УТВЕРЖДЕН

BY.СЮИК.00314-06 34 01-ЛУ

ПОДСИСТЕМА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
КОМПЛЕКС ПРОГРАММНЫЙ
УДОСТОВЕРЯЮЩИЙ ЦЕНТР

Руководство оператора

BY.СЮИК.00314-06 34 01

Листов 51

2017

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

№ изм.	Подп.	Дата

Литера O_1

АННОТАЦИЯ

В настоящем документе описывается последовательность действий по запуску программного обеспечения «Подсистемы криптографической защиты информации. Комплекса программного Удостоверяющий центр» и порядок взаимодействия администратора с данным программным обеспечением.

Для понимания изложенного в документе материала необходимы навыки администрирования операционной системы семейства Microsoft Windows™ XP (x86), Server 2003 (x86), 7 (x86, x64), 10, а также знание основ криптографии и нормативных правовых актов в области технического нормирования и стандартизации – СТБ 1176.1-99, СТБ 1176.2-99, СТБ 34.101.17-2012, СТБ 34.101.19-2012, СТБ 34.101.26-2012, СТБ 34.101.31-2011, СТБ 34.101.45-2013, СТБ 34.101.47-2017, СТБ 34.101.49-2012.

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 программный Удостоверяющий центр» BY.СЮИК.00314-06 (далее – КП УЦ) входит в состав подсистемы криптографической защиты информации (далее - ПС КЗИ).

Программное обеспечение (далее – ПО) КП 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.

КП УЦ обеспечивает реализацию функций:

1) выпуска СОК;

2) отзыва СОК;

3) аутентификации администратора КП 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 КП УЦ;

7) выпуска СОК для «Подсистемы криптографической защиты информации. Комплекса программного Регистрационный центр» BY.СЮИК.00363-03 (далее – КП РЦ);

8) импорта СОК и СОС других КП 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 КП УЦ;

18) ведения журналов аудита;

19) обеспечения оперативной проверки статуса СОК по протоколу OCSP;

20) обеспечения работоспособности с применением «Комплекса программно-аппаратного защиты ПЭВМ от несанкционированного доступа «Барьер» СЮИК.467458.001 (далее - ПАК «Барьер»).

Функции криптографических преобразований в КП УЦ выполняются, входящей в его

состав «Подсистемой криптографической защиты информации. Комплексом программным Средств обеспечения безопасности» РБ.СЮИК.00364-03 (далее – КП СОБ).

С КП УЦ взаимодействуют три категории пользователей:

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

В документе описаны действия администратора КП УЦ. Действия других пользователей описаны в документах «Подсистема криптографической защиты информации. Комплекс программный Регистрационный центр. Руководство оператора» BY.СЮИК.00363-03 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

КП УЦ работает под управлением ОС Microsoft Windows™ XP (x86), Server 2003 (x86), 7 (x86, x64), 10.

Для работы ПО необходима ПЭВМ, укомплектованная устройством CD-ROM и 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 ПО включает в себя:

- любую из ОС Microsoft Windows™ XP (x86), Server 2003 (x86), 7 (x86, x64), 10;
- 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. Настройка среды

Настройкой среды занимается оператор в роли «Администратор».

Настройка среды может включать в себя:

- настройку даты и времени, выбор часового пояса и синхронизацию системного времени с сервером времени;
- настройку переменных среды окружения;
- настройку сетевых параметров;
- настройку параметров безопасности среды.

3.2. Инсталляция КП УЦ

КП УЦ находится на поставляемом установочном компакт-диске.

Инсталляция КП УЦ осуществляется путем выполнения следующих действий:

1. Установить КП СОБ (папка с именем «CryptoService») с поставляемого диска с КП УЦ в соответствии с п. 3 документа «Подсистема криптографической защиты информации. Комплекс программный Средств обеспечения безопасности. Руководство оператора» РБ.СЮИК.00364-03 34 01.

2. Скопировать папку «CA» с установочного диска в рабочую директорию КП СОБ.

Для корректной работы КП УЦ в его рабочей директории должны находиться папки, описанные в таблице 1.

Таблица 1 – Перечень папок, необходимых для корректной работы КП УЦ

Наименование папки	Описание применения
.issued_certificates	Папка для внутреннего использования. В данной папке по умолчанию сохраняются все выпущенные СОК.
archivation\buffering	Папка для внутреннего использования. В данную папку сохраняются промежуточные данные при архивировании БД. Задается в настроечных параметрах.
archivation\storage	Папка, в которую по умолчанию сохраняются архивные данные. Задается в настроечных параметрах.
certificates	Папка, в которую по умолчанию помещается корневой СОК. Задается в настроечных параметрах.
crl	Папка для хранения файлов СОС. Задается в настроечных параметрах.
database	Папка, в которую по умолчанию помещается файл БД. Задается в настроечных параметрах.
keys	Папка, в которую по умолчанию помещается корневой личный ключ. Задается в настроечных параметрах.
ReferenceBooks	Папка для внутреннего использования, из которой по умолчанию загружаются справочники. Задается в настроечных параметрах.
reservation	Папка, в которую по умолчанию сохраняются резервные копии БД. Задается в настроечных параметрах.
transport\temp	Папка для внутреннего использования, в которую сохраняются электронные письма, которые забираются из почтового ящика и еще не прошли обработку.

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

Таблица 2 – Типы файлов, используемых и создаваемых при работе КП РЦ

Расширение файла	Тип файла
.cer	Файлы СОК.
.crl	Файлы СОС.
.fdb	Файлы БД.
.sck	Файлы личного ключа.
.rbf	Файлы справочников.
.eml	Файлы электронных писем.
.log	Файлы локальных журналов.
.ini	Файлы настроек.
Без расширения	Файлы архивов, резервных копий.

Для корректной работы КП УЦ могут понадобиться некоторые из нижеперечисленных системных библиотек, которые необходимо скопировать с поставляемого производителем диска из папки «Вспомогательное окружение\system_dlls» в рабочую директорию КП УЦ либо в системную папку по пути «%SystemRoot%\system32» (путь определен в переменной окружения «Path») без замены существующих:

- zlib1.dll;
- msvcr71.dll;
- libeay32.dll (23.03.2007);
- ssleay32.dll (23.03.2007).

Для корректной работы КП УЦ необходима установленная и запущенная служба СУБД Firebird. Рекомендуется использовать службу версии 2.5.2. Инсталляционный файл находится на поставляемом производителем диске по пути «Вспомогательное окружение\Firebird 2.5.2 (win32)\Firebird-2.5.2.26540_0_Win32.exe». Инструкция по инсталляции службы СУБД Firebird описана в приложении А.

3.3. Настройка КП УЦ

Так как ПО работает совместно с входящим в его состав КП СОБ, то настройка ПО включает в себя настройку КП СОБ и настройку собственно КП УЦ. Настройка КП СОБ подробно описана в п.п. 5, 7 документа «Подсистема криптографической защиты информации. Комплекс программный Средств обеспечения безопасности. Руководство оператора» РБ.СЮИК.00364-03 34 01.

КП 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 клиентских КП СОБ и проходят предварительную проверку в КП РЦ. Для повышения безопасности ПС КЗИ в КП 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 КП УЦ упакованными в SOAP-конверты. Администрирование КП УЦ может осуществляться в ручном режиме путем редактирования файла настроек («settings.ini») в рабочей директории КП УЦ (CA), а также посредством консоли с графическим интерфейсом – отдельного программного модуля, который обменивается данными с КП 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.

Пример файла настроек КП УЦ «settings.ini» представлен в приложении Б.

3.3.1. Настройка параметров модуля архивирования

Для включения или отключения модуля архивирования используется параметр `Archiving` в секции `[Application]` настроечного файла. Если параметр выставлен в 1, то модуль включен, если в 0 - отключен.

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 сохраняться файлы архивов; `AfterExpireTermBeforeArchiving` – период времени в месяцах, указывает, сколько сертификат после прекращения действия будет находиться в основном хранилище до перемещения его в архив.

В секции `[ArchiveStorage]` настраиваются параметры хранилища архивов:

- тип хранилища (`ArchiveType`), единственное допустимое значение для этого параметра – «`Filesystem`»;
- относительный путь к хранилищу (`ArchivesPath`).

3.3.2. Настройка параметров резервного копирования

Для включения или отключения модуля резервного копирования используется параметр `Reservation` в секции `[Application]` настроечного файла. Если параметр выставлен в 1, то модуль включен, если в 0 - отключен.

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.

3.3.3. Настройка параметров хранилища сертификатов

Основные параметры секции `[Database]`:

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

3.3.4. Настройка параметров КП СОБ

Без КП СОБ работа КП УЦ 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 ПО проверяет запущен ли КП СОБ. Если это не выполнено, КП УЦ 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`.

3.3.5. 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]`. Основные параметры:

- `DeleteMessages` – флаг удаления писем с сервера;
- `FromAddr` – адрес собственного электронного почтового ящика КП УЦ, используется в КП РЦ для классификации входящих сообщений;
- `TimeOut` – таймаут обмена по сокетам в секундах;
- `IncomingSrvPort` – порт сервера входящей почты;
- `IncomingSrvAddr` – сетевой адрес сервера входящей почты;
- `IncomingSslVersion` – тип SSL для доступа к серверу входящей почты, если не используется, то необходимо установить значение параметра «`None`»;
- `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 для доступа к серверу исходящей почты, если не используется, то необходимо установить значение параметра «`None`»;
- `OutgoingUser` – имя пользователя сервера исходящей почты;
- `OutgoingPass` – пароль пользователя исходящей почты;
- `ProxyType` – тип используемого прокси сервера;
- `Port` – порт http-сервера;
- `CtrlChanlInterrogateTime` - период чтения данных из защищенного канала в миллисекундах, если установлено значение 0, то удаленное подключение по

защищенному каналу запрещено;

- `HttpInterrogateTime` - период извлечения сообщений из очереди http-запросов в миллисекундах;
- `MailInterrogateTime` - период извлечения сообщений из почтового ящика в миллисекндах;
- `ThreadCount` - максимально количество потоков для обработки http-соединений;
- `TempPath` - путь к директории для хранения временных файлов.

3.3.6. Настройка параметров корневого сертификата и личного ключа

Для работы КП УЦ необходимо настроить параметры корневого СОК и его личного ключа. Они находятся в секции `[CertificateInfo]`.

Серийный номер сертификата указывается в параметре `SN`.

Путь к корневому СОК задается в параметре `CertificatePath`. Если СОК находится в файловой системе, то допустимо указывать как абсолютный, так и относительный путь. Если корневой СОК хранится в ПАК «Барьер», то путь к нему задается следующим образом:

`bar:\cert\N?tmcardid=XXXXXXXXXXXXXXXX,`

где bar:\ - специальное обозначение ПАК «Барьер»,

cert – идентификатор области для хранения данных,

N – номер области для хранения данных,

XXXXXXXXXXXXXXXX – уникальный идентификатор ТМ-карты, представлен в виде строки из шестнадцати HEX-символов.

Настройками личного ключа КП УЦ являются путь к нему (параметр `PrivateKeyPath`) и пароль (параметр `PrivateKeyPass`).

Если личный ключ находится в файловой системе, то допустимо указывать как абсолютный, так и относительный путь. Если корневой личный ключ хранится в ПАК «Барьер», то путь к нему задается следующим образом:

`bar:\key\N?tmcardid=XXXXXXXXXXXXXXXX,`

где bar:\ - специальное обозначение ПАК «Барьер»,

key – идентификатор области для хранения данных,

N – номер области для хранения данных,

XXXXXXXXXXXXXXXX – уникальный идентификатор ТМ-карты, представлен в виде строки из шестнадцати HEX-символов.

Если не задавать значение параметра `PrivateKeyPass`, то после запуска КП УЦ запросит ввод пароля к личному ключу. Вводимые символы при этом отображаться не будут.

3.3.7. 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 КП УЦ) и `Recipient` – получатель изменений (для Реестров). Также в этой секции представлены транспортные настройки для репликации:

- `IncomingSrvPort` – порт сервера входящей почты;
- `IncomingSrvAddr` – сетевой адрес сервера входящей почты;
- `IncomingSslVersion` – тип SSL для доступа к серверу входящей почты, если не используется, то необходимо установить значение параметра «`None`»;
- `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, если не используется, то необходимо установить значение параметра «`None`»;
- `OutgoingSrvUser` – имя пользователя сервера исходящей почты;
- `OutgoingSrvPass` – пароль пользователя исходящей почты;
- `ProxyType` – тип используемого прокси-сервера, если не используется, то необходимо установить значение параметра «`None`»;
- `MailInterrogateTime` - период извлечения сообщений из почтового ящика в миллисекундах;
- `RecipientAddress` – адрес почтового ящика, в который будут поступать сообщения об изменении хранилища;
- `e-mailNNN` – список адресов, по которым будет рассылаться сообщения об изменении хранилища; для Реестров этот список пуст. NNN – порядковый номер получателя репликаций.

3.3.8. Настройка выпуска списков отозванных сертификатов

Секция `[Crl]` содержит два параметра:

- `CrlIssuerNumber` – порядковый номер распространителя СОС. Например, для основного КП УЦ задается параметр равный 0, для одного Реестра – 1 и т.д. Максимальное допустимое значение равно 255.

- `PeriodOfIssueCrl` - период автоматического выпуска списка отозванных сертификатов в минутах. Максимальное допустимое значение равно 35700 минут. Списки отозванных сертификатов сохраняются в виде файлов с расширением «.crl» в рабочей директории КП УЦ по пути «crl\archive\».

3.3.9. Настройка доверенных сертификатов администраторов КП РЦ

В секции `[TrustedCertificates]` в параметрах `OID#N` перечисляются идентификаторы открытых ключей доверенных сертификатов администраторов КП РЦ, от которых можно обрабатывать заявки. N – порядковый номер очередного идентификатора, $0 < N < 256$.

3.4. Подготовка к запуску КП УЦ

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

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

СОК должны находиться в хранилище СОК (БД) КП УЦ, и в локальном хранилище КП СОБ.

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

- Des_DLL.dll,
- LogClientSocket.dll,
- ContactDevice.dll,
- BarPciKeys.dll,
- Ailurus_HTTP_api.dll,
- Des_Auth.dll.

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

Перед запуском КП УЦ необходимо убедиться в том, что служба СУБД Firebird установлена и запущена.

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

3.5. Запуск КП УЦ

Запуск КП УЦ производится непосредственным запуском исполняемого файла «CA_Application.exe» из места расположения ПО на жестком диске. Консольное окно КП УЦ представлено на рис. 1.

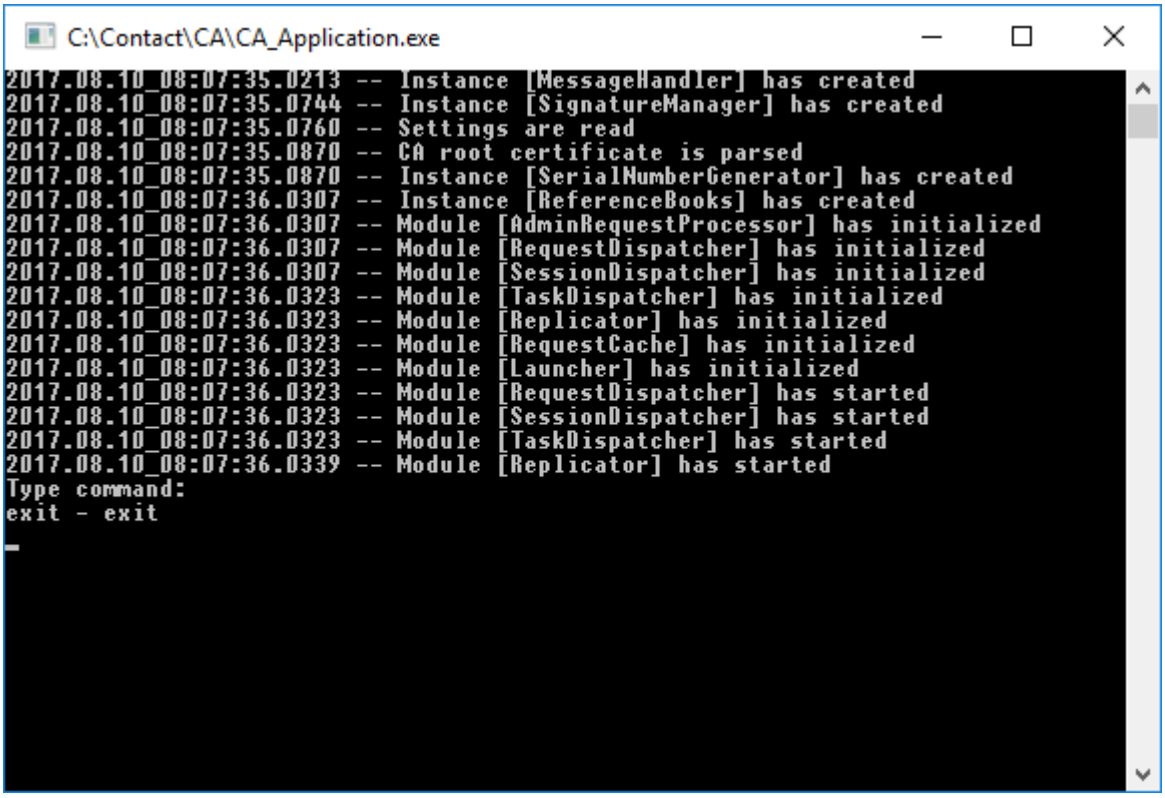

Рис. 1

Если в настроечном файле не был задан пароль к личному ключу, то во время инициализации модулей КП УЦ в консольном окне будет запрошен пароль (рис. 2).

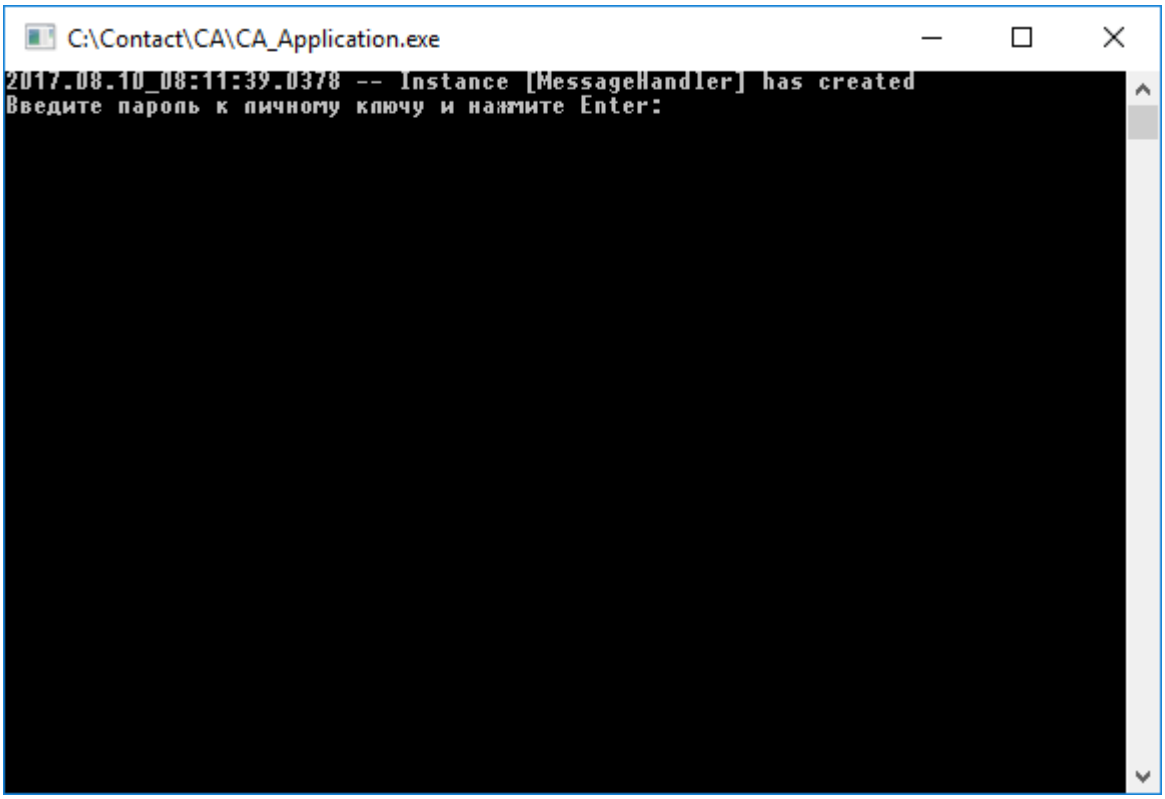

Рис. 2

После ввода пароля к личному ключу (введенные символы не отображаются) необходимо нажать клавишу «Enter», после чего продолжится инициализация модулей КП УЦ (рис. 3).

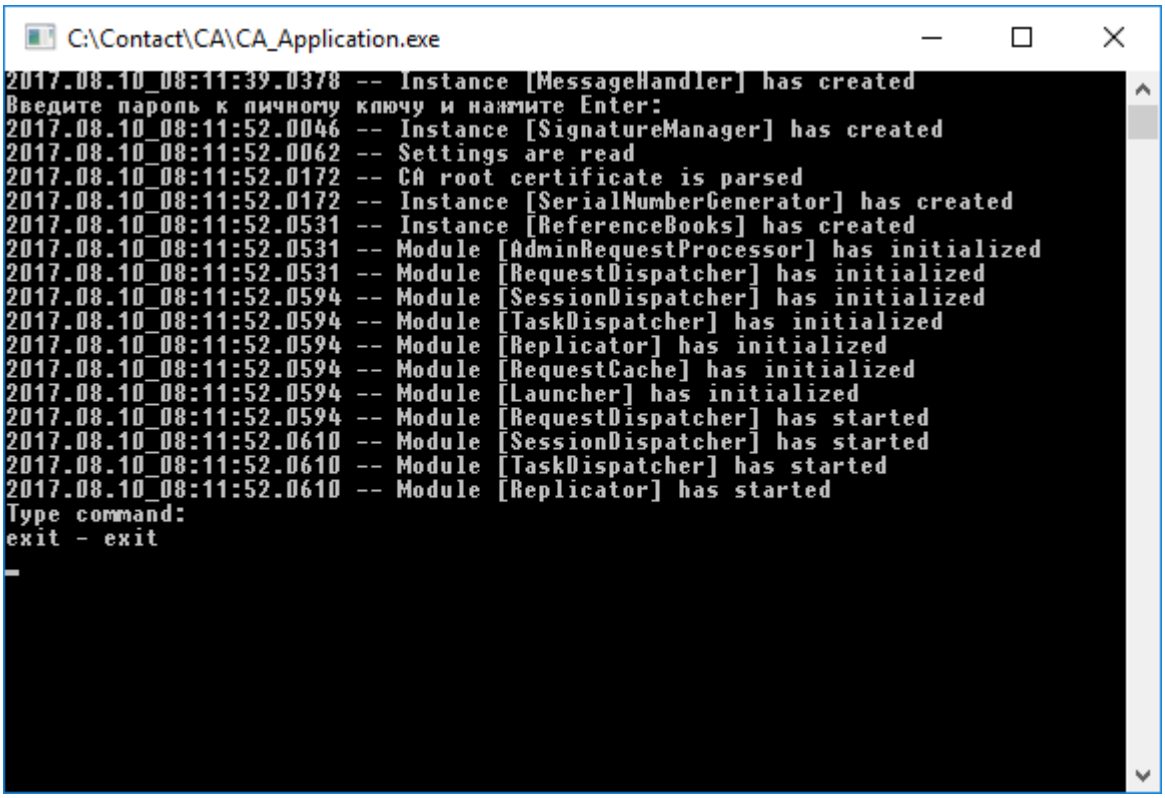

Рис. 3

3.6. Порядок выполнения КП УЦ

3.6.1. Особенности работы с КП СОБ

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

Функции самотестирования КП УЦ выполняются КП СОБ, при этом производится контроль целостности файлов ПО КП УЦ и КП СОБ, входящего в его состав, и тестирование криптографических алгоритмов.

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.

3.6.2. Администрирование

Администрирование КП УЦ осуществляется путем внесения, удаления и корректировки конфигурационного файла («settings.ini») и конфигурационного файла КП СОБ. Пример настроечного файла КП УЦ представлен в приложении Б.

В качестве отдельно поставляемого приложения может использоваться ПО «Консоль администрирования комплекса программного 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 программного Удостоверяющий центр. Руководство оператора» BY.СЮИК.00380-02 34 01.

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

3.6.3. Реестр СОК

ПО может быть настроено таким образом, что КП 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.

3.6.4. Просмотр версии КП УЦ

Для просмотра номера версии ПО необходимо после запуска КП УЦ открыть из рабочей директории в текстовом редакторе файл журнала «CA_log.log» и найти запись уведомления модуля «CA_Launcher» (рис. 4).

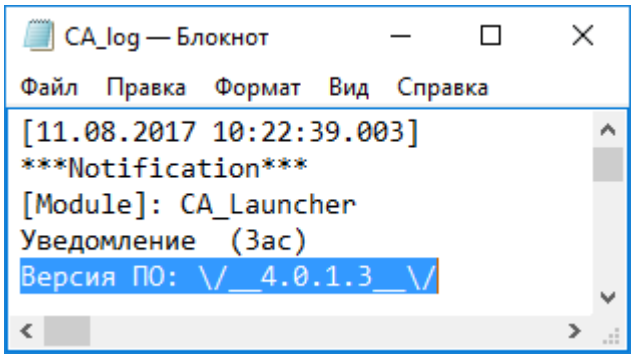

Рис. 4

3.6.5. Резервное копирование и восстановление хранилища сертификатов

КП 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)

Перед восстановлением хранилища сертификатов необходимо задать путь к файлу восстанавливаемого хранилища в настроечном файле КП УЦ в параметре DbPath секции [Database]. В процессе этот файл будет создан. Если на момент восстановления такой файл существует, процедура восстановления завершиться ошибкой.

Восстановление хранилища сертификатов (файла БД) из резервной копии с предварительной проверкой ЭЦП выполняется путем запуска КП УЦ со специальным параметром командной строки «–restoredb», после которого указывается путь к файлу трейлера безопасности.

Параметр и путь к файлу трейлера разделяются знаком «=». Например:

```
-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.

3.7. Завершение работы КП УЦ

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

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

4. СООБЩЕНИЯ ОПЕРАТОРУ

При успешном запуске КП УЦ в консольном окне появляется надпись:

```
type command:
exit – exit
```

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

1) При отсутствии в рабочей директории КП УЦ файлов (одного или нескольких) библиотеки динамической компоновки оператору выдается сообщение с указанием недостающей библиотеки (рис. 5-7). При появлении одного из таких сообщений следует поместить отсутствующий файл в рабочую директорию приложения.

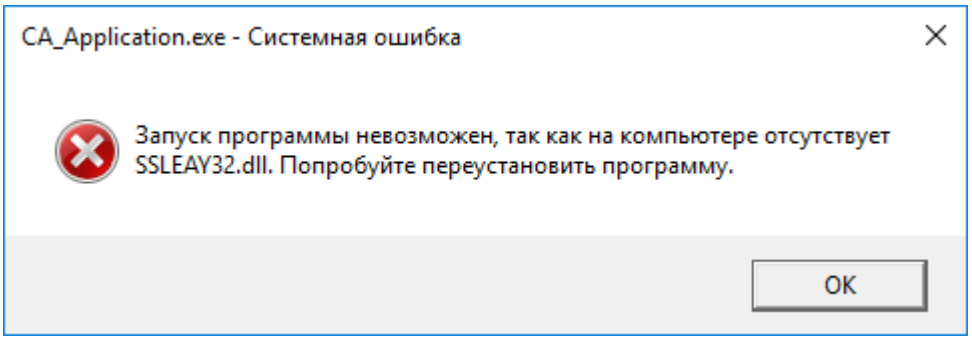

Рис. 5

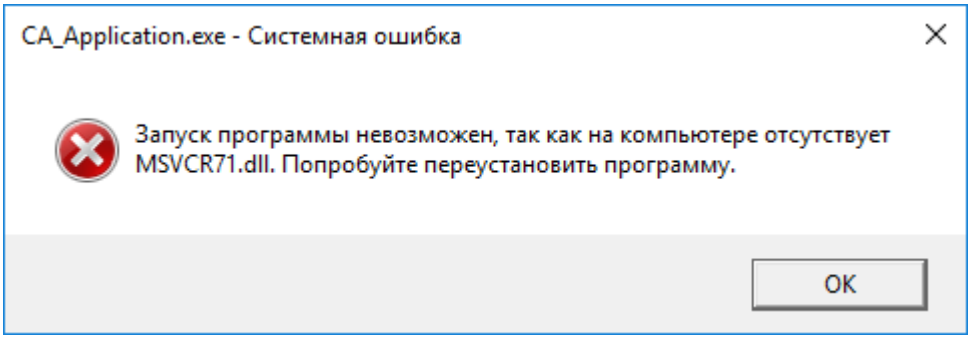

Рис. 6

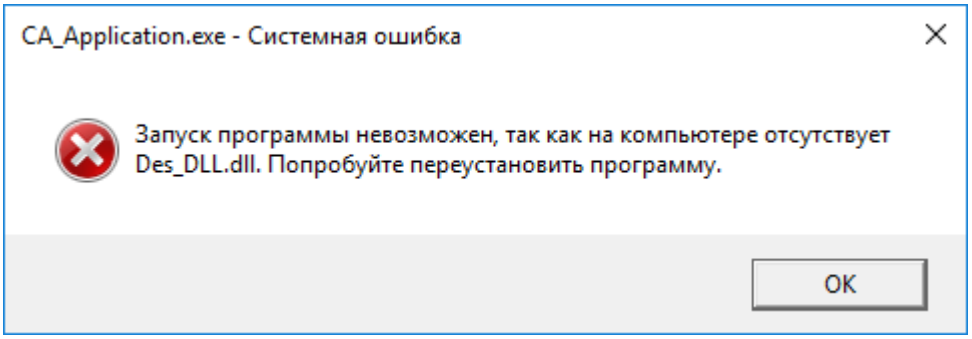

Рис. 7

2) Появление сообщения представленного на рис. 8 означает, что не была установлена служба СУБД Firebird, а сообщение на рис. 9 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».

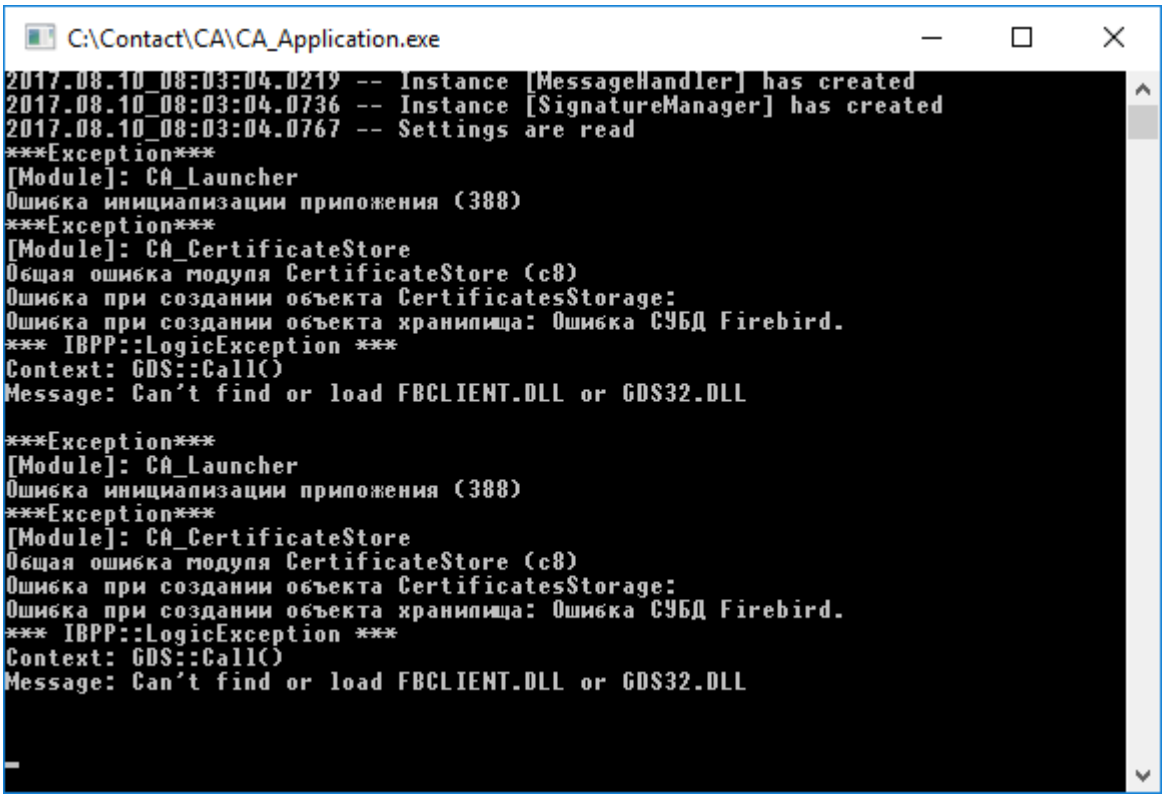

Рис. 8

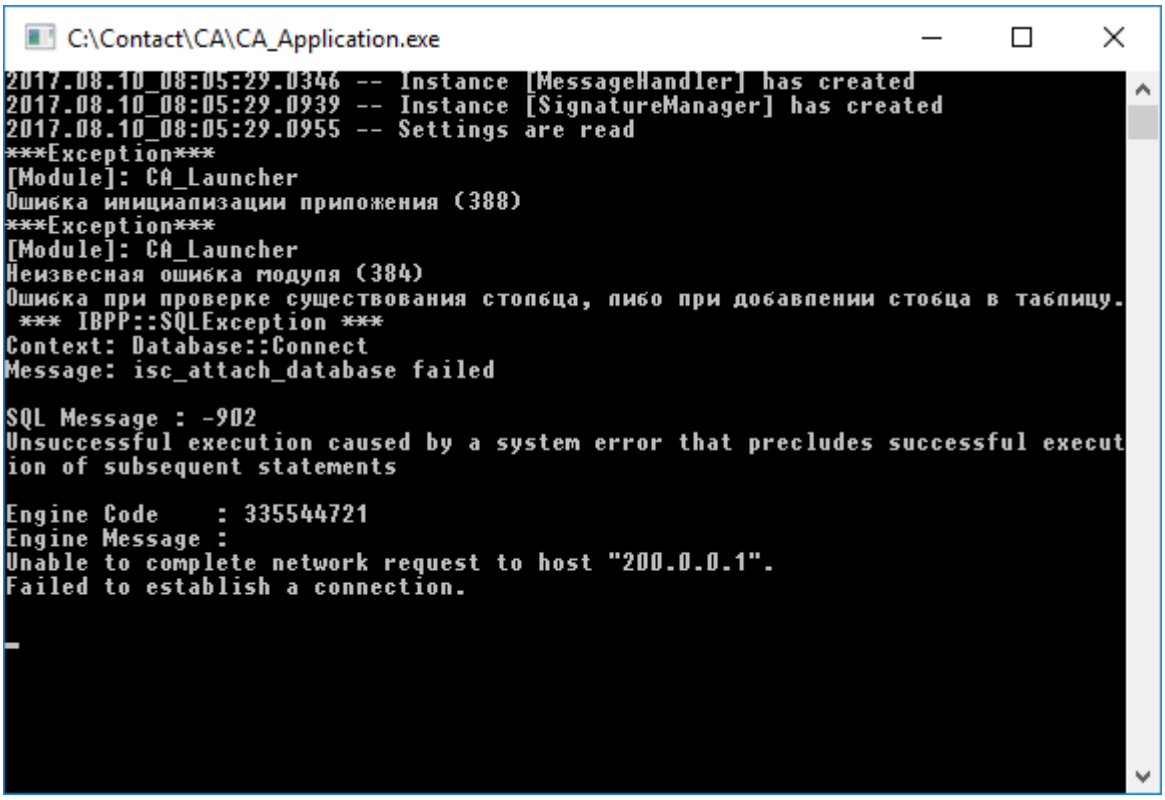

Рис. 9

3) Если во время запуска КП УЦ не работает КП СОБ, а в настроечном файле КП УЦ неверно указан путь к исполняемому модулю КП СОБ, или работа КП СОБ заблокирована, то в консоль будет выводиться сообщение о том, что КП СОБ не запущен (рис. 10), до тех пор, пока КП СОБ не начнет работу.

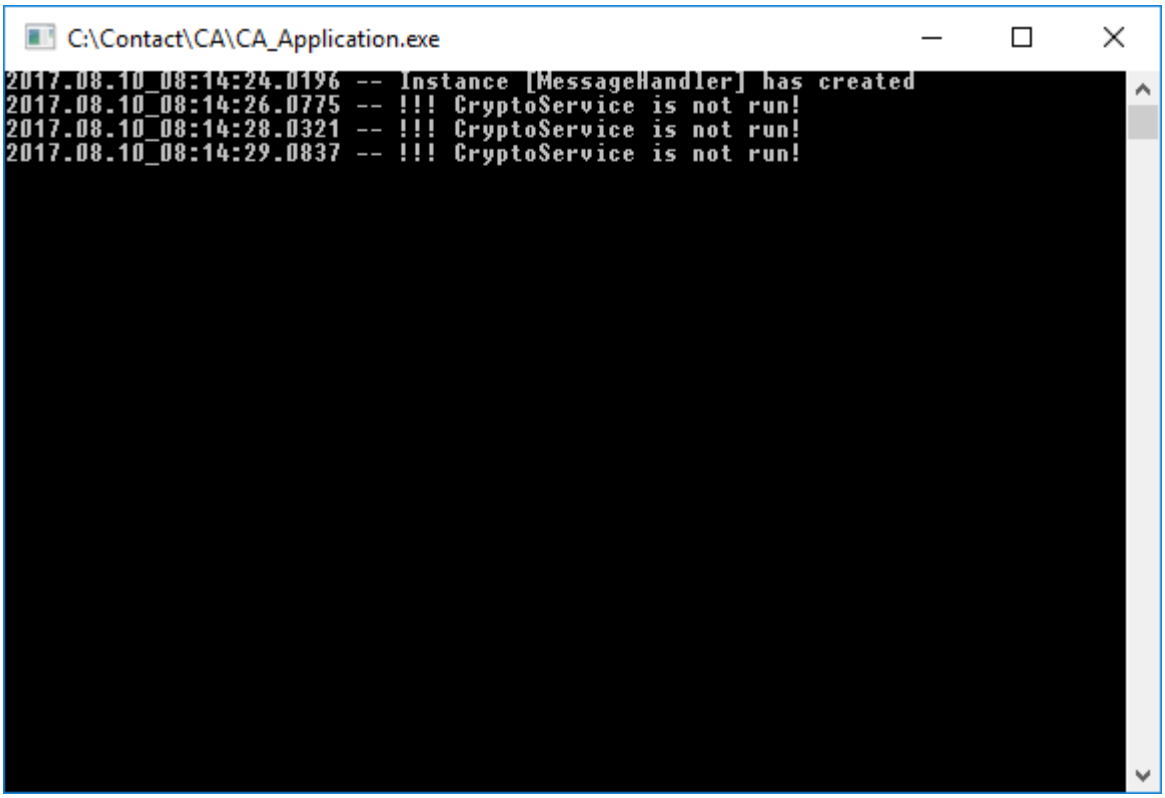

Рис. 10

4) Если в консольное окно КП УЦ выводится сообщение, представленное на рис. 11, это означает, что порт HTTP, который указан в настройках КП УЦ, уже занят. Скорее всего предпринята попытка запуска второй копии ПО КП УЦ.

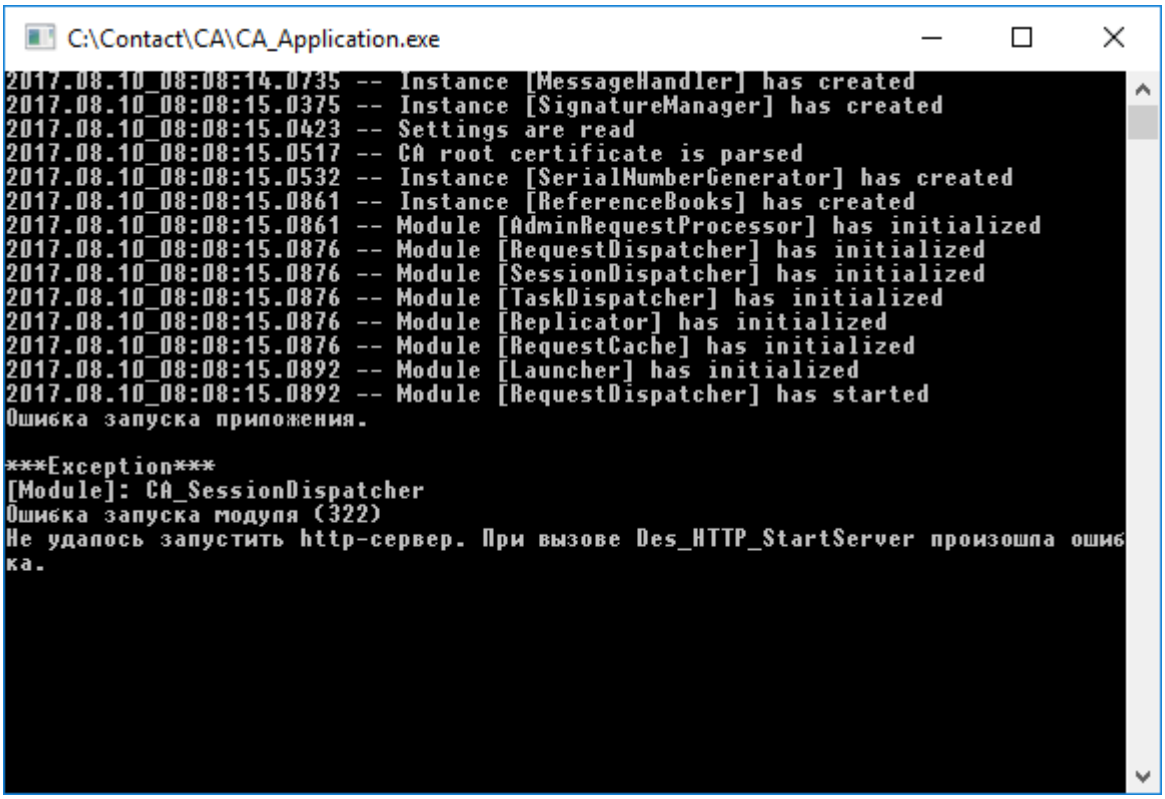

Рис. 11

5) Если в настроечном файле КП УЦ не был указан пароль к личному ключу, а в консоли был введен неправильный пароль, то выведется сообщение, представленное на рис. 12.

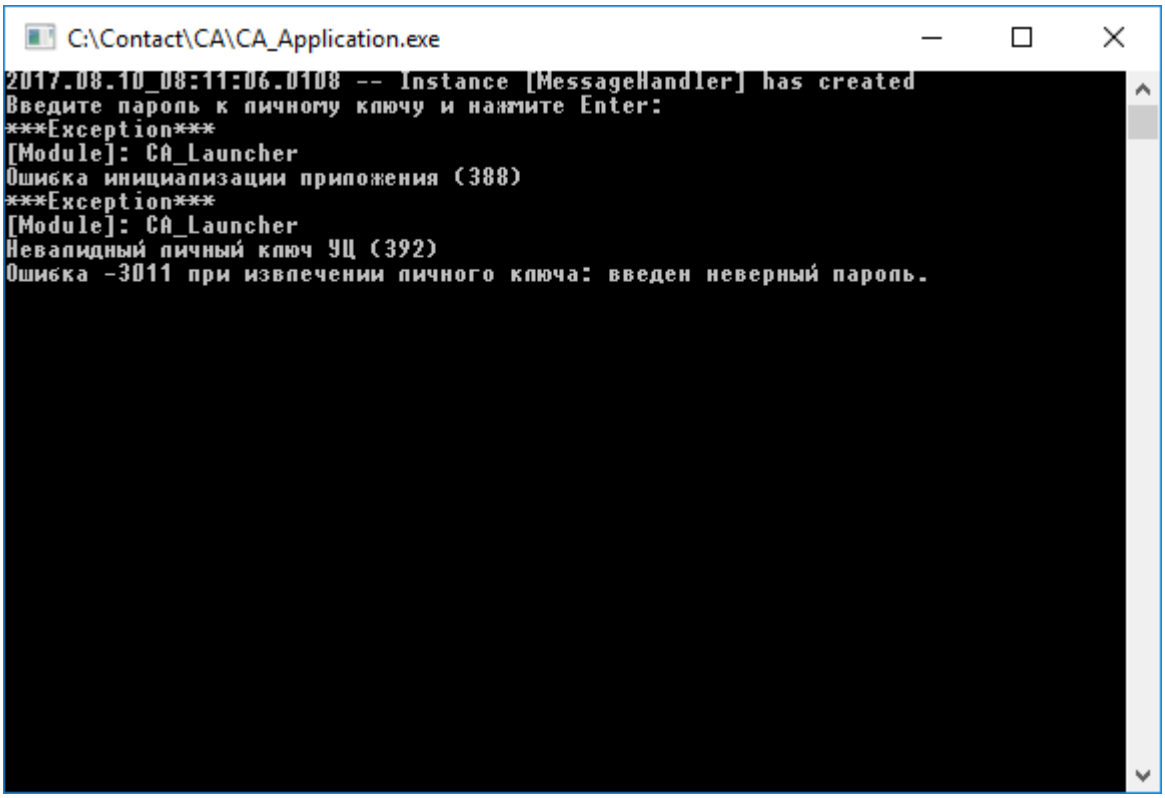

Рис. 12

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

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

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

ПРИЛОЖЕНИЕ А

Установка и запуск службы СУБД Firebird

Для установки службы СУБД Firebird с поставляемого производителем диска необходимо из папки «Вспомогательное окружение\Firebird 2.5.2 (win32)» запустить исполняемый файл «Firebird-2.5.2.26540_0_Win32.exe». Отобразится окно выбора языка, который будет использован в процессе установки (рис. 13). Далее необходимо нажать кнопку «OK».

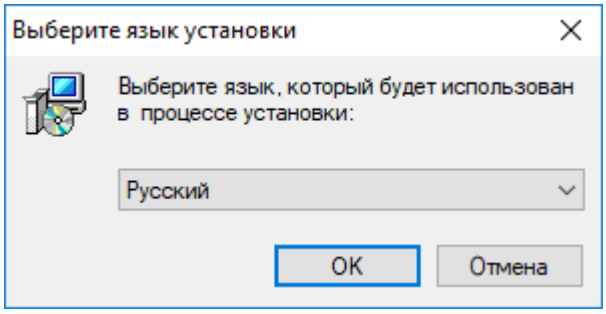

Рис. 13

Откроется приветственное окно мастера установки Firebird (рис. 14). Необходимо нажать кнопку «Далее».

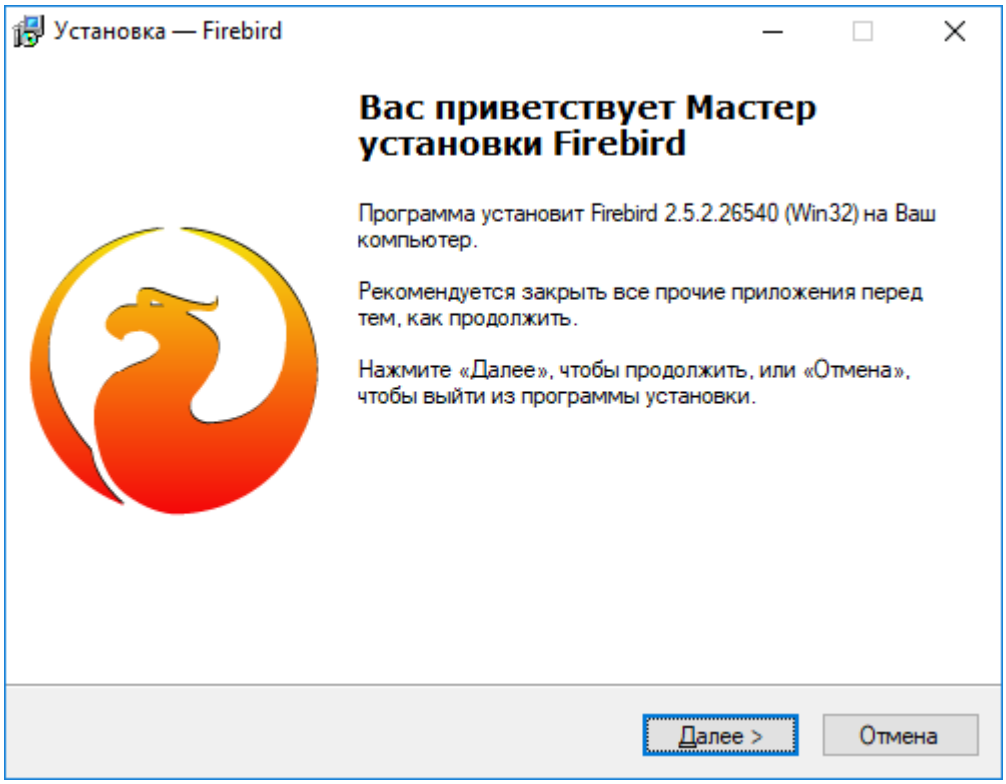

Рис. 14

Отобразится окно с лицензионным соглашением (рис. 15). Необходимо прочитать его, в нижней части окна установить переключатель «Я принимаю условия соглашения» и нажать кнопку «Далее».

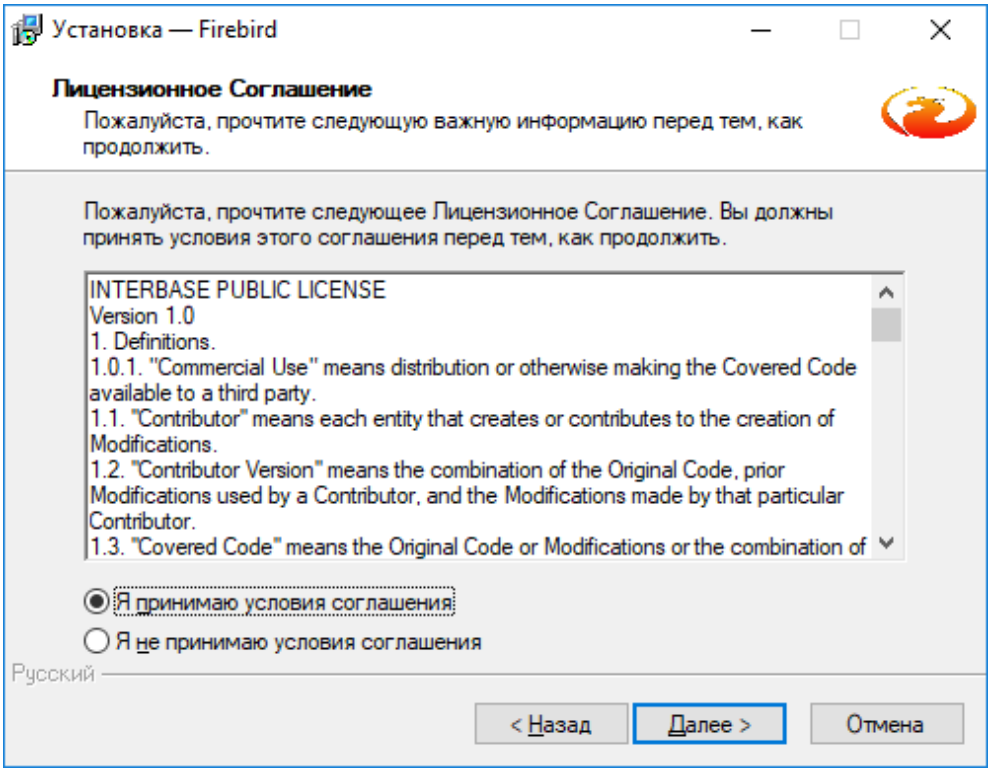

Рис. 15

Далее откроется информационное окно содержащее руководство по установке службы Firebird (рис. 16). Необходимо его прочитать, а затем нажать кнопку «Далее».

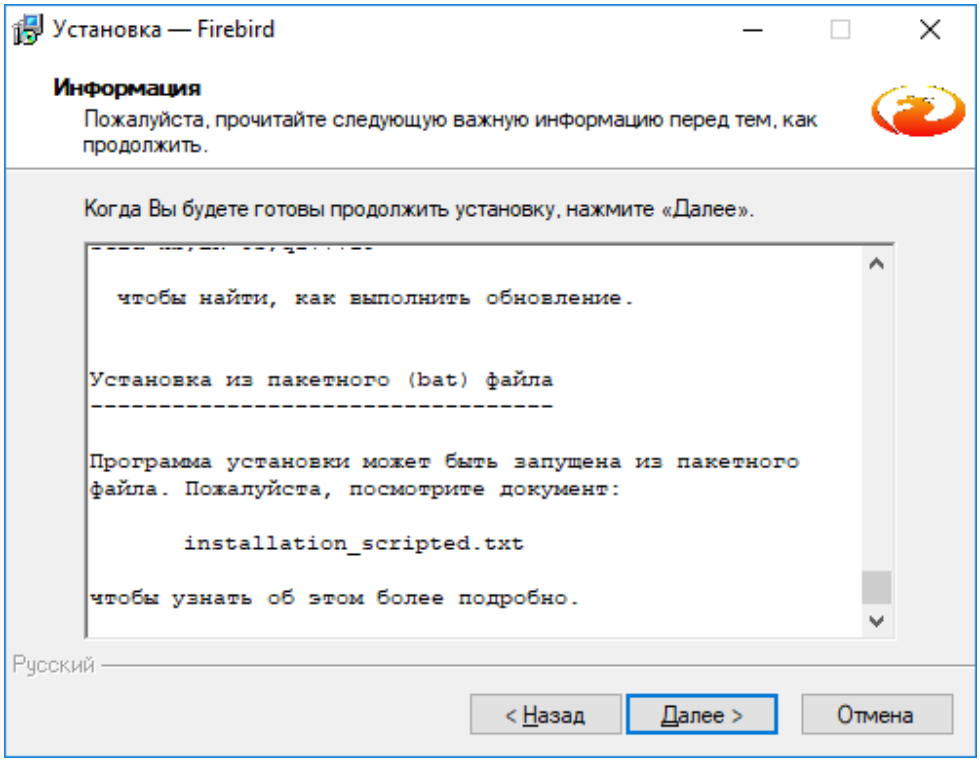

Рис. 16

Откроется окно выбора места установки Firebird (рис. 17). В поле ввода необходимо прописать путь к директории для установки либо нажать кнопку «Обзор…» и выбрать папку в открывшемся стандартном окне выбора директории, нажать кнопку «Далее».

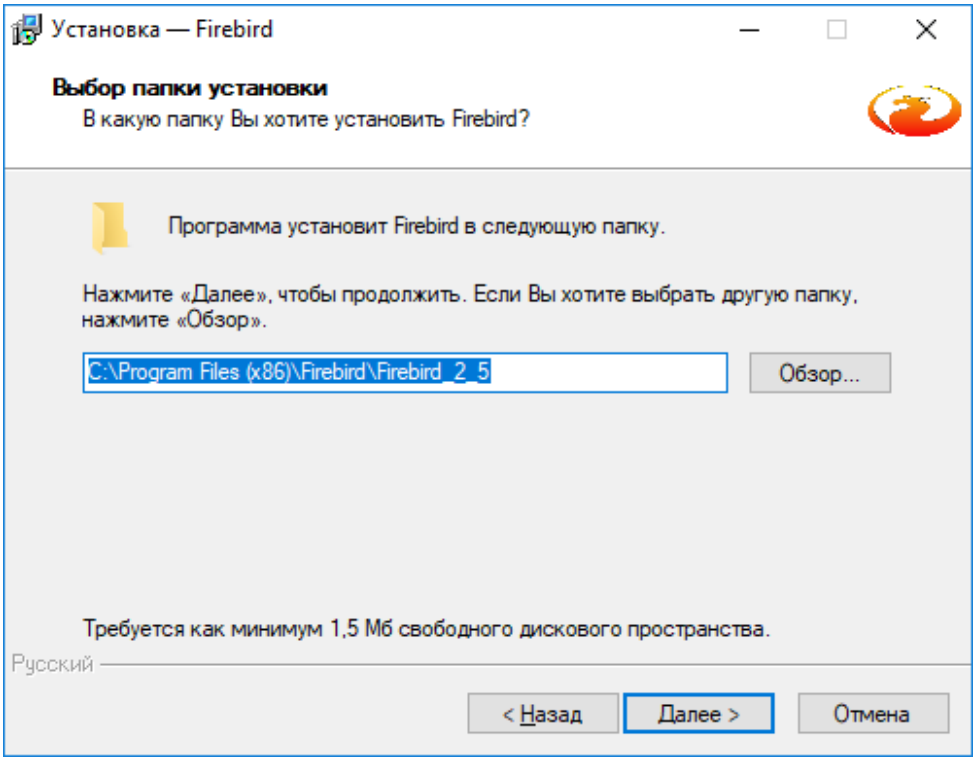

Рис. 17

Откроется окно выбора компонентов (рис. 18). Рекомендуется оставить выбор по умолчанию и нажать кнопку «Далее».

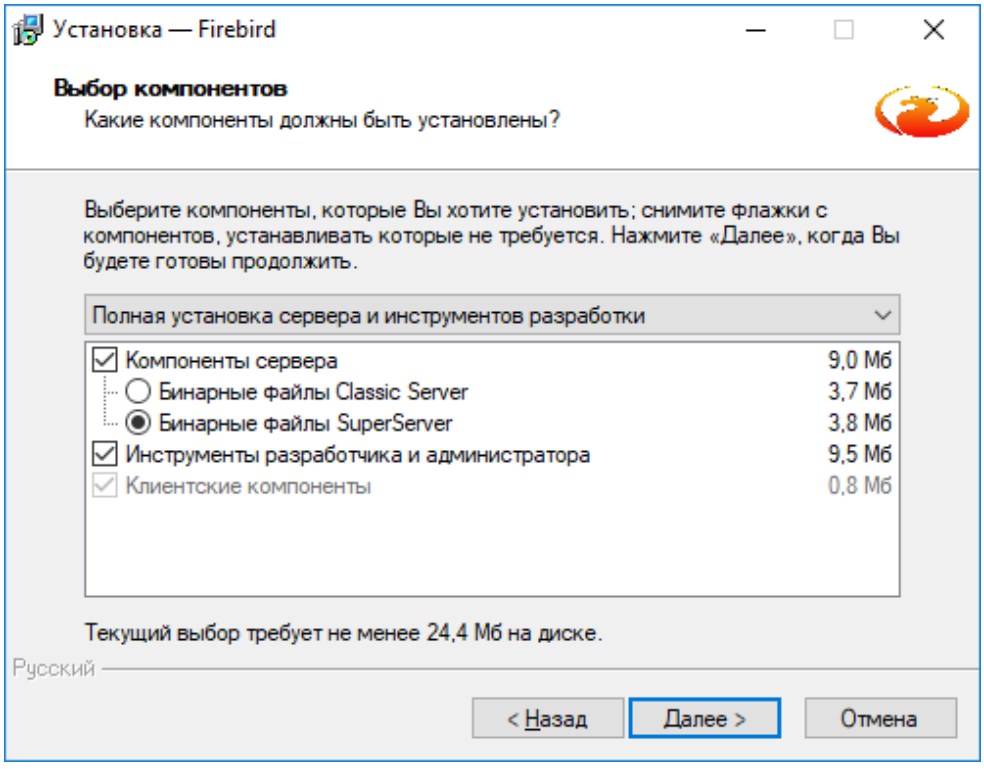

Рис. 18

Откроется окно настройки создания ярлыков (рис. 19). Если не нужно создавать папку в меню «Пуск», то необходимо установить флажок «Не создавать папку в меню “Пуск”». Затем необходимо нажать кнопку «Далее».

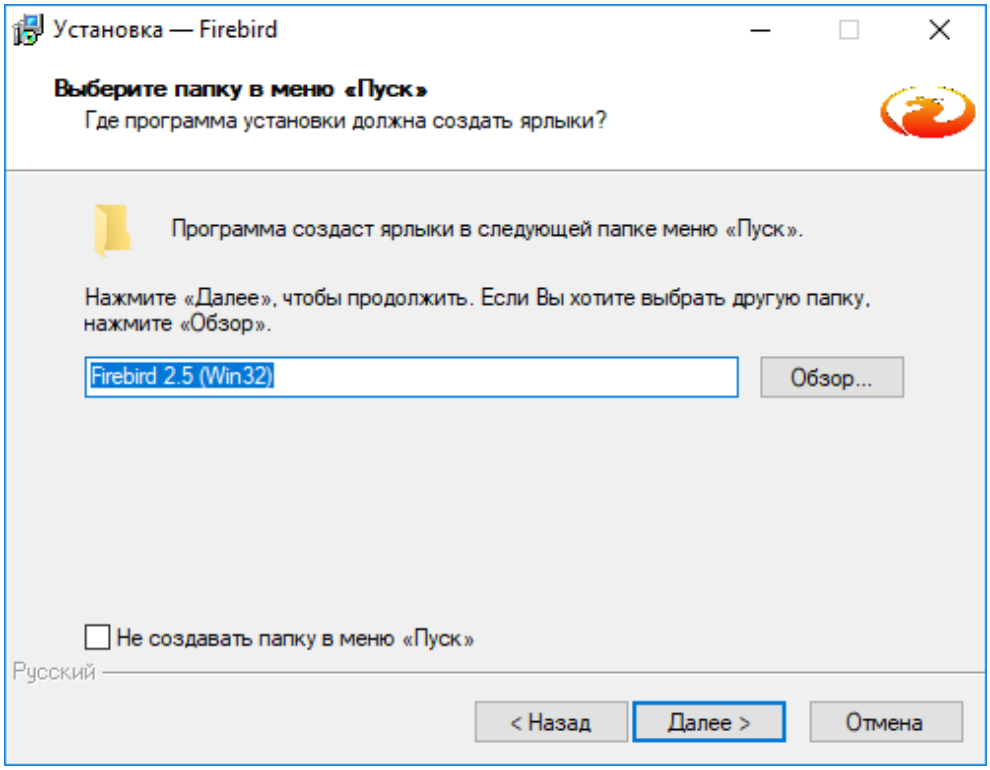

Рис. 19

Откроется окно выбора дополнительных задач. Рекомендуется выставить настройки, как показано на рис. 20, и нажать кнопку «Далее».

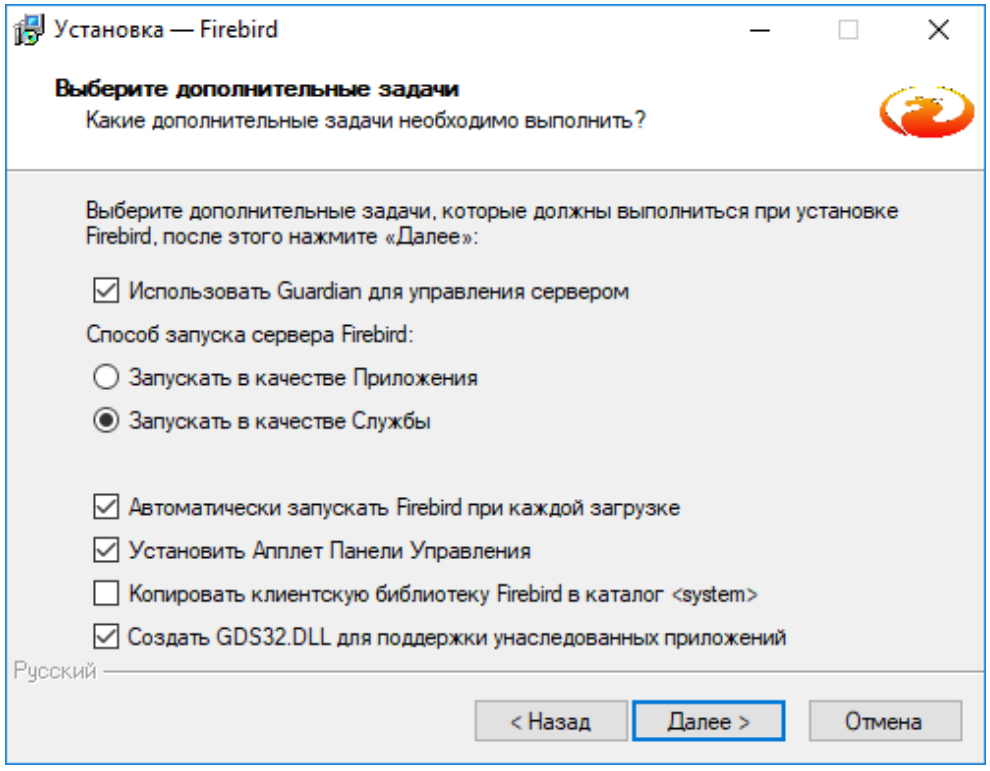

Рис. 20

Откроется окно, содержащее все выбранные опции установки (рис. 21). Необходимо убедиться в том, что все настройки корректны, и нажать кнопку «Установить».

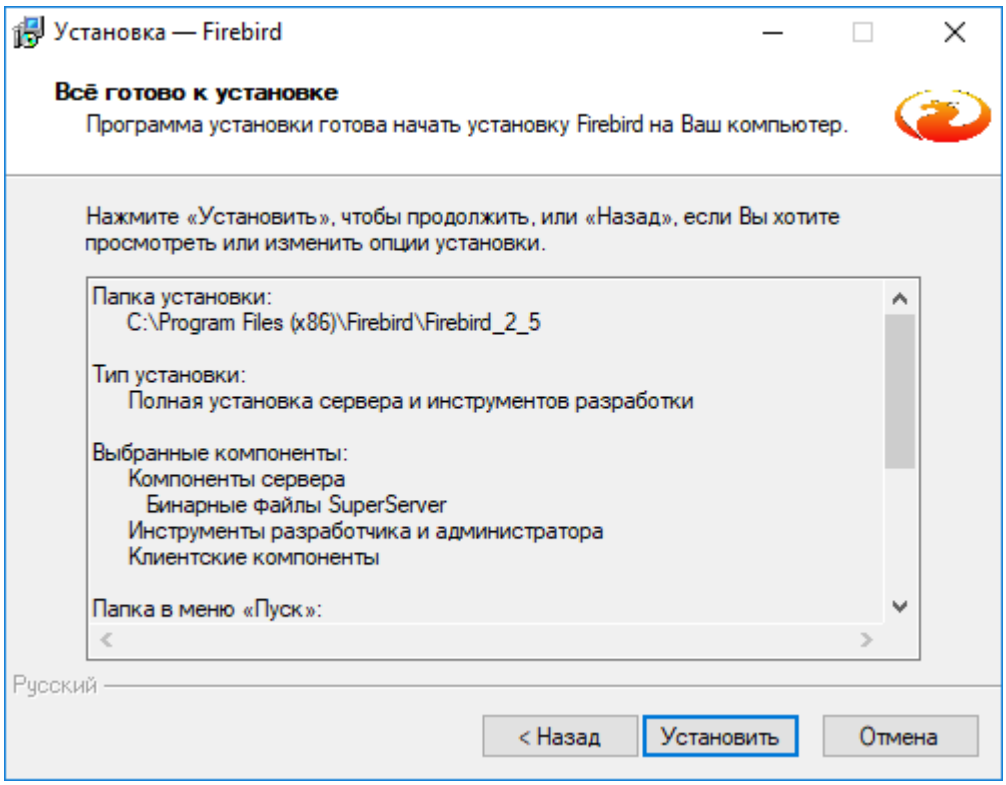

Рис. 21

Откроется окно с индикатором прогресса установки (рис. 22).

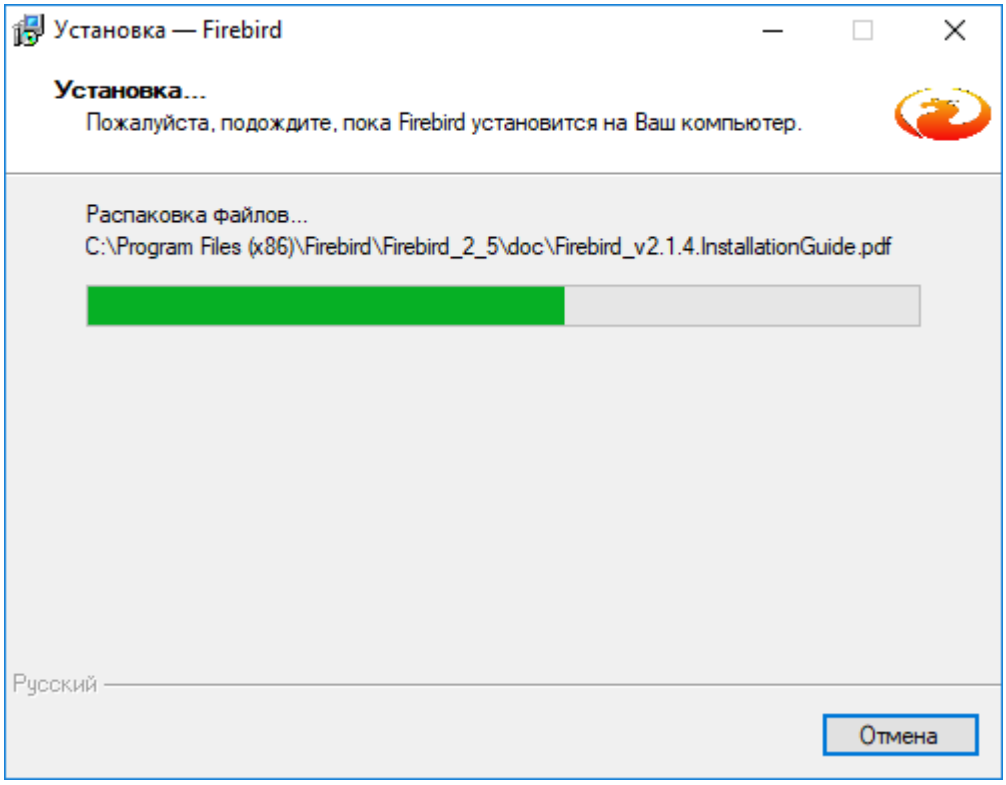

Рис. 22

После завершения установки откроется окно с информацией (рис. 23), с которой необходимо ознакомиться, а затем нажать кнопку «Далее».

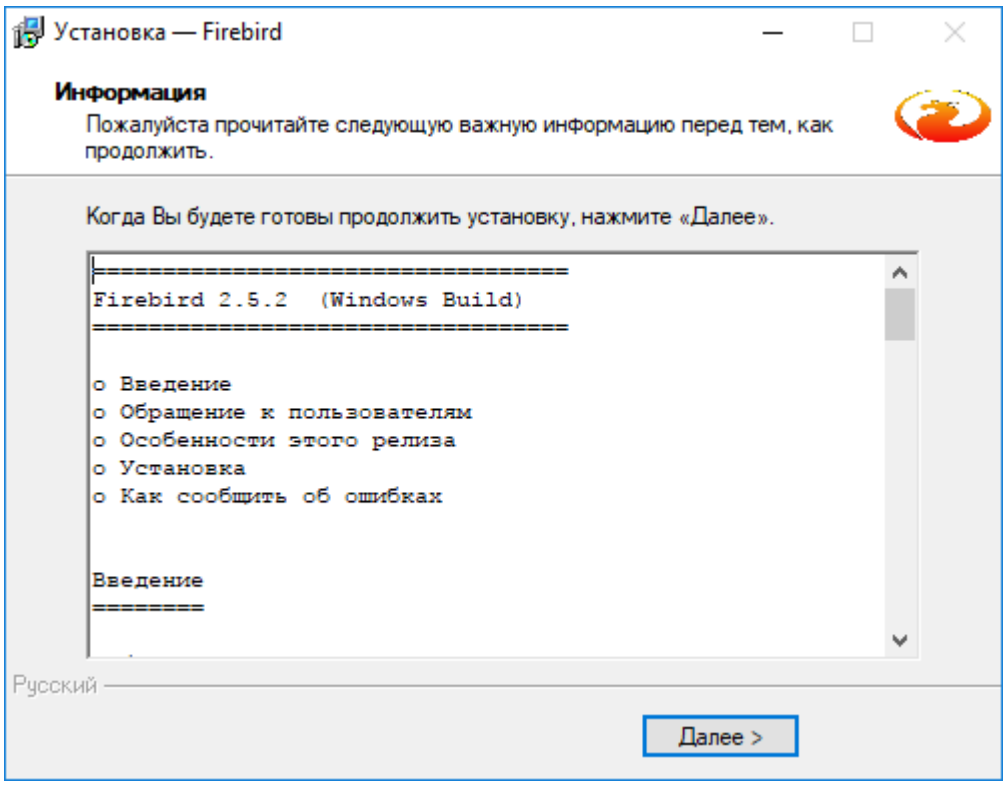

Рис. 23

Откроется окно завершения мастера установки (рис. 24). Необходимо установить флажок «Запустить Службу Firebird?» и нажать кнопку «Завершить».

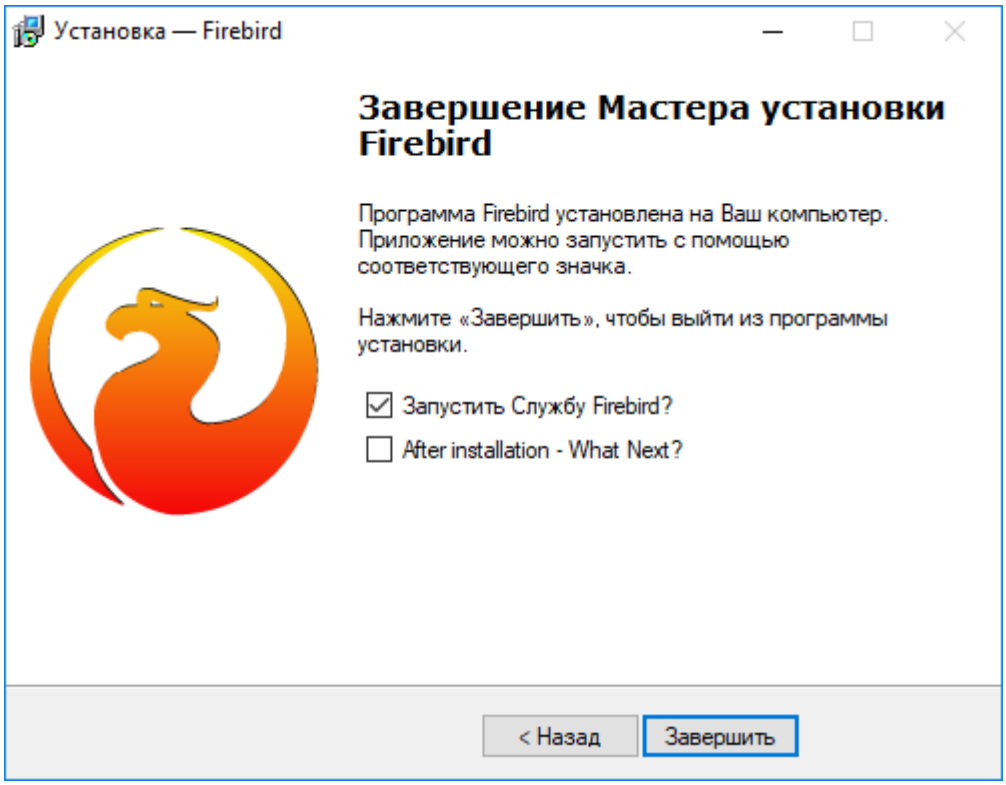

Рис. 24

ПРИЛОЖЕНИЕ Б

Пример файла настройки КП УЦ

```
; 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 СОБ
[CryptoService]
; сетевой адрес хоста, на котором запущен модуль КП СОБ
HostAddr="127.0.0.1"
; порт, на котором КП СОБ "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 СОБ (если КП СОБ при запуске КП УЦ не запущен,
то он запустится автоматически по этому пути)
Path = "e:\CryptoService\CryptoService_41.exe"
; временя через которое КП УЦ получает состояние КП СОБ в секундах(по
умолчанию 10 секунд)
PeriodForStateCS = 120
;
[MessageHandler]
ApplicationName="Контакт КП 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
; пароли администраторов консоли
AuthPassword#1="12345678"
;
; 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 КП 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="111115111111111107da0000000000000001"
CertificatePath=".\certificates\Root111115111111111107da0000000000000001.cer"
PrivateKeyPath=".\keys\Root_111115111111111107da0000000000000001.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 КП 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 В

Описание работы утилиты SpecializedCertIssuing

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.

В.1. Настройка утилиты

Настройка приложения «SpecializedCertIssuing.exe» осуществляется путем редактирования в текстовом редакторе файла «SpecCertIssuingSettings.xml», который расположен в рабочей директории КП 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.

В.2. Запуск утилиты

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

При возникновении ошибок при запуске приложения на экране отобразятся диалоговые окна, сообщающие об ошибке (рис. 25-27).

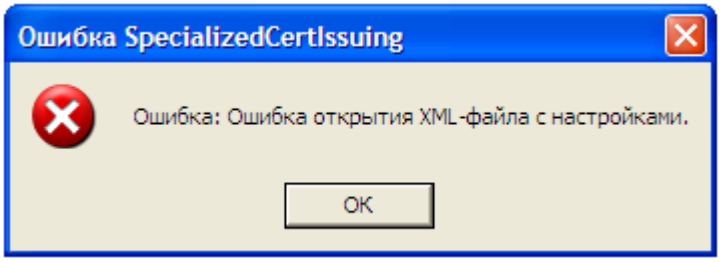

Рис. 25

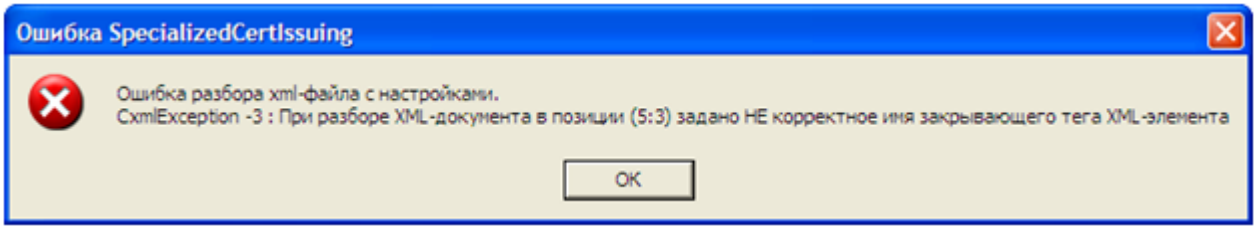

Рис. 26

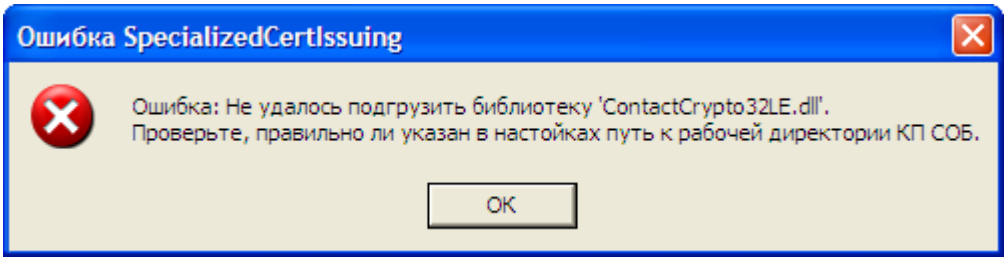

Рис. 27

Если при настройке приложения был указан корректный абсолютный путь к рабочей директории КП СОБ, но на экран выводится сообщение, отображенное на рис. 28, то необходимо скопировать с поставляемого производителем диска из папки «Вспомогательное окружение\system_dlls» в рабочую директорию КП УЦ в папку «SpecializedCertIssuing» системную библитеку «msvcr71.dll».

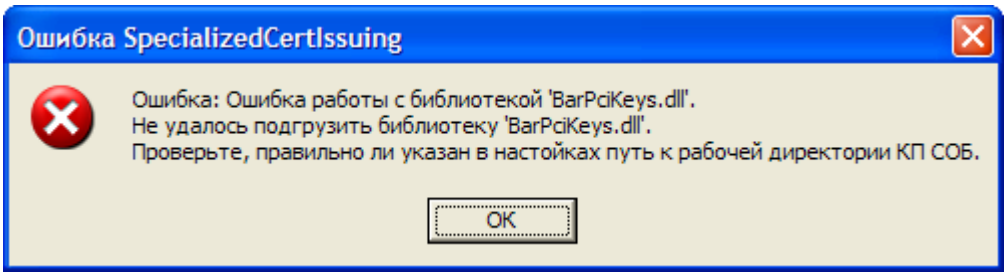

Рис. 28

В случае успешного запуска отобразится главное окно приложения (рис. 29).

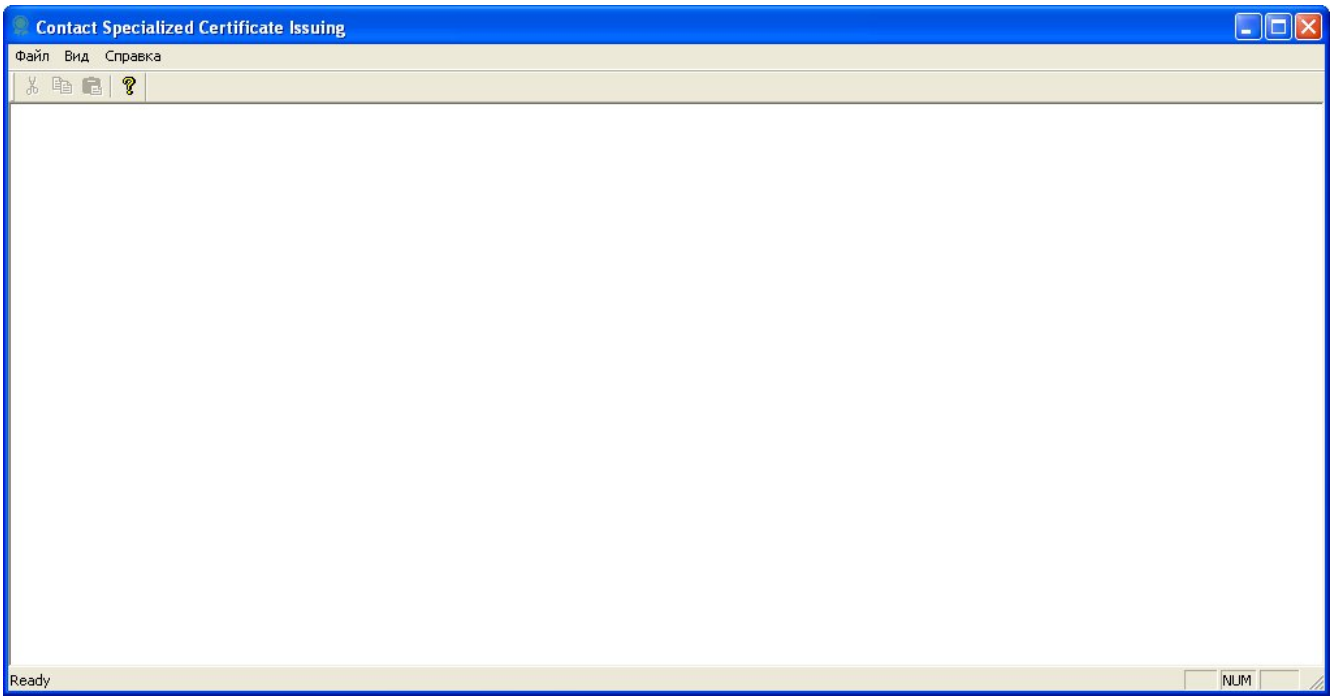

Рис. 29

B.3. Выполнение утилиты

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\"/>
```

```
    <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, $7E1_{16} = 2017_{10}$),

`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 КП 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» (рис. 30).

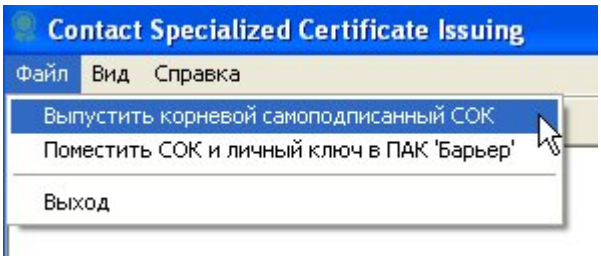

Рис. 30

Затем в окне выбора файла (рис. 31) выбрать настроечный файл, содержащий информацию о выпускаемом СОК.

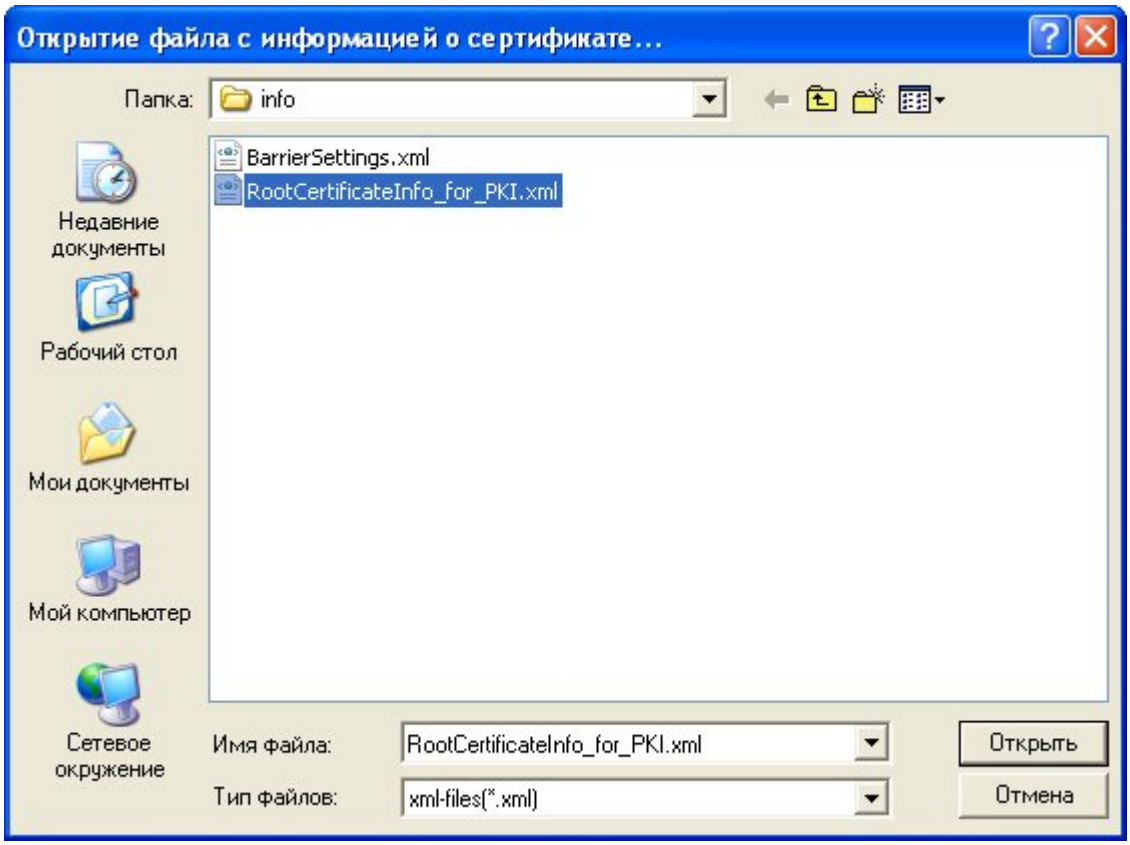

Рис 31

Далее необходимо ввести пароль с подтверждением к новому личному ключу КП УЦ в окне, представленном на рис. 32. После ввода нажать кнопку «ОК».

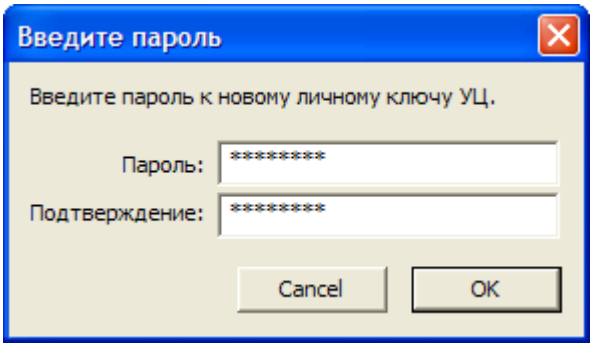

Рис. 32

В случае успешного формирования СОК на экране отобразится соответствующее сообщение (рис. 33).

Рис. 33

Если в настроечном файле был указан идентификатор ТМ-карты администратора КП УЦ, то дополнительно будет выведено сообщение о помещении СОК в ПАК «Барьер» (рис. 34).

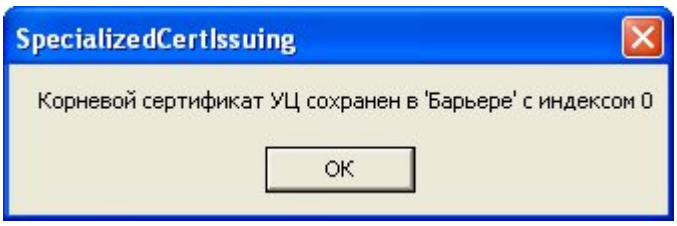

Рис. 34

Также на экран выведется сообщение о сохранении файла личного ключа (рис. 35).

Рис. 35

Если в настроечном файле был указан идентификатор ТМ-карты администратора КП УЦ, то дополнительно будет выведено сообщение о помещении личного ключа в ПАК «Барьер» (рис. 36).

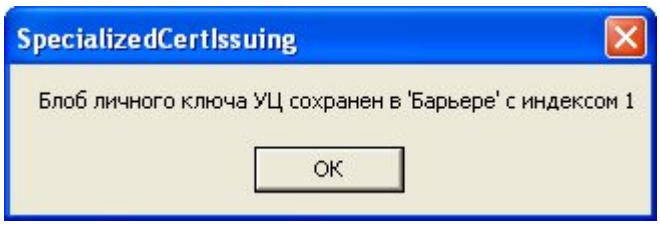

Рис. 36

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 КП 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» (рис. 37).

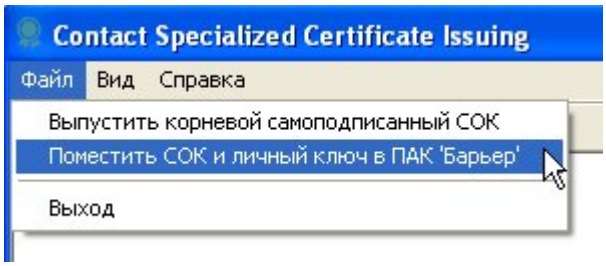

Рис. 37

Затем в окне выбора файла (рис. 38) выбрать настроечный файл, содержащий идентификатор ТМ-карты администратора КП УЦ.

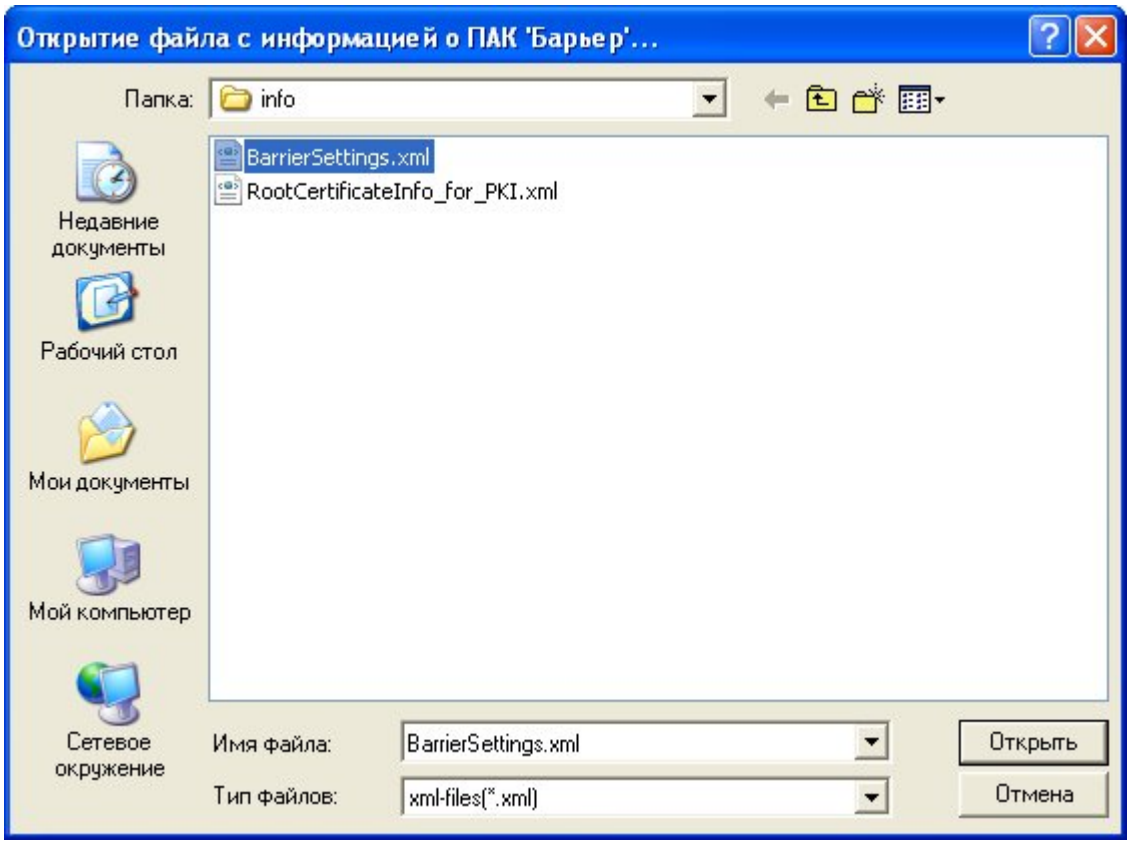

Рис. 38

Далее последовательно в окнах выбора файла (рис. 39, 40) выбрать файл СОК и файл личного ключа.

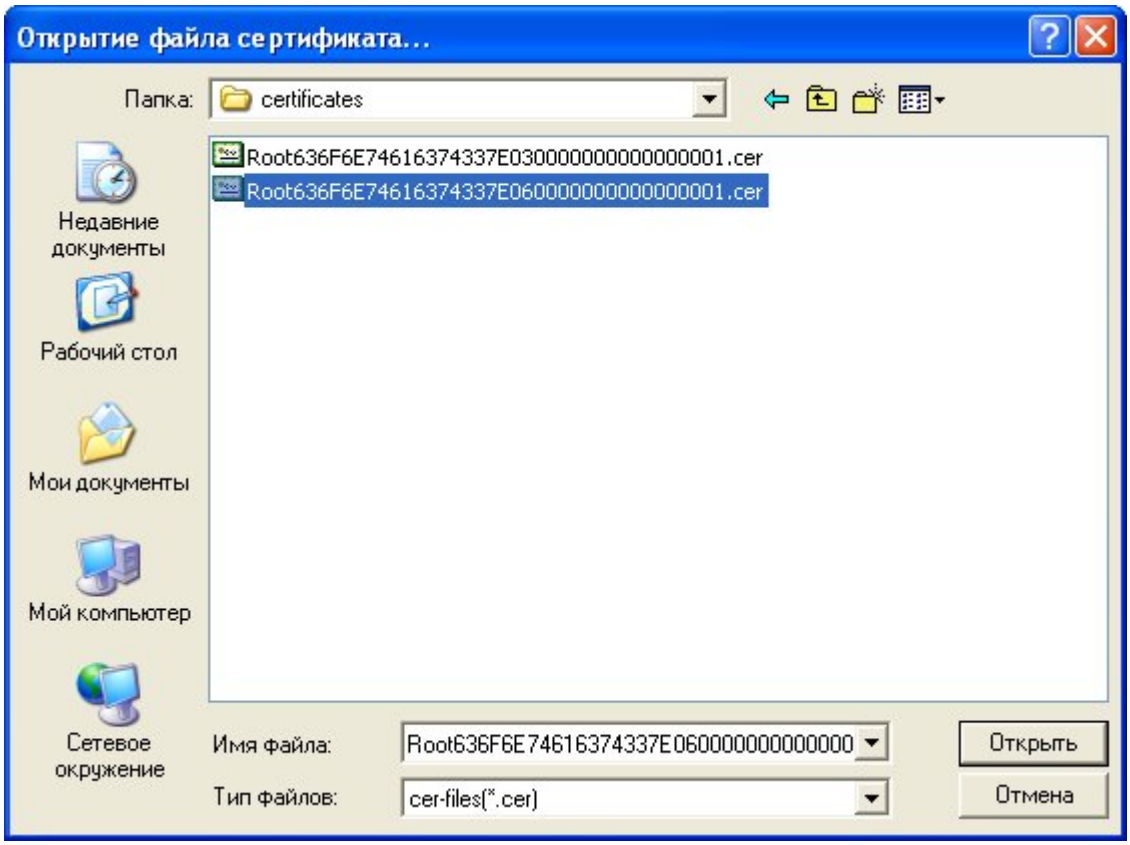

Рис. 39

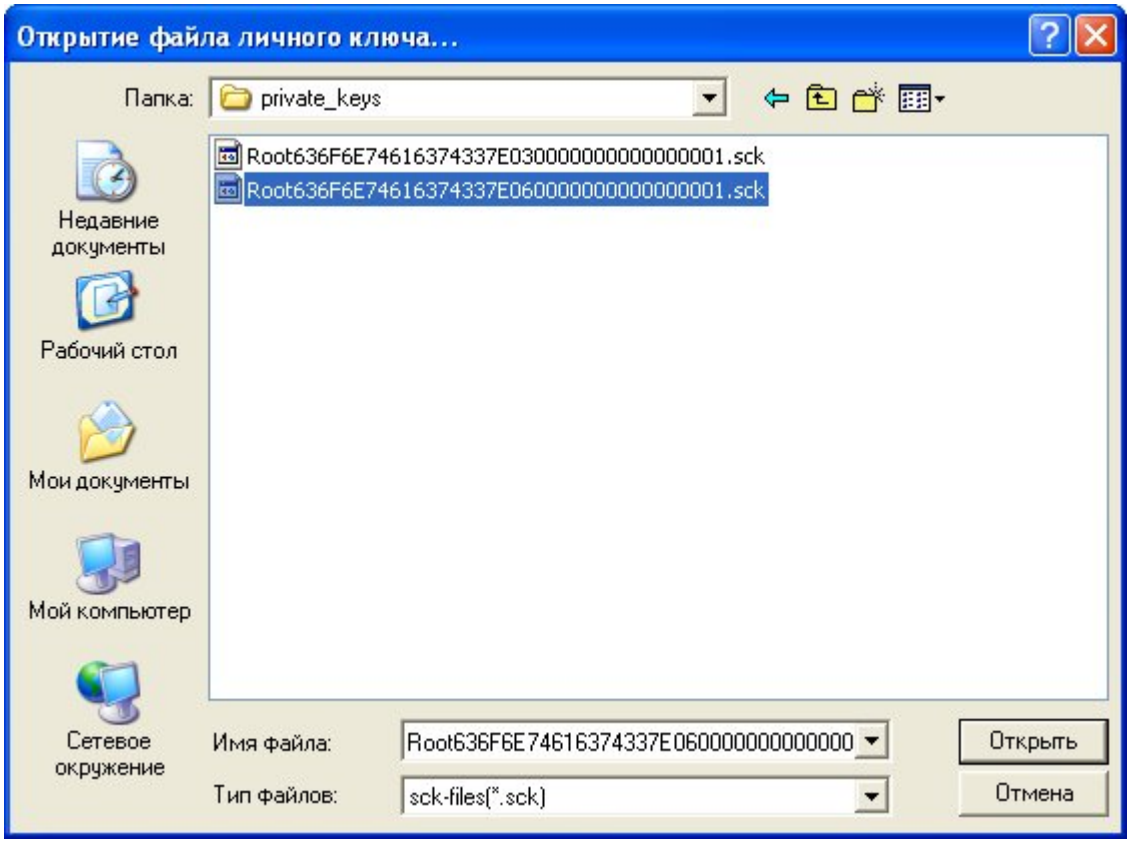

Рис. 40

После успешного помещения СОК и личного ключа в память ПАК «Барьер» на экран выведутся соответствующие сообщения (рис. 41, 42).

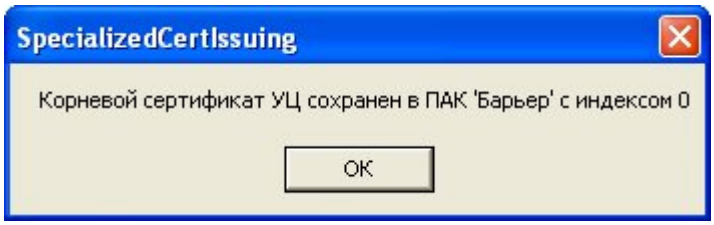

Рис. 41

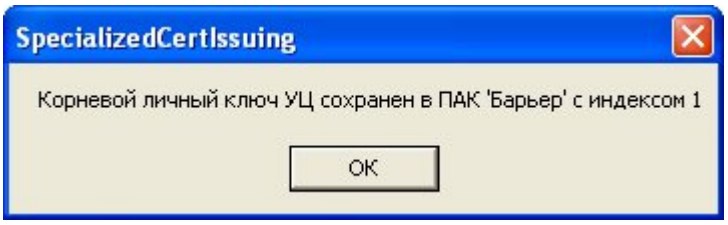

Рис. 42

B.4. Завершение работы утилиты

Для завершения работы приложения «SpecializedCertIssuing.exe» необходимо выбрать пункт «Выход» из меню «Файл» (рис. 43).

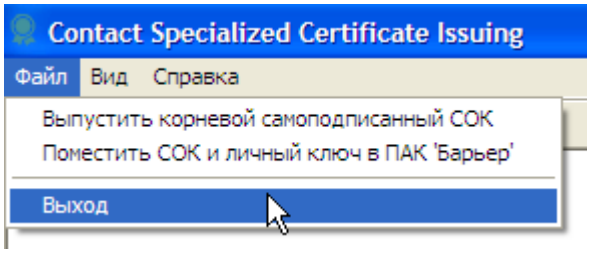

Рис. 43

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

В настоящем документе приняты следующие сокращения:

БД	– база данных
КП РЦ	– Подсистемы криптографической защиты информации. Комплекс программный Регистрационный центр BY.СЮИК.00363-03
КП СОБ	– Подсистема криптографической защиты информации. Комплекс программный Средств обеспечения безопасности РБ.СЮИК.00364-03
КП УЦ	– Подсистема криптографической защиты информации. Комплекс программный Удостоверяющий центр BY.СЮИК.00314-06
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
ЭЦП	– электронная цифровая подпись

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопрово-дительного докум. и дата	Подп.	Дата
	изменен-ных	заменен-ных	новых	аннули-рованных					