УТВЕРЖДЕН

BY.СЮИК.00314-05 34 01-ЛУ

ПОДСИСТЕМА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
КОМПЛЕКС ПРОГРАММНО-АППАРАТНЫЙ
УДОСТОВЕРЯЮЩИЙ ЦЕНТР
СПЕЦИАЛЬНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Руководство оператора

BY.СЮИК.00314-05 34 01

Листов 35

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

2016

№ изм.	Подп.	Дата

Литера

АННОТАЦИЯ

В настоящем документе описывается последовательность действий по запуску программного обеспечения комплекса программно-аппаратного Удостоверяющий центр и порядок взаимодействия администратора с данным программным обеспечением.

Для понимания изложенного в документе материала необходимы навыки администрирования операционной системы семейства MS Windows XP, Server 2003, а также знание основ криптографии и нормативных правовых актов в области технического нормирования и стандартизации – СТБ 1176.1, СТБ 1176.2, ГОСТ 28147-89, СТБ 34.101.17, СТБ 34.101.19, СТБ 34.101.23, СТБ 34.101.26, СТБ 34.101.31, СТБ 34.101.45, СТБ 34.101.47, СТБ 34.101.49 и СТБ 34.101.66.

Данный документ предназначен для администраторов, обеспечивающих надежную и безопасную работу подсистемы криптографической защиты информации и электронной цифровой подписи в рамках инфраструктуры распределения открытых ключей, и не предусматривает описания стандартных действий оператора в среде операционной системы.

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

«Подсистема криптографической защиты информации. Комплекс программно-аппаратный Удостоверяющий центр» СЮИК.466533.001 (далее – КПА УЦ) входит в состав подсистемы криптографической защиты информации (далее КС КЗИ).

Специальное программное обеспечение BY.СЮИК.00314-05 (далее – СПО) КПА УЦ предназначено для выпуска и управления сертификатами открытых ключей (СОК), которые применяются для выработки и проверки электронной цифровой подписи (ЭЦП), а также для выработки общих ключей, используемых в процедурах шифрования и аутентификации.

КПА УЦ обеспечивает реализацию функций:

1) выпуска СОК;

2) отзыва СОК;

3) аутентификации администратора КПА УЦ;

4) хранения СОК и обеспечения доступа к ним;

5) приостановления действия и возобновления действия СОК;

6) выпуска списков отозванных сертификатов (СОС) в соответствии с политикой КПА УЦ, в том числе периодического;

7) выпуска СОК для «Подсистемы криптографической защиты информации. Комплекса программного Регистрационный центр» BY.СЮИК.00363-02 (далее – КП РЦ);

8) импорта СОК и СОС других КПА УЦ;

9) формирования СОК;

10) предоставления доступа к хранимым СОК и СОС;

11) долгосрочного хранения СОК и СОС, выводимых из оперативного обращения;

12) хранения архива СОК и СОС;

13) настройки состава сведений, включаемых в СОК;

14) формирования отчетов по выпущенным и отозванным СОК;

15) взаимодействия с КП РЦ

16) автоматизации передачи СОК в КП РЦ;

17) резервного копирования и восстановления базы данных КПА УЦ;

18) ведения журналов аудита;

19) обеспечения оперативной проверки статуса СОК по протоколу OCSP;

20) обеспечения работоспособности на машине вычислительной универсальной СЮИК.466218.001 под управлением ОС семейства MS Windows XP, Server 2003, с применением ПАК «Барьер».

Функции криптографических преобразований в КПА УЦ выполняются, входящим в его состав «Подсистемой криптографической защиты информации. Комплексом программным Средств обеспечения безопасности» РБ.СЮИК.00364-03 (далее – КП СОБ).

Со СПО КПА УЦ взаимодействуют три категории пользователей:

- администраторы КПА УЦ;
- авторизованные пользователи: администраторы КП РЦ и конечные пользователи, формирующие заявки на выпуск сертификатов открытых ключей и заявки на отзыв (приостановку) сертификатов;
- неавторизованные пользователи: пользователи инфраструктуры открытых ключей, обращающиеся за информацией СОК и их состоянием.

В документе описаны действия администратора КПА УЦ. Действия других пользователей описаны в документах «Подсистема криптографической защиты информации. Комплекс программный Регистрационный центр. Руководство оператора» BY.СЮИК.00363-02 34 01 и «Подсистема криптографической защиты информации. Комплекс программный Средств обеспечения безопасности. Руководство оператора» РБ.СЮИК.00364-03 34 01.

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

СПО КПА УЦ работает под управлением ОС MS Windows XP, Server 2003.

Для работы СПО необходима машина вычислительная универсальная СЮИК.466218.001 с эксплуатационными параметрами 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:

- Комплекс программно-аппаратный защиты ПЭВМ от несанкционированного доступа «Барьер» СЮИК.467458.001 (далее – ПАК «Барьер»);
- средство подключения ПЭВМ к сети передачи данных (сетевая карта или модем);
- источник бесперебойного питания.

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

- любую из ОС MS Windows XP, Server 2003;
- файловую систему FAT12, FAT16, FAT32, NTFS;

При работе с электронной почтой необходимо определить следующие элементы:

- адреса TCP/IP;
- номера портов ввода/вывода;
- имя почтового ящика, в который будут поступать заявки на выпуск СОК;
- пароль доступа к почтовому ящику.

3. ВЫПОЛНЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

3.1. Инсталляция СПО

СПО поставляется в инсталлированном производителем виде на машине вычислительной универсальной СЮИК.466218.001 и не требует дополнительных действий по инсталляции.

3.2. Настройка СПО

Так как СПО работает совместно с входящим в его состав КП СОБ, то настройка СПО включает в себя настройку КП СОБ и настройку собственно СПО. Настройка КП СОБ подробно описана в документе «Подсистема криптографической защиты информации. Комплекс программный Средств обеспечения безопасности. Руководство оператора» РБ.СЮИК.00364-03 34 01.

КПА УЦ принимает входящие запросы по HTTP-протоколу и по электронной почте, обрабатывает их, и результат обработки запроса возвращается пользователю. Заявки на выпуск, отзыв и приостановку СОК формируются при помощи КП СОБ и проходят предварительную проверку в КП РЦ. Для повышения безопасности ПС КЗИ в КПА УЦ обрабатываются только те заявки, которые получены от доверенных КП РЦ и подписаны личным ключом администратора КП РЦ, соответствующим открытому ключу, идентификатор которого указан в списке доверенных. Запросы и заявки приходят в КПА УЦ упакованными в SOAP-конверты. Администрирование КПА УЦ может осуществляться в ручном режиме путем редактирования файла настроек (settings.ini) в рабочей директории СПО (CA), а также посредством консоли с графическим интерфейсом – отдельного программного модуля, который обменивается данными с КПА УЦ по защищенному каналу. Для защиты канала передачи данных используется процедура аутентификации, при этом процедура аутентификации и поддержка защищенного канала выполняется сервером аутентификации, использующим сервис КП СОБ.

3.2.1. Настройка параметров модуля архивирования

Настройка архивирования происходит путем редактирования секции [Archiving] в настроечном файле. Параметры Year, Month, Day и Hour – это дата первого архивирования; параметр Period – период архивирования в месяцах; BufferizationPath – относительный путь, куда будут сохранятся файлы архивов; AfterExpireTermBeforeArchiving – период времени в месяцах, указывает сколько сертификат после прекращения действия будет находиться в основном хранилище до перемещения его в архив.

3.2.2. Настройка параметров резервного копирования

В секции [Reservation] в параметре ReservationPath указывается путь, куда будут сохраняться резервные копии.

В секции [ReservationTaskList] указывается список заданий резервирования в следующем формате:

TaskN = Period | dd/mm/yyyy|p|n,

где N – целое число, номер задания,

Period = {Day, Month, Year, Week } – имя поддиректории, относительно пути хранения резервных копий (указывается параметром ReservationPath в секции [Reservation]), в которую будут помещаться резервные копии,

dd/mm/yyyy – дата первого запуска задания,

p – периодичность запуска задания (в днях),

n – количество резервных копий, которое будет создано.

3.2.3. Настройка параметров хранилища сертификатов

Основные параметры секции [Database]:

- DbmsType – тип используемой СУБД;
- DbmsSrvAddr – сетевой адрес хоста, на котором запущена СУБД;
- Username – имя пользователя СУБД;
- Password – пароль пользователя СУБД;
- DbPath – алиас БД или путь к файлу СУБД.

3.2.4. Настройка параметров КП СОБ

Без КП СОБ работа СПО невозможна. Поэтому необходимо настроить параметры КП СОБ. Они находятся в секции [CryptoService]. В параметрах HostAddr и Port указываются сетевой адрес хоста и порт, на котором КП СОБ ожидает подключения. Параметры SockRdTimeout и SockWrTimeout – таймауты на чтение и запись данных в сокет в секундах.

При старте СПО проверяет запущен ли КП СОБ. Если это не выполнено СПО пробует запустить КП СОБ по пути указанном в параметре Path, а также проверяет состояние КП СОБ через промежуток времени в секундах, указанный в параметре PeriodForStateCS.

3.2.5. Настройка параметров диспетчера сеансов

Диспетчер сеансов обеспечивает передачу пользовательских запросов от модуля транспорта к диспетчеру запросов и модулю удаленного администрирования. Параметры

диспетчера сеансов находятся в секции [SessionDispatcher]. Далее описаны основные из них:

- DeleteMessages – флаг удаления писем с сервера;
- FromAddr – адрес e-mail удостоверяющего центра;
- TimeOut – таймаут (в секундах) обмена по сокетам;
- IncomingSrvPort – порт сервера входящей почты;
- IncomingSrvAddr – сетевой адрес сервера входящей почты;
- IncomingSslVersion – тип SSL (если используется) для доступа к серверу входящей почты;
- IncomingUser – имя пользователя сервера входящей почты;
- IncomingPass – пароль пользователя сервера входящей почты;
- OutgoingSrvPort – порт сервера исходящей почты;
- OutgoingSrvAddr – сетевой адрес сервера исходящей почты;
- OutgoingSslVersion – тип SSL (если используется) для доступа к серверу исходящей почты;
- OutgoingUser – имя пользователя сервера исходящей почты;
- OutgoingPass – пароль пользователя исходящей почты;
- ProxyType – тип используемого прокси сервера;
- Port – порт http-сервера.

3.2.6. Настройка параметров корневого сертификата и личного ключа

Для работы КПА УЦ необходимо настроить параметры корневого сертификата и его личного ключа. Они находятся в секции [CertificateInfo]. Серийный номер сертификата указывается в параметре SN, путь к нему – в параметре CertificatePath. Настройками личного ключа КПА УЦ являются путь к нему (параметр PrivateKeyPath) и пароль (параметр PrivateKeyPass).

3.2.7. Настройка параметров репликации изменений в хранилище сертификатов

В секции [ReplicationSettings] находятся параметры, связанные с репликацией изменений в хранилище сертификатов. В параметре Role указывается роль приложения в репликации. Возможны два значения: Distributor – распространитель изменений (для основного КПА УЦ) и Recipient – получатель изменений (для Реестров). Также в этой секции представлен транспортные настройки для репликации:

- IncomingSrvPort – порт сервера входящей почты;
- IncomingSrvAddr – сетевой адрес сервера входящей почты;

- IncomingSslVersion – тип SSL для доступа к серверу входящей почты;
- IncomingSrvUser – имя пользователя сервера входящей почты;
- IncomingSrvPass – пароль пользователя сервера входящей почты;
- OutgoingSrvPort – порт сервера исходящей почты;
- OutgoingSrvAddr – сетевой адрес сервера исходящей почты;
- OutgoingSslVersion – тип SSL для доступа к серверу исходящей почты;
- OutgoingSrvUser – имя пользователя сервера исходящей почты;
- OutgoingSrvPass – пароль пользователя исходящей почты;
- ProxyType – тип используемого прокси-сервера;
- RecipientAddress – адрес почтового ящика, в который будут поступать сообщения об изменении хранилища;
- e-mail000 – список адресов, по которым будет рассылаться сообщения об изменении хранилища; для Реестров этот список пуст.

3.2.8. Настройка выпуска списков отозванных сертификатов

Секция [Crl] содержит два параметра:

- CrlIssuerNumber – порядковый номер распространителя СОС. Например, для КПА УЦ задается параметр равный 0, для одного Реестра – 1 и т.д. Максимальное допустимое значение равно 255.
- PeriodOfIssueCrl, в котором указывается период автоматического выпуска списка отозванных сертификатов в минутах. Максимальное допустимое значение равно 35700 минут.

3.2.9. Настройка доверенных сертификатов администраторов КП РЦ

В секции [TrustedCertificates] в параметрах OID#1, OID#2 и так далее перечисляются идентификаторы ключей доверенных сертификатов администраторов КП РЦ, от которых можно обрабатывать заявки.

3.3 Подготовка к запуску СПО

Для эффективной работы и выполнения всех функций СПО необходимо наличие, по меньшей мере, следующих пар личных/открытых (СОК) ключей:

1) пара ключей – личный/открытый (корневой СОК) КПА УЦ;
2) пара ключей – личный/открытый (СОК) администратора КП РЦ;

СОК должны находиться в хранилище СОК КПА УЦ, и в локальном хранилище КП СОБ.

Перед запуском СПО необходимо удостовериться в том, что в рабочей директории присутствуют следующие файлы библиотек динамической компоновки:

- Des_DLL.dll,
- ssleay32.dll,
- libeay32.dll,
- LogClientSocket.dll,
- ContactDevice.dll,
- BarPciKeys.dll,
- Ailurus_HTTP_api.dll,
- Des_Auth.dll,
- zlib1.dll,
- msvcr71.dll.

При отсутствии DLL-файлов во время запуска приложения будет выдано соответствующее предупреждающее сообщение.

Для выполнения криптопреобразований необходимых в работе СПО КПА УЦ следует запустить модуль КП СОБ, выполнив предварительно его настройку.

3.4. Запуск СПО

Запуск СПО КПА УЦ производится непосредственным запуском исполняемого файла CA_Application.exe из места расположения СПО на жестком диске КПА УЦ. Консольное окно КПА УЦ представлено на рис. 1.

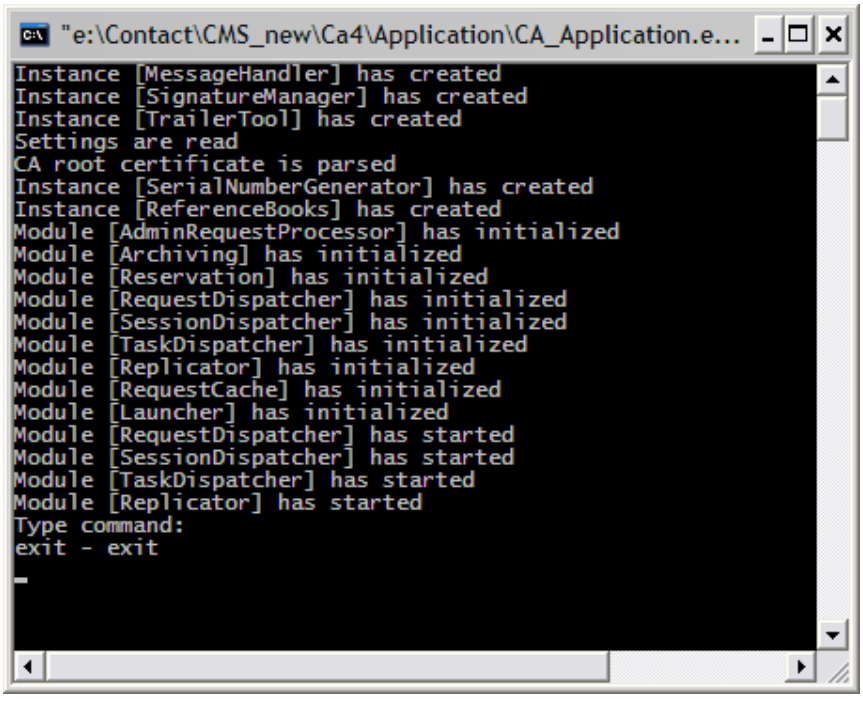

Рис. 1

3.5. Порядок выполнения СПО

3.5.1. Особенности работы с СПО

СПО не имеет визуального пользовательского интерфейса. Функции криптографических преобразований в СПО КПА УЦ выполняются КП СОБ.

Порядок работы с КП СОБ подробно описан в документе «Подсистема криптографической защиты информации. Комплекс программный Средств обеспечения безопасности. Руководство оператора» РБ.СЮИК.00364-03 34 01.

3.5.2. Администрирование

Администрирование СПО КПА УЦ осуществляется путем внесения, удаления и корректировки конфигурационного файла (settings.ini) и конфигурационного файла КП СОБ. Пример настроечного файла СПО КПА УЦ представлен в приложении А.

В качестве отдельно поставляемого приложения может использоваться ПО «Консоль администрирования комплекса программно-аппаратного Удостоверяющий центр» BY.СЮИК.00380-02 (далее – Консоль администрирования). Консоль администрирования может быть запущена локально или удаленно в пределах сегмента локальной сети. Консоль администрирования предоставляет возможность работы в диалоговом режиме с разнообразными окнами, каждое из которых предназначено для выполнения определенных действий администратора. Для простоты управления этими окнами в программе существует ряд функциональных кнопок.

Детальная работа с Консолью администрирования описана в документе «Консоль администрирования комплекса программно-аппаратного Удостоверяющий центр. Руководство оператора» BY.СЮИК.00380-02 34 01.

Для осуществления операции выпуска самоподписанного корневого сертификата используется утилита «RootCertificateIssuing.exe» (приложение Б).

3.5.3. Реестр СОК

СПО может быть настроено таким образом, что КПА УЦ функционирует в качестве реестра сертификатов открытых ключей, который может быть представлен несколькими точками распространения, предназначен для обслуживания внешних клиентов и выполняет следующие функции:

- предоставление информации о статусе СОК;
- обеспечение хранения и распространения СОК и СОС;

- внесение изменений в базы данных реестра СОК и СОС и регулярности обновления информации.

3.5.4. Резервное копирование хранилища сертификатов

СПО КПА УЦ позволяет создавать резервные копии хранилища сертификатов для его последующего восстановления в случае необходимости. Резервные копии создаются по расписанию, указанному в настроечном файле.

После создания файла резервной копии, выполняется вычисление ЭЦП для этого файла и создается трейлер безопасности, в который помещаются данные, ЭЦП и другая сопутствующая информация. Имя файла трейлера безопасности получается из имени подписываемого файла добавлением скобок и префикса SignBA:

Файл резервной копии: my_db_17_12_2014_63545

Файл трейлера безопасности: SignBA(my_db_17_12_2014_63545)

Восстановление хранилища сертификатов (файла БД) из резервной копии (с предварительной проверкой ЭЦП) выполняется путем запуска СПО КПА УЦ со специальным параметром командной строки «–restored», после которого указывается путь к файлу трейлера безопасности. Параметр и путь к файлу трейлера разделяются знаком «=»:

```
-restoredb=D:\CA\reservation\Day\SignBA(17_6_2011_54011360_Day)
```

В результате успешной проверки ЭЦП и восстановления хранилища из резервной копии в директории, прописанной в настроечном файле, появляется файл БД.

3.6. Завершение работы СПО

Для корректного завершения работы СПО КПА УЦ в консольное окно программы необходимо ввести команду «exit» и нажать клавишу Enter, после чего дождаться закрытия консольного окна.

Не рекомендуется завершать работу СПО КПА УЦ путем нажатия на кнопку закрытия в правом верхнем углу окна.

Не рекомендуется выключать или перезагружать КПА УЦ, не завершив корректно работу СПО.

4. СООБЩЕНИЯ ОПЕРАТОРУ

Так, при успешном запуске СПО КПА УЦ появляется надпись:

```
type command:
exit – exit
```

В случае ошибки запуска СПО КПА УЦ может появиться одно из следующих сообщений, за которым, последует детальное объяснение причины ошибки:

1) При отсутствии в рабочей директории СПО файлов (одного или нескольких) библиотеки динамической компоновки оператору выдается сообщение с указанием недостающей библиотеки (рис. 2). При появлении одного из предыдущих сообщений следует поместить отсутствующий файл в рабочую директорию приложения.

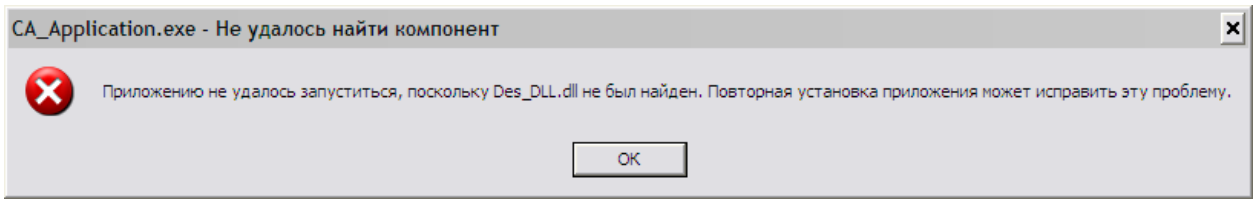

Рис. 2

2) Появление сообщения представленного на рис. 3 означает, что приложение не может подключиться к СУБД хранилища сертификатов. Следует посмотреть, запущена ли служба СУБД Firebird, и проверить значения параметров в секции [Database] файла настроек "settings.ini".

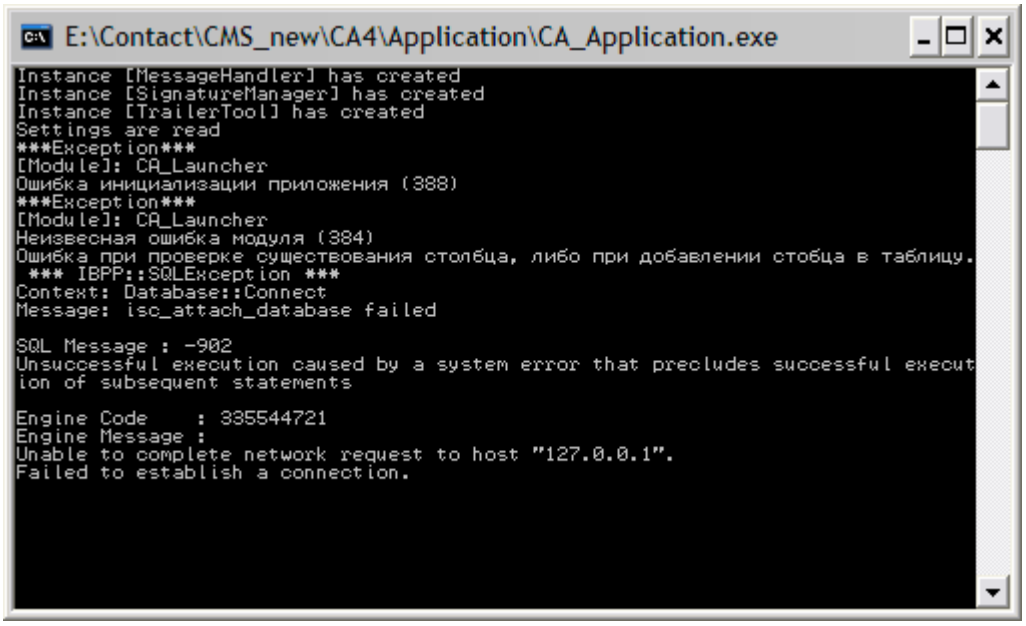

Рис. 3

3) Если в консольное окно СПО выводится сообщение, представленное на рис. 4, это означает, что предпринята попытка запуска второй копии СПО.

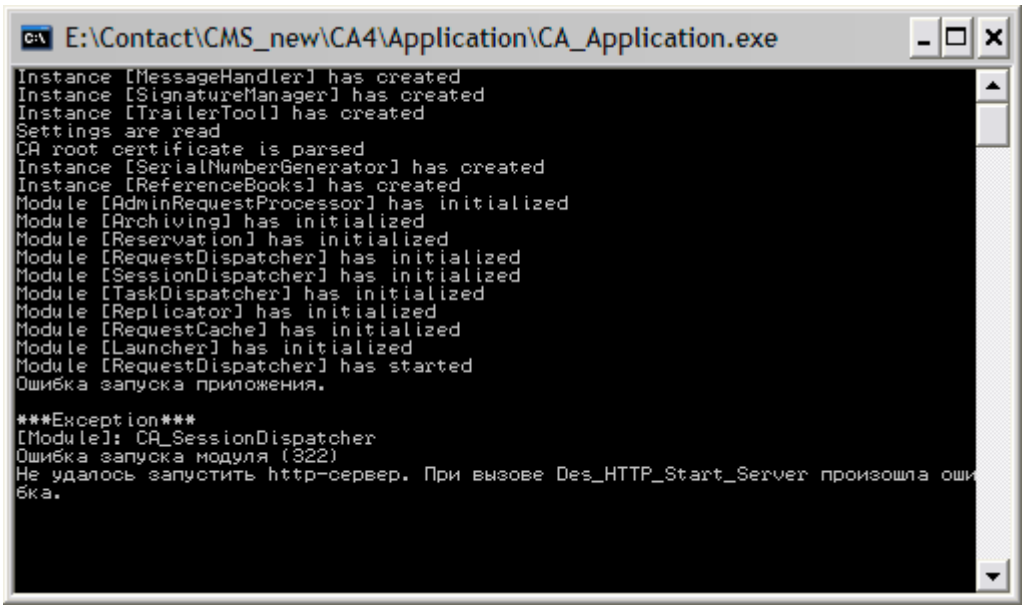

Рис. 4

4) "Ошибка инициализации приложения". Возможные причины возникновения данной ошибки – отсутствие (или неверное значение) параметра конкретного модуля в настроечном файле.

5) "Ошибка завершения приложения". При возникновении такого рода ошибки следует остановить приложение средствами ОС и отослать журнал работы приложения разработчику.

6) "Ошибка запуска приложения". При возникновении такого рода ошибки следует остановить приложение средствами ОС и отослать журнал работы приложения разработчику.

Приложение А

Пример файла настройки СПО

```
; параметры приложения: список запускаемых модулей (используется для отладки)
[Application]
Archiving=1
Reservation=1
RequestDispatcher=1
RequestSynchronizer=0
SessionDispatcher=1
TasksDispatcher=1
CertificationTester=0
;
;параметры справочников организационных единиц
[ReferenceBooks]
;директория из которой будут загружаться справочники
LoadFrom=".\ReferenceBooks\"
;интервал сохранения изменений (в секундах)
;если 0 - справочники сохраняются после каждой заявки с изменениями
SaveInterval=1000
;
; параметры модуля архивирования
[Archiving]
Year=2011
Month=08
Day=25
Hour=17
Period=5
BufferizationPath=".\archivation\bufferization\"
AfterExpireTermBeforeArchiving=9
;
; параметры хранилища архивов
[ArchiveStorage]
```

```
; тип хранилища
ArchiveType=Filesystem
; путь к хранилищу
ArchivesPath=".\archivation\storage\"
;
; параметры резервного копирования и восстановления БД на место текущей БД (данную секцию можно включать, если включена проверка на запуск КП)
[BackupRestore]
;параметр для включения модуля (1-включено, 0-выключено)
TurnOn = 0
;параметр для журналирования модуля (1-включено, 0-выключено)
Logging = 1
;путь к папке для хранения резервных копий БД(хранятся две последние копии)
PathForBackup = ".\Database\tempBackup"
;путь с именем для временного размещения старого файла БД
NewPuthForTempOldDB = ".\Database\tempOldDB.FBD"
;дата первого резервного копирования и восстановления
Year=2015
Month=05
Day=29
Hour=16
;период  в днях
Period=7
;
; параметры хранилища сертификатов
[Database]
; тип используемой СУБД
DbmsType="firebird"
; сетевой адрес хоста, на котором запущена СУБД
DbmsSrvAddr="127.0.0.1"
; имя пользователя СУБД
Username="sysdba"
; пароль пользователя СУБД
```

```
Password="masterkey"
; алиас БД или путь к файлу СУБД
DbPath=".\Database\SOURCEBUILD0v2.FDB"
; ключевые слова, допустимые в запросе
AllowedKeywords="SELECT, FROM, WHERE, AND, OR, SEARCH, SEAR_ID,
SEAR_SERNUM, SEAR_OID, SEAR_NICK, SEAR_LASTNAME, SEAR_FIRSTNAME,
SEAR_MIDDLENAME, SEAR_FULLNAME, SEAR_ORGANIZATION_NAME,
SEAR_ORGANIZATION_UNITNAME, SEAR_LOCALITY_NAME, SEAR_CERT_STARTTIME,
SEAR_CERT_ENDTIME, SEAR_KEY_STARTTIME, SEAR_KEY_ENDTIME,
SEAR_REVOCATION_STARTTIME, SEAR_REVOCATION_REASON, SEAR_KEY_USAGE,
CERTIFICATES, CERT_SEAR_ID, CERT_BUFFER, HISTORY, HIST_SEAR_ID,
HIST_SUSPENTION_STARTTIME, HIST_SUSPENTION_ENDTIME, CRL, CRL_SEAR_ID,
CRL_SERNUM, CRL_REASON, CRL_STARTTIME, ARCHIVE, ARCH_SEAR_ID,
ARCH_SERNUM, ARCH_OID, ARCH_DUMPING_TIME"
;
; параметры КП (CryptoService)
[CryptoService]
; сетевой адрес хоста, на котором запущен модуль КП
HostAddr="127.0.0.1"
; порт, на котором КП "ожидает" подключения
Port=49018
; таймаут (в секундах) чтения данных из сокета
SockRdTimeout=9000
; таймаут (в секундах) записи данных в сокет
SockWrTimeout=9000
; путь к .exe-файлу КП (если при запуске КПА УЦ КП не запущен, то он
запустится автоматически по этому пути)
Path = "e:\CryptoService\CryptoService_41.exe"
; временя через которое КПА УЦ получает состояние криптосервиса в
секундах(по умолчанию 10 секунд)
PeriodForStateCS = 120
;
[MessageHandler]
ApplicationName="Контакт КПА УЦ"
FileLogging=1
```

```
LogFile="CA_log.log"
Trace=1
TraceFile="CA_trace.log"
; журналирование функций, которые работают с БД (1-включено, 0 - отключено)
LogDataBase=1
; адрес хоста, на котором запущена служба журнала
HostAddr="200.0.0.201"
; порт, на хотором служба журнала ожидает подключения
Port=10200
; таймаут (в секундах) операций обмена
TimeOut=5
;
; параметры проверки подписи
[RequestProcessor]
Trace=1
; режимы обработки запросов: 1 - только заявки, 2 - только запросы, 3 - запросы и заявки
Mode=3
CheckSignCrlRequest=0
CheckSignOcspRequest=0
CheckSignAllHistoryRequest=0
CheckSignStatusRequest=0
CheckSignStatusByNickRequest=0
CheckSignListHistoryRequest=0
StoreCertificates=1
StoreCertificatesPath=".\.issued_certificates\"
; продолжительность действия личного ключа по умолчанию (если не указано в заявке), мес
DefaultPrivateKeyDuration = 24
; продолжительность действия сертификата открытого ключа по умолчанию (если не указано в заявке), мес
DefaultCertificationDuration = 24
;
```

```
; параметры удаленного управления
[RemoteControl]
; порт сервера аутентификации
Port=49000
; таймаут (в секундах) операций обмена по сокетам
TimeOut=1
; OID сертификата администратора системы (необходим для Des_Auth)
OID="8a4fa92e6825e6e6fb51afc72aa18bf545f7b2e46c7c703eef8204297df2f741"
; путь к личному ключу администратора системы
PrivateKeyPath=".\keys\Key_2014-12-17_09-49-17_8A4FA92E_Admin1.sck"
; пароль к личному ключу администратора системы
PrivateKeyPass="11111111"
; список OID'ов сертификатов пользователей, которые могут подключаться
удаленно
OID#1="07874c3176f6836b923a87d002d46aed01eae3dc8ad8a1f60f05fa0a1fee704
e"
;
; параметры диспетчера запросов
[RequestDispatcher]
Trace=1
; максимальный размер входной очереди (очередь запросов)
RequestQueueSize=64
; максимальный размер выходной очереди (очередь ответов)
ReplyQueueSize=32
;
; параметры синхрорнизатора запросов
[RequestSynchronizer]
Trace=0
; роль хоста
Role="Server"
; сетевой адрес резервного КПА УЦ
ServerAddr="127.0.0.1"
BufferizationFolder=".\synchronization\bufferization\"
NonSynchronizedFolder=".\synchronization\not synchronized\"
;
```

```
; параметры модуля, используемого для репликации изменений в хранилище сертификатов
[ReplicationSettings]
; Role="Distributor" (распространитель изменений) Role="Recipient" (получатель изменений), все остальные значения "отключают" работу модуля
Role="Distributor"
Trace=0
ExtraTrace=0
; журналирование почты синхронизации (1-включено, 0-выключено)
LoggingMailReplication = 1
; фильтр разделения сообщений
MessagesFilter=""
; таймаут (в секундах) обмена по сокетам
TimeOut=150
; порт сервера входящей почты
IncomingSrvPort=110
; сетевой адрес сервера входящей почты
IncomingSrvAddr="127.0.0.1"
; тип SSL (если используется) для доступа к серверу входящей почты
IncomingSslVersion="None"
; имя пользователя сервера входящей почты
IncomingSrvUser="ca_replication"
; пароль пользователя сервера входящей почты
IncomingSrvPass="ca"
; порт сервера исходящей почты
OutgoingSrvPort=25
; сетевой адрес сервера исходящей почты
OutgoingSrvAddr="127.0.0.1"
; тип SSL (если используется) для доступа к серверу исходящей почты
OutgoingSslVersion="None"
; имя пользователя сервера исходящей почты
OutgoingSrvUser="ca_replication"
; пароль пользователя исходящей почты
OutgoingSrvPass="ca"
```

```
; тип используемого прокси-сервера
ProxyType="None"
; период извлечения сообщений из почтового ящика
MailInterrogateTime=8192
; период чтения сообщений (необработанных) из временной директории
DirectoryScanTime=4096
; путь к директории для хранения временных файлов
TempPath=".\transport\replicator\"
; путь для хранения писем синхронизации, при обработке которых возникли ошибки
ErrorEmailPath =".\transport\ErrorReplicatorEmail\"
; адрес почтового ящика, в который будут поступать сообщения об изменении хранилища
RecipientAddress="ca_replication@contact"
; список адресов, по которым будет рассылаться сообщения об изменении хранилища
e-mail000="reg_replication@contact"
;
; параметры модуля резервирования
[Reservation]
ReservationPath=".\reservation\"
;
; список заданий резервирования
[ReservationTaskList]
Task1=Day|08/10/2014|1|1
Task2=Month|08/10/2014|30|1
Task3=Year|08/10/2014|356|1
Task4=Week|08/10/2014|7|1
;
; параметры сертификата
[CertificateInfo]
SN="11111511111111107da0000000000000001"
CertificatePath=".\certificates\Root11111511111111107da0000000000000001.cer"
PrivateKeyPath=".\keys\Root_11111511111111107da0000000000000001.sck"
```

```
PrivateKeyPass="11111111"
;
; параметры диспетчера сеансов
[SessionDispatcher]
Trace=1
; журналирование почты (1-включено, 0-выключено)
LoggingMail = 1
; флаг удаления писем с сервера
DeleteMessages=1
; фильтр разделения сообщений
MessagesFilter=""
; адрес e-mail удостоверяющего центра (используется в КП РЦ для
классификации входящих сообщений)
FromAddr="ca_requests@contact"
; таймаут (в секундах) обмена по сокетам
TimeOut=150
; порт сервера входящей почты
IncomingSrvPort=110
; сетевой адрес сервера входящей почты
IncomingSrvAddr="127.0.0.1"
; тип SSL (если используется) для доступа к серверу входящей почты
IncomingSslVersion="None"
; имя пользователя сервера входящей почты
IncomingUser="ca_requests"
; пароль пользователя сервера входящей почты
IncomingPass="ca"
; порт сервера исходящей почты
OutgoingSrvPort=25
; сетевой адрес сервера исходящей почты
OutgoingSrvAddr="127.0.0.1"
; тип SSL (если используется) для доступа к серверу исходящей почты
OutgoingSslVersion="None"
; имя пользователя сервера исходящей почты
OutgoingUser="ca_requests"
; пароль пользователя исходящей почты
```

```
OutgoingPass="ca"
; тип используемого прокси сервера
ProxyType="None"
; порт http-сервера
Port=4080
; период чтения данных из защищенного канала
CtrlChanlInterrogateTime=128
; Период извлечения сообщений из очереди http-запросов
HttpInterrogateTime=1024
; период извлечения сообщений из почтового ящика
MailInterrogateTime=8192
; максимально количество потоков для обработки http-соединений
ThreadCount=64
; путь к директории для хранения временных файлов
TempPath=".\transport\temp\"
; интервал между попытками чтения данных из защищенного канала
SecChannelRdInterval=3000
; интервал между попытками записи данных в защищенный канал
SecChannelWrInterval=3000
; количество попыток записи данных в защищенный канал
SecChannelWrAttempt=7
;
[Crl]
; порядковый номер распространителя СОС (напр., для КПА УЦ - 0, для
; Реестра1 - 1 и т.д.; максимальное значение = 255)
CrlIssuerNumber = 0
;период выпуска СОС (в минутах)
PeriodOfIssueCrl = 3600
;
; список сертификатов КП РЦ, от которых можно обрабатывать заявки
[TrustedCertificates]
OID#1="aac21603cae2c95aa5ff69470db8112c47c62a24f6b9118105a1b101df8a6a5
0"
```

Приложение Б

Выпуск корневого сертификата

Приложение «SpecializedCertIssuing.exe» предназначено для генерации корневого личного ключа и формирования корневого самоподписанного сертификата парного ему открытого ключа и помещения их в ПАК «Барьер».

Примечание. ПАК «Барьер» поддерживает хранение файлов личного ключа и СОК размером не больше чем по 3 Кбайта.

Ключевая пара генерируется по СТБ 34.101.45 с уровнем криптостойкости 128. Сертификат открытого ключа формируется в соответствии с СТБ 34.101.19.

Б.1. Настройка приложения

Настройка приложения «SpecializedCertIssuing.exe» осуществляется путем редактирования в текстовом редакторе файла «SpecCertIssuingSettings.xml», который расположен в рабочей директории КПА УЦ в папке «SpecializedCertIssuing» и имеет следующий вид:

```
<?xml version="1.0" encoding="windows-1251"?>
<SpecCertIssuingSettings>
     <CryptoServiceAbsolutePath>
          c:\CONTACT\Applications\CryptoService\
     </CryptoServiceAbsolutePath>
</SpecCertIssuingSettings>
```

В теге `<CryptoServiceAbsolutePath>` необходимо указать абсолютный путь к рабочей директории КП СОБ.

Б.2. Запуск приложения

Запуск приложения осуществляется непосредственным запуском исполняемого файла «SpecializedCertIssuing.exe» из рабочей директории КПА УЦ из папки «SpecializedCertIssuing».

При возникновении ошибок при запуске приложения на экране отобразятся диалоговые окна, сообщающие об ошибке (рисунки 5-7).

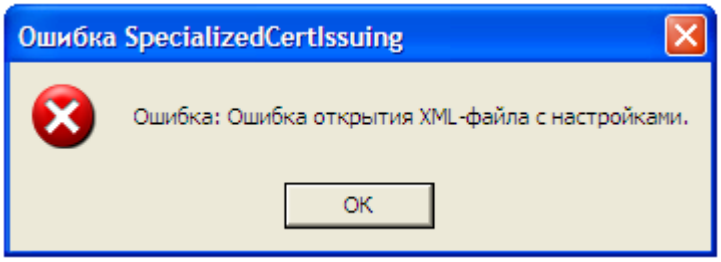

Рисунок 5

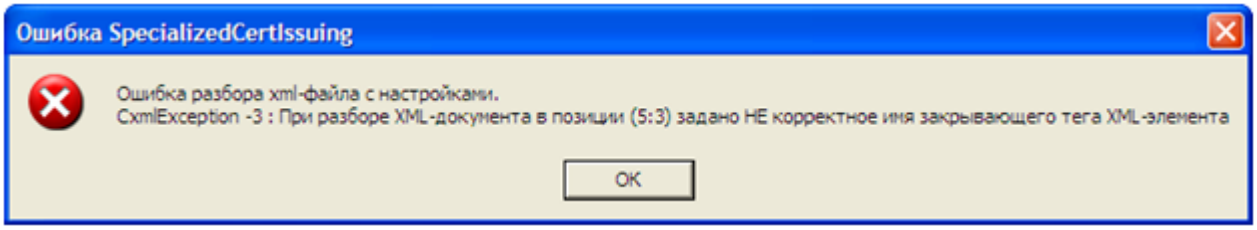

Рисунок 6

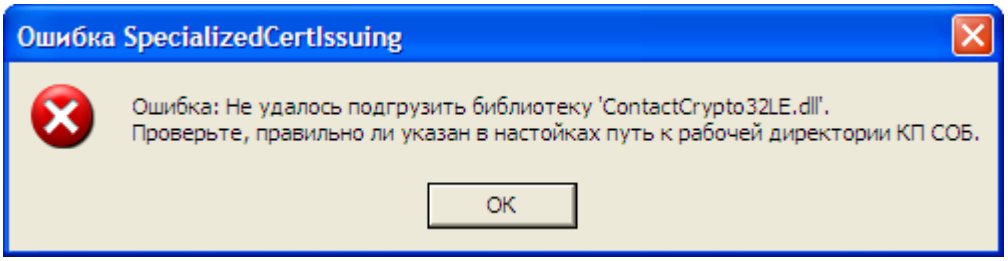

Рисунок 7

В случае успешного запуска отобразится главное окно приложения, представленное на рисунке 8.

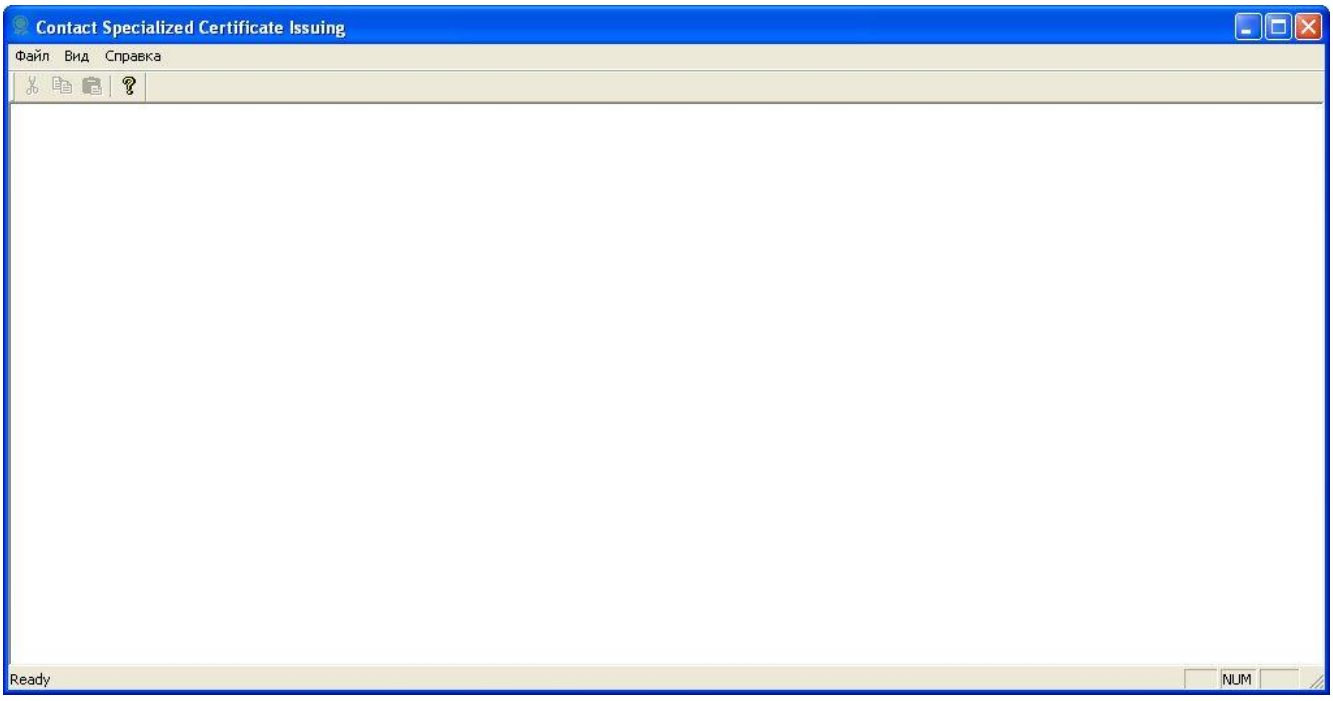

Рисунок 8

Б.3. Работа в приложении

Для того чтобы сгенерировать личный ключ и сформировать сертификат парного ему открытого ключа необходимо задать параметры нового СОК и личного ключа путем создания xml-файла, имеющего следующую структуру:

```
<?xml version="1.0" encoding="windows-1251"?>
<RootCertificateInfo>
     <SerialNumber Value="436F6E74616374337E030000000000000001"/>
     <NameAttributes>
          <CommonName OId="2.5.4.3" Value="УЦ для тестирования"/>
          <Country OId="2.5.4.6" Value="BY"/>
          <City OId="2.5.4.7" Value="г.Минск"/>
          <StreetAddress OId="2.5.4.9" Value="ул. Энгельса, д.7"/>
          <Organization OId="2.5.4.10" Value="ЗАО 'НТЦ Контакт'"/>
     </NameAttributes>
     <CertificateDuration Unit="месяц" Value="120"/>
     <PrivateKeyDuration  Unit="месяц" Value="119"/>
     <KeyUsageFlags      CRLsigning="True"      OCSPsigning="True"
KeyAgreement="True" KeyEncipherment="True"/>
     <CertificatesFolder Value=".\certificates\"/>
     <PrivateKeyPassword Value="11111111"/>
     <PrivateKeysFolder Value=".\private_keys\"/>
     <!-- <Barrier TMcardId="0011223344556677"/> -->
</RootCertificateInfo>
```

В атрибуте `Value` тега `SerialNumber` указывается серийный номер нового сертификата. Формат серийного номера следующий:

`xxxxxxxxxxxxxxxxYYYMccccccccccccccc`,

где `xxxxxxxxxxxxxxxx` – 16 hex-цифр, содержат уникальное обозначение организации. Только есть одна особенность: старшая шестнадцатеричная цифра (она подчеркнута) серийного номера должна быть больше 0 и меньше 8, это связано с особенностями кодирования типа Integer в ASN1.

`YYY` – 3 hex-цифры, содержат значение года выпуска (например, $7DF_{16} = 2015_{10}$),

`M` – 1 hex-цифра, содержит значение месяца выпуска,

`ccccccccccccccc` – счетчик сертификатов в hex-представлении, для корневого, как правило, равен 0000000000000001. Количество шестнадцатеричных цифр счётчика должно

быть чётным и не превышать 20.

Тег `NameAttributes` содержит параметры секции Subject (а так как сертификат будет самоподписанным, то и секции Issuer). Помимо тегов предложенных по умолчанию, можно добавлять свои, но их формат должен быть аналогичен предложенным: обязательно должны присутствовать атрибуты `OId` и `Value`.

В атрибуте `Unit` тега `CertificateDuration` указывается единица измерения продолжительности действия корневого сертификата. Допустимые значения – «год» либо «месяц». В атрибуте `Value` тега `CertificateDuration` указывается продолжительность действия корневого сертификата в указанных единицах. Период действия сертификата будет установлен следующим образом: начало = время выпуска сертификата, окончание = начало + `CertificateDuration`.

В атрибуте `Unit` тега `PrivateKeyDuration` указывается единица измерения продолжительности действия личного ключа. Допустимые значения – «год» либо «месяц». В атрибуте `Value` тега `PrivateKeyDuration` указывается продолжительность действия личного ключа в указанных единицах. Период действия рассчитывается аналогично периоду действия сертификата. Если данный тег отсутствует, то период действия личного ключа задается равным периоду действия сертификата.

Атрибуты тега `KeyUsageFlags` задают параметры использования ключа. Атрибуты `CRLsigning`, `KeyAgreement` и `KeyEncipherment` со значением `True` устанавливают в расширении KeyUsage (2.5.29.15) биты CRLSign, keyAgreement и keyEncipherment (см. СТБ 34.101.19 п. 6.2.1.3) соответственно в единицу. Биты digitalSignature, nonRepudiation и keyCertSign будут установлены в единицу по умолчанию без возможности изменения. Значение `True` в атрибуте `OCSPsigning` добавит в сертификат расширение ExtKeyUsage (2.5.29.37) с ОИД’ом id-kp-OCSPSigning в значении расширения (см СТБ 34.101.19 п. 6.2.1.12).

В атрибуте `Value` тега `CertificatesFolder` указывается путь, куда сохранится свежевыпущенный корневой сертификат. Допускается относительный путь (считается от exe-файла приложения) или абсолютный путь.

В атрибуте `Value` тега `PrivateKeyPassword` задается пароль к новому личному ключу парному корневому сертификату. Допустима длина пароля не менее 8 символов.

В атрибуте `Value` тега `PrivateKeysFolder` указывается путь, куда сохранится сгенерированный личный ключ, парный корневому сертификату. Допускается относительный путь (считается от exe-файла приложения) или абсолютный путь.

В атрибуте `TMcardId` тега `Barrier` указывается идентификатор ТМ-карты администратора КПА УЦ. Если тег `Barrier` присутствует в настроечном файле, то

сформированные СОК и личный ключ поместятся в память ПАК «Барьер».

После создания файла с информацией о сертификате, файл нужно сохранить в файловой системе с расширением «.xml».

Чтобы сформировать самоподписанный СОК и личный ключ необходимо в главном окне приложения выбрать пункт «Выпустить коневой самоподписанный СОК» из меню «Файл» (рисунок 9).

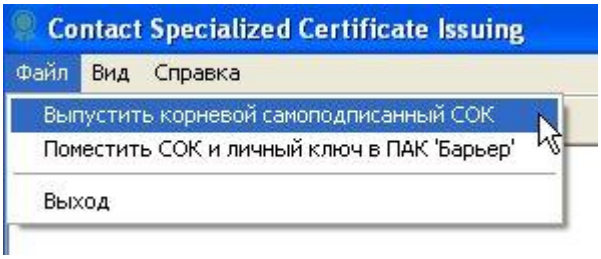

Рисунок 9

Затем в окне выбора файла (рисунок 10) выбрать настроечный файл, содержащий информацию о выпускаемом СОК.

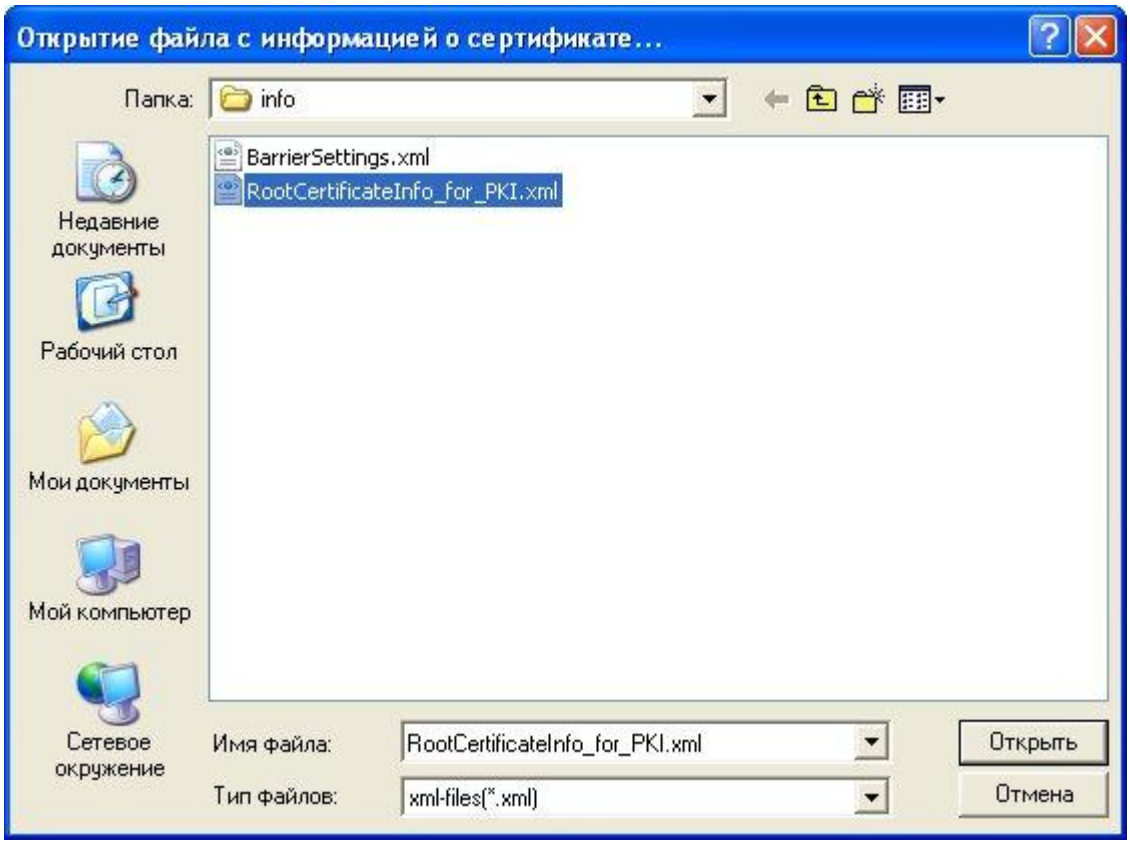

Рисунок 10

В случае успешного формирования СОК на экране отобразится соответствующее сообщение (рисунок 11).

Рисунок 11

Если в настроечном файле был указан идентификатор ТМ-карты администратора КПА УЦ, то дополнительно будет выведено сообщение о помещении СОК в ПАК «Барьер» (рисунок 12).

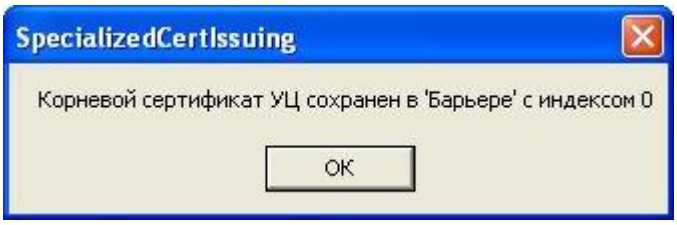

Рисунок 12

Также на экран выведется сообщение о сохранении файла личного ключа (рисунок 13).

Рисунок 13

Если в настроечном файле был указан идентификатор ТМ-карты администратора КПА УЦ, то дополнительно будет выведено сообщение о помещении личного ключа в ПАК «Барьер» (рисунок 14).

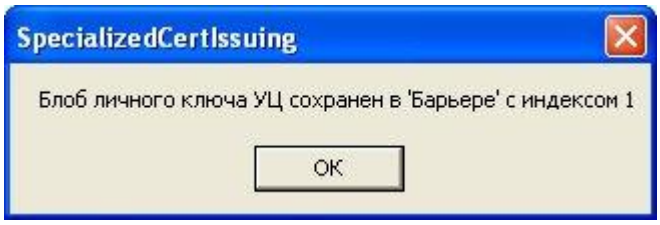

Рисунок 14

Для того чтобы записать личный ключ и СОК в память ПАК «Барьер» необходимо создать xml-файл со следующей структурой:

```
<?xml version="1.0" encoding="windows-1251"?>
<PutCertificateAndPrivKeyIntoBarier>
     <Barrier TMcardId="0011223344556677"/>
</PutCertificateAndPrivKeyIntoBarier>
```

В атрибуте `TMcardId` тега `Barrier` указывается идентификатор ТМ-карты администратора КПА УЦ.

После создания файла с информацией о ПАК «Барьер», файл нужно сохранить в файловой системе с расширением «.xml».

Затем необходимо выбрать пункт «Поместить СОК и личный ключ в ПАК ‘Барьер’» из меню «Файл» (рисунок 15).

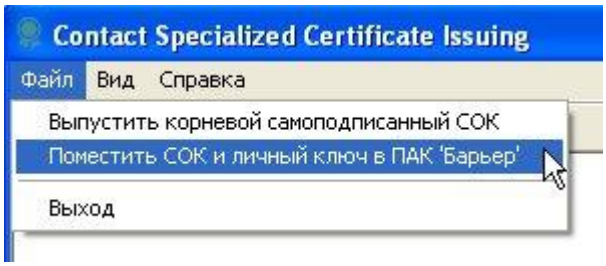

Рисунок 15

Затем в окне выбора файла (рисунок 16) выбрать настроечный файл, содержащий идентификатор ТМ-карты администратора КПА УЦ.

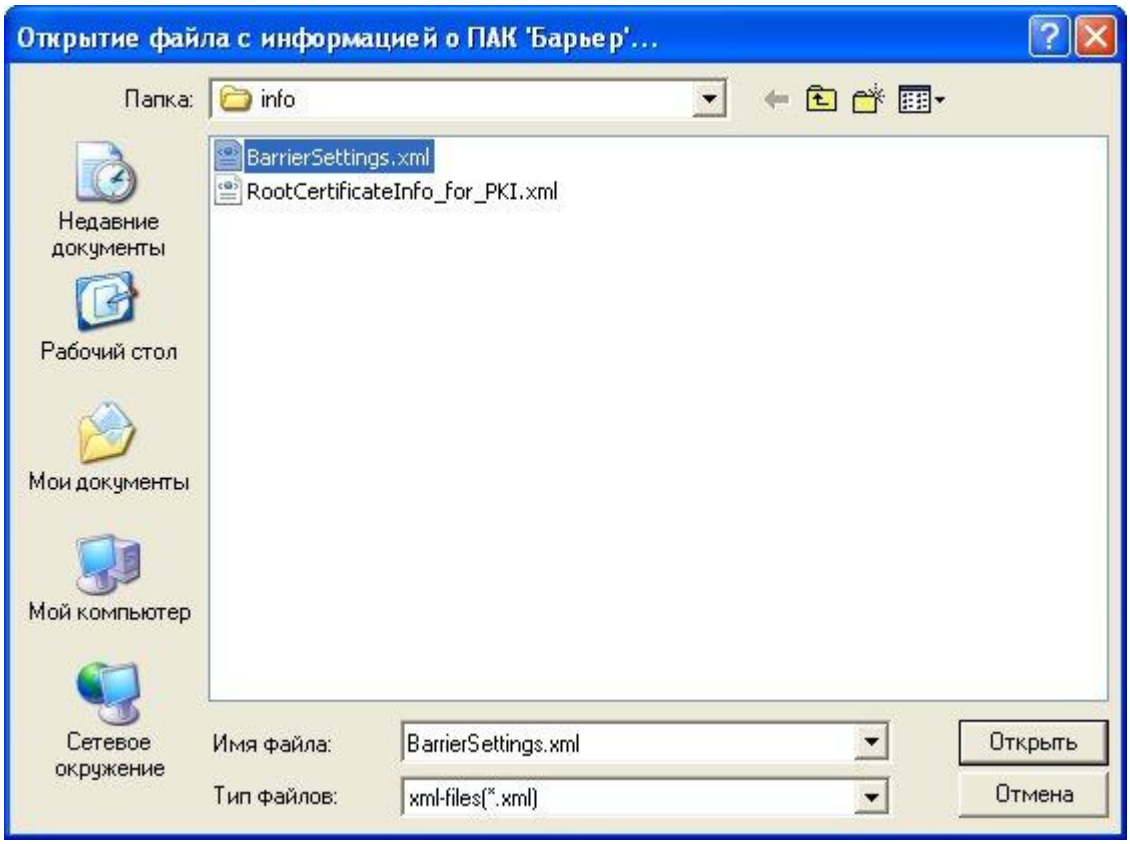

Рисунок 16

Далее последовательно в окнах выбора файла (рисунки 17, 18) выбрать файл СОК и файл личного ключа.

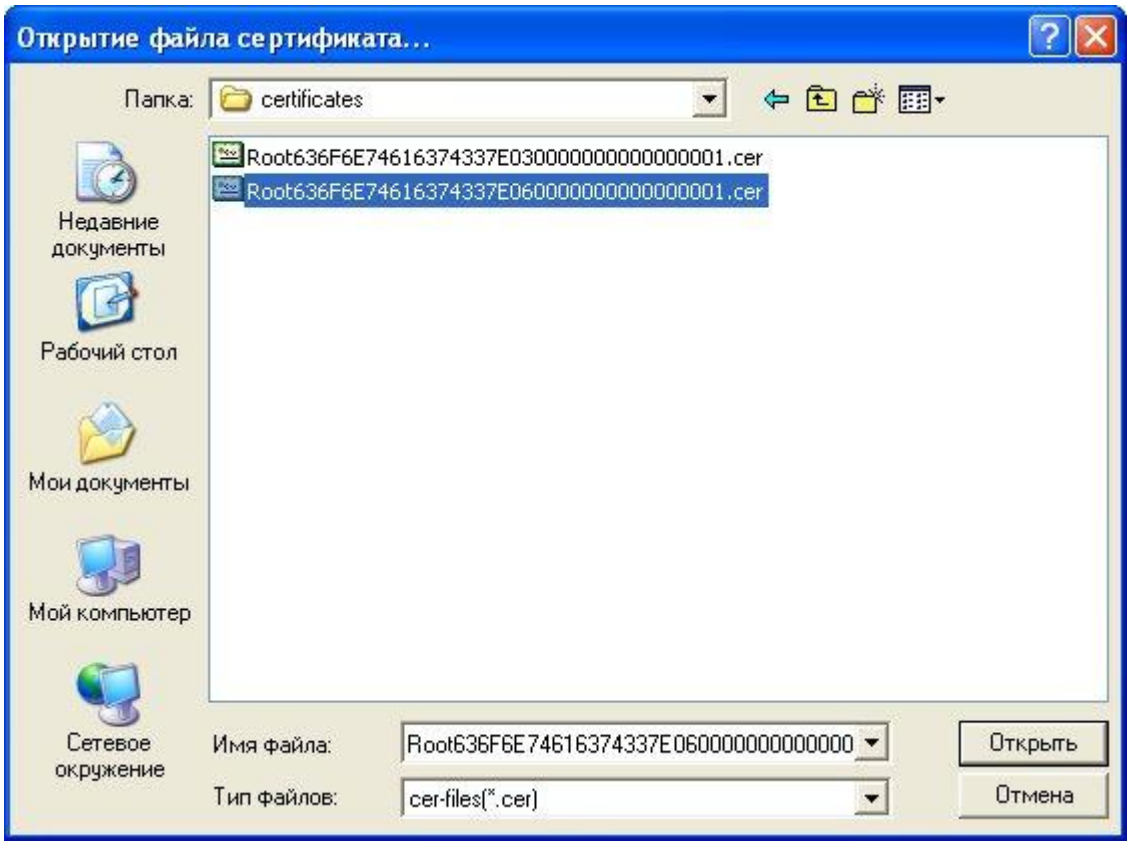

Рисунок 17

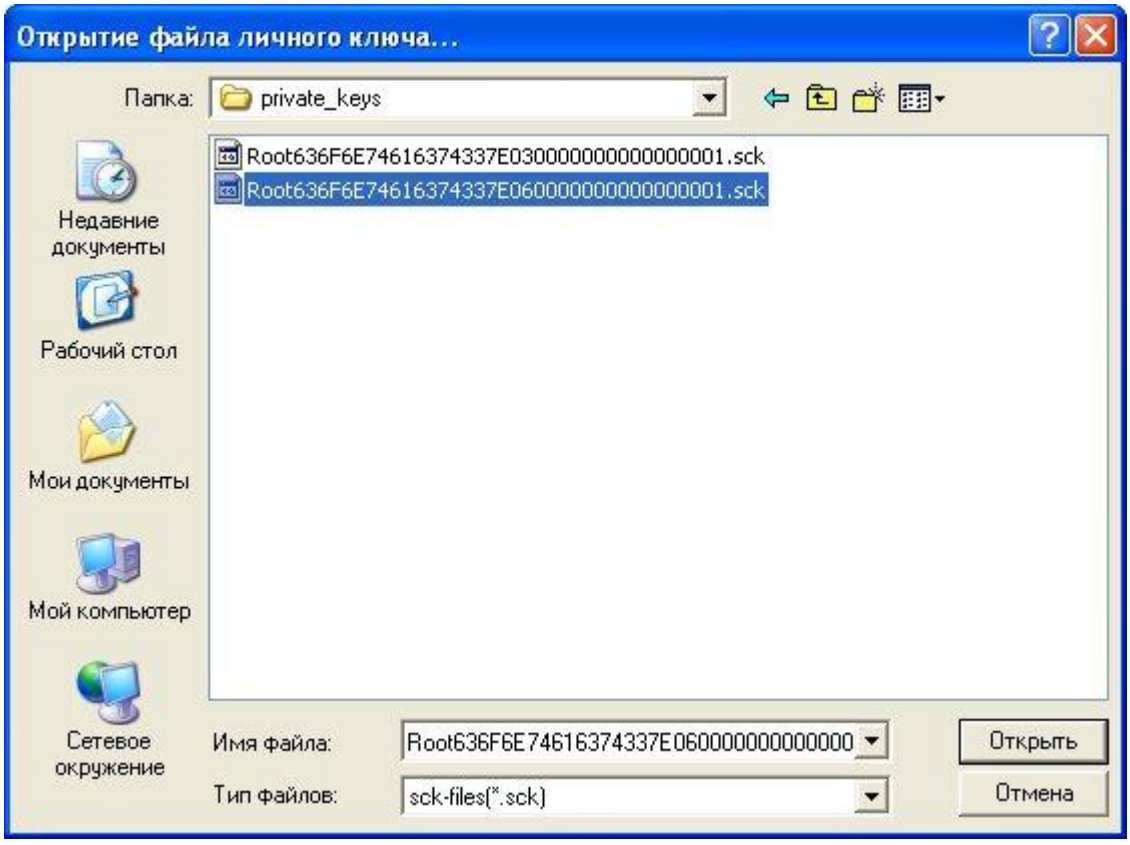

Рисунок 18

После успешного помещения СОК и личного ключа в память ПАК «Барьер» на экран выведутся соответствующие сообщения (рисунки 18, 19).

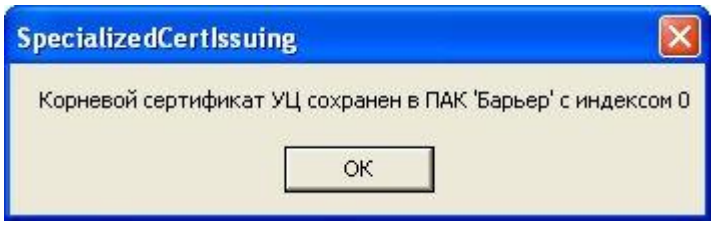

Рисунок 18

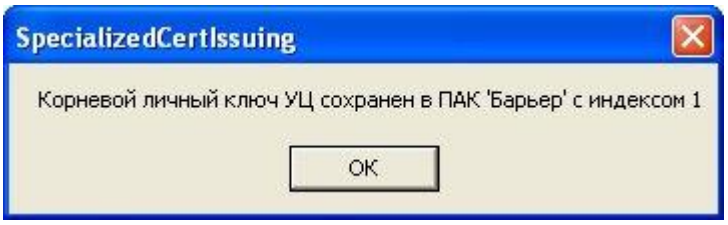

Рисунок 19

Б.4. Завершение работы приложения

Для завершения работы приложения «SpecializedCertIssuing.exe» необходимо выбрать пункт «Выход» из меню «Файл» (рисунок 20).

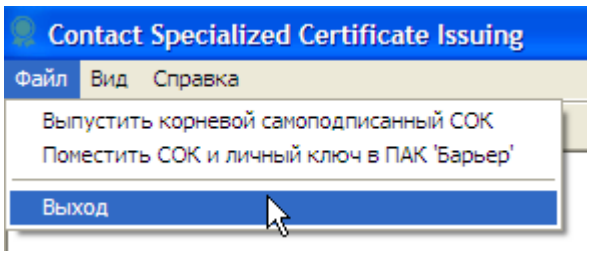

Рисунок 20

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
НСД	– несанкционированный доступ
ОЗУ	– оперативное запоминающее устройство
ОК	– открытый ключ
ОС	– операционная система
ПАК «Барьер»	– Комплекс программно-аппаратный защиты ПЭВМ от несанкционированного доступа «Барьер» СЮИК.467458.001
ПЗУ	– постоянное запоминающее устройство
ПО	– программное обеспечение
ПЭВМ	– персональная электронно-вычислительная машина
СОК	– сертификат открытого ключа
СОС	– список отозванных сертификатов
СПО	– Специальное программное обеспечение BY.СЮИК.00314-05
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					