УТВЕРЖДЕН

RU.НКБГ.70014-01И6

СКЗИ
Автоматизированное рабочее место генерации ключей
АРМ ГК-4

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата
2442	11.07.19	2033		

Руководство пользователя

RU.НКБГ.70014-01И6

(с учетом Извещений об изменении
НКБГ.142-18 от 26.04.2018 г. и № И57/Д от 04.02.2019)

Листов 41

Содержание

1. Общие положения

Средство криптографической защиты информации (СКЗИ) «Автоматизированное рабочее место генерации ключей АРМ ГК-4» RU.НКБГ.70014-01 версии 4.2 (далее – СКЗИ АРМ ГК-4 или АРМ ГК-4) предназначено для формирования ключевых носителей с ключевой информацией (мастер-ключом и ключами парной связи), необходимых для работы криптосредств разработки ООО «Фактор-ТС».

Данные криптосредства используют симметричные ключи и обеспечивают криптографическую защиту информации, не содержащей сведений, составляющих государственную тайну.

СКЗИ АРМ ГК-4 поддерживает изготовление ключей парной связи нескольких форматов (см. п. 1.1).

Изготовление ключей парной связи определённого формата должно быть согласовано с отделом криптографической защиты организации, эксплуатирующей криптосредства разработки ООО «Фактор-ТС».

СКЗИ АРМ ГК-4 класса КС1 функционирует как самостоятельное ПО и не требует использования дополнительных средств защиты информации (СЗИ), за исключением штатных средств ОС.

СКЗИ АРМ ГК-4 класса КС2 функционирует совместно с аппаратно-программным модулем доверенной загрузки (АПМДЗ). АПМДЗ должен иметь сертификат соответствия требованиям ФСБ России к АПМДЗ по классу «3Б» и обеспечивать защиту от несанкционированного доступа (НСД) с момента включения питания ПЭВМ до загрузки операционной системы.

СКЗИ АРМ ГК-4 класса КС3 функционирует совместно с АПМДЗ и программным модулем «Программа создания замкнутой среды DiCheck» RU.НКБГ.70018-01 (ПО DiCheck).

Примечание. Изделие класса КС2 включает функции изделия класса КС1, изделие класса КС3 включает функции изделия классов КС1, КС2.

При использовании СКЗИ АРМ ГК-4 по классу КС3 обязательна комиссионная работа не менее двух человек из числа лиц, допущенных к пользованию криптосредством.

1.1. Распределение ключей с использованием симметричной ключевой системы

Алгоритм шифрования по ГОСТ 28147-89 является *симметричным*, т.е. для зашифрования и расшифрования информации используются одни и те же ключевые элементы. Иными словами, в шифраторы отправителя и получателя защищаемой информации должны быть загружены *одинаковые* ключи шифрования (К) (Рис. 1.1).

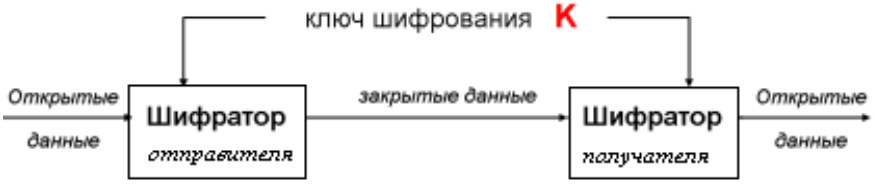

Рис. 1.1

Совокупность узлов сети связи, между которыми ведется обмен информацией с использованием криптографической защиты, образуют криптографическую сеть.

АРМ ГК-4 выполняет генерацию *одинаковых* ключей для каждой пары узлов криптографической сети.

Указанный способ обеспечения ключами узлов криптографической сети называется *симметричной* ключевой системой. Некоторые принципы реализации *симметричной* ключевой системы для АРМ ГК-4 описаны ниже.

Криптографическим номером называют порядковый номер узла в криптографической сети.

Полный набор ключей для всех узлов сети вырабатывается на АРМ ГК-4. Указанный набор удобно рассматривать в виде сетевой таблицы.

Замечание. Принцип работы АРМ ГК-4 не предусматривает изготовление собственно сетевой таблицы (см. раздел 1.2. 5). Здесь она рассматривается лишь для наглядности описания *симметричной* ключевой системы.

Сетевая таблица представляет собой квадратную диагонально-симметричную матрицу, размер которой (**N**) равен числу узлов в криптографической сети. В ячейках таблицы хранятся ключи шифрования $\mathbf{K_{i,j}}$ *для связи между парой узлов сети*, номера которых i и j определяются номерами соответствующих строки и столбца сетевой таблицы.

Данные ключи шифрования принято называть ключами парной связи. Для *симметричной* ключевой системы ключи парной связи различны для каждой пары узлов сети, но всегда, в силу свойств сетевой таблицы, $\mathbf{K_{i,j} = K_{j,i}}$ (Рис. 1.2).

Рис. 1.2

На АРМ ГК-4 для каждого узла формируется свой сетевой набор ключей – строка сетевой таблицы, соответствующая криптографическому номеру узла (Рис. 1.3).

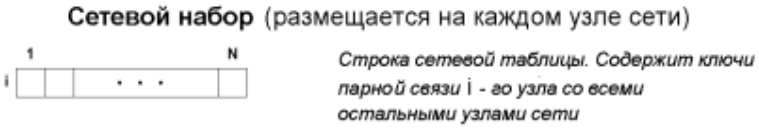

Рис. 1.3

Сетевые наборы записываются на ключевые носители и доставляются на места эксплуатации способом, исключающим их компрометацию.

Ключи парной связи имеют ограниченный срок действия. Максимальный срок действия ключей парной связи – один год. Эксплуатирующей организацией может быть установлен меньший срок. По истечении срока действия ключей производится их плановая замена. Она заключается в формировании новых сетевых наборов и ключевых носителей и доставке последних на узлы связи.

Для того, чтобы различать сетевые наборы ключей парной связи при их плановой смене, им присваивается пятизначный цифровой идентификатор – номер серии. Кроме того, номер серии позволяет различать сетевые наборы в различных сетях.

Таким образом, любой сетевой набор ключей парной связи характеризуется:

- криптографическим номером, соответствующим номеру узла;

- номером серии.

СКЗИ АРМ ГК-4 предназначено для изготовления ключей парной связи следующих форматов:

- Формат **Фактор** – базовый формат сетевого набора ключей парной связи, используется большинством СКЗИ разработки ООО «Фактор-ТС»;
- Формат **Фактор-М** – формат, представляющий собой набор ключей формата **Фактор**, характеризующихся единым номером серии, но различными криптографическими номерами;
- Формат **Фактор-MS** – формат, представляющий набор ключей формата **Фактор**, характеризующихся различными номерами серии, но с одинаковым криптографическим номером;
- Формат **Фактор-КВ2** – формат, аналогичный формату ДСРФ, в котором ключи парной связи могут использоваться СКЗИ Dionis по классу КС3 и ниже;
- Формат **Фактор-КВ2М** – формат, представляющий собой набор ключей формата **Фактор-КВ2**, характеризующихся единым номером серии, но различными криптографическими номерами.

1.2. Принципы работы АРМ ГК-4

1.2.1. Подготовка АРМ ГК-4 к эксплуатации

Для подготовки АРМ ГК-4 к эксплуатации необходимо:

1) в соответствии с разделом 2 (с. 8) данного руководства установить СКЗИ АРМ ГК-4;
2) установить АПМДЗ в соответствии с эксплуатационной документацией на данное изделие;
3) установить ПО DiCheck (если требуется) в соответствии с эксплуатационной документацией.

1.2.2. Генерация ключей

Генерация ключей и формирование ключевых носителей заданной серии на АРМ ГК-4 выполняется в следующем порядке (Рис. 1.4):

1) формирование ключевого носителя с мастер-ключом (КНМК);
2) формирование ключевых носителей с сетевыми наборами ключей парной связи (КНПС) для узлов сети на основе мастер-ключа.

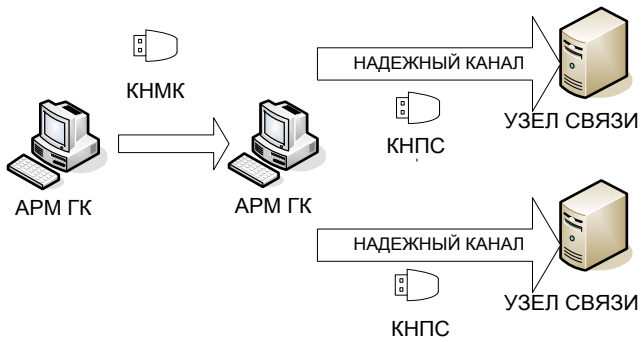

Рис. 1.4

Информацию, записанную на КНМК, АРМ ГК-4 использует для изготовления сетевых наборов ключей парной связи и формирования КНПС.

Срок действия мастер-ключа – 3 года, ключей парной связи – 1 год.

КНМК формируется для каждой серии сетевой таблицы только один раз и содержит всю необходимую информацию, позволяющую:

- создать ключи парной связи и сформировать ключевые носители для всех узлов сети или выборочно для некоторых из них;
- в любой момент восстановить сетевой набор и ключевой носитель для любого узла сети;
- произвести формирование ключевых носителей для новых узлов.

Ключевые носители доставляются на узлы связи исключительно по защищенному («надежному») каналу связи, например, фельдъегерской почтой либо с использованием телекоммуникационных средств с применением независимой криптографической защиты.

В отличие от технологий, предполагающих предварительное изготовление сетевой таблицы, алгоритм работы АРМ ГК-4 позволяет избежать формирования и хранения сетевой таблицы на жестком магнитном диске: сетевые наборы записываются *исключительно* на ключевые носители узлов и при выключенном питании АРМ ГК-4 ни в какой момент времени не содержит ключевой информации.

1.2.3. Дополнительные экземпляры ключевых носителей

Для обеспечения сохранности ключевой информации в случае физического повреждения ключевого носителя необходимо с помощью АРМ ГК-4 предварительно сформировать несколько дополнительных экземпляров (создать дубликаты) ключевых носителей КНМК и КНПС либо позже воспользоваться специальной программой **Копирование ключевых данных**, входящей в комплект поставки АРМ ГК-4 (см. раздел 6, с. 28).

ВНИМАНИЕ! На КНМК и КНПС кроме ключей записывается служебная информация, которая при формировании любого дополнительного количества экземпляров ключевых носителей обновляется с целью обеспечения безопасности СКЗИ, поэтому создание дубликатов ключевых носителей допускается *исключительно* средствами АРМ ГК-4.

1.2.4. Этикетки ключевых носителей

На этикетку КНМК должны быть нанесены:

- наименование КНМК;
- номер серии;
- номер дубликата КНМК;
- количество узлов в сети.

На этикетку КНПС должны быть нанесены:

- наименование КНПС;
- номер серии;
- криптографический номер узла;
- номер дубликата КНПС (при необходимости).

1.3. Условия применения АРМ ГК-4

Требования к оборудованию:

- в качестве аппаратной платформы функционирования АРМ ГК-4 может быть использован любой Intel-совместимый компьютер, обладающий следующими характеристиками:
  - как минимум, процессор семейства Pentium IV 2,4 Ггц (рекомендуется - Intel Core2 Duo или процессор более высокой производительности);
  - ОЗУ объемом не менее 1 Гбайт (рекомендуется 2 и более Гбайт);

- устройство чтения CD/DVD;
- минимум два доступных пользователю USB-разъема;
- свободный разъем системной шины (PCI, PCI-Express или MiniPCI-express), от типа которого зависит выбор типа АПМДЗ;

- состав программного обеспечения АРМ ГК-4:
  - программа формирования ключевых носителей с мастер-ключом **Формирование ключевого носителя с мастер-ключом** (**`masterkey.exe`**);
  - программа формирования ключевых носителей с сетевыми наборами ключей парной связи **Генерация ключей абонентов** (**`genkwin.exe`**);
  - программа **Генерация ключей абонентов в формате Фактор (MS)** **`(genmulkey.exe)`** предназначена для изготовления специальных ключевых носителей с сетевыми наборами ключей парной связи соответствующего формата;
  - программа проверки целостности ПО АРМ ГК-4 **Проверка целостности** (**`checkwin.exe`**) и файл **`chksum`**; файл **`chksum`** содержит список подлежащих проверке файлов программного обеспечения и эталонных значений контрольных сумм этих файлов; содержимое файла **`chksum`** приведено в документе «Автоматизированное рабочее место генерации ключей АРМ ГК-4. Формуляр. RU.НКБГ.70014-01ФО»;
  - программа уничтожения ключей парной связи по заданному направлению (всех ключей связей с выбывшим абонентом сети), а также быстрой очистки ключевого носителя в случае компрометации **Стирание ключа** (**`clearkey.exe`**);
  - программа копирования мастер-ключей на дополнительные ключевые носители **Копирование ключевых данных** (**`copykeyutil.exe`**);
  - программа удаления АРМ ГК-4 **Удаление всех программ АРМ ГК-4** (**`unins000.exe`**) и соответствующий конфигурационный файл **`unins000.dat`**;
  - файл узла замены **`uz.src`**;
  - библиотеки программных модулей (**`*.dll`**).

Примечание. В зависимости от разрядности операционной системы ПО АРМ ГК-4 может быть поставлено в одном из двух исполнений:
- исполнение **`x86`** - для работы на ОС разрядностью **`x86`**;
- исполнение **`x64`** - для работы на ОС разрядностью **`x64`**.

2. Установка СКЗИ АРМ ГК-4

СКЗИ АРМ ГК-4 поставляется на одном носителе - компакт-диске.

Комплект поставки состоит из:

- программы установки АРМ ГК-4 **`setup.exe`**;
- директории, содержащей файлы с эксплуатационной документацией на АРМ ГК-4.

Инсталляция АРМ ГК-4 возможна прямо с носителя, содержащего файл **`setup.exe`**, или после копирования установочного файла **`setup.exe`** на жесткий диск.

Для инсталляции ПО АРМ ГК-4 необходимо осуществить последовательность операционных шагов, которые сопровождаются комментариями и являются стандартными для установки ПО в операционной системе WINDOWS.

Внешний вид главного окна программы установки выглядит в соответствии с Рис. 2.1:

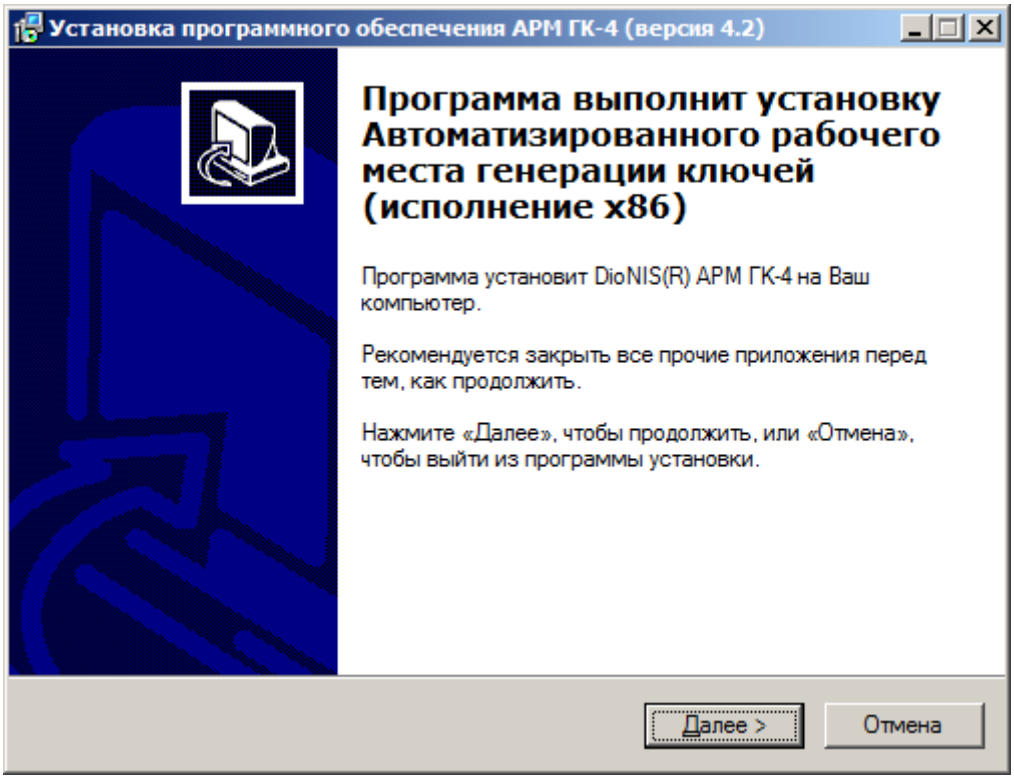

Рис. 2.1

ВНИМАНИЕ! Если на компьютере уже установлена программа АРМ ГК-4, то необходимо предварительно удалить предыдущую версию с помощью программы **Удаление всех программ АРМ ГК-4** (ярлык программы находится в папке стартового меню WINDOWS, в которую он был помещен в процессе предыдущей инсталляции). Установка ПО АРМ ГК-4 в ту же папку без удаления старой версии невозможна.

В процессе инсталляции запрашивается папка для установки АРМ ГК-4.

Замечание. По умолчанию программой предлагается путь **`<Системный диск>:\ARM_GK-4`**, который желательно не менять - для удобства обновления версии программы. Но возможен выбор любой другой папки для установки ПО.

Затем запрашивается название папки в стартовом меню WINDOWS, в которую будут помещены ярлыки для запуска программ формирования ключевых носителей (**Генерация мастер-ключа, Генерация ключей абонентов** и **Генерация ключей абонентов Фактор (MS)**) и служебных программ (**Копирование ключевых данных**, **Стирание ключа**, **Проверка целостности** и **Удаление всех программ АРМ ГК-4**).

По умолчанию предлагается название папки **АРМ ГК-4**.

После сбора всех сведений на экран выводится окно с параметрами, выбранными пользователем (Рис. 2.2).

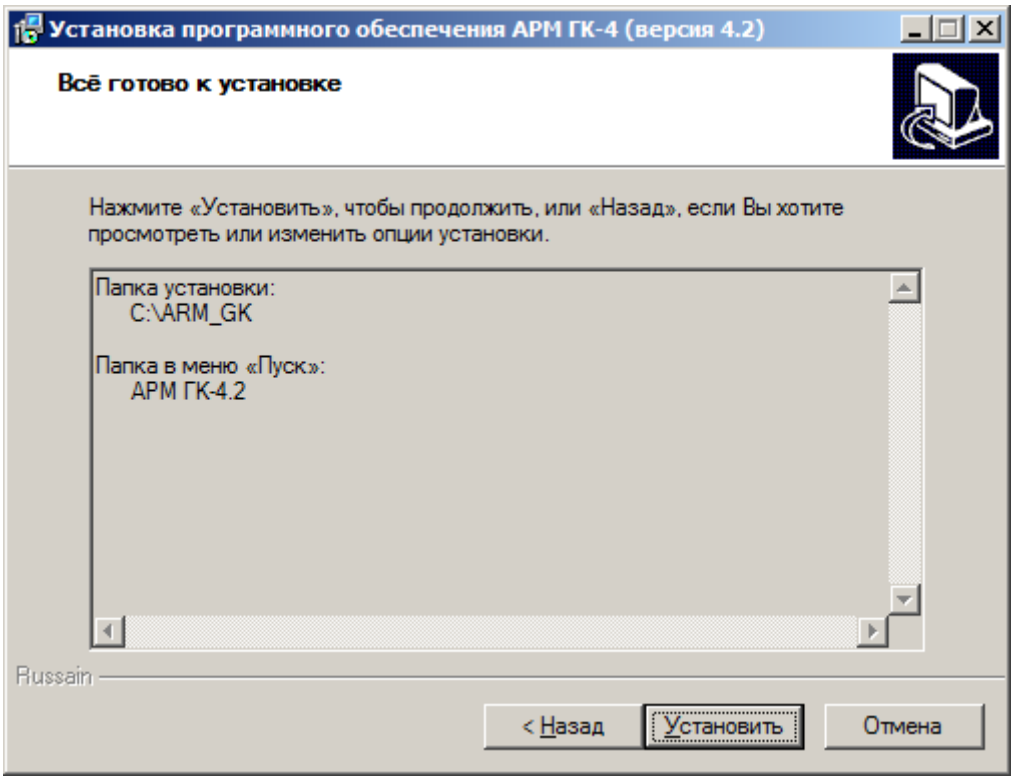

Рис. 2.2

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

После завершения инсталляции АРМ ГК-4 появляется окно с уведомлением о завершении установки ПО АРМ ГК-4. Окно закрывается нажатием кнопки **Завершить**.

3. Проверка целостности и регистрация ПО

3.1. Проверка целостности

Основные характеристики изделия контролируются с помощью процедуры проверки целостности программного обеспечения АРМ ГК-4.

Проверка выполняется путем сравнения значений контрольных сумм подлежащих проверке файлов ПО.

Список подлежащих проверке файлов и эталонных значений их контрольных сумм содержится в файле **chksum**, входящем в состав ПО АРМ ГК-4, и дублируется в Формуляре на изделие («Автоматизированное рабочее место генерации ключей АРМ ГК-4. Формуляр. RU.НКБГ.70014-01ФО»).

При первом включении АРМ ГК-4 пользователь обязан визуально сверить значения контрольных сумм файла **chksum** с соответствующими значениями, содержащимися в Формуляре.

Несоответствие указанных значений контрольных сумм свидетельствует о нарушении целостности программного обеспечения АРМ ГК-4 и влечет за собой запрет на эксплуатацию системы до полной переустановки АРМ ГК-4.

Начинать эксплуатацию изделия можно только в случае полной идентичности сверяемых контрольных сумм.

При каждом последующем включении питания ПЭВМ контроль целостности ПО АРМ ГК-4 обеспечивается автоматически посредством АПМДЗ, включенного в состав СКЗИ.

При первоначальной настройке АПМДЗ в перечень контролируемых объектов в обязательном порядке включаются перечисленные ниже файлы и, кроме того, могут быть внесены любые другие файлы.

Контроль целостности ПО АРМ ГК-4 необходимо периодически проводить с помощью программы **Проверка целостности** (**checkwin.exe**). Периодичность проверки зависит от условий эксплуатации и определяется политикой безопасности эксплуатирующей организации.

Для проверки целостности ПО АРМ ГК-4 необходимо запустить программу **Проверка целостности** (**checkwin.exe**) из стартового меню WINDOWS (**Пуск ⇨ Программы ⇨ АРМ ГК-4 ⇨ Проверка целостности**).

Программа вычислит контрольные суммы файлов, приведенных в файле **chksum**, входящем в состав ПО АРМ ГК-4, и сравнит их с эталонными.

Файл **chksum** содержит список файлов программного обеспечения, подлежащих проверке, и эталонные значения контрольных сумм этих файлов.

В случае обнаружения несовпадения программа укажет файл, где имеет место ошибка контрольной суммы. В этом случае программное обеспечение требует *обязательной* замены.

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

3.2. Регистрация ПО

Процедура регистрации ПО АРМ ГК-4 выполняется путём вызова модуля регистрации (ARMGKLicence.exe), который автоматически вызывается при первом запуске программы **Генерация мастер-ключа** (см. 4).

При этом будет отображено окно регистрации (Рис 3.1)

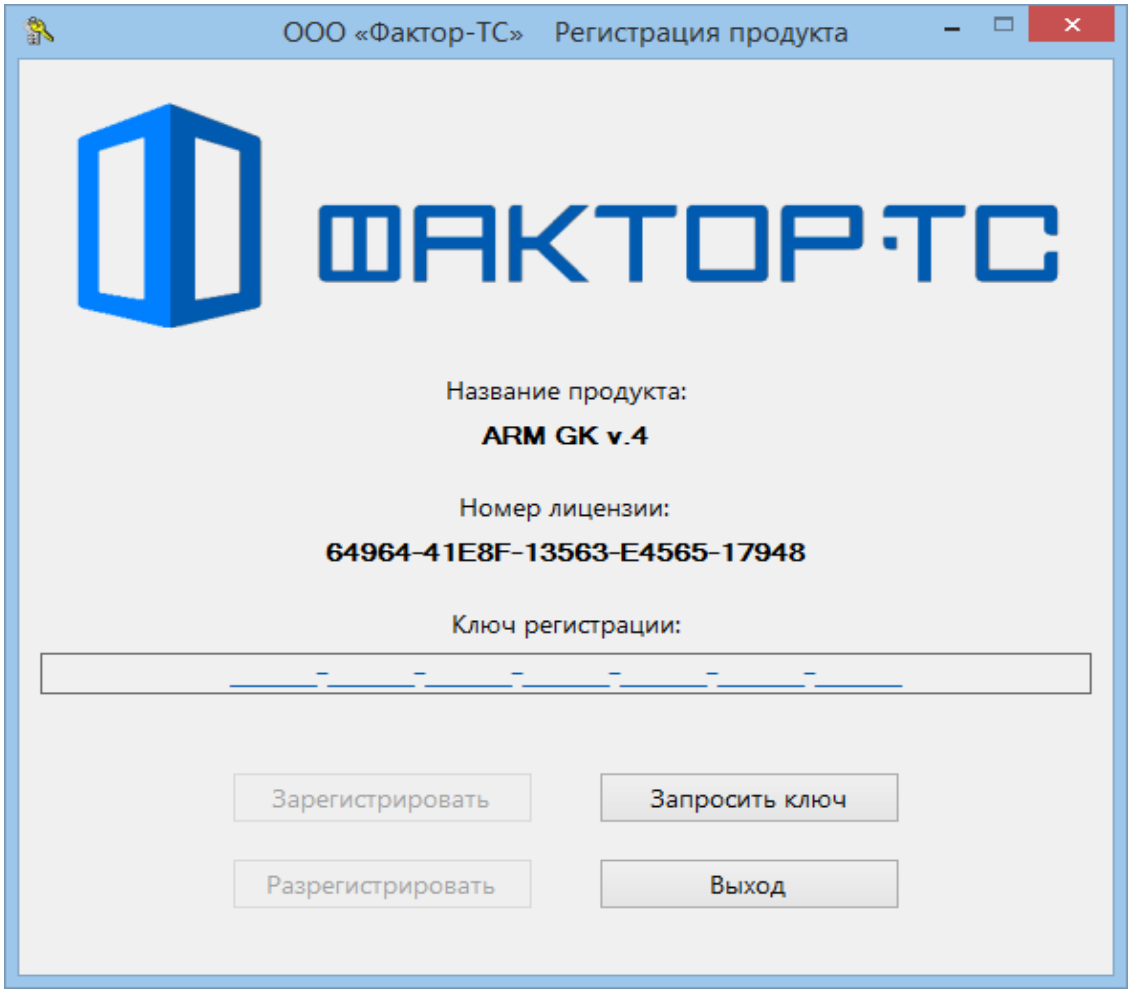

Рис. 3.1

Оператор АРМ ГК-4 на месте эксплуатации изделия должен запросить ключ регистрации ПО АРМ ГК-4 через службу технической поддержки Разработчика ПО (Рис .3.2) любым, из ниже предлагаемых способов, кроме отправки запроса на электронную почту, по причине изоляции рабочей станции, содержащей установленное ПО АРМ ГК-4 (см. Правила пользования).

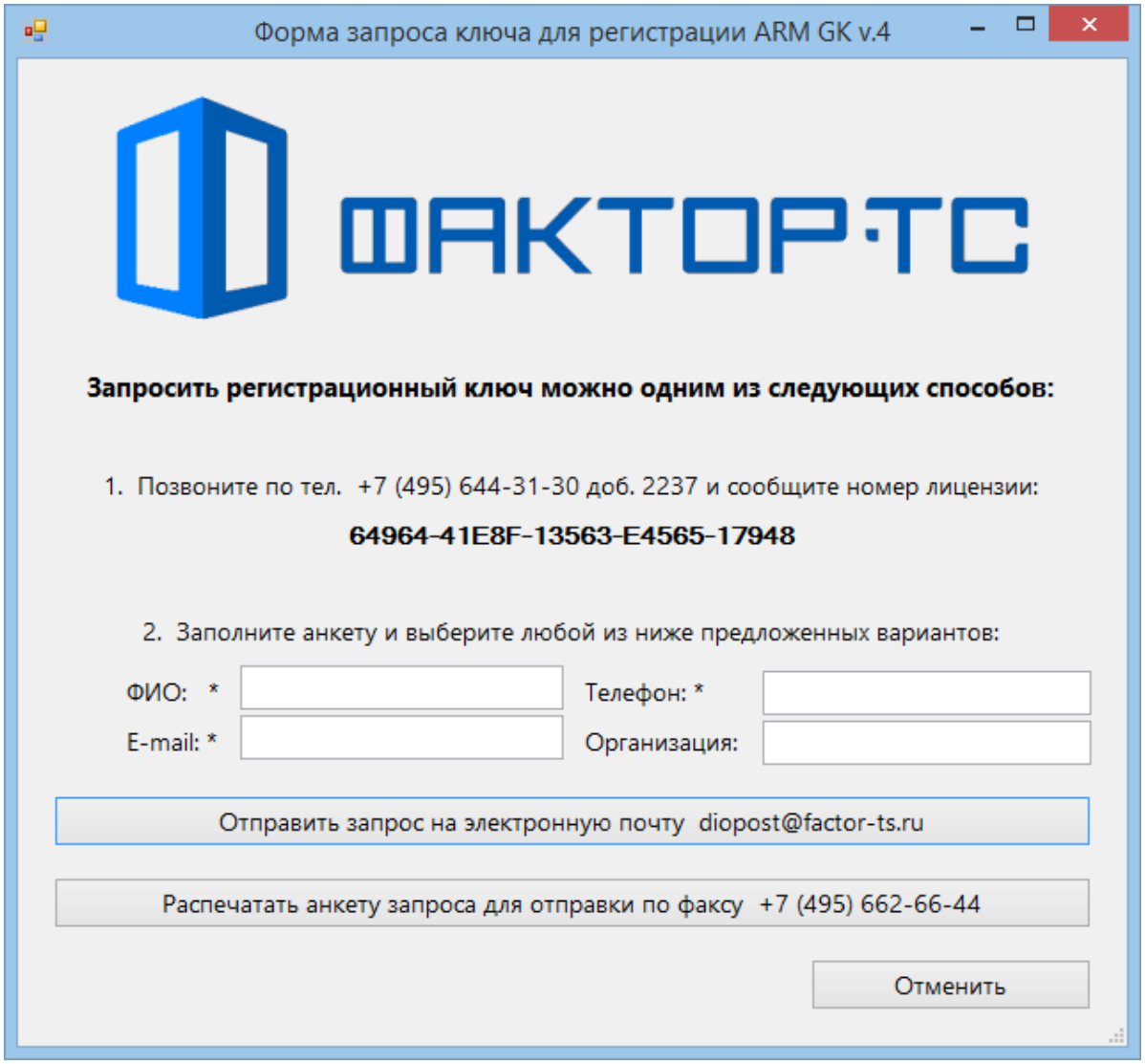

Рис 3.2

Получив ключ регистрации, оператору требуется ввести значение в соответствующее поле окна, отображённого на Рис.3.1. При правильно введённом значении ключа, будет отображено соответствующее сообщение (Рис.3.3) и запущена программа **Генерация мастер-ключа** (см. 4).

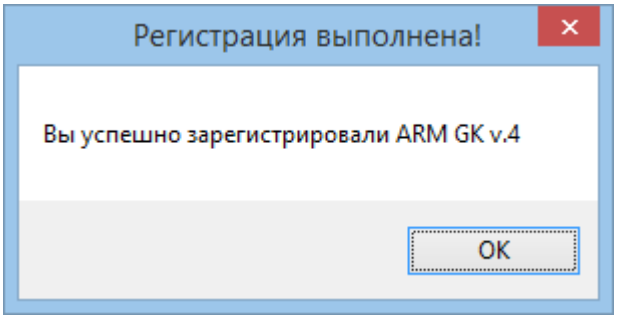

Рис.3.3

4. Формирование ключевого носителя с мастер-ключом

Ключевой носитель с мастер-ключом формируется АРМ ГК-4 каждый раз при возникновении необходимости сгенерировать сетевые наборы ключей парной связи новой серии.

Программа **Генерация мастер-ключа** выполняет генерацию мастер-ключа и служебной информации с последующей записью их на ключевой носитель (КНМК).

После запуска программы на экран будет выведено окно **Изготовление мастер-ключа** (Рис. 4.1).

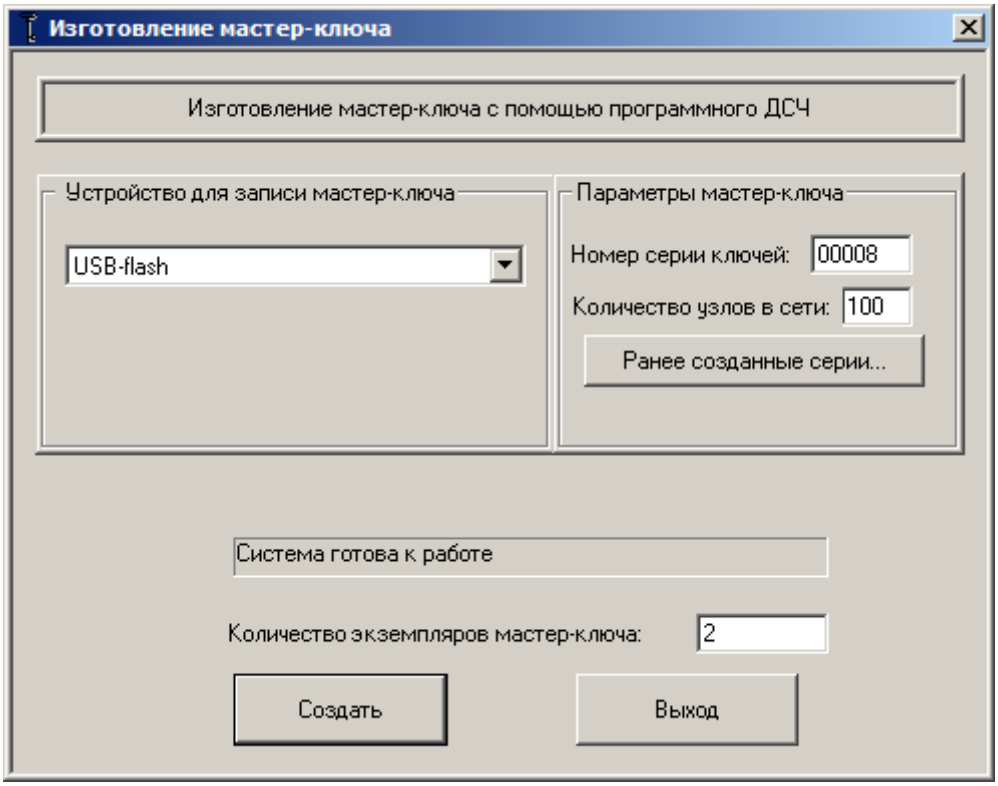

Рис. 4.1

Передвижение по полям и нажатие кнопок в окне **Изготовление мастер-ключа** и в других окнах программ АРМ ГК-4 можно выполнять с помощью компьютерной мыши, а при ее отсутствии - с помощью клавиш **<Tab>** – ***движение вниз*** и **<Shift+Tab>** – ***движение вверх***; для передвижения внутри поля служат клавиши **<←>** – ***движение влево***, **<→>** – ***движение вправо***.

Под заголовком **`Устройство для записи мастер-ключа`** (Рис. 4.1) содержится раскрывающийся список видов сменных носителей для записи мастер-ключа:

- **`USB-flash;`**
- **`RuToken(USB);`**
- **`EToken(USB).`**

Из данного списка необходимо выбрать тип устройства, используемого оператором для записи мастер-ключа.

При выбранном поле **`USB-flash`** запись мастер-ключа будет возможна не только на стандартный носитель **`USB-flash`**, но и специализированный носитель **`Рутокен ЭЦП flash`**.

Если выбрано устройство **RuToken (USB)**, то в группе появляется поле **Папка для мастер-ключа** (Рис. 4.2), в которое должен быть занесен номер создаваемой папки, в которой будет сохранен мастер-ключ. Допускается ввод значений в диапазоне от 2 до 65535.

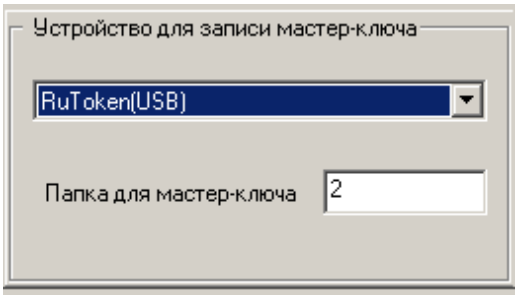

Рис. 4.2

Под заголовком **Параметры мастер-ключа** (Рис. 4.1) содержатся поля с характеристиками серий ключей.

В поле **Номер серии ключей** по умолчанию содержится очередной свободный номер серии ключей (пятизначное десятичное число), следующий за последним использованным номером и автоматически увеличивающийся на единицу при создании очередного мастер-ключа.

ВНИМАНИЕ! Использование номера серии ключей, отличного от предложенного системой, разрешено только в том случае, когда ключи данной серии ранее заведомо не изготавливались, что необходимо для корректного учета изготовленных ключей. В случае повторного использования одного и того же номера серии ключей система на этапе создания мастер-ключа выдаст сообщение об ошибочной ситуации.

В поле **Количество узлов в сети** необходимо ввести число абонентов, которые будут обмениваться информацией в сети связи. Число выбирается с учетом возможного добавления в сеть новых абонентов и увеличения количества ключевых носителей.

При нажатии на кнопку **Ранее созданные серии** открывается окно **Ранее созданные серии ключей** (Рис. 4.3) с таблицей для просмотра ранее созданных серий ключей.

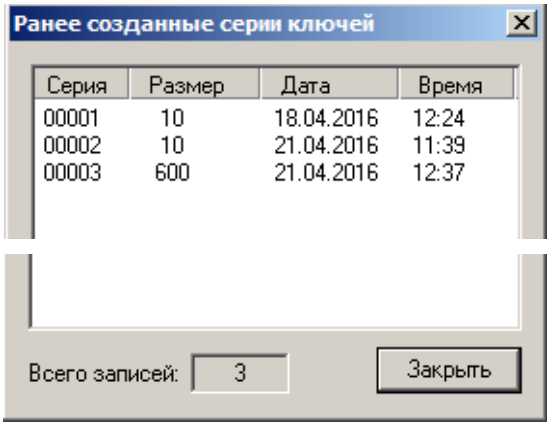

Рис. 4.3

В таблице выводятся порядковый номер серии ключей (под заголовком **Серия**), количество узлов в сети (под заголовком **Размер**), а также дата и время создания серии ключей. Серии ключей и дополнительная информация о них сохраняются в файле **series.lst**, расположенном в папке ПО АРМ ГК-4, созданной на этапе инсталляции.

В поле **Количество экземпляров мастер-ключа** (Рис. 4.1) следует ввести желаемое количество экземпляров мастер-ключа заданной серии. Дополнительные

экземпляры (дубликаты) мастер-ключа необходимы для восстановления мастер-ключа заданной серии, записанного на сломанном сменном носителе (см. раздел 1.2.3., с. 6).

В строке, находящейся над полем **Количество экземпляров мастер-ключа**, отображается состояние системы на данном этапе (на Рис. 4.1 - **Система готова к работе**).

После заполнения всех полей в окне **Изготовление мастер-ключа** (Рис. 4.1) можно запустить процесс создания мастер-ключа нажатием кнопки **Создать**.

На экране появится предупреждающее сообщение о том, что будет выполнено создание случайной последовательности чисел с помощью программного датчика случайных чисел (ДСЧ). При каждом запуске ПО **Изготовление мастер-ключа** потребуется выполнение процедуры первичной инициализации ДСЧ (Рис. 4.4):

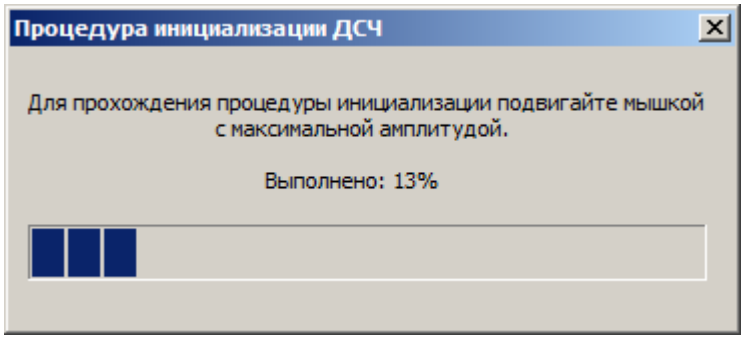

Рис 4.4

При успешном завершении процедуры инициализации на экране появится предупреждающее сообщение (Рис. 4.5):

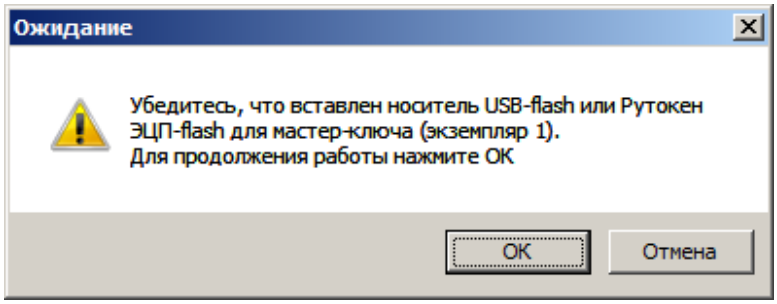

Рис. 4.5

Для записи мастер-ключа необходимо вставить требуемый чистый сменный носитель и нажать **ОК**.

Для носителя **USB-flash** после нажатия кнопки **ОК** (Рис. 4.) откроется окно выбора логического диска (Рис. 4.).

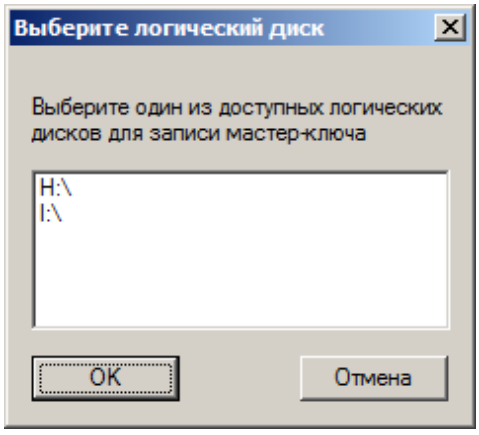

Рис. 4.6

После выбора диска и нажатия кнопки **OK** начнется процесс генерации мастер-ключа и записи на носитель.

Для носителя **RuToken (USB)** после нажатия кнопки **OK** (Рис. 4.) необходимо ввести текущий пароль пользователя **RuToken (USB)** (Рис. 4.).

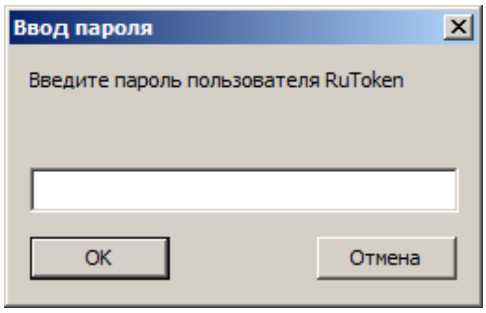

Рис. 4.7

- Для носителя **EToken (USB)** после нажатия кнопки ОК (Рис. 4.) также потребуется ввести текущий пароль пользователя **EToken (USB).**

  После ввода паролей начнется процесс создания мастер-ключа и записи на носитель.

В процессе генерации и записи мастер-ключа возможно возникновение следующих ошибочных ситуаций:

- Сменный носитель не готов для записи мастер-ключа. Программа выдаст сообщение об ошибочной ситуации и запрос на повтор операции записи. Необходимо подготовить устройство для записи.
- Носитель **USB-flash** содержит несоответствующую информацию. Перед формированием КНМК программой производится анализ содержимого носителя: запись ключевой информации на носитель не производится в случае обнаружения непредусмотренной информаций. Программа выдаст соответствующее сообщение и запрос на повтор операции записи. Необходимо подготовить устройство для записи.
- На носителе **RuToken (USB)** или **EToken (USB)** уже существует папка с выбранным номером (Рис. 4.1). Программа выдаст соответствующее сообщение и запрос на повтор операции записи. Необходимо указать другой номер папки для записи мастер-ключа или заменить носитель.

  При успешном завершении записи мастер-ключа выдается соответствующее сообщение.

Если в поле **Количество экземпляров мастер-ключа** (Рис. 4.1) пользователем было введено значение больше единицы, то после завершения записи мастер-ключа на первый носитель на экране появится сообщение (Рис. 4.):

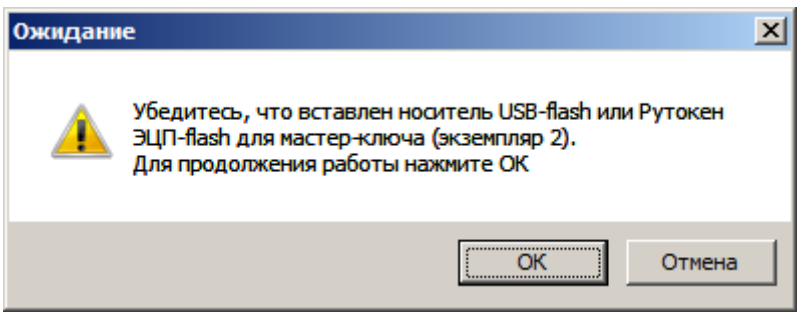

Рис. 4.8

Следует вставить в компьютер чистый носитель для записи мастер-ключа и нажать кнопку **OK** (Рис. 4.): повторится процесс записи мастер-ключа на носитель, аналогичный описанному выше.

В случае обнаружения недостачи носителей для создания заданного количества дубликатов ключевых носителей с мастер-ключом следует нажать кнопку **Отмена** для остановки процесса копирования.

При необходимости создания ключей другой серии процесс генерации мастер-ключа новой серии повторно запускается нажатием кнопки **Создать** (Рис. 4.1).

При отсутствии такой необходимости выход из программы осуществляется нажатием кнопки **Выход** (Рис. 4.1).

5. Формирование ключевых носителей с сетевыми наборами ключей парной связи

Программа Генерация ключей абонентов выполняет генерацию сетевых наборов ключей парной связи и формирует ключевые носители с ключами парной связи (КНПС) всех форматов, кроме формата **Фактор-MS**. Для создания ключа формата **Фактор-MS** используется отдельное ПО (см. раздел 6, с. 28).

Ключевой носитель с сетевыми наборами ключей парной связи заданной серии формируется на АРМ ГК-4 с использованием мастер-ключа заданной серии.

Для генерации сетевых наборов ключей парной связи необходим ввод мастер-ключа и служебной информации с ключевого носителя с мастер-ключом (КНМК).

После запуска программы на экран будет выведено окно **Ввод мастер-ключа** (Рис. 5.1).

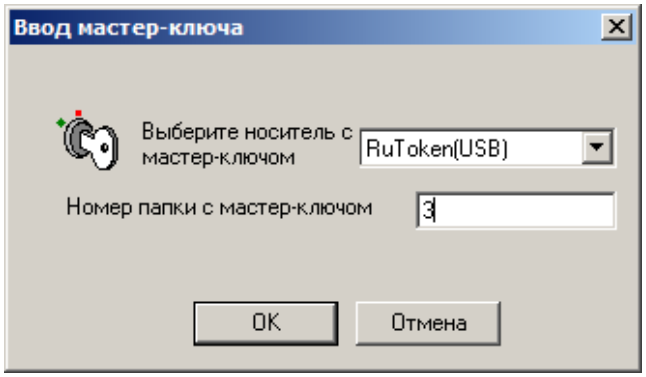

Рис. 5.1

Поле **Выберите носитель с мастер-ключом** содержит раскрывающийся список устройств - сменных носителей, с которых могут быть считаны мастер-ключ и служебная информация:

- **USB-flash;**
- **RuToken(USB);**
- **EToken(USB).**

Из данного списка необходимо выбрать устройство с мастер-ключом для считывания.

Если выбран носитель **RuToken(USB)**, то в окне **Ввод мастер-ключа** (Рис. 5.1) появляется дополнительное поле **Номер папки с мастер-ключом**, в которое необходимо занести номер папки на носителе, содержащей мастер-ключ.

Если выбран носитель **USB-flash**, появится окно **Выберите логический диск**, в котором требуется выбрать логический диск, содержащий мастер-ключ (Рис. 5.2).

В качестве носителя **USB-flash** также может использоваться специальный носитель **Рутокен ЭЦП Flash**, содержащий логический раздел с мастер-ключом.

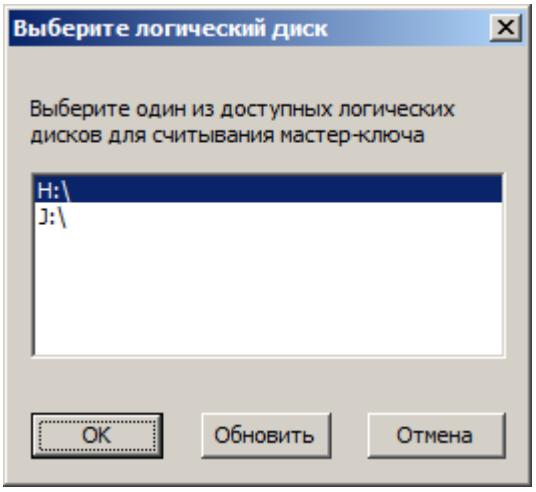

Рис. 5.2

Для продолжения работы после заполнения всех полей следует нажать кнопку **OK** (Рис. 5.1 и Рис. 5.2).

При выборе устройства **RuToken (USB)** или **EToken (USB)** потребуется ввод пароля пользователя устройства (Рис. 5.3).

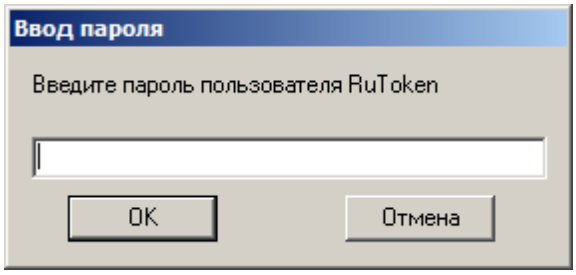

Рис. 5.3

При вводе мастер-ключа возможны следующие ошибочные ситуации:

- Сменный носитель, содержащий мастер-ключ и служебную информацию (на Рис. 5.1 – **RuToken (USB)**), не готов для считывания информации. Программа выдаст сообщение об ошибочной ситуации. Необходимо подготовить данное устройство и ввести информацию нажатием кнопки **OK**.
- Носитель для считывания не содержит необходимой для генерации сетевых наборов ключей парной связи информации или информация была испорчена. Программа выдаст сообщение об ошибочной ситуации. Необходимо подготовить на носителе необходимую информацию и ввести ее нажатием кнопки **OK**.
- Ключевой носитель с мастер-ключом может быть просрочен: прошло более трех лет с момента формирования данного КНМК.

После успешного завершения процесса ввода мастер-ключа и служебной информации открывается окно для изготовления сетевых наборов ключей парной связи (ключей абонентов) **Создание ключей абонентов** (Рис. 5.4):

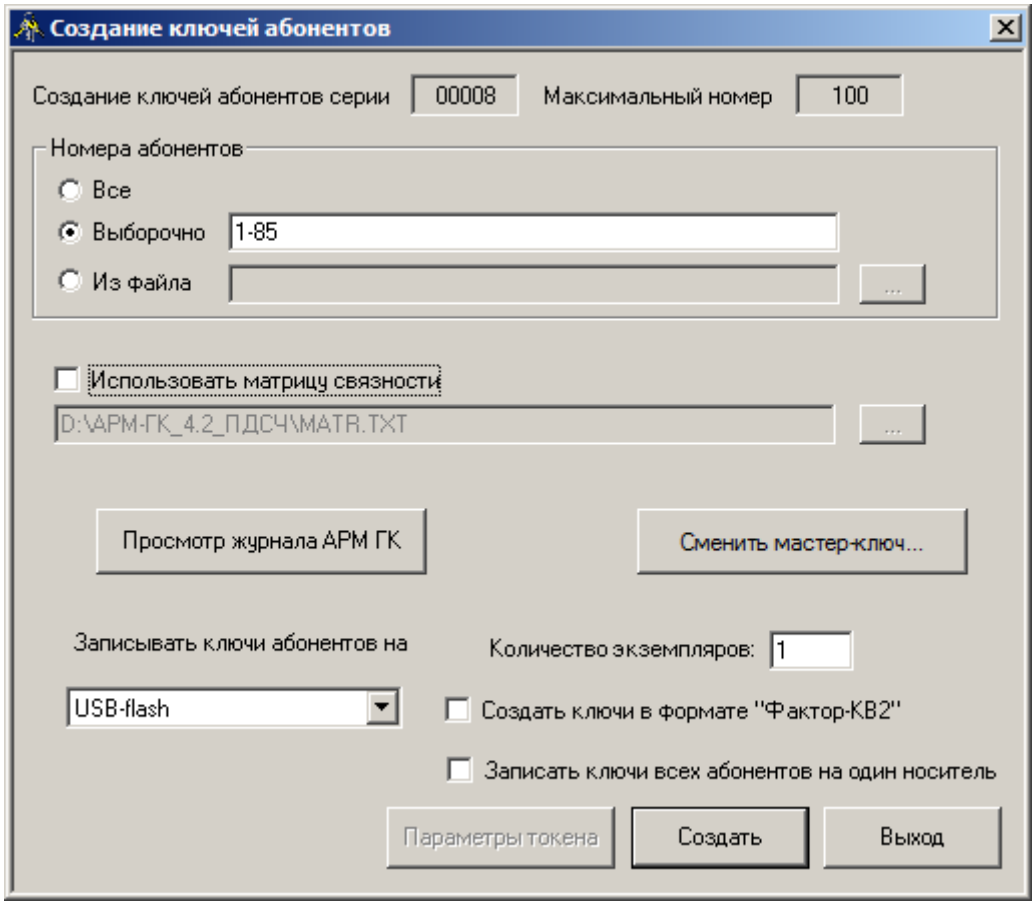

Рис. 5.4

Поле **Создание ключей абонентов серии** (Рис. 5.4) содержит номер серии сетевых наборов ключей парной связи, равный номеру серии мастер-ключа, который считывается автоматически с КНМК на этапе ввода мастер-ключа.

Поле **Максимальный номер** (Рис. 5.4) содержит общее число абонентов в сети связи, которое считывается автоматически с КНМК на этапе ввода мастер-ключа.

Группа **Номера абонентов** (Рис. 5.4) содержит набор полей, предназначенных для выбора абонентов, для которых будут создаваться сетевые наборы ключей парной связи.

Необходимо выбрать один из способов задания номеров абонентов:

- **Все** – для всех абонентов создаются сетевые наборы ключей парной связи;
- **Выборочно** – оператору необходимо ввести номера абонентов, для которых он создаст сетевые наборы ключей парной связи, в порядке, задаваемом списком. Например, `1,2,3-5,10` или `1,4,7,9;`
- **Из файла** – оператору необходимо ввести имя и полный путь местонахождения файла с номерами абонентов, для которых он создаст сетевые наборы ключей парной связи; файл также можно выбрать при помощи кнопки обзора файловой системы компьютера (кнопка справа от поля с именем файла); файл со списком абонентов заранее создается в любом текстовом редакторе (*кроме* Microsoft Word).

Замечание. Вариант подбора списка абонентов **Из файла** допускается *только* для ключевых носителей с одним сетевым набором ключей парной связи формата **Фактор** и **Фактор-КВ2**. Список абонентов задается аналогично списку в поле **Выборочно**. При переносе элемента списка на новую строку запятая после последнего элемента предыдущей строки *НЕ* ставится. Например: **`1,2`**
`5,9`

Поле **Использовать матрицу связности** (Рис. 5.4) является необязательным и используется, когда оператор хочет ограничить взаимную связь абонентов. По умолчанию, если данное поле не выбрано, для всех заданных ранее абонентов формируется КНПС, содержащий ключи парной связи со всеми остальными абонентами криптографической сети. Активировать поле можно, установив флажок **Использовать матрицу связности**. В поле следует ввести полный путь к файлу, содержащему матрицу связности, заранее подготовленному с помощью любого текстового редактора (*кроме* Microsoft Word). Файл также можно выбрать при помощи кнопки обзора файловой системы компьютера (кнопка справа от поля с именем файла).

С помощью матрицы связности можно запретить запись некоторых ключей на КНПС, сделав невозможной связь владельца КНПС с некоторыми «соседями» по криптографической сети.

Описание разрешенных и запрещенных взаимных связей абонентов криптографической сети формируется в файле, содержащем матрицу связности, с помощью следующих правил:

- файл описания матрицы связности состоит из одной или нескольких секций, где каждая секция описывает связи одного абонента;
- секция начинается со строки, которая содержит номер абонента в квадратных скобках (например, `[15]);`
- за начальной строкой секции могут следовать несколько строк с описанием связей (описатель связей) данного абонента (правила формирования описателей связей абонента приведены ниже);
- в файле может быть задана одна специальная секция **[*]**, в которой описываются связи всех абонентов, не указанных в остальных секциях;
- в файле описания матрицы связности по умолчанию действуют два правила:

  1) первое: если для какого-либо абонента не задана ни одна секция с описанием связей и отсутствует секция **[*]**, то для него *разрешены* связи со всеми абонентами криптографической сети;
  2) второе: если задана секция, не содержащая ни одного описателя связей (пустая), то все связи такого абонента *запрещены*.

Правила формирования описателей связей абонента:

- описатель связей абонента может состоять из следующего набора элементов: **<целое число>, -<целое число>, <диапазон>, -<диапазон>, *,-***;
- **<Целое число>** находится в диапазоне от **1** до **N**, где **N** – количество абонентов криптографической сети;
- **<Целое число>** показывает, что связь с абонентом, имеющим данный номер, *разрешена*;
- **-<Целое число>** показывает, что связь с абонентом, имеющим данный номер, *запрещена*;
- *****показывает, что *разрешена* связь со всеми остальными абонентами;
- **-*** показывает, что связь с другими абонентами *запрещена*;
- **<диапазон>** показывает диапазон номеров абонентов, для которых *разрешены* связи с данным абонентом;
- **-<диапазон>** показывает диапазон номеров абонентов, для которых *запрещены* связи с данным абонентом.

Замечание. Описатель связей абонента обрабатывается в следующем порядке. В матрице связности до обработки описателя все связи данного абонента с другими абонентами запрещены. Затем осуществляется последовательный просмотр всех элементов описателя (во всех строках) для выявления абонентов, с которыми связь разрешена или запрещена. Итоговое разрешение или запрещение связи с каждым абонентом формируется в результате пошаговой обработки всех элементов описателя. В случае, когда в описателе связь с одним и тем же абонентом указывается несколько раз, берется *последнее* значение элемента описателя. Например, `5-15, -7-8`: первым элементом описателя связь с абонентами 7 и 8 разрешается, а вторым - запрещается. В итоге связь с абонентами 7 и 8 будет запрещена.

ВНИМАНИЕ! Элементы описателя связей абонента записываются *СТРОГО* через запятую, и описатель *НЕ* заканчивается точкой. При переносе элемента описателя связей на следующую строку запятая между ним и предыдущим элементом *НЕ* ставится.

Рассмотрим пример файла с матрицей связности.

Пусть **N = 20**. Первый абонент может связываться со всеми абонентами, кроме **3** и **5**, второй – с **1**, **13** и **15**, пятый и шестой не могут связываться ни с кем, а все остальные абоненты - с абонентами, номера которых попадают в диапазон **[5 -15]**, за исключением **7** и **8** абонента.

Тогда содержимое файла будет иметь следующий вид:

```
[1]
*,-3,-5
[2]
1,13,15
[5]
-*
[6]
[*]
5-15,-7-8
```

Поле **Записывать ключи абонентов на** (Рис. 5.4) содержит раскрывающийся список устройств - сменных носителей для записи сетевых наборов ключей парной связи абонентов:

- **USB-flash**;
- **RuToken(USB)**;
- **EToken(USB).**

Из данного списка необходимо выбрать устройство, используемое оператором для записи сетевых наборов ключей парной связи (на Рис. 5.4 – устройство **USB-flash**).

Примечание. Не рекомендуется использовать носители **RuToken (USB)** или **EToken (USB)** для записи полной ключевой строки в сериях, где количество абонентов более 256.

В поле **Количество экземпляров** (Рис. 5.4) необходимо ввести желаемое количество экземпляров сетевых наборов ключей парной связи заданной серии для каждого

абонента. Дополнительные экземпляры сетевых наборов ключей парной связи необходимы для восстановления сетевых наборов ключей парной связи заданной серии при физическом нарушении сменного носителя, на котором они записаны (см. раздел 1.2.3., с. 6).

Ключи парной связи могут быть представлены в одном из двух форматов, выбор которых определяется сочетанием установленных/снятых флажков в переключателе **Создать ключи в формате Фактор-КВ2**:

- **Фактор** – доступен, если флажок на переключателе не установлен;
- **Фактор-КВ2** – доступен, если флажок на переключателе установлен.

Хранение ключей парной связи может быть представлено в двух видах, выбор которых определяется сочетанием установленных/снятых флажков в переключателе **Записать ключи всех абонентов на один носитель**:

- **Фактор**, **Фактор-КВ2** – хранение на носителе одного сетевого набора ключей парной связи выбранного формата; доступен, если флажок на переключателе не установлен;
- **Фактор-М**, **Фактор-КВ2М** – хранение на носителе нескольких сетевых наборов ключей парной связи выбранного формата; доступен, если флажок на переключателе установлен.

Для устройств **USB-flash** доступно создание ключей парной связи в форматах **Фактор** (**Фактор-М**), **Фактор-КВ2** (**Фактор-КВ2М**).

Для устройств **RuToken (USB)** или **EToken (USB)** доступно создание ключей парной связи исключительно в формате **Фактор**.

Если выбрано устройство **RuToken (USB)** или **EToken (USB)**, пользователю становится доступна кнопка **Параметры**, а переключатели **Создать ключи в формате Фактор-КБ2** и **Записать ключи всех абонентов на один носитель** становятся неактивными (Рис. 5.5).

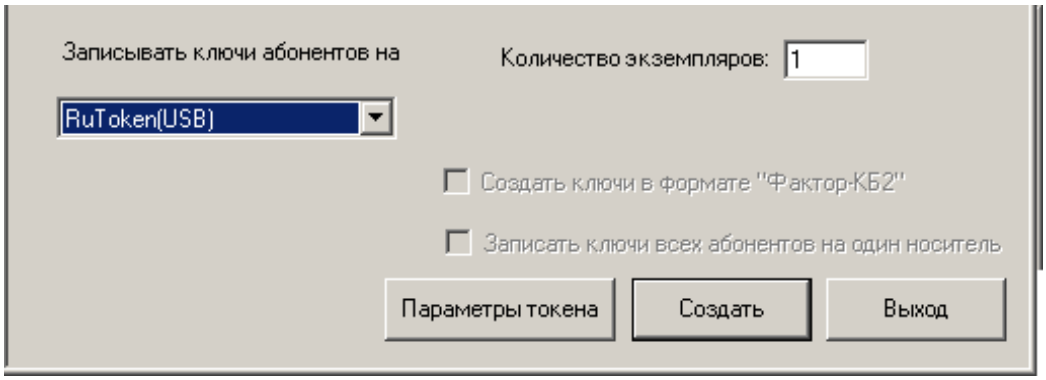

Рис. 5.5

При нажатии на кнопку **Параметры** открывается окно, где можно указать номер папки ключей абонентов (Рис. 5.6).

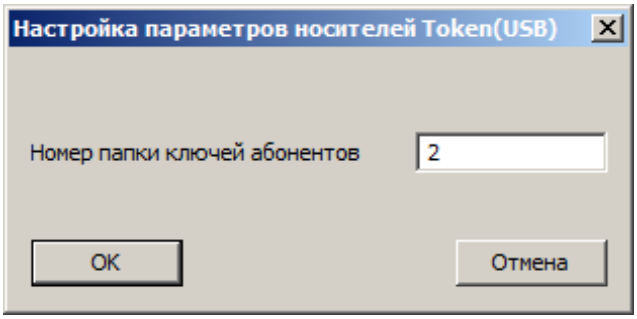

Рис. 5.6

После заполнения всех полей запуск процесса создания сетевых наборов ключей парной связи инициируется нажатием кнопки **Создать** (Рис. 5.4 и Рис. 5.5).

Замечание. При записи информации на носители **RuToken (USB)** или **EToken (USB)** в USB-порты рабочей станции должно быть вставлено не более одного носителя каждого типа.

После нажатия кнопки **Создать** (Рис. 5.4) появится окно **Вставьте ключевой носитель**:

Рис. 5.7 – для носителя **USB-flash**;

Рис. 5.8 - для носителей **RuToken (USB)** или **EToken (USB)**.

Создание и запись информации на носитель начнется после нажатия кнопки **OK**.

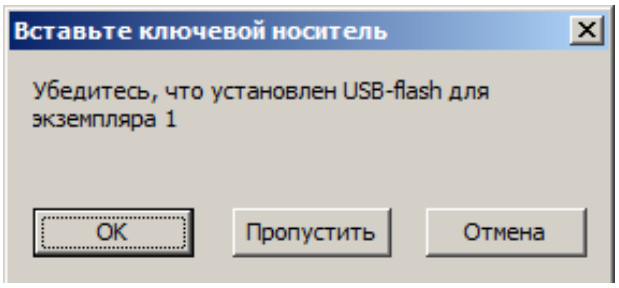

Рис. 5.7

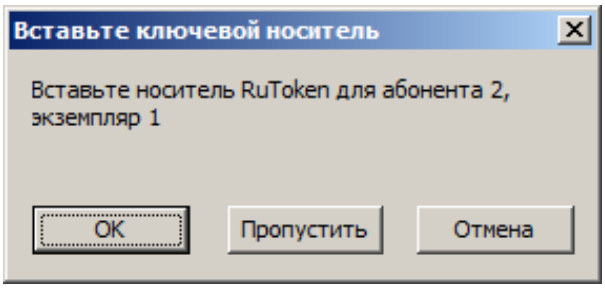

Рис. 5.8

При выборе носителя **USB-flash** появится окно **Выберите логический диск**, предлагающее выбрать логический диск, доступный для записи ключа абонента. (Рис. 5.9).

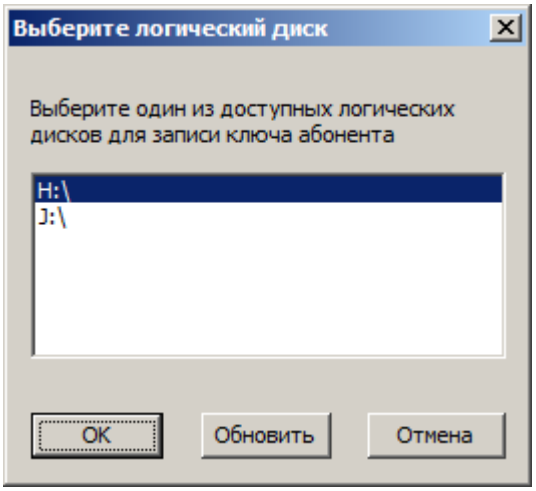

Рис. 5.9

При использовании носителей **RuToken (USB)** и **EToken (USB)** необходимо ввести текущий пароль пользователя носителя (Рис. 5.10).

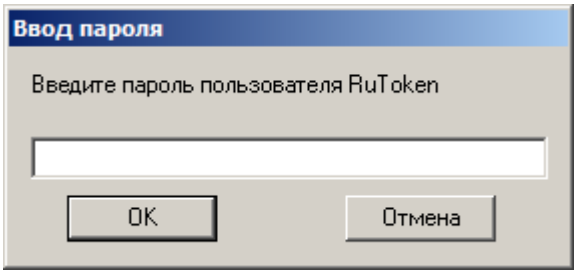

Рис. 5.10

После завершения процесса создания информации и ее записи на носитель на экран будет выведено соответствующее сообщение (Рис. 5.11).

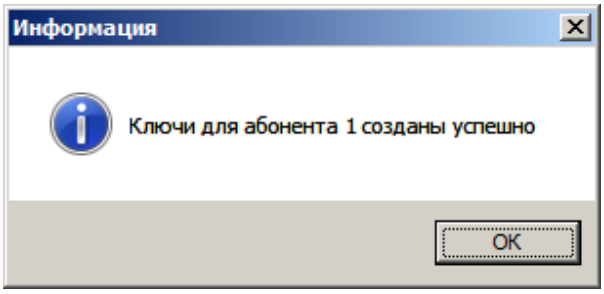

Рис. 5.11

Если в группе полей **Номера абонентов** (Рис. 5.4) пользователем указано более одного абонента, то на экране появится следующее сообщение (Рис. 5.12):

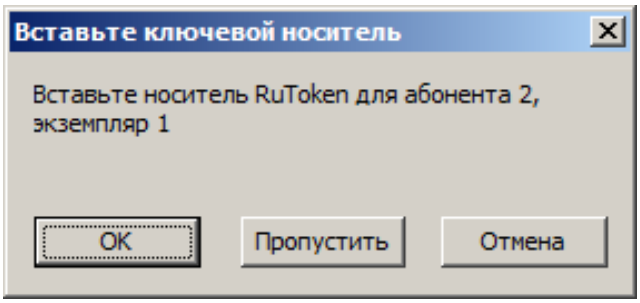

Рис. 5.12

Необходимо вставить чистый носитель для записи ключей и нажать кнопку **OK** (Рис. 5.12): повторится процесс записи ключей для последующих абонентов, аналогичный описанному выше.

При необходимости создания ключей другой серии процесс генерации ключей парной связи новой серии повторно запускается нажатием кнопки **Создать** (Рис. 5.4).

При отсутствии такой необходимости выход из программы осуществляется нажатием кнопки **Выход** (Рис. 5.4).

В процессе заполнения приведенных выше полей возможно возникновение следующих ошибочных ситуаций:

1. Группа полей **Номера абонентов** (Рис. 5.4):

- Поле **Выборочно**:

– Неверно задан список абонентов (узлов): список включает номера абонентов, превышающие максимальный номер. Программа выдаст соответствующее сообщение. Необходимо ввести номера абонентов с учетом общего количества абонентов (максимального номера).

– Неверно задан список абонентов (узлов): список содержит недопустимые символы (например, **k**, **;**, **=**, \). Необходимо ввести список, состоящий только из целых чисел, входящих в диапазон от **1** до **N**, где **N** - количество абонентов.

– Список абонентов пуст. Программа выдаст соответствующее сообщение. Необходимо заполнить список.

- Поле **Из файла**:

– Неверно задано имя файла, содержащего список абонентов. Программа выдаст соответствующее сообщение. Необходимо ввести имя существующего файла и полный путь к нему.

– Выбранный файл имеет недопустимый формат или содержит информацию, записанную в некорректном виде (см. ошибки в поле **Выборочно**). Программа выдаст соответствующее сообщение.

2. Поле **Использовать матрицу связности** (Рис. 5.4):

- Неверно задано имя файла, содержащего список абонентов. Программа выдаст соответствующее сообщение. Необходимо ввести имя существующего файла и полный путь к нему.
- Выбранный файл имеет недопустимый формат или содержит информацию, записанную в некорректном виде. Программа выдаст соответствующее сообщение. Необходимо следовать правилам описания связей абонента с другими абонентами криптографической сети, рассмотренным ранее.

Ошибки ввода паролей носителей **RuToken (USB)** или **EToken (USB)**:

- Пароли пользователей изделия не могут быть записаны на носитель. Причина: у данных носителей имеется встроенная функция допустимой «сложности» пароля. В данном случае требуется либо ввести более «сложный» пароль, либо отформатировать носитель с изменением значений данной функции.

В процессе записи сетевых наборов ключей парной связи возможно возникновение следующих ошибочных ситуаций:

- Устройство для записи сетевых наборов ключей парной связи не готово для записи. Программа выдаст сообщение об ошибочной ситуации. Необходимо подготовить устройство для записи.
- Выбранный для записи носитель **USB-flash** содержит какую-либо информацию. Перед формированием КНПС программа производит анализ содержимого носителя для записи и не производит запись на уже заполненный информацией носитель.
- На текущем устройстве для записи **RuToken (USB)** или **EToken (USB)** уже существует папка с выбранным номером. Программа выдаст соответствующее сообщение об ошибочной ситуации.
- Строка ключевой информации при попытке записи на носитель **EToken (USB)** превышает допустимый размер - 32768 байт. Запись ключевой информации на носитель не производится. Программа выдаст соответствующее сообщение с предложением заменить носитель.
- В КНПС форматов Фактор-М и Фактор-КВ2М может использоваться серия слишком большого размера. Перед формированием КНПС программа производит анализ доступного дискового пространства на носителе и не производит запись в случае нехватки свободного места. Выдаётся сообщение об ошибочной ситуации.

Процесс изготовления сетевых наборов ключей парной связи абонентов протоколируется в файле **journal.txt**, расположенном в папке ПО АРМ ГК-4, созданной на этапе инсталляции (раздел 9, с. 38). Данный файл может быть просмотрен с помощью любого текстового редактора.

Кнопка **Сменить мастер-ключ** (рис. 5.4) позволяет загрузить мастер ключ другой серии без физического выхода из программы. При этом все сведения о текущем мастер-ключе будут удалены. При нажатии данной кнопки пользователю предлагается подтвердить либо опровергнуть данное действие (рис. 5.13)

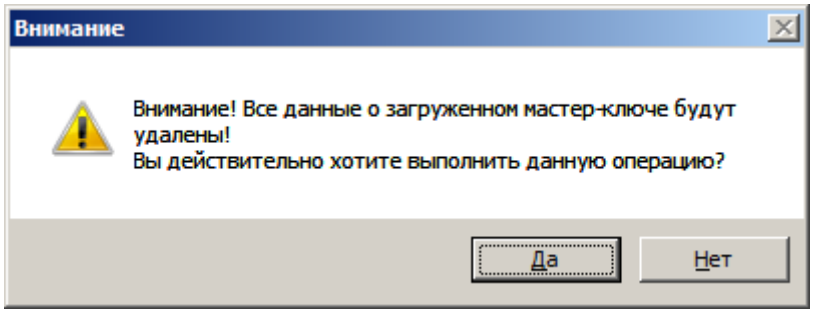

Рис. 5.13

В случае утвердительного ответа все данные о загруженном мастер-ключе будут стёрты и повторно отобразится окно **Ввод мастер-ключа** (рис. 5.1). В случае отмены загрузки нового мастер-ключа программа завершит свою работу.

Кнопка **Просмотр журнала АРМ-ГК** позволяет посмотреть журнал работы ПО АРМ ГК (рис 5.14). Подробнее см. раздел 9, с. 40 настоящего руководства.

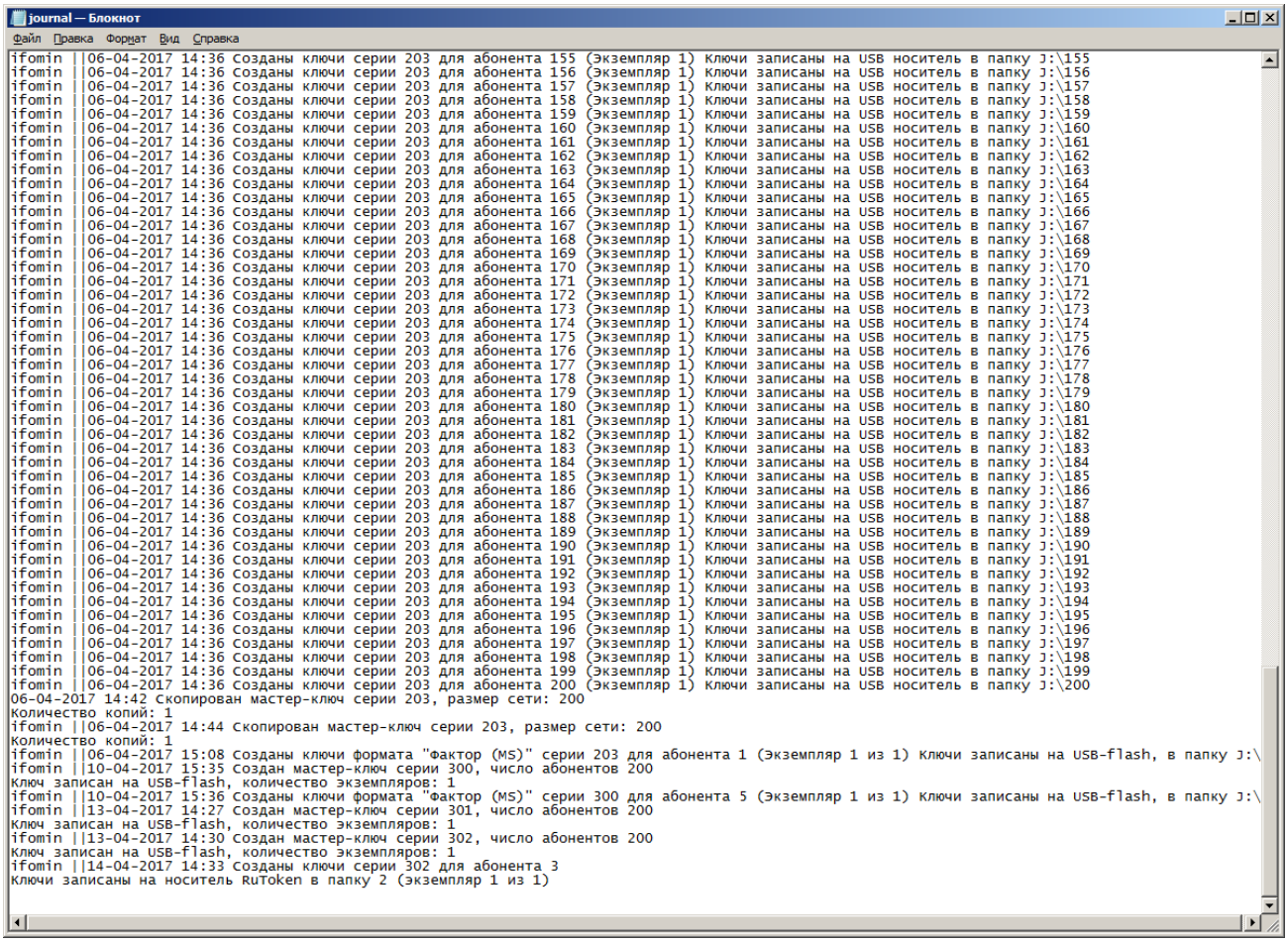

Рис. 5.14

6. Генерация ключей абонентов формата «Фактор-MS»

Программное средство создания ключей формата **Фактор-MS** выделено в отдельный программный модуль, получивший название **Генерация ключей абонентов «Фактор (MS)».**

При запуске программного обеспечения отображается основное окно программного модуля. (Рис. 6.1).

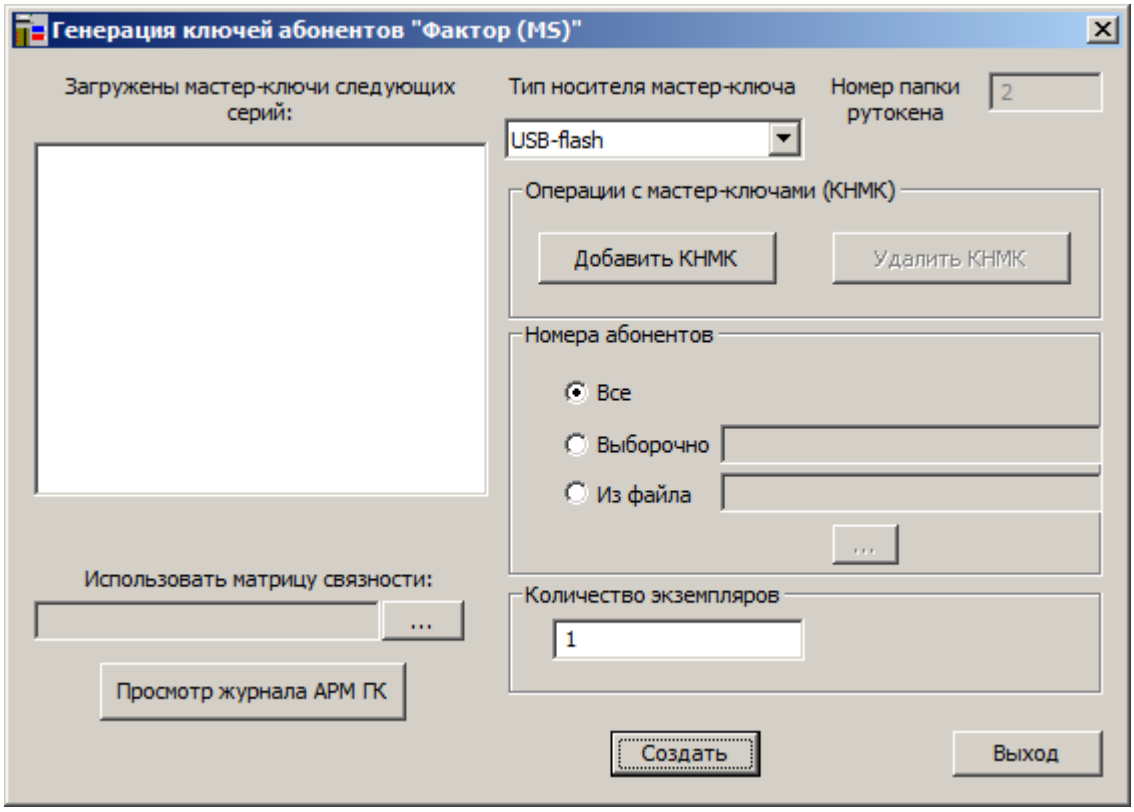

Рис 6.1

В поле **Загружены мастер-ключи следующих серий** отображаются сведения о загруженных мастер-ключах с носителей КНМК. Должен быть загружен как минимум один мастер-ключ для успешного создания КНПС формата **Фактор-MS.**

Раскрывающийся список **Тип носителя мастер-ключа** позволяет указать тип носителя, с которого требуется загрузить мастер-ключ. Возможно выбрать один из следующих типов носителей:

- **USB-flash;**
- **RuToken(USB);**
- **EToken(USB).**

Из данного списка необходимо выбрать устройство с мастер-ключом для считывания.

Если выбран тип носителя **RuToken(USB)**, то в окне программы (Рис. 5.1) станет доступным дополнительное поле **Номер папки рутокена**, в которое необходимо занести номер папки на носителе типа **Rutoken (USB),** содержащей мастер-ключ.

Если выбран тип носителя **USB-flash**, то в качестве носителя КНМК также может использоваться носитель **Рутокен ЭЦП Flash**, содержащий логический раздел с мастер-ключом.

Группа кнопок **Операции с мастер-ключами (КНМК)** содержит две кнопки: **Добавить КНМК** и **Удалить КНМК** (по умолчанию недоступна!)

При нажатии кнопки **Добавить КНМК** оператору будет предложено:

- выбрать доступный логический диск съёмного носителя, содержащий мастер-ключ, при выбранном типе носителя **USB-flash** (рис. 6.2);
- ввести пароль токена (рис. 6.3) при выбранном типе носителя **RuToken(USB)** или **EToken(USB)**.

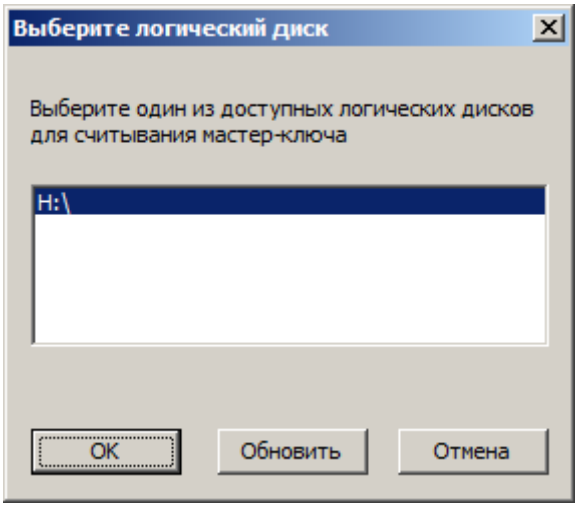

Рис. 6.2

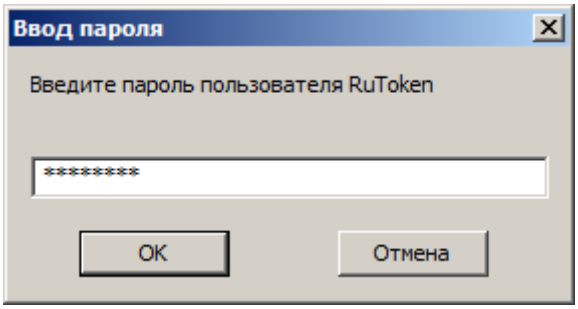

Рис. 6.3

По результатам успешной загрузки мастер-ключей с КНМК сведения о номере серии и размере будут отображаться в поле **Загружены мастер-ключи следующих серий** (рис 6.4.).

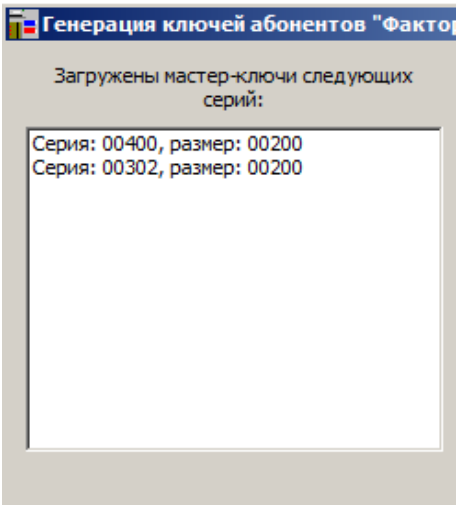

Рис. 6.4

Согласно требованиям, предъявляемым к ключам формата **Фактор-MS**, все загружаемые ключи должны быть рассчитаны на одинаковое количество узлов в сети. При

попытке загрузить мастер-ключ с размерностью сети, отличающейся от размерности сети ранее загруженных мастер-ключей, программа выдаст сообщение об ошибке (рис 6.5.).

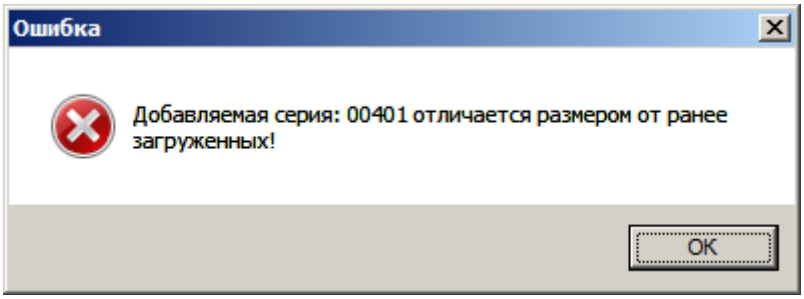

Рис. 6.5

Замечание. Допускается одновременная загрузка не более 10 мастер-ключей различных серий!

При необходимости, доступна возможность удаления ранее загруженного мастер-ключа. Для этого требуется выбрать соответствующий мастер-ключ в списке поля **Загружены мастер-ключи следующих серий**. После чего становится доступна кнопка **Удалить КНМК** (рис. 6.6).

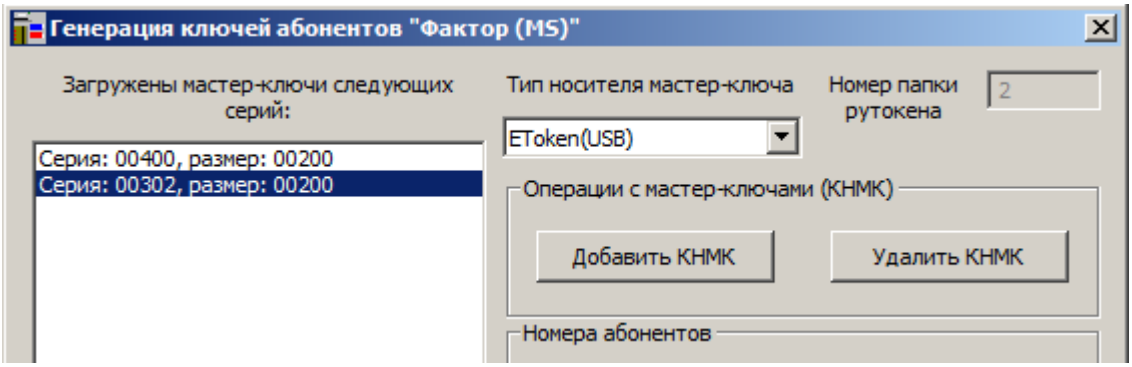

Рис. 6.6

При успешном выполнении операции удаления мастер-ключа, будет выведено соответствующее сообщение (рис. 6.7), а кнопка **Удалить КНМК** снова станет недоступна.

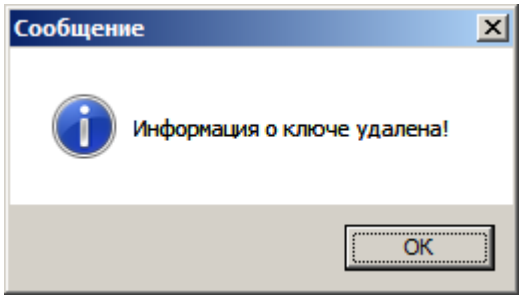

Рис. 6.7

Группа полей «**номера абонентов**», кнопка **Просмотр журнала АРМ ГК**, а также поле **Использовать матрицу связности** (рис. 6.1) полностью аналогичны полям программы **Генерация ключей абонентов** (см. главу 5).

В поле **Количество экземпляров** требуется указать количество экземпляров, создаваемых КНПС для каждого из заданных абонентов.

Кнопка **Создать** запускает непосредственно процесс создания ключей абонентов формата **Фактор-MS.** При нажатии данной кнопки предложено вставить USB-носитель для записи ключевой информации (рис. 6.8) и выбрать логический диск (рис. 6.9).

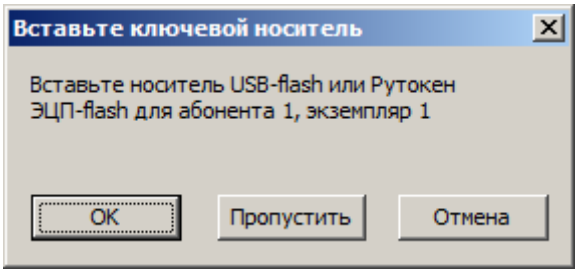

Рис.6.8

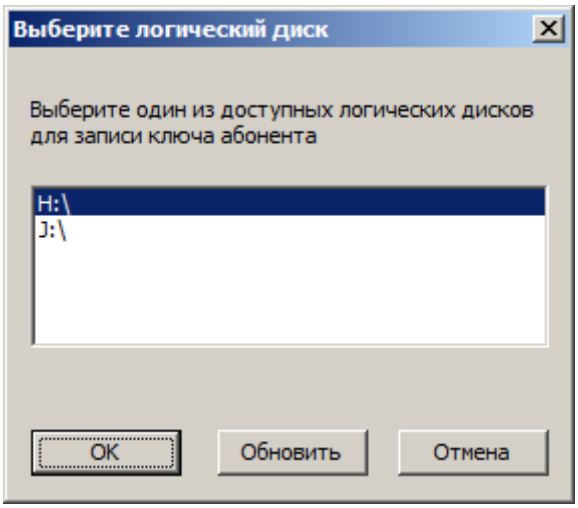

Рис 6.9.

Замечание. Формат **Фактор-MS** доступен для записи только на носители **USB-flash** или **Рутокен ЭЦП flash**. Запись ключей данного формата на **RuToken (USB)** и **EToken (USB)** не поддерживается ввиду ограниченного свободного места защищённой памяти данных типов носителей.

После завершения процесса создания информации и ее записи на носитель на экран будет выведено соответствующее сообщение (Рис. 6.10)

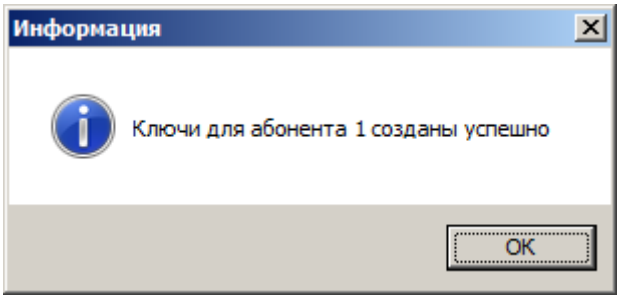

Рис 6.10.

7. Копирование ключевых данных КНМК

Для обеспечения надежности хранения ключевой информации на КНМК в связи с высоким риском физической порчи носителей необходимо создание дополнительных экземпляров ключевых носителей с мастер-ключом (дубликатов) на рабочем месте оператора АРМ ГК-4.

Программа **Копирование ключевых данных** выполняет копирование мастер-ключа и служебной информации с исходного КНМК на дополнительный КНМК (дубликат).

После запуска программы на экран будет выведено окно **Копирование мастер-ключа** (Рис. 7.1).

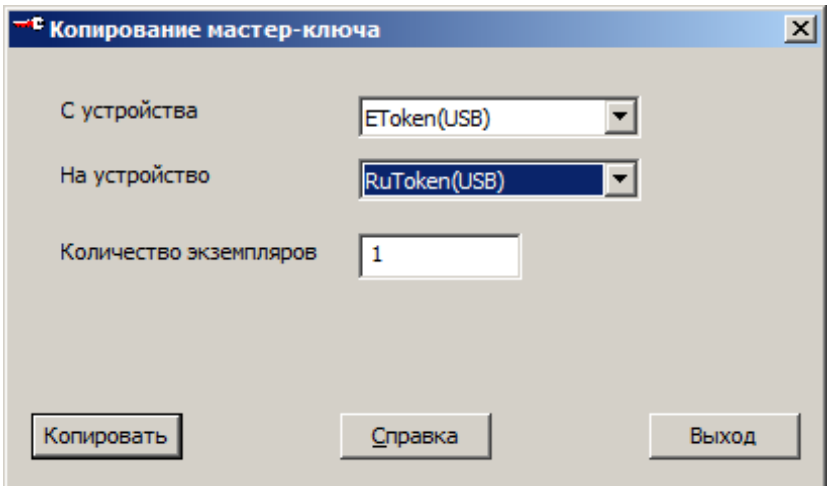

Рис. 7.1

Справку по работе с программой можно получить, нажав кнопку **Справка.**

Поле **С устройства** содержит раскрывающийся список типов доступных устройств - сменных носителей:

- **USB-flash**;
- **RuToken(USB)**;
- **EToken(USB)**.

Из данного списка необходимо выбрать сменный носитель, который является исходным для копирования (на Рис. 7.1– **EToken(USB)**).

Поле **На устройство** содержит раскрывающийся список типов сменных носителей, аналогичный приведенному выше. Из данного списка необходимо выбрать устройство, которое будет использоваться оператором для копирования на него информации с исходного для копирования носителя (на Рис. 7.1 – **RuToken(USB)**).

При выбранном элементе списков **USB-flash** также доступно копирование с логического диска носителя (на логический диск) носителя **Рутокен ЭЦП flash.**

В поле **Количество экземпляров** необходимо ввести желаемое количество экземпляров ключевого носителя.

Процесс копирования ключевой информации запускается нажатием кнопки **Копировать**.

Программа выполнит временное сохранение содержимого исходного для копирования носителя в оперативную память и запросит устройство, на которое будет перенесена копируемая информация.

После заполнения описанных выше полей окна **Копирование мастер-ключа** и нажатия кнопки **Копировать** (Рис. 7.1) необходимо вставить исходный для копирования носитель в разъем компьютера.

При копировании ключевых данных с носителя типа **USB-flash** в появившемся окне необходимо выбрать логический диск для считывания мастер-ключа, после чего на экран будет выдано информационное сообщение, содержащее данные о серии мастер-ключа и размере сети (рис. 7.2).

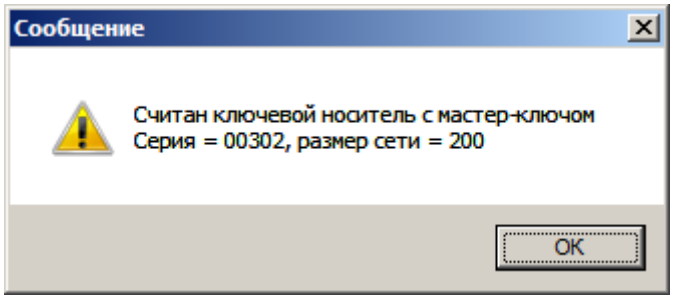

Рис. 7.2

При копировании ключевых данных на носитель типа **USB-flash** следует выбрать логический диск для записи, после чего начнется процесс копирования ключевой информации.

При копировании ключевых данных с устройств **RuToken (USB)** или **EToken (USB)** программа потребует ввода пароля носителя, а также, при использовании **RuToken (USB)**, указания номера папки с ключевой информацией на исходном носителе (Рис. 7.3).

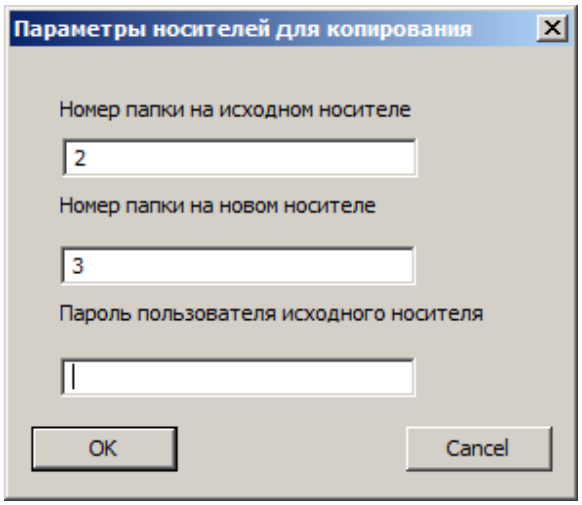

Рис. 7.3

При копировании ключевых данных на устройства **RuToken (USB)** программа потребует ввода номера папки, в которую будет помещена ключевая информация (Рис. 7.3).

Для носителей **RuToken (USB)** и **EToken (USB)** необходимо ввести пароль пользователя (Рис. 7.4, Рис. 7.5)

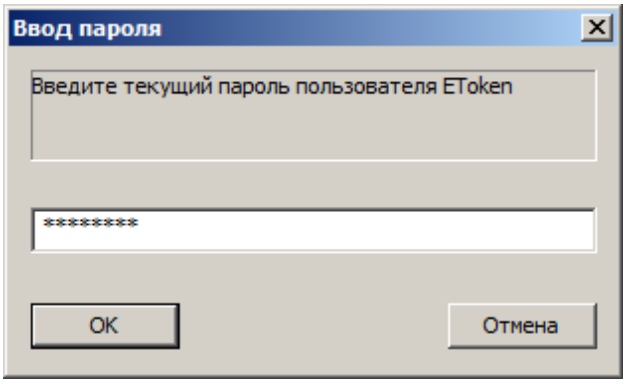

Рис. 7.4

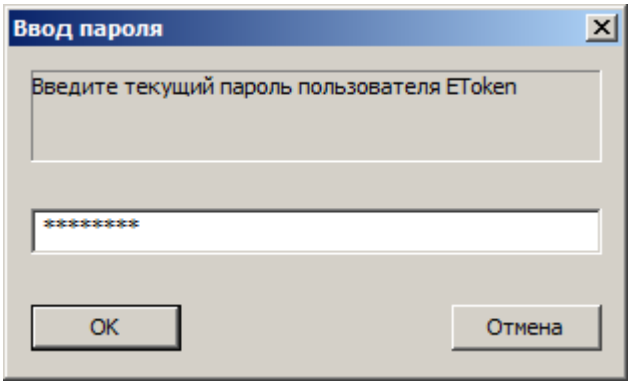

Рис. 7.5

При успешном завершении копирования данных ключевого носителя выдаются соответствующие сообщения (Рис. 7.6).

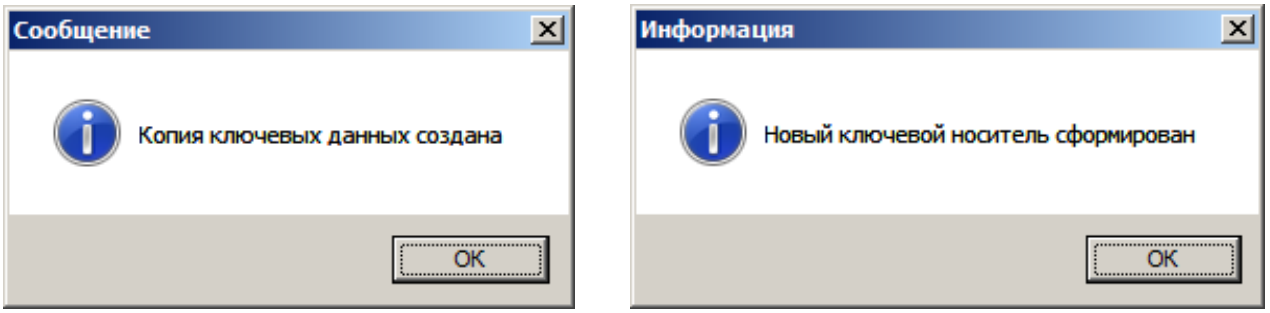

Рис. 7.6

В процессе копирования данных ключевого носителя возможно возникновение следующих ошибочных ситуаций:

- Носитель, являющийся исходным для копирования, не готов для считывания информации с него. Программа выдаст сообщение об ошибочной ситуации. Необходимо подготовить устройство для считывания.
- Носитель, на который будет записываться информация с исходного носителя, не готов для записи. Программа выдаст сообщение об ошибочной ситуации. Необходимо подготовить устройство для записи.
- Информация исходного ключевого носителя была испорчена. Программа выдаст сообщение об ошибочной ситуации.
- Ключевой носитель с мастер-ключом является просроченным: прошло больше трёх лет с момента формирования исходного КНМК.
- Исходный для копирования носитель содержит информацию, отличную от состава ключевой информации КНМК. Перед копированием данных исходного носителя производится определение типа содержащейся на нем информации. Копирование данных носителя не производится, если на нем содержится информация, отличная от ключевой информации КНМК. Программа выдаст соответствующее сообщение.

Выйти из программы можно в любой момент нажатием кнопки **Выход** (Рис. 7.1).

Примечание. Срок действия дубликатов КНМК равен сроку действия исходного КНМК.

8. Уничтожение ключевой информации на КНПС

В случае вывода абонента с заданным номером из криптографической сети необходимо уничтожение одного или нескольких ключей парной связи по заданному направлению на рабочем месте оператора АРМ ГК-4. Программа **Стирание ключа** выполняет уничтожение ключей парной связи по заданному направлению.

После запуска программы на экран будет выведено окно **Уничтожение ключей по направлениям** (Рис. 8.1).

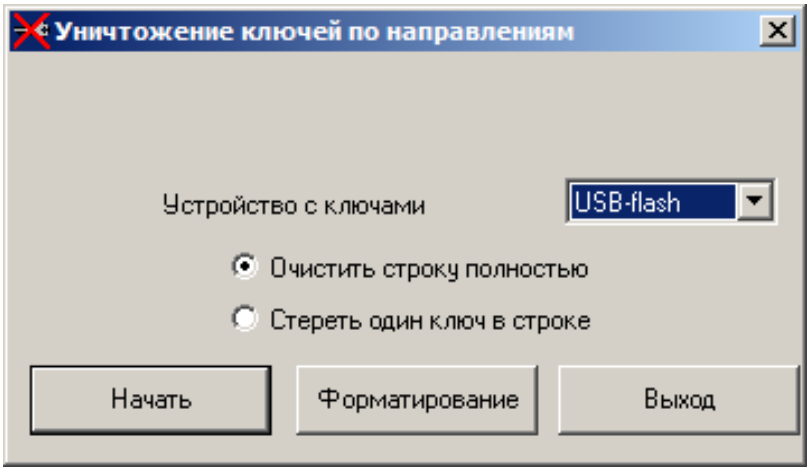

Рис. 8.1

Поле **Устройство с ключами** (Рис. 8.1) содержит раскрывающийся список типов устройств - сменных носителей с ключами парной связи (КНПС):

- **USB-flash**;
- **RuToken(USB)**;
- **EToken(USB)**.

Из данного списка необходимо выбрать ключевой носитель, с которого будет удален один или все ключи парной связи по заданному направлению. При выбранном типе ключевого носителя **USB-flash** также становится доступно использование носителя **Рутокен ЭЦП flash**.

Если выбран носитель **RuToken (USB)**, то активизируется поле **Номер папки на ключевом носителе**, в которое необходимо внести номер удаляемой папки с ключами парной связи.

В АРМ ГК-4 предусмотрены две операции с ключами:

- уничтожение всех ключей в случае компрометации ключевой информации (переключатель **Очистить строку полностью**);
- уничтожение одного ключа парной связи (переключатель **Стереть один ключ в строке**).

Процесс уничтожения ключей запускается нажатием кнопки **Начать**.

Кнопка **Форматирование** запускает принудительное удаление ВСЕЙ информации на носителе типа **USB-flash** с обязательным предварительным заполнением содержимого ключевых файлов псевдослучайной последовательностью чисел. Удален может быть как КНПС *любого* формата, так и КНМК.

Для форматирования носителей **RuToken (USB)** или **EToken (USB)** требуется использовать штатные утилиты производителей данных изделий.

После заполнения полей окна **Уничтожение ключей по направлениям**, выбора способа уничтожения ключей и нажатия кнопки **Начать** (Рис. 8.1) необходимо вставить КНПС указанного типа.

Если требуется уничтожить ключи на носителе **USB-flash**, то далее следует выбрать логический диск для считывания ключевой информации (Рис. 8.2).

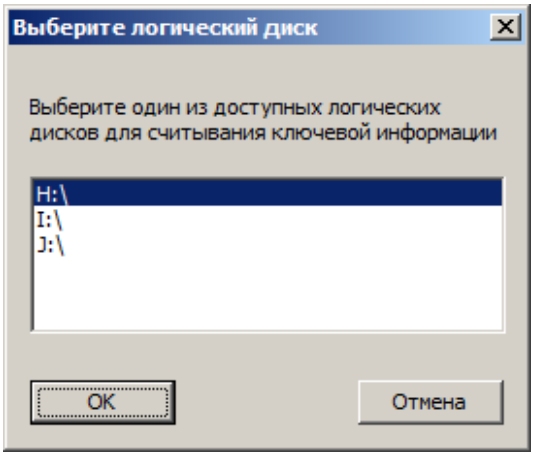

Рис. 8.2

При использовании КНПС формата **Фактор-М, Фактор-MS** или **Фактор-КБ2М** пользователю будет предложено выбрать для уничтожения один из доступных на данном носителе ключей (Рис. 8.3).

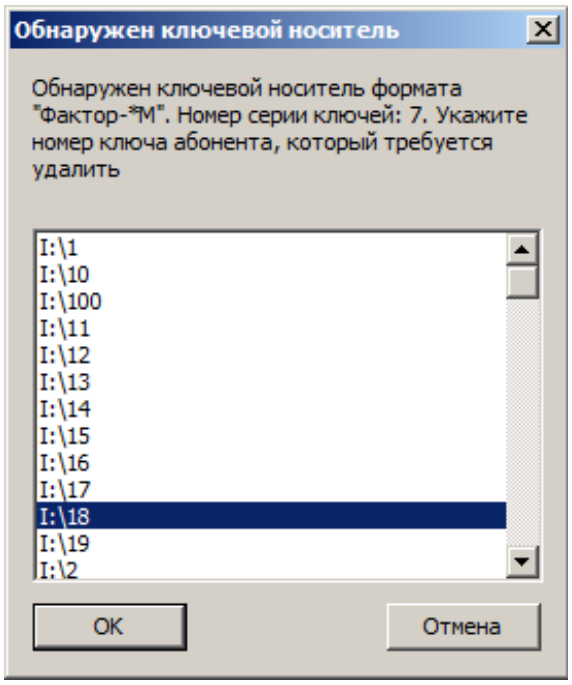

Рис. 8.3

Если требуется уничтожить информацию на носителе **RuToken (USB)** или **EToken (USB)**, то для дальнейшей работы необходимо ввести пароль пользователя (Рис. 8.4).

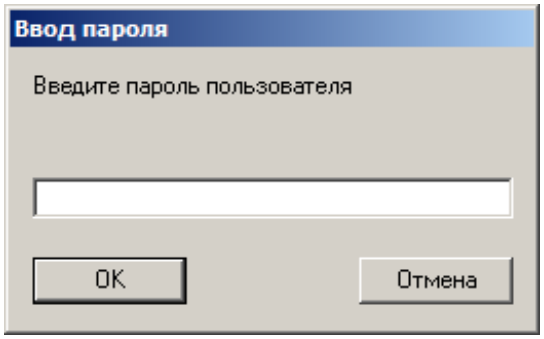

Рис. 8.4

При уничтожении одного ключа парной связи программа выдаст информацию об обнаруженном ею КНПС (серию, номер, размер сети) и на экран будет выведено окно **Стирание ключа на ключевом носителе** (Рис. 8.5).

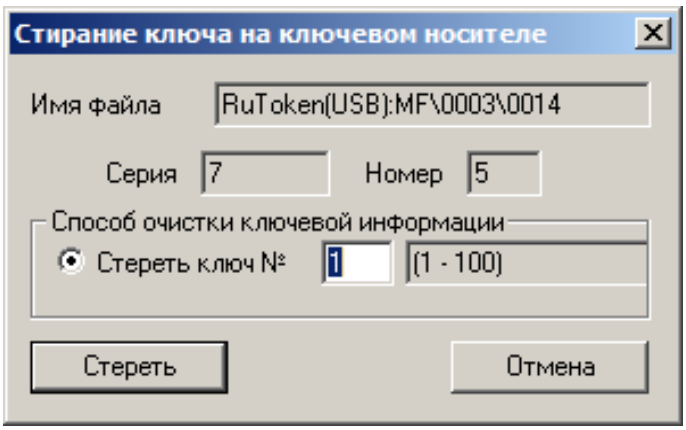

Рис. 8.5

Процесс уничтожения ключа парной связи по заданному направлению запускается нажатием кнопки **Стереть** (Рис. 8.5).

Нажатие на кнопку **Отмена** возвращает пользователя в окно **Уничтожение ключей по направлениям** (Рис. 8.1).

Поле **Имя файла** (Рис. 8.5) показывает имя файла, который содержит сетевые наборы ключей парной связи. Данное поле заполняется программой автоматически после считывания информации с КНПС и не подлежит изменению пользователем.

Поле **Серия** содержит серию сетевых наборов ключей парной связи. Данное поле заполняется программой автоматически после считывания информации с КНПС и не подлежит изменению пользователем.

Поле **Номер** показывает номер абонента, *для которого* необходимо уничтожить ключ парной связи. Данное поле заполняется программой автоматически после считывания информации с КНПС и не подлежит изменению пользователем.

В поле **Стереть ключ №** вводится направление уничтожения ключа парной связи, т.е. номер абонента криптографической сети, связь *с которым* у данного абонента уничтожается. В соседнем поле показан диапазон возможных направлений уничтожения связи.

После того, как будет заполнено поле **Стереть ключ №** в окне **Стирание ключа на ключевом носителе** (Рис. 8.5) и нажата кнопка **Стереть**, программой будет выдан дополнительный запрос на подтверждение удаления ключа с КНПС, т.к. данная операция является необратимой (Рис. 8.6).

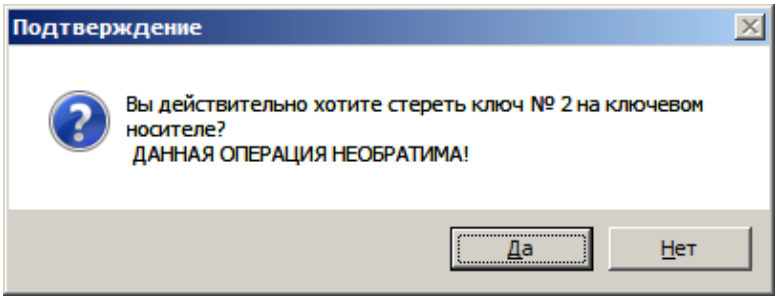

Рис. 8.6

После подтверждения программа удалит выбранный ключ парной связи. В случае успешного удаления выдается соответствующее сообщение.

При уничтожении всех ключей программа стирает всю ключевую строку, главный ключ, а также серию и номер абонента.

При нажатии кнопки **`Форматирование`** окна **Уничтожение ключей по направлениям** (Рис. 8.1) запускается процедура удаления всей ключевой информации.

Также потребуется выбрать логический диск носителя **`USB-flash`** (Рис. 8.2). Поскольку данная операция является полностью необратимой, то пользователю будет выдано предупреждение, отображенное на Рис. 8.7:

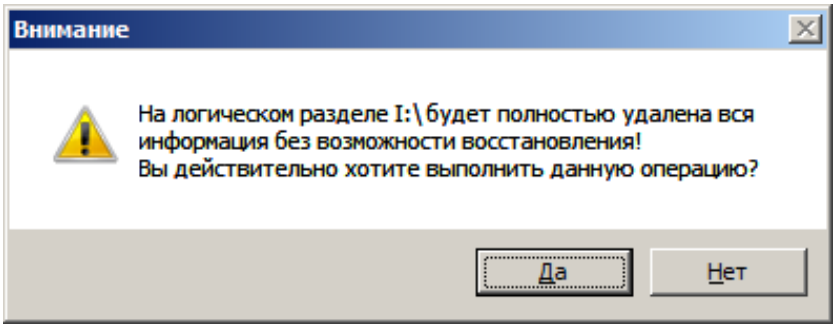

Рис. 8.7

При утвердительном ответе запускается процедура удаления содержимого на данном логическом диске, которая будет завершена сообщением, отображенным на Рис. 8.8, либо сообщением об ошибке в случае возникновения внештатной ситуации.

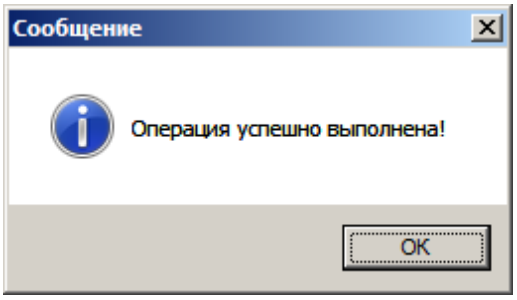

Рис. 8.8

В процессе удаления выбранного ключа парной связи возможно возникновение следующих ошибочных ситуаций:

- Носитель не готов для считывания информации с него. Программа выдаст сообщение об ошибочной ситуации. Необходимо подготовить устройство для удаления ключа парной связи.
- При выполнении операций удаления ключей парной связи информация на КНПС испорчена или содержит недопустимые данные. Программа выдаст сообщение об ошибочной ситуации.

- В поле **Стереть ключ №** было введено значение, не являющееся числом, или число, выходящее из диапазона возможных направлений уничтожения связи. Программа выдаст сообщение об ошибочной ситуации.
- Неверно введен пароль абонента при стирании ключевой информации с носителя **RuToken (USB)** или **EToken (USB)**. Программа выдаст сообщение об ошибочной ситуации.
- Неверно введен пароль пользователя при полной очистке информации с носителя **RuToken (USB)**. Программа выдаст сообщение об ошибочной ситуации.
- Невозможно запустить утилиту форматирования **EToken (USB)**. Программа выдаст сообщение об ошибочной ситуации.

Выйти из программы можно в любой момент нажатием кнопки **Выход** (Рис. 8.1).

9. Ведение журнала работы «АРМ ГК-4»

В ходе работы ПО АРМ ГК-4 предусмотрено обязательное автоматическое ведение журнала в электронном виде. Данный журнал предназначен для хранения сведений о формировании экземпляров ключевых носителей, а также сведений о стирании ключей с ключевых носителей.

Файл, содержащий данную информацию, называется **journal.txt** и хранится в папке установки ПО АРМ ГК-4. Просмотреть данный файл возможно с помощью любого стандартного для ОС WINDOWS текстового редактора (например, WordPad) или средствами ПО АРМ ГК-4 (с помощью программ **Генерация ключей абонента** и **Генерация ключей абонента формата Фактор (MS)**).

Ниже приведен пример фрагмента журнала.

journal.txt:

```
14-02-2013 13:26 Удаление ключа с КНПС (формат "Фактор-КБ2") серии
412 для абонента 7, стерт ключ 3

28-02-2013 17:45 Создан мастер-ключ серии 16, число абонентов 4
Ключ записан на носитель EToken(USB) в папку 3, количество копий: 1

01-03-2013 13:31 Создан мастер-ключ серии 17, число абонентов 4
Ключ записан на стандартный USB-носитель, количество копий: 1

01-03-2013 13:38 Созданы ключи серии 11 для абонента 1 (Копия 1 из
1) Ключи записаны на носитель F:\

01-03-2013 13:41 Созданы ключи серии 11 для абонента 1
Ключи сохранены на носителе RuToken в папку 5 (Копия 1 из 1)

01-03-2013 13:43 Скопирован мастер-ключ серии 11, размер сети: 4
Количество копий: 1

01-03-2013 13:43 Скопирован мастер-ключ серии 11, размер сети: 4
Количество копий: 1

01-03-2013 13:46 Созданы ключи формата "Фактор-КБ2М", серии 11 для
абонента 1 (Копия 1) Ключи записаны в папку F:\1

01-03-2013 13:46 Созданы ключи формата "Фактор-КБ2М", серии 11 для
абонента 2 (Копия 1) Ключи записаны в папку F:\2

01-03-2013 13:46 Созданы ключи формата "Фактор-КБ2М", серии 11 для
абонента 3 (Копия 1) Ключи записаны в папку F:\3

01-03-2013 13:46 Созданы ключи формата "Фактор-КБ2М", серии 11 для
абонента 4 (Копия 1) Ключи записаны в папку F:\4

01-03-2013 13:50 Скопирован мастер-ключ серии 11, размер сети: 14

01-03-2013 13:52 Удалены ключи с носителя КНПС серии 11 с номером
абонента 1
```

Лист регистрации изменений

Номер изменения	Номера листов (страниц) изменённых	заменённых	новых	аннулированных	Всего листов (стр.) в документе	№ документа	Входящий № сопроводительного документа	Подпись	Дата
1		все				НКБГ.142-18			26.04.2018
2		все				И57/Д			04.02.2019