УТВЕРЖДЁН

RU.НКБГ.70010-02 91 - ЛУ

МОДУЛЬ ГЕНЕРАЦИИ КЛЮЧЕЙ

«МГК-3»

Руководство пользователя

RU.НКБГ.70010-02 91

Листов 27

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата
2246				

Содержание

1. Общие сведения

Полное наименование изделия - СКЗИ «Модуль генерации ключей «МГК-3»

Краткое наименование - СКЗИ «МГК-3» или МГК-3

Обозначение изделия - RU.НКБГ.70010-02

Программа СКЗИ «Модуль генерации ключей МГК-3» выполняет генерацию несимметричных ключевых пар (открытого и закрытого ключей) и формирует запросы на выпуск обычных и квалифицированных сертификатов ключа.

Несимметричная ключевая пара (открытый и закрытый ключи) предназначена для шифрования и/или для формирования электронной подписи ЭП. Обычный сертификат служит для шифрования и/или для проверки неквалифицированной ЭП. Квалифицированный сертификат служит для шифрования и/или для проверки квалифицированной ЭП.

Закрытый ключ записывается на ключевой носитель, а дополнительная информация, необходимая для его использования, и открытый ключ входят в запрос на сертификат и записываются в указанный пользователем файл.

Сформированный запрос на сертификат передается в Удостоверяющий Центр по надежному каналу связи (например, фельдъегерской службой). Результатом обработки запроса является либо выпущенный сертификат (обычный или квалифицированный), либо сообщение об ошибке.

Закрытый и открытый ключи записывается на носитель в формате PKCS#15 в соответствии с документом:

«Методические рекомендации технического комитета по стандартизации «Криптографическая защита информации» (ТК 26). Ключевой контейнер» (Утверждены решением заседания технического комитета по стандартизации «Криптографическая защита информации» - Протокол № 10 от 27.11.2012 г.).

При этом обеспечивается шифрование закрытого ключа на ключе, выработанном из пароля с обеспечением целостности. Ключ из пароля вырабатывается в соответствии с документом:

«Методические рекомендации технического комитета по стандартизации «Криптографическая защита информации» (ТК 26). Парольная защита с использованием алгоритмов ГОСТ (Утверждены решением заседания технического комитета по стандартизации «Криптографическая защита информации» - Протокол № 10 от 27.11.2012 г.).

Пароль состоит не менее, чем из 6 символов из алфавита, содержащего малые и большие латинские буквы и цифры, вырабатывается пользователем.

Запросы к удостоверяющему центру на выпуск сертификатов формируются в соответствии с PKCS#10 и подписываются с использованием закрытого ключа, соответствующего открытому ключу, содержащемуся в запросе.

Открытые ключи ЭП и запросы записываются на ключевые носители в открытом виде.

При формировании контейнеров PKCS#15 и запросов PKCS#10 используются следующие стандарты, алгоритмы и форматы:

- шифрование и имитозащита в соответствии с требованиями ГОСТ 28147-89;
- формирование и проверка ЭП в соответствии с требованиями ГОСТ 34.11- 2012 и ГОСТ Р 34.10-2012.

Получаемые в результате работы МГК-3 ключевая пара и запрос на сертификат соответствуют Инфраструктуре Открытых Ключей, а именно, международным стандартам и рекомендациям X.509, RFC 3280, RFC 2314 (PKCS#10), RFC 4491, PKCS#15 с поддержкой российских криптоалгоритмов, а также следующим нормативным документам:

- Федеральному закону РФ от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;
- Приказу ФСБ РФ от 27 декабря 2011 г. № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи».

Генерация ключевой информации происходит с помощью биологического датчика случайных чисел (ДСЧ). Во время выполнения программы имеется возможность генерации нескольких пар ключей для различных пользователей без переинициализации ДСЧ.

Результатом работы программы являются:

1. Ключевая информация, сгенерированная программой и записанная на ключевой носитель.

   Закрытый ключ (и необходимая для его использования информация) размещается на ключевом носителе в т.н. «контейнере» («контейнере закрытого ключа»).
2. Запрос на выпуск обычного или квалифицированного сертификата ключа, записанный либо на ключевой носитель, либо на отдельный носитель, предназначенный для передачи в Удостоверяющий Центр.

При условии соблюдения правил пользования МГК-3 обеспечивает защиту информации по классам:

- КС1 при обычном использовании;
- КС2 при наличии АПМДЗ (аппаратно-программного модуля доверенной загрузки), сертифицированного по классу 3Б или выше по требованиям ФСБ России;
- КС3 при использовании АПМДЗ, сертифицированного по классу 3Б или выше по требованиям ФСБ России, и Программы «DiCheck» RU.НКБГ.70018-01, обеспечивающей возможность создания замкнутой среды функционирования.

Примечание – описание Программы «DiCheck» содержится в документе «Программа создания замкнутой среды «DiCheck» Руководство по настройке» RU.НКБГ.70018-01 90».

2. Условия применения программы МГК-3

Программа МГК-3 обеспечивает выполнение решаемых ею задач при соблюдении требований, содержащихся в следующих документах: «СКЗИ Модуль генерации ключей «МГК-3» Правила пользования» RU.НКБГ.70010-02 90 и «СКЗИ Модуль генерации ключей «МГК-3» Формуляр» RU.НКБГ.70010-02 30.

2.1. Требования к оборудованию и операционной среде

СКЗИ «МГК-3» функционирует на IBM-совместимом компьютере под управлением 32-разрядных и 64-разрядных версий операционных систем WINDOWS XP, WINDOWS 2003 Server, WINDOWS 2003 Server R2, WINDOWS Server 2008, WINDOWS Vista, WINDOWS Server 2008 R2, WINDOWS 7, WINDOWS Server 2012, WINDOWS 8, WINDOWS 8.1, WINDOWS 10.

Компьютер должен быть оснащен устройством для считывания съемных носителей (USB-порт и проч.).

2.2. Ключевые носители

В качестве ключевых носителей могут быть использованы любые носители, которые ОС WINDOWS может определить как съемные и перезаписываемые (Flash-накопители и.т.п.). В качестве ключевых носителей также могут использоваться устройства ruToken или eToken.

Перед использованием ключевые носители должны быть очищены от посторонней информации.

Ключевой носитель содержит закрытую информацию. Пользователь должен обеспечить его надежное хранение. КАТЕГОРИЧЕСКИ запрещается модифицировать содержимое ключевого носителя. В то же время на носителе не должна быть установлена защита от записи. Условия хранения и использования ключевых носителей должны соответствовать документу «СКЗИ Модуль генерации ключей «МГК-3» Правила пользования» RU.НКБГ.70010-02 90.

2.3. Установка МГК-3

МГК-3 поставляется в виде дистрибутивного пакета на одном носителе (на компакт-диске), который содержит программу установки МГК-3 **SETUP.EXE**.

Для инсталляции МГК-3 пользователь должен обладать правами администратора ОС WINDOWS.

Инсталляция МГК-3 состоит из установки основного ПО (собственно МГК-3) и, при необходимости, установки дополнительного программного обеспечения поддержки носителей eToken и/или ruToken.

> *Внимание* - Если на компьютере уже установлена программа МГК-3, то ее необходимо предварительно деинсталлировать с помощью программы **Uninstall Модуль генерации ключей** (ярлык программы находится в той папке стартового меню WINDOWS, куда он был помещен в процессе предыдущей инсталляции МГК-3).

Для инсталляции МГК-3 необходимо пройти через последовательность шагов, отвечая на задаваемые вопросы.

В процессе инсталляции (Рис. 1) будет запрошена папка для размещения МГК-3. Предлагается поддиректория в стандартной системной директории: **<**Системный диск**>\Program Files(x86)\Factor-TS\Request3**, название которой без необходимости менять не рекомендуется.

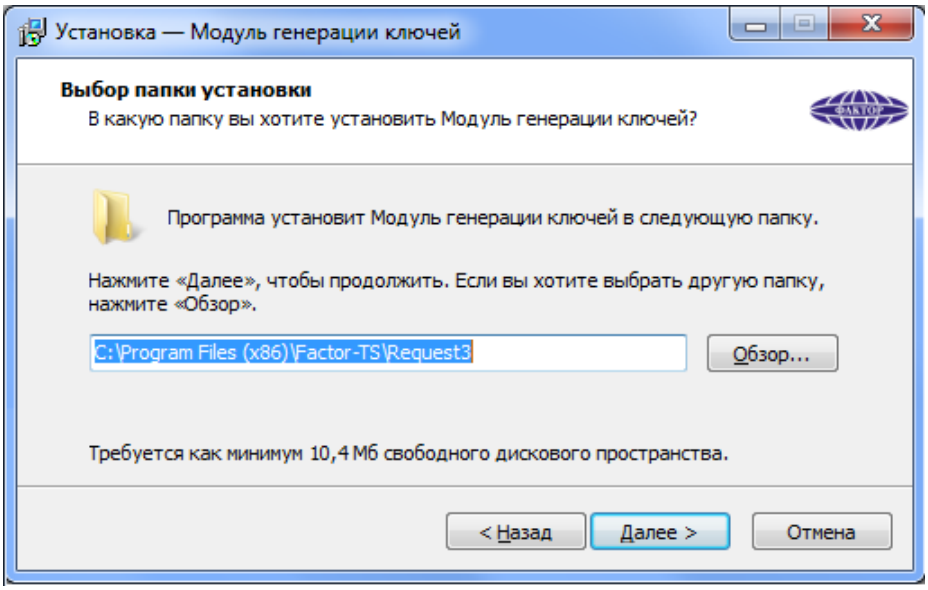

Рис. 1

На следующем шаге (Рис. 2) запрашивается название папки в стартовом меню WINDOWS, в которую будут помещены ярлыки для запуска основной программы (**Модуль генерации ключей МГК-3**) и для запуска служебных программ (**Контрольные суммы** и программа **Uninstall Модуль генерации ключей**). Для папки предлагается название **`FACTOR Applications\Модуль генерации ключей 3.0`**.

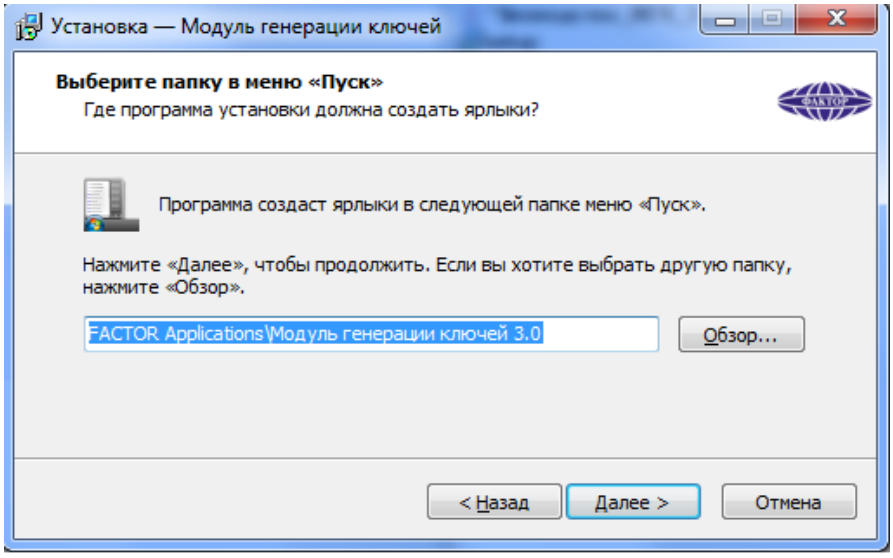

Рис. 2

Затем, как показано на Рис. 3, на экран выводится окно с перечнем выбранных пользователем параметров:

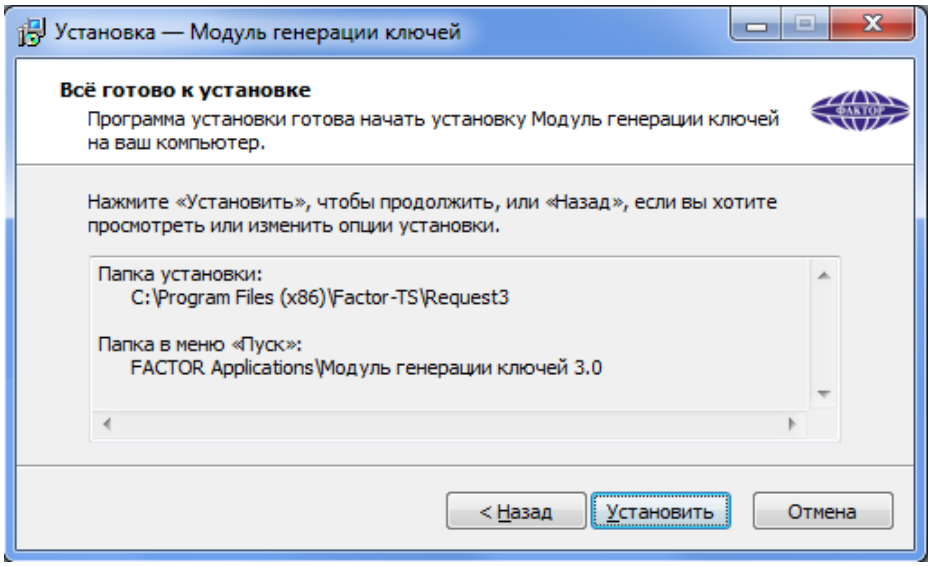

Рис. 3

После нажатия кнопки **`Установить`** будет выполнена инсталляция.

В состав программного обеспечения МГК-3 входят:

- программа генерации ключей и запросов на сертификат **Модуль генерации ключей МГК-3** (**`request.exe`**);
- программа проверки целостности ПО **CHECKWIN.EXE** и список файлов программного обеспечения, подлежащих проверке, вместе с эталонными значениями контрольных сумм. Эталонные значения контрольных сумм приведены в документе «СКЗИ Модуль генерации ключей «МГК-3». Формуляр» RU.НКБГ.70010-02 30;
- программа удаления модуля генерации ключей **Uninstall Модуль генерации ключей** (**`unins000.exe`**) и соответствующий конфигурационный файл **`unins000.dat`**;
- конфигурационный файл **`request.ini`**;
- библиотеки программных модулей (**`*.dll`**).

По окончании инсталляции будет выдано окно с запросом на запуск программы проверки контрольных сумм (Рис. 4).

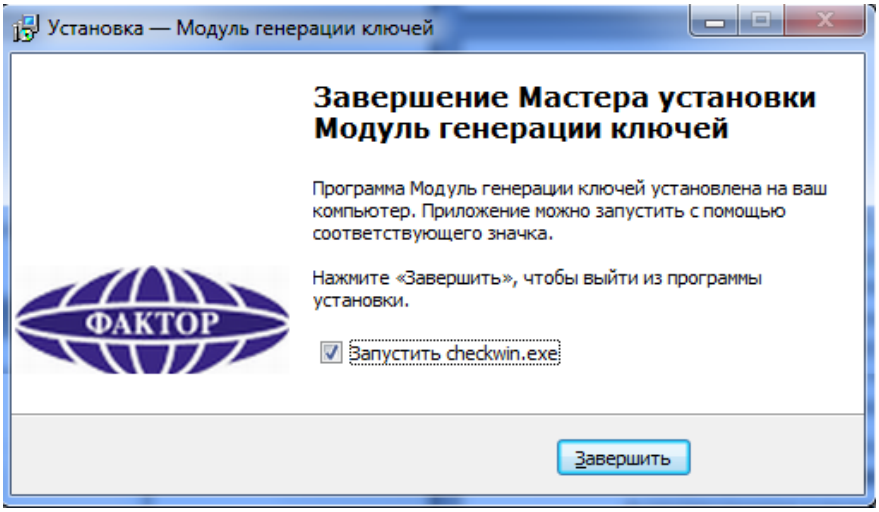

Рис. 4

Примечание. Если предполагается работа с носителями eToken и ruToken, на ПЭВМ пользователя должно быть установлено ПО поддержки (драйверы) этих носителей.
Версии ПО драйверов носителей:

- для eToken – **RTE_3.66**, **eToken PKI Client 5.1 SP1 для Microsoft Windows** (доступно на официальном сайте http://www.aladdin-rd.ru);
- для ruToken – **rtDrivers.x64/x86.v.2.85.00.0444** (доступно на официальном сайте http://www.rutoken.ru).

2.4. Проверка контрольных сумм МГК-3

При первом включении МГК-3 пользователь должен выполнить проверку целостности полученного программного обеспечения: вызвать программу проверки контрольных сумм из стартового меню WINDOWS (**Пуск ⇨ Программы ⇨ FACTOR Applications ⇨ Модуль генерации ключей 3.0 ⇨ Checkwin**). Программа **Checkwin** вычислит контрольные суммы на файлы, приведенные в списке, сравнит их с эталонными значениями и выведет на экран список проверенных файлов вместе со значениями контрольных сумм.

Примечание - при первом включении МГК-3 пользователь должен визуально убедиться в идентичности значений контрольных сумм, выведенных на экран, и контрольных сумм, содержащихся в формуляре).

Если суммы совпадут, то программа выдаст сообщение, что контрольные суммы проверены успешно.

Если будет обнаружено несовпадение, то программа укажет файл, для которого имеет место ошибка контрольной суммы. В этом случае требуется обязательная замена программного обеспечения.

Можно задать автоматический вызов программы проверки контрольных сумм сразу после инсталляции, установив в окне на Рис. 4 флажок **Запустить checkwin.exe**.

В дальнейшем следует периодически при запуске МГК-3 проводить контроль целостности ПО. Периодичность проверки зависит от условий эксплуатации и определяется политикой безопасности эксплуатирующей организации. Периодический контроль можно выполнять так же, как и при первом включении, с помощью программы **CHECKWIN.EXE**.

В составе МГК-3, обеспечивающего защиту по классам КС2 и КС3, используется средство доверенной загрузки (АПМДЗ), в таких изделиях контроль целостности ПО выполняется этим средством (при соответствующей настройке) автоматически при каждом включении ПЭВМ, на которой функционирует МГК-3.

В составе МГК-3, обеспечивающего защиту по классу КС3, используется средство для создания функционально замкнутой среды (ПО «DiCheck»). При первом включении такого изделия пользователь должен выполнить проверку целостности ПО «DiCheck». Порядок проверки рассмотрен в документе «Программа создания замкнутой среды «DiCheck» RU.НКБГ.70018-01 90». Все контролируемые файлы ПО «DiCheck» должны быть включены в список проверяемых файлов АПМДЗ.

3. Генерация ключей и запросов на сертификаты

Генерация ключей пар и формирование запросов на выпуск сертификатов ключа (обычных или квалифицированных) могут выполняться пользователем ПО МГК на своем рабочем месте или специально назначенным для этих работ оператором в зависимости от принятого в организации регламента.

После запуска программы на экран будет выведено главное окно **Модуль генерации ключей** с формой, содержащей исходные данные, необходимые для формирования ключей и запросов на сертификаты (Рис. 5).

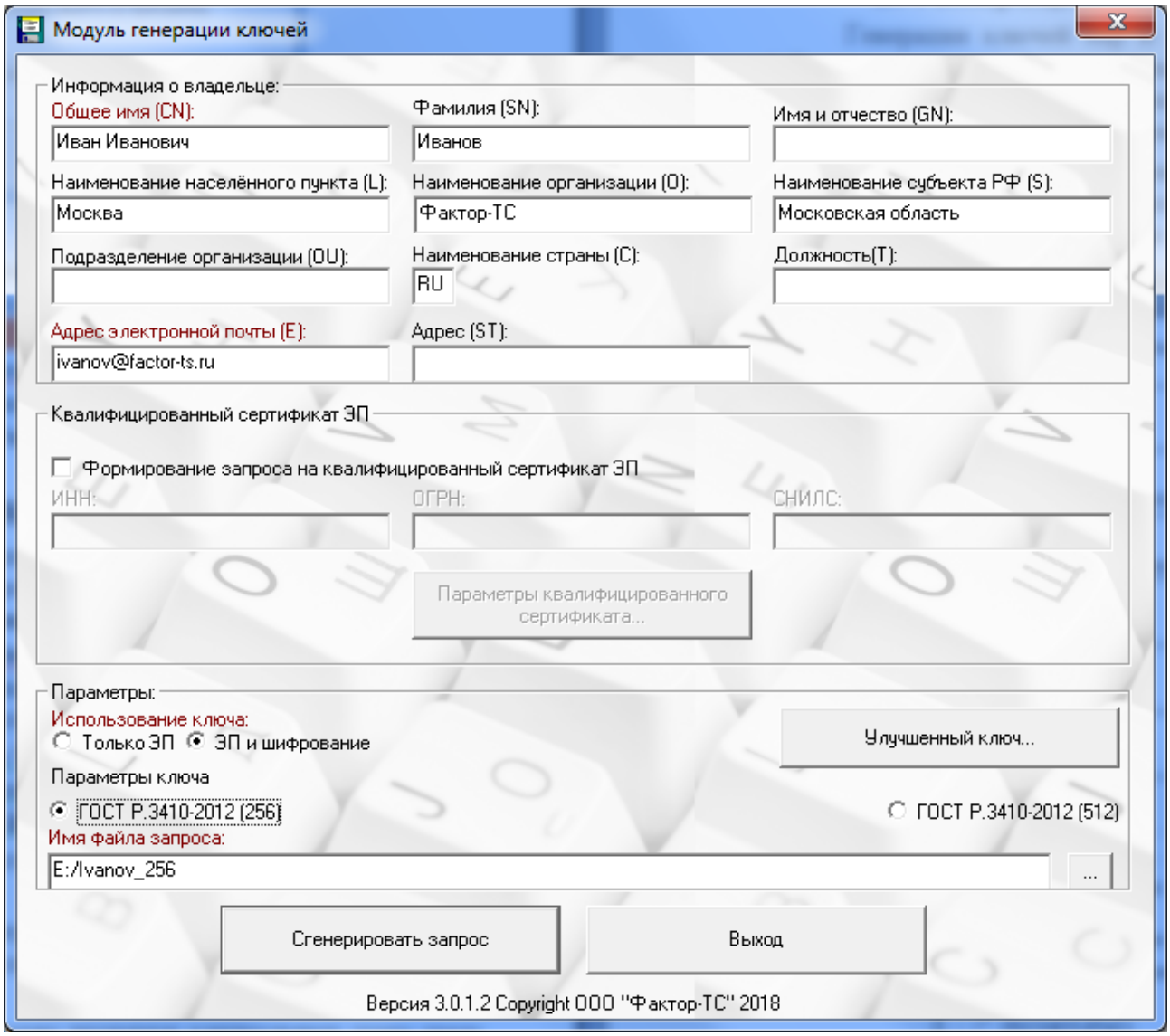

Рис. 5

Примечание. Набор полей, доступных и заблокированных, обязательных и необязательных для заполнения, в окне **Модуль генерации ключей** (Рис. 5 или Рис. 8), задается в конфигурационном файле **`request.ini`**, помещенном в директорию установки программы (см. раздел 4.1, с. 20). Состав полей может быть изменен администратором Удостоверяющего Центра на основе собственной политики выдачи сертификатов, после чего соответствующая информация должна быть занесена пользователем МГК в конфигурационный файл **`request.ini`**.

Названия обязательных для заполнения полей выводится на экране красным цветом

Перед запуском процесса генерации ключевой пары необходимо выполнить следующие подготовительные операции.

1. Заполнение формы с исходными данными: ввод идентификационных данных о владельце сертификата, выбор необходимых значений параметров для сертификата и указание месторасположения файла, который будет содержать запрос на сертификат (см. раздел 3.1, с. 10).
2. Инициализация биологического датчика случайных чисел (раздел 3.2, с. 16).

3. Выбор съемного ключевого носителя для записи закрытого ключа вместе с дополнительной информацией (раздел 3.3, с. 17).

Далее следует собственно работа МГК-3 по генерации ключевой пары и формированию запроса на сертификат, запись закрытого ключа и дополнительной информации на выбранный съемный носитель и запись запроса на сертификат в указанное на этапе первой подготовительной операции место (раздел 3.4, с. 18).

3.1. Заполнение формы с исходными данными

Поля под заголовком **Информация о владельце** (Рис. 5)

Группа полей задает основную информацию о владельце сертификата.
Группа имеет два обязательных для заполнения поля:

- **Общее имя[CN]** – имя, фамилия (отчество, если имеется) физического лица или название юридического лица - владельца сертификата;
- **Адрес электронной почты[E]** – адрес электронной почты владельца сертификата; в качестве адреса электронной почты должен быть указан реальный работающий адрес, который необходим как для контактов участников информационного обмена с владельцем сертификата, так и для работы с почтовыми агентами (например, **DioPost**).

Назначения остальных полей (не обязательных для заполнения) в данной группе следующие:

- **Фамилия[SN]** – фамилия физического лица, владельца сертификата;
- **Имя и отчество[GN]** – имя и отчество физического лица, владельца сертификата;
- **Наименование организации[O]** — название юридического лица;
- **Подразделение организации[OU]** — наименование подразделения юридического лица;
- **Должность[T]** — наименование должности владельца сертификата;
- **Адрес[ST]** – адрес места нахождения физического или юридического лица (владельца сертификата), включающий название улицы, номер дома, корпуса, строения, квартиры, помещения;
- **Наименование населённого пункта[L]** — название соответствующего населенного пункта;
- **Наименование субъекта РФ[S]** – название соответствующего субъекта Российской Федерации;
- **Наименование страны[C]** — двух символьный код страны проживания владельца сертификата (значение по умолчанию **RU** — Россия).

Поля под заголовком **Параметры** (Рис. 5).

Переключатель **Использование ключа –** в зависимости от выбранного значения переключателя сгенерированный ключ сможет поддерживать:

- **Только ЭП** – только одну функцию **–** «Формирование ЭП»;
- **ЭП и шифрование** – две функции – «Формирование ЭП» и «Шифрование».

Переключатель **Параметры ключа** служит для выбора длины «контейнера закрытого ключа» формата PKCS#15.

Имя файла запроса (обязательный параметр) - в поле должно быть занесено имя файла (с указанием полного пути), в который будет записан сгенерированный запрос на сертификат. Файл можно выбрать при помощи кнопки обзора файловой системы компьютера (кнопка справа от поля с именем файла).

В частности, для размещения файла можно указать тот же съемный носитель, который предназначен для хранения закрытого ключа (см. раздел 3.3, с. 17).

Примечание. Рекомендованное расширение имени данного файла - **req**, оно добавляется автоматически.

Улучшенный ключ (обязательный параметр) – после нажатия кнопки на экране появится окно **Выбор параметров** (Рис. 6) с таблицей, содержащей параметры использования ключа.

В *первом столбце* таблицы (под заголовком **Имя**) выводится название параметра, определяющего, область использования ключа.

Во *втором столбце* (под заголовком **OID-Object Identifier**) - значение идентификатора OID, соответствующего области использования ключа.

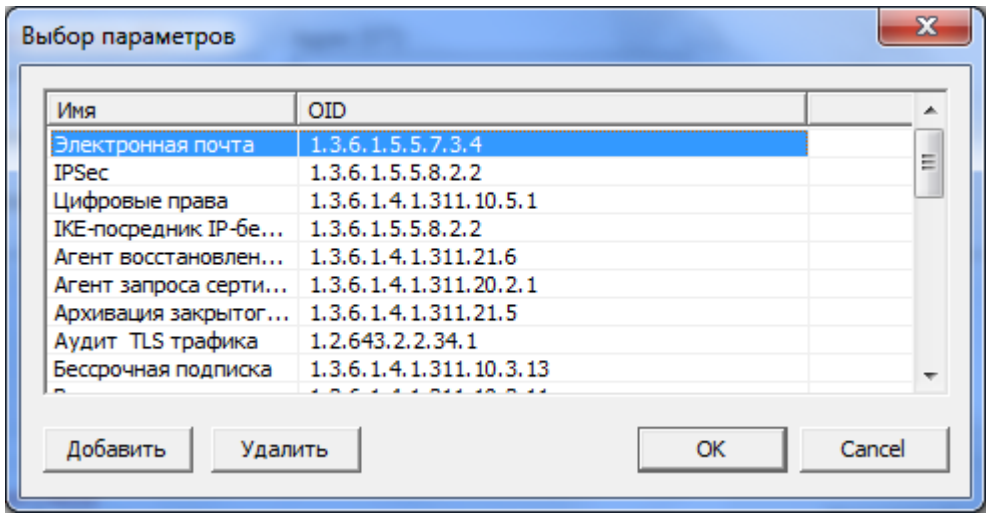

Рис. 6

Полный список параметров приведен в конфигурационном файле **request.ini** (см. раздел 4.1, с. 20).

Необходимо выбрать один или несколько параметров и нажать кнопку **ОК**. Для выбора нескольких параметров следует нажать клавишу <Ctrl> и, удерживая ее нажатой, выделить требуемые элементы в списке.

Для удаления параметра из списка следует выбрать элемент и нажать кнопку **Удалить.**

Если в списке нет требуемого параметра использования ключа, его можно добавить вручную. При нажатии на кнопку **Добавить** (Рис. 6) появляется диалоговое окно **OID** с двумя полями: **Название** и **Значение OID** (Рис. 7).

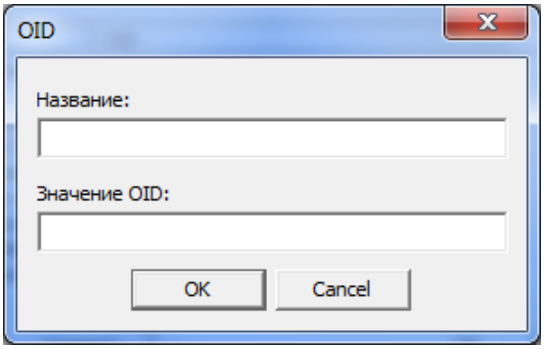

Рис. 7

Примечание. Дополнительные идентификаторы OID-параметров использования выбираются из числа стандартных или введенных в организации после регистрации уникального номера OID. Получение номера OID для организации может быть осуществлено путем подачи заявки в Агентство по выделению имен и уникальных параметров протоколов Internet (IANA – Internet Assigned Numbers Authority). Регистрация частного номера организации в российском сегменте мирового пространства идентификаторов осуществляется Уполномоченным федеральным органом исполнительной власти РФ по применению ЭП.

Следует заполнить поля и нажать кнопку **ОК**, после чего созданный параметр будет внесен в список в окне **Выбор параметров** (Рис. 6) и станет доступным для выбора пользователем.

Если необходимо сформировать запрос на неквалифицированный сертификат, то на этом заполнение формы с исходными данными (Рис. 5) заканчивается и следует переходить к действиям, описанным в разделе 3.2, с. 16.

Если требуется сформировать запрос на квалифицированный сертификат, то надо в окне Рис. 5 установить флажок **Формирование запроса на квалифицированный сертификат**, после чего окно **Модуль генерации ключей** приобретает вид, показанный на Рис. 8.

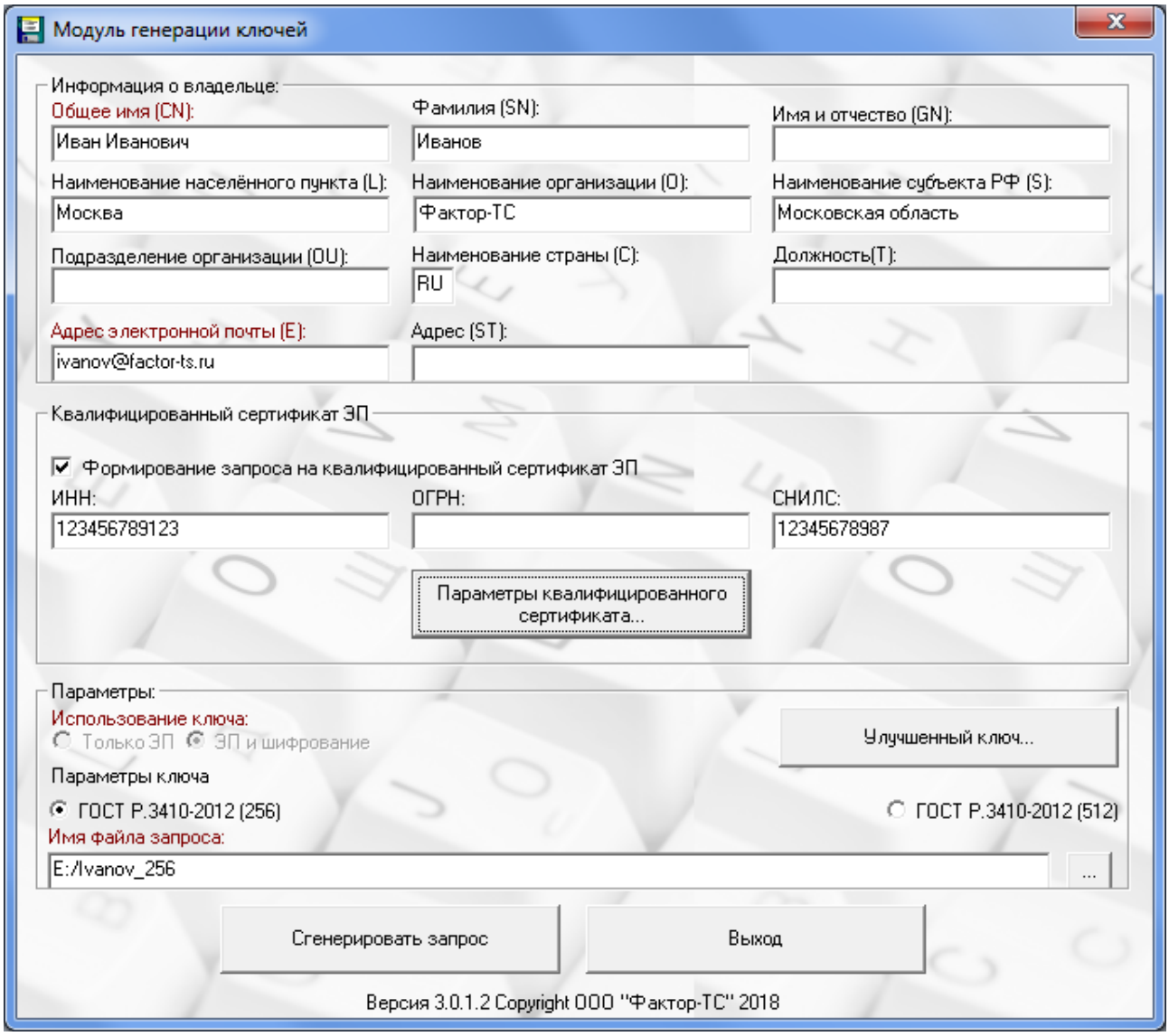

Рис. 8

В группе под заголовком **Параметры** переключатель **Использование ключа** становится неактивным.

В группе параметров под заголовком **Информация о владельце** становятся активными поля:

- **ИНН** – идентификационный номер налогоплательщика, владельца квалифицированного сертификата;
- **ОГРН** – основной государственный регистрационный номер владельца квалифицированного сертификата (для юридических лиц);
- **СНИЛС** – страховой номер индивидуального лицевого счета владельца квалифицированного сертификата.

Становится активной кнопка **Параметры квалифицированного сертификата**. Нажатие кнопки приводит к открытию одноименного окна с формой, предназначенной для ввода информации, необходимой для создания квалифицированного сертификата (Рис. 9).

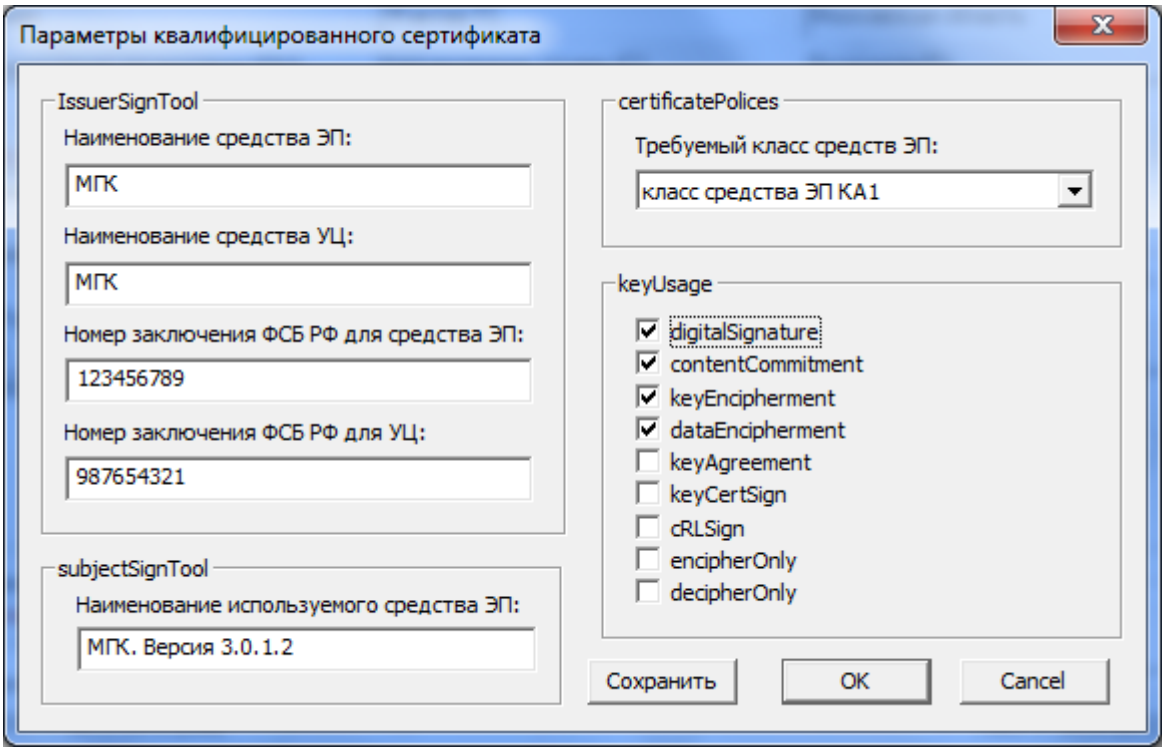

Рис. 9

В группу параметров под заголовком **IssuerSignTool** включены следующие поля, обязательные для заполнения:

- **Наименование средства ЭП** – наименование средства, которое было использовано для создания ключа ЭП, ключа проверки ЭП и квалифицированного сертификата;
- **Наименование средства УЦ** - наименование средства, которое было использовано на аккредитованном УЦ для создания ключа ЭП, ключа проверки ЭП и квалифицированного сертификата;
- **Номер заключения ФСБ РФ для средства ЭП** – реквизиты заключения ФСБ России о подтверждении соответствия указанного выше средства ЭП требованиям, установленным в соответствии с Федеральным законом;
- **Номер заключения ФСБ РФ для УЦ** – реквизиты заключения ФСБ России о подтверждении соответствия указанного выше средства УЦ требованиям, установленным в соответствии с Федеральным законом.

Под заголовком **subjectSignTool** расположено поле (не обязательное для заполнения) **Наименование используемого средства ЭП**, в которое заносится наименование средства ЭП, используемое владельцем сертификата.

Под заголовком **certificatePolices** расположено поле (обязательное для заполнения) **Требуемый класс средств ЭП**.

Из раскрывающегося списка следует выбрать класс средства, которое будет использоваться:

- **класс средства ЭП КС1**
- **класс средства ЭП КС2**
- **класс средства ЭП КС3**

- **класс средства ЭП КВ1**
- **класс средства ЭП КВ2**
- **класс средства ЭП КА1**

Группа флажков под заголовком **keyUsage** позволяет определить области использования ключа проверки квалифицированной ЭП, установив флажок около одного или нескольких значений из списка:

- **digitalSignature** — область использования ключа включает проверку ЭП под электронными документами, отличными от квалифицированных сертификатов и списков уникальных номеров квалифицированных сертификатов ключей ЭП, действие которых на определенный момент было прекращено УЦ до истечения их действия (далее — список аннулированных сертификатов), предназначенными для выполнения процедур аутентификации или контроля целостности;
- **contentCommitment** — область использования ключа включает проверку ЭП под электронными документами, отличными от квалифицированных сертификатов и списков аннулированных сертификатов, в отношении которых ставится задача обеспечения невозможности отказа подписавшего лица от своего действия;
- **keyEncipherment** — область использования ключа включает зашифрование закрытых или секретных ключей, например, в целях их защищенной доставки;
- **dataEncipherment** — область использования ключа включает непосредственно зашифрование пользовательских данных без дополнительного использования методов симметричной криптографии;
- **keyAgreement** — область использования ключа включает согласование ключей;
- **keyCertSign** — область использования ключа включает проверку подписей под квалифицированными сертификатами;
- **cRLSign** — область использования ключа включает проверку подписей под списками аннулированных сертификатов;
- **encipherOnly** — область использования ключа включает зашифрование данных в процессе согласования ключей (при выборе данного пункта автоматически устанавливается флажок **keyAgreement**);
- **decipherOnly** — область использования ключа включает расшифрование данных в процессе согласования ключей (при выборе данного пункта автоматически устанавливается флажок **keyAgreement**).

Если не выбрать ни одной области использования ключа, то при попытке дальнейшей работы (см. ниже, раздел 3.2 с. 16) будет выдано предупреждающее сообщение о том, что данные о желаемых областях использования не будут помещены в запрос на квалифицированный сертификат.

Заполнив все поля в окне **Параметры квалифицированного сертификата** (Рис. 9) следует нажать кнопку **Сохранить**, при этом появится предупреждающее сообщение (Рис. 10). Для того чтобы выполнить запись, нужно закрыть окно нажатием кнопки **Да**.

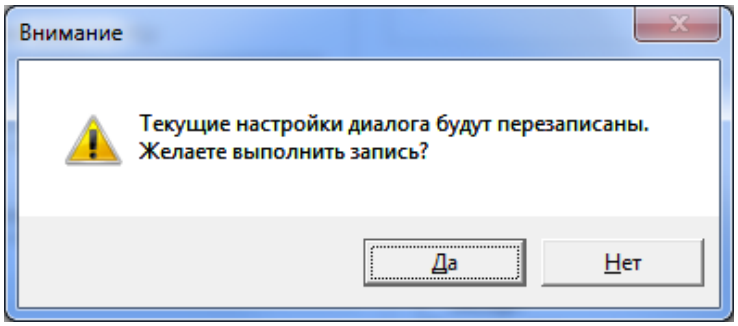

Рис. 10

Замечании.: Для сохранения настроек МГК-3 должен быть открыт с параметром «**Запуск от имени администратора**».

При нажатии кнопки **Cancel** программа возвращается в главное окно (Рис. 8) без изменения настроек.

Параметры квалифицированного сертификата сохраняются в конфигурационном файле инициализации **request.ini** и при следующем запуске программы автоматически заносятся в поля окна **Параметры квалифицированного сертификата** (Рис. 9).

Обращаем Ваше внимание!

МГК-3 не позволит продолжить работу, если не будут заполнены обязательные поля в окне **Модуль генерации ключей** (Рис. 5 или Рис. 8), поля группы под заголовком **IssuerSignTool** в окне **Параметры квалифицированного сертификата** (Рис. 9), а также если не будет выбрано ни одного параметра использования ключа в окне **Выбор параметров** (Рис. 6). Программой будет выдано предупреждающее сообщение и предоставлена возможность ввести недостающие параметры.

3.2. Инициализация ПКДСЧ

После того как будут заполнены все необходимые поля, следует в окне **Модуль генерации ключей** (Рис. 5 или Рис. 8) нажать кнопку **Сгенерировать запрос**.

Программа предложит выполнить инициализацию датчика случайных чисел. Для прохождения процедуры инициализации ДСЧ (Рис. 11), необходимо перемещать курсор мыши на экране компьютера, желательно с максимальной амплитудой.

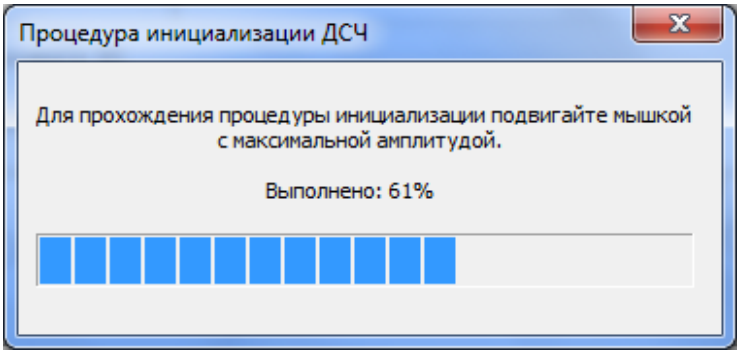

Рис. 11

В окне (Рис. 11) отображается индикатор процесса инициализации ДСЧ и процент выполнения процесса. До тех пор, пока инициализация не будет закончена, генерация ключевой пары и запроса на сертификат не начнется.

3.3. Выбор носителя

После успешного завершения инициализации ДСЧ на экран будет выведено окно **Выберите носитель** (Рис. 12) со списком носителей, позволяющее выбрать съемный носитель для записи закрытого ключа (и дополнительной информации).

Если ни одного устройства для записи закрытого ключа не установлено, то список носителей пуст. Для продолжения работы необходимо установить устройство для записи и в окне **Выберите носитель** (Рис. 12) нажать кнопку **Повтор**.

В *первом столбце* таблицы (под заголовком **Носитель**) для носителей НГМД и Flash-памяти выводится системное имя считывающего устройства; для носителей типа eToken – последовательность символов, которая начинается с **AKS ifdh**, и далее следует его порядковый номер; для носителей типа ruToken – последовательность символов, которая начинается с **Aktiv Co.ruToken**, и далее следует его порядковый номер.

Пользователь должен выделить строчку с нужным устройством и нажать кнопку **Выбрать**.

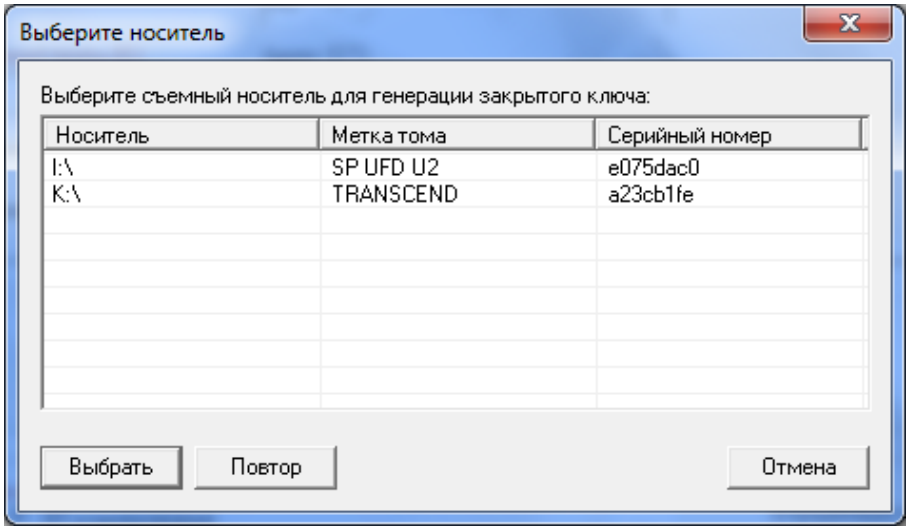

Рис. 12

1. Если выбран носитель eToken или ruToken, на экран выводится окно (Рис. 13) для ввода пароля (пароль устанавливает производитель носителя, в дальнейшем пользователь может изменить пароль).

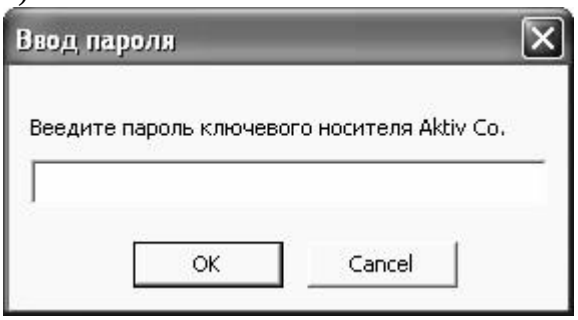

Рис. 13

Следует ввести пароль и нажать кнопку ОК. При вводе ошибочного пароля на экран будет выведено сообщение об ошибке, процедура генерации заканчится и на экране активизируется главное окно (Рис. 5 или Рис. 8).

При нажатии кнопки **Cancel** программа выдаст сообщение о том, что операция генерации ключевого носителя прервана, и вернется в главное окно.

2. При выборе носителя Flash-накопителя будет выдан запрос, позволяющий установить пароль на ключевой носитель (Рис. 14). Пароль устанавливать не обязательно.

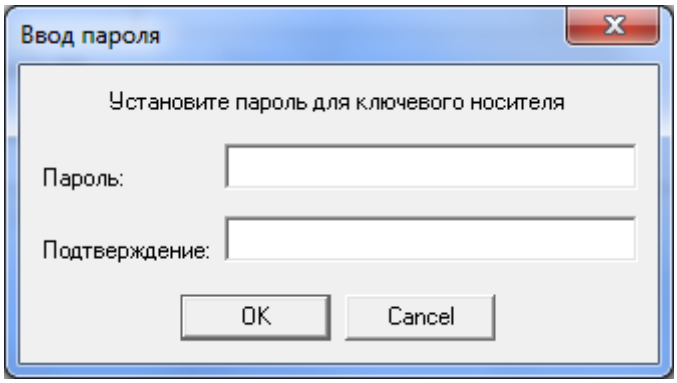

Рис. 14

Если пароль будет установлен, то система будет требовать ввода этого пароля каждый раз при обращении к ключевому носителю. В дальнейшем пароль НЕЛЬЗЯ ни заменить, ни отменить.

Вне зависимости от того, будете Вы устанавливать пароль на ключевой носитель или нет, для продолжения работы из последнего окна (Рис. 14) необходимо выходить нажатием кнопки **ОК**.

При нажатии кнопки **Cancel** программа выдаст сообщение о том, что операция генерации ключевого носителя прервана оператором, и вернется в главное окно.

3.4. Генерация ключевой пары и запроса на сертификат

После выбора носителя программа МГК-3 выполняет следующие действия:

- генерирует ключевую пару;
- записывает закрытый ключ с дополнительной информацией на выбранный съемный носитель;
- записывает в указанный файл - **Имя файла запроса** (Рис. 5 или Рис. 8) - запрос на сертификат, включающий в себя открытый ключ, информацию о выбранных пользователем параметрах ключа и другую информацию;
- выдает на экран сообщение об успешном формировании запроса на сертификат и возвращается в главное окно **Модуль генерации ключей** (Рис. 5 или Рис. 8).

Для завершения работы, если требуется сгенерировать только одну ключевую пару (и запрос на сертификат), следует нажать кнопку **Выход** (Рис. 5 или Рис. 8) и выйти из программы.

Для генерирования новой ключевой пары (и нового запроса на сертификат) необходимо внести изменения в полях формы (Рис. 5 или Рис. 8), при этом необходимо обязательно ввести новое имя файла для размещения запроса на сертификат (иначе прежний запрос на сертификат будет утерян) и нажатием кнопки **Сгенерировать запрос** запустить новый процесс.

При генерации второй и последующих ключевых пар инициализация ДСЧ не требуется. Она необходима только при повторном запуске программы.

> *Обращаем Ваше внимание!* При повторной генерации ключей без изменения данных в полях формы (Рис. 5 или Рис. 8) полученная ключевая пара будет отличаться от предыдущей.

На один ключевой носитель рекомендуется записывать только один закрытый ключ. После выполнения программы МГК-3 на ключевом носителе (если в качестве него выбран Flash-накопитель) будут размещены файлы с именами, имеющими одинаковую основную часть имени и различные расширения (основная часть имен файлов - <идентификатор_ключа> – задается ДСЧ):

- <идентификатор_ключа>**.p15 –** закрытый ключ и дополнительная информация, необходимая для его использования;
- <идентификатор_ключа>**.nam –** файл ссылки на контейнер закрытого ключа.

Если ключевым носителем служит Flash-накопитель, то на него можно поместить файл, содержащий запрос на сертификат. Для этого в главном окне (Рис. 5 или Рис. 8) в поле **Имя файла запроса** надо указать файл на данном носителе.

4. Входные и выходные данные

4.1. Входные данные

Входными данными для программы МГК-3 являются.

1. Информация, введенная пользователем программы в форму ввода главного окна программы (Рис. 5 или Рис. 8).
2. Данные, вводимые пользователем в ответ на запросы программы, такие как выбор ключевого носителя, а также данные, необходимые для инициализации биологического датчика случайных чисел и т.п.
3. Файл инициализации **request.ini**.

Состав файла инициализации

Файл **request.ini**, входящий в состав МГК-3, служит для заполнения полей формы в главном окне (Рис. 5 или Рис. 8). Этот файл является изменяемым и может заполняться и распространяться, например, администратором Удостоверяющего Центра. Пользователь может редактировать содержимое файла, учитывая рекомендации администратора Удостоверяющего Центра.

Файл **request.ini** изначально имеет следующий вид:

```
[General]
CommonName=1   // Общее имя
Surname=0      // Фамилия
GivenName=0    // Имя и отчество
localityName=0           // Наименование населённого пункта
stateOrProvinceName=0    // Наименование субъекта РФ
organizationName=0       // Наименование организации
organizationalUnitName=0 // Подразделение организации
title=0                  // Должность
countryName=0            // Наименование страны
streetAddress=0          // Адрес
emailAddress=1           // Адрес электронной почты
INN=0                    // ИНН
OGRN=0                   // ОГРН
SNILS=0                  // СНИЛС
<жжжжж
EPName=                  // Наименование средства ЭП
CAName=                  // Наименование средства УЦ
ZakAttributesEP=    // Номер заключения ФСБ РФ для средства ЭП
ZakAttributesCA=    // Номер заключения ФСБ РФ для УЦ
SubjectSignToolName= // Наименование используемого средства ЭП
EPClassCheck=5      // Требуемый класс средств ЭП
CAClassCheck=0      //
LastUsages=27       // Параметры использования ключа
```

```
Usages0=1      // Область использования ключа проверки ЭП
Usages1=1
Usages2=1
Usages3=1
Usages4=0
Usages5=0
Usages6=0
Usages7=0
Usages8=0

//Соответствие полей RFC 5280
[rfc5280]
CommonNameSz=1
SurnameSz=1
GivenNameSz=1
localityNameSz=1
stateOrProvinceNameSz=1
organizationNameSz=1
organizationalUnitNameSz=1
titleSz=1
countryNameSz=1
emailAddressSz=1
streetAddressSz=1
INNSz=1
OGRNSz=1
SNILSSz=1

// Параметры использования ключа
[USAGE0]
Name=Электронная почта
Value=1.3.6.1.5.5.7.3.4
[USAGE1]
Name=IPSec
Value=1.3.6.1.5.5.8.2.2
[USAGE2]
Name=Цифровые права
Value=1.3.6.1.4.1.311.10.5.1
[USAGE3]
Name=IKE-посредник IP-безопасности
Value=1.3.6.1.5.5.8.2.2
[USAGE4]
Name=Агент восстановления ключей
```

```
Value=1.3.6.1.4.1.311.21.633
[USAGE5]
Name=Агент запроса сертификата
Value=1.3.6.1.4.1.311.20.2.1
[USAGE6]
Name=Архивация закрытого ключа
Value=1.3.6.1.4.1.311.21.5
[USAGE7]
Name=Аудит  TLS трафика
Value=1.2.643.2.2.34.1
[USAGE8]
Name=Бессрочная подписка
Value=1.3.6.1.4.1.311.10.3.13
[USAGE9]
Name=Восстановление ключа
Value=1.3.6.1.4.1.311.10.3.11
[USAGE10]
Name=Восстановление файлов
Value=1.3.6.1.4.1.311.10.3.4.1
[USAGE11]
Name=Встроенная проверка системных компонентов Windows
Value=1.3.6.1.4.1.311.10.3.8
[USAGE12]
Name=Вход со смарт картой
Value=1.3.6.1.4.1.311.20.2.2
[USAGE13]
Name=Квалифицированное подчинение
Value=1.3.6.1.4.1.311.10.3.10
[USAGE14]
Name=Конечная система IP-безопасности
Value=1.3.6.1.5.5.7.3.5
[USAGE15]
Name=Лицензии пакета ключей
Value=1.3.6.1.4.1.311.10.6.1
[USAGE16]
Name=Окончание туннеля IP-безопасности
Value=1.3.6.1.5.5.7.3.6
[USAGE17]
Name=Подписывание документа
Value=1.3.6.1.4.1.311.10.3.12
[USAGE18]
Name=Подписывание кода
```

```
Value=1.3.6.1.5.5.7.3.3
[USAGE19]
Name=Подписывание списка доверия (Microsoft)
Value=1.3.6.1.4.1.311.10.3.1
[USAGE20]
Name=Подпись корневого списка
Value=1.3.6.1.4.1.311.10.3.9
[USAGE21]
Name=Подпись ответа службы OCSP
Value=1.3.6.1.5.5.7.3.9
[USAGE22]
Name=Пользователь IP-безопасности
Value=1.3.6.1.5.5.7.3.7
[USAGE23]
Name=Почтовая репликация службы каталогов
Value=1.3.6.1.4.1.311.21.19
[USAGE24]
Name=Проверка подлинности клиента
Value=1.3.6.1.5.5.7.3.2
[USAGE25]
Name=Проверка подлинности сервера
Value=1.3.6.1.5.5.7.3.1
[USAGE26]
Name=Проверка сервера лицензий
Value=1.3.6.1.4.1.311.10.6.2
[USAGE27]
Name=Установка штампа времени
Value=1.3.6.1.5.5.7.3.8
```

В разделе `General` данного файла:

- обязательные для заполнения поля получают значение `1`,
- необязательные – `0`,
- неактивные (поля, не доступны для заполнения) – `2`.

В разделе `rfc5280` файла **`request.ini`**:

- поля, для которых проводится контроль длины в соответствии с RFC 5280, получают значение `1`,
- поля, для которых контроль длины не проводится, получают значение `0`.

Внимание! Установка `0` в значении полей может привести к несовместимости запроса и сертификата с различными продуктами.

Названия о*бязательных* для заполнения полей выводятся в главном окне (Рис. 5 или Рис. 8) красным цветом шрифта, *неактивные* поля затемнены, и их заполнение невозможно.

4.2. Выходные данные

Выходными данными программы являются:

3. Ключевая информация, сгенерированная программой и записанная на ключевой носитель. Состав ключевой информации приведен в разделе 3.4, с. 18.
4. Запрос на сертификат, предназначенный для передачи в Удостоверяющий Центр, записанный либо на ключевой носитель, либо на отдельный магнитный носитель.

Приложение. Список терминов

Термин	Определение
Аккредитация Удостоверяющего Центра	Признание уполномоченным федеральным органом соответствия Удостоверяющего Центра требованиям Федерального закона.
Владелец сертификата ключа проверки электронной подписи	Лицо, которому в установленном Федеральным законом порядке выдан сертификат ключа проверки электронной подписи (ЭП).
Закрытый ключ	Уникальная последовательность символов, известная только его владельцу, используемая при шифровании информации и/или для создания электронной подписи в электронных документах.
Квалифицированный сертификат ключа проверки электронной подписи (далее – квалифицированный сертификат)	Сертификат ключа проверки электронной подписи, выданный аккредитованным Удостоверяющим Центром или доверенным лицом аккредитованного Удостоверяющего Центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее – уполномоченный федеральный орган).
Ключ электронной подписи (ЭП)	Уникальная последовательность символов, предназначенная для создания ЭП.
Ключ проверки электронной подписи (ЭП)	Уникальная последовательность символов, однозначно связанная с ключом электронной подписи (ЭП) и предназначенная для проверки подлинности ЭП (далее – проверка ЭП).
Ключевая пара (несимметричная ключевая пара)	Пара, состоящая из закрытого ключа и соответствующего ему открытого ключа.
Ключевой носитель	Сменный носитель информации (дискета, flash-память и т.п.), содержащий ключевую информацию.
Открытый ключ	Уникальная последовательность символов: - однозначно соответствующая закрытому ключу, - доступная любому пользователю - участнику информационного обмена и предназначенная для подтверждения подлинности ЭП в электронных документах и/или для шифрования информации.
Датчик случайных чисел (ДСЧ)	Реализованный программным образом алгоритм выработки случайных последовательностей, учитывающий индивидуальные особенности использования пользователем МГК-3 манипулятора «мышь».
Сертификат ключа	Документ на бумажном носителе или электронный документ с электронной подписью уполномоченного лица Удостоверяющего Центра, который включает в себя открытый ключ и данные, идентифицирующие владельца сертификата ключа.
Сертификат ключа проверки электронной подписи (ЭП)	Электронный документ или документ на бумажном носителе, выданные Удостоверяющим Центром либо доверенным лицом Удостоверяющего Центра и подтверждающие принадлежность ключа проверки ЭП владельцу сертификата ключа проверки ЭП.
Средства Удостоверяющего Центра	Программные и (или) аппаратные средства, используемые для реализации функций Удостоверяющего Центра.
Средства электронной подписи (ЭП)	Шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций — созда-

Термин	Определение
	ние ЭП, проверка ЭП, создание ключа ЭП и ключа проверки ЭП.
Удостоверяющий Центр (УЦ)	Юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом: - создает сертификаты ключей проверки электронных подписей и выдает такие сертификаты лицам, обратившимся за их получением (заявителям); - устанавливает сроки действия сертификатов ключей проверки электронных подписей; - аннулирует выданные этим удостоверяющим центром сертификаты ключей проверки электронных подписей; - выдает по обращению заявителя средства ЭП, содержащие ключ ЭП и ключ проверки ЭП (в том числе созданные Удостоверяющим Центром) или обеспечивающие возможность создания ключа ЭП и ключа проверки ЭП заявителем; - ведет реестр выданных и аннулированных этим Удостоверяющим Центром сертификатов ключей проверки ЭП (далее - реестр сертификатов), в том числе включающий в себя информацию, содержащуюся в выданных этим Удостоверяющим Центром сертификатах ключей проверки ЭП, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных подписей и об основаниях таких прекращения или аннулирования; - устанавливает порядок ведения реестра сертификатов, не являющихся квалифицированными, и порядок доступа к нему, а также обеспечивает доступ лиц к информации, содержащейся в реестре сертификатов, в том числе с использованием информационно-телекоммуникационной сети "Интернет"; - создает по обращениям заявителей ключи электронных подписей и ключи проверки электронных подписей; - проверяет уникальность ключей проверки электронных подписей в реестре сертификатов; - осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей; - осуществляет иную деятельность, связанную с использованием ЭП.
Электронная подпись (ЭП)	Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образов связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Лист регистрации изменений

Номер изменения	Номера листов (страниц)				Всего листов (стр.) в документе	№ документа	Входящий № сопроводительного документа	Подпись	Дата
	измененных	замененных	новых	аннулированных					