора в тегах с произвольным названием перечисляется информация, которая будет помещена в секцию Subject СОК для администратора. Тип атрибута секции Subject СОК для администратора указывается в атрибуте OId XML-шаблона, а значение атрибута секции Subject СОК — в атрибуте Value XML-шаблона.

2) В секции PublicKeyAlgorithm должны быть указаны следующие значения объектного

идентификатора алгоритма и уровня криптостойкости:

а) в атрибуте OId – 1.2.112.0.2.0.34.101.45.2.1;

б) в атрибуте CryptoLevel – 128;

Ключевая пара для администратора генерируется только по СТБ 34.101.45 с уровнем криптостойкости 128 используя стандартные долговременные параметры.

3) В секции KeyUsageFlags в атрибутах с помощью значений «True» или «False» указывается, будет ли установлен соответствующий бит в расширении KeyUsage (область применения ключа);

4) В секции CertificateDuration указывается период действия выпускаемого СОК:

а) в атрибуте Unit – единицы измерения (месяц, год);

б) в атрибуте Value – период действия;

5) В секции PrivateKeyDuration указывается период действия личного ключа для администратора:

а) в атрибуте Unit – единицы измерения (месяц, год);

б) в атрибуте Value – период действия.

6.10.3. Для выпуска сертификата открытого ключа для администратора по XML-шаблону следует подвести курсор к иконке  и нажать на правую кнопку мыши. В правом нижнем углу будет высвечено меню как на рис. 99.

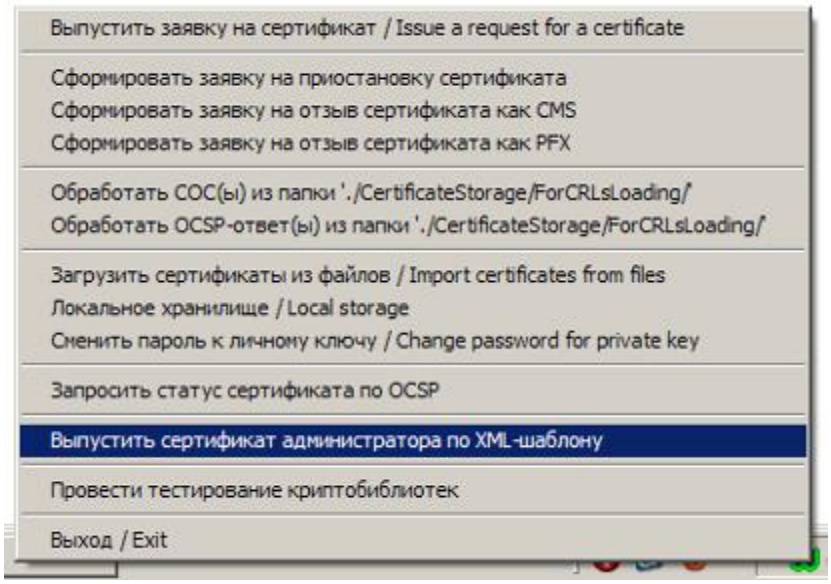

Рис. 99

6.10.4 После выбора пункта меню «Выпустить сертификат администратора по XML-шаблону» на экран будет выведено окно «Ввод пароля», в которое необходимо ввести пароль к корневому личному ключу КПА УЦ (рис. 100).

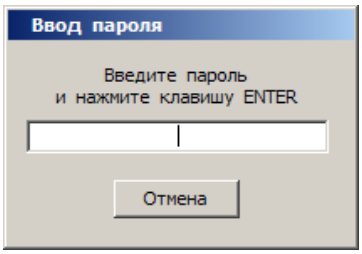

Рис. 100

При вводе неправильного пароля, будет выведено сообщение об ошибке (рис. 101) и процедура выпуска сертификата администратора по XML-шаблону будет завершена.

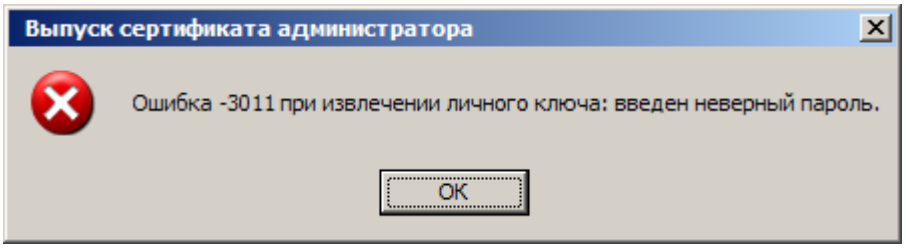

Рис. 101

Далее необходимо указать XML-шаблон, на основании которого будет выпущен сертификат (рис. 102).

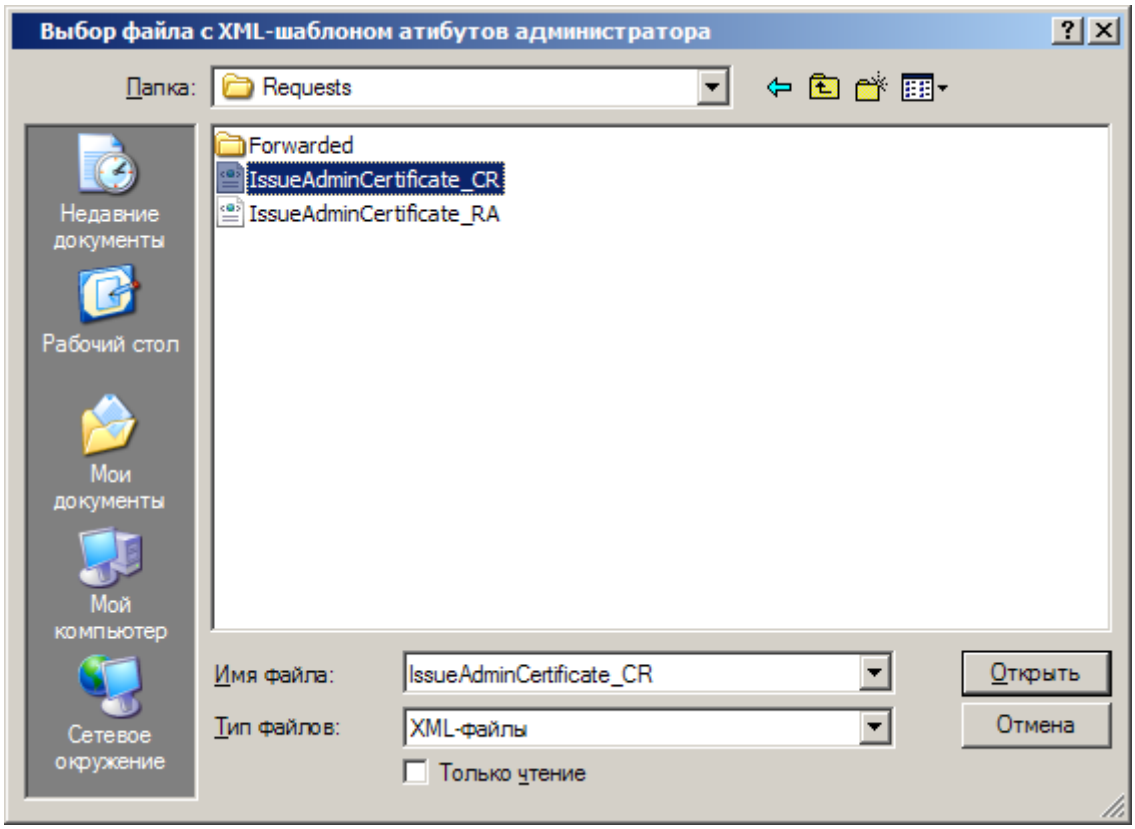

Рис. 102

После выбора XML-шаблона появится окно для ввода пароля к личному ключу и подтверждения пароля (рис. 103). Минимальная длина пароля составляет 8 символов.

Подтверждение пароля должно полностью совпадать с введенным паролем. Количество попыток ввода пароля неограниченно.

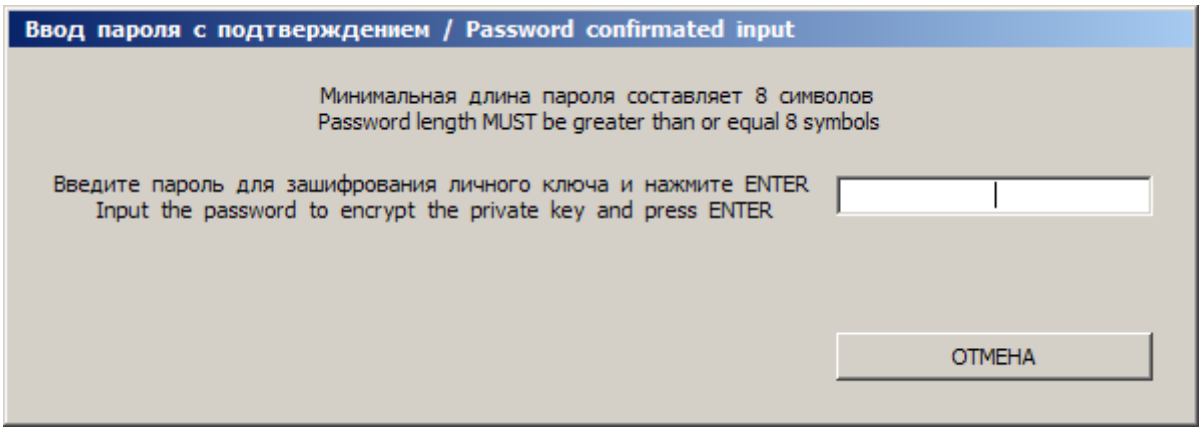

Рис. 103

Далее в диалоговом окне «Выбор имени файла для сохранения личного ключа» нужно выбрать, где будет сохранен файл с личный ключ, и по необходимости изменить имя файла, содержащего личный ключ (рис. 104).

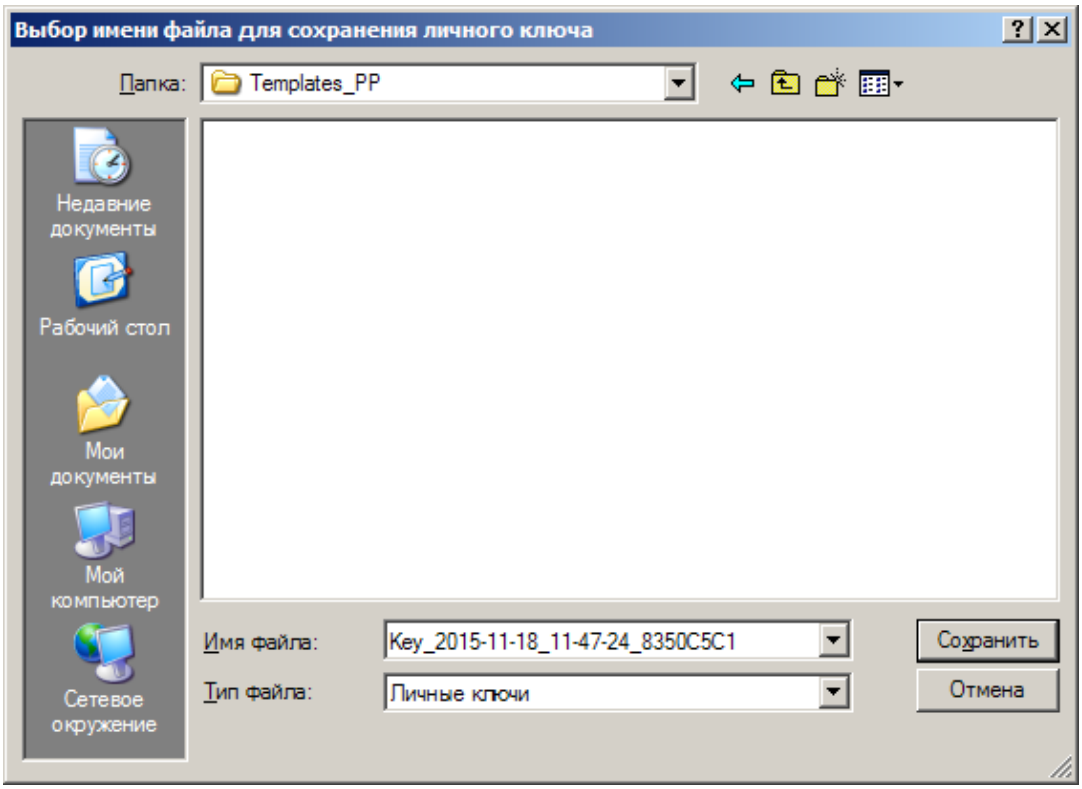

Рис. 104

После сохранения файла с личным ключом будет сформирована карточка открытого ключа и выведено сообщение с именем карточки и предложением о ее редактировании (рис. 105). Карточка открытого ключа сохраняется в рабочей директории в папке PublicKeyCards и имеет расширение .rtf.

Чтобы просмотреть и/или редактировать карточку открытого ключа, необходимо нажать

кнопку «Да», в результате чего карточка открытого ключа будет выведена на экран монитора (рис. 106).

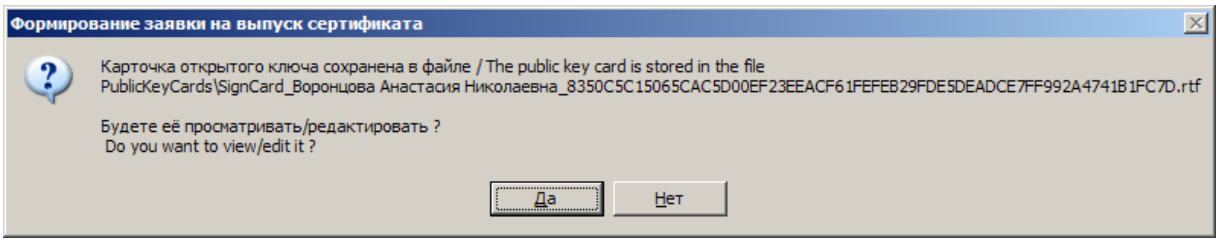

Рис. 105

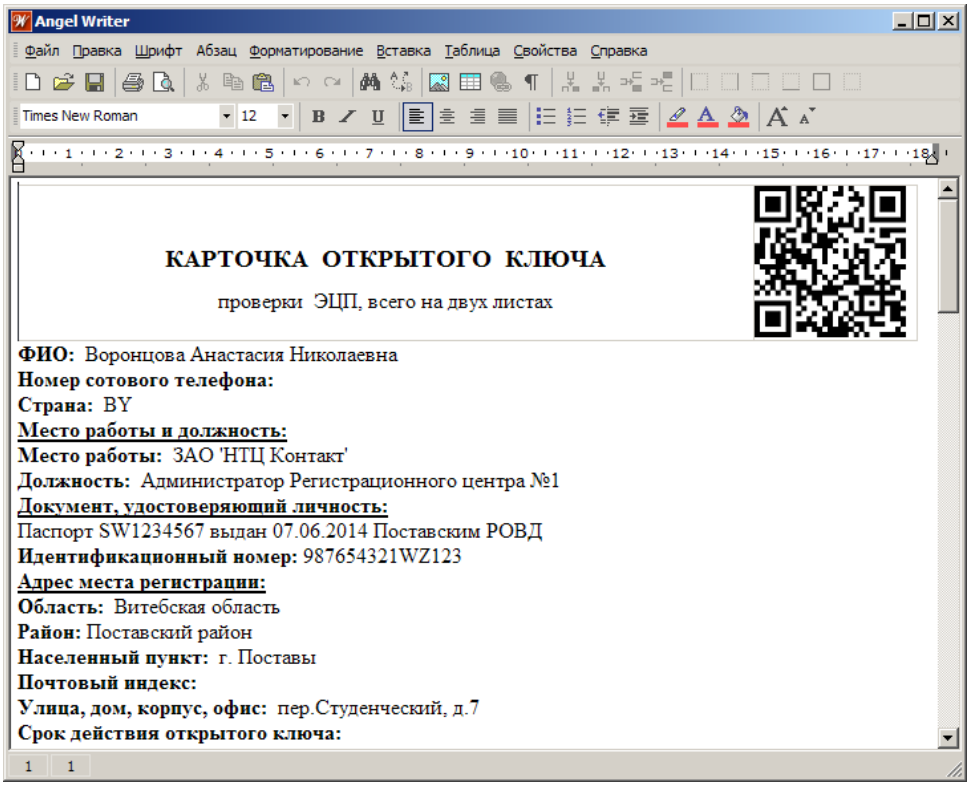

Рис. 106

В результате успешного завершения процедуры выпуска сертификата администратора по XML-шаблону, будет выдано сообщение как на рис. 107.

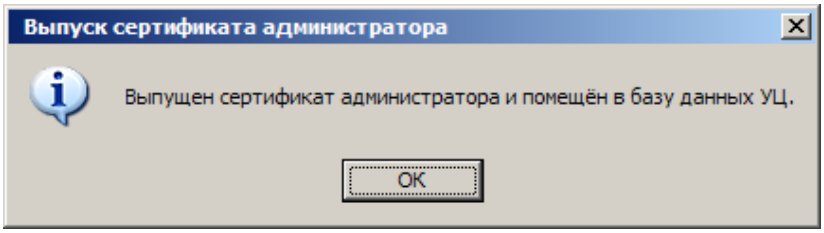

Рис. 107

Когда в рабочей директории по пути PublicKeyCards\Templates не найден соответствующий шаблон для карточки открытого ключа, будут выданы сообщения об ошибках (рис. 108-110) и карточка открытого ключа не будет сформирована.

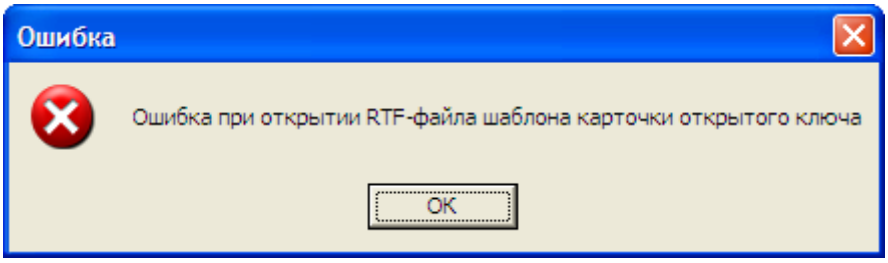

Рис. 108

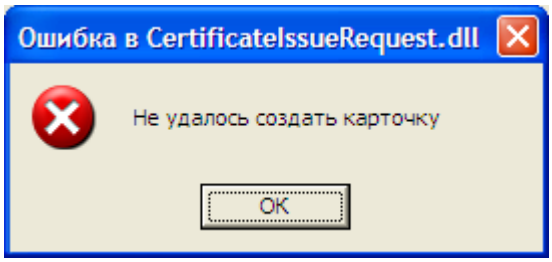

Рис. 109

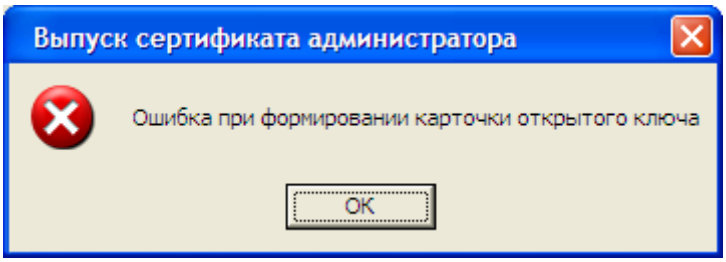

Рис. 110

6.11. Проверка целостности и тестирование криптобиблиотек

Внимание: перед проведением проверки целостности и тестирования криптобиблиотек следует завершить работу всех модулей КП СОБ кроме программы CryptoService_41.

6.11.1. Для проверки целостности и тестирования криптобиблиотек следует подвести курсор к иконке  и нажать на правую кнопку мыши. В правом нижнем углу будет высвечено меню как на рис. 111. Перед запуском проверки целостности и тестирования криптобиблиотек все модули КП СОБ должны быть закрыты (кроме CryptoService_41).

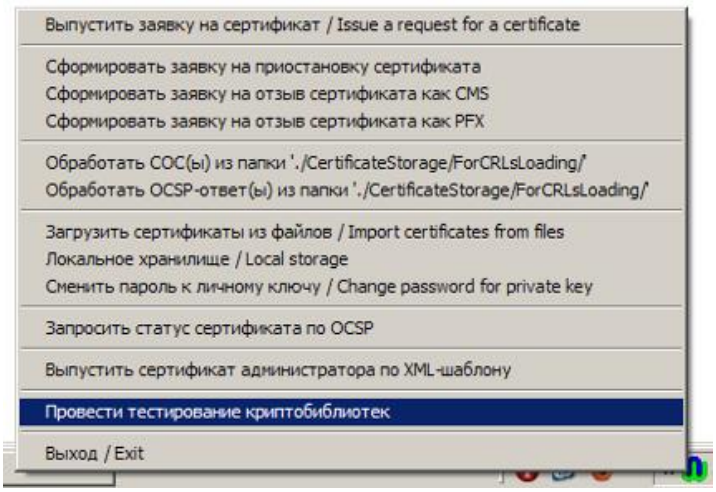

Рис. 111

После выбора пункта меню «Провести тестирование криптобиблиотек» тестирование будет проведено автоматически и выдано сообщение о результате тестирования (рис. 112, 113). В результате успешного тестирования в рабочей директории КП СОБ будет создан файл Integrity.testing, который будет содержать посчитанные контрольные характеристики контролируемых файлов. Если при тестировании выявлены ошибки, то КП СОБ завершит работу.

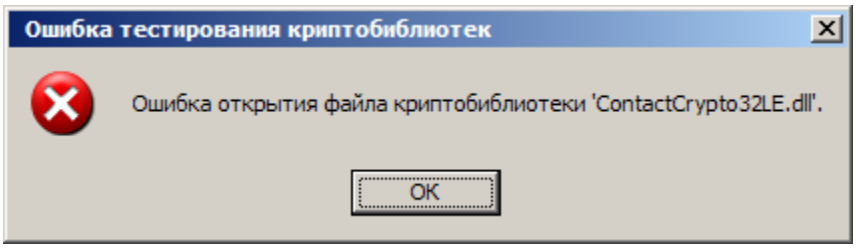

Рис. 112

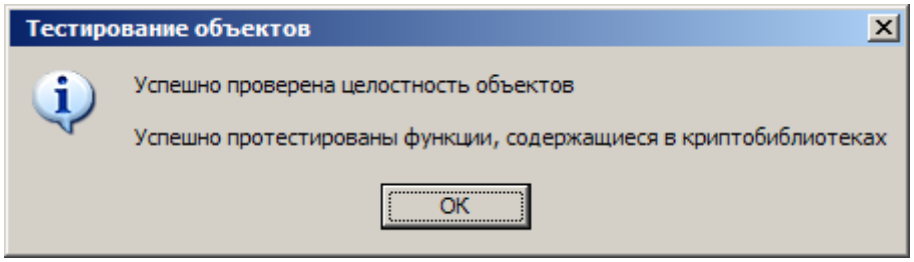

Рис. 113

В качестве долговременных параметров при тестировании криптобиблиотек используются те же, что для криптографических алгоритмов и протоколов вне сервиса тестирования.

6.12. Запрос сертификата по HTTP

6.12.1. Для запроса сертификата по HTTP нужно подвести курсор к иконке  и нажать на правую кнопку мыши. В правом нижнем углу будет высвечено меню как на рис. 114.

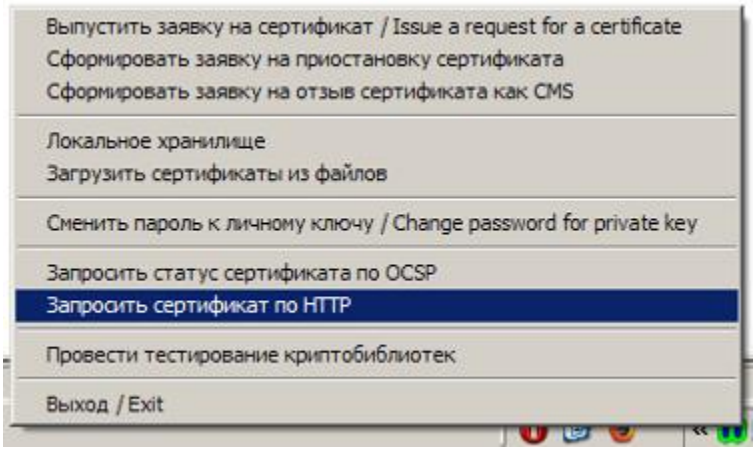

Рис. 114

После выбора пункта меню «Запросить сертификат по HTTP» на экран будет выведено окно «Запрос сертификата вручную по HTTP» (рис. 115).

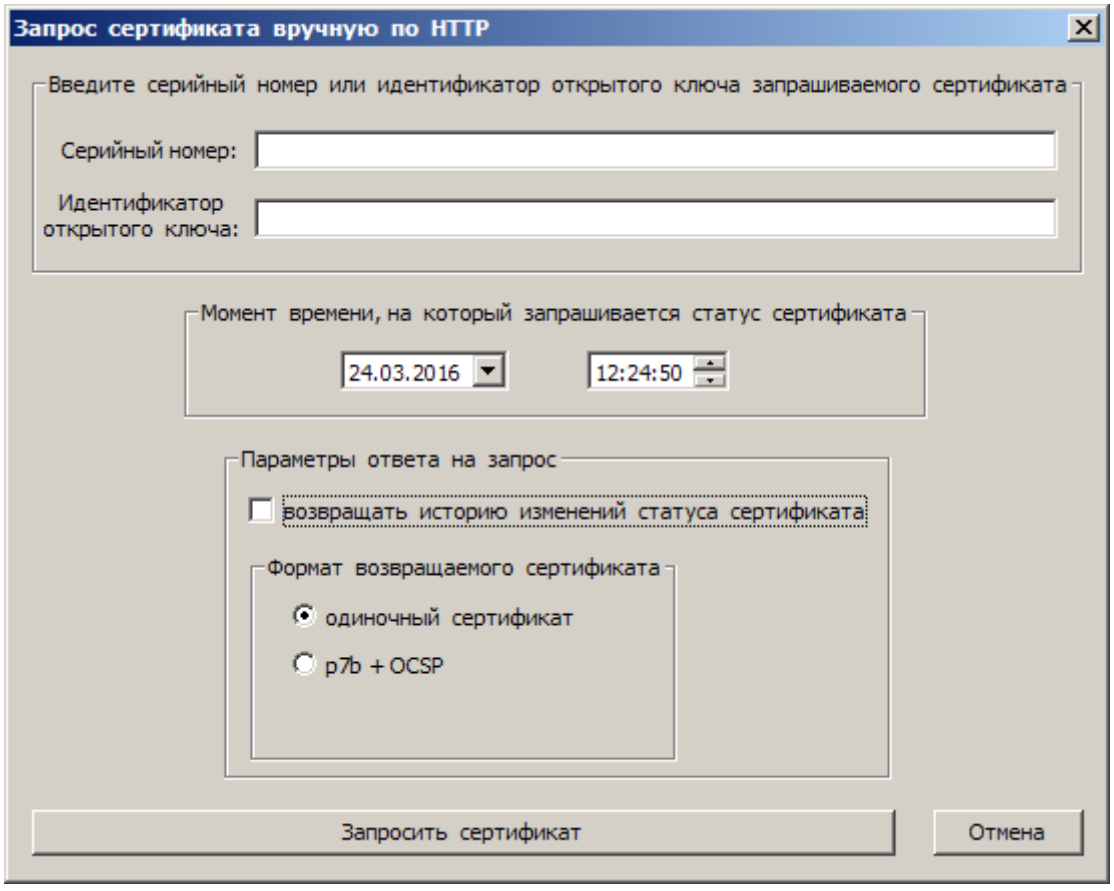

Рис. 115

В данном окне в области «Введите серийный номер или идентификатор открытого ключа запрашиваемого сертификата» в соответствующих полях необходимо указать серийный номер или идентификатор открытого ключа отзываемого сертификата.

Серийный номер и идентификатор открытого ключа можно скопировать из локального хранилища (п. 6.7 настоящего документа). Так же серийный номер и идентификатор открытого ключа можно получить способом, описанным в п. 6.2.4 настоящего документа.

6.12.2. После того, как серийный номер или идентификатор открытого ключа скопирован, следует вернуться к окну «Введите серийный номер или идентификатор открытого ключа запрашиваемого сертификата» (рис. 115), поместить курсор в соответствующее поле и нажать комбинацию клавиш «Ctrl + V» на клавиатуре. В результате номер сертификата отобразиться в данной строчке (рис. 116).

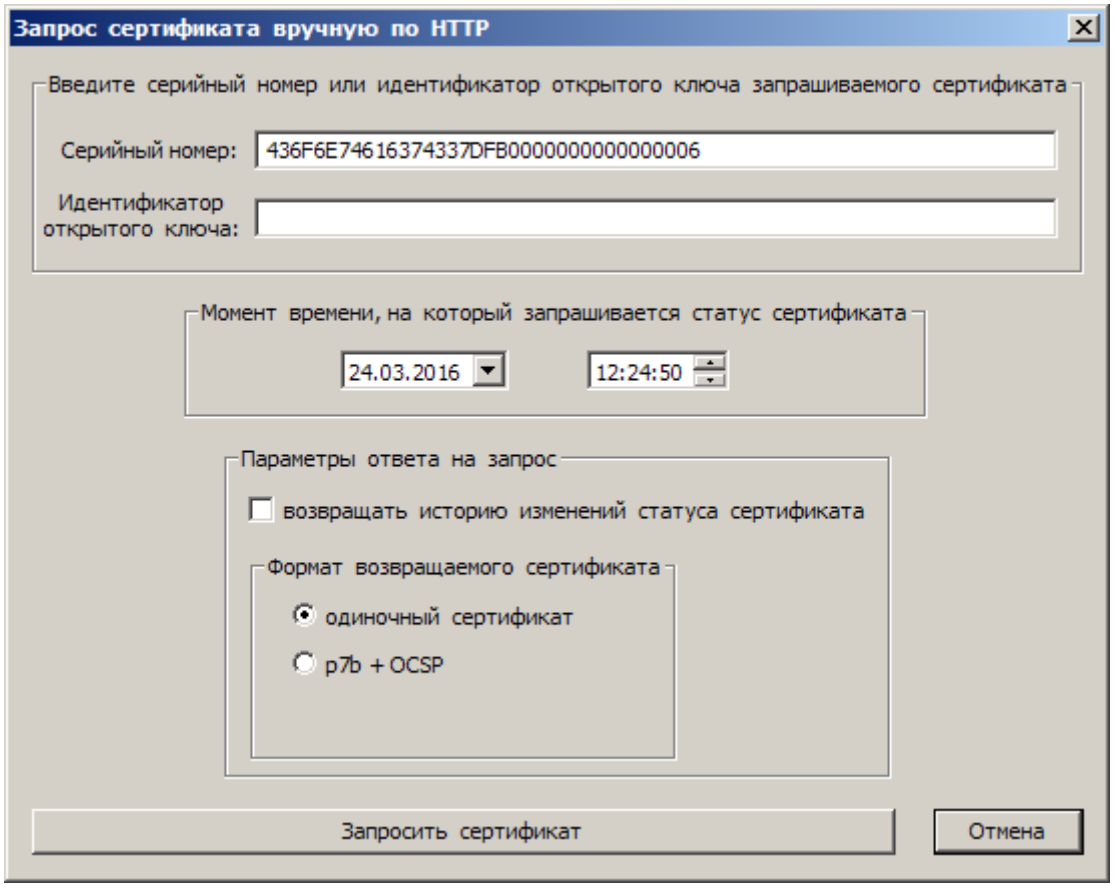

Рис. 116

6.12.3. Затем следует ввести в соответствующие поля значения времени, на который запрашивается статус сертификата (по умолчанию используется текущие значения времени и даты) (рис. 117).

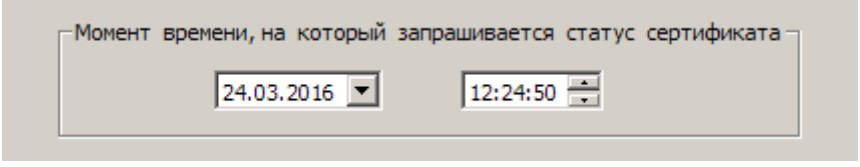

Рис. 117

6.12.4. Далее в области «Параметры ответа на запрос» – «Формат возвращаемого сертификата» следует выбрать один из режимов возвращаемого сертификата (рис. 118).

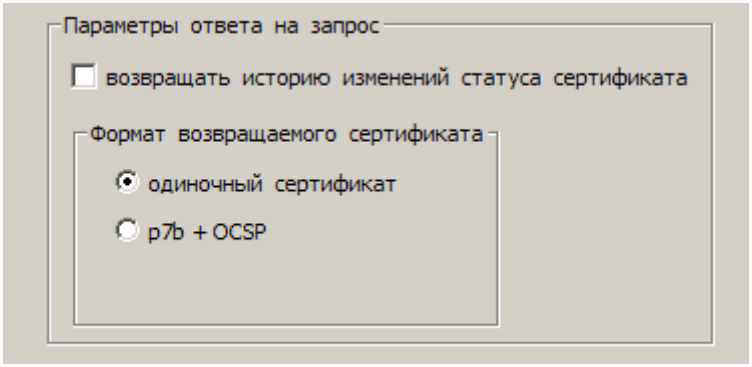

Рис. 118

6.12.5. Для запроса сертификата по HTTP необходимо нажать кнопку «Запросить сертификат» (рис. 116). В результате выполнения процедуры получения сертификата по HTTP будет выдано сообщение (рис. 119) и запрашиваемый сертификат будет подгружен в локальное хранилище.

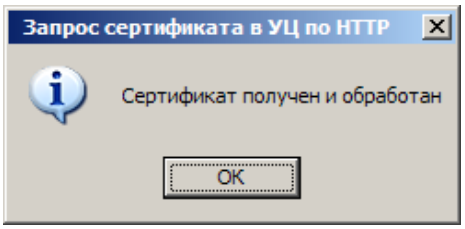

Рис. 119

Если была нажата кнопка «Запросить сертификат» при пустых полях «Серийный номер» и «Идентификатор открытого ключа», то будет выдано сообщение-предупреждение (рис. 120).

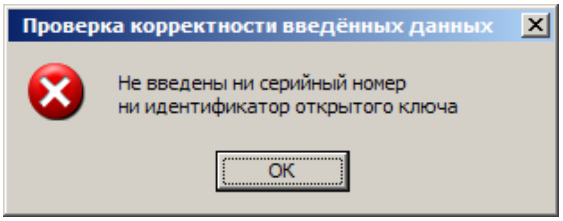

Рис. 120

При необходимости отмены запроса сертификата по HTTP, следует нажать кнопку «Отмена», при этом будет выведено сообщение как на рис. 121.

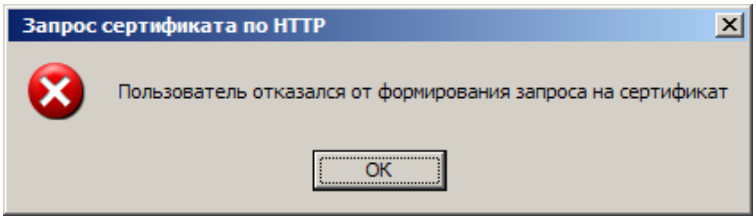

Рис. 121

Если во время запроса сертификата по HTTP произошла ошибка связи с КПА УЦ, будет выдано сообщение как на рис. 122. Причинами данной ошибки могут быть:

– отсутствие связи с КПА УЦ по HTTP;

– некорректные параметры транспортных настроек атрибутов КПА УЦ, указанные в настроечном файле CryptoServiceSettings.xml в секции Transport – секция CA – HTTP (см. п. 6.1).

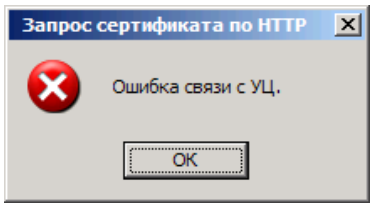

Рис. 122

Структуры SOAP-конвертов запроса сертификата по HTTP и ответа приведены в приложении 1.

6.13. Завершение работы программы

Для прекращения работы программы нужно подвести курсор к иконке  и нажать на правую кнопку мыши. В правом нижнем углу будет высвечено меню как на рис. 123. Следует выбрать последний пункт меню и завершить работу программы.

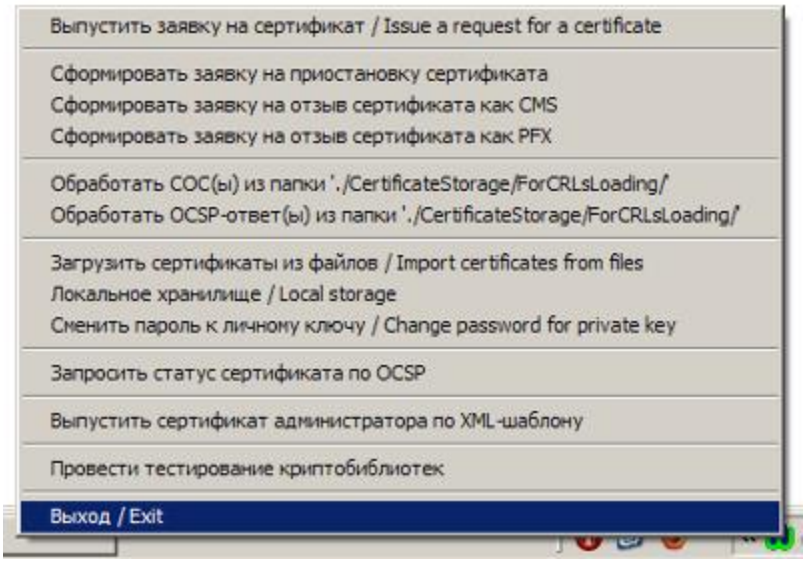

Рис. 123

6.14. Архивное копирование и восстановление данных

Перед началом архивного копирования программный модуль КП СОБ должен быть выгружен. Архивное копирование осуществляется путем копирования на любой носитель информации (компакт-диск, файловая система, USB-накопитель и др.) файла локального

хранилища CertificateStorage.v10, который находится в рабочей директории КП СОБ в папке CertificateStorage.

Восстановление данных производится до загрузки КП СОБ путем помещения архивной копии локального хранилища CertificateStorage.v10 в папку CertificateStorage в рабочей директории КП СОБ.

6.15. Разделение и восстановление секрета

6.15.1. В КП СОБ есть возможность разделения и восстановления секрета согласно СТБ 34.101.60.

Секрет — это произвольная последовательность длиной 128, 192 или 256 бит. При разделении секрета используются два внешних параметра:

1) количество участников N;

2) величина кворума K, причём 2 <= K <= N.

После разделения секрета каждый из участников получает свой частичный секрет. Для восстановления первоначального секрета необходимо наличие частичных секретов в количестве не меньшем величины кворума K.

ВНИМАНИЕ! На предприятии-потребителе должны быть определены и изложены организационные меры по обеспечению конфиденциальности секретов, которые должны предусматривать выдачу каждому участнику не более одного частичного секрета. Носители ключевой информации, содержащие частичные секреты, должны храниться в сейфах, доступ в которые должен быть разрешен только владельцам НКИ.

Для разделения и восстановления секрета необходимо в рабочей директории КП СОБ в папке ShareSecret выбрать файл ShareSecret.exe и двойным щелчком левой кнопки мыши запустить его на выполнение. Появится диалоговое окно «Реализация алгоритмов разделения секрета СТБ 34.101.60-2014» как на рис. 124.

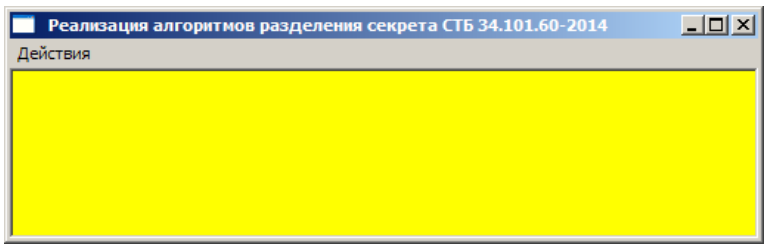

Рис. 124

Если во время запуска КП СОБ находится в состоянии блокировки, то появится сообщение как на рис. 125 и после нажатия кнопки «OK» работа приложения для разделения и восстановления секрета будет прекращена.

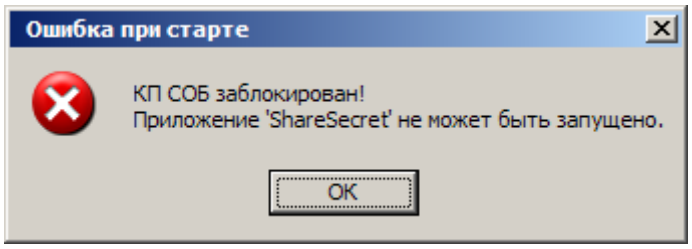

Рис. 125

Меню «Действия» данного приложения содержит следующие пункты (рис. 126):

1) «Разделить секрет» для вычисления частичных секретов и сохранения их в файлах;

2) «Восстановить секрет» для выбора частичных секретов и восстановления общего секрета;

3) «Разделить личный ключ из блоба» для разделения личного ключа и сохранения частичных секретов в файлах;

4) «Восстановить личный ключ в блоб» для выбора частичных секретов, восстановления личного ключа и формирования блоба личного ключа;

5) «Выход из приложения».

Разделять и восстанавливать возможно только личные ключи, сгенерированные по СТБ 34.101.45 с уровнем криптостойкости 128.

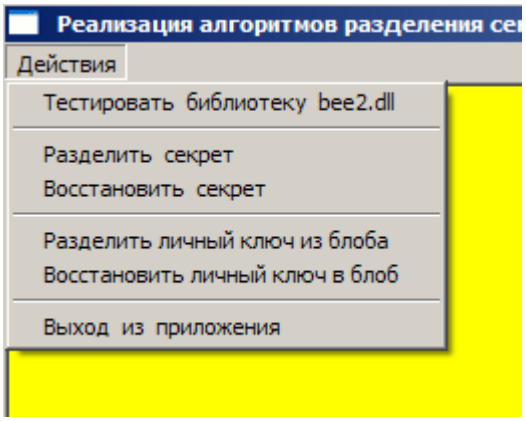

Рис. 126

6.15.2. При выборе пункта меню «Разделить секрет» появится диалоговое окно «Выбор файла с секретом», где необходимо выбрать файл, содержащий секрет длиной 16, 24 либо 32 байта, и нажать кнопку «Открыть» (рис. 127).

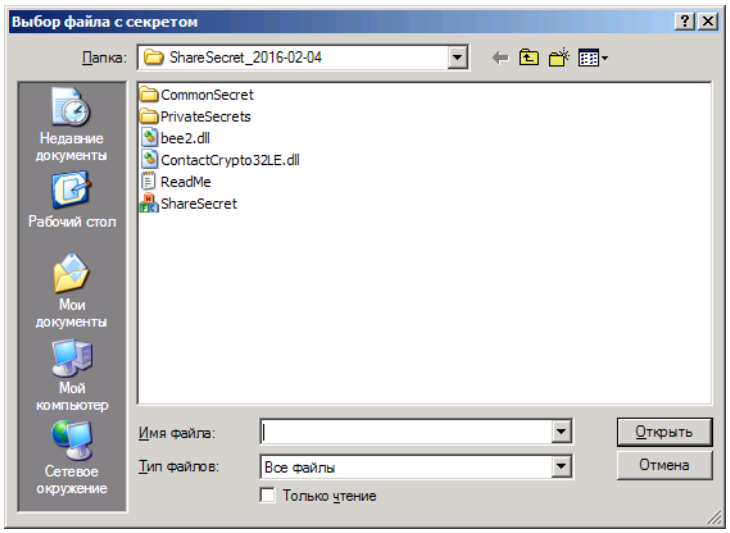

Рис. 127

Если выбранный файл, содержит некорректные данные для разделения секрета, то будет выдано предупреждение как на рис. 128. В противном случае появится диалоговое окно «Выбор параметров разделения секрета» (рис. 129), где необходимо в соответствующих полях указать:

– количество участников;

– величину кворума;

– общий открытый ключ (выбор между стандартным ключом из таблицы А.1 СТБ 34.101.60 и генерацией нового);

– открытые ключи участников (выбор между стандартными ключами из таблиц А.2, А.3 или А.4 СТБ 34.101.60 в зависимости от длины секрета и генерацией новых открытых ключей участников);

– уникальный номер текущей процедуры разделения секрета (необязательное поле для ввода);

– выбор вычисления контрольных слов, используемых для дополнительной проверки секретов в процедуре восстановления секрета (Приложение В СТБ 34.101.60).

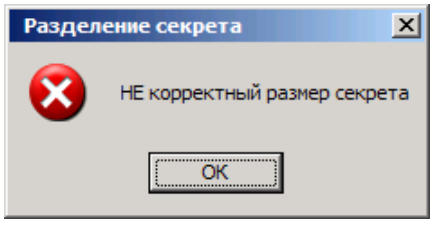

Рис. 128

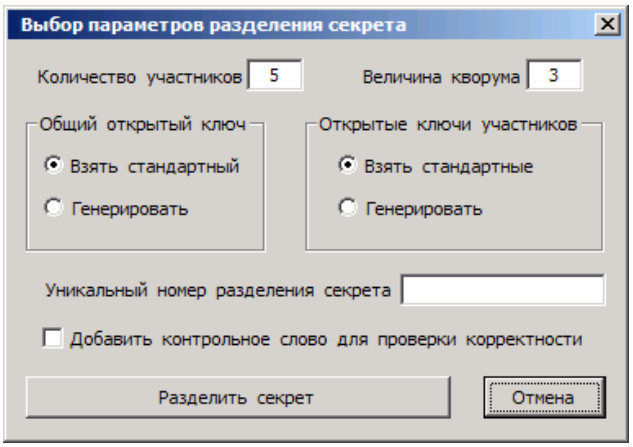

Рис. 129

Если в диалоговом окне «Выбор параметров разделения секрета» (рис. 129) указать некорректное количество участников или величину кворума, будет выдано соответствующее сообщение (рис. 130-132).

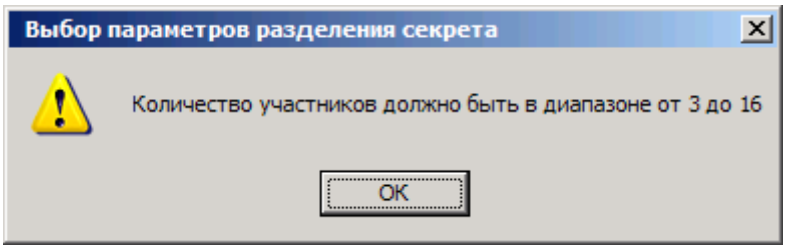

Рис. 130

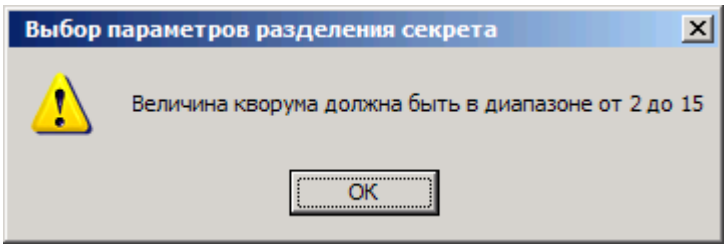

Рис. 131

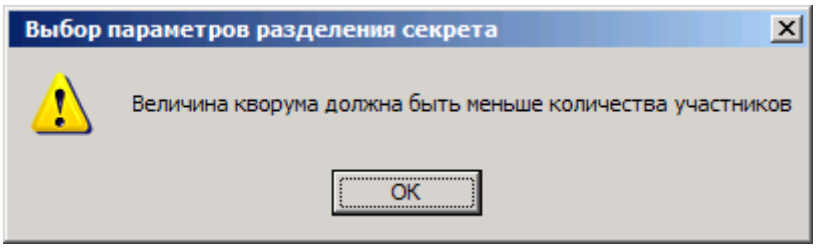

Рис. 132

Для отмены процедуры разделения секрета необходимо нажать кнопку «Отмена» диалогового окна «Выбор параметров разделения секрета» (рис. 129), при этом будет выдано сообщение как на рис. 133.

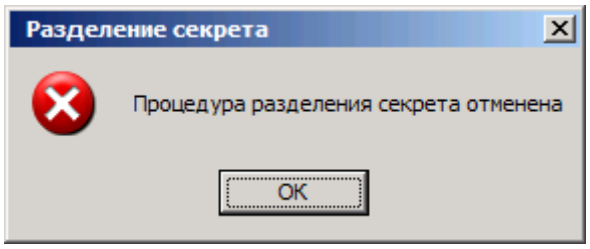

Рис. 133

После того как необходимые параметры разделения секрета заданы для сохранения частичных секретов необходимо нажать кнопку «Разделить секрет» (рис. 129).

При этом будет выдано сообщение как на рис. 134. После нажатия кнопки «OK» появится диалоговое окно «Выбор имени файла частичного секрета №_» (рис. 135), где надо указать директорию для сохранения частичного секрета и нажать кнопку «Сохранить». Далее аналогичные действия необходимо выполнить для заданного количества участников.

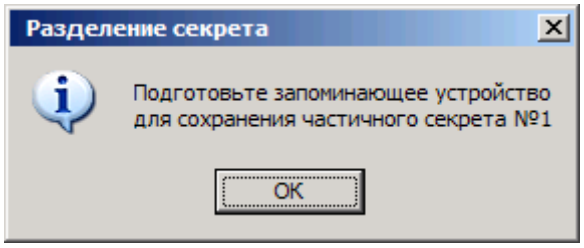

Рис. 134

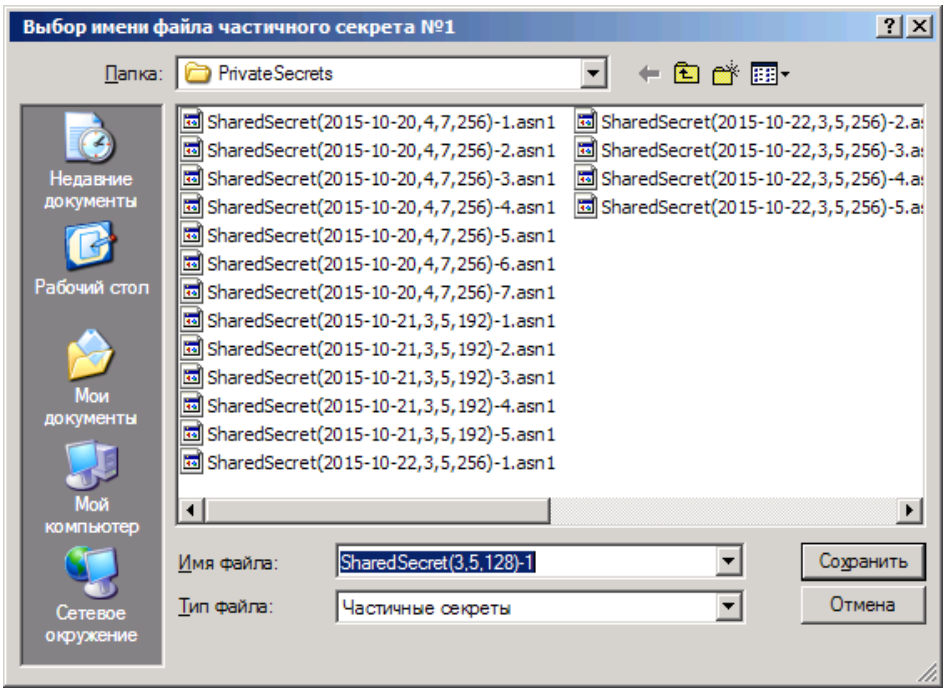

Рис. 135

Если при сохранении частичного секрета была нажать кнопка «Отмена», то будет выдано предупреждение как на рис. 136, файл частичного секрета не будет сохранен и процедура разделения секрета будет завершена.

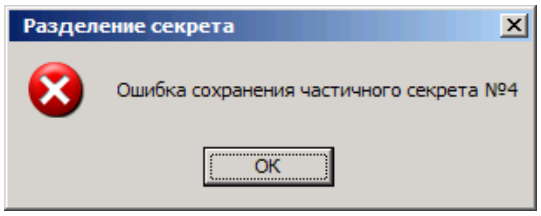

Рис. 136

Когда все частичные секреты сохранены, то процедура разделения секрета завершается и будет выдано соответствующее сообщение (рис. 137).

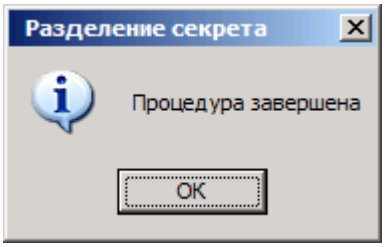

Рис. 137

6.15.3. Для восстановления секрета необходимо выбрать пункт меню «Восстановить секрет» (рис. 125). При этом появиться сообщение как на рис. 138.

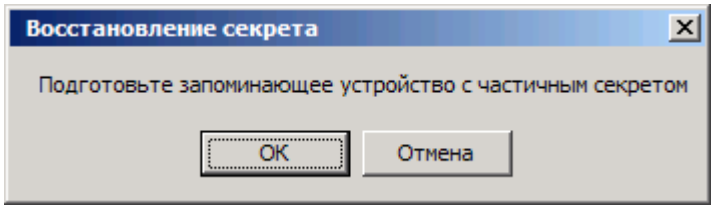

Рис. 138

Если нажата кнопка «OK», то будет выдано диалоговое окно «Выбор файла с частичным секретом» (рис. 139), где необходимо выбрать файл с очередным частичным секретом и нажать кнопку «Открыть». Если выбран файл, содержащий некорректные данные для восстановления секрета, то будет выдано сообщение как на рис. 140.

Для отмены процедуры восстановления секрета необходимо нажать кнопку «Отмена», при этом будет выдано предупреждение как на рис. 141.

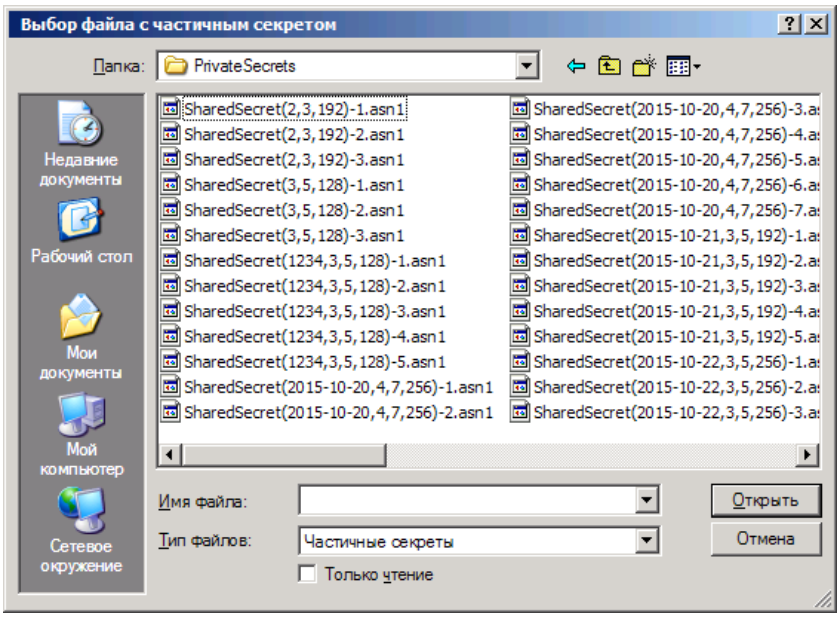

Рис. 139

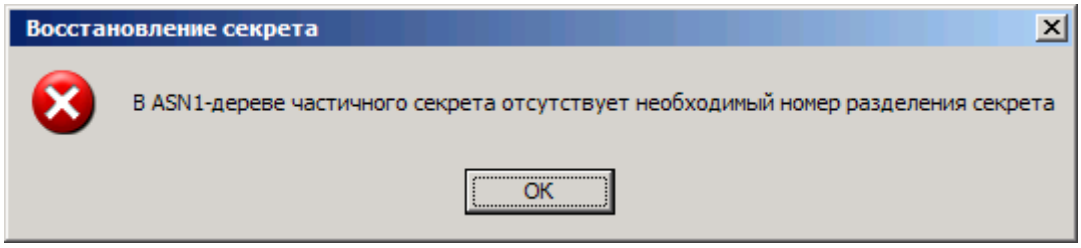

Рис. 140

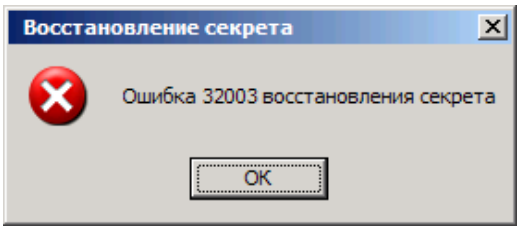

Рис. 141

Если в диалоговом окне «Выбор файла с частичным секретом» (рис. 138) нажать кнопку «Открыть», то в диалоговом окне «Реализация алгоритмов разделения секрета СТБ 34.101.60-2014» будет указано количество выбранных частичных секретов и минимально необходимое количество частичных секретов, а так же будет выдано сообщение «Восстановление секрета» (рис. 142).

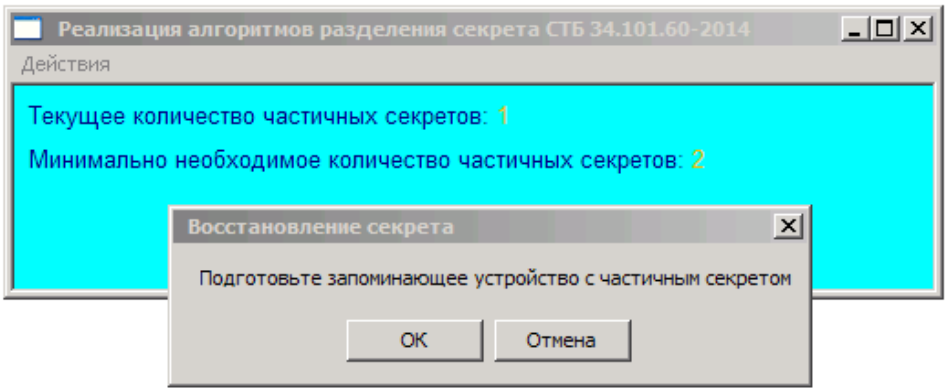

Рис. 142

Для очередного выбора файла с частичным секретом необходимо нажать кнопку «OK» в диалоговом окне «Восстановление секрета» (рис. 142) и выполнить действия описанные выше.

Для восстановления общего секрета, после того как выбраны все необходимые файлы с частичными секретами, в диалоговом окне «Восстановление секрета» (рис. 142) следует нажать кнопку «Отмена».

Если количество выбранных файлов с частичными секретами меньше, чем минимально необходимое количество, то будет выдано предупреждение как на рис. 143. В противном случае происходит восстановление общего секрета, предлагается задать имя файла для сохранения восстановленного секрета (рис. 144).

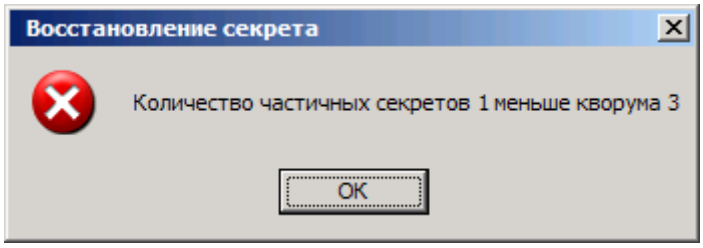

Рис. 143

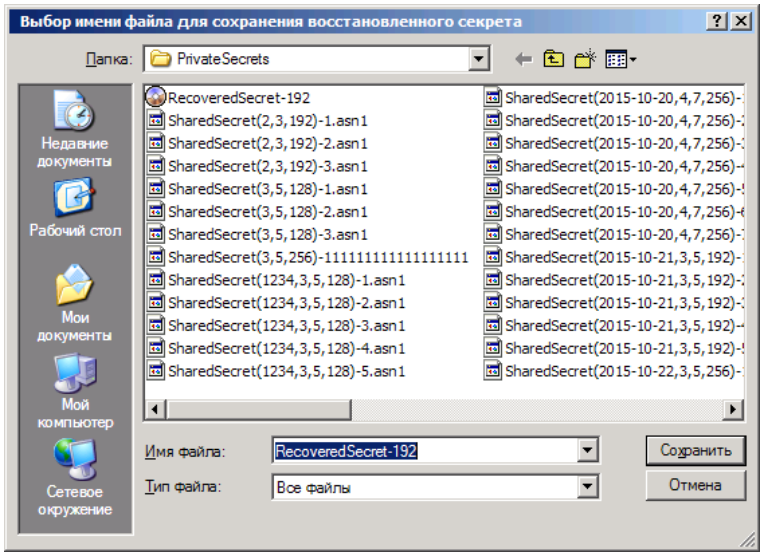

Рис. 144

Если в диалоговом окне «Выбор имени файла для сохранения восстановленного секрета» (рис. 144) нажать кнопку «Отмена», восстановленный секрет не будет сохранен в файл, будет выдано сообщение как на рис. 145 и процедура восстановления секрета будет завершена. Если же нажата кнопка «Сохранить», то восстановленный секрет будет сохранен в файл и будет выдано сообщение с указанием пути к файлу с восстановленным секретом (рис. 146).

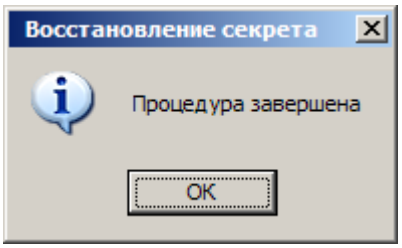

Рис. 145

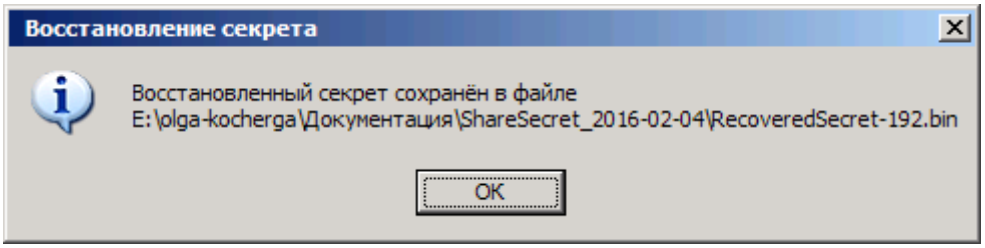

Рис. 146

6.15.4. Действия по разделению личного ключа из блоба аналогичны действиям, выполняем при разделении секрета после выбора пункта меню «Разделить секрет» (см. п. 6.15.2).

За исключением того, что после выбора пункта меню «Разделить личный ключ из блоба» появится диалоговое окно «Выбор файла с личным ключом», где необходимо выбрать файл личного ключа и нажать кнопку «Открыть» (рис. 147).

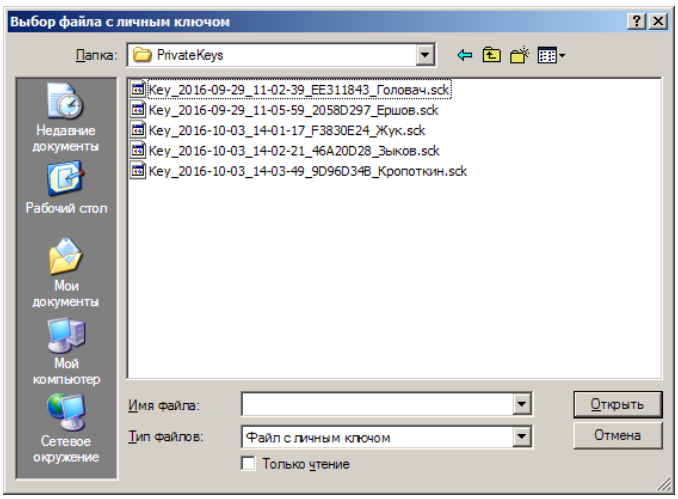

Рис. 147

Если выбранный файл, содержит некорректные данные для разделения личного ключа из

блоба, то будет выдано соответствующее сообщение (рис. 148) и процедура разделения личного ключа из блоба будет прекращена.

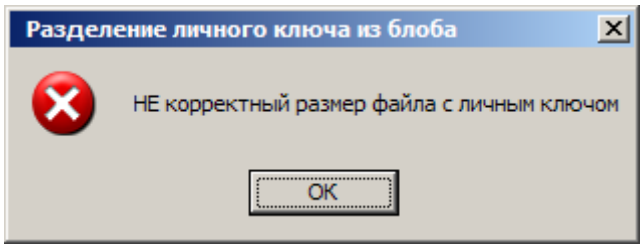

Рис. 148

После выбора файла с личным ключом, в диалоговом окне «Ввод пароля к личному ключу» необходимо ввести пароль к личному ключу (рис. 149) и нажать кнопку Enter.

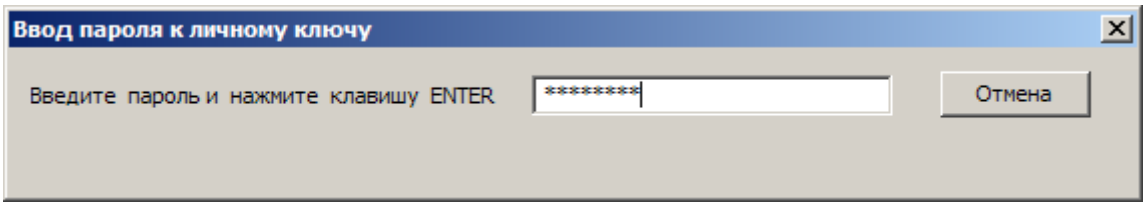

Рис. 149

Если возникли ошибки при извлечении личного ключа из блоба, то будет выдано соответствующее сообщение (рис. 150-152) и процедура разделения личного ключа из блоба будет прекращена.

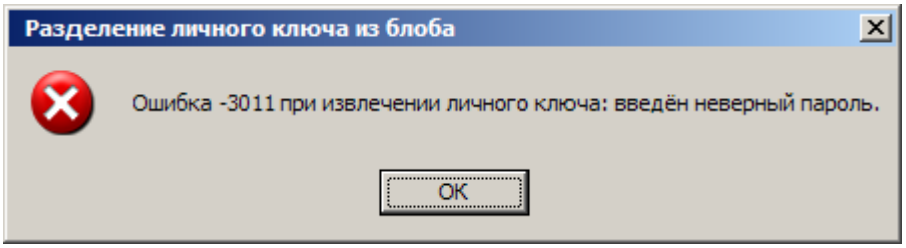

Рис. 150

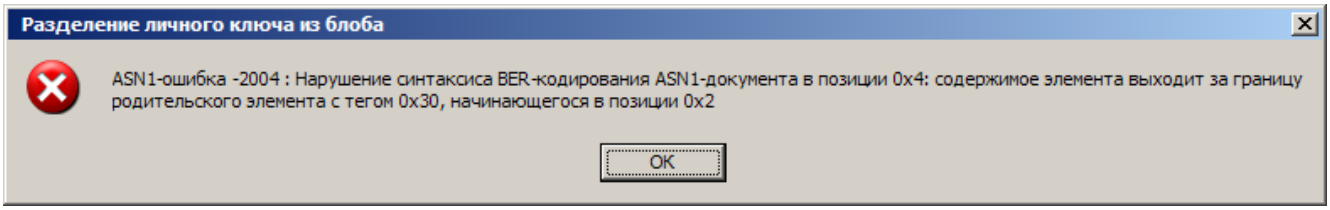

Рис. 151

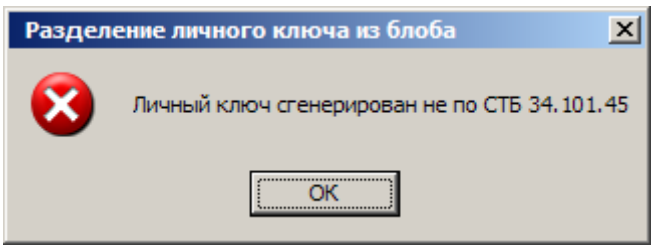

Рис. 152

6.15.5. Действия по восстановлению личного ключа в блоб аналогичны действиям, выполняем при восстановлении секрета после выбора пункта меню «Восстановить секрет» (см. п. 6.15.3).

За исключением того, что после выбора требуемого количества частичных секретов необходимо выбрать сертификат открытого ключа, парный восстанавливаемому личному ключу (рис. 153).

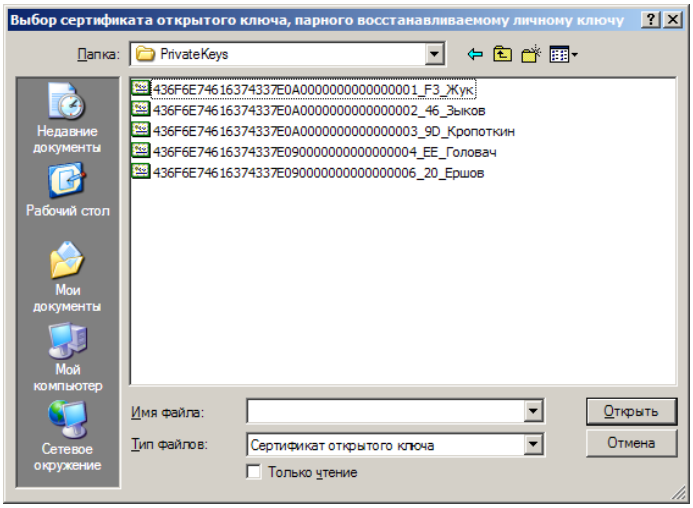

Рис. 153

Если выбранный сертификат открытого ключа не является парным для восстанавливаемого личного ключа, то будет выдано соответствующее сообщение об ошибке (рис. 154-157) и процедура восстановления личного ключа в блоб будет прекращена.

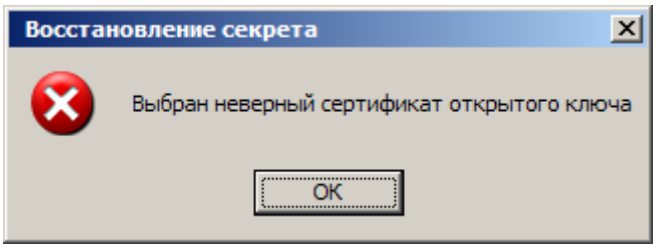

Рис. 154

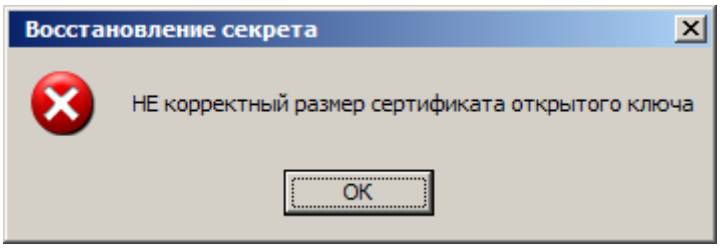

Рис. 155

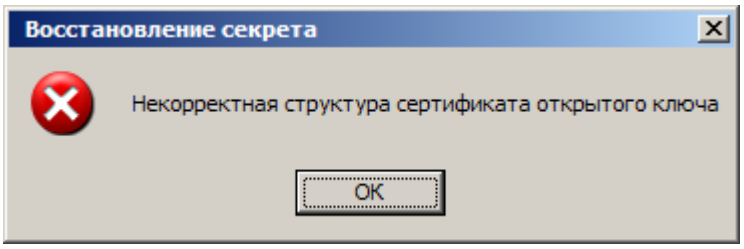

Рис. 156

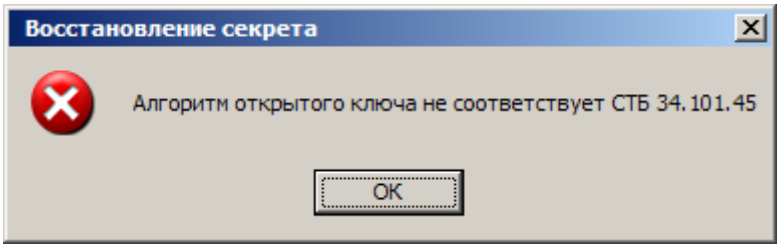

Рис. 157

После выбора сертификата, парного восстанавливаемому личному ключу, в диалоговом окне «Ввод пароля к личному ключу с подтверждением» необходимо ввести новый пароль и подтверждение (рис. 158). Если длина введенного пароля меньше 8 символов, будет выдано сообщение как на рис. 159. Если подтверждение пароля не совпадает с введенным паролем, то будет выдано сообщение как на рис. 160.

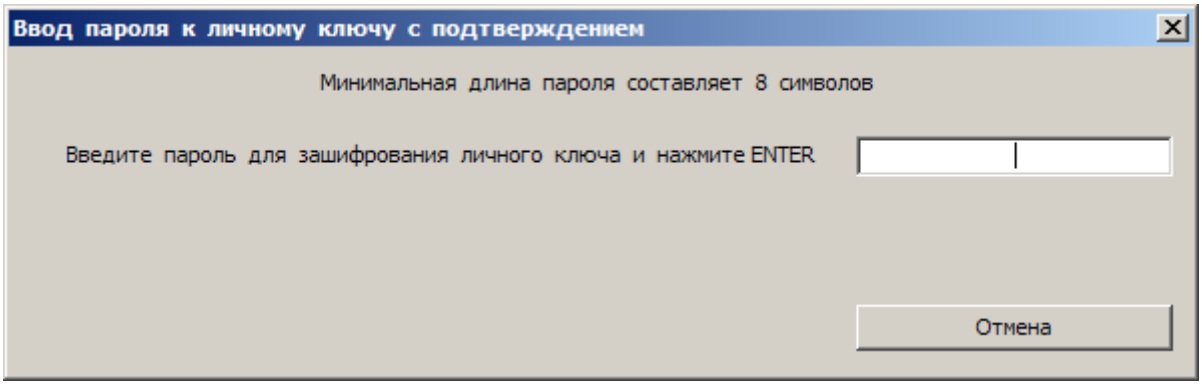

Рис. 158

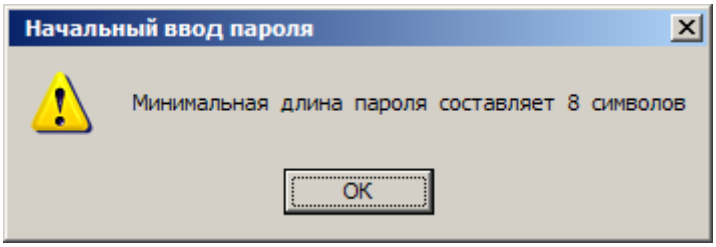

Рис. 159

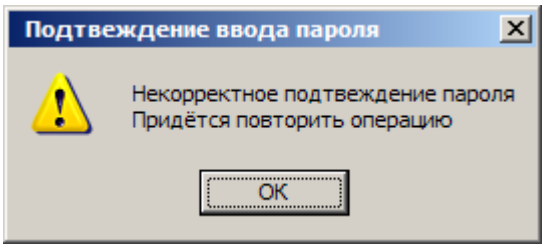

Рис. 160

6.15.6. Для закрытия диалогового окна и выхода из приложения необходимо выбрать пункт меню «Выход из приложения» (рис. 126).

6.16. Управление личными ключами

6.16.1. В КП СОБ предусмотрена возможность управления личными ключами с использованием НКИ (под НКИ понимаются носители ключевой информации, такие как файловая система, «Устройство хранения информации защищенное мобильное «Меркурий» СЮИК.466216.001 (далее – УХИ «Меркурий»), iKey Rainbow, Touch Memory) для выполнения следующих операций:

– чтение личных ключей с НКИ;
– запись личных ключей на НКИ;
– получение списка личных ключей на НКИ;
– смена пароля к личному ключу;
– копирование/перемещение личных ключей;
– переименование личных ключей;
– удаление личного ключа;
– работа с личными ключами через удобный для пользователя интерфейс.

Для управления ключами используется утилита PrivateKeysManager. Для ее запуска необходимо в рабочей директории КП СОБ в папке PrivateKeysManager выбрать файл PKManager.exe и двойным щелчком левой кнопки мыши запустить его на выполнение. Появится диалоговое окно «Менеджер личных ключей» как на рис. 161. Завершить работу программы можно закрыв данное окно.

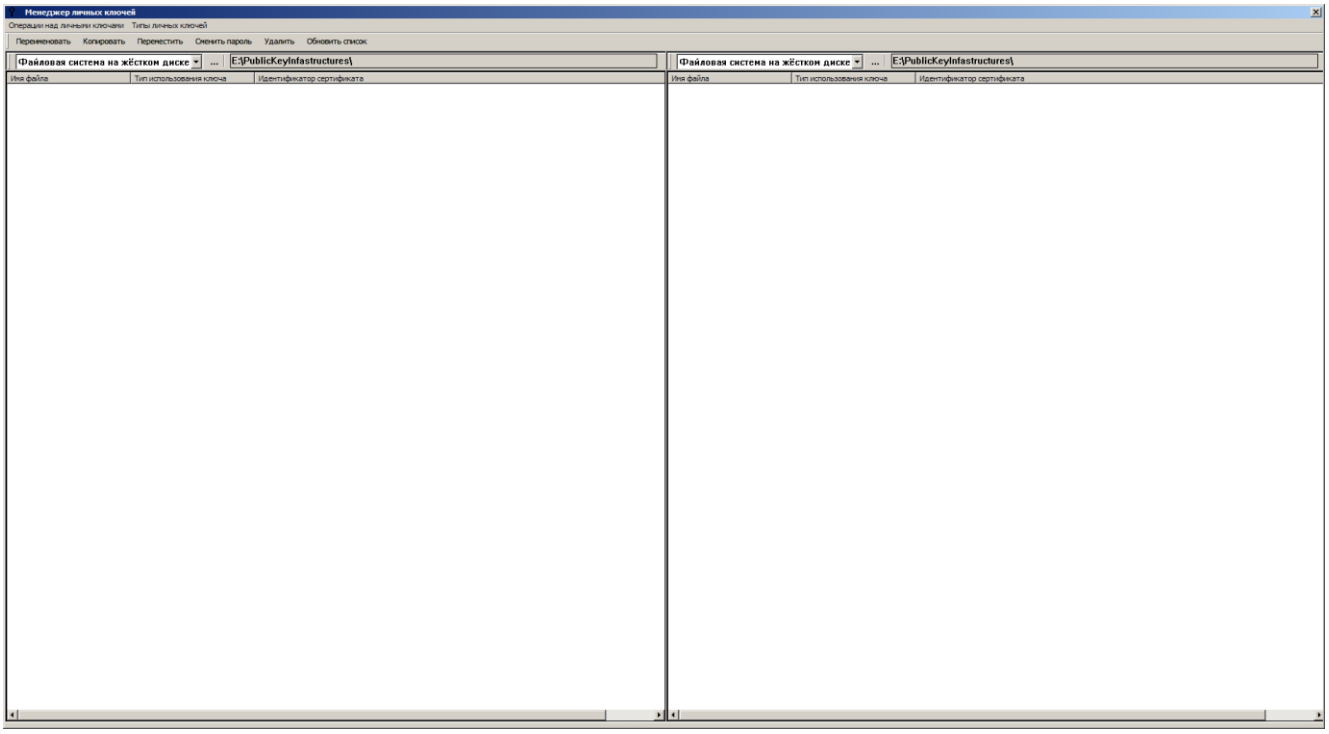

Рис. 161

Если во время запуска КП СОБ находится в состоянии блокировки, то появится сообщение как на рис. 162 и после нажатия кнопки «ОК» работа приложения будет прекращена.

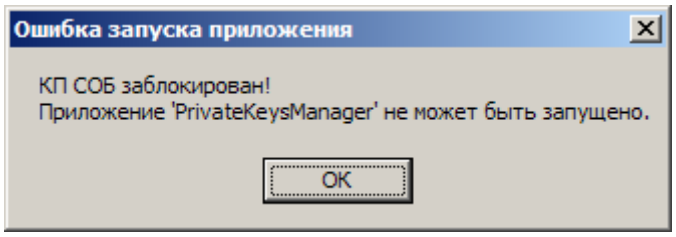

Рис. 162

6.16.2. Для выбора носителя ключевой информации необходимо в раскрывающемся списке носителей (рис. 163) выбрать необходимый.

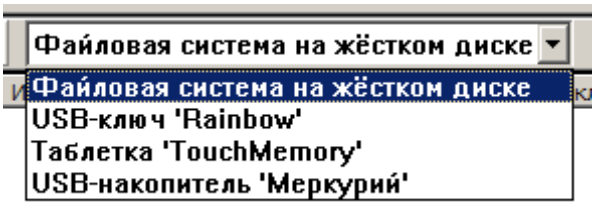

Рис. 163

Если программа не обнаружит носитель, то появится сообщение об ошибке (рис. 164).

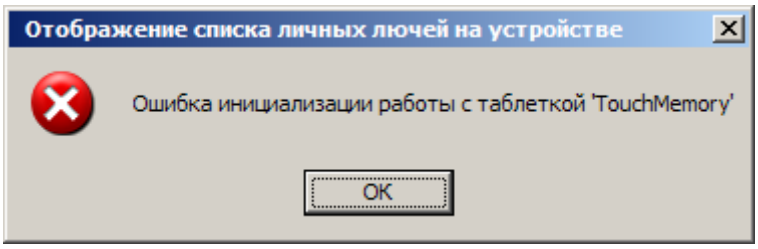

Рис. 164

При выборе в качестве НКИ «USB-накопитель «Меркурий», отобразится окно, в котором необходимо указать имя ключевой области (рис. 165). Если заданная область не найдена, появится сообщение с предложением о создании новой ключевой области рис. 166. Если выбрана кнопка «Да», то на УХИ «Меркурий» будет создана новая ключевая область с заданным именем. Если выбрана кнопка «Нет», то будет выдано сообщение о том, что ключевая область с заданным именем не создана (рис. 167).

Рекомендуется работать с УХИ «Меркурий» только в 32-х разрядной ОС.

Рис. 165

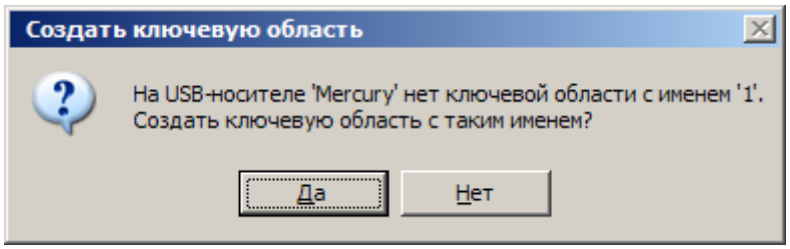

Рис. 166

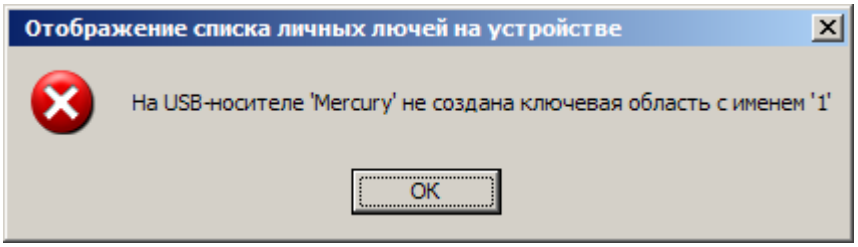

Рис. 167

При выборе в качестве НКИ «Файловая система на жёстком диске», также необходимо задать путь к папке с ключами, нажав кнопку «…» и в открывшемся окне «Обзор папок», выбрать необходимую папку.

Если в выбранной папке или устройстве имеются ключи, они отобразятся в рабочей области программы (рис. 168).

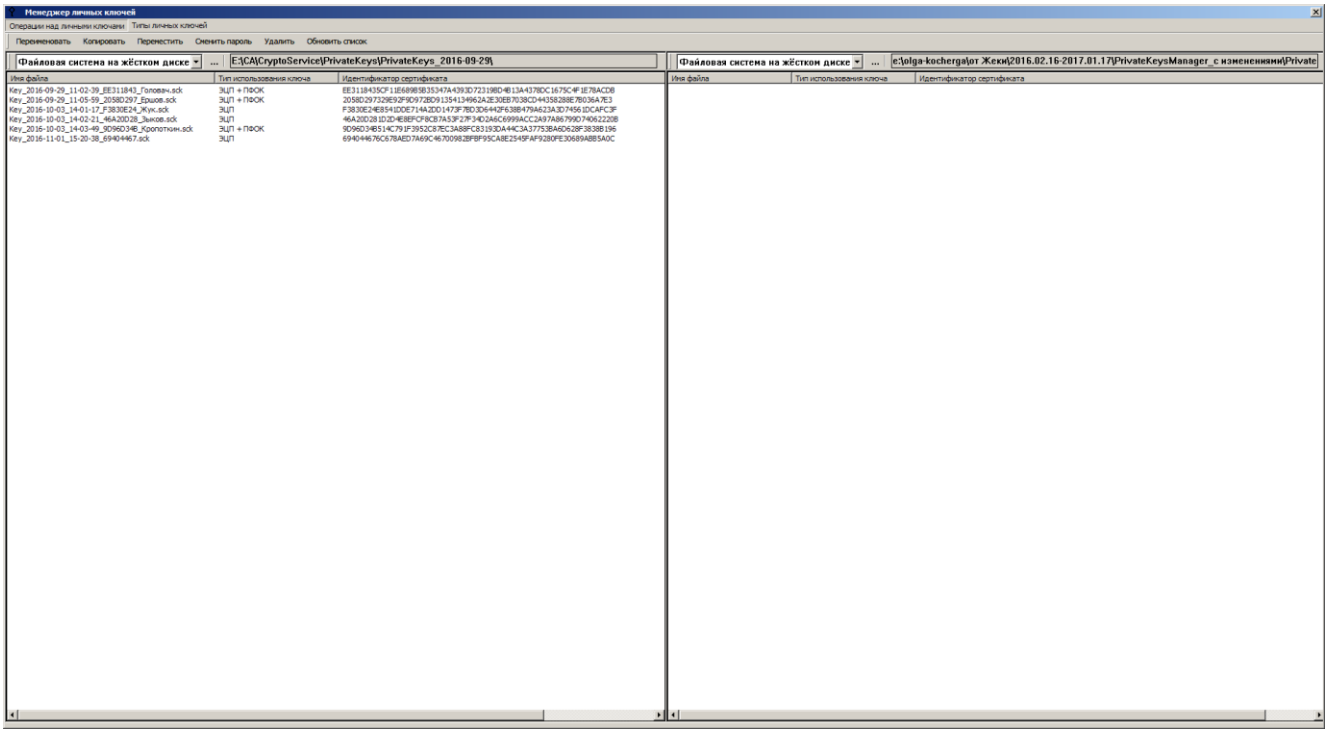

Рис. 168

6.16.3. Для осуществления сортировки личных ключей по имени файла, типу использования ключа или идентификатору сертификата, необходимо нажать на заголовок соответствующего столбца (рис. 169).

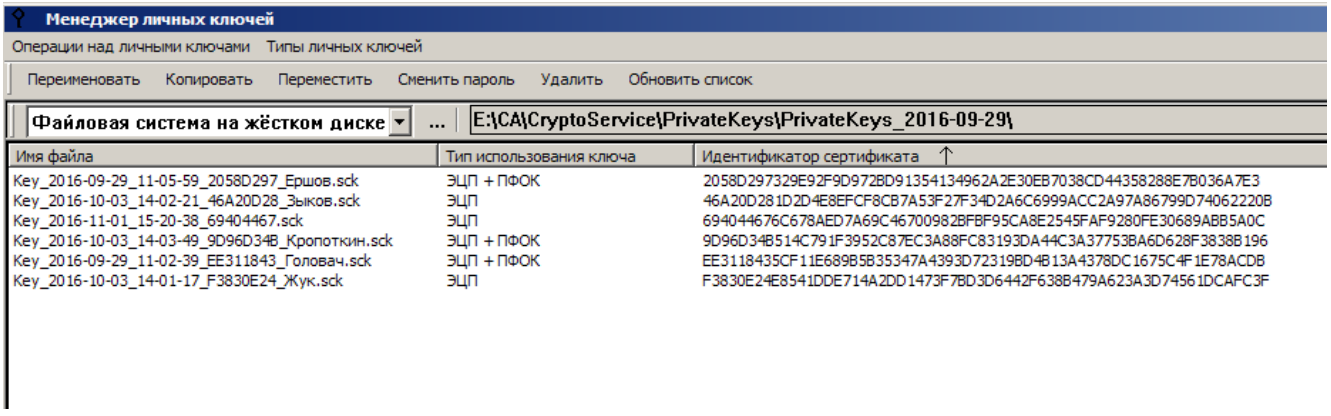

Рис. 169

6.16.4. Для задания типа отображаемых личных ключей, необходимо выбрать пункт меню «Типы личных ключей» – «ЭЦП» и/или «Типы личных ключей» – «ПФОК» (рис. 170).

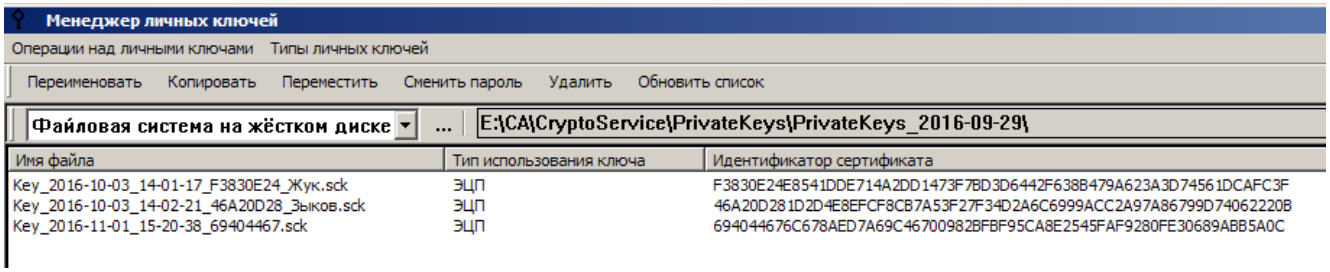

Рис. 170

6.16.5. Для переименования личного ключа необходимо выбрать личный ключ, затем выбрать пункт меню «Операции над личными ключами» – «Переименовать» (нажать на панели инструментов одноименную кнопку или выбрать из контекстного меню) после чего в открывшемся окне задать новое имя личного ключа (рис. 171).

Рис. 171

После успешного выполнения переименования, отобразится окно с сообщением, аналогичное рис. 172.

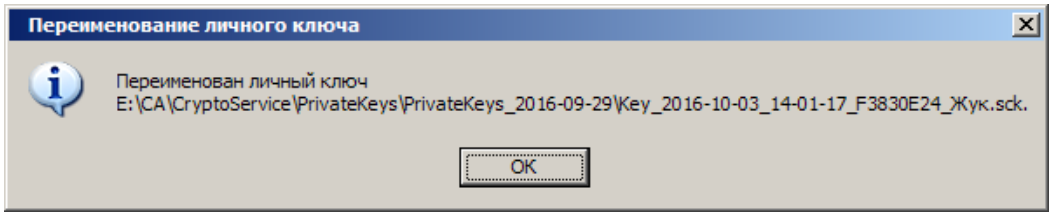

Рис. 172

6.16.6. Для копирования личного ключа необходимо выбрать в одной области главного окна (рис. 146) место (папку в файловой системе, имя на ключевой области на USB-носителе «Меркурий» или другое устройство) (рис. 163), куда необходимо скопировать ключ, а во второй области главного окна выбрать необходимый ключ, затем выбрать пункт меню «Операции над личными ключами» – «Копировать» (нажать на панели инструментов одноименную кнопку или выбрать из контекстного меню). В открывшемся окне «Копирование файла личного ключа» подтвердить копирование личного ключа (рис. 173).

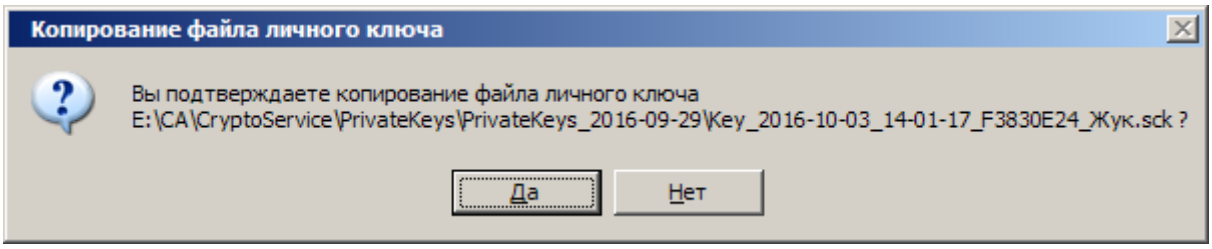

Рис. 173

После этого необходимо подтвердить или отказаться от изменения пароля личного ключа (рис. 174).

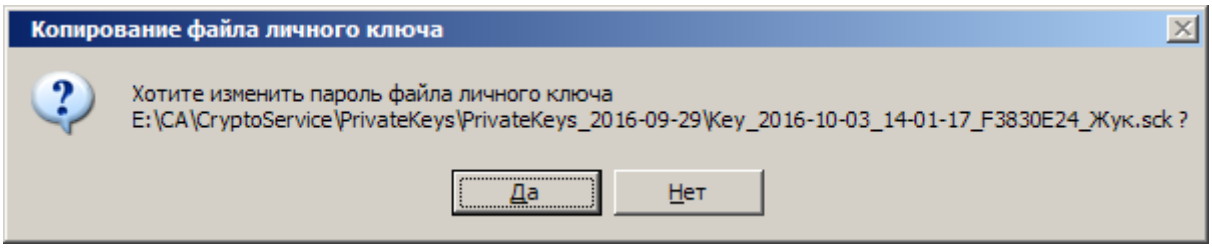

Рис. 174

При подтверждении изменения пароля в открывшемся окне ввести старый пароль и новый пароль с подтверждением (рис. 175). После успешного выполнения копирования, отобразится соответствующее сообщение.

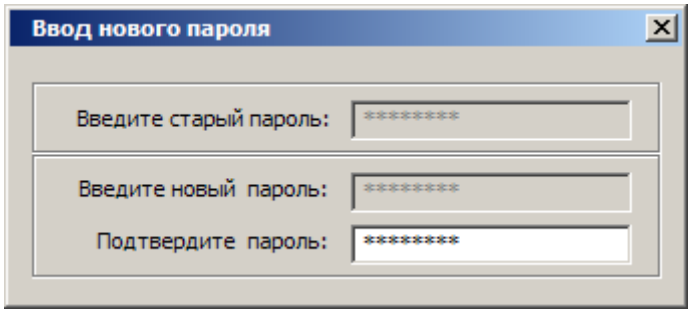

Рис. 175

6.16.7. Перемещение личного ключа осуществляется аналогично копированию личного ключа, за исключением того, что для выполнения данного действия необходимо выбрать пункт меню «Операции над личными ключами» – «Переместить» (нажать на панели инструментов одноименную кнопку или выбрать из контекстного меню) и в окне «Ввод нового имени файла» задать новое имя личного ключа (рис. 171).

6.16.8. Для изменения пароля личного ключа необходимо выбрать файл с личным ключом, затем пункт меню «Операции над личными ключами» – «Сменить пароль» (нажать на панели инструментов одноименную кнопку или выбрать из контекстного меню). В открывшемся окне ввести старый пароль и новый пароль с подтверждением (рис. 175). После успешного выполнения изменения пароля, отобразится соответствующее сообщение.

6.16.9. Для удаления личного ключа необходимо выбрать личный ключ, затем пункт меню «Операции над личными ключами» – «Удалить» (нажать на панели инструментов одноименную кнопку или выбрать из контекстного меню). В открывшемся окне подтвердить удаление личного ключа (рис. 176).

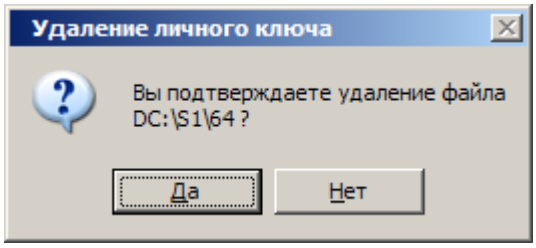

Рис. 176

После чего в следующем окне ввести пароль к удаляемому личному ключу (рис. 177). После успешного выполнения удаления личного ключа, отобразится соответствующее сообщение.

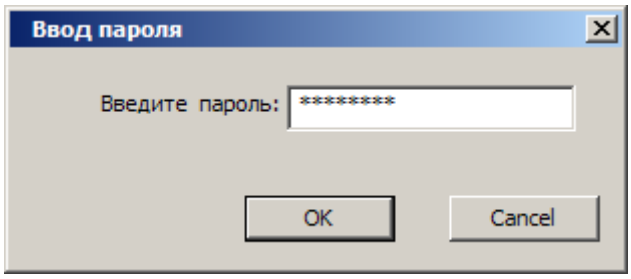

Рис. 177

6.17. Просмотр номера версии КП СОБ

Для просмотра номера версии КП СОБ необходимо в рабочей директории КП СОБ вызвать контекстное меню файла исполняемого модуля CryptoService_41.exe и выбрать пункт «Свойства» (рисунок 178).

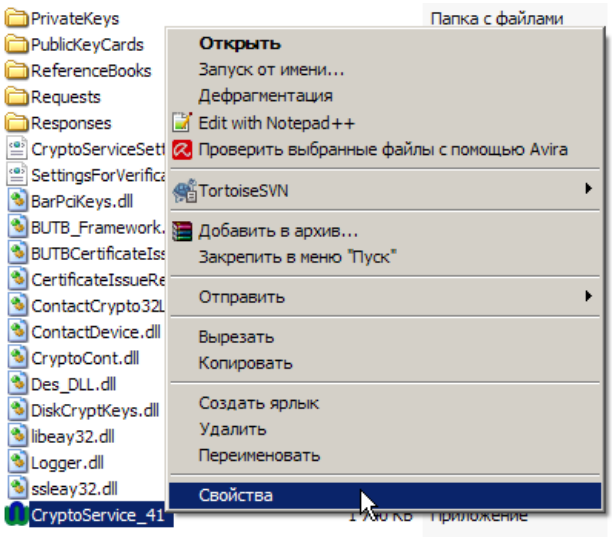

Рисунок 178

В диалоговом окне «Свойства: CryptoService_41» выбрать вкладку «Версия» (для ОС Microsoft Windows™ XP (x86), Server 2003 (x86)) или вкладку «Подробно» (для ОС Microsoft Windows™ 7 (x86, x64), 10). В списке выбрать «Версия продукта» и в поле «Значение:» просмотреть номер версии (рисунок 179).

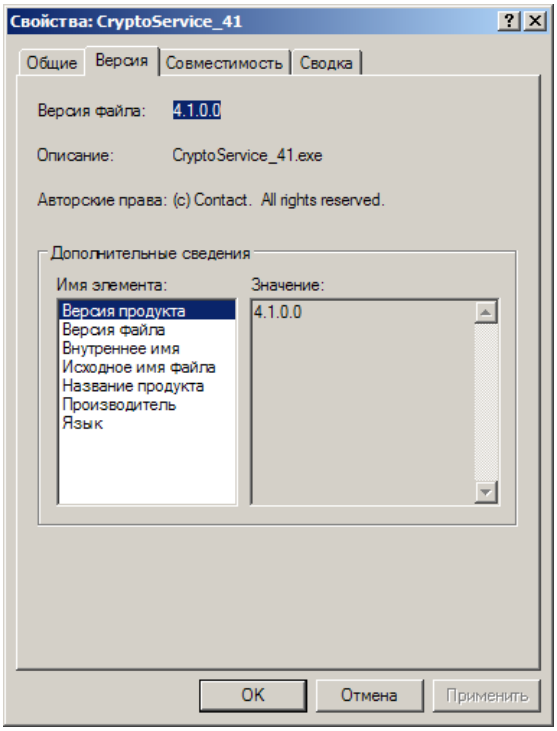

Рисунок 179

6.18. Установка защищенного соединения с помощью TLS

6.18.1. Настройка модуля установки защищенного соединения

Настройка модуля производится редактированием настроечных файлов TestBelTLSdllSettings.xml, ClientSettings.xml, ServerSettings.xml, host, которые расположены в рабочей директории КП СОБ в папке TLS.

Для настройки соединения используется файл host, где задается IP-адрес сервера и порт, на котором необходимо открыть сокет либо к которому необходимо подключиться. IP-адрес должен быть написан одинаковый для серверной и клиентской сторон.

В файле TestBelTLSdllSettings.xml указываются следующие настройки:

– в теге TLSdllFileName указывается путь к библиотеке реализации TLS;

– в теге ServerSettings указывается путь к файлу настроек сервера TLS;

– в теге ClientSettings указывается путь к файлу настроек клиента TLS.

Другие настройки применяются к настройкам протокола TLS для сервера и клиента и содержатся в файлах ClientSettings.xml и ServerSettings.xml:

1) в атрибуте ConnectionEnd указывается одно из значений «Client» или «Server», в зависимости от типа настроек: для сервера TLS или клиента TLS;

2) основные параметры настройки, указанные в секции Logging:

а) атрибут DebugLogging – параметр логирования информации;

б) LogName – имя файла журнала.

3) в секции PrivateKey указывается путь к личному ключу сервера TLS или клиента TLS, а в атрибуте Password – пароль к личному ключу сервера TLS или клиента TLS;

4) в секции CertificateChain перечисляются все СОК из цепочки сертификатов сервера TLS или клиента TLS, а в тегах Certificate указывается путь к каждому СОК из цепочки;

5) в секции OrderedCipherSuites в тегах CipherSuite в атрибуте Name указываются поддерживаемые криптонаборы в порядке убывания приоритетности. Возможны следующие варианты (в соответствии с СТБ 34.101.65 Приложение В таблица В.1):

а) TLS_DHT_BIGN_WITH_BELT_DWP_HBELT;

б) TLS_DHT_BIGN_WITH_BELT_CTR_MAC_HBELT;

в) TLS_DHE_BIGN_WITH_BELT_DWP_HBELT;

г) TLS_DHE_BIGN_WITH_BELT_CTR_MAC_HBELT;

д) TLS_DHT_PSK_BIGN_WITH_BELT_DWP_HBELT;

е) TLS_DHT_PSK_BIGN_WITH_BELT_CTR_MAC_HBELT;

ж) TLS_DHE_PSK_BIGN_WITH_BELT_DWP_HBELT;

и) TLS_DHE_PSK_BIGN_WITH_BELT_CTR_MAC_HBELT;

6) в секции PSKname указывается путь к таблице секретов (см. приложение 6). Примеры таблиц секретов находятся в рабочей директории КП СОБ по пути TLS\PSK_tables (серверная таблица секретов в файле ServerTable.psk, клиентская таблица секретов — ClientTable_0040.psk);

7) в секции OrderedCompressionMethods в тегах CompressionMethod в атрибуте Name указываются поддерживаемые алгоритмы сжатия в порядке убывания приоритетности. Возможны следующие варианты:

а) Deflate – алгоритм сжатия «Deflate";

б) NULL – пустой алгоритм сжатия;

8) в секции HashAndSignatureAlgorithms в тегах HashSignPair в атрибуте Name указываются поддерживаемые пары алгоритма хеширования и алгоритма ЭЦП. В атрибуте Name должно быть установлено значение «BeltHash+BignSign», указывающее на то, что будет использоваться хеширование согласно СТБ 34.101.31 и ЭЦП согласно СТБ 34.101.45;

9) в секции SessionsRenegotiation в атрибутах IsRenegotiable и IsCritical указывается допустимость и критичность переустановки сессии соответственно;

10) в секции ClientAuthentication в атрибуте Is указываются требования к аутентификации клиента (задаются только для сервера TLS). Возможны следующие варианты:

а) Reqiured – обязательна;

б) Desirable – желательна;

в) None – не требуется;

11) в секции AcceptableCAs в тегах DistinguishedName задаются отличительные имена признаваемых удостоверяющих центров (задаются только для сервера TLS). В каждом теге DistinguishedName указывается секция Subject доверенного корневого СОК в ASN1 виде закодированная в BASE64.

6.18.2. Запуск модуля установки защищенного соединения

Загрузка модуля осуществляется путем запуска приложения ContactBelTLS.exe из папки TLS в рабочей директории КП СОБ.

Если во время запуска КП СОБ находится в состоянии блокировки, то появится сообщение как на рис. 180 и после нажатия кнопки «ОК» работа приложения будет прекращена.

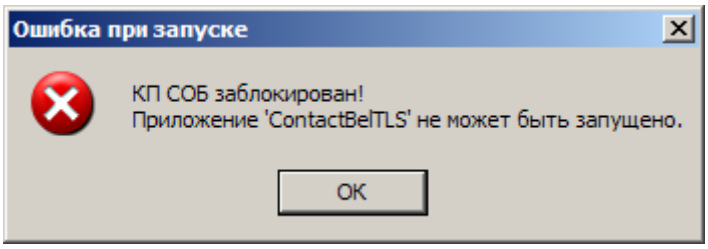

Рис. 180

В случае если при запуске КП СОБ не был найден файл настроек TestBelTLSdllSettings.xml, либо в данном файле настроек задан некорректный путь к файлу настроек сервера (клиента) TLS или библиотеке TLS.dll, либо не найден файл с сетевыми настройками host, то будет выдано соответствующее сообщение (рис. 181) и после нажатия кнопки «OK» работа приложения будет прекращена.

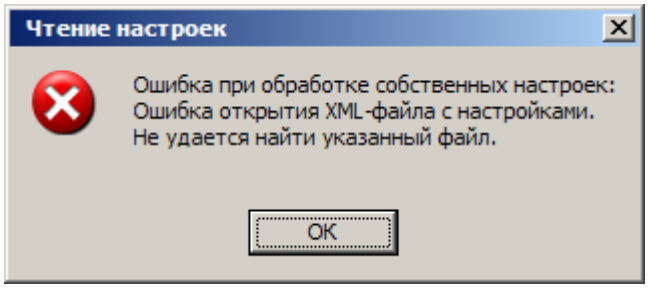

Рис. 181

6.18.3. Порядок работы

Вся работа с приложением осуществляется через графический интерфейс в виде пунктов меню (рис. 182).

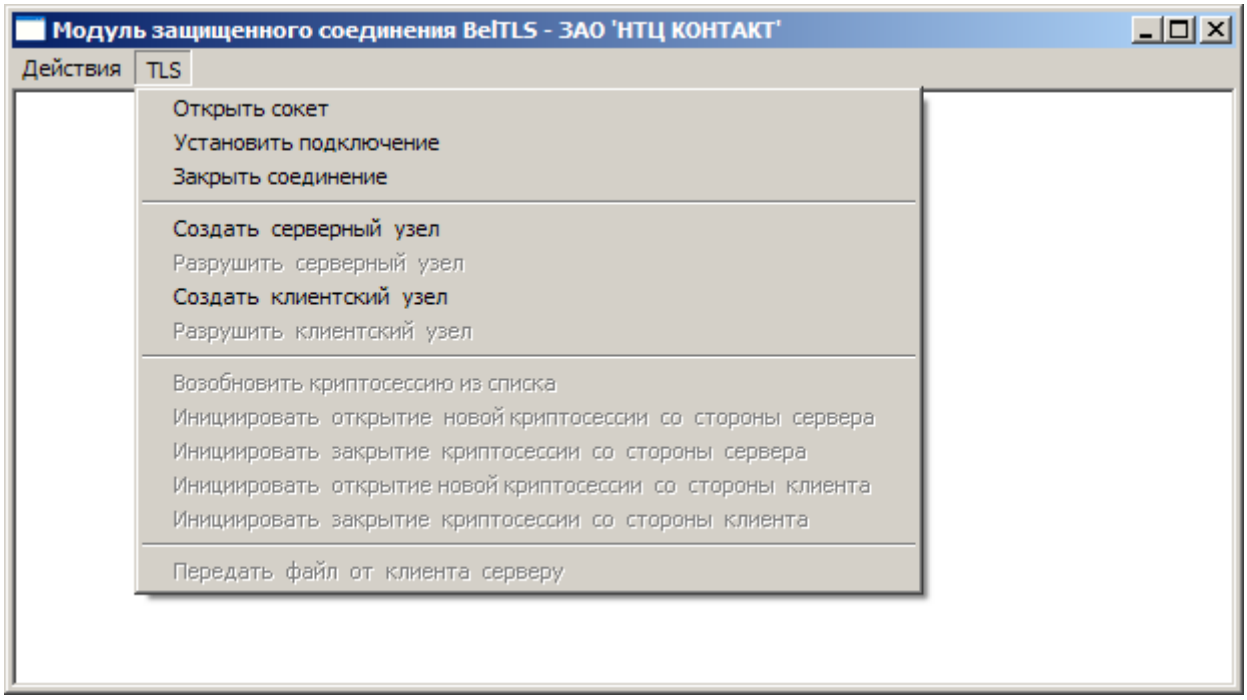

Рис. 182

1. Установка соединения на между устройствами на уровне сокетов.

Для установки соединения между устройствами на уровне сокетов необходимо на одном устройстве (сервере) сначала выбрать пункт меню «Открыть сокет», а затем на другом (клиенте) – «Установить подключение». В случае ошибки при открытии сокета или при попытке повторно открыть уже открытый сокет будет выдано сообщение как на рис. 183, в противном случае приложение продолжит свою работу.

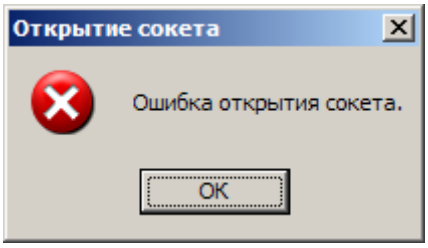

Рис. 183

При успешном связывании на сервере (рис. 184) и на клиенте (рис. 185) будут выведены соответствующие сообщения.

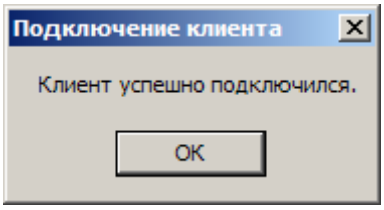

Рис. 184

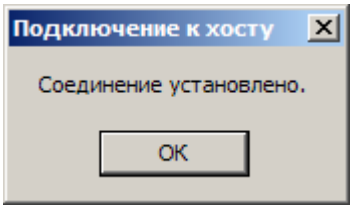

Рис. 185

2. Создание узлов TLS

Для дальнейшей работы необходимо создать клиентский и серверный TLS-узлы выбрав из меню «TLS» пункты «Создать серверный узел» и «Создать клиентский узел». Значения не имеет то, на каком устройстве будет создан клиентский TLS-узел и на каком серверный.

После успешного создания узлов на экране отображаются соответствующие сообщения (рис. 186, 187).

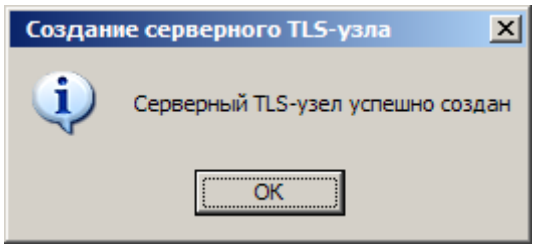

Рис. 186

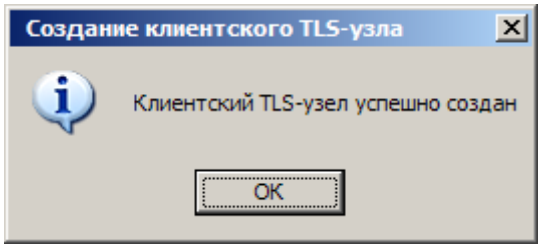

Рис. 187

3. Открытие криптосессии

Для открытия криптосессии используются функции из меню TLS «Инициировать открытие новой криптосессии со стороны сервера» и «Инициировать открытие новой криптосессии со стороны клиента». Вызывать функции необходимо в зависимости от созданного TLS-узла (клиентского или серверного).

При успешном открытии криптосессии, например, со стороны клиента будет выведено сообщение, представленное на рис. 188.

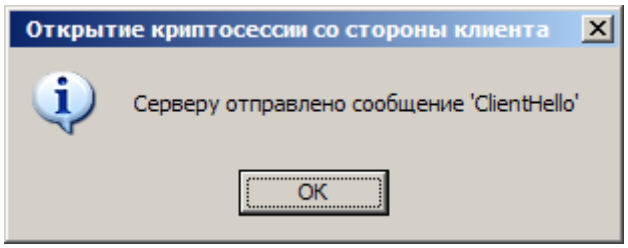

Рис. 188

После успешного открытия криптосессии на стороне сервера отобразятся сообщение и информация, представленные на рис. 189, 190.

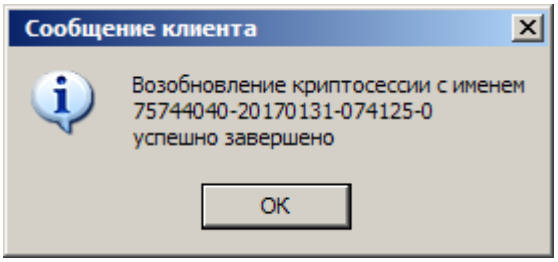

Рис. 189

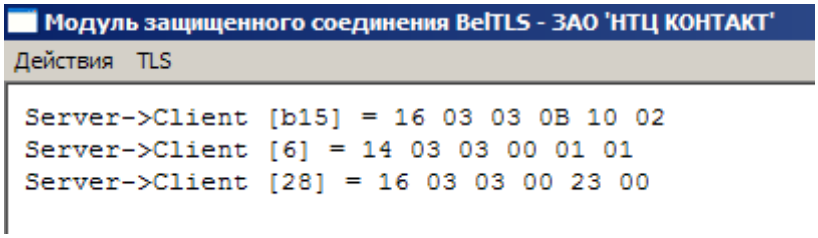

Рис. 190

На стороне клиента при этом отобразятся сообщение и информация, представленные на рис. 191, 192.

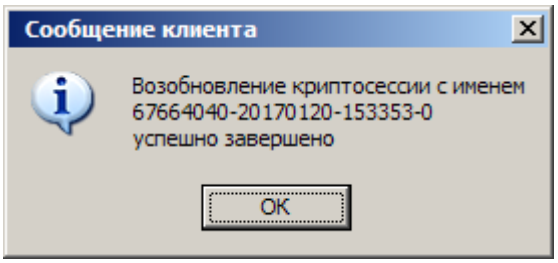

Рис. 191

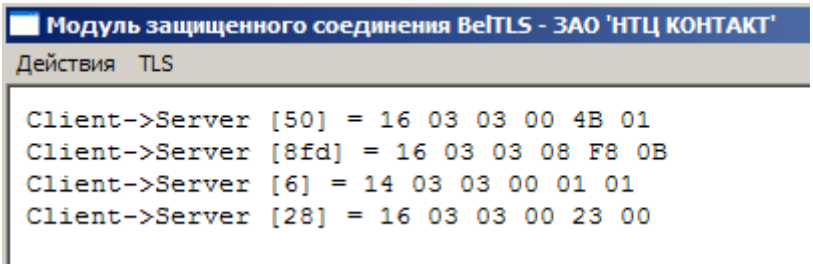

Рис. 192

4. Передача файла

После успешной установки соединения и успешного открытия криптосессии между устройствами можно передать файл от клиента к серверу. Для этого необходимо вызвать функцию из меню TLS «Передать файл от клиента к серверу» и выбрать файл через диалоговое окно. Файл можно передавать размером до 2 мегабайт. При успешной передаче файла будет выведено соответствующее сообщение (рис. 193, 194).

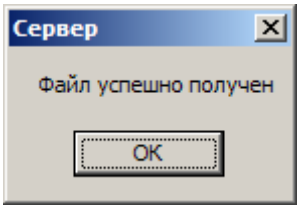

Рис.193

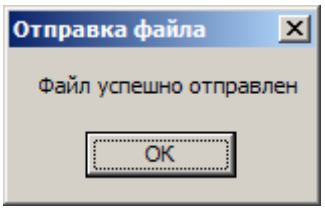

Рис. 194

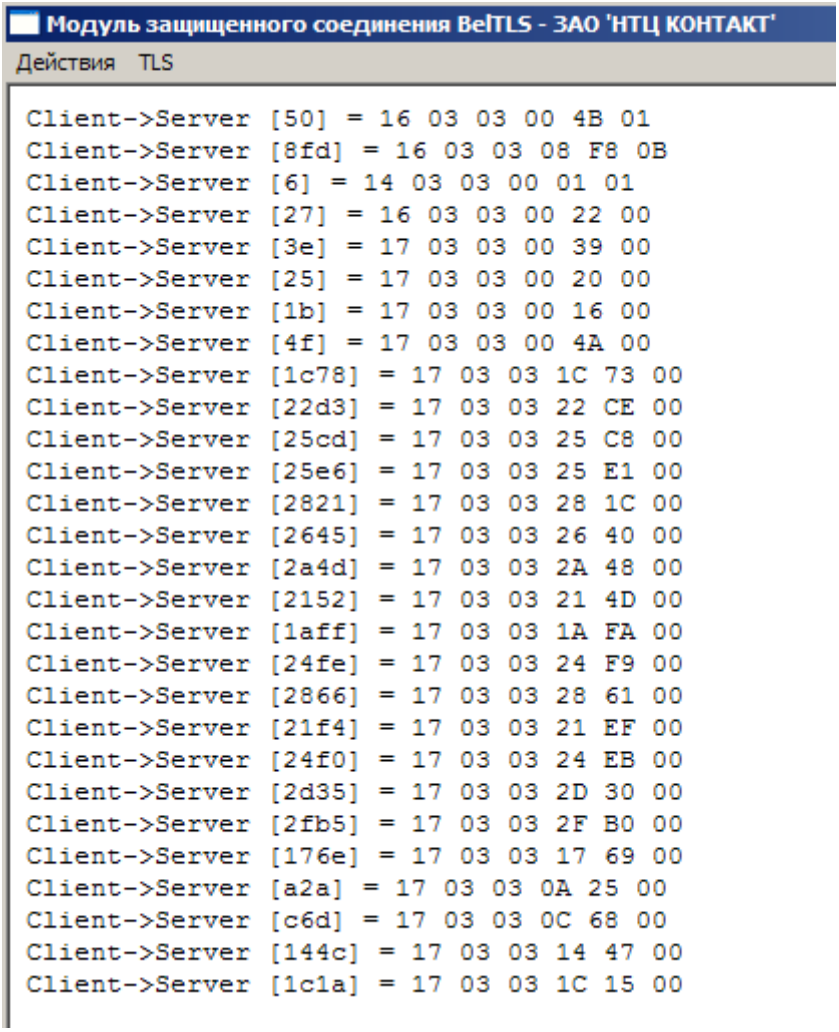

Рис. 195

5. Закрытие криптосессии

Для закрытия открытой криптосессии необходимо вызывать функцию из меню TLS «Инициировать закрытие криптосессии со стороны сервера» или «Инициировать закрытие криптосессии со стороны клиента», в зависимости от созданного TLS-узла, через который установлена активная криптосессия.

При успешном или неуспешном закрытии текущей криптосессии, например, со стороны сервера будут выведены соответствующие сообщения (рис. 196-198).

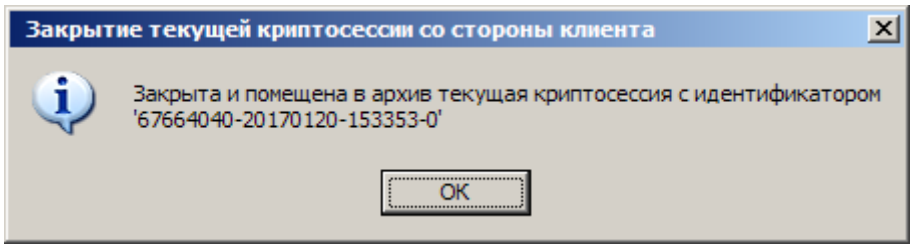

Рис. 196

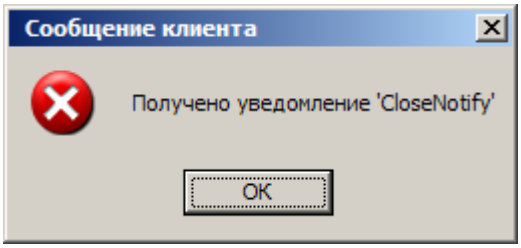

Рис. 197

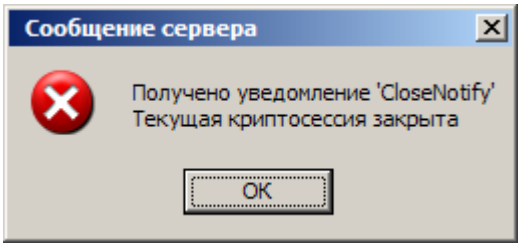

Рис. 198

6. Возобновление криптосессии

Для возобновления криптосессии из списка архивных криптосессии необходимо вызвать функцию из меню TLS «Возобновить криптосессию из списка». После чего появится окно, в котором необходимо выбрать возобновляемую криптосессию (рис. 199).

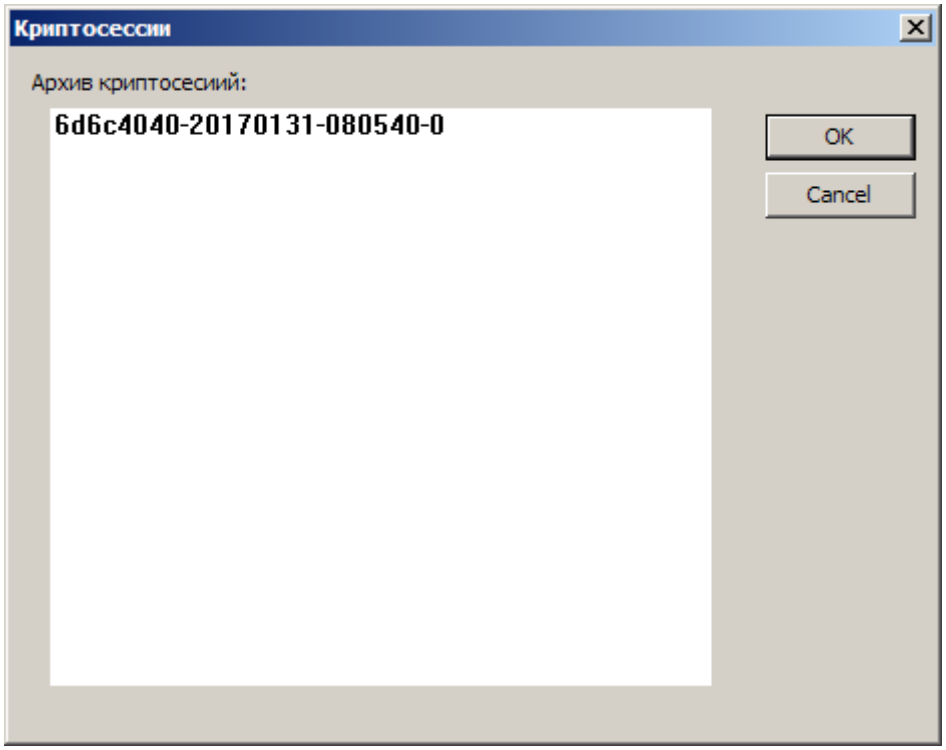

Рис. 199

При успешном возобновлении криптосессии будут выведены соответствующие сообщения (рис. 200, 201).

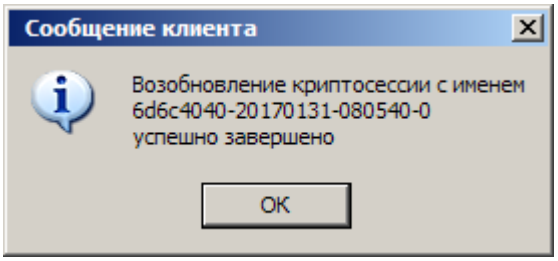

Рис. 200

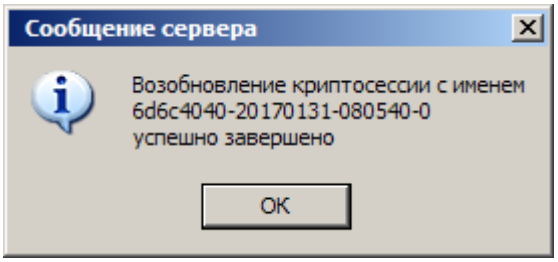

Рис. 201

7. Разрушение TLS-узлов

Для разрушения TLS узлов необходимо вызвать функцию меню TLS «Разрушить серверный узел» или «Разрушить клиентский узел». При успешном разрушении узлов будет выведено соответствующее сообщение (рис. 202, 203).

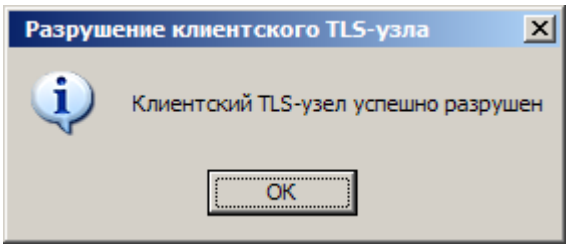

Рис. 202

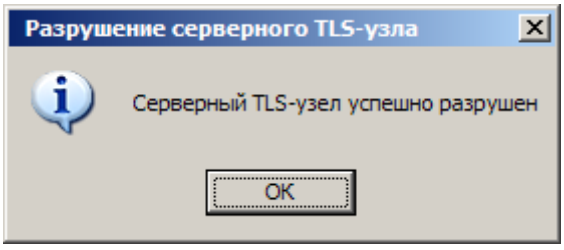

Рис. 203

8. Закрытие соединения

Для закрытия соединения через сокеты необходимо сначала закрыть созданную криптосессию, разрушить созданные TLS-узлы, после чего на стороне сервера вызвать функцию из меню TLS «Закрыть соединение».

6.19 Согласование ключа

6.19.1. Запуск модуля согласования ключа

Для запуска модуля согласования ключа необходимо в рабочей директории КП СОБ в папке KeyAgreement щелкнуть двойным кликом мыши на исполняемом файле KeyAgreement.exe. В случае если модуль согласования ключа запустится без ошибок, на экране отобразится главное окно приложения (рис. 204). Оно содержит панель меню, поле вывода и кнопку «ОК» для завершения работы приложения.

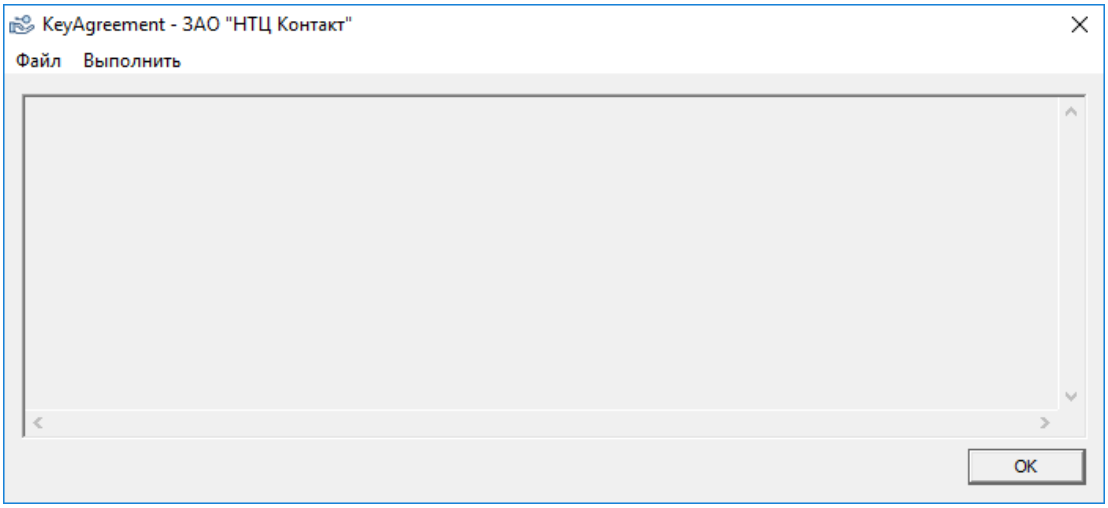

Рис. 204

В поле вывода отображаются сообщения с указанием их типа и даты. Сообщения имеют следующий вид:

«DD.MM.YYYY HH:mm:ss.MsMsMs [MT] message», где

DD – двухзначное представление дня вывода сообщения,

MM - двухзначное представление месяца вывода сообщения,

YYYY - четырехзначное представление года вывода сообщения,

HH - двухзначное представление часа вывода сообщения,

mm - двухзначное представление минут вывода сообщения,

ss - двухзначное представление секунд вывода сообщения,

MsMsMs – трехзначное представление миллисекунд вывода сообщения,

MT – тип сообщения («+» - положительное информационное, «-» - сообщение об ошибке),

message – текст сообщения.

Если при запуске модуля согласования ключа в рабочей директории КП СОБ в папке «KeyAgreement» не будут найдены файлы библиотек «CryptoCont.dll» и «ContactCrypto32LE.dll», на экран будет выведено соответствующее сообщение (рис. 205, 206).

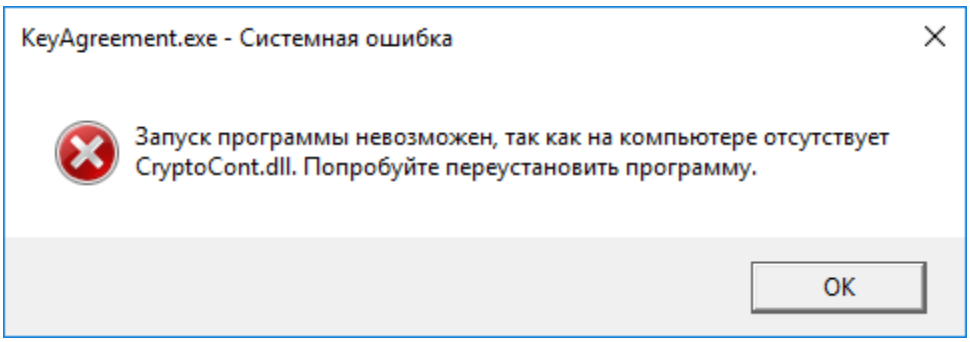

Рис. 205

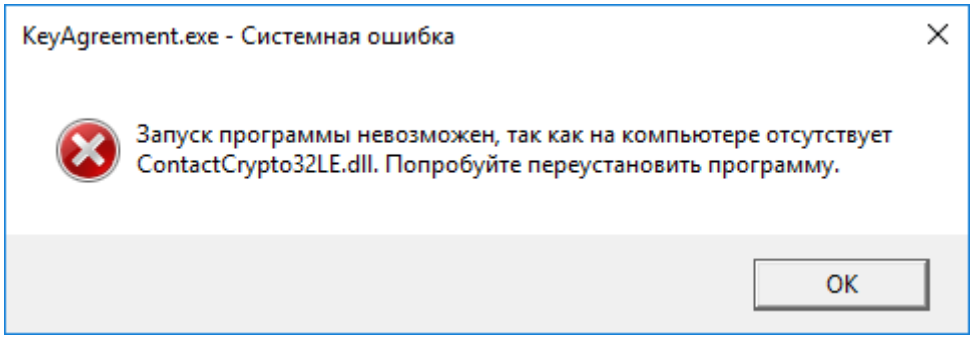

Рис. 206

Если в момент запуска модуля согласования ключа КП СОБ находится в состоянии блокировки, то на экран выведется сообщение, представленное на рисунке 207.

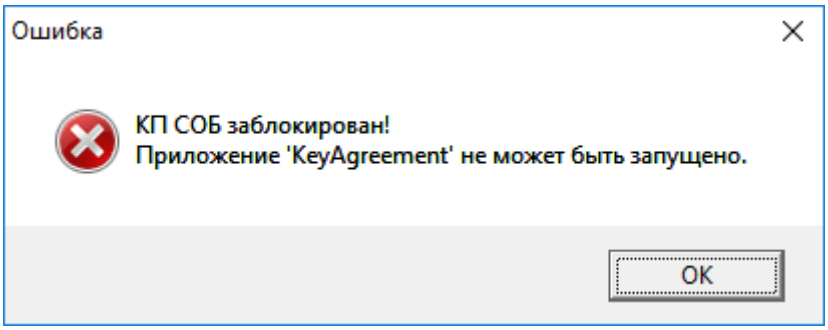

Рис. 207

Если при запуске приложение «KeyAgreement» не может найти, прочитать или разобрать файл с настройками «KeyAgreementSettings.xml», на экран выведется соответствующее сообщение (рис. 208, 209).

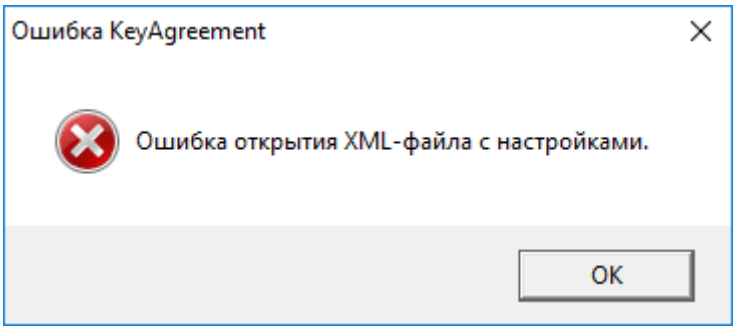

Рис. 208

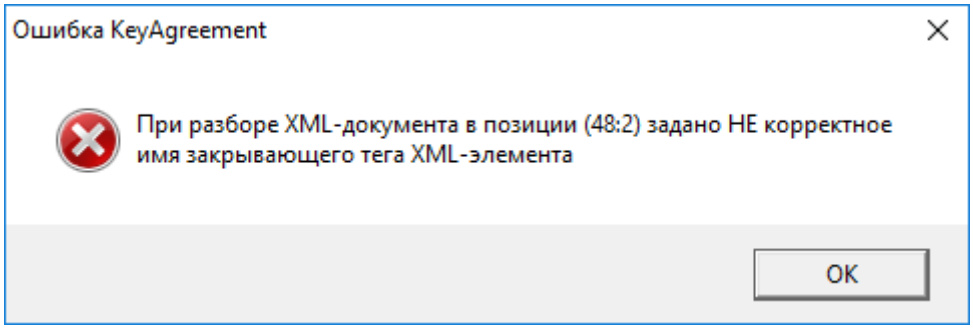

Рис. 209

6.19.2. Настройка модуля согласования ключа

Настройка параметров приложения осуществляется после его запуска. Для этого необходимо в главном окне приложения выбрать из меню «Файл» пункт «Параметры…» (рис. 210) и открыть нужную вкладку в диалоговом окне «Параметры KeyAgreement».

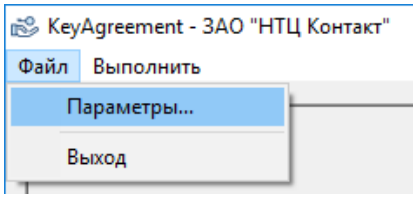

Рис. 210

Настройка производится в зависимости от того, в каком режиме приложение будет работать – в режиме сервера или в режиме клиента.

6.19.2.1. Настройка модуля согласования ключа для работы в режиме сервера осуществляется в диалоговом окне «Параметры KeyAgreement» на вкладке «Сервер» (рис. 211).

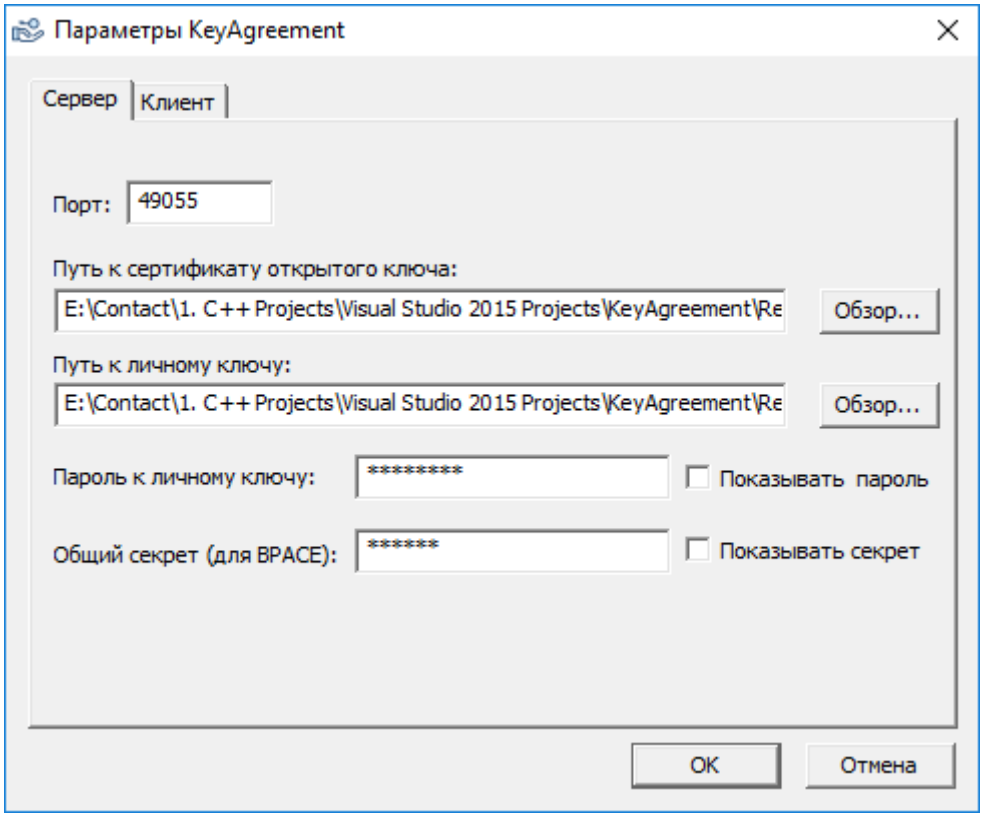

Рис. 211

В поле «Порт» необходимо указать номер порта, на котором будет запущен слушающий сокет. Допустим ввод только чисел.

В поле «Путь к сертификату открытого ключа» необходимо указать путь к СОК сервера, который будет участвовать в протоколе формирования общего ключа. Для того чтобы указать файл СОК, необходимо нажать кнопку «Обзор…» рядом с полем «Путь к сертификату открытого ключа». Откроется стандартное диалоговое окно выбора файла (рис. 212).

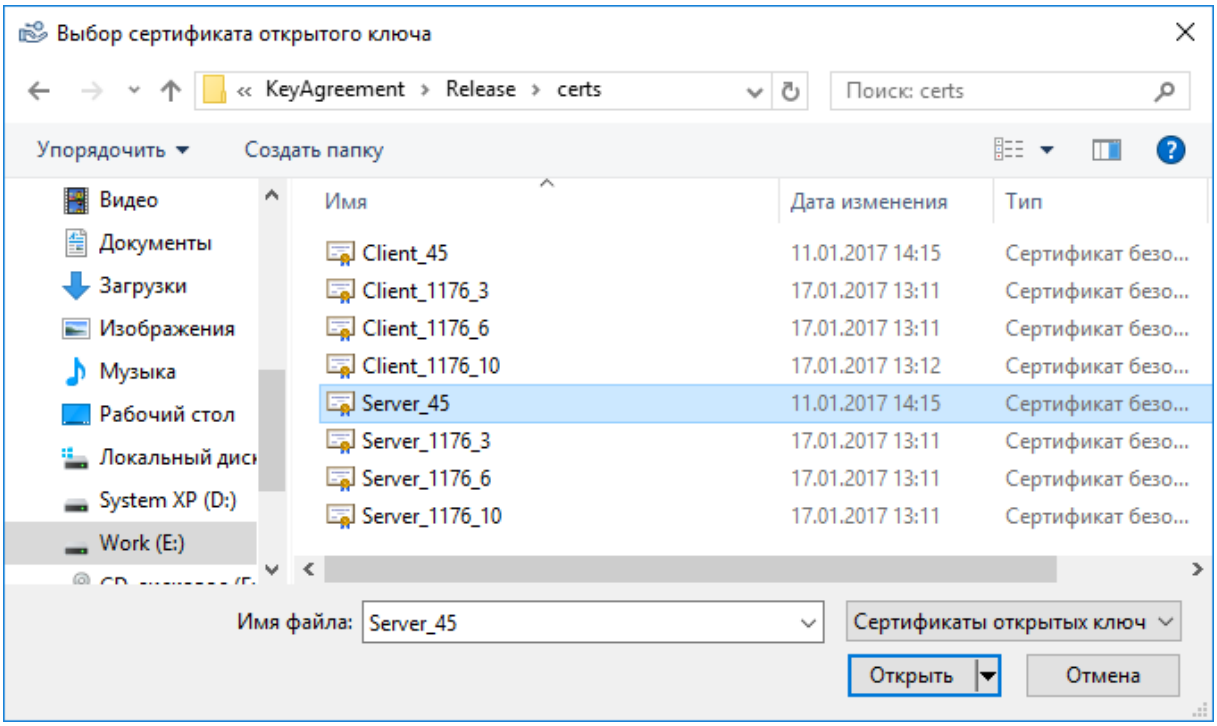

Рис. 212

В открывшемся окне необходимо выбрать файл СОК из файловой системы и нажать кнопку «Открыть». Допустим выбор файла СОК с расширением «.cer». Путь к выбранному файлу отобразится в поле «Путь к сертификату открытого ключа».

В поле «Путь к личному ключу» необходимо указать путь к личному ключу сервера, который будет участвовать в протоколе формирования общего ключа. Для того чтобы указать файл личного ключа, необходимо нажать кнопку «Обзор…» рядом с полем «Путь к личному ключу». Откроется стандартное диалоговое окно выбора файла (рис. 213).

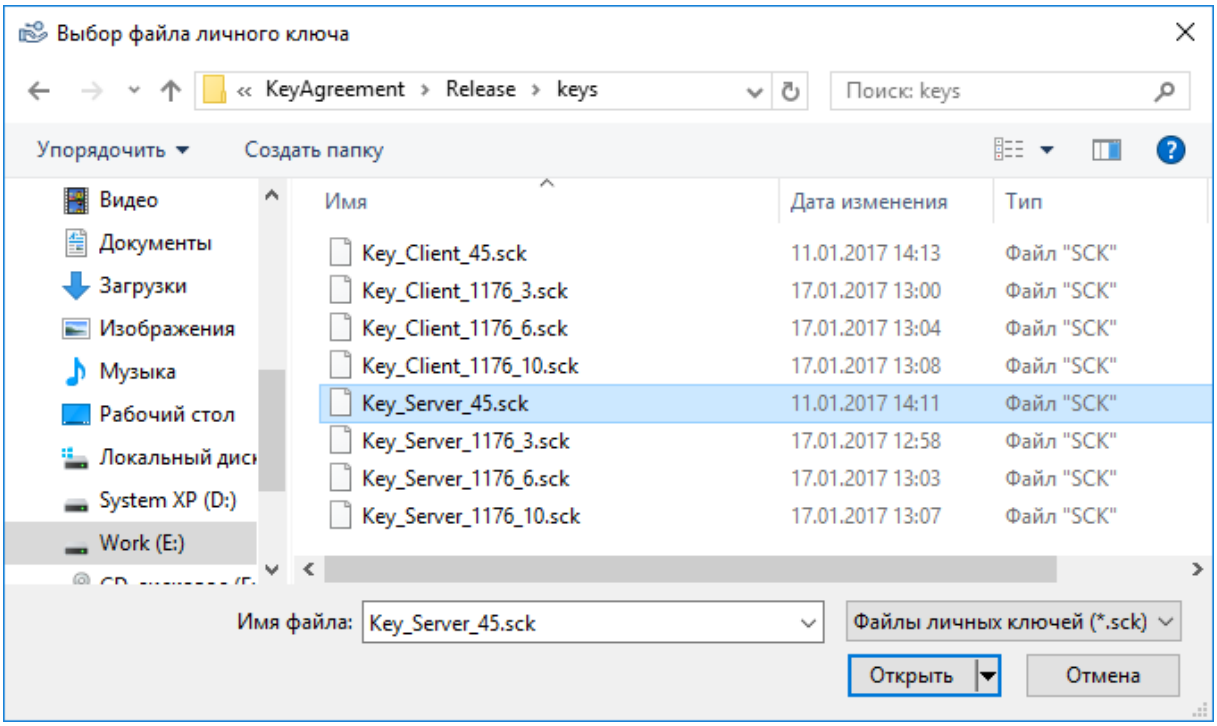

Рис. 213

В открывшемся окне необходимо выбрать файл личного ключа и нажать кнопку «Открыть». Допустим выбор файла личного ключа с расширением «.sck». Путь к выбранному файлу отобразится в поле «Путь к личному ключу».

В поле «Пароль к личному ключу» необходимо указать пароль к выбранному файлу личного ключа. По умолчанию все введенные в это поле символы отображаются символами «*». Чтобы визуально проверить корректность введенного пароля можно установить галочку «Показывать пароль» рядом с полем «Пароль к личному ключу». Введенный пароль в таком случае будет отображаться в явном виде (рис. 214).

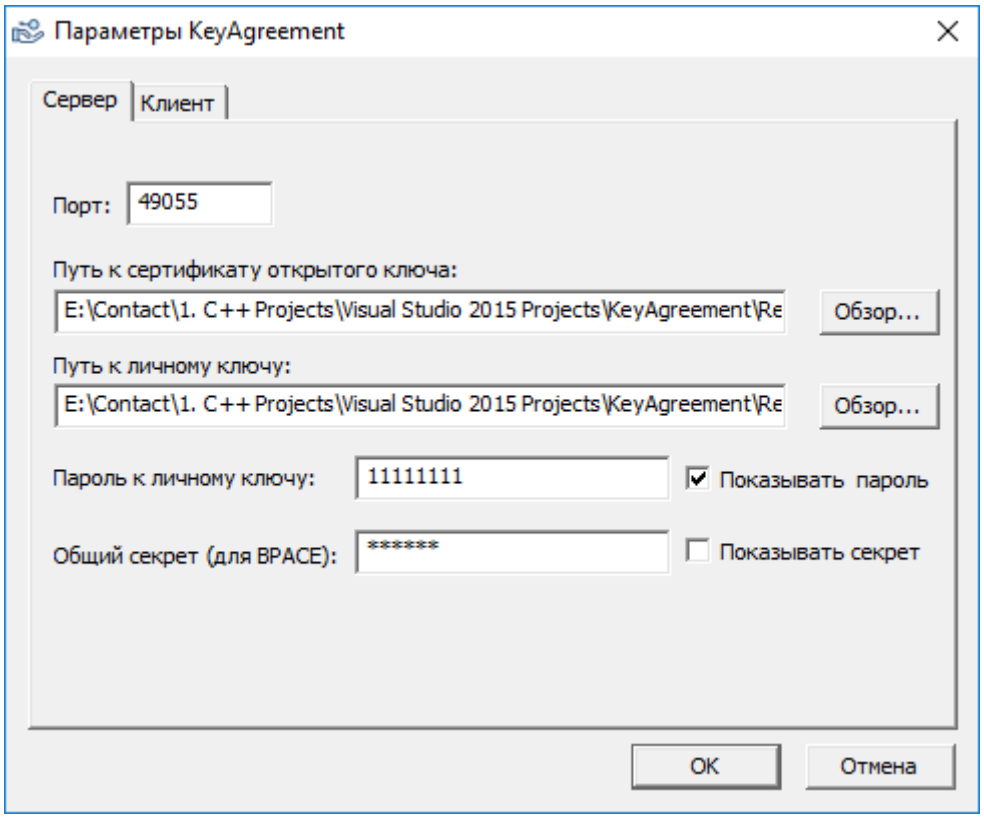

Рис. 214

В поле «Общий секрет (для BPACE)» необходимо указать общий секрет на случай, если от клиента поступит запрос на согласование ключа по протоколу BPACE, описанному в СТБ 34.101.66. Галочка «Показывать секрет» предназначена для того, чтобы отображать или скрывать значение введенного общего секрета.

Чтобы измененные параметры вступили в силу, после завершения редактирования необходимо в диалоговом окне «Параметры KeyAgreement» нажать кнопку «ОК».

6.19.2.2. Настройка модуля согласования ключа для работы в режиме клиента осуществляется в диалоговом окне «Параметры KeyAgreement» на вкладке «Клиент».

В области «Адрес сервера» необходимо ввести IP-адрес машины, на которой работает сервер, и номер порта прослушивающего сокета.

В выпадающем списке «Алгоритм согласования ключа» необходимо выбрать один из шести предложенных вариантов протокола формирования общего ключа.

В выпадающем списке «Алгоритм и режим шифрования» необходимо выбрать один из пяти предложенных вариантов алгоритмов и режимов шифрования данных на согласованном ключе при передаче файла от клиента серверу.

Дальнейший набор параметров зависит от того, какой алгоритм и протокол согласования ключа был выбран.

Если выбран вариант «РД РБ ПФОК. Протокол без аутентификации сторон» или «РД РБ ПФОК. Протокол одностороннего формирования ключа», то дополнительных параметров не требуется (рис. 215).

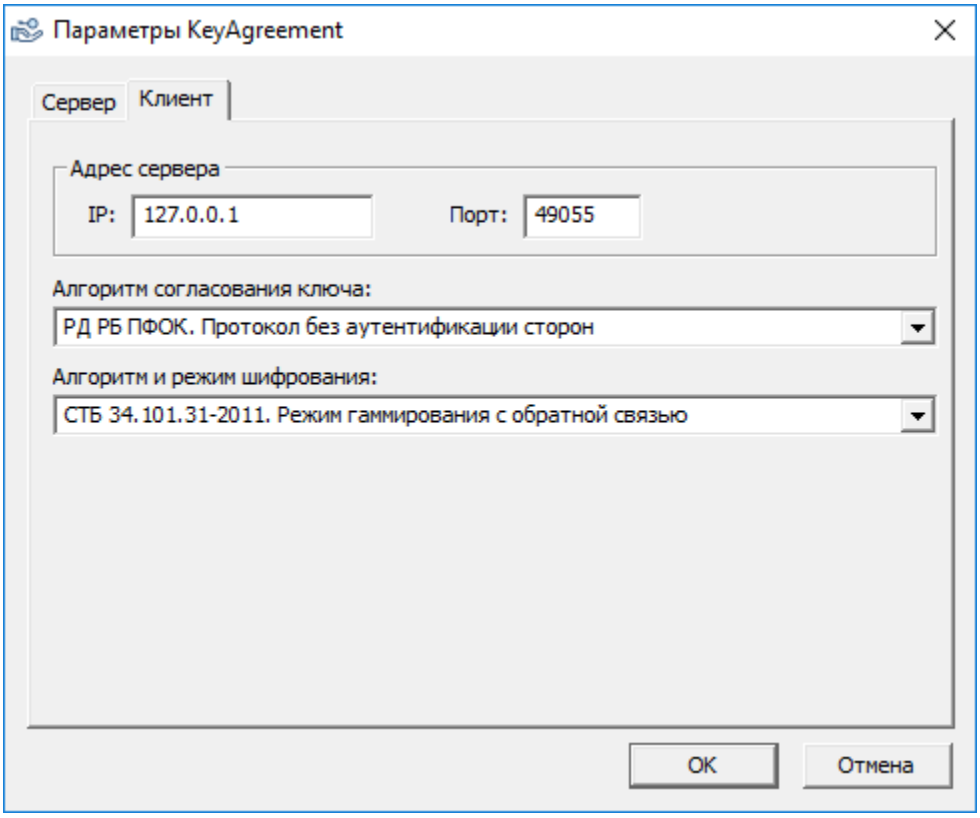

Рис. 215

Если выбран вариант «РД РБ ПФОК. Протокол с аутентификацией сторон», «СТБ 34.101.66-2014. Протокол BMQV» или «СТБ 34.101.66-2014. Протокол BSTS» (рис. 216), то необходимо указать следующие параметры:

- в поле «Путь к сертификату открытого ключа» необходимо указать путь к СОК клиента, который будет участвовать в протоколе формирования общего ключа. Для того чтобы указать файл СОК, необходимо нажать кнопку «Обзор…» рядом с полем «Путь к сертификату открытого ключа». Откроется стандартное диалоговое окно выбора файла. В открывшемся окне необходимо выбрать файл СОК из файловой системы и нажать кнопку «Открыть». Допустим выбор файла СОК с расширением «.cer». Путь к выбранному файлу отобразится в поле «Путь к сертификату открытого ключа»;

- в поле «Путь к личному ключу» необходимо указать путь к личному ключу клиента, который будет участвовать в протоколе формирования общего ключа. Для того чтобы указать файл личного ключа, необходимо нажать кнопку «Обзор…» рядом с полем «Путь к личному ключу». Откроется стандартное диалоговое окно выбора файла. В открывшемся окне необходимо выбрать файл личного ключа и нажать кнопку «Открыть». Допустим выбор файла

личного ключа с расширением «.sck». Путь к выбранному файлу отобразится в поле «Путь к личному ключу».

- в поле «Пароль к личному ключу» необходимо указать пароль к выбранному файлу личного ключа. Галочка «Показывать пароль» предназначена для того, чтобы отображать или скрывать значение введенного пароля.

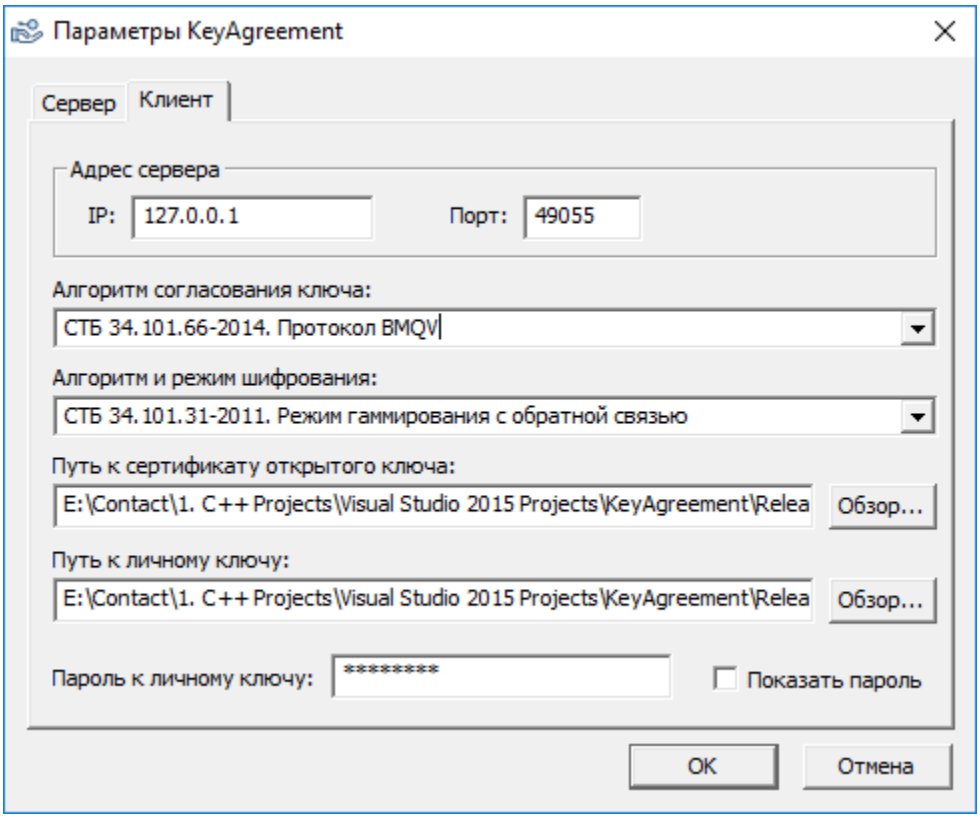

Рис. 216

Если выбран вариант «СТБ 34.101.66-2014. Протокол BPACE», то в поле «Общий секрет» необходимо указать значение общего секрета (рис. 217). Галочка «Показывать секрет» предназначена для того, чтобы отображать или скрывать значение введенного общего секрета.

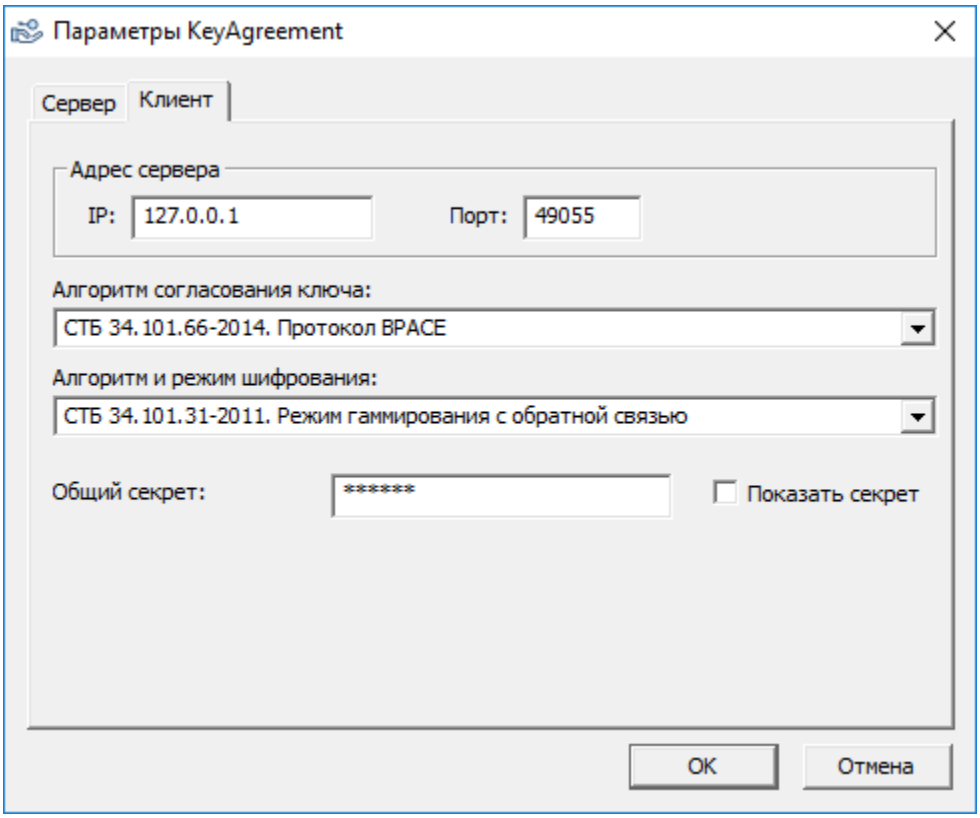

Рис. 217

Чтобы измененные параметры вступили в силу, после завершения редактирования необходимо в диалоговом окне «Параметры KeyAgreement» нажать кнопку «ОК».

6.19.3. Порядок работы модуля согласования ключа

Приложение «KeyAgreement» может работать в двух режимах – режим сервера и режим клиента. Приложение, работающее в режиме сервера, должно запускаться первым.

6.19.3.1. Порядок работы модуля согласования ключа в режиме сервера.

После запуска и настройки сервер необходимо запустить. Для этого нужно выбрать пункт «Запустить сервер» из меню «Выполнить» (рис. 218).

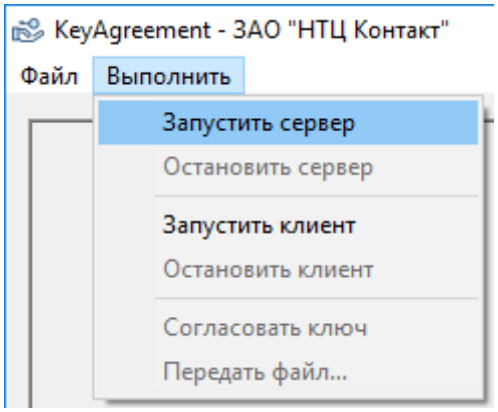

Рис. 218

После успешного запуска сервера в поле вывода отобразится соответствующее сообщение, а также изменится текст в заголовке главного окна (рис. 219).

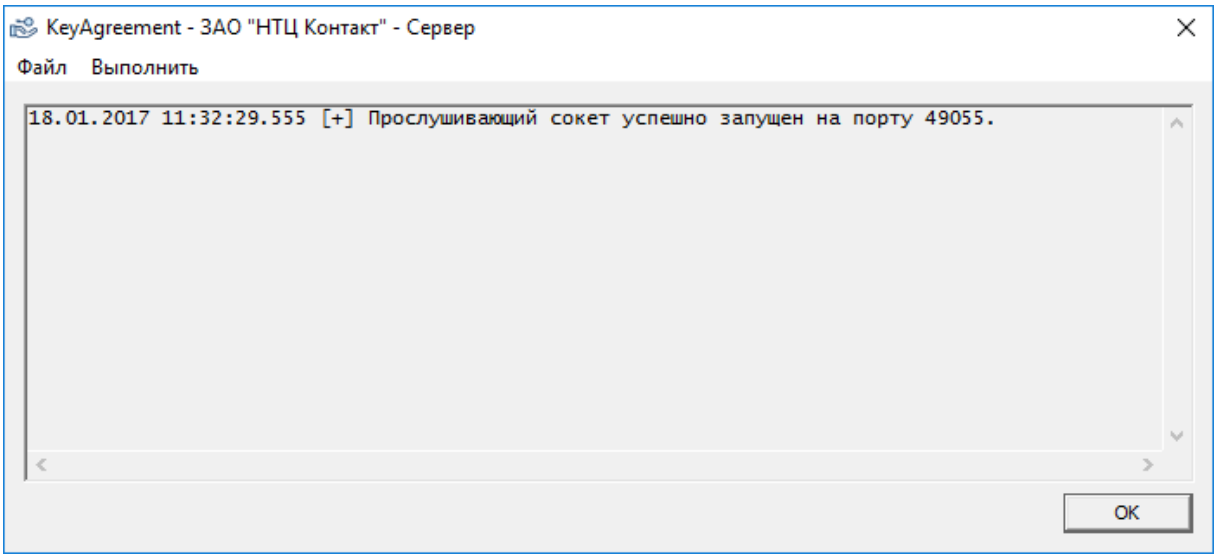

Рис. 219

Если во время запуска произошла какая-то ошибка, то сообщение об этом также отобразится в поле вывода. Например, если на момент запуска сервера указанный в настройках номер порта окажется занятым, то выведется сообщение, представленное на рисунке 220.

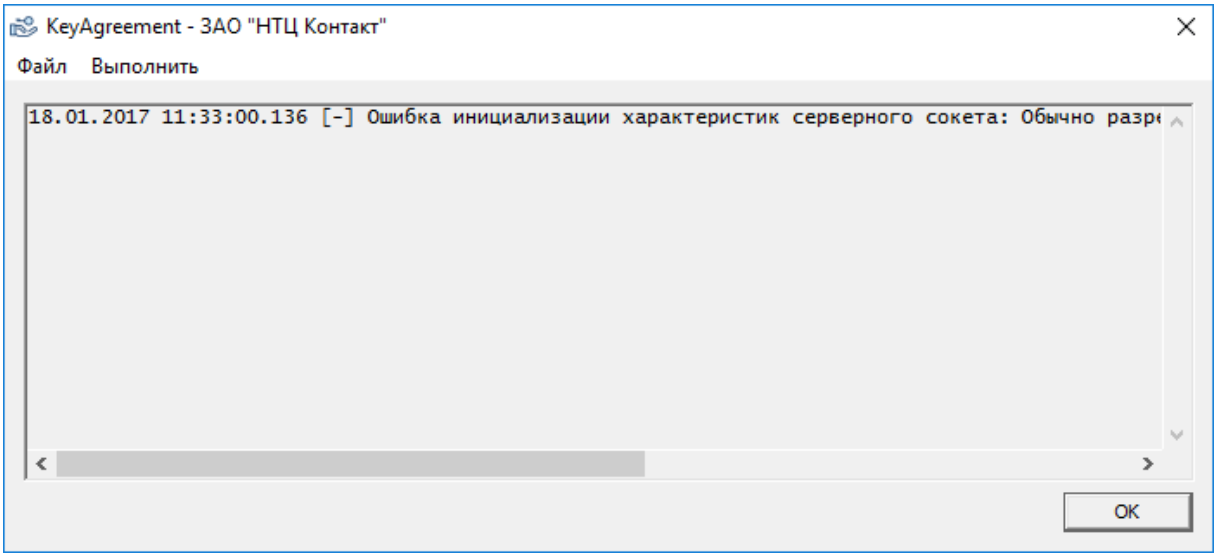

Рис. 220

После запуска прослушивающего сокета сервер работает в режиме ожидании подключения клиента. После подключения клиента и выполненной успешно инициализации параметров сессии в поле вывода отобразится соответствующее сообщение (рис. 221).

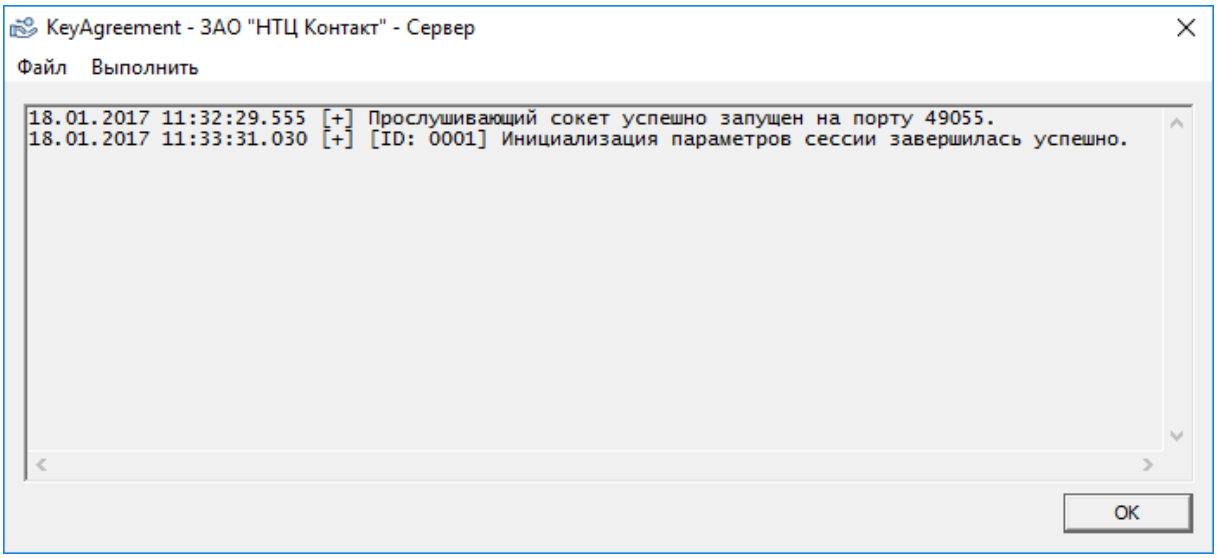

Рис. 221

После успешно завершенной процедуры согласования ключа в поле вывода отобразится сообщение, представленное на рисунке 222.

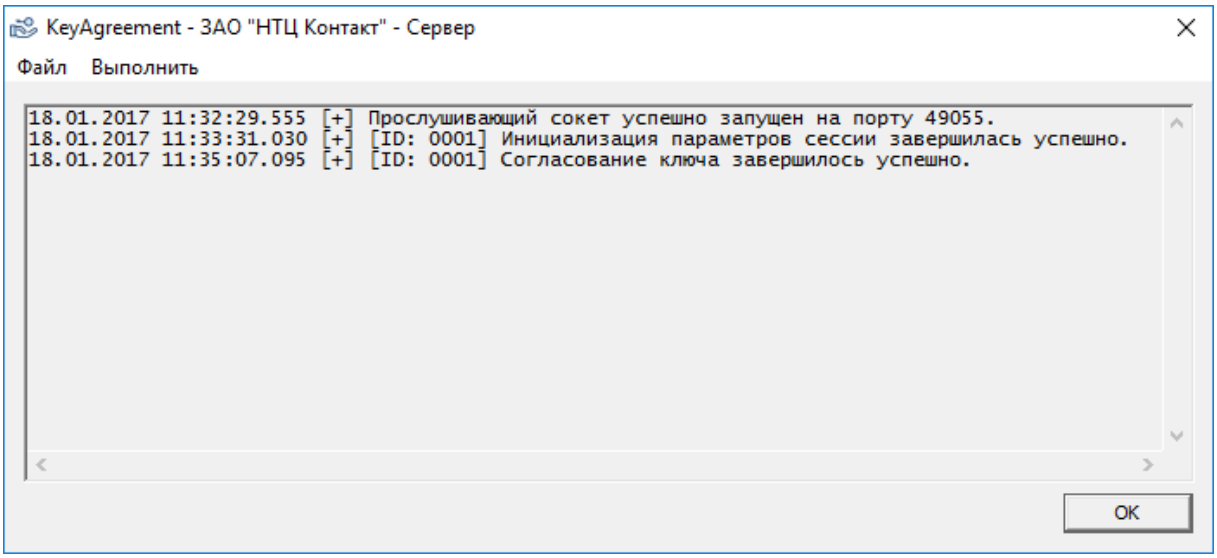

Рис. 222

При передаче от клиента зашифрованных на согласованном раннее ключе данных сервер принимает данные, расшифровывает на том же ключе и сохраняет получившиеся данные в рабочую директорию КП СОБ в папку «KeyAgreement\received» в файл с именем следующего вида:

«DD-MM-YYYY_HH-mm-ss-MsMsMs_any_name.ext», где

DD – двухзначное представление дня сохранения файла,

MM - двухзначное представление месяца сохранения файла,

YYYY - четырехзначное представление года сохранения файла,

HH - двухзначное представление часа сохранения файла,

mm - двухзначное представление минут сохранения файла,

ss - двухзначное представление секунд сохранения файла,

MsMsMs – трехзначное представление миллисекунд сохранения файла,

any_name.ext – имя файла, которое пришло в запросе от клиента вместе с зашифрованными данными.

После принятия сервером зашифрованных данных и успешного расшифрования в поле вывода отобразится сообщение, представленное на рисунке 223.

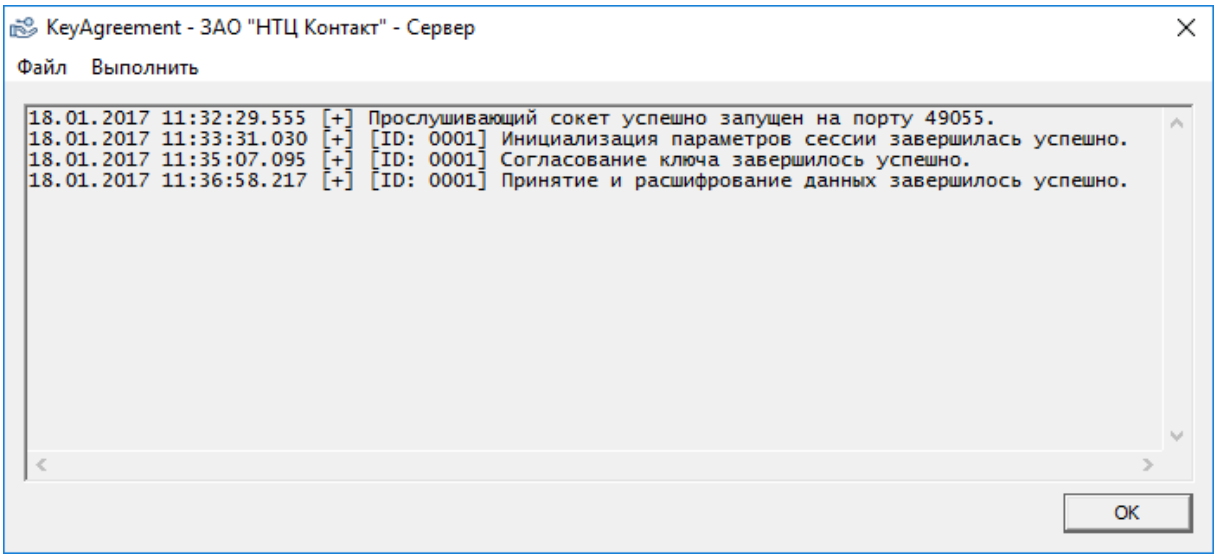

Рис. 223

Если клиент присылает сообщение о том, что он завершает текущую сессию, то в поле вывода отобразится сообщение, представленное на рисунке 224.

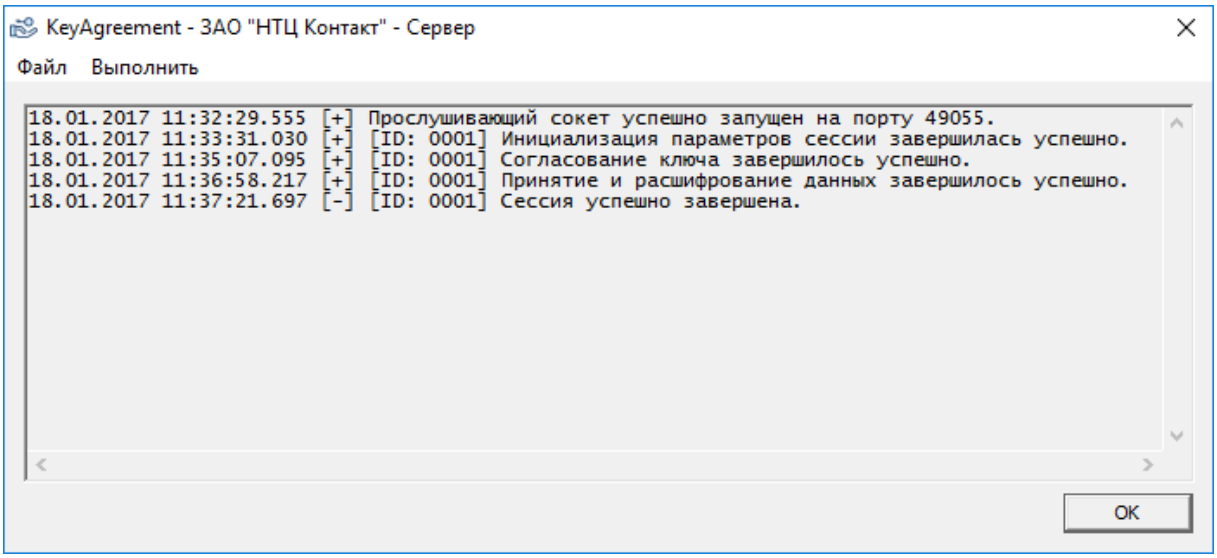

Рис. 224

Для корректного завершения работы сервера необходимо дождаться отключения всех клиентов и выбрать пункт «Остановить сервер» из меню «Выполнить» (рис. 225), после чего в поле вывода отобразится соответствующее сообщение (рис. 226).

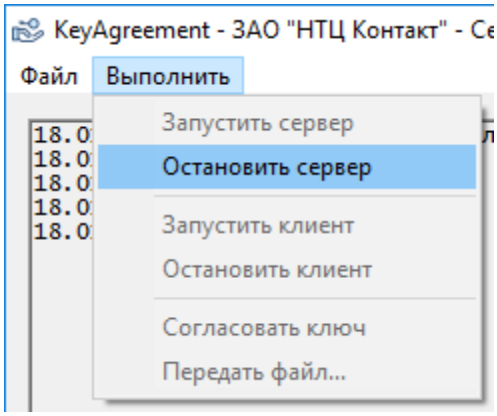

Рис. 225

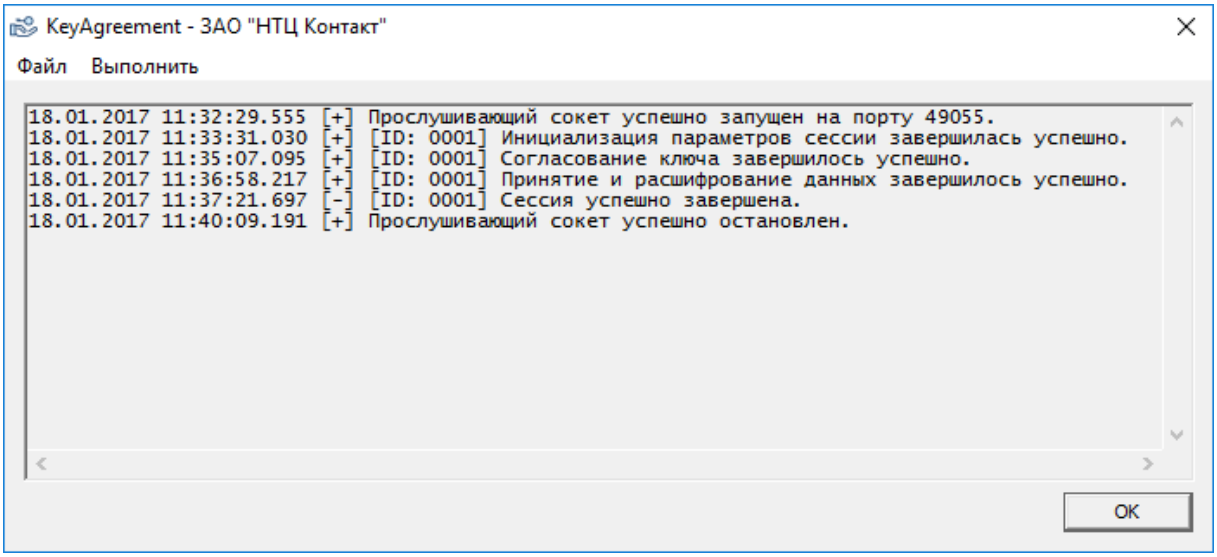

Рис. 226

6.19.3.2. Порядок работы модуля согласования ключа в режиме клиента.

После запуска и настройки приложения клиент необходимо запустить. Запускать клиент стоит после запуска сервера. Для того чтобы запустить клиент необходимо выбрать пункт «Запустить клиент» из меню «Выполнить» (рис. 227).

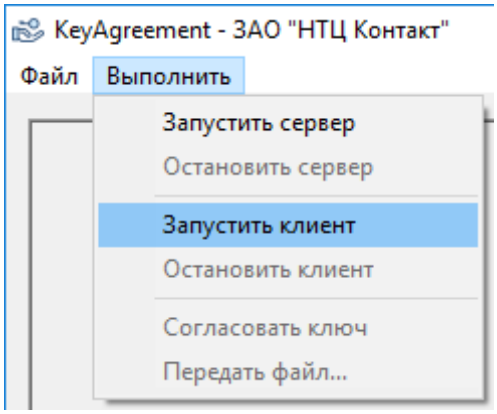

Рис. 227

После успешного запуска клиента в поле вывода отобразятся соответствующие сообщения, а также изменится текст в заголовке главного окна (рис. 228).

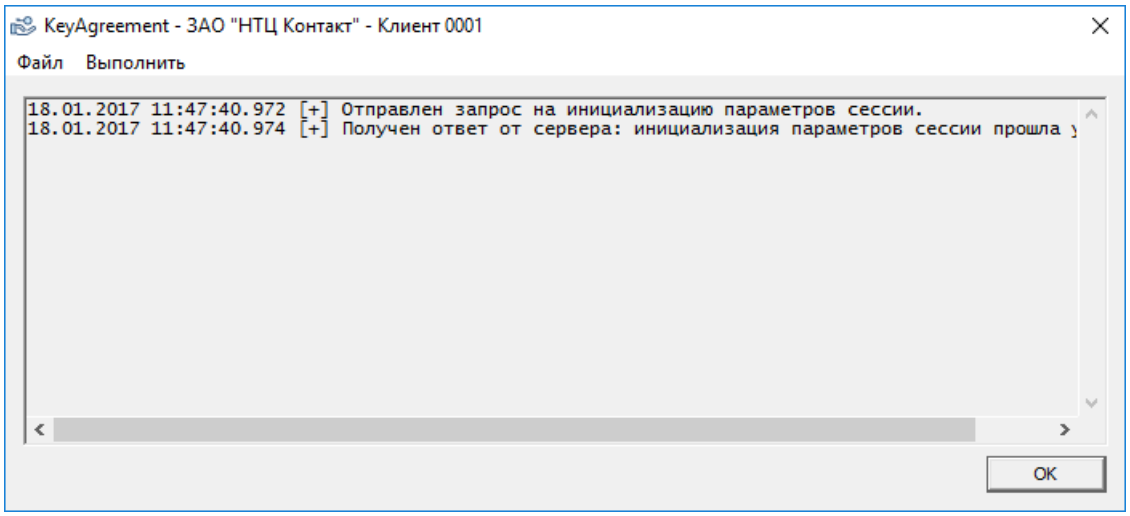

Рис. 228

Если при запуске клиента сервер недоступен, то в поле вывода отобразится сообщение, представленное на рисунке 229.

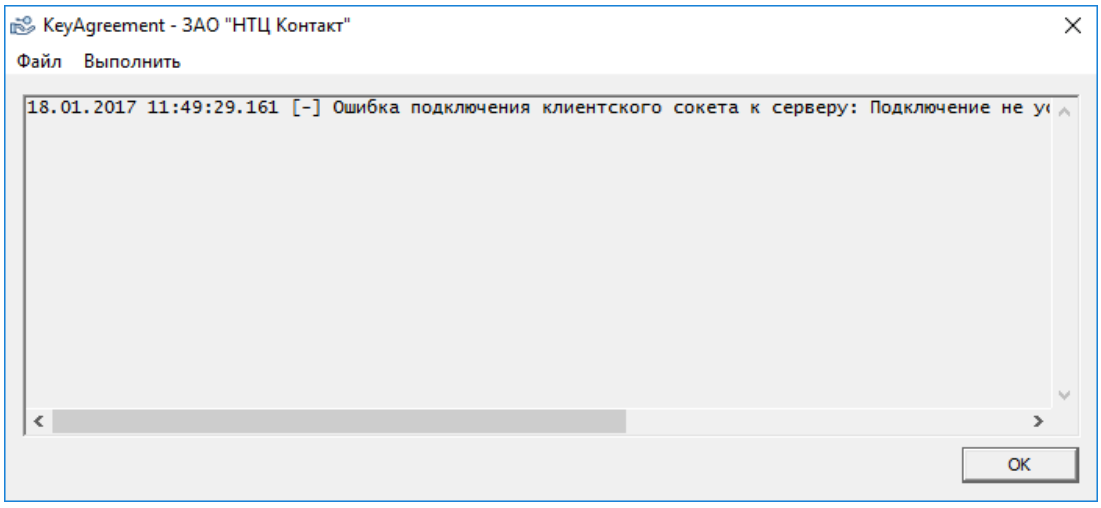

Рис. 229

После успешного подключения клиента к серверу и инициализации параметров сессии, клиенту становится доступна процедура согласования ключа. Для этого необходимо выбрать пункт «Согласовать ключ» из меню «Выполнить» (ри. 230).

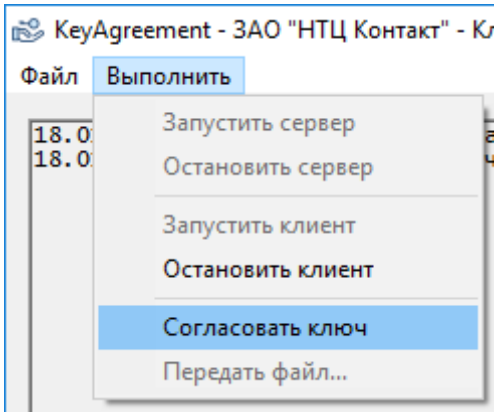

Рис. 230

После успешного согласования ключа в поле вывода отобразятся сообщения, представленные на рисунке 231.

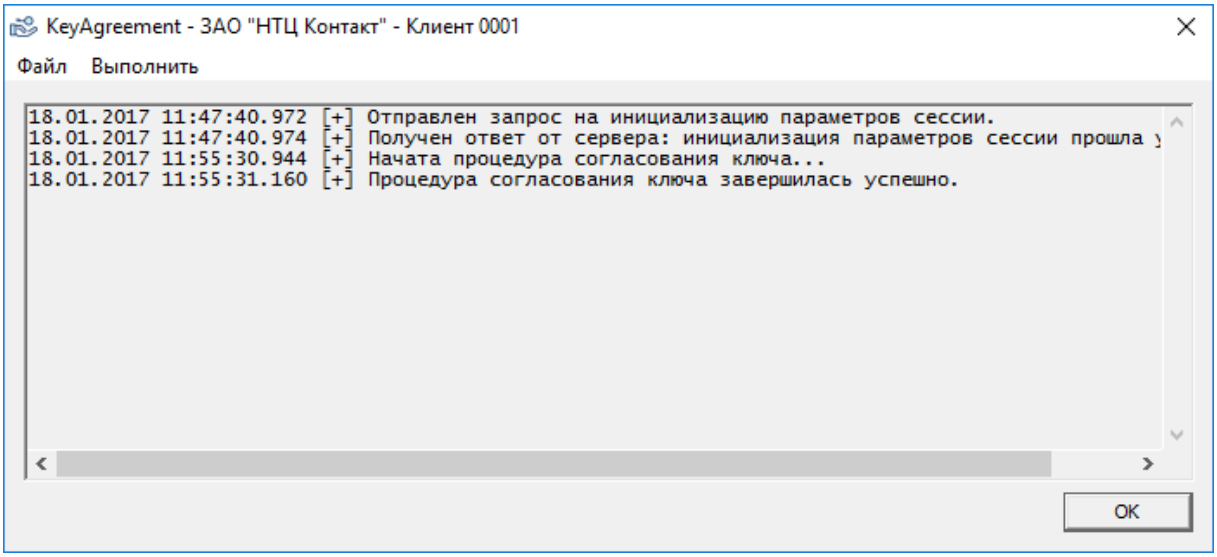

Рис. 231

После того как между клиентом и сервером успешно согласован ключ, клиенту доступна возможность передать серверу файл, зашифрованный на согласованном ключе. Для этого необходимо выбрать пункт «Передать файл…» из меню «Выполнить» (рис. 232).

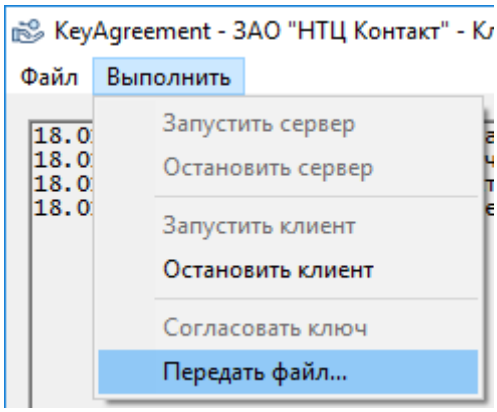

Рис. 232

В результате откроется стандартное диалоговое окно выбора файла из файловой системы, где необходимо указать файл для передачи и нажать кнопку «Открыть» (рис. 233). Размер файла при этом не должен превышать 32 Мбайта.

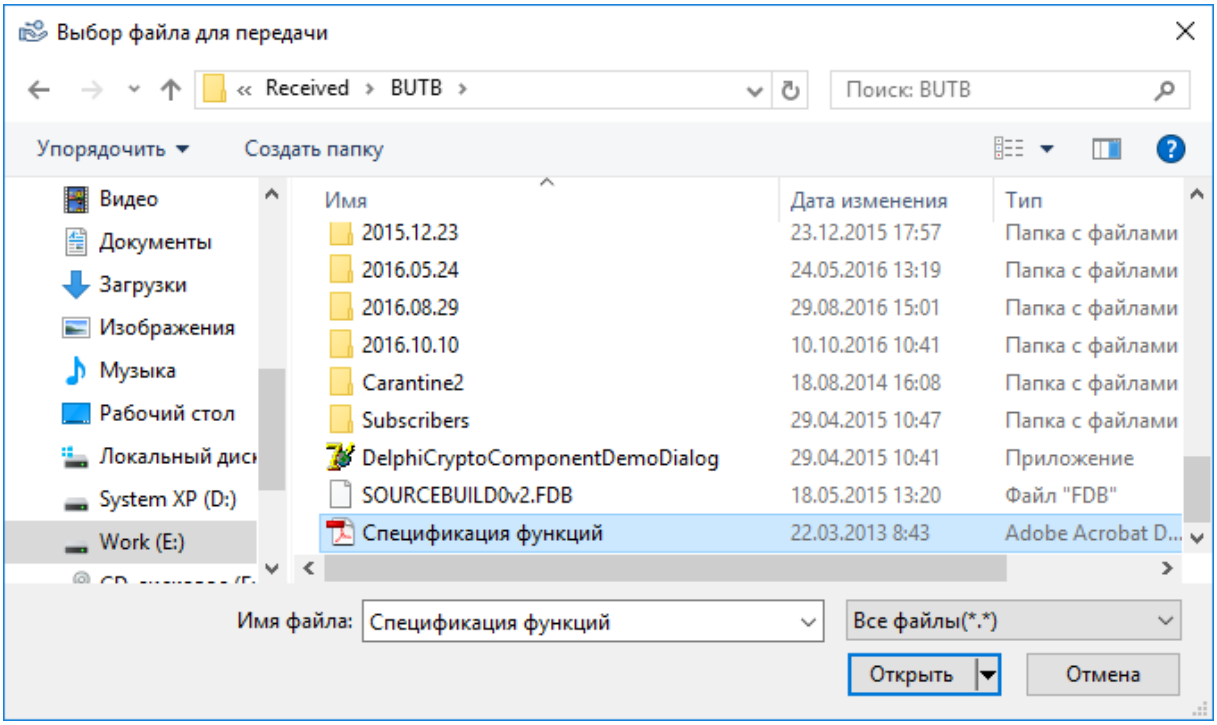

Рис. 233

После успешного зашифрования данных, пересылки их серверу и получения положительного ответа от сервера в поле вывода отобразится сообщение, представленное на рисунке 234.

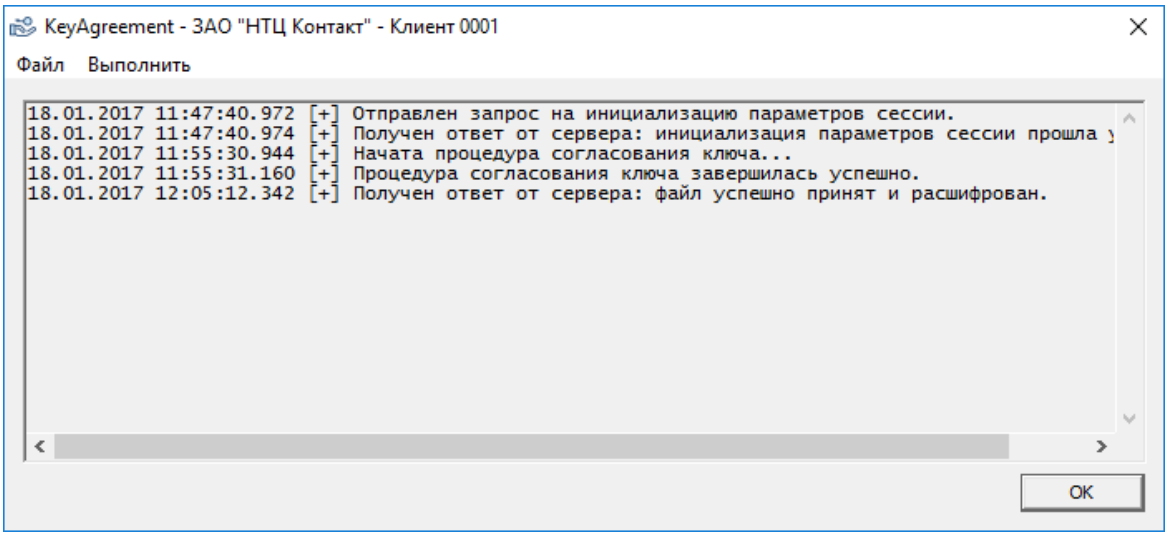

Рис. 234

Для корректного завершения работы клиента необходимо выбрать пункт «Остановить клиент» из меню «Выполнить» (рис. 235).

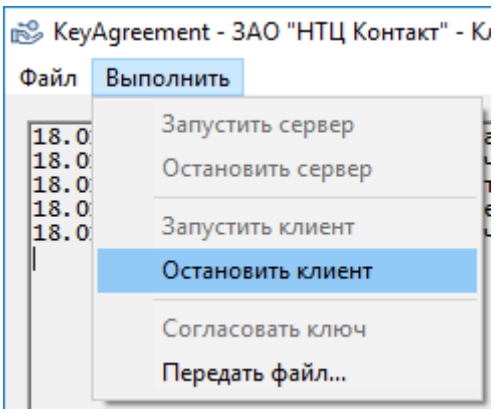

Рис. 235

После успешной остановки клиента в поле вывода отобразится соответствующее сообщение (рис. 236).

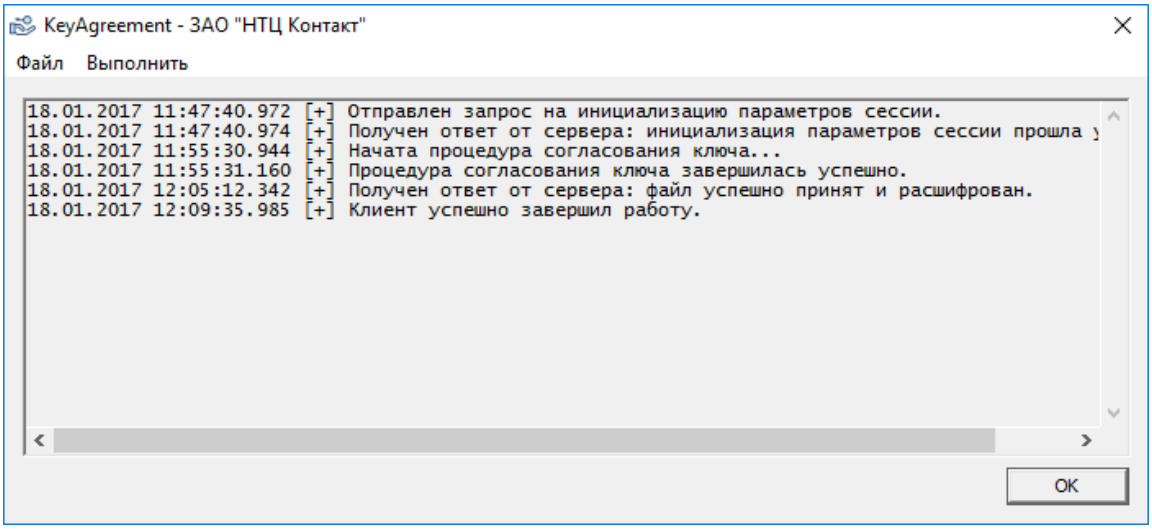

Рис. 236

6.19.3.3. Для просмотра версии модуля согласования ключа необходимо нажать левой кнопкой мыши на иконку приложения в левом верхнем углу ( ) и в появившемся меню выбрать пункт «About KeyAgreement…» (рис. 237).

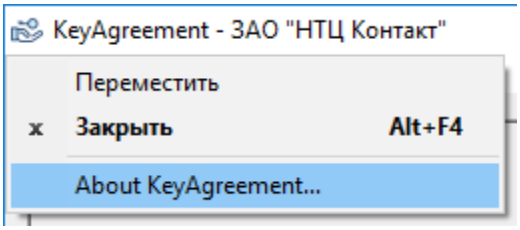

Рис. 237

В открывшемся диалоговом окне «Справка KeyAgreement» отображается версия модуля согласования ключа (рис. 238).

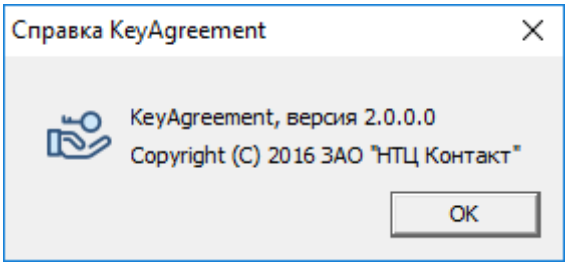

Рис. 238

6.19.4. Завершение работы модуля согласования ключа

Корректно завершить работу приложения можно после закрытия всех текущих сессий выполнением одного из следующих действий:

- нажать кнопку «ОК» в правом нижнем углу главного окна приложения;

- нажать кнопку закрытия приложения ( ) в правом верхнем углу главного окна приложения;

- нажать левой кнопкой мыши на иконку в левом верхнем углу ( ) и в появившемся меню выбрать пункт «Закрыть»;

- выбрать пункт «Выход» их меню «Файл» (рис. 239).

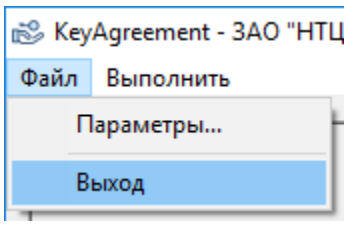

Рис. 239

7. НАСТРОЙКА КП СОБ

Настройка КП СОБ осуществляется путем редактирования записей в текстовом файле «CryptoServiceSettings.xml», находящимся в директории, из которой загружается программа.

Внесение изменений в файл может быть произведено любым тестовым редактором.

Все настройки для удобства разбиваются на отдельные блоки – секции, в которых настраиваемые параметры относятся к одному из свойств программы.

Структура файла настройки представлена в приложении 2.

Для выполнения криптографических операций КП СОБ должен иметь доступ к СОК пользователя, запрашивающего криптооперацию. СОК может быть получен из локального хранилища или из хранилища сертификатов КПА УЦ. Требуемый сертификат запрашивается в следующей последовательности:

1) запрос СОК из локального хранилища;
2) запрос СОК из хранилища сертификатов КПА УЦ, при этом возможны варианты:
   а) запрос по протоколу http;
   б) зарос по электронной почте.

Запись СОК в локальное хранилище осуществляется следующим образом:

1) скопировать СОК в директорию «CRYPTO_SERVICE_DIR\CertificateStorage\ForCertificatesLoading»;
2) запустить КП СОБ и выбрать в пользовательском меню пункт «Загрузить сертификаты из файлов».

Для выполнения криптоопераций КП СОБ должен иметь актуальную базу списка отозванных сертификатов (СОС), которая обновляется либо путем периодического обращения к КПА УЦ по http, либо вручную из файла. Период обращения к КПА УЦ по http настраивается.

Обновление СОС из файла осуществляется следующим образом:

1) Скопировать файл, содержащий СОС в директорию «CRYPTO_SERVICE_DIR\CertificateStorage\ForCRLsLoading»;
2) Запустить КП СОБ и выбрать в пользовательском меню пункт «Обработать СОС из папки».

Основными параметрами КП СОБ являются следующие параметры:

1) Основные параметры настройки, указанные в секции BasicSettings:
   а) аттрибут DebugLogging – параметр логирования отладочной информации;
   б) FrameworkName – путь к главной рабочей библиотеке;
   в) SystrayMenu – список пунктов всплывающего меню приложения.
2) Параметры настройки журналирования, указанные в секции Logging:

а) LocalLogName – имя файла локального журнала;

б) MaxLocalLogSize – максимальный размер файла локального журнала;

в) MessageLevelsMask – фильтр уровня сохраняемых в локальном журнале сообщений;

г) GlobalLoggerAdress – сетевой адрес регионального менеджера журналирования.

3) Параметры локальных настроек, указанные в секции LocalHost:

а) AccessAddress – IP-адрес, откуда допустимо обращение к КП СОБ по сокету. При пустой строке обращение допустимо отовсюду;

б) SocketPortNumber – номер порта прослушивающего сокета;

в) AdministratorKeyPhrase – защищённая ключевая фраза для авторизации администратора.

4) Параметры настроек КПА УЦ, указанные в секции CA:

а) RootPrivateKey – путь к личному ключу КПА УЦ;

б) FirebirdDB – настройки базы данных 'Firebird':

– ServerHost – хост, на котором запущена служба 'Firebird';

– DB_UserName – имя пользователя базы данных;

– DB_UserPassword – пароль к базе данных;

– DB_FilePath – путь к файлу базы данных.

Внимание! Данная секция настроек присутствует только в КП СОБ функционирующего в составе КПА УЦ и используется при таких специфических операциях как выпуск администраторских сертификатов.

5) Параметры настроек управления ключами, указанные в секции KeysManagment:

а) PrivateKeysStorage – путь к хранилищу личных ключей;

б) Параметры настроек локального хранилища сертификатов, указанные в секции CertificateStorage:

– MainDir – корневая папка локального хранилища сертификатов;

– CertificateOriginalsDir – путь, по которому сохраняются СОК в форматах '.cer' и '.xml';

– LoadingCertificatesDir – путь, по которому вручную подгружаются СОК;

– LoadingCRLsDir – путь, по которому вручную подгружаются СОС;

– CertificateStorageFile – имя файла локального хранилища СОК;

– StandardLTPsFile – имя файла со стандартными наборами долговременных параметров;

– HistoryQuiryPeriod – период запроса истории изменений состояний СОК.

в) Параметры настройки выработки ЭЦП, указанные в секции Signing:

– DefaultSignKey – путь к личному ключу ЭЦП по умолчанию.

г) Параметры настройки расшифрования, указанные в секции Decrypting:

– DefaultCrptKey – путь к личному ключу расшифрования по умолчанию.

д) Параметры настройки аутентификации, указанные в секции Authentication:

– DefaultAuthKey – путь к личному ключу аутентификации по умолчанию.

6) Параметры транспортных настроек, указанные в секции Transport:

а) Параметры настройки транспортных атрибутов КПА УЦ, указанные в секции CA:

– HTTP – в атрибуте URL указывается http-адрес КПА УЦ, где номер порта, должен соответствовать номеру порта, на котором работает http-сервер КПА УЦ; в атрибутах SendingTimeout и ReceivingTimeout – таймауты отправки и получения запросов соответственно;

– EMail – адрес электронной почты КПА УЦ и таймаут отправки.

б) Параметры настройки транспортных атрибутов КП РЦ, указанные в секции RA:

– EMail – адрес электронной почты КП РЦ и таймаут отправки.

в) Параметры настройки собственных транспортных атрибутов КП СОБ, указанные в секции Owned:

– EMail – адрес собственной электронной почты КП СОБ;

– SMTP_Server – в атрибуте Address указывается адрес почтового сервера, используемого для отправки почтовых сообщений; Port – порт, на котором работает сервер исходящей почты; SSL_port – порт SSL исходящей почты.

– POP_Server – в атрибуте Address указывается адрес почтового сервера входящей почты; в атрибуте Port – порт, на котором работает сервер входящей почты; SSL_port – порт SSL входящей почты.

– EMailProxy – параметры доступа к серверу почтового прокси-сервера; в атрибутах Type, Address, Port, Login и Password указываются тип, IP-адрес, порт, логин и пароль доступа к прокси-серверу соответственно;

– SSL_version – версия SSL;

– InquiryPeriod – период опроса собственного почтового ящика;

г) Folders – директории для сохранения запросов и ответов;

д) RequeryByHTTP – максимальное количество повторений HTTP-запроса и величина задержки между повторениями.

7) Настройки для формирования заявки на выпуск сертификата в секции CertificateIssueRequest используются для первоначального заполнения полей формы заявки на выпуск сертификата.

8. СООБЩЕНИЯ

КП СОБ в процессе выполнения осуществляет аудит своей работы и формирует журнал в файл с именем «CryptoServiceLocalLog.txt».

В журнале указывается информация о СОК (идентификатор ключа), дата и время выполнения операции и результаты ее выполнения. В файл также помещается источник сообщения и текстовое пояснение.

В файл «CryptoServiceLocalLog.txt» заносится следующая информация:

1) дата и время запуска программы;
2) принятые параметры (кроме ключей и паролей);
3) результаты проверки принятых параметров;
4) результаты обращения к базе сертификатов;
5) результаты проверки сертификата;
6) результаты проверки личных ключей на соответствие открытым ключам;
7) идентификатор ключа;
8) результаты выполнения функций программы;
9) результат работы программы;
10) результат взаимодействия с файловой подсистемой.

Информационные сообщения и сообщения об ошибках предваряются текущей датой и временем, а также следующими идентификаторами:

– INF – информационное сообщение;
– WRN – предупреждающее сообщение;
– ERR – сообщение об ошибке.

Пример информации из файла журнала приведен в приложении 4.

Перечень информационных сообщений и сообщений об ошибках генерируемых КП СОБ и помещаемых в журнал аудита приведен в приложении 5.

8.1. Перечень сообщений оператору

Для удобства работы оператора КП СОБ в процессе работы формирует ряд сообщений оператору. Все сообщения можно разделить по смысловой нагрузке на следующие группы:

– информационные сообщения;
– предупреждающие сообщения;
– сообщения об ошибках;
– критические сообщения.

8.1.1. Информационные сообщения

Информационные сообщения предназначены для обеспечения удобства работы пользователя, они несут информацию о завершении операции. Ответом на эти сообщения является нажатие клавиши «Ok» в диалоговом окне.

Ниже приведен перечень информационных сообщений:

"ASN1-заявка сохранена в файле *'имя файла'* «;

"OCSP-запрос сформирован и сохранён в файле *'имя файла'* «;

"SOAP-заявка сохранена в файле *'имя файла'* «;

"SOAP-заявка типа *'тип SOAP-заявки'* Id=*'идентификатор SOAP-заявки'* успешно отправлена в РЦ";

"В локальное хранилище не подгружено ни одного сертификата с жёсткого диска";

"В локальное хранилище подгружено *'количество подгруженных СОК'* сертификата с жёсткого диска";

"Выпущен сертификат администратора и помещён в базу данных УЦ";

"Не обработано ни одного OCSP-ответа с жёсткого диска";

"Не обработано ни одного COC'а с жёсткого диска";

"Обработано *'количество обработанных OCSP-ответов'* OCSP-ответа с жёсткого диска";

"Обработано *'количество обработанных СОС'* COC'а с жёсткого диска";

"Пользователь изменил пароль к своему личному ключу";

"Продолжим работу с пустым хранилищем сертификатов в памяти?";

"Успешно сформирована заявка на выпуск сертификата";

"Успешно сформирована заявка на отзыв сертификата как CMS";

"Успешно сформирована заявка на отзыв сертификата как PFX";

"Успешно сформирована заявка на приостановку сертификата";

"Успешно проверена целостность объектов";

"Успешно протестированы функции, содержащиеся в этих криптобиблиотеках».

8.1.2. Предупреждающие сообщения

Предупреждающие сообщения предназначены для обеспечения удобства работы пользователя, они несут информацию о причине, по которой операция не может быть завершена. Ответом на эти сообщения является нажатие клавиши «Ok» в диалоговом окне и выполнение необходимых действий.

Ниже приведен перечень предупреждающих сообщений:

"Введённый Вами серийный номер уже есть в запросе";

"Вы забыли ввести пароль…";

"Не найден сертификат с серийным номером *'серийный номер СОК'* «;

"Идентификатор открытого ключа должен содержать чётное количество шестнадцатеричных цифр";

"Количество введённых шестнадцатеричных цифр серийного номера - НЕ чётно";

"Минимальная длина пароля составляет *'количество символов пароля'* символов";

"Момент окончания приостановки сертификата НЕ ПОЗЖЕ момента начала его приостановки";

"Не введены ни серийный номер, ни идентификатор открытого ключа";

"Не закрыты диалоговые окна. Перед завершением работы их необходимо закрыть";

"Некорректное подтверждение пароля. Придётся повторить операцию";

"Серийный номер должен содержать чётное количество шестнадцатеричных цифр».

8.1.3. Сообщения об ошибках

Сообщения об ошибках предназначены для информирования пользователя о неудачном выполнении операции. Ответом на эти сообщения является нажатие клавиши «Ok» в диалоговом окне и повторное выполнение операции. В случае повторения сообщения об ошибке необходимо обратиться за помощью к администратору.

Ниже приведен перечень сообщения об ошибках:

"Ошибка выделения памяти для ASN1-заявки";

"Ошибка выделения памяти для XML-сертификата";

"Ошибка выделения памяти для серийного номера";

"Ошибка *'код ошибки'* при отправке SOAP-заявки типа *'тип SOAP-заявки'* Id=*'идентификатор SOAP-заявки'* в РЦ";

"Ошибка определения размера файла с ASN1-заявкой";

"Ошибка определения размера файла с личным ключом";

"Ошибка открытия файла с ASN1-заявкой";

"Ошибка открытия файла с личным ключом";

"Ошибка чтения файла с ASN1-заявкой";

"Ошибка чтения файла с личным ключом».

8.1.4. Критические сообщения

Критические сообщения выдаются при обнаружении критических событий (нарушение целостности ПО, ошибка самотестирования криптоалгоритмов). После чего ПО переходит в состояние блокировки. Выход из состояния блокировки осуществляется администратором путем переустановки ПО.

Ниже приведен перечень критических сообщений:

"Приложению не удалось запуститься, поскольку *'имя файла'* не был найден. Повторная установка приложения может исправить эту проблему";

"Ошибка при выполнении тестового набора *'название тестового набора' «*;

"Ошибка загрузки основной рабочей библиотеки";

"Нарушена целостность файла *'имя файла' «*;

"Ошибка открытия файла *'имя файла' «.*

ПРИЛОЖЕНИЕ 1

ПРИМЕРЫ SOAP-КОНВЕРТОВ

В настоящем приложении представлены примеры SOAP-конвертов заявки на выпуск, отзыв и приостановку; запроса на получение CRL; запроса на получение OCSP; запроса сертификатов; ответа на заявку на выпуск сертификата, запрос на получение OCSP и запрос на получение CRL; ответа на заявку на отзыв сертификата; ответа на заявку на приостановку сертификата; ответа на запрос сертификатов; ответа на заявку или запрос с ошибкой.

А. SOAP-конверт заявки на выпуск, отзыв и приостановку

Ниже представлен пример SOAP-конверта заявки на выпуск сертификата. В теге `<RequestInfo>` представлена информация о заявке, а именно: тип заявки (атрибут `Type` тега `<RequestInfo>`), уникальный идентификатор заявки (атрибут `Id` тега `<RequestInfo>`) и обратные адреса, на которые придет ответ на заявку (тег `<ReturnAddresses>`).

Тег `<SOAP-SEC:Signature>` содержит информацию о подписи и собственно подпись по спецификации формата XML.

В контенте тега `<RequestData>` содержится заявка в формате ASN1 и закодированная в base64. Структура заявки на выпуск сертификата описана в СТБ 34.101.17, а на отзыв и приостановку – в СТБ 34.101.18 и СТБ 34.101.23.

Заявки на отзыв и приостановку отличаются от заявок на выпуск только значением атрибута `Type` (отзыв – `RevokeCertificate`, приостановка – `SuspendCertificate`) и контентом тега `<RequestData>`.

```
<?xml version="1.0» encoding="UTF-8"?>
<e:Envelope xmlns:e="http://www.w3.org/2003/05/soap-envelope">
   <e:Header>
      <RequestInfo Type="IssueCertificate» Id="tqbVaVEcDm3ACV05">
         <ReturnAddresses>
            <Address> testing@contact </Address>
         </ReturnAddresses>
      </RequestInfo>
      <SOAP-SEC:Signature xmlns:SOAP-SEC="http://schemas.xmlsoap.org/soap/
       security/2000-12">
         <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
            <SignedInfo>
               <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/
```

```
            xml-exc-c14n#"/>
            <SignatureMethod Algorithm="1.2.112.0.2.0.34.101.45.12"/>
            <Reference URI="#SignedData">
               <DigestMethod Algorithm="1.2.112.0.2.0.34.101.31.81"/>
               <DigestValue>
                  DalevRd1Za5iw1fcuRmWa4lZtInEb9s+qU7vaW63yoQ=
               </DigestValue>
            </Reference>
         </SignedInfo>
         <SignatureValue>
            zrjKJ6re/66pHO8EZgJjL4iaKVufUoNvBDUrAsu35J67G3IAtwKWNld
            u0jhDbdfG
         </SignatureValue>
         <KeyInfo>
            <KeyName>
               EEBB47D4C10FDDFF2389E61D57B53A2E7FCBDFF06DC651AE4C0CED2B8
               2A94D6F
            </KeyName>
         </KeyInfo>
      </Signature>
   </SOAP-SEC:Signature>
</e:Header>
<e:Body>
   <RequestData Id="SignedData» SigningTime="2014-12-16T12:43:26Z">
      MIIEMDCCA+oCAQAwggIGMQ8wDQYDVQQRDAYyMjAyMjIxCzAJBgNVBAYMAkJZMSgwJgY
      DVQQIDB/QkdGA0LXRgdGC0LrQsNGPINC+0LHQu9Cw0YHRgtGMMSkwJwYKKwYBBAHefA
      ICBQwZ0J/QuNC90YHQutC40Lkg0YDQsNC50L7QvTEXMBUGA1UEBwwO0LMuINCc0LjQv
      dGB0LoxJjAkBgNVBAkMHdGD0LsuINCa0LjRgNC+0LLQsCDQtNC+0LwgMTAgMSowKAYD
      VQQKDCHQmtCw0YDRgtC+0L3QvdCw0Y8g0YTQsNCx0YDQuNC60LAxGDAWBgkrBgEEAeJ
      waAMMCTU1NTU1NTU1NTE5MDcGA1UEAwww0JrRgNC+0L/QvtGC0LrQuNC90LAg0J3QuN
      C90LAg0JzQsNC60LDRgNC+0LLQvdCwMR0wGwYDVQQEDBTQmtGA0L7Qv9C+0YLQutC40
      L3QsDERMA8GA1UEKgwI0J3QuNC90LAxJDAiBgNVBCkMG9Cd0LjQvdCwINCc0LDQutCw
      0YDQvtCy0L3QsDFWMFQGCisGAQQB3nwCAhEMRtCf0LDRgdC/0L7RgNGCIFNXMTIzNDU
      2NyDQstGL0LTQsNC9IDE2LjEyLjIwMTQg0J/QuNC90YHQutC40Lwg0KDQntCS0JQxHz
      AdBgkrBgEEAeJwBQMMEDEyMzQ1Njc4NjYzNDUzNDUwXTAYBgoqcAACACJlLQIBBgoqc
      AACACJlLQMBA0EABykbPp1Ezr+Gbv3ah43KDhznlGWI6z9beMjc1q19KXFsthyH3gvC
      pck+PtTtztxr8WkonYFW3UJiuDLRBkqiMaCCAXowJwYDVR0OBCDuu0fUwQ/d/yOJ5h1
      XtTouf8vf8G3GUa5MDO0rgqlNbzApBgNVHSMwIoAg7rtH1MEP3f8jieYdV7U6Ln/L3/
      BtxlGuTAztK4KpTW8wCgYDVR0PAwMHyAAwKQYDVR0QMCKADzIwMTQxMjE2MTI0MjIwW
      oEPMjAxNTExMTYxMjQyMjBaMCoGCCpwAQIBAQUFMB4XDTE0MTIxNjEyNDIyMFoXDTE1
      MTIxNjEyNDIyMFowEQYDVR0lMAoGCCqFAwYDAQIBMIGtBgorBgEEAd58AgICMYGeMCc
```

```
            GCysGAQQB3nwCAgIBDBjQlNC+0LLQtdGA0LXQvdC90L7RgdGC0YwwEwYLKwYBBAHefA
            ICAgIMBDM0NTYwHgYLKwYBBAHefAICAgMYDzIwMTQxMjE2MDAwMDAwWjAeBgsrBgEEA
            d58AgICBBgPMjAxNDEyMTYwMDAwMDBaMB4GCysGAQQB3nwCAgIFGA8yMDE0MTIxOTIz
            NTk1OVowDQYJKnAAAgAiZS0MBQADMQBfpkejB1GPjcD1q1uPjCbGKm59lo6RKe5nPgi
            wCr8KF4xYuDqk9qHpVIhh8ONnY0I=
         </RequestData>
      </e:Body>
   </e:Envelope>
```

Б. SOAP-конверт запроса на получение CRL

SOAP-конверт с запросом CRL не подписывается. В теге <OnTime> указывается дата, на которую запрашивается СОС.

```
<?xml version="1.0» encoding="utf-8"?>
<e:Envelope xmlns:e="http://www.w3.org/2003/05/soap-envelope">
   <e:Header>
      <RequestInfo Type="GetCRL» Id="AB1y0WzRv42Nz4G8V+UW">
         <ReturnAddresses>
            <Address> testing@contact </Address>
         </ReturnAddresses>
      </RequestInfo>
   </e:Header>
   <e:Body>
      <RequestData>
   <OnTime> 2010-11-14T20:00:00Z </OnTime>
      </RequestData>
   </e:Body>
</e:Envelope>
```

В. SOAP-конверт запроса на получение OCSP

В тег <RequestData> помещается запрос OCSP в формате ASN1, структура которого описана в СТБ 34.101.26, завернутый в base64.

```
<?xml version="1.0» encoding="utf-8"?>
<e:Envelope xmlns:e="http://www.w3.org/2003/05/soap-envelope">
   <e:Header>
      <RequestInfo Type="GetOCSP» Id="AB1y0WzRv42Nz4G8V+UW">
         <ReturnAddresses>
            <Address> testing@contact </Address>
         </ReturnAddresses>
      </RequestInfo>
```

```
   </e:Header>
   <e:Body>
      <RequestData>
         MIIBhzCCAYOgAwIBADCCAXowfDB6MA0GCSsGAQQB3nwBAgUABCDYsCPMcPlw6WayhNr
         H+n/vNS2kdloTlFL/z0TZDqzioQQgSWl3cJeI8uGEUyQWxcV1r0hMe1DGiqOwiBvu3h
         T1hqACJUY5QUUwMTAwMDA0QUMyNUVFMjZBQTY4Q0MxNkRGRjkwREMwMgAwfDB6MA0GC
         SsGAQQB3nwBAgUABCDYsCPMcPlw6WayhNrH+n/vNS2kdloTlFL/z0TZDqzioQQgSWl3
         cJeI8uGEUyQWxcV1r0hMe1DGiqOwiBvu3hT1hqACJTBFOTcwMDAwMDBGRDg4MUExRDM
         xQjZFRDM4NkRGRjkwREMwMgAwfDB6MA0GCSsGAQQB3nwBAgUABCDYsCPMcPlw6WayhN
         rH+n/vNS2kdloTlFL/z0TZDqzioQQgSWl3cJeI8uGEUyQWxcV1r0hMe1DGiqOwiBvu3
         hT1hqACJTA1REIwMDAwMDBDREVFMDhBNDA0QTA5OThENkRGRjkwREMwMgA=
      </RequestData>
   </e:Body>
</e:Envelope>
```

Г. SOAP-конверт запроса сертификатов

В SOAP-конверте запроса на сертификаты в теге <RequestData> указывается список запрашиваемых сертификатов. В атрибуте WithHistory тега <Certificate> можно указать, что данный сертификат вернется с историей (true) либо без истории (false), а в атрибуте CertificateChain указывается в каком виде необходимо вернуть сертификат: значение no – вернется один сертификат, значение withCRL – вернется цепочка сертификатов в формате p7b со списком отозванных сертификатов (СТБ 34.101.23), значение withOCSP – вернется цепочка сертификатов в формате p7b с OCSP (СТБ 34.101.23). Запрашивать сертификат можно по серийному номеру (тег <SN>) либо по идентификатору ключа (тег <KeyId>). Так же необходимо указать время в теге <OnTime>, на которое нужно узнать статус сертификата.

```
<?xml version="1.0» encoding="utf-8"?>
<e:Envelope xmlns:e="http://www.w3.org/2003/05/soap-envelope">
   <e:Header>
      <RequestInfo Type="GetCertificates» Id="AB1y0WzRv42Nz4G8V+UW">
         <ReturnAddresses>
            <Address> testing@contact </Address>
         </ReturnAddresses>
      </RequestInfo>
   </e:Header>
   <e:Body>
      <RequestData>
         <Certificate WithHistory="false» CertificateChain="withCRL">
```

```
            <SN> 111111111111117DE800000000000001 </SN>
            <OnTime> 2009-10-01T02:00:00Z </OnTime>
         </Certificate>
         <Certificate WithHistory="true» CertificateChain="no">
            <KeyId>
               EBAC4D1779B7F50F0FDCBCE1060148C5EB1F2DA1E6655D18103BC35001F96718
            </KeyId>
            <OnTime> 2009-10-01T02:00:00Z </OnTime>
         </Certificate>
      </RequestData>
   </e:Body>
</e:Envelope>
```

Д. SOAP-конверт ответа на заявку на выпуск сертификата, запрос на получение OCSP и запрос на получение CRL

В SOAP-конверте ответа на выпуск в теге <ReplyData> находится свежевыпущенный СОК, структура которого описана в СТБ 34.101.19, закодированный в base64. В атрибутах тега <ReplyInfo> указана основная информация об ответе: тип заявки и уникальный идентификатор. В ответе на запрос OCSP или CRL в тег <ReplyData> помещается ответ OCSP или выпущенный СОС, структуры которых описаны в СТБ 34.101.26 и СТБ 34.101.19 соответственно, закодированные в base64.

```
<?xml version="1.0» encoding="UTF-8"?>
<e:Envelope xmlns:e="http://www.w3.org/2003/05/soap-envelope">
   <e:Header>
      <ReplyInfo Id="tqbVaVEcDm3ACV05» Type="IssueCertificate"/>
      <SOAP-SEC:Signature xmlns:SOAP-SEC="http://schemas.xmlsoap.org/soap/
       security/2000-12">
         <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
            <SignedInfo>
               <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/
                xml-exc-c14n#"/>
               <SignatureMethod Algorithm="1.2.112.0.2.0.1176.2.11"/>
               <Reference URI="#SignedData"/>
            </SignedInfo>
            <SignatureValue>

      AQIAAPfV+Eb3eHyd35xbvjxZRwrasR/LJwZCMcFn7iY8xzp/xJy8Bv9MfsCXQb
               Ztg4vKKlBLYhzI6ftDndypyXBq+j4BAAAA
            </SignatureValue>
```

```
            <KeyInfo>
               <KeyName>
                  B323918789ACE6C4EFD1C34B8CA6374ED116F90A81E3EB3B81C11F9
                  1C1235B94
   </KeyName>
            </KeyInfo>
         </Signature>
      </SOAP-SEC:Signature>
   </e:Header>
   <e:Body>
      <ReplyData Id="SignedData» PerformedAt="2014-12-16T12:48:08Z»
       SigningTime="2014-12-16T12:48:08Z">
         MIIFCzCCBLSgAwIBAgISEREVERERERF97AAAAAAAAAAMMA0GCSsGAQQB3nwBAgUAMIG
         aMVMwUQYDVQQDHkoEIwQ0BD4EQQRCBD4EMgQ1BEAETwROBEkEOAQ5ACAEJgQ1BD0EQg
         RAACAENAQ7BE8AIARCBDUEQQRCBDgEQAQ+BDIEMAQ9BDgETzEfMB0GA1UECh4WBB0EI
         gQmACAEGgQ+BD0EQgQwBDoEQjETMBEGA1UEBx4KBBwEOAQ9BEEEOjENMAsGA1UEBh4E
         AEIAWTAeFw0xNDEyMTYxMjQ4MDdaFw0xNTEyMTYxMjQyMjBaMIICBjEPMA0GA1UEEQw
         GMjIwMjIyMQswCQYDVQQGDAJCWTEoMCYGA1UECAwf0JHRgNC10YHRgtC60LDRjyDQvt
         Cx0LvQsNGB0YLRjDEpMCcGCisGAQQB3nwCAgUMGdCf0LjQvdGB0LrQuNC5INGA0LDQu
         dC+0L0xFzAVBgNVBAcMDtCzLiDQnNC40L3RgdC6MSYwJAYDVQQJDB3Rg9C7LiDQmtC4
         0YDQvtCy0LAg0LTQvtC8IDEwIDEqMCgGA1UECgwh0JrQsNGA0YLQvtC90L3QsNGPING
         E0LDQsdGA0LjQutCwMRgwFgYJKwYBBAHicGgDDAk1NTU1NTU1NTUxOTA3BgNVBAMMMN
         Ca0YDQvtC/0L7RgtC60LjQvdCwINCd0LjQvdCwINCc0LDQutCw0YDQvtCy0L3QsDEdM
         BsGA1UEBAwU0JrRgNC+0L/QvtGC0LrQuNC90LAxETAPBgNVBCoMCNCd0LjQvdCwMSQw
         IgYDVQQpDBvQndC40L3QsCDQnNCw0LrQsNGA0L7QstC90LAxVjBUBgorBgEEAd58AgI
         RDEbQn9Cw0YHQv9C+0YDRgiBTVzEyMzQ1Njcg0LLRi9C00LDQvSAxNi4xMi4yMDE0IN
         Cf0LjQvdGB0LrQuNC8INCg0J7QktCUMR8wHQYJKwYBBAHicAUDDBAxMjM0NTY3ODY2M
         zQ1MzQ1MF0wGAYKKnAAAgAiZS0CAQYKKnAAAgAiZS0DAQNBAAcpGz6dRM6/hm792oeN
         yg4c55RliOs/W3jI3NatfSlxbLYch94LwqXJPj7U7c7ca/FpKJ2BVt1CYrgy0QZKojG
         jggFiMIIBXjApBgNVHQ4EIgQg7rtH1MEP3f8jieYdV7U6Ln/L3/BtxlGuTAztK4KpTW
         8wKwYDVR0jBCQwIoAgsyORh4ms5sTv0cNLjKY3TtEW+QqB4+s7gcEfkcEjW5QwDwYDV
         R0PAQH/BAUDAwfIADArBgNVHRAEJDAigA8yMDE0MTIxNjEyNDIyMFqBDzIwMTUxMTE2
         MTI0MjIwWjATBgNVHSUEDDAKBggqhQMGAwECATCBsAYKKwYBBAHefAICAgSBoTGBnjA
         nBgsrBgEEAd58AgICAQwY0JTQvtCy0LXRgNC10L3QvdC+0YHRgtGMMBMGCysGAQQB3n
         wCAgICDAQzNDU2MB4GCysGAQQB3nwCAgIDGA8yMDE0MTIxNjAwMDAwMFowHgYLKwYBB
         AHefAICAgQYDzIwMTQxMjE2MDAwMDAwWjAeBgsrBgEEAd58AgICBRgPMjAxNDEyMTky
         MzU5NTlaMA0GCSsGAQQB3nwBAgUAA0IAAYCtPJ2eTsv9la+a4PKoUZJJmlQn0i7No09
         V7v3wCquBL7nuBHjpH1I2TZ5AmKj2SnabHyR4gSKl3q31MjHV4HU=
      </ReplyData>
   </e:Body>
</e:Envelope>
```

Е. SOAP-конверт ответа на заявку на отзыв сертификата

В теге <ReplyData> в ответе на отзыв СОК указывается серийный номер (<SN>) или идентификатор ключа (<KeyId>) отозванного сертификата и время отзыва (<RevokeTime>).

```
<?xml version="1.0» encoding="UTF-8"?>
<e:Envelope xmlns:e="http://www.w3.org/2003/05/soap-envelope">
   <e:Header>
      <ReplyInfo Id="tqbVaVEcDm3ACV06» Type="RevokeCertificate"/>
      <SOAP-SEC:Signature xmlns:SOAP-SEC="http://schemas.xmlsoap.org/soap/
       security/2000-12">
         <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
            <SignedInfo>
               <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/
                xml-exc-c14n#"/>
               <SignatureMethod Algorithm="1.2.112.0.2.0.1176.2.11"/>
               <Reference URI="#SignedData"/>
            </SignedInfo>
            <SignatureValue>
               QIAAPfV+Eb3eHyd35xbvjxZRwrasR/LJwZCMcFn7iY8xzp/xJy8Bv9MfsCXQb
               Ztg4vKKlBLYhzI6ftDndypyXBq+j4BAAAA
            </SignatureValue>
            <KeyInfo>
               <KeyName>
                  B323918789ACE6C4EFD1C34B8CA6374ED116F90A81E3EB3B81C11F9
                  1C1235B94
   </KeyName>
            </KeyInfo>
         </Signature>
      </SOAP-SEC:Signature>
   </e:Header>
   <e:Body>
      <ReplyData Id="SignedData» PerformedAt="2014-12-16T12:48:08Z»
       SigningTime="2014-12-16T12:48:08Z">
         <SN> 11111511111111117DEC0000000000000011 </SN>
         <RevokeTime> 2014-12-16T17:55:20Z </RevokeTime>
      </ReplyData>
   </e:Body>
</e:Envelope>
```

Ж. SOAP-конверт ответа на заявку на приостановку сертификата

В теге <ReplyData> в ответе на приостановку СОК указывается серийный номер (<SN>) или идентификатор ключа (<KeyId>) приостановленного сертификата, время начала приостановки (<SuspendStartTime>) и опционально время окончания приостановки (<SuspendEndTime>).

```
<?xml version="1.0» encoding="UTF-8"?>
<e:Envelope xmlns:e="http://www.w3.org/2003/05/soap-envelope">
   <e:Header>
      <ReplyInfo Id="tqbVaVEcDm3ACV07» Type="SuspendCertificate"/>
      <SOAP-SEC:Signature xmlns:SOAP-SEC="http://schemas.xmlsoap.org/soap/
       security/2000-12">
         <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
            <SignedInfo>
               <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/
                xml-exc-c14n#"/>
               <SignatureMethod Algorithm="1.2.112.0.2.0.1176.2.11"/>
               <Reference URI="#SignedData"/>
            </SignedInfo>
            <SignatureValue>
               QIAAPfV+Eb3eHyd35xbvjxZRwrasR/LJwZCMcFn7iY8xzp/xJy8Bv9MfsCXQb
               Ztg4vKKlBLYhzI6ftDndypyXBq+j4BAAAA
            </SignatureValue>
            <KeyInfo>
               <KeyName>
                  B323918789ACE6C4EFD1C34B8CA6374ED116F90A81E3EB3B81C11F9
                  1C1235B94
               </KeyName>
            </KeyInfo>
         </Signature>
      </SOAP-SEC:Signature>
   </e:Header>
   <e:Body>
      <ReplyData Id="SignedData» PerformedAt="2014-12-16T12:48:08Z»
       SigningTime="2014-12-16T12:48:08Z">
         <KeyId>
            ECB5C351DA70E2A4D503E0C32D32F080B374FD548F52BD70B06C2EF01346150B
         </KeyId>
         <SuspendStartTime> 2014-12-22T14:14:08Z </SuspendStartTime>
         <SuspendEndTime> 2015-12-22T14:10:36Z </SuspendEndTime>
```

```
      </ReplyData>
   </e:Body>
</e:Envelope>
```

И. SOAP-конверт ответа на запрос сертификатов

В ответе на запрос сертификатов по каждому запрошенному сертификату может вернуться следующая информация:

- буфер сертификата или цепочки сертификатов (тег <Buffer>),
- статус сертификата,
- время, на которое запрашивался статус,
- использование ключа,
- если сертификат запрашивался с историей, то в информации о сертификате в теге <History> будут отображаться все события истории, связанные с данным сертификатом.

Если сертификат не был найден в хранилище или произошла ошибка во время получения конкретного сертификата, то вернется сообщение об ошибке с текстовым пояснением (тег <ErrorReport>).

```
<?xml version="1.0» encoding="UTF-8"?>
<e:Envelope xmlns:e="http://www.w3.org/2003/05/soap-envelope">
   <e:Header>
      <ReplyInfo Id="tqbVaVEcDm3ACV10» Type="GetCertificates"/>
      <SOAP-SEC:Signature xmlns:SOAP-SEC="http://schemas.xmlsoap.org/soap/
       security/2000-12">
         <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
            <SignedInfo>
               <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/
                xml-exc-c14n#"/>
               <SignatureMethod Algorithm="1.2.112.0.2.0.1176.2.11"/>
               <Reference URI="#SignedData"/>
            </SignedInfo>
            <SignatureValue>
               QIAAPfV+Eb3eHyd35xbvjxZRwrasR/LJwZCMcFn7iY8xzp/xJy8Bv9MfsCXQb
               Ztg4vKKlBLYhzI6ftDndypyXBq+j4BAAAA
            </SignatureValue>
            <KeyInfo>
               <KeyName>
                  B323918789ACE6C4EFD1C34B8CA6374ED116F90A81E3EB3B81C11F9
                  1C1235B94
```

```
            </KeyName>
         </KeyInfo>
      </Signature>
   </SOAP-SEC:Signature>
</e:Header>
<e:Body>
   <ReplyData Id="SignedData» PerformedAt="2014-12-17T14:24:52Z">
      <Certificate>
         <SN> 111111111111117DEC00000000000001 </SN>
         <ErrorReport ReturnCode="-203">
            <Message> Сертификат не найден </Message>
            <Details> Ошибка при получении сертификата и информации о нём
                   из базы данных. Ошибка при получении статуса
                   сертификата на дату: Сертификат не найден.</Details>
         </ErrorReport>
      </Certificate>
      <Certificate>
         <Buffer>
            MIIGGzCCBc2gAwIBAgISAtyQ/21sjbFuN8c+fAAAAMCNMA0GCSsGAQQB3nwBA
            gUAMIHEMVUwUwYDVQQDHkwEIwQ0BD4EQQRCBD4EMgQ1BEAETwROBEkEOAQ5AC
            AEJgQ1BD0EQgRAACAEEAQhBBEAIAAiBBEENQQ7BDAEQARDBEEEMQQwBD0EOgA
            iMRMwEQYDVQQHHgoEHAQ4BD0EQQQ6MSswKQYDVQQKHiIEEAQhBBEAIAAiBBEE
            NQQ7BDAEQARDBEEEMQQwBD0EOgAiMQ0wCwYDVQQGHgQAQgBZMRowGAYJKoZIh
            vcNAQkBFgtjZW50cmVAYmFuazAiGA8yMDA5MDYwODEyMjQyNFoYDzIwMTQwNj
            A4MTIyMTM1WjCCAV8xPTA7BgNVBAMeNAQiBDUEQQRCACAENwQwBDIENQRABDg
            EQgQ1BDsETAQ9BDAETwAgBD8EPgQ0BD8EOARBBEwxGzAZBgNVBAceEgQQBDEE
            QAQwBDwEPgQyBDoEMDEZMBcGA1UECh4QBDIENQRABD4EMgQwBD4EQDETMBEGA
            1UECx4KBDIEPgQ/BDIEPjETMBEGA1UEDB4KBDIEPgQyBDAEPjENMAsGA1UEBh
            4EAEIAWTEYMBYGCisGAQQB3nwCAgEeCAA4ADAAMAAwMYGSMIGPBgorBgEEAd5
            8AgIeHoGAAEQANQBGADEANwBFAEYAQgA0ADIARABBADAARQAyAEMAQwA4ADQA
            RgBGAEUAQwAwADkAQQAzAEMAQgBEAEIANwBEADIAMgA3AEIARQBCAEEAMQA0A
            DYANQAxADcAMABBADEAMAA4ADAARAAwADQANAA1ADgANAAyADYAMgBGAEIwgg
            HhMIIBWQYJKwYBBAHefAECoIIBSjCCAUaAAgP+gQIAr4KBgD+4wdETEDbOXX4
            atNLTkBWtIATsufMkBNVyOEfFa32c7JAHGFuOvXN/pWBtNC2U5WcQDi6EyTxF
            ZgGKKWWqT26VcMLM/aT43KU/Sdt3IXV8ZdSArMm3ER1T6SctRzE7vkkdEFRjL
            3U0wrTGopqP5shMtPtNENCuVPsis599RJF5gxZqsQz9MiQhY6O5gvAtX+dpbY
            rqmngBhIGADMxQjL8kM8jWnTyAU8w1iCE2X3M87lrqd1d5iQ42DOqmphNLDq0
            zjQLt2kNGt50ZCgdzXj5+bABDYG2EsYVUNmi8Tz+SVI246lNBx+ipoWOPaCqK
            M2rnBpwtr/fbR/HIajAjGehSQedSQJKc+EcUO/+PeAKxzG36NorTYvxtpPaFH
            gP9AAAD/bc5nHdXrrmtAMHrwi13zuGA6ABwVnAnHwOBgQAqRMhGrnVFtnp2sp
            I4/gxYy9GY+Xd3k8uHivJiijwiu5oDIH0F1enkaABGtVF0Vi4Xt9aJvx+7K5T
```

FzFQDAZ/vPVoMJw2cOof4+yIHLdshfsi0SVMXXnsEyf6BAkAM36qaF9KGhgXJ
Af/2xCrWAJqiK6w4MfDSY/7Ps9obH6E4HaOCAW4wggFqMCsGA1UdAQQkMCKAI
GI0eKhAVHNPwsDuYDso2bfAVRpiHSF/5AJNa3aTZUOmMCkGA1UdDgQiBCCLLI
D6PrI1SUpe7Mvi9MjgAKIYSvTK6HWRZ5IrdLptHzAPBgNVHRMBAf8EBTADAgE
AMC4GA1UdEAEB/wQkMCKADzIwMDkwNjA4MTIyNDI0WoEPMjAxMzA2MDgxMjIx
MzVaMA8GA1UdDwEB/wQFAwMHgAAwgb0GA1UdIAEB/wSBsjCBrzCBrAYSKwYBB
AGB4i4HgUmBSQAAAAAAMIGVMIGSBggrBgEFBQcCAjCBhR6BggAiBBIEPQRDBE
IEQAQ1BD0EPQQ4BDkAIAQ0BD4EOgRDBDwENQQ9BEIEPgQ+BDEEPgRABD4EQgA
iACAALQAgBDcEMAQyBDUEQAQ4BEIENQQ7BEwEPQQwBE8AIAQ/BD4ENAQ/BDgE
QQRMACAAKAQaBDAEPQRGBDUEOwRPBEAEOARPACkwDQYJKwYBBAHefAECBQADO
QAlSnpEziNYBdrXc16OydPg6XoPctwBZUGPhtNgMVeS1irkqG8dhIQb1NDgM3
f1ipbWeju2e6DYBQ==

```
   </Buffer>
   <Status> 1 </Status>
   <StatusOnDate> 2011-11-24T17:23:39Z</StatusOnDate>
   <KeyUsage> 0 </KeyUsage>
</Certificate>
<Certificate>
   <Buffer>
```

MIIGGzCCBc2gAwIBAgISAtyQ/21sjbFuN8c+fAAAAMCNMA0GCSsGAQQB3nwBA
gUAMIHEMVUwUwYDVQQDHkwEIwQ0BD4EQQRCBD4EMgQ1BEAETwROBEkEOAQ5AC
AEJgQ1BD0EQgRAACAEEAQhBBEAIAAiBBEENQQ7BDAEQARDBEEEMQQwBD0EOgA
iMRMwEQYDVQQHHgoEHAQ4BD0EQQQ6MSswKQYDVQQKHiIEEAQhBBEAIAAiBBEE
NQQ7BDAEQARDBEEEMQQwBD0EOgAiMQ0wCwYDVQQGHgQAQgBZMRowGAYJKoZIh
vcNAQkBFgtjZW50cmVAYmFuazAiGA8yMDA5MDYwODEyMjQyNFoYDzIwMTQwNj
A4MTIyMTM1WjCCAV8xPTA7BgNVBAMeNAQiBDUEQQRCACAENwQwBDIENQRABDg
EQgQ1BDsETAQ9BDAETwAgBD8EPgQ0BD8EOARBBEwxGzAZBgNVBAceEgQQBDEE
QAQwBDwEPgQyBDoEMDEZMBcGA1UECh4QBDIENQRABD4EMgQwBD4EQDETMBEGA
1UECx4KBDIEPgQ/BDIEPjETMBEGA1UEDB4KBDIEPgQyBDAEPjENMAsGA1UEBh
4EAEIAWTEYMBYGCisGAQQB3nwCAgEeCAA4ADAAMAAwMYGSMIGPBgorBgEEAd5
8AgIeHoGAAEQANQBGADEANwBFAEYAQgA0ADIARABBADAARQAyAEMAQwA4ADQA
RgBGAEUAQwAwADkAQQAzAEMAQgBEAEIANwBEADIAMgA3AEIARQBCAEEAMQA0A
DYANQAxADcAMABBADEAMAA4ADAARAAwADQANAA1ADgANAAyADYAMgBGAEIwgg
HhMIIBWQYJKwYBBAHefAECoIIBSjCCAUaAAgP+gQIAr4KBgD+4wdETEDbOXX4
atNLTkBWtIATsufMkBNVyOEfFa32c7JAHGFuOvXN/pWBtNC2U5WcQDi6EyTxF
ZgGKKWWqT26VcMLM/aT43KU/Sdt3IXV8ZdSArMm3ER1T6SctRzE7vkkdEFRjL
3U0wrTGopqP5shMtPtNENCuVPsis599RJF5gxZqsQz9MiQhY6O5gvAtX+dpbY
rqmngBhIGADMxQjL8kM8jWnTyAU8w1iCE2X3M87lrqd1d5iQ42DOqmphNLDq0
zjQLt2kNGt50ZCgdzXj5+bABDYG2EsYVUNmi8Tz+SVI246lNBx+ipoWOPaCqK
M2rnBpwtr/fbR/HIajAjGehSQedSQJKc+EcUO/+PeAKxzG36NorTYvxtpPaFH
gP9AAAD/bc5nHdXrrmtAMHrwi13zuGA6ABwVnAnHwOBgQAqRMhGrnVFtnp2sp

```
                I4/gxYy9GY+Xd3k8uHivJiijwiu5oDIH0F1enkaABGtVF0Vi4Xt9aJvx+7K5T
                FzFQDAZ/vPVoMJw2cOof4+yIHLdshfsi0SVMXXnsEyf6BAkAM36qaF9KGhgXJ
                Af/2xCrWAJqiK6w4MfDSY/7Ps9obH6E4HaOCAW4wggFqMCsGA1UdAQQkMCKAI
                GI0eKhAVHNPwsDuYDso2bfAVRpiHSF/5AJNa3aTZUOmMCkGA1UdDgQiBCCLLI
                D6PrI1SUpe7Mvi9MjgAKIYSvTK6HWRZ5IrdLptHzAPBgNVHRMBAf8EBTADAgE
                AMC4GA1UdEAEB/wQkMCKADzIwMDkwNjA4MTIyNDI0WoEPMjAxMzA2MDgxMjIx
                MzVaMA8GA1UdDwEB/wQFAwMHgAAwgb0GA1UdIAEB/wSBsjCBrzCBrAYSKwYBB
                AGB4i4HgUmBSQAAAAAAMIGVMIGSBggrBgEFBQcCAjCBhR6BggAiBBIEPQRDBE
                IEQAQ1BD0EPQQ4BDkAIAQ0BD4EOgRDBDwENQQ9BEIEPgQ+BDEEPgRABD4EQgA
                iACAALQAgBDcEMAQyBDUEQAQ4BEIENQQ7BEwEPQQwBE8AIAQ/BD4ENAQ/BDgE
                QQRMACAAKAQaBDAEPQRGBDUEOwRPBEAEOARPACkwDQYJKwYBBAHefAECBQADO
                QAlSnpEziNYBdrXc16OydPg6XoPctwBZUGPhtNgMVeS1irkqG8dhIQb1NDgM3
                f1ipbWeju2e6DYBQ==
            </Buffer>
            <Status> -2</Status>
            <StatusOnDate> 2011-11-24T17:23:39Z</StatusOnDate>
            <KeyUsage> 0 </KeyUsage>
            <History>
               <Event Time="2008-10-27T00:00:00Z» Status="3"/>
               <Event Time="2008-11-27T00:00:00Z» Status="0"/>
            </History>
         </Certificate>
      </ReplyData>
   </e:Body>
</e:Envelope>
```

К. SOAP-конверт ответа на заявку или запрос с ошибкой

В ошибочном ответе в атрибуте `Type` тега <ReplyInfo> указан тип заявки или запроса, ответ на которую содержится в SOAP-конверте, а тег <ErrorReport> содержит информацию об ошибке: атрибут `ReturnCode` – код ошибки, тег <Message> – текстовое пояснение ошибки, тег <Details> – детали ошибки.

```
<?xml version="1.0» encoding="UTF-8"?>
<e:Envelope xmlns:e="http://www.w3.org/2003/05/soap-envelope">
   <e:Header>
      <ReplyInfo Id="tqbVaVEcDm3ACV10» Type="SuspendCertificate"/>
      <SOAP-SEC:Signature xmlns:SOAP-SEC="http://schemas.xmlsoap.org/soap/
       security/2000-12">
         <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
            <SignedInfo>
               <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/
```

```
                xml-exc-c14n#"/>
                <SignatureMethod Algorithm="1.2.112.0.2.0.1176.2.11"/>
                <Reference URI="#SignedData"/>
            </SignedInfo>
            <SignatureValue>
               QIAAPfV+Eb3eHyd35xbvjxZRwrasR/LJwZCMcFn7iY8xzp/xJy8Bv9MfsCXQb
               Ztg4vKKlBLYhzI6ftDndypyXBq+j4BAAAA
            </SignatureValue>
            <KeyInfo>
               <KeyName>
                  B323918789ACE6C4EFD1C34B8CA6374ED116F90A81E3EB3B81C11F9
                  1C1235B94
               </KeyName>
            </KeyInfo>
         </Signature>
      </SOAP-SEC:Signature>
   </e:Header>
   <e:Body>
      <ErrorReport Id="SignedData» ReturnCode="-205"
       SigningTime="2014-12-16T13:10:16Z">
        <Message> Ошибка хранилища сертификатов </Message>
        <Details>
          Ошибка при приостановке сертификата: Требуемые даты приостановки
          выходят за границы периода действия ключа
        </Details>
      </ErrorReport>
   </e:Body>
</e:Envelope>
```

ПРИЛОЖЕНИЕ 2

СТРУКТУРА ФАЙЛА НАСТРОЙКИ

Ниже приведен пример файла настройки CryptoServiceSettings.xml.

```
<?xml version="1.0» encoding="windows-1251"?>
<CryptoServiceSettings InfrastructureName="BUTB">
  <BasicSettings Unicity="Yes» DebugLogging="Yes">
    <FrameworkName Description="Путь к главной рабочей библиотеке">
      .\BUTB_Framework.dll
    </FrameworkName>
    <SystrayMenu Description="Список пунктов всплывающего меню
    приложения">
      <SystrayMenuItem Id="33001» Name="Выпустить заявку на
      сертификат» Separator="No"/>
      <SystrayMenuItem Id="33011» Name="Сформировать заявку на
      приостановку сертификата» Separator="No"/>
      <SystrayMenuItem Id="33012» Name="Сформировать заявку на отзыв
      сертификата как CMS» Separator="Yes"/>
      <SystrayMenuItem Id="33002» Name="Локальное хранилище»
      Separator="No"/>
      <SystrayMenuItem Id="33003» Name="Загрузить сертификаты из
      файлов» Separator="Yes"/>
      <SystrayMenuItem Id="33004» Name="Сменить пароль к личному
      ключу» Separator="Yes"/>
      <SystrayMenuItem Id="33020» Name="Запросить статус сертификата
      по OCSP» Separator="No"/>
      <SystrayMenuItem Id="33021» Name="Запросить сертификат по
      HTTP» Separator="Yes"/>
      <SystrayMenuItem Id="33069» Name="Провести тестирование
      криптобиблиотек» Separator="Yes"/>
    </SystrayMenu>
  </BasicSettings>
  <Logging Description="Настройки журналирования">
    <LocalLogName Description="Имя файла локального журнала">
      .\CryptoServiceLocalLog.txt
    </LocalLogName>
    <MaxLocalLogSize Description="Максимальный размер циклического
    файла локального журнала">
      0x10000
    </MaxLocalLogSize>
    <MessageLevelsMask Description="Фильтр уровня сохраняемых в
    локальном журнале сообщений">
      0xffffffff
    </MessageLevelsMask>
    <GlobalLoggerAdress Description="Сетевой адрес регионального
    менеджера журналирования">
      200.0.0.57:10200
    </GlobalLoggerAdress>
```

```
</Logging>
<LocalHost Description="Локальные настройки">
  <AccessAddress Description="IP-адрес, откуда допустимо обращение
  к CryptoService'у по сокету (при пустой строке обращение
  допустимо отовсюду)"/>
  <SocketPortNumber Description="Номер порта прослушивающего сокета">
    49018
  </SocketPortNumber>
  <AdministratorKeyPhrase Description="Защищённая ключевая фраза
  для авторизации администратора">
    YXkfMUZz5QGkxycY6LWeZk366lvOX8c6yxV9CKnOGsMtpk2F
  </AdministratorKeyPhrase>
</LocalHost>
<KeysManagment Description="Настройки управления ключами">
  <PrivateKeysStorage Description="Путь к хранилищу личных ключей">
    .\PrivateKeys\
  </PrivateKeysStorage>
  <CertificateStorage Description="Настройки локального хранилища
  сертификатов">
    <MainDir Description="Корневая папка локального хранилища
    сертификатов">
      CertificateStorage
    </MainDir>
    <CertificateOriginalsDir Description="Папка с сертификатами в
    форматах '.cer' и '.xml'">
      CertificateOriginals
    </CertificateOriginalsDir>
    <LoadingCertificatesDir Description="Папка с подгружаемыми
    вручную сертификатами">
      ForCertificatesLoading
    </LoadingCertificatesDir>
    <LoadingCRLsDir Description="Папка с подгружаемыми вручную
    списками отозванных сертификатов">
      ForCRLsLoading
    </LoadingCRLsDir>
    <CertificateStorageFile Description="Имя файла локального
    хранилища сертификатов">
      CertificateStorage.v10
    </CertificateStorageFile>
    <StandardLTPsFile Description="Имя файла со стандартными
    наборами долговременных параметров">
      StdLTPs.ber
    </StandardLTPsFile>
    <HistoryQuiryPeriod Value="2 min» Description="Период запроса
    истории изменений состояний сертификатов"/>
  </CertificateStorage>
  <Signing Description="Настройки выработки ЭЦП">
    <DefaultSignKey Description="Путь к личному ключу ЭЦП по умолчанию»
   Path=«.\PrivateKeys\sign_key_Тэстовый_ИВЦ_МФ1_123_05_11_10_17_12_43.sck"/>
  </Signing>
  <Decrypting Description="Настройки расшифрования">
```

```
    <DefaultCrptKey Description="Путь к личному ключу
    расшифрования по умолчанию» Path=«.\PrivateKeys\
   crpt_key_Тэстовый_ИВЦ_МФ1_123_05_11_10_17_12_43.sck"/>
  </Decrypting>
  <Authentication Description="Настройки аутентификации">
    <DefaultAuthKey Description="Путь к личному ключу
    аутентификации по умолчанию» Path=«.\PrivateKeys\
    crpt_key_Тэстовый_ИВЦ_МФ1_123_05_11_10_17_12_43.sck"/>
  </Authentication>
</KeysManagment>
<Transport Description="Транспортные настройки">
  <HTTP-Request Repeat="2» Delay="5 msec"/>
  <CA Description="Транспортные атрибуты УЦ">
    <HTTP URL="http://200.0.0.197:4080» SendingTimeout="60 sec»
    ReceivingTimeout="300 sec">
      <Proxy Type="0» Address="« Port="8080» Login="« Password=""/>
    </HTTP>
    <EMail Address="ca_requests@contact» SendingTimeout="60 sec"/>
  </CA>
  <RA Description="Транспортные атрибуты РЦ">
    <HTTP URL="http://127.0.0.1:4090» SendingTimeout="60 sec»
    ReceivingTimeout="300 sec">
      <Proxy Type="0» Address="« Port="8080» Login="« Password=""/>
    </HTTP>
    <EMail Address="ra_requests@contact» SendingTimeout="60 sec"/>
  </RA>
  <Owned Description="Собственные транспортные настройки">
    <EMail Address="ra_cs1@contact» Login="ra_cs1» Password="1»
    SendingTimeout="60 sec"/>
    <SMTP_Server Address="200.0.0.197» Port="25» SSL_port="465"/>
    <POP_Server Address="200.0.0.197» Port="110» SSL_port="995"/>
    <EMailProxy Type="0» Address="« Port="8080» Login="« Password=""/>
    <SSL_version ForSending="0» ForReceiving="0">
      <!--  0 - не использовать SSL;  2 - SSL версии 2;
      3 - SSL версии 3;  4 - SSL версии 2,3;  5 - TLS версии 1 -->
    </SSL_version>
    <InquiryPeriod Value="1 sec» Description="Период опроса
    собственного почтового ящика"/>
  </Owned>
  <Folders ForRequests="Requests» ForResponses="Responses"/>
  <RequeryByHTTP Amount="3» Delay="50 msec»
  Description="Максимальное количество повторений HTTP-запроса и
  величина задержки между повторениями"/>
</Transport>
<CertificateIssueRequest Description="Настройки для формирования
заявки на выпуск сертификата">
  <PersonalPage Description="Вкладка с персональными данными">
    <LegalStatus OId="1.2.643.6.3.1.2» Section="Extentions»
    Description="Юридический статус">
      <LegalStatusForm OId="1.2.643.6.3.1.2.2»
      Default="Физическое лицо / Private person"/>
```

```
  </LegalStatus>
  <Location Description="Юридический адрес или место регистрации">
    <PostalCode Description="Почтовый индекс» Default="220000»
    Section="Subject» OId="2.5.4.17"/>
    <Country Description="Страна» Default="Беларусь / Belarus»
    Section="Subject» OId="2.5.4.6"/>
    <Province Description="Область» Default="« Section="Subject»
    OId="2.5.4.8"/>
    <District Description="Район» Default="« Section="Subject»
    OId="1.3.6.1.4.1.12156.2.2.5"/>
    <Locality Description="Населённый пункт» Default="г. Минск»
    Section="Subject» OId="2.5.4.7"/>
    <StreetAddress Description="Локальный адрес» OId="2.5.4.9">
      <Street Description="Улица» Default="ул. Свердлова"/>
      <House Description="Дом» Default="15"/>
      <Building Description="Корпус» Default="А"/>
      <Apartment Description="Квартира/офис» Default="78"/>
    </StreetAddress>
  </Location>
  <Organization Description="Полное наименование организации -
  владельца ключа» Default='ИП «Маргарита"' Section="Subject»
  OId="2.5.4.10"/>
  <PersonalData Description="Данные о представителе">
    <IdentityCard Description="Документ, удостоверяющий
    личность» Section="Subject» OId="1.3.6.1.4.1.12156.2.2.17">
      <Name Description="Наименование документа»
      Default="Паспорт"/>
      <Number Description="Серия и номер документа»
      Default="SW1234567"/>
      <IssueDate Description="Дата выдачи документа»
      Default="30.06.2013"/>
      <IssuedBy Description="Кем выдан документ»
      Default="Браславским РОВД"/>
    </IdentityCard>
    <PersonalNumber Description="Идентификационный номер»
    Default="987654321WZ4444» Section="Extentions»
    OId="1.2.112.1.2.1.1.1.1.1"/>
    <MobilePhoneNumber Description="Номер мобильного телефона»
    Default="+375298880808"/>
    <CommonName Description="Фамилия, имя, отчество» OId="2.5.4.3">
      <Surname Description="Фамилия» Default="Гераськo»
      Section="Subject» OId="2.5.4.4"/>
      <FirstName Description="Имя» Default="Егор»
      Section="Subject» OId="2.5.4.42"/>
      <SecondName Description="Отчество» Default="Витальевич»
      Section="Subject» OId="2.5.4.41"/>
    </CommonName>
  </PersonalData>
  <Position Default="инженер» OId="2.5.4.12» Section="Subject»
  Description="Должность"/>
</PersonalPage>
```

```
<KeypairPage Description="Вкладка с параметрами личного и
открытого ключей">
  <SignAlgorithm Description="Алгоритм ЭЦП» Default="СТБ
  34.101.45» Section="CryptoParams"/>
  <!-- SignAlgorithm: «СТБ 1176.2» «СТБ 34.101.31 + СТБ 1176.2»
  «СТБ 34.101.45» -->
  <CryptoLevel Description="Уровень криптостойкости»
  Default="128» Section="CryptoParams"/>
  <!-- Для  СТБ 34.101.45 выбор из { 128, 192, 256 };
  в противном случае выбор из {  3, 6, 10 } -->
  <CommonKeys Description="Генерировать ли ключ ПФОК»
  Default="Yes» Section="CryptoParams"/>
  <CertificateDuration Description="Длительность действия
  сертификата в МЕСЯЦАХ» Default="12"/>
  <PrivateKeyDuration Description="Длительность действия личного
  ключа в МЕСЯЦАХ» Default="11"/>
</KeypairPage>
<PrivilegesPage Description="Вкладка с параметрами полномочного
документа">
  <ProcurationDocument Section="Extentions»
  OId="1.3.6.1.4.1.12156.2.2.2">
    <ProcurationDocumentName Description="Наименование
    полномочного документа» Default="« OId="1.3.6.1.4.1.12156.2.2.2.1"/>
    <ProcurationDocumentNumber Description="Номер полномочного
    документа» Default="« OId="1.3.6.1.4.1.12156.2.2.2.2"/>
    <ProcurationDocumentDate Description="Дата выдачи
    полномочного документа» Default="« OId="1.3.6.1.4.1.12156.2.2.2.3"/>
  </ProcurationDocument>
  <ProcurationDocumentDuration Description="Длительность
  действия полномочного документа в ДНЯХ» Default="3"/>
  <PartnersPermissions Section="Extentions» OId="1.2.643.6">
    <BTB-Center Default="Yes» OId="1.2.643.6.7»
    Description="Использование в работе систем электронного
    докуметооборота и электронных торговых систем B2B-CENTER"/>
  </PartnersPermissions>
  <TradePermissions Section="Extentions»
  OId="1.3.6.1.4.1.40346.1">
    <VisitorPermission Default="Yes» OId="1.3.6.1.4.1.40346.1.1»
    Description="Посетитель торгов"/>
    <BrockerPermission Default="No» OId="1.3.6.1.4.1.40346.1.2»
    Description="Биржевой брокер"/>
  </TradePermissions>
  <TradeSectionAccess Section="Extentions»
  OId="1.3.6.1.4.1.40346.2">
    <SectionMetall Default="Yes» OId="1.3.6.1.4.1.40346.2.1»
    Description="Право участия в секции металлопродукции"/>
    <SectionTimber Default="Yes» OId="1.3.6.1.4.1.40346.2.2»
    Description="Право участия в секции лесопродукции"/>
    <SectionAgri Default="Yes» OId="1.3.6.1.4.1.40346.2.3»
    Description="Право участия в секции сельхозпродукции"/>
    <SectionPPT Default="Yes» OId="1.3.6.1.4.1.40346.2.4»
```

```
        Description="Право участия в секции ПиПТ"/>
      </TradeSectionAccess>
    </PrivilegesPage>
    <CertificateValidity Duration="1 year» InsertToIssueRequest="Yes"/>
  </CertificateIssueRequest>
</CryptoServiceSettings>
```

ПРИЛОЖЕНИЕ 3

СТРУКТУРА XML-ШАБЛОНА ДЛЯ ВЫПУСКА СЕРТИФИКАТА ОТКРЫТОГО КЛЮЧА ДЛЯ АДМИНИСТРАТОРА

Ниже приведен пример файла XML-шаблона IssueAdminCertificate_RA.xml.

```
<?xml version="1.0» encoding="UTF-8"?>
<IssueAdminCertificate>
  <Subject>
    <CommonName OId="2.5.4.3» Value="Васильев Михаил Арамович"/>
    <Country OId="2.5.4.6» Value="BY"/>
    <Province OId="2.5.4.8» Value="Гродненская область"/>
    <District OId="1.3.6.1.4.1.12156.2.2.5» Value="Волковыский
    район"/>
    <Locality OId="2.5.4.7» Value="г. Волковыск"/>
    <StreetAddress OId="2.5.4.9» Value="ул.Мира, д.5"/>
    <IdentityCard OId="1.3.6.1.4.1.12156.2.2.17» Value="Паспорт
    SW1234568 выдан 12.03.2011 Борисовским РОВД"/>
    <PersonalNumber OId="1.2.112.1.2.1.1.1.1.1»
    Value="432101234AZ108"/>
    <Organization OId="2.5.4.10» Value="ЗАО 'НТЦ Контакт'"/>
    <Title OId="2.5.4.12» Value="Администратор Регистрационного
     центра №2"/>
  </Subject>
  <PublicKeyAlgorithm OId="1.2.112.0.2.0.34.101.45.2.1» CryptoLevel="128"/>
  <KeyUsageFlags KeyEncipherment="True» DataEncipherment="True»
  KeyAgreement="True» KeyCertSign="False» CRLSign="False»
  EncipherOnly="False» DecipherOnly="False» OCSPsigning="False» />
  <CertificateDuration Unit="месяц» Value="60"/>
  <PrivateKeyDuration  Unit="месяц» Value="59"/>
</IssueAdminCertificate>
```

ПРИЛОЖЕНИЕ 4

ПРИМЕР СООБЩЕНИЙ ИЗ ФАЙЛА ЖУРНАЛА

2016-01-25 13:40:30.046 INF |S:StartFramework |M:Стартовал CryptoService

2016-01-25 13:40:30.062 INF |S:StartFramework |M:Создан прослушивающий сеть сокет

2016-01-25 13:40:30.109 INF |S:CryptoCore.SelfTesting |M:Успешно проверена целостность криптобиблиотеки 'CryptoCont.dll'.

2016-01-25 13:40:30.328 INF |S:CryptoCore.SelfTesting |M:Успешно проверена целостность криптобиблиотеки 'ContactCrypto32LE.dll'.

2016-01-25 13:40:33.890 INF |S:CryptoCore.SelfTesting |M:Успешно протестированы функции, содержащиеся в криптобиблиотеках.

2016-01-25 13:40:33.890 INF |S:StartFramework |M:Инициализировано криптоядро.

2016-01-25 13:40:33.906 INF |S:StartFramework |M:Построено дерево объектных идентификаторов.

2016-01-25 13:40:33.921 INF |S:StartFramework |M:Запущен поток периодических запросов истории изменений состояний сертификатов.

2016-01-25 13:40:33.921 INF |S:StartFramework |M:Загружено локальное хранилище сертификатов.

2016-01-25 13:40:33.937 INF |S:StartFramework |M:Запущен поток опроса почтового ящика CryptoService'a.

2016-01-25 13:40:33.937 INF |S:StartFramework |M:Инициализирован транспортный менеджер.

2016-01-25 13:40:33.937 INF |S:StartFramework |M:Запущен поток, прослушивающий сокеты.

2016-01-25 13:40:34.968 INF |S:EMailInquiring |M:Опрошен почтовый ящик CryptoService'a. Глобальный фильтр = 'ContactCMS', локальный фильтр = '8C89A501FF0B'

2016-01-25 13:40:34.968 INF |S:EMailInquiring |M:Результат опроса почтового ящика CryptoService'a = 0. Количество новых писем = 0.

2016-01-25 13:41:18.125 INF |S:HandleCommand |M:Выбран пункт меню № 33001 = 'Выпустить заявку на сертификат / Issue a request for a certificate'

2016-01-25 13:41:49.921 INF |S:Transporter.SendRequestByEMail |M:SOAP-заявка типа 'IssueCertificate' Id='2zw1dNaBF7AP8Td1' успешно отправлена в РЦ.

2016-01-25 13:41:51.687 INF |S:CertificateStorage.ProcessIssueCertificateResponseSOAP |M:Получено извещение с идентификатором '2zw1dNaBF7AP8Td1' на заявку на выпуск сертификата с кодом возврата = 100 и текстом: Заявка помещена в карантин и ожидает проверки администратором информационной безопасности РЦ версии 2. Значения одного или нескольких полей не соответствуют имеющимся в справочниках. Информация о заявке: 2zw1dNaBF7AP8Td1, Демидов Егор Витальевич

ПРИЛОЖЕНИЕ 5

ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ СООБЩЕНИЙ И СООБЩЕНИЙ ОБ ОШИБКАХ

ASN1-заявка сохранена в файле *'имя файла'*.

OCSP-запрос не подписан.

OCSP-запрос сформирован и сохранён в файле *'имя файла'*.

OCSP-ответ из файла *'имя файла'* не корректен.

OCSP-сервер перегружен. Повторите запрос позже.

SOAP-заявка сохранена в файле *'имя файла'*.

SOAP-заявка типа *'тип SOAP-заявки'* Id=*'идентификатор SOAP-заявки'* успешно отправлена в РЦ.

SOAP-конверт выходит за границы входного пакета.

SOAP-конверт имеет слишком маленький размер.

SOAP-ответ НЕ подписан.

SOAP-ответ с идентификатором *'идентификатор SOAP-ответа'* на заявку на выпуск сертификата содержит пустое тело.

TBS-секция выходит за границы входного пакета.

TBS-секция имеет слишком маленький размер.

TBS-секция ответа на OCSP-запрос пуста.

TBS-секция COC пуста.

Адрес SOAP-ответа равен НУЛЮ.

Буфер с данными для хэширования выходит за границы входного пакета.

В ASN1-заявке задан неизвестный объектный идентификатор алгоритма ЭЦП.

В ASN1-заявке задан неизвестный объектный идентификатор набора долговременных параметров.

В ASN1-заявке задан неизвестный объектный идентификатор открытого ключа.

В ASN1-заявке задан некорректный объектный идентификатор алгоритма хэширования подписанных данных CMS.

В ASN1-заявке задан некорректный объектный идентификатор алгоритма хэширования включённых данных CMS.

В ASN1-заявке задан некорректный объектный идентификатор алгоритма хэширования подписанных данных CMS = *'объектный идентификатор'*.

В ASN1-заявке задан некорректный объектный идентификатор алгоритма хэширования

включённых данных CMS = *'объектный идентификатор'*.

В ASN1-заявке задан некорректный объектный идентификатор в атрибуте типа включённых данных CMS.

В ASN1-заявке задан некорректный объектный идентификатор неструктурированных включённых данных CMS.

В ASN1-заявке задан некорректный объектный идентификатор подписанных данных CMS.

В ASN1-заявке задан объектный идентификатор неизвестного алгоритма ЭЦП.

В ASN1-заявке задана некорректная версия контейнера подписанта CMS.

В ASN1-заявке задана некорректная версия *'номер версии'*.

В ASN1-заявке задана некорректная версия подписанных данных CMS.

В ASN1-заявке задана некорректная версия формате PFX.

В ASN1-заявке значение атрибута хэша включённых данных CMS не равно вычисленному.

В ASN1-заявке нарушена структура атрибута - идентификатора открытого ключа заявителя.

В ASN1-заявке нарушена структура атрибута - идентификатора открытого ключа подписанта заявки.

В ASN1-заявке нарушена структура атрибута - контейнера расширений сертификата Microsoft.

В ASN1-заявке нарушена структура атрибута.

В ASN1-заявке отсутствует версия контейнера подписанта CMS.

В ASN1-заявке отсутствует версия подписанных данных CMS.

В ASN1-заявке отсутствует версия.

В ASN1-заявке отсутствует значение S пары Эль-Гамаля.

В ASN1-заявке отсутствует значение W пары Эль-Гамаля.

В ASN1-заявке отсутствует значение атрибута времени подписания включённых данных CMS.

В ASN1-заявке отсутствует значение атрибута типа включённых данных CMS.

В ASN1-заявке отсутствует значение атрибута хэша включённых данных CMS.

В ASN1-заявке отсутствует значение пары Эль-Гамаля.

В ASN1-заявке отсутствует значение подписи включённых данных CMS.

В ASN1-заявке отсутствует значение ЭЦП.

В ASN1-заявке отсутствует идентификатор открытого ключа подписанта CMS.

В ASN1-заявке отсутствует контейнер алгоритма подписи включённых данных CMS.

В ASN1-заявке отсутствует контейнер алгоритма хэширования подписанных данных CMS.

В ASN1-заявке отсутствует контейнер включённых данных CMS.

В ASN1-заявке отсутствует контейнер двойного набора долговременных параметров.

В ASN1-заявке отсутствует контейнер набора долговременных параметров СТБ 1176.2.

В ASN1-заявке отсутствует контейнер объектного идентификатора алгоритма хэширования включённых данных CMS.

В ASN1-заявке отсутствует контейнер открытого ключа.

В ASN1-заявке отсутствует контейнер пары открытых ключей.

В ASN1-заявке отсутствует контейнер подписанных атрибутов CMS.

В ASN1-заявке отсутствует контейнер подписанных данных CMS.

В ASN1-заявке отсутствует контейнер подписанных данных формата PFX.

В ASN1-заявке отсутствует контейнер подписанта CMS.

В ASN1-заявке отсутствует контейнер подписантов CMS.

В ASN1-заявке отсутствует набор алгоритмов хэширования подписанных данных CMS.

В ASN1-заявке отсутствует набор долговременных параметров.

В ASN1-заявке отсутствует объектный идентификатор алгоритма подписи включённых данных CMS.

В ASN1-заявке отсутствует объектный идентификатор алгоритма хэширования подписанных данных CMS.

В ASN1-заявке отсутствует объектный идентификатор алгоритма хэширования включённых данных CMS.

В ASN1-заявке отсутствует объектный идентификатор алгоритма ЭЦП.

В ASN1-заявке отсутствует объектный идентификатор включённых данных CMS.

В ASN1-заявке отсутствует объектный идентификатор двойного набора долговременных параметров.

В ASN1-заявке отсутствует объектный идентификатор долговременных параметров эллиптической кривой.

В ASN1-заявке отсутствует объектный идентификатор набора долговременных параметров СТБ 1176.2.

В ASN1-заявке отсутствует объектный идентификатор открытого ключа.

В ASN1-заявке отсутствует объектный идентификатор подписанного атрибута CMS.

В ASN1-заявке отсутствует объектный идентификатор подписанных данных CMS.

В ASN1-заявке отсутствует объектный идентификатор типа включённых данных CMS.

В ASN1-заявке отсутствует обязательный подписываемый атрибут времени подписания включённых данных CMS.

В ASN1-заявке отсутствует обязательный подписываемый атрибут типа включённых данных CMS.

В ASN1-заявке отсутствует обязательный подписываемый атрибут хэш-значения от включённых данных CMS.

В ASN1-заявке отсутствует открытый ключ ПФОК.

В ASN1-заявке отсутствует открытый ключ ЭЦП.

В ASN1-заявке отсутствует секция 'SubjectName'.

В ASN1-заявке отсутствует секция 'SubjectPublicKeyInfo'.

В ASN1-заявке отсутствует секция 'TBS'.

В ASN1-заявке отсутствует секция алгоритма ЭЦП.

В ASN1-заявке отсутствует секция атрибутов.

В ASN1-заявке отсутствует секция долговременных параметров.

В ASN1-заявке отсутствует секция ЭЦП.

В ASN1-заявке содержится некорректный тег подписанного атрибута CMS.

В SOAP-конверте отсутствует заголовок.

В SOAP-конверте отсутствует тело.

В SOAP-конверте шаблона заявки отсутствует заголовок 'e:Header'.

В SOAP-конверте шаблона заявки отсутствует тело 'e:Body'.

В SOAP-ответе задан некорректный серийный номер сертификата.

В SOAP-ответе задано некорректное время выполнения запроса.

В SOAP-ответе задано некорректное время изменения состояния сертификата.

В SOAP-ответе на заявку на выпуск сертификата с идентификатором *'идентификатор открытого ключа'* отсутствует сертификат в кодировке Base64.

В SOAP-ответе на заявку на выпуск сертификата с идентификатором *'идентификатор открытого ключа'* содержится некорректная кодировка Base64 сертификата.

В SOAP-ответе некорректно задано время выполнения запроса.

В SOAP-ответе некорректно задано время изменения состояния сертификата.

В SOAP-ответе некорректно задано новое состояние сертификата.

В SOAP-ответе отсутствует время его подписания.

В SOAP-ответе отсутствует его идентификатор.

В SOAP-ответе отсутствует его тип.

В SOAP-ответе отсутствует заголовок.

В SOAP-ответе отсутствует значение ЭЦП.

В SOAP-ответе отсутствует идентификатор ключа подписанта.

В SOAP-ответе отсутствует идентификатор открытого ключа подписанта.

В SOAP-ответе отсутствует контейнер сертификатов.

В SOAP-ответе отсутствует секция подписанта.

В SOAP-ответе отсутствует серийный номер сертификата.

В SOAP-ответе отсутствует сертификат в кодировке Base64.

В SOAP-ответе отсутствует событие изменения статуса сертификата.

В SOAP-ответе отсутствует тело.

В SOAP-ответе содержится некорректная Base64-кодировка сертификата.

В SOAP-ответе содержится некорректная Base64-кодировка ЭЦП.

В SOAP-ответе содержится некорректное время его подписания.

В SOAP-ответе содержится некорректное значение идентификатора открытого ключа подписанта.

В SOAP-ответе содержится ЭЦП некорректной длины.

В XML-шаблоне задан некорректный OId атрибута владельца.

В XML-шаблоне задан некорректный OId открытого ключа.

В XML-шаблоне задано некорректное значение атрибута владельца.

В XML-шаблоне не задан OId открытого ключа.

В XML-шаблоне не задан уровень криптостойкости ключевой пары.

В XML-шаблоне не задана единица измерения срока действия сертификата.

В XML-шаблоне отсутствует секция 'Subject'.

В XML-шаблоне отсутствует срок действия сертификата.

В заголовке SOAP-конверта отсутствует информационный элемент.

В заголовке SOAP-конверта отсутствует тип запроса/ответа.

В заголовке SOAP-конверта содержится некорректный тип запроса/ответа.

В заголовке SOAP-конверта шаблона заявки отсутствует значение ЭЦП.

В заголовке SOAP-конверта шаблона заявки отсутствует идентификатор ключа подписанта SOAP-конверта.

В заголовке SOAP-конверта шаблона заявки отсутствует секция подписи 'Signature'.

В заголовке SOAP-конверта шаблона заявки отсутствует трейлер подписи 'SOAP-SEC:Signature'.

В заголовке SOAP-конверта шаблона заявки содержатся некорректное значение ЭЦП в кодировке 'Base64'.

В заголовке SOAP-конверта шаблона заявки содержится некорректная длина идентификатора ключа подписанта SOAP-конверта.

В значении компоненты 'IssuerDomainPolicy' отображения политики сертификата содержится недопустимая политика 'AnyPolicy'.

В корневом сертификате УЦ отсутствует расширение идентификатора ключа издателя сертификата.

В локальное хранилище не подгружено ни одного сертификата с жёсткого диска.

В локальное хранилище подгружен сертификат, содержащийся в SOAP-ответе на заявку с идентификатором *'идентификатор заявки'*.

В локальное хранилище подгружено *'количество подгруженных СОК'* сертификата с жёсткого диска.

В локальном хранилище сертификатов на диске отсутствуют долговременные параметры и сертификаты.

В настройках CryptoService'a не задан период опроса собственного почтового ящика.

В настройках CryptoService'a некорректен адрес прокси-сервера.

В настройках CryptoService'a некорректен логин прокси-сервера.

В настройках CryptoService'a некорректен пароль прокси-сервера.

В настройках CryptoService'a отсутствует IP-адрес и порт УЦ.

В настройках CryptoService'a отсутствует Proxy-адрес для УЦ.

В настройках CryptoService'a отсутствует Proxy-логин для УЦ.

В настройках CryptoService'a отсутствует Proxy-пароль для УЦ.

В настройках CryptoService'a отсутствует Proxy-порт для УЦ.

В настройках CryptoService'a отсутствует Proxy-тип для УЦ.

В настройках CryptoService'a отсутствует адрес POP3-сервера.

В настройках CryptoService'a отсутствует адрес SMTP-сервера.

В настройках CryptoService'a отсутствует адрес локального почтового ящика.

В настройках CryptoService'a отсутствует адрес почтового ящика РЦ.

В настройках CryptoService'a отсутствует адрес почтового ящика УЦ.

В настройках CryptoService'a отсутствует величина задержки в МИЛЛИСЕКУНДАХ между повторными HTTP-запросами.

В настройках CryptoService'a отсутствует версия SSL.

В настройках CryptoService'a отсутствует имя корневой папки локального хранилища сертификатов.

В настройках CryptoService'a отсутствует имя папки с подгружаемыми вручную сертификатами.

В настройках CryptoService'a отсутствует имя папки с подгружаемыми вручную списками отозванных сертификатов.

В настройках CryptoService'a отсутствует имя папки с сертификатами в форматах '.cer' и '.xml'.

В настройках CryptoService'a отсутствует имя пользователя базы данных.

В настройках CryptoService'a отсутствует имя файла локального хранилища сертификатов.

В настройках CryptoService'a отсутствует либо некорректен SSL-порт SMTP-сервера.

В настройках CryptoService'a отсутствует либо некорректен SSL-порт POP3-сервера.

В настройках CryptoService'a отсутствует либо некорректен порт POP3-сервера.

В настройках CryptoService'a отсутствует либо некорректен порт SMTP-сервера.

В настройках CryptoService'a отсутствует либо некорректен порт прокси-сервера.

В настройках CryptoService'a отсутствует логин локального почтового ящика.

В настройках CryptoService'a отсутствует максимальное количество повторений HTTP-запросов.

В настройках CryptoService'a отсутствует пароль к базе данных.

В настройках CryptoService'a отсутствует пароль локального почтового ящика.

В настройках CryptoService'a отсутствует путь к личному ключу УЦ.

В настройках CryptoService'a отсутствует секция локального хранилища сертификатов 'CertificateStorage'.

В настройках CryptoService'a отсутствует секция управления ключами 'KeysManagment'.

В настройках CryptoService'a отсутствует секция УЦ.

В настройках CryptoService'a отсутствует таймаут HTTP-передачи на УЦ.

В настройках CryptoService'a отсутствует таймаут HTTP-приёма от УЦ.

В настройках CryptoService'a отсутствует таймаут отправки с локального почтового ящика.

В настройках CryptoService'a отсутствует тип прокси-сервера.

В настройках CryptoService'a отсутствует хост, на котором запущена служба 'Firebird'.

В настройках CryptoService'a отсутствуют HTTP-атрибуты УЦ.

В настройках CryptoService'a отсутствуют Proxy-атрибуты УЦ.

В настройках CryptoService'a отсутствуют атрибуты POP3-сервера.

В настройках CryptoService'a отсутствуют атрибуты SMTP-сервера.

В настройках CryptoService'a отсутствуют атрибуты прокси-сервера.

В настройках CryptoService'a отсутствуют локальные почтовые атрибуты.

В настройках CryptoService'a отсутствуют локальные транспортные настройки.

В настройках CryptoService'a отсутствуют настройки базы данных 'Firebird'.

В настройках CryptoService'a отсутствуют парметры запросов по HTTP.

В настройках CryptoService'a отсутствуют почтовые атрибуты РЦ.

В настройках CryptoService'a отсутствуют почтовые атрибуты УЦ.

В настройках CryptoService'a отсутствуют транспортные атрибуты РЦ.

В настройках CryptoService'a отсутствуют транспортные атрибуты УЦ.

В настройках CryptoService'a отсутствуют транспортные настройки.

В настройках CryptoService'a отсутствуют элементы 'PrivateKeysStorage', содержащие пути к хранилищам личных ключей.

В настройках локального хранилища сертификатов отсутствует имя файла со стандартными наборами долговременных параметров.

В подписанном SOAP-конверте отсутствует значение ЭЦП.

В подписанном SOAP-конверте отсутствует идентификатор открытого ключа подписанта.

В подписанном SOAP-конверте отсутствует секция подписанта.

В подписанном SOAP-конверте содержится некорректная Base64-кодировка ЭЦП.

В подписанном SOAP-конверте содержится некорректное значение идентификатора ключа подписанта.

В подписанном SOAP-конверте содержится некорректное значение идентификатора открытого ключа подписанта.

В подписанном SOAP-конверте содержится ЭЦП некорректной длины.

В подписанном SOAP-ответе отсутствует значение ЭЦП.

В подписанном SOAP-ответе отсутствует идентификатор открытого ключа подписанта.

В подписанном SOAP-ответе отсутствует секция подписанта.

В подписанном SOAP-ответе содержится некорректная Base64-кодировка ЭЦП.

В подписанном SOAP-ответе содержится ЭЦП некорректной длины.

В позиции *'номер позиции'* упакованной ASN1-заявки содержится недопустимый символ Base64.

В расширении *'объектный идентификатор'* корневого сертификата УЦ отсутствует значение.

В расширениях OCSP-ответа отсутствует идентификатор ключа подписанта.

В расширениях COC отсутствует идентификатор ключа подписанта.

В секции расширений сертификата содержатся расширения с одинаковыми объектными идентификаторами.

В сертификате не заданы ни серийный номер издателя, ни идентификатор открытого ключа издателя.

В сертификате отсутствует версия.

В сертификате отсутствует открытый ключ.

В сертификате отсутствует секция TBS.

В сертификате отсутствует секция владельца.

В сертификате отсутствует секция идентификатора алгоритма ЭЦП.

В сертификате отсутствует секция издателя.

В сертификате отсутствует секция открытого ключа.

В сертификате отсутствует секция периода действия сертификата.

В сертификате отсутствует серийный номер.

В сертификате с серийным номером *'серийный номер СОК'* в расширении PolicyMappings в issuerDomainPolicy указано значение AnyPolicy.

В сертификате с серийным номером *'серийный номер СОК'* в расширении PolicyMappings в subjectDomainPolicy указано значение AnyPolicy.

В сертификате с серийным номером *'серийный номер СОК'* в расширении BasicConstraints отсутствует компонент cA.

В сертификате с серийным номером *'серийный номер СОК'* в расширении KeyUsage не установлен бит KeyCertSign.

В сертификате с серийным номером *'серийный номер СОК'* отсутствует расширение BasicConstraints.

В сертификате *'серийный номер СОК'* в расширении SubjectAltName *'тип' 'значение'* не принадлежит дереву PERMITTED_SUBTREES.

В сертификате *'серийный номер СОК'* в расширении SubjectAltName *'тип' 'значение'* принадлежит дереву EXCLUDED_SUBTREES.

В сертификате *'серийный номер СОК'* не возможна проверка имен с типом *'тип'* в расширении Subject, т.к. данное подмножество в дереве разрешенных имен PERMITTED_SUBTREES является пустым.

В сертификате *'серийный номер СОК'* не возможна проверка имен с типом *'тип'* в расширении SubjectAltName, т.к. данное расширение в дереве разрешенных имен PERMITTED_SUBTREES является пустым.

В сертификате *'серийный номер СОК'* ошибка содержимого элемента *'значение'* при проверке запрещенных имен в секции Subject.

В сертификате *'серийный номер СОК'* при проверке допустимых имен в расширении Subject имя *'значение'* с типом *'тип'* не принадлежит дереву PERMITTED_SUBTREES.

В сертификате *'серийный номер СОК'* при проверке допустимых имен в расширении SubjectAltName имя *'значение'* с типом *'тип'* не принадлежит дереву PERMITTED_SUBTREES.

В сертификате *'серийный номер СОК'* при проверке запрещенных имен в расширении SubjectAltName имя *'значение'* с типом *'тип'* принадлежит дереву EXCLUDED_SUBTREES.

В сертификате *'серийный номер СОК'* присутствует имя *'значение'* с типом *'тип'*, а в дереве

разрешенных имен PERMITTED_SUBTREES множество для данного типа является пустым.

В теле SOAP-конверта отсутствует упакованная ASN1-заявка.

В теле SOAP-конверта отсутствует элемент 'RequestData'.

В теле SOAP-конверта содержится упакованная ASN1-заявка слишком маленького размера.

В теле SOAP-конверта шаблона заявки отсутствует собственно шаблон 'Subscriber'.

В трейлере ЭЦП содержится некорректный размер оригинального файла.

В хранилищах личных ключей, заданных в настройках CryptoService'a, не найдено ни одного ключа.

В хранилищах личных ключей, заданных в настройках CryptoService'a, не найдено личного ключа с идентификатором *'идентификатор открытого ключа'*.

В хранилищах личных ключей, заданных в настройках CryptoService'a, не найдено личного ключа с идентификатором *'идентификатор открытого ключа'*.

В шаблоне заявки 'Subscriber' отсутствует время его подписания.

В шаблоне заявки 'Subscriber' отсутствует юридический статус.

В шаблоне заявки 'Subscriber' содержится некорректное время его подписания.

В шаблоне заявки 'Subscriber' содержится некорректный юридический статус.

Введён неверный пароль.

Введённый Вами серийный номер уже есть в запросе.

Верификация маршрута сертификации завершена с отрицательным результатом.

Верификация маршрута сертификации начата.

Верификация маршрута сертификации не произведена, т.к. подгружен только один сертификат.

Верификация маршрута сертификации успешно завершена.

Версия сертификата с серийным номером *'серийный номер СОК'* не равна 3.

Во входном XML-запросе задан некорректный тип криптооперации.

Во входном XML-запросе на конвертование XML-заявки в SOAP задан некорректный пароль к личному ключу подписанта.

Во входном XML-запросе на конвертование XML-заявки в SOAP отсутствует идентификатор сертификата.

Во входном XML-запросе на конвертование XML-заявки в SOAP отсутствует пароль к личному ключу.

Во входном XML-запросе на конвертование XML-заявки в SOAP отсутствует время подписания.

Во входном XML-запросе на конвертование XML-заявки в SOAP отсутствуют данные для

подписания.

Во входном XML-запросе на конвертование XML-заявки в SOAP содержатся некорректные данные для подписания в кодировке 'Base64'.

Во входном XML-запросе на конвертование XML-заявки в SOAP содержится некорректная длина идентификатора сертификата.

Во входном XML-запросе на конвертование XML-заявки в SOAP содержится некорректное время подписания.

Во входном XML-запросе на подписание данных задан некорректный пароль к личному ключу подписанта.

Во входном XML-запросе на подписание данных отсутствует время подписания.

Во входном XML-запросе на подписание данных отсутствует идентификатор сертификата.

Во входном XML-запросе на подписание данных отсутствует пароль к личному ключу.

Во входном XML-запросе на подписание данных отсутствует формат представления сертификата.

Во входном XML-запросе на подписание данных отсутствуют данные для подписания.

Во входном XML-запросе на подписание данных содержатся некорректные данные для подписания в кодировке 'Base64'.

Во входном XML-запросе на подписание данных содержится некорректное значение идентификатора сертификата.

Во входном XML-запросе на подписание данных содержится некорректная длина идентификатора сертификата.

Во входном XML-запросе на подписание данных содержится некорректное время подписания.

Во входном XML-запросе на подписание данных содержится некорректный формат представления сертификата.

Во входном XML-запросе на проверку ЭЦП под данными отсутствует значение ЭЦП.

Во входном XML-запросе на проверку ЭЦП под данными отсутствует формат представления сертификата.

Во входном XML-запросе на проверку ЭЦП под данными отсутствуют данные для проверки ЭЦП.

Во входном XML-запросе на проверку ЭЦП под данными содержатся некорректные данные для проверки ЭЦП в кодировке 'Base64'.

Во входном XML-запросе на проверку ЭЦП под данными содержится некорректное значение ЭЦП в кодировке 'Base64'.

Во входном XML-запросе на проверку ЭЦП под данными содержится некорректный формат представления сертификата.

Во входном XML-запросе на проверку ЭЦП содержится идентификатор ключа подписанта некорректной длины.

Во входном XML-запросе на проверку ЭЦП содержится подпись некорректной битовой длины.

Во входном XML-запросе на формирование заявки на выпуск сертификата по шаблону отсутствует SOAP-конверт шаблона.

Во входном XML-запросе на формирование заявки на выпуск сертификата по шаблону содержатся некорректный SOAP-конверт шаблона в кодировке 'Base64'.

Во входном XML-запросе отсутствует маска использования ключа.

Во входном XML-запросе отсутствует тип криптооперации.

Во входном XML-запросе отсутствует флаг валидности ключа.

Во входном XML-запросе отсутствует формат представления сертификата.

Во входном XML-запросе содержится некорректная маска использования ключа.

Во входном XML-запросе содержится некорректный флаг валидности ключа.

Во входном XML-запросе содержится некорректный формат представления сертификата.

Во входном пакете задан неизвестный объектный идентификатор алгоритма хэширования *'объектный идентификатор'*.

Во входном пакете задан неизвестный объектный идентификатор алгоритма хэширования.

Во входном пакете задано некорректное значение начального вектора хэширования.

Входной пакет имеет недостаточный размер.

Входной пакет содержит недопустимые флаги типа данных о личном ключе.

Входной пакет содержит недопустимые флаги.

Выбран пункт меню № *'идентификатор пункта меню'*.

Выпущен сертификат администратора и помещён в базу данных УЦ.

Данные о личном ключе имеют размер, превышающий допустимый размер для входного пакета размером *'размер пакета'*.

Длина цепочки сертифкатов больше, чем значение компонента pathLenConstraint расширения BasicConstraints точки доверия.

Для самоподписанного сертификата с серийным номером *'серийный номер СОК'* не найден набор долговременных параметров.

Загружено локальное хранилище сертификатов.

Задан неизвестный объектный идентификатор алгоритма подписи OCSP-ответа = *'объектный идентификатор'*.

Задан неизвестный объектный идентификатор алгоритма подписи СОС = *'объектный идентификатор'*.

Задано некорректное имя подписанного файла.

Задано некорректное имя результирующего файла.

Запрошен сертификат в УЦ по HTTP.

Запрошена криптооперация: подписание данных.

Запрошена криптооперация: проверка ЭЦП под данными.

Запрошена криптооперация: формирование заявки на выпуск сертификата по шаблону.

Запущен поток опроса почтового ящика CryptoService'a.

Запущен поток, прослушивающий сокеты.

Значение компонента pathLenConstraint расширения BasicConstraints точки доверия меньше 0.

Значение расширения идентификатора ключа издателя сертификата - пусто.

Идентификатор открытого ключа должен содержать чётное количество шестнадцатеричных цифр.

Извещение с идентификатором *'идентификатор извещения'* заявку на выпуск сертификата не содержит текста.

Извещение с идентификатором *'идентификатор извещения'* заявку на выпуск сертификата содержит некорректный текст.

Извещение с идентификатором *'идентификатор извещения'* на заявку на выпуск сертификата содержит некорректный код возврата.

Инициализирован транспортный менеджер.

Инициализировано криптоядро.

Исходный файл *'имя файла'* - пуст.

Клиент не имеет полномочий делать OCSP-запрос на данный OCSP-сервер.

Ключ с идентификатором *'идентификатор открытого ключа'* не может использоваться для подписания произвольных документов.

Количество атрибутов в значении расширения атрибутов директории владельца сертификата равно НУЛЮ.

Количество введённых шестнадцатеричных цифр серийного номера - НЕ чётно.

Контейнер P7B не содержит сертификатов.

Личный ключ с идентификатором *'идентификатор открытого ключа'* не является ключом ЭЦП.

Локальное хранилище сертификатов сохранено в файле *'полное имя файла с локальным хранилищем сертификатов'*.

Минимальная длина пароля составляет *'количество символов пароля'* символов.

Момент окончания приостановки сертификата НЕ ПОЗЖЕ момента начала его приостановки.

Нарушена структура ASN1-заявки.

Нарушена структура корневого сертификата УЦ: секция расширений не является последней в секции 'TBS'.

Нарушена структура секции долговременных параметров в локальном хранилище сертификатов на диске.

Нарушена структура секции наборов долговременных параметров в локальном хранилище сертификатов на диске.

Нарушена структура секции одиночных долговременных параметров в локальном хранилище сертификатов на диске.

Нарушена структура секции сертификатов в локальном хранилище на диске.

Нарушена структура секции сертификатов локального хранилища на жёстком диске.

Нарушена структура трейлера ЭЦП: не корректен объектный идентификатор алгоритма Belt-хэширования.

Нарушена структура трейлера ЭЦП: не корректен тег версии.

Нарушена структура трейлера ЭЦП: не корректен тег времени подписания.

Нарушена структура трейлера ЭЦП: не корректен тег значения подписи.

Нарушена структура трейлера ЭЦП: не корректен тег идентификатора ключа подписанта.

Нарушена структура трейлера ЭЦП: не корректен тег имени оригинального файла.

Нарушена структура трейлера ЭЦП: не корректен тег корневого элемента.

Нарушена структура трейлера ЭЦП: не корректен тег размера оригинального файла.

Нарушена структура трейлера ЭЦП: не корректно имя оригинального файла.

Нарушена структура трейлера ЭЦП: не корректно хэш-значение.

Нарушена структура трейлера ЭЦП: отсутствует хэш-значение.

Нарушена структура трейлера ЭЦП: отсутствуют элементы после версии.

Нарушена структура файла со списком заявок/запросов.

Нарушена структура файла со стандартными наборами долговременных параметров.

Нарушена целостность файла *'имя файла'*.

Нарушена целостность криптобиблиотеки 'ContactCrypto32LE.dll'.

Нарушена целостность криптобиблиотеки 'CryptoCont.dll'.

Нарушена целостность файла со стандартными наборами долговременных параметров.

Начальный ввод пароля.

Не введены ни серийный номер, ни идентификатор открытого ключа.

Не действителен личный ключ или сертификат подписанта ASN1-заявки с идентификатором *'идентификатор открытого ключа'*.

Не действителен личный ключ или сертификат подписанта OCSP-ответа с серийным номером *'серийный номер СОК'*.

Не действителен личный ключ или сертификат подписанта OCSP-ответа с идентификатором открытого ключа *'идентификатор открытого ключа'*.

Не действителен личный ключ или сертификат подписанта OCSP-ответа с серийным номером *'серийный номер'*.

Не действителен личный ключ или сертификат подписанта SOAP-ответа с идентификатором *'идентификатор открытого ключа'*.

Не действителен личный ключ или сертификат подписанта с идентификатором *'идентификатор открытого ключа'*.

Не действителен личный ключ или сертификат подписанта СОС с идентификатором открытого ключа *'идентификатор открытого ключа'*.

Не действителен личный ключ или сертификат с идентификатором *'идентификатор открытого ключа'* подписанта SOAP-ответа.

Не действителен личный ключ или сертификат с идентификатором *'идентификатор открытого ключа'*.

Не допустимая битовая длина личного ключа ПФОК РД РБ.

Не допустимая битовая длина личного ключа СТБ 1176.2-99.

Не допустимый размер блоба личного ключа старой версии.

Не задан номер СОС и идентификатор ключа издателя СОС.

Не задан номер СОС.

Не задано значение расширения времени подписания сертификата.

Не задано значение расширения личного номера из документа, удостоверяющего личность.

Не задано значение расширения УНП.

Не задано значение расширения форматов бланка карточки открытого ключа, применяемых в ГосСУОК.

Не закрыты диалоговые окна. Перед завершением работы их необходимо закрыть.

Не известный объектный идентификатор алгоритма ЭЦП издателя сертификата.

Не известный объектный идентификатор параметра полномочного документа.

Не корректен битовый размер ЭЦП издателя сертификата по СТБ 1176.2.

Не корректен битовый размер ЭЦП издателя сертификата по СТБ 34.101.45.

Не корректен защищённый ключ ASN1-блоба личного ключа.

Не корректен идентификатор открытого ключа ASN1-блоба личного ключа.

Не корректен компонент 'EDIPartyName' структуры 'GeneralName'.

Не корректен компонент 'ORAddress' структуры 'GeneralName'.

Не корректен компонент 'ORAddress.BuiltInDomainDefinedAttributes.BuiltInDomainDefinedAttribute' структуры 'GeneralName'.

Не корректен компонент 'ORAddress.BuiltInDomainDefinedAttributes.BuiltInDomainDefinedAttribute.Type' структуры 'GeneralName'.

Не корректен компонент 'ORAddress.BuiltInDomainDefinedAttributes.BuiltInDomainDefinedAttribute.Value' структуры 'GeneralName'.

Не корректен компонент 'ORAddress.BuiltlnStandardAttributes' структуры 'GeneralName'.

Не корректен компонент 'ORAddress.BuiltlnStandardAttributes.AdministrationDomainName' структуры 'GeneralName'.

Не корректен компонент 'ORAddress.BuiltlnStandardAttributes.CountryName' структуры 'GeneralName'.

Не корректен компонент 'ORAddress.BuiltlnStandardAttributes.OrganizationalUnitNames' структуры 'GeneralName'.

Не корректен компонент 'ORAddress.BuiltlnStandardAttributes.PersonalName' структуры 'GeneralName'.

Не корректен компонент 'ORAddress.BuiltlnStandardAttributes.PrivateDomainName' структуры 'GeneralName'.

Не корректен компонент 'ORAddress.ExtensionAttributes.ExtensionAttribute' структуры 'GeneralName'.

Не корректен компонент 'ORAddress.ExtensionAttributes.ExtensionAttribute.Type' структуры 'GeneralName'.

Не корректен компонент 'ORAddress.ExtensionAttributes.ExtensionAttribute.Value' структуры 'GeneralName'.

Не корректен компонент 'OtherName' структуры 'GeneralName'.

Не корректен корневой тег дерева P7B.

Не корректен корневой тег.

Не корректен объектный идентификатор алгоритма выработки имитовставки ASN1-блоба личного ключа.

Не корректен объектный идентификатор алгоритма генерации ключа защиты по паролю ASN1-блоба личного ключа.

Не корректен объектный идентификатор алгоритма защиты ключа ASN1-блоба личного ключа.

Не корректен объектный идентификатор инкапсулированных данных CMS дерева P7B.

Не корректен объектный идентификатор подписанных данных CMS дерева P7B.

Не корректен объектный идентификатор типа ответа на OCSP-запрос = *'объектный идентификатор'*.

Не корректен размер базовой точки эллиптической кривой.

Не корректен размер долговременного параметра 'H'.

Не корректен размер значения расширения области применения ключа.

Не корректен размер идентификатора открытого ключа подписанта OCSP-ответа.

Не корректен размер идентификатора открытого ключа подписанта СОС.

Не корректен размер инициализирующей d-последовательности.

Не корректен размер инициализирующей l-последовательности.

Не корректен размер инициализирующей Z-последовательности.

Не корректен размер открытого ключа ПФОК РД РБ.

Не корректен размер открытого ключа СТБ 34.101.45.

Не корректен размер открытого ключа ЭЦП-1176.2.

Не корректен размер параметра 'A' эллиптической кривой.

Не корректен размер параметра 'B' эллиптической кривой.

Не корректен размер параметра 'Seed' эллиптической кривой.

Не корректен размер порядка группы точек эллиптической кривой.

Не корректен размер серийного номера сертификата подписанта OCSP-ответа.

Не корректен размер серийного номера сертификата подписанта СОС.

Не корректен синтаксис OCSP-запроса.

Не корректен статус OCSP-ответа.

Не корректен тег OId'a алгоритма ЭЦП корневого сертификата УЦ.

Не корректен тег OId'a алгоритма ЭЦП секции 'TBS' корневого сертификата УЦ.

Не корректен тег OId'a расширения корневого сертификата УЦ.

Не корректен тег TBS-секции ответа на OCSP-запрос.

Не корректен тег TBS-секции СОС.

Не корректен тег URI-ссылки на положение о сертификации.

Не корректен тег алгоритма ЭЦП корневого сертификата УЦ.

Не корректен тег алгоритма ЭЦП секции 'TBS' корневого сертификата УЦ.

Не корректен тег атрибута в значении расширения атрибутов директории владельца сертификата.

Не корректен тег атрибута издателя СОС.

Не корректен тег атрибута.

Не корректен тег базовой точки эллиптической кривой.

Не корректен тег версии корневого сертификата УЦ.

Не корректен тег версии.

Не корректен тег времени отзыва сертификата с серийным номером *'серийный номер СОК'*.

Не корректен тег времени создания OCSP-ответа.

Не корректен тег даты выпуска CRL.

Не корректен тег долговременного параметра 'A'.

Не корректен тег долговременного параметра 'G'.

Не корректен тег долговременного параметра 'H'.

Не корректен тег долговременного параметра 'L'.

Не корректен тег долговременного параметра 'N'.

Не корректен тег долговременного параметра 'P'.

Не корректен тег долговременного параметра 'Q'.

Не корректен тег долговременного параметра 'R'.

Не корректен тег значения атрибута в значении расширения атрибутов директории владельца сертификата.

Не корректен тег значения атрибута издателя СОС.

Не корректен тег значения атрибута.

Не корректен тег значения открытого ключа ПФОК РД РБ.

Не корректен тег значения открытого ключа ЭЦП-1176.2.

Не корректен тег значения открытого ключа.

Не корректен тег значения параметра полномочного документа.

Не корректен тег значения подписи СОС.

Не корректен тег значения расширения OCSP-ответа.

Не корректен тег значения расширения доступа к торговым секциям.

Не корректен тег значения расширения запрета произвольной политики.

Не корректен тег значения расширения идентификатора ключа подписанта СОС.

Не корректен тег значения расширения идентификатора ключа подписанта OCSP-ответа.

Не корректен тег значения расширения 'Номер СОС'.

Не корректен тег значения расширения *'объектный идентификатор'*.

Не корректен тег значения расширения ограничения имён.

Не корректен тег значения расширения ограничения политик.

Не корректен тег значения расширения основных ограничений применения ключа.

Не корректен тег значения расширения периода действия личного ключа.

Не корректен тег значения расширения полномочий в торговой системе.

Не корректен тег значения расширения полномочий на работу в системах электронного документооборота.

Не корректен тег значения расширения полномочного документа.

Не корректен тег значения расширения расширенной области применения ключа.

Не корректен тег значения расширения юридического статуса.

Не корректен тег значения расширенной области применения ключа.

Не корректен тег идентификатора OCSP-сервера.

Не корректен тег идентификатора алгоритма подписи OCSP-ответа.

Не корректен тег идентификатора алгоритма подписи COC.

Не корректен тег идентификатора сертификата.

Не корректен тег имени OCSP-сервера.

Не корректен тег имени в значении расширения альтернативного имени владельца сертификата.

Не корректен тег инициализирующего числа 'D'.

Не корректен тег инициализирующей d-последовательности.

Не корректен тег инициализирующей l-последовательности.

Не корректен тег инициализирующей r-последовательности.

Не корректен тег инициализирующей Z-последовательности.

Не корректен тег квалификатора политики сертификата.

Не корректен тег компоненты 'IssuerDomainPolicy' отображения политики сертификата.

Не корректен тег компоненты 'SubjectDomainPolicy' отображения политики сертификата.

Не корректен тег контейнера алгоритма ЭЦП издателя сертификата.

Не корректен тег контейнера атрибутов.

Не корректен тег контейнера долговременных параметров ПФОК РД РБ.

Не корректен тег контейнера долговременных параметров СТБ 1176.2-99.

Не корректен тег контейнера долговременных параметров ЭЦП-1176.2.

Не корректен тег контейнера долговременных параметров.

Не корректен тег контейнера идентификатора алгоритма ЭЦП издателя сертификата.

Не корректен тег контейнера идентификатора ключа издателя сертификата.

Не корректен тег контейнера инкапсулированных данных CMS дерева P7B.

Не корректен тег контейнера объектных идентификаторов хэширования подписанных

данных CMS дерева P7B.

Не корректен тег контейнера открытых ключей ЭЦП-1176.2 и ПФОК РД РБ.

Не корректен тег контейнера отозванного сертификата.

Не корректен тег контейнера параметров эллиптической кривой.

Не корректен тег контейнера подписанных данных CMS дерева P7B.

Не корректен тег контейнера расширений OCSP-ответа.

Не корректен тег контейнера расширений корневого сертификата УЦ.

Не корректен тег контейнера сертификатов дерева P7B.

Не корректен тег корневого ASN1-элемента OCSP-ответа.

Не корректен тег корневого ASN1-элемента COC.

Не корректен тег контейнера атрибутов в значении расширения атрибутов директории владельца сертификата.

Не корректен тег контейнера имён в значении расширения альтернативного имени владельца сертификата.

Не корректен тег контейнера имён в значении расширения альтернативного имени издателя сертификата.

Не корректен тег контейнера квалификаторов политики сертификата.

Не корректен тег контейнера отображений политик в значении расширения отображения политик сертификата.

Не корректен тег контейнера политик в значении расширения политик сертификата.

Не корректен тег кофактора группы точек эллиптической кривой.

Не корректен тег наименование организации в квалификаторе политики сертификата.

Не корректен тег начала периода действия сертификата.

Не корректен тег номера уведомления пользователя в квалификаторе политики сертификата.

Не корректен тег номеров уведомлений пользователя в квалификаторе политики сертификата.

Не корректен тег объектного идентификатора алгоритма открытого ключа.

Не корректен тег объектного идентификатора алгоритма открытого ключа ASN1-сертификата.

Не корректен тег объектного идентификатора алгоритма ЭЦП издателя сертификата.

Не корректен тег объектного идентификатора атрибута издателя COC.

Не корректен тег объектного идентификатора атрибута.

Не корректен тег объектного идентификатора квалификатора политики сертификата.

Не корректен тег объектного идентификатора параметра полномочного документа.

Не корректен тег объектного идентификатора политики сертификата.

Не корректен тег объектного идентификатора расширения OCSP-ответа.

Не корректен тег объектного идентификатора расширения COC.

Не корректен тег объектного идентификатора расширения.

Не корректен тег одиночного ответа на OCSP-запрос.

Не корректен тег окончания периода действия сертификата.

Не корректен тег описателя поля, над которым построена эллиптическая кривая.

Не корректен тег открытого ключа СТБ 34.101.45.

Не корректен тег отображения политики сертификата.

Не корректен тег параметра 'A' эллиптической кривой.

Не корректен тег параметра 'B' эллиптической кривой.

Не корректен тег параметра 'Seed' эллиптической кривой.

Не корректен тег параметров алгоритма ЭЦП издателя сертификата.

Не корректен тег периода действия корневого сертификата УЦ.

Не корректен тег поддерева типа 'GeneralSubtree'.

Не корректен тег подписанной части.

Не корректен тег политики сертификата.

Не корректен тег порядка группы точек эллиптической кривой.

Не корректен тег порядка поля, над которым построена эллиптическая кривая.

Не корректен тег расширения COC.

Не корректен тег секции 'TBS' корневого сертификата УЦ.

Не корректен тег секции алгоритма открытого ключа.

Не корректен тег секции владельца корневого сертификата УЦ.

Не корректен тег секции владельца сертификата.

Не корректен тег секции издателя CRL.

Не корректен тег секции издателя корневого сертификата УЦ.

Не корректен тег секции издателя сертификата.

Не корректен тег секции открытого ключа корневого сертификата УЦ.

Не корректен тег секции открытого ключа.

Не корректен тег секции периода действия сертификата.

Не корректен тег секции расширений OCSP-ответа.

Не корректен тег секции расширений.

Не корректен тег серийного номера корневого сертификата УЦ.

Не корректен тег серийного номера отозванного сертификата.

Не корректен тег серийного номера сертификата.

Не корректен тег серийного номера.

Не корректен тег списка ответов на OCSP-запрос.

Не корректен тег статуса OCSP-ответа.

Не корректен тег текста уведомления пользователя в квалификаторе политики сертификата.

Не корректен тег тела ответа 'BasicOCSPResponse' на OCSP-запрос.

Не корректен тег тела ответа на OCSP-запрос.

Не корректен тег типа атрибута в значении расширения атрибутов директории владельца сертификата.

Не корректен тег типа поля, над которым построена эллиптическая кривая.

Не корректен тег уведомления пользователя в квалификаторе политики сертификата.

Не корректен тег флага критичности расширения *'объектный идентификатор'*.

Не корректен тег хэш-значения открытого ключа OCSP-сервера.

Не корректен тег ЭЦП корневого сертификата УЦ.

Не корректен тег ЭЦП под сертификатом.

Не корректна битовая длина ключа ASN1-блоба личного ключа.

Не корректна версия ASN1-блоба личного ключа.

Не корректна версия контейнера подписанных данных CMS дерева P7B.

Не корректна версия набора долговременных параметров.

Не корректна версия ответа на OCSP-запрос.

Не корректна версия СОС.

Не корректна длина подписи по СТБ 1176.2 под OCSP-ответом.

Не корректна длина подписи по СТБ 1176.2 под СОС.

Не корректна длина подписи по СТБ 34.101.45 под OCSP-ответом.

Не корректна длина подписи по СТБ 34.101.45 под СОС.

Не корректна секция '[0] EXPLICIT' ответа на OCSP-запрос.

Не корректна секция 'ResponseBytes' ответа на OCSP-запрос.

Не корректна секция описания алгоритма генерации ключа защиты по паролю ASN1-блоба личного ключа.

Не корректна секция описания алгоритма защиты ключа ASN1-блоба личного ключа.

Не корректна секция параметров алгоритма генерации ключа защиты по паролю ASN1-блоба личного ключа.

Не корректна секция параметров алгоритма защиты ключа ASN1-блоба личного ключа.

Не корректна секция цепочки сертификатов OCSP-ответа.

Не корректна синхропосылка алгоритма генерации ключа защиты по паролю ASN1-блоба личного ключа.

Не корректна структура значения расширения ограничения имён.

Не корректна структура значения расширения ограничения политик.

Не корректна структура значения расширения основных ограничений применения ключа.

Не корректна структура контейнера идентификатора алгоритма ЭЦП издателя сертификата.

Не корректна структура параметра полномочного документа.

Не корректна структура поддерева типа 'GeneralSubtree'.

Не корректна структура секции долговременных параметров ПФОК РД РБ.

Не корректна структура секции долговременных параметров.

Не корректная длина IP-адреса.

Не корректно время начала действия личного ключа в значении расширения периода действия личного ключа.

Не корректно время окончания действия личного ключа в значении расширения периода действия личного ключа.

Не корректно значение долговременного параметра 'A'.

Не корректно значение долговременного параметра 'G'.

Не корректно значение долговременного параметра 'L'.

Не корректно значение долговременного параметра 'N'.

Не корректно значение долговременного параметра 'P'.

Не корректно значение долговременного параметра 'Q'.

Не корректно значение долговременного параметра 'R'.

Не корректно значение инициализирующего числа 'D'.

Не корректно значение порядка поля, над которым построена эллиптическая кривая.

Не корректно значение расширения идентификатора ключа владельца сертификата.

Не корректно значение расширения идентификатора ключа издателя сертификата.

Не корректно значение расширения области применения ключа.

Не корректно значение расширения *'объектный идентификатор'*.

Не корректно значение уникального идентификатора владельца сертификата.

Не корректно значение уникального идентификатора издателя сертификата.

Не корректно количество итераций алгоритма генерации ключа защиты по паролю ASN1-блоба личного ключа.

Не корректны параметры алгоритма выработки имитовставки ASN1-блоба личного ключа.

Не корректны флаги использования ключа ASN1-блоба личного ключа.

НЕ корректный размер двойного набора долговременных параметров { СТБ 1176.2 + ПФОК РД РБ } в локальном хранилище сертификатов на диске.

НЕ корректный размер набора долговременных параметров ПФОК РД РБ в локальном хранилище сертификатов на диске.

НЕ корректный размер набора долговременных параметров СТБ 1176.2 в локальном хранилище сертификатов на диске.

НЕ корректный размер набора долговременных параметров СТБ 34.101.45 в локальном хранилище сертификатов на диске.

Не найден ОТКРЫТЫЙ КЛЮЧ в сертификате точки доверия.

Не найден открытый ключ.

Не найден серийный номер.

Не найден сертификат издателя.

Не найден сертификат подписанта ASN1-заявки с идентификатором *'идентификатор открытого ключа'*.

Не найден сертификат подписанта OCSP-ответа с идентификатором открытого ключа *'идентификатор открытого ключа'*.

Не найден сертификат подписанта OCSP-ответа с серийным номером *'серийный номер СОК'*.

Не найден сертификат подписанта SOAP-ответа с идентификатором *'идентификатор открытого ключа'*.

Не найден сертификат подписанта с идентификатором *'идентификатор открытого ключа'*.

Не найден сертификат подписанта СОС с идентификатором открытого ключа *'идентификатор открытого ключа'*.

Не найден сертификат подписанта СОС с серийным номером *'серийный номер СОК'*.

Не найден сертификат с идентификатором *'идентификатор открытого ключа'* подписанта SOAP-ответа.

Не найден сертификат с идентификатором *'идентификатор открытого ключа'*.

Не найден сертификат с серийным номером *'серийный номер СОК'*.

Не найден сертификат.

Не найдена TBS-секция.

Не найдена версия.

Не найдена секция алгоритма подписи сертификата.

Не найдена секция владельца сертификата.

Не найдена секция издателя сертификата.

Не найдена секция открытого ключа.

Не найдена секция срока действия сертификата.

Не найдено ИМЯ в сертификате точки доверия.

Не найдены ДОЛГОВРЕМЕННЫЕ ПАРАМЕТРЫ АЛГОРИТМА в сертификате точки доверия.

Не обработано ни одного OCSP-ответа с жёсткого диска.

Не обработано ни одного COC'а с жёсткого диска.

Не поддерживаемая версия сертификата v. *'номер версии'*.

Не совпадают идентификаторы алгоритма подписи COC в секции TBS и собственно COC.

Не совпадают объектные идентификаторы алгоритма ЭЦП издателя сертификата в секциях 'TBS' и 'ЭЦП'.

Не удалось загрузить библиотеку 'CertificateIssueRequest.dll' формирования заявки на выпуск сертификата.

Не удалось найти функцию ClearListElements в библиотеке.

Не удалось найти функцию 'FillIssueRequestList' в библиотеке 'CertificateIssueRequest.dll' формирования заявки на выпуск сертификата.

Не удалось найти функцию 'FillSignCard' в библиотеке 'CertificateIssueRequest.dll' формирования карточки открытого ключа.

Не удалось подгрузить в локальное хранилище сертификат, содержащийся в SOAP-ответе на заявку с идентификатором *'идентификатор заявки'*.

Не удалось сформировать заявку.

Не указан путь к xml-файлу сертификата.

Неверная структура xml-файла сертификата "*путь к файлу сертификата* '. Отсутствует информация об издателе.

Неверная структура xml-файла сертификата "*путь к файлу сертификата* '. Отсутствует период действия сертификата.

Неверная структура xml-файла сертификата "*путь к файлу сертификата* '. Отсутствует информация о владельце.

Неверная структура xml-файла сертификата "*путь к файлу сертификата* '. Отсутствует информация об открытом ключе.

Неверная структура xml-файла сертификата "*путь к файлу сертификата* '. Отсутствуют расширения сертификата.

Недействительна ЭЦП под сертификатом с серийным номером *'серийный номер СОК'*.

Недоступен сертификат издателя сертификата с серийным номером *'серийный номер СОК'*.

Неизвестное КРИТИЧНОЕ расширение.

Неизвестный объектный идентификатор алгоритма ЭЦП издателя сертификата.

Неизвестный объектный идентификатор *'объектный идентификатор'* квалификатора политики сертификата.

Некорректное подтверждение пароля. Придётся повторить операцию.

Некорректный заголовок локального хранилища сертификатов на диске.

Некорректный размер XML-файла с настройками.

Некорректный размер локального хранилища сертификатов на диске.

Некорректный размер файла *'имя файла'*.

Некорректный размер файла криптобиблиотеки 'ContactCrypto32LE.dll'.

Некорректный размер файла криптобиблиотеки 'CryptoCont.dll'.

Некорректный размер файла с личным ключом.

Некорректный размер файла со списком заявок/запросов.

Некорректный размер файла со стандартными наборами долговременных параметров.

Обнаружены различные наборы долговременных параметров с одинаковым индексом.

Обнаружены различные одиночные долговременные параметры с одинаковым индексом.

Обработано *'количество обработанных OCSP-ответов'* OCSP-ответа с жёсткого диска.

Обработано *'количество обработанных COC'* COC'а с жёсткого диска.

Объектный идентификатор алгоритма хэширования выходит за границы входного пакета.

Опрошен почтовый ящик CryptoService'а. Глобальный фильтр = *'глобальный фильтр электронной почты'*, локальный фильтр = *'локальный фильтр электронной почты'*.

Отказ в выпуске сертификата администратора.

Отказ от ввода пароля к личному ключу УЦ.

Отрицательный результат проверки ЭЦП под SOAP-ответом с идентификатором *'идентификатор SOAP-ответа'* на заявку на выпуск сертификата.

Отсутствует значение идентификатора ключа подписанта OCSP-ответа.

Отсутствует значение идентификатора ключа подписанта COC.

Отсутствует значение расширения OCSP-ответа.

Отсутствует значение расширения *'объектный идентификатор'*.

Отсутствует наименование организации в квалификаторе политики сертификата.

Отсутствует объектный идентификатор алгоритма подписи OCSP-ответа.

Отсутствует объектный идентификатор алгоритма подписи COC.

Отсутствует секция наборов долговременных параметров в локальном хранилище сертификатов на диске.

Отсутствует секция расширений в сертификате версии 3.

Отсутствуют номера уведомлений пользователя в квалификаторе политики сертификата.

Ошибка при хэшировании пароля к блобу личного ключа.

Ошибка -800 при обработке запроса *'идентификатор запроса'* по HTTP.

Ошибка OCSP-сервера при формировании ответа на OCSP-запрос.

Ошибка во время выработки ЭЦП по СТБ 1176.2-99.

Ошибка во время выработки ЭЦП под секцией 'TBS' сертификата администратора.

Ошибка во время подписания SOAP-конверта.

Ошибка во время подписания данных.

Ошибка выделения памяти для permitted_subtrees.

Ошибка выделения памяти для ASN1-заявки.

Ошибка выделения памяти для excluded-subtrees .

Ошибка выделения памяти для IAP-заявки.

Ошибка выделения памяти для initial-excludded-subtrees.

Ошибка выделения памяти для initial-permitted-subtrees.

Ошибка выделения памяти для OId'a набора долговременных параметров.

Ошибка выделения памяти для OId'a открытого ключа.

Ошибка выделения памяти для SOAP-запроса.

Ошибка выделения памяти для SOAP-заявки.

Ошибка выделения памяти для SOAP-конверта.

Ошибка выделения памяти для user-initial-policy-set.

Ошибка выделения памяти для valid_policy_tree.

Ошибка выделения памяти для XML-ответа.

Ошибка выделения памяти для XML-сертификата.

Ошибка выделения памяти для X-координаты открытого ключа СТБ 34.101.45.

Ошибка выделения памяти для Y-координаты открытого ключа СТБ 34.101.45.

Ошибка выделения памяти для аварийного ответа на криптооперацию.

Ошибка выделения памяти для алгоритма ЭЦП.

Ошибка выделения памяти для блоба личного ключа.

Ошибка выделения памяти для буфера файла.

Ошибка выделения памяти для выходного SOAP-конверта.

Ошибка выделения памяти для выходного пакета.

Ошибка выделения памяти для двойного набора долговременных параметров { СТБ 1176.2 + ПФОК РД РБ }.

Ошибка выделения памяти для дерева настроек верификации.

Ошибка выделения памяти для документа, удостоверяющего личность.

Ошибка выделения памяти для значения атрибута в значении расширения атрибутов директории владельца сертификата.

Ошибка выделения памяти для значения компонента 'ORAddress.ExtensionAttributes.ExtensionAttribute.Value' структуры 'GeneralName'.

Ошибка выделения памяти для значения компонента 'OtherName' структуры 'GeneralName'.

Ошибка выделения памяти для значения открытого ключа ПФОК.

Ошибка выделения памяти для значения открытого ключа ЭЦП.

Ошибка выделения памяти для значения расширения.

Ошибка выделения памяти для идентификатора ключа владельца сертификата.

Ошибка выделения памяти для идентификатора ключа издателя сертификата.

Ошибка выделения памяти для идентификатора ключа подписанта SOAP-ответа.

Ошибка выделения памяти для идентификатора ключа.

Ошибка выделения памяти для идентификатора открытого ключа в структуре 'KeysPair'.

Ошибка выделения памяти для идентификатора открытого ключа подписанта.

Ошибка выделения памяти для имени оригинального файла.

Ошибка выделения памяти для канонизации шаблона заявки 'Subscriber'.

Ошибка выделения памяти для канонической формы подписанной части SOAP-ответа.

Ошибка выделения памяти для канонической формы подписанной части SOAP-конверта.

Ошибка выделения памяти для личного ключа.

Ошибка выделения памяти для личного номера из документа, удостоверяющего личность.

Ошибка выделения памяти для локального адреса.

Ошибка выделения памяти для набора долговременных параметров ПФОК РД РБ.

Ошибка выделения памяти для набора долговременных параметров СТБ 34.101.45.

Ошибка выделения памяти для набора долговременных параметров СТБ 1176.2.

Ошибка выделения памяти для наименования должности.

Ошибка выделения памяти для наименования населённого пункта.

Ошибка выделения памяти для наименования области.

Ошибка выделения памяти для наименования организации.

Ошибка выделения памяти для наименования района.

Ошибка выделения памяти для наименования страны.

Ошибка выделения памяти для начала действия личного ключа.

Ошибка выделения памяти для начала действия сертификата.

Ошибка выделения памяти для объектного идентификатора алгоритма предварительного хэширования для СТБ 34.101.45.

Ошибка выделения памяти для объектного идентификатора двойного набора долговременных параметров { СТБ 1176.2 + ПФОК РД РБ }.

Ошибка выделения памяти для объектного идентификатора набора долговременных параметров СТБ 34.101.45.

Ошибка выделения памяти для объектного идентификатора набора долговременных параметров СТБ 1176.2.

Ошибка выделения памяти для объектного идентификатора набора долговременных параметров ПФОК РД РБ.

Ошибка выделения памяти для объектного идентификатора набора долговременных параметров.

Ошибка выделения памяти для объектного идентификатора расширения сертификата.

Ошибка выделения памяти для окончания действия личного ключа.

Ошибка выделения памяти для окончания действия сертификата.

Ошибка выделения памяти для ответа на запрос *'идентификатор запроса'* по HTTP.

Ошибка выделения памяти для открытого ключа.

Ошибка выделения памяти для подписываемой части ASN1-заявки.

Ошибка выделения памяти для подписываемой части IAP-заявки.

Ошибка выделения памяти для подписываемой части SOAP-конверта.

Ошибка выделения памяти для полного имени.

Ошибка выделения памяти для почтового индекса.

Ошибка выделения памяти для разобранного сертификата.

Ошибка выделения памяти для сериализации секции 'TBS' сертификата администратора.

Ошибка выделения памяти для серийного номера издателя.

Ошибка выделения памяти для серийного номера сертификата в структуре 'KeysPair'.

Ошибка выделения памяти для серийного номера.

Ошибка выделения памяти для сертификата издателя.

Ошибка выделения памяти для сертификата.

Ошибка выделения памяти для события изменения состояния сертификата.

Ошибка выделения памяти для уровня криптостойкости.

Ошибка выделения памяти для флага ПФОК.

Ошибка выделения памяти для юридического статуса.

Ошибка выделения памяти под SOAP-конверт заявки/запроса.

Ошибка выделения памяти под XML-шаблон атрибутов администратора.

Ошибка выделения памяти под долговременные параметры.

Ошибка выделения памяти под долговременный параметр.

Ошибка выделения памяти под запись истории сертификата.

Ошибка выделения памяти под запрос OCSP.

Ошибка выделения памяти под идентификатор открытого ключа сертификата локального хранилища.

Ошибка выделения памяти под локальное хранилище сертификатов.

Ошибка выделения памяти под настройки.

Ошибка выделения памяти под оригинал корневого сертификата УЦ.

Ошибка выделения памяти под открытый ключ.

Ошибка выделения памяти под серийный номер сертификата локального хранилища.

Ошибка выделения памяти под сертификат локального хранилища.

Ошибка выделения памяти под список заявок/запросов.

Ошибка выделения памяти под стандартные наборы долговременных параметров.

Ошибка выделения памяти под файл *'имя файла'* с OCSP-ответом.

Ошибка выделения памяти под файл *'имя файла'* со списком отозванных сертификатов.

Ошибка выделения памяти под файл *'имя файла'*.

Ошибка выделения памяти под элемент стека выделенных байтовых буферов, содержащих ASN1-документы.

Ошибка выделения памяти при формировании ASN1-заявки.

Ошибка выделения памяти при формировании карточки открытого ключа.

Ошибка выделения памяти при формировании личного ключа.

Ошибка вычисления хэш-значения.

Ошибка генерации ключевой пары ПФОК РД РБ.

Ошибка генерации ключевой пары СТБ 1176.2-99.

Ошибка добавления элемента типа 'DirectoryName' в дерево имен.

Ошибка добавления элемента типа 'DNS-name' в дерево имен.

Ошибка добавления элемента типа 'IP-address' в дерево имен.

Ошибка добавления элемента типа 'Rfc822-name' в дерево имен.

Ошибка добавления элемента типа 'UniformResourceIdentifier' в дерево имен.

Ошибка закрытия результирующего файла *'имя файла'*.

Ошибка записи ASN1-заявки в файл.

Ошибка записи блоба личного ключа в файл.

Ошибка записи данных в выходной файл *'имя файла'*.

Ошибка записи данных в результирующий файл *'имя файла'*.

Ошибка записи личного ключа в файл.

Ошибка записи сертификата администратора в файл.

Ошибка записи трейлера ЭЦП в выходной файл *'имя файла'*.

Ошибка записи файла с локальным хранилищем сертификатов.

Ошибка инициализации библиотеки сокетов.

Ошибка инициализации криптоядра.

Ошибка инициализации локального хранилища сертификатов.

Ошибка инициализации работы с USB-носителем личных ключей 'Rainbow'.

Ошибка инициализации работы с носителем ключей 'TouchMemory'.

Ошибка инициализации транспортного менеджера.

Ошибка инициализации характеристик серверного сокета.

Ошибка *'код ошибки'* во время выработки ЭЦП по СТБ 1176.2-99 под CMS-заявкой на отзыв сертификата.

Ошибка *'код ошибки'* во время выработки ЭЦП по СТБ 1176.2-99 под CMS-заявкой на приостановку сертификата.

Ошибка *'код ошибки'* во время выработки ЭЦП по СТБ 1176.2-99 под SOAP-конвертом.

Ошибка *'код ошибки'* во время выработки ЭЦП по СТБ 1176.2-99 под SOAP-заявкой на отзыв сертификата.

Ошибка *'код ошибки'* во время выработки ЭЦП по СТБ 1176.2-99 под SOAP-заявкой на приостановку сертификата.

Ошибка *'код ошибки'* во время выработки ЭЦП по СТБ 1176.2-99.

Ошибка *'код ошибки'* во время проверки ЭЦП по СТБ 1176.2-99.

Ошибка *'код ошибки'* при отправке SOAP-заявки типа *'тип SOAP-заявки'* Id=*'идентификатор SOAP-заявки'* в РЦ.

Ошибка *'код ошибки'* при передаче *'номер запроса'* -го запроса *'идентификатор запроса'*.

Ошибка *'код ошибки'* создания контекста выработки ЭЦП по СТБ 1176.2-99.

Ошибка *'код ошибки'* создания контекста проверки ЭЦП по СТБ 1176.2-99.

Ошибка *'номер ошибки'* при подписании SOAP-конверта.

Ошибка *'номер ошибки'* при создании потока, прослушивающего сокеты.

Ошибка *'номер ошибки'* хэширования TBS-секции OCSP-ответа.

Ошибка определения размера исходного файла *'имя файла'*.

Ошибка определения размера подписанного файла *'имя файла'*.

Ошибка определения размера сертификата издателя.

Ошибка определения размера сертификата.

Ошибка определения размера файла с ASN1-заявкой.

Ошибка определения размера файла с XML-шаблоном атрибутов администратора.

Ошибка определения размера файла с личным ключом.

Ошибка определения размера файла с оригиналом корневого сертификата УЦ.

Ошибка открытия XML-файла с настройками.

Ошибка открытия исходного файла *'имя файла'*.

Ошибка открытия подписанного файла *'имя файла'*.

Ошибка открытия файла для сохранения ASN1-заявки.

Ошибка открытия файла для сохранения SOAP-заявки.

Ошибка открытия файла для сохранения блоба личного ключа.

Ошибка открытия файла для сохранения личного ключа.

Ошибка открытия файла для сохранения сертификата администратора.

Ошибка открытия файла *'имя файла'* с OCSP-ответом.

Ошибка открытия файла *'имя файла'* со списком отозванных сертификатов.

Ошибка открытия файла криптобиблиотеки 'ContactCrypto32LE.dll'.

Ошибка открытия файла криптобиблиотеки 'CryptoCont.dll'.

Ошибка открытия файла *'путь к файлу'* с личным ключом.

Ошибка открытия файла с ASN1-заявкой.

Ошибка открытия файла с XML-шаблоном атрибутов администратора.

Ошибка открытия файла с личным ключом.

Ошибка открытия файла с локальным хранилищем сертификатов.

Ошибка открытия файла с оригиналом корневого сертификата УЦ.

Ошибка открытия файла с сертификатом издателя.

Ошибка открытия файла с сертификатом.

Ошибка открытия файла со стандартными наборами долговременных параметров.

Ошибка перечисления личных ключей на USB-носителе 'Меркурий'.

Ошибка перечисления файлов с личным ключом в директории *'имя директории'*.

Ошибка подписания секции 'CertificationRequestInfo' ASN1-заявки.

Ошибка получения секции настроек для выпуска заявки.

Ошибка построения дерева объектных идентификаторов.

Ошибка при выборе устройства iKey (USB ключ Rainbow).

Ошибка при выборе устройства TouchMemory.

Ошибка при выполнении тестового набора *'название тестового набора'*.

Ошибка при выработке имитовставки от блоба личного ключа.

Ошибка при заворачивании ASN1-заявки в SOAP-конверт: Ошибка выделения памяти под SOAP-конверт заявки.

Ошибка при загрузке идентификаторов объектов: Некорректный размер файла 'Object Identifiers.xml' с идентификаторами объектов.

Ошибка при загрузке идентификаторов объектов: Ошибка выделения памяти для чтения идентификаторов объектов.

Ошибка при загрузке идентификаторов объектов: Ошибка выделения памяти для структуры идентификатора объекта.

Ошибка при загрузке идентификаторов объектов: Ошибка открытия файла 'Object Identifiers.xml' с идентификаторами объектов.

Ошибка при загрузке идентификаторов объектов: Ошибка чтения файла 'Object Identifiers.xml' с идентификаторами объектов.

Ошибка при записи файла ASN1-сертификата.

Ошибка при записи файла XML-сертификата.

Ошибка при контрольной Bign-выработке идентификационную ЭЦП.

Ошибка при контрольной Bign-выработке ЭЦП.

Ошибка при контрольной Bign-проверке идентификационной ЭЦП.

Ошибка при контрольной Bign-проверке ЭЦП.

Ошибка при контрольной Brng-генерации ПСЧ в режиме HMAC.

Ошибка при контрольной Brng-генерации ПСЧ в режиме счётчика.

Ошибка при контрольной выработке имитовставка hMac-hBel от 256-битного сообщения на 232-битном ключе.

Ошибка при контрольной выработке имитовставка hMac-hBel от 256-битного сообщения на 256-битном ключе.

Ошибка при контрольной выработке имитовставка hMac-hBel от 256-битного сообщения на 336-битном ключе.

Ошибка при контрольной выработке имитовставки по ГОСТ 28147-89.

Ошибка при контрольной выработке общего ключа по протоколу BMQV.

Ошибка при контрольной выработке общего ключа по протоколу BPACE.

Ошибка при контрольной выработке общего ключа по протоколу BSTS.

Ошибка при контрольной выработке ЭЦП по СТБ 1176.2-99 для 10-го уровня.

Ошибка при контрольной выработке ЭЦП по СТБ 1176.2-99 для 3-го уровня.

Ошибка при контрольной выработке ЭЦП по СТБ 1176.2-99 для 6-го уровня.

Ошибка при контрольной генерации ключевой пары по СТБ 1176.2-99 для 3-го уровня.

Ошибка при контрольной генерации ключевой пары по СТБ 1176.2-99 для 6-го уровня.

Ошибка при контрольной генерации ключевой пары по СТБ 1176.2-99 для 10-го уровня.

Ошибка при контрольной генерации ключевой пары ПФОК стороны A для 3-го уровня.

Ошибка при контрольной генерации ключевой пары ПФОК стороны A для 6-го уровня.

Ошибка при контрольной генерации ключевой пары ПФОК стороны A для 10-го уровня.

Ошибка при контрольной генерации ключевой пары ПФОК стороны B для 3-го уровня.

Ошибка при контрольной генерации ключевой пары ПФОК стороны B для 6-го уровня.

Ошибка при контрольной генерации ключевой пары ПФОК стороны B для 10-го уровня.

Ошибка при контрольной генерации секретного и обменного чисел ПФОК стороны A для 3-го уровня.

Ошибка при контрольной генерации секретного и обменного чисел ПФОК стороны B для 3-го уровня.

Ошибка при контрольной генерации секретного и обменного чисел ПФОК стороны A для 6-го уровня.

Ошибка при контрольной генерации секретного и обменного чисел ПФОК стороны B для 6-го уровня.

Ошибка при контрольной генерации секретного и обменного чисел ПФОК стороны A для 10-го уровня.

Ошибка при контрольной генерации секретного и обменного чисел ПФОК стороны B для 10-го уровня.

Ошибка при контрольном Belt-выработки имитовставки от 104 битов.

Ошибка при контрольном Belt-выработки имитовставки от 384 битов.

Ошибка при контрольном Belt-зашифровании гаммированием 384 битов.

Ошибка при контрольном Belt-зашифровании гаммированием с обратной связью 384 битов.

Ошибка при контрольном Belt-зашифровании простой заменой 376 битов.

Ошибка при контрольном Belt-зашифровании простой заменой 384 битов.

Ошибка при контрольном Belt-зашифровании сцеплением блоков 288 битов.

Ошибка при контрольном Belt-зашифровании сцеплением блоков 384 битов.

Ошибка при контрольном Belt-преобразовании ключа 256->128.

Ошибка при контрольном Belt-преобразовании ключа 256->192.

Ошибка при контрольном Belt-преобразовании ключа 256->256.

Ошибка при контрольном Belt-расшифровании гаммированием с обратной связью

384 битов.

Ошибка при контрольном Belt-расшифровании простой заменой 288 битов.

Ошибка при контрольном Belt-расшифровании простой заменой 384 битов.

Ошибка при контрольном Belt-расшифровании сцеплением блоков 288 битов.

Ошибка при контрольном Belt-расшифровании сцеплением блоков 384 битов.

Ошибка при контрольном Belt-снятии защите с ключа.

Ошибка при контрольном Belt-снятии защиты с данных.

Ошибка при контрольном Belt-хэшировании 104 битов.

Ошибка при контрольном Belt-хэшировании 256 битов.

Ошибка при контрольном Belt-хэшировании 384 битов.

Ошибка при контрольном Belt-щифровании и имитозащите данных.

Ошибка при контрольном Belt-щифровании и имитозащите ключа.

Ошибка при контрольном Bign-вычислении открытого ключа по заданному личному.

Ошибка при контрольном Bign-извлечении ключевой пары из подписи доверенной стороны под идентификатором.

Ошибка при контрольном Bign-построении ключа защиты по паролю.

Ошибка при контрольном Bign-разборе токена ключа.

Ошибка при контрольном Bign-создании токена ключа.

Ошибка при контрольном зашифровании гаммированием с обратной связью по ГОСТ 28147-89.

Ошибка при контрольном зашифровании простой заменой по ГОСТ 28147-89.

Ошибка при контрольном одностороннем формировании общего ключа ПФОК стороной А для 3-го уровня.

Ошибка при контрольном одностороннем формировании общего ключа ПФОК стороной В для 3-го уровня.

Ошибка при контрольном одностороннем формировании общего ключа ПФОК для 3-го уровня.

Ошибка при контрольном одностороннем формировании общего ключа ПФОК стороной А для 6-го уровня.

Ошибка при контрольном одностороннем формировании общего ключа ПФОК стороной В для 6-го уровня.

Ошибка при контрольном одностороннем формировании общего ключа ПФОК для 6-го уровня.

Ошибка при контрольном одностороннем формировании общего ключа ПФОК стороной А для 10-го уровня.

Ошибка при контрольном одностороннем формировании общего ключа ПФОК стороной В для 10-го уровня.

Ошибка при контрольном одностороннем формировании общего ключа ПФОК для 10-го уровня.

Ошибка при контрольном разрушении контекста хэширования по СТБ 1176.1-99.

Ошибка при контрольном разрушении контекста выработки имитовставки по ГОСТ 28147-89.

Ошибка при контрольном разрушении контекста зашифрования гаммированием с обратной связью по ГОСТ 28147-89.

Ошибка при контрольном разрушении контекста зашифрования простой заменой по ГОСТ 28147-89.

Ошибка при контрольном разрушении контекста расшифрования гаммированием с обратной связью по ГОСТ 28147-89.

Ошибка при контрольном разрушении контекста расшифрования простой заменой по ГОСТ 28147-89.

Ошибка при контрольном разрушении контекста шифрования гаммированием по ГОСТ 28147-89.

Ошибка при контрольном расшифровании гаммированием с обратной связью по ГОСТ 28147-89.

Ошибка при контрольном расшифровании простой заменой по ГОСТ 28147-89.

Ошибка при контрольном создании контекста выработки имитовставки по ГОСТ 28147-89.

Ошибка при контрольном создании контекста зашифрования гаммированием с обратной связью по ГОСТ 28147-89.

Ошибка при контрольном создании контекста зашифрования простой заменой по ГОСТ 28147-89.

Ошибка при контрольном создании контекста расшифрования гаммированием с обратной связью по ГОСТ 28147-89.

Ошибка при контрольном создании контекста расшифрования простой заменой по ГОСТ 28147-89.

Ошибка при контрольном создании контекста хэширования по СТБ 1176.1-99.

Ошибка при контрольном создании контекста шифрования гаммированием по ГОСТ 28147-89.

Ошибка при контрольном формировании общего ключа ПФОК без аутентификации сторон для 3-го уровня.

Ошибка при контрольном формировании общего ключа ПФОК без аутентификации сторон для 6-го уровня.

Ошибка при контрольном формировании общего ключа ПФОК без аутентификации сторон для 10-го уровня.

Ошибка при контрольном формировании общего ключа ПФОК с аутентификацией сторон для 3-го уровня.

Ошибка при контрольном формировании общего ключа ПФОК с аутентификацией сторон

для 6-го уровня.

Ошибка при контрольном формировании общего ключа ПФОК с аутентификацией сторон для 10-го уровня.

Ошибка при контрольном формировании общего ключа ПФОК стороной А без аутентификации сторон для 3-го уровня.

Ошибка при контрольном формировании общего ключа ПФОК стороной А с аутентификацией сторон для 3-го уровня.

Ошибка при контрольном формировании общего ключа ПФОК стороной А без аутентификации сторон для 6-го уровня.

Ошибка при контрольном формировании общего ключа ПФОК стороной А с аутентификацией сторон для 6-го уровня.

Ошибка при контрольном формировании общего ключа ПФОК стороной А без аутентификации сторон для 10-го уровня.

Ошибка при контрольном формировании общего ключа ПФОК стороной А с аутентификацией сторон для 10-го уровня.

Ошибка при контрольном формировании общего ключа ПФОК стороной В без аутентификации сторон для 3-го уровня.

Ошибка при контрольном формировании общего ключа ПФОК стороной В с аутентификацией сторон для 3-го уровня.

Ошибка при контрольном формировании общего ключа ПФОК стороной В без аутентификации сторон для 6-го уровня.

Ошибка при контрольном формировании общего ключа ПФОК стороной В с аутентификацией сторон для 6-го уровня.

Ошибка при контрольном формировании общего ключа ПФОК стороной В без аутентификации сторон для 10-го уровня.

Ошибка при контрольном формировании общего ключа ПФОК стороной В с аутентификацией сторон для 10-го уровня.

Ошибка при контрольном хэшировании по СТБ 1176.1-99.

Ошибка при контрольном шифровании гаммированием по ГОСТ 28147-89.

Ошибка при определении размера xml-файла сертификата "*путь к файлу сертификата* '.

Ошибка при открытии xml-файла сертификата '*путь к файлу сертификата*'.

Ошибка при открытии файла *'имя файла'*.

Ошибка при отправке запроса OCSP.

Ошибка при перечислении устройств iKey (USB ключ Rainbow).

Ошибка при перечислении устройств TouchMemory.

Ошибка при расшифровании личного ключа.

Ошибка при создании контекста выработки имитовставки от блоба личного ключа.

Ошибка при создании контекста хэширования пароля к блобу личного ключа.

Ошибка при создании контекста шифрования для расшифрования личного ключа.

Ошибка при создании папки для оригиналов сертификата.

Ошибка при создании файла XML-сертификата.

Ошибка при старте потоковой функции опроса почтового ящика CryptoService'a.

Ошибка при формировании ASN1-заявки.

Ошибка при формировании IAP-заявки.

Ошибка при формировании SOAP-запроса на всеобщую историю сертификатов.

Ошибка при формировании блоба личного ключа.

Ошибка при формировании карточки открытого ключа.

Ошибка при формировании личного ключа.

Ошибка разбора xml-файла сертификата '*путь к файлу сертификата*'.

Ошибка связи с УЦ.

Ошибка сервера при обработке запроса *'идентификатор запроса'* по HTTP.

Ошибка создания временного файла для сохранения локального хранилища сертификатов.

Ошибка создания выходного файла *'имя файла'*.

Ошибка создания контекста хэширования.

Ошибка создания папки для заявок и запросов: *'путь директории для заявок и запросов'*.

Ошибка создания папки для обработанных ответов на заявки и запросы: *'путь директории для обработанных ответов на заявки и запросы*.

Ошибка создания папки для ответов на заявки и запросы: *'путь директории для ответов на заявки и запросы'*.

Ошибка создания папки для отправленных заявок и запросов: *'путь директории для отправленных заявок и запросов'*.

Ошибка создания папки с локальным хранилищем сертификатов: *'путь к папке с локальным хранилищем сертификатов'*.

Ошибка создания папки с подгружаемыми вручную сертификатами: *'путь к папке с подгружаемыми вручную СОК'*.

Ошибка создания папки с подгружаемыми вручную списками отозванных сертификатов: *' путь к папке с подгружаемыми вручную СОС'*.

Ошибка создания папки с сертификатами в форматах '.cer' и '.xml': *'путь к папке с*

сертификатами в форматах '.cer' и '.xml'.

Ошибка создания результирующего файла *'имя файла'.*

Ошибка создания серверного сокета.

Ошибка создания характеристик серверного сокета.

Ошибка сохранения во временном файле долговременных параметров.

Ошибка сохранения во временном файле заголовка локального хранилища сертификатов.

Ошибка установки серверного сокета на прослушивание сети.

Ошибка чтения XML-файла с настройками.

Ошибка чтения xml-файла сертификата "*путь к файлу сертификата* '.

Ошибка чтения исходного файла *'имя файла'.*

Ошибка чтения подписанного файла *'имя файла'.*

Ошибка чтения размера оригинального файла.

Ошибка чтения трейлера ЭЦП.

Ошибка чтения файла *'имя файла'* с OCSP-ответом.

Ошибка чтения файла *'имя файла'* со списком отозванных сертификатов.

Ошибка чтения файла *'имя файла'.*

Ошибка чтения файла криптобиблиотеки 'ContactCrypto32LE.dll'.

Ошибка чтения файла криптобиблиотеки 'CryptoCont.dll'.

Ошибка чтения файла *'путь к файлу'* с личным ключом.

Ошибка чтения файла с ASN1-заявкой.

Ошибка чтения файла с XML-шаблоном атрибутов администратора.

Ошибка чтения файла с корневым сертификатом.

Ошибка чтения файла с личным ключом.

Ошибка чтения файла с локальным хранилищем сертификатов.

Ошибка чтения файла с оригиналом корневого сертификата УЦ.

Ошибка чтения файла со списком заявок/запросов.

Ошибка чтения файла со стандартными наборами долговременных параметров.

Пароль выходит за границы входного пакета.

Пароль имеет размер, меньший 8.

Перечисление личных ключей на устройстве или в папке с именем *'имя директории'.*

Подпись под ASN1-заявкой недействительна.

Подпись под OCSP-ответом недействительна.

Подпись под SOAP-конвертом недействительна.

Подпись под SOAP-ответом недействительна.

Подпись под СОС недействительна.

Подпись ПФОК РД РБ под ASN1-заявкой недействительна.

Подпись СТБ 1176.2 под ASN1-заявкой недействительна.

Подпись СТБ 34.101.45 под ASN1-заявкой недействительна.

Поиск личного ключа на устройстве или в папке с именем *'имя директории'*.

Получен SOAP-ответ с идентификатором *'идентификатор SOAP-ответа'* неизвестного типа.

Получен ответ на запрос *'идентификатор запроса'* по HTTP.

Получен ответ неизвестного типа на заявку на выпуск сертификата с идентификатором *'идентификатор открытого ключа '*.

Получен пустой ответ на заявку или запрос.

Получено извещение с идентификатором *'идентификатор извещения'* на заявку на выпуск сертификата с кодом возврата = *'код возврата'* и текстом: *'текст извещения'*.

Получено сообщение об ошибке с идентификатором *'идентификатор ошибки'* на заявку на выпуск сертификата с кодом возврата = *'код возврата'* и текстом: *'текст сообщения'*.

Пользователь изменил пароль к своему личному ключу.

Пользователь отказался изменять пароль к своему личному ключу.

Пользователь отказался от ввода пароля доступа к личному ключу.

Пользователь отказался от формирования запроса на сертификат.

Пользователь отказался от формирования заявки на отзыв сертификата.

Пользователь отказался от формирования заявки на приостановку сертификата.

Пользователь отказался подписывать заявку.

Порт *'номер порта'* уже занят для прослушивания сети. Измените в настройке 'LocalHost.SocketPortNumber' номер порта и запустите CryptoService вновь.

Построено дерево объектных идентификаторов.

При запросе сертификата в локальном хранилище адрес поисковой характеристики равен NULL.

При обработке сертификата с серийным номером *'серийный номер СОК'* значение переменной EXPLICIT_POLICY не больше нуля и дерево политик VALID_POLICY_TREE равно нулю.

При перечислении личных ключей задано имя неизвестного устройства - носителя ключей.

При перечислении личных ключей на USB-носителе 'Меркурий' отсутствует имя ключевой области.

При перечислении личных ключей на устройстве или в папке на диске НЕ задано имя устройства или папки.

При поиске личного ключа задано имя неизвестного устройства - носителя ключей.

При поиске личного ключа на USB-носителе 'Меркурий' отсутствует имя ключевой области.

При поиске личного ключа на устройстве или в папке на диске НЕ задано имя устройства или папки.

При проверке сертификата с серийным номером *'серийный номер СОК'* MAX_PATH_LENGTH не больше нуля.

При проверке ЭЦП не найден сертификат подписанта с идентификатором *'идентификатор открытого ключа'*.

Пустая цепочка сертификатов.

Размер идентификатора ключа издателя превышает 255 байтов.

Размер серийного номера издателя превышает 255 байтов.

Размер серийного номера издателя равен НУЛЮ.

Размер серийного номера превышает 255.

Размер серийного номера равен НУЛЮ.

Расширенная область применения ключа - ПУСТА.

Результат опроса почтового ящика CryptoService'a = *'количество непрочитанных писем'*. Количество новых писем = *'количество новых писем'*.

Самоподписанный сертификат НЕ является сертификатом УЦ.

Секция издателя сертификата - ПУСТА.

Серийный номер должен содержать чётное количество шестнадцатеричных цифр.

Сертификат не найден - ошибка обработки запроса.

Сертификат не найден.

Сертификат подписанта с идентификатором *'идентификатор открытого ключа'* на момент времени *'дата и время'*- действителен.

Сертификат подписанта с идентификатором *'идентификатор открытого ключа'* на момент времени *'дата и время'* - недействителен.

Сертификат подписанта шаблона заявки 'Subscriber' с идентификатором *'идентификатор открытого ключа'* на момент времени *'дата и время'* недействителен.

Сертификат с идентификатором *'идентификатор открытого ключа'* на момент времени *'дата и время'* недействителен.

Сертификат с идентификатором *'идентификатор открытого ключа'* на момент времени *'дата и вермя'* недействителен.

Сертификат с правами издания сертификатов НЕ является сертификатом УЦ.

Сертификат с серийным номером *'серийный номер СОК'* уже содержится в локальном

хранилище.

Слишком маленький размер подписанного файла *'имя файла'*.

Содержится критичное неизвестное расширение *'объектный идентификатор'*.

Сообщение об ошибке с идентификатором *'идентификатор ошибки'* на заявку на выпуск сертификата содержит некорректный текст.

Сообщение об ошибке с идентификатором *'идентификатор ошибки'* на заявку на выпуск сертификата содержит некорректный код возврата.

Сообщение об ошибке с идентификатором *'идентификатор ошибки'* на заявку на выпуск сертификата не содержит текста.

СОС из файла *'имя файла'* не корректен.

Стартовал CryptoService.

Тело сертификата выходит за границы входного пакета.

Успешно обработан OCSP-ответ из файла *'имя файла'*.

Успешно обработан СОС из файла *'имя файла'*.

Успешно сформирована заявка на выпуск сертификата.

Успешно сформирована заявка на отзыв сертификата как CMS.

Успешно сформирована заявка на отзыв сертификата как PFX.

Успешно сформирована заявка на приостановку сертификата.

Успешно проверена целостность криптобиблиотеки 'ContactCrypto32LE.dll'.

Успешно проверена целостность криптобиблиотеки 'CryptoCont.dll'.

Успешно протестированы функции, содержащиеся в криптобиблиотеках.

Флаги использования ключа не содержат флагов ЭЦП = 0x1860000.

Целостность ASN1-заявки в формате PFX обеспечена имитовставкой MAC. Данный режим не поддерживается.

ЭЦП под SOAP-ответом – недействительна.

ЭЦП под SOAP-ответом с идентификатором *'идентификатор SOAP-ответа'* на заявку на выпуск сертификата - действительна.

ЭЦП под шаблоном заявки 'Subscriber' - недействительна.

ЭЦП, содержащаяся в подписанном файле, недействительна.

ПРИЛОЖЕНИЕ 6

ПРЕДВАРИТЕЛЬНО РАСПРЕДЕЛЕННЫЕ СЕКРЕТЫ ДЛЯ TLS

Файл предварительно распределённых секретов (pre-shared keys) - это двоичный файл, состоящий из 16-байтового заголовка и таблицы секретов, имеющей два столбца: идентификаторов секретов и значений секретов.

Заголовок состоит из четырёх 32-битных чисел в формате «Little endian":

1) количество строк таблицы;
2) длина идентификатора секрета (положительное число, не превосходящее 128) - ширина первого столбца таблицы;
3) длина значения секрета (положительное число, не превосходящее 64) - ширина второго столбца таблицы;
4) количество подтаблиц, на которые разбита данная таблица (в клиентских файлах предварительно распределённых секретов это число равно 1).

Предполагается, что серверная сторона генерирует секреты с помощью качественного физического датчика случайных чисел либо сертифицированного датчика псевдослучайных чисел, формирует для каждого секрета уникальный идентификатор и сохраняет эти пары в файле вышеописанной структуры. Затем разбивает всё множество секретов на некоторое количество подмножеств. Каждое такое подмножество сохраняется в файле вышеописанной структуры и пересылается по защищённому каналу определённому клиенту.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

В настоящем документе приняты следующие сокращения:

БД	– база данных
КПА УЦ	– Подсистема криптографической защиты информации. Комплекс программно-аппаратный Удостоверяющий центр СЮИК.466533.001
КП РЦ	– Подсистемы криптографической защиты информации. Комплекс программный Регистрационный центр BY.СЮИК.00363-02
КП СОБ	– Подсистема криптографической защиты информации. Комплекс программный Средств обеспечения безопасности РБ.СЮИК.00364-03
НЖМД	– накопитель на жестком магнитном диске
НКИ	- носитель ключевой информации
ОЗУ	– оперативное запоминающее устройство
ОС	– операционная система
ПЗУ	– постоянное запоминающее устройство
ПО	– программное обеспечение
ПЭВМ	– персональная электронно-вычислительная машина
СОК	– сертификат открытого ключа
СОС	– список отозванных сертификатов
ЭЦП	– электронная цифровая подпись

Лист регистрации изменений

Изм	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного докум. и дата	Подп.	Дата
	измененных	замененных	новых	аннулированных					

№ изм.	Подп.	Дата