

# ФАКТОР-ТС

## Автоматизированное рабочее место генерации ключей Версия 3.0

### *Руководство пользователя*

НКБГ.501430.735И6

Листов 27

<i>Инв. № подл.</i>	<i>Подпись и дата</i>
<i>Взам. инв. №</i>	<i>Инв. № дубл.</i>
<i>Подпись и дата</i>	<i>Подпись и дата</i>

## Содержание

<b>1. Общие положения.....</b>	<b>4</b>
1.1. <i>Распределение ключей с использованием симметричной ключевой системы .....</i>	<i>4</i>
1.2. <i>Принципы работы АРМ ГК.....</i>	<i>6</i>
1.2.1. <i>Подготовка АРМ ГК к эксплуатации .....</i>	<i>6</i>
1.2.2. <i>Генерация ключей.....</i>	<i>6</i>
1.2.3. <i>Дополнительные копии ключевых носителей .....</i>	<i>6</i>
1.2.4. <i>Этикетки ключевых носителей .....</i>	<i>7</i>
1.3. <i>Преодоление последствий компрометации ключей.....</i>	<i>7</i>
1.4. <i>Требования к срокам действия ключевых носителей и к организации хранения, уничтожения и заказа ключевых носителей .....</i>	<i>8</i>
1.5. <i>Состав ЦГК .....</i>	<i>9</i>
<b>2. Установка ПО АРМ ГК.....</b>	<b>10</b>
<b>3. Генерация ключевого носителя с мастер-ключом.....</b>	<b>12</b>
<b>4. Генерация ключевых носителей с сетевыми наборами ключей парной связи .....</b>	<b>15</b>
<b>5. Копирование ключевых носителей КНМК и КНПС.....</b>	<b>21</b>
<b>6. Генерация ключевого носителя с исходным материалом.....</b>	<b>23</b>
<b>7. Уничтожение ключевой информации на КНПС .....</b>	<b>24</b>
<b>8. Ведение журнала работы АРМ ГК.....</b>	<b>26</b>
<b>9. Состав ключевой информации .....</b>	<b>27</b>
9.1. <i>Состав ключевой дискеты (флеш-диска) КНМК .....</i>	<i>27</i>
9.2. <i>Состав ключевой дискеты (флеш-диска) КНПС.....</i>	<i>27</i>
9.3. <i>Состав ключевой дискеты (флеш-диска) КНИМ.....</i>	<i>27</i>
9.4. <i>Состав ключевого носителя RuToken, содержащего КНПС .....</i>	<i>27</i>
9.5. <i>Состав ключевого носителя EToken, содержащего КНПС .....</i>	<i>27</i>

## Список терминов

Термин	Определение
<b>Криптографическая защита</b>	Защита данных при помощи криптографического преобразования данных
<b>Криптографическое преобразование данных</b>	Преобразование данных при помощи алгоритма шифрования, имитозащиты, электронной цифровой подписи <sup>1</sup>
<b>Алгоритм шифрования (шифр)</b>	Набор логических правил, определяющих взаимно однозначное преобразование множества открытых данных во множество зашифрованных
<b>Шифратор</b>	Алгоритм шифрования, реализованный аппаратным, аппаратно-программным или программным образом
<b>Ключ шифрования</b>	Переменный параметр алгоритма шифрования, сохраняемый в тайне
<b>Зашифрование данных</b>	Процесс преобразования открытых данных в зашифрованные при помощи шифра
<b>Расшифрование данных</b>	Процесс преобразования зашифрованных данных в открытые при помощи шифра
<b>Шифрование</b>	Процесс зашифрования или расшифрования данных
<b>Криптографическая сеть</b>	Совокупность узлов сети связи, между которыми ведется обмен информацией с использованием криптографической защиты
<b>Мастер-ключ</b>	Ключевая информация, необходимая для генерации ключей парной связи заданной серии
<b>Исходный материал</b>	Ключевая информация, необходимая для генерации мастер-ключа
<b>Ключ парной связи</b>	Ключ, который используется в шифре для связи двух абонентов
<b>Сетевая таблица</b>	Квадратная матрица ключей парной связи всех узлов криптографической сети
<b>Сетевой набор ключей (сетевой набор)</b>	Строка сетевой таблицы, содержащая набор ключей парной связи данного узла для связи со всеми другими узлами криптографической сети
<b>Номер серии ключей (серии сетевой таблицы)</b>	Цифровой идентификатор сетевой таблицы, действующей в данной криптографической сети в течение заданного срока
<b>Ключевой носитель</b>	Носитель, содержащий ключевую информацию
<b>Ключевой носитель с исходным материалом (КНИМ)</b>	Ключевой носитель, содержащий информацию, необходимую для формирования средствами АРМ ГК ключевых носителей с мастер-ключом
<b>Ключевой носитель с мастер-ключом (КНМК)</b>	Ключевой носитель, содержащий информацию, необходимую для формирования средствами АРМ ГК ключевых носителей с ключами парной связи
<b>Ключевой носитель с ключами парной связи (КНПС)</b>	Ключевой носитель, содержащий сетевой набор ключей
<b>Программный датчик случайных чисел (ПДСЧ)</b>	Реализованный программным образом алгоритм выработки псевдослучайных последовательностей
<b>Программно-клавиатурный датчик случайных чисел (ПКДСЧ)</b>	Реализованный программным образом алгоритм выработки случайных последовательностей, учитывающий индивидуальные особенности использования оператором ПЭВМ клавиатуры или манипулятора «мышь».
<b>Компрометация ключей</b>	Несанкционированное разглашение ключевой информации

<sup>1</sup> Термины «Алгоритм имитозащиты» и «Электронная цифровая подпись» в данном руководстве не используются

# 1. Общие положения

Изделие «Автоматизированное рабочее место «Центр генерации ключей», НКБГ.5014306.712 (далее **АРМ ГК**) выполняет генерацию ключей для средств криптографической защиты информации (**СКЗИ**), используемых в технологии ДИОНИС.

Указанные СКЗИ используют алгоритм шифрования ГОСТ 28147-89 Системы обработки информации. Защита криптографическая.

АРМ ГК сертифицирован в системе сертификации ФСБ по уровням защищенности КС1, КС2 и КС3 согласно «Требованиям к средствам криптографической защиты конфиденциальной информации».

Уровень защищенности КС1 гарантирует безопасную эксплуатацию АРМ ГК в условиях, когда на местах эксплуатации АРМ ГК отсутствуют внутренние нарушители (допускается наличие только внешних нарушителей).

Уровень защищенности КС2:

- гарантирует безопасную эксплуатацию АРМ ГК в условиях, когда на местах эксплуатации допускается наличие внутреннего нарушителя, который не является пользователем АРМ ГК;
- предусматривает эксплуатацию АРМ ГК только при условии его укомплектования сертифицированным ФСБ аппаратным модулем доверенной загрузки (электронным замком);
- предусматривает генерацию ключевой информации программным датчиком случайных чисел (ПДСЧ), который инициализируется исходным материалом, предоставляемым уполномоченной организацией (ФСБ).

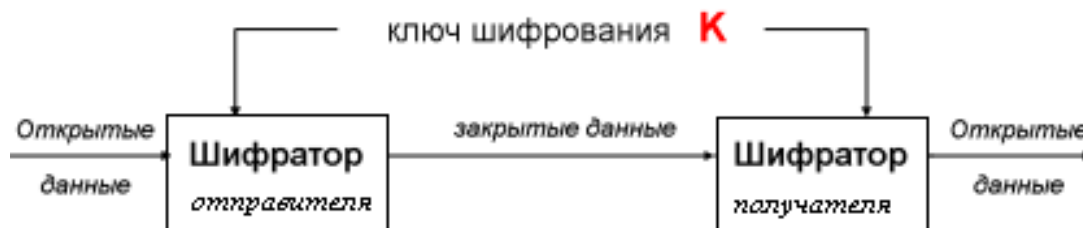
Для обеспечения безопасной эксплуатации АРМ ГК по уровню защищенности КС3 требуется:

- комиссия (совместная) работа ответственных лиц, допущенных к работе с АРМ ГК;
- хранение ключевого носителя с мастер-ключом в сейфе, опечатанном всеми ответственными лицами;
- использование АПМДЗ, имеющего защиту от логического отключения из BIOS-Setup, имеющего возможность создания функционально-замкнутой среды а также позволяющего выполнить вход в ОС только под учетной записью, прошедшей аутентификацию АПМДЗ.

Для генерации ключей в АРМ ГК кроме исходного материала используются случайные последовательности, вырабатываемые оператором с помощью программно-клавиатурного датчика случайных чисел (ПКДСЧ).

## 1.1. Распределение ключей с использованием симметричной ключевой системы

Алгоритм шифрования 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).



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

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

Указанный способ обеспечения ключами узлов криптографической сети называется **симметричной ключевой системой**.

Опишем некоторые принципы реализации симметричной ключевой системы для АРМ ГК.

Криптографическим номером называют порядковый номер узла в криптографической сети.

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

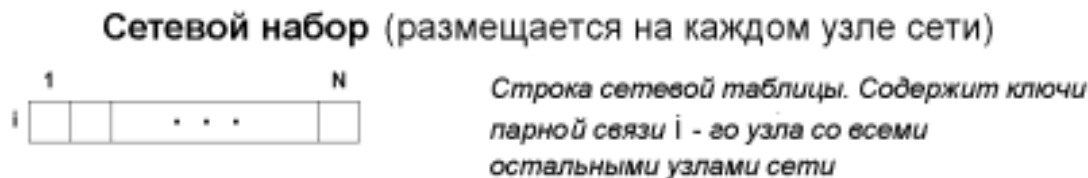
*Замечание.* Принцип работы АРМ ГК, в действительности, не предусматривает изготовление сетевой таблицы (см. раздел 1.2. ). Здесь она рассматривается лишь для наглядности описания симметричной ключевой системы.

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

В этом смысле 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  $K_{i,j} = K_{j,i}$ .



На АРМ ГК для каждого узла формируется свой сетевой набор ключей - строка сетевой таблицы, соответствующая криптографическому номеру узла:



Средствами АРМ ГК предусмотрена возможность создания неполной (разреженной) ключевой строки, в которую будут записаны только указанные элементы.

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

Ключи парной связи имеют ограниченный срок действия. Максимальный срок действия ключей парной связи - один год - установлен ФСБ. Эксплуатирующей организацией может быть установлен меньший срок. По истечении срока действия ключей производится их плановая замена (см. раздел 1.4. ). Она заключается в выработке 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.

## 1.2. Принципы работы АРМ ГК

### 1.2.1. Подготовка АРМ ГК к эксплуатации

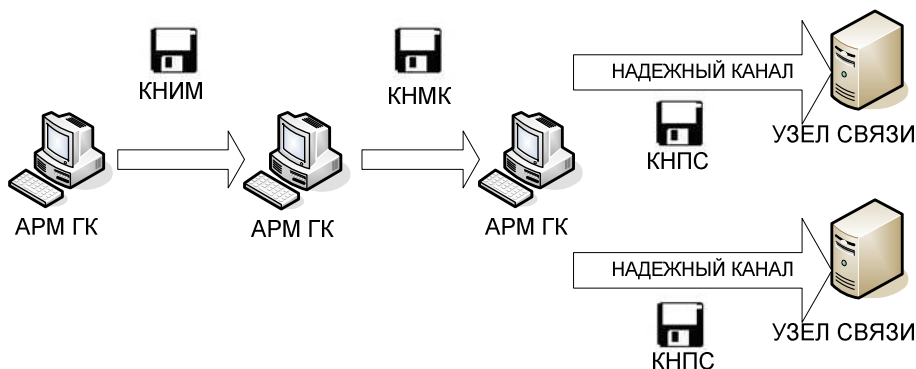
Для подготовки АРМ ГК к эксплуатации необходимо:

1. В соответствии с разделом 2 данного руководства установить ПО АРМ ГК.
2. Для уровней защищенности КС2, КС3 в соответствии с эксплуатационной документацией установить электронный замок.
3. В соответствии с разделом 6 данного руководства средствами АРМ ГК изготовить ключевой носитель с исходным материалом (КНИМ).

### 1.2.2. Генерация ключей

Генерация ключей и ключевых носителей заданной серии на АРМ ГК выполняется в следующем порядке.

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



Таким образом, ключевой носитель с мастер-ключом (КНМК) изготавливается на АРМ ГК на основе исходного материала (с ключевого носителя КНИМ, изготовленного на АРМ ГК). Информацию, записанную на КНМК, АРМ ГК использует для изготовления сетевых наборов ключей парной связи (КНПС).

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

- вычислить ключи парной связи и изготовить 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 генерацию ключевых носителей для новых узлов в случае увеличения размерности сети.

В отличие от технологий, предполагающих предварительное изготовление сетевой таблицы, в данном случае алгоритм работы АРМ ГК позволяет избежать формирования и хранения сетевой таблицы на жестком магнитном диске (сетевые наборы записываются *ТОЛЬКО* на ключевые носители узлов).

В результате при выключенном питании АРМ ГК ни в какой момент времени не содержит ключевой информации.

Ключевые носители КНПС должны быть доставлены на узлы связи обязательно по защищенному («надежному») каналу связи, например, фельдъегерской почтой либо с использованием телекоммуникационных средств, но обязательно с применением независимого контура криптографической защиты.

### 1.2.3. Дополнительные копии ключевых носителей

Для обеспечения надежности хранения ключевой информации на ключевых носителях необходимо с помощью АРМ ГК изготовить несколько копий ключевых носителей (КНМК и КНПС), либо воспользоваться специальной программой копирования ключевых носителей, входящей в комплект поставки АРМ ГК (см. раздел 5).

**ВНИМАНИЕ!** На носители КНМК и КНПС кроме ключей записывается служебная информация, необходимая для инициализации ПДСЧ, входящих в состав СКЗИ узлов. При изготовлении любой дополнитель-

ной копии ключевого носителя данная информация обновляется, что существенно для безопасной работы СКЗИ. Поэтому изготовление дополнительных копий ключевых носителей допускается *ТОЛЬКО* средствами АРМ ГК. Изготовление копий другими средствами приводит к нарушению стойкости СКЗИ.

Изготовление дополнительного ключевого носителя КНИМ для АРМ ГК не обязательно. В случае его выхода из строя в любой момент времени можно изготовить новый ключевой носитель КНИМ.

#### 1.2.4. Этикетки ключевых носителей

1. На этикетку ключевого носителя КНИМ должно быть нанесено наименование ключевого носителя КНИМ.
2. На этикетку ключевого носителя КНМК должны быть нанесены:
  - наименование ключевого носителя КНМК;
  - номер серии;
  - номер копии носителя КНМК;
  - количество узлов в сети.
3. На этикетку ключевого носителя КНПС должны быть нанесены:
  - наименование ключевого носителя КНПС;
  - номер серии;
  - криптографический номер узла;
  - номер копии носителя КНПС.

### 1.3. Преодоление последствий компрометации ключей

В данном разделе сформулированы *рекомендации* по преодолению последствий компрометации ключей.

Мероприятия по восстановлению связи после компрометации ключей предполагают наличие в сети Центра управления ключевой системой (ЦУКС).

В целях восстановления связи в сети после компрометации ключей рекомендуется изготавливать так называемые **резервные ключевые носители**.

Для этого формируются сетевые наборы размера **большого**, чем число **N** узлов в сети.

Поясним это на примере. Пусть в сети связи имеется 10 абонентов. При изготовлении ключевого носителя с мастер-ключом зададим размерность сети **N** равную 25.

При изготовлении ключевых носителей КНПС узлу с номером 1 выделим носитель с криптографическим номером 1, узлу с номером 2 - носитель с номером 2 и т.д. Наконец, узлу с номером 10 выделим носитель с криптографическим номером 10.

Далее, дополнительно, узлу с номером 1 выделим носитель с криптографическим номером 11, узлу с номером 2 - носитель с номером 12 и т.д. Наконец, узлу с номером 10 выделим носитель с криптографическим номером 20.

Ключевые носители с криптографическими номерами 1-10 и 11-20 доставляются на места эксплуатации.

Таким образом, каждому узлу выдается по два ключевых носителя. Ключевой носитель с *меньшим* криптографическим номером будем называть *действующим*, а ключевой носитель с *большим* криптографическим номером будем называть *резервным*. Например, узлу с номером 2 выдается действующий ключевой носитель с криптографическим номером 2 и резервный ключевой носитель с криптографическим номером 12.

*Неиспользованные* ключевые носители с криптографическими номерами 21, 22, ..., 25 остаются в распоряжении ЦУКС в качестве *резерва* ЦУКС.

Узлы связи	№1	№2	...	№10	Резерв Администратора ЦУКС
Действующий криптономер	1	2	...	10	21-25
Резервный криптономер	11	12	...	20	

**ВНИМАНИЕ!** Резервные и действующие ключевые носители должны храниться на узлах связи с использованием мер, исключаяющих их одновременную компрометацию.

Администраторы узлов сначала вводят в эксплуатацию действующие ключевые носители.

В случае компрометации действующих ключевых носителей администратор узла имеет возможность оперативно ввести в действие имеющийся у него резервный ключевой носитель (сделав его действующим), сведя к минимуму последствия потери связи.

В адрес скомпрометированного узла должен быть направлен ключевой носитель из числа резерва ЦУКС, чтобы на данном узле всегда находились два ключевых носителя (действующий и резервный).

*ВНИМАНИЕ!* Участники сети связи должны быть оповещены о введении в действие на данном узле ключевого носителя с новым криптографическим номером.

В случае включения в сеть связи нового узла, администратор данного узла должен получить два ключевых носителя из числа резерва (действующий и резервный).

В приведенном примере для сети связи из  $N$  узлов ( $N=10$ ) было изготовлено  $2N+0.5\bullet N$  ключевых носителей КНПС, из которых  $2N$  доставлено на места эксплуатации и  $0.5\bullet N$  оставлено в распоряжении администратора АРМ ГК.

Возможно решение, когда изготавливается любое другое число резервных ключевых носителей, например  $N+R, 3\bullet N$ , из которых  $N$  доставляется на узлы, а  $R, 3\bullet N$  остаются в резерве администратора АРМ ГК (резервные ключевые носители в этом случае заранее на узлы не доставляются).

*Замечание.* Число изготавливаемых резервных ключевых носителей определяется **политикой безопасности** эксплуатирующей организации.

При изготовлении резервных и действующих ключевых носителей **следует** предусмотреть изготовление средствами АРМ ГК **нескольких копий** данных носителей на случай их физической порчи.

#### **1.4. Требования к срокам действия ключевых носителей и к организации хранения, уничтожения и заказа ключевых носителей**

Срок действия ключевых носителей КНИМ, КНМК и КНПС – не более 1 года.

Эксплуатирующей организацией может быть установлен и меньший срок.

По истечении установленного срока ключевая информация на ключевых носителях КНИМ, КНМК и КНПС должна быть уничтожена.

По истечении срока действия носителя с исходным материалом (КНИМ) средствами АРМ ГК должен быть изготовлен новый ключевой носитель.

Ключевые носители КНМК и КНПС очередной серии изготавливаются по мере необходимости. Время действия ключевых носителей КНМК и КНПС одной серии **должно** совпадать.

Изготовленные ключевые носители (КНИМ, КНМК и КНПС) следует хранить в сейфе пользователя АРМ ГК (для уровня защищенности КСЗ ключевые носителя хранятся только в сейфе, опечатанном всеми ответственными лицами, допущенными к работе на АРМ ГК). Пользователи АРМ ГК несут ответственность за сохранность данных ключевых носителей при их хранении.

При наличии в организации, эксплуатирующей АРМ ГК, подразделения, обеспечивающего централизованное хранение ключевых носителей, последние должны храниться в сейфе уполномоченных лиц данного подразделения и выдаваться пользователям АРМ ГК с отметкой в «Журнале учета ключевых носителей». Уполномоченные лица указанного подразделения несут персональную ответственность за сохранность ключевых носителей при их хранении.

Уничтожение ключей на ключевых носителях выполняется в случае порчи ключевой информации, записанной на носитель, окончания срока действия ключей, а также в случае компрометации ключей.

В случае использования стандартного ключевого носителя стирание выполняется путем переформатирования носителей штатными средствами с физическим уничтожением информации на носителе, например, с использованием команды `format /u <имя носителя>`.

Для очистки ключевого носителя RuToken имеются встроенные в АРМ ГК программные средства, а для носителя EToken используется утилита ETFormat, запуск которой возможен из АРМ ГК. Установку данной утилиты следует выполнить в ту же папку, куда установлено ПО АРМ ГК.

Уничтожение ключевых носителей выполняется в случае физической неисправности данных носителей, делающих невозможным устойчиво правильное считывание ключей с данного носителя и запись ключей на данный носитель, а также выполнение операции стирания ключей на носителе.

Носитель, пришедший в негодность вследствие физической неисправности, должен быть уничтожен физически способом, исключающим возможность восстановления информации, записанной на ключевой носитель (сжигание, оплавление, измельчение).

### 1.5. Состав ЦГК

1. Персональная ЭВМ с операционной системой Windows 2000/XP/2003 Server с процессором семейства Pentium, объемом оперативной памяти 128 Мбайт и выше, с дисководом 3,5". Для уровней защищенности КС2, КС3 обязательно наличие свободного разъема системной шины стандарта PCI .
2. Для уровней защищенности КС2, КС3 сертифицированный ФСБ аппаратный модуль доверенной загрузки (электронный замок).
3. Программное обеспечение АРМ ГК:
  - программа проверки целостности ПО **CHECKWIN** и файл **checksum**;
  - программа генерации ключевых носителей с исходным материалом **GENSRC**;
  - программа генерации ключевых носителей с мастер-ключом **MASTERKEY**;
  - программа генерации ключевых носителей с сетевыми наборами ключей парной связи **GENKWIN**;
  - программа уничтожения с ключевых носителей КНМК ключа парной связи по заданному направлению, а также быстрой очистки ключевого носителя в случае компрометации **CLEARKEY**.

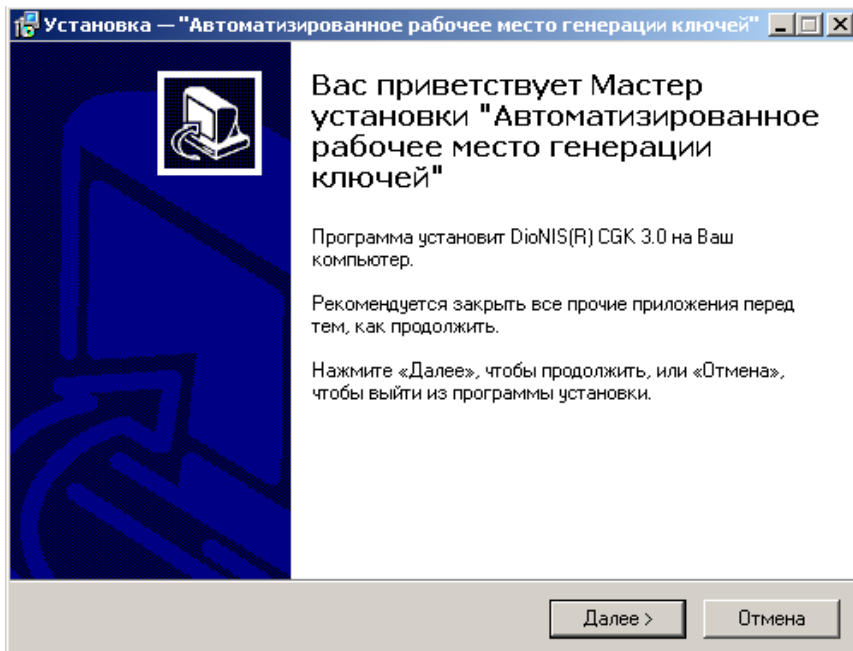
## 2. Установка ПО АРМ ГК

Программное обеспечение (ПО) АРМ ГК поставляется на одном носителе (гибком магнитном диске или на компакт-диске). Комплект поставки ПО состоит из единственного установочного файла **SETUP.EXE**, а также файлов с документацией.

Если в ходе работы предполагается запись сетевых наборов ключей парной связи на носители RuToken или EToken, то перед установкой ПО АРМ ГК требуется установить драйверы соответствующих устройств, в противном случае запись ключевой информации на данные устройства будет невозможна.

Инсталляция АРМ ГК возможна прямо с носителя, содержащего файл **SETUP.EXE**, или после копирования установочного файла **SETUP.EXE** на жесткий магнитный диск.

Начинается установка с предупреждающего сообщения:



Для инсталляции ПО АРМ ГК необходимо пройти через последовательность шагов, которые сопровождаются комментариями и являются стандартными для установки ПО в операционной системой Windows. Перед инсталляцией программа запросит папку, в которую будет установлено ПО АРМ ГК, и название рабочей группы в меню "Программы", в которую будет помещены ярлыки для запуска программ генерации ключевых носителей:

- генерация мастер-ключа;
- генерация ключей абонентов;
- генерация исходного материала.

Данные программы имеют названия **MASTERKEY** и **GENKWIN**.

Кроме того, в эту же рабочую группу помещаются служебные программы:

- копирование ключевых носителей;
- стирание ключа;
- проверка целостности ПО.

Данные программы называются соответственно **COPYKEY**, **CLEARKEY** и **CHECKWIN**.

По умолчанию программой предлагается название созданной рабочей группы «Центр генерации ключей».

*Рекомендации.* Выбор папки для установки **ПО АРМ ГК**. По умолчанию программой предлагается путь **C:\Program Files\Factor-TS\CGK**, который желательно не менять для удобства обновления версии программы. Хотя возможен выбор любой другой папки для установки ПО.

После установки ПО АРМ ГК необходимо проверить целостность полученного программного обеспечения программными средствами, поставляемыми с АРМ ГК, а также обеспечить контроль целостности ПО АРМ ГК с помощью АПМДЗ (для уровней защищенности КС2, КС3) в соответствии с Правилами пользования АРМ ГК, входящими в комплект поставки.

В качестве программного средства поставляется программа **CHECKWIN** и файл **chksum**, входящие в состав ПО АРМ ГК.

Файл **chksum** содержит список файлов программного обеспечения, подлежащих обязательной проверке, вместе с эталонными значениями контрольных сумм. Содержимое файла **chksum** дублируется в формуляре на изделие АРМ ГК. Оператор должен, прежде всего, сверить значения контрольных сумм файла **chksum** со значениями, содержащимися в формуляре на изделие АРМ ГК. И только убедившись в их идентичности, приступать к дальнейшей проверке.

Необходимо из меню «Центр генерации ключей» запустить программу **CHECKWIN**.

Программа вычислит контрольные суммы файлов, приведенных в списке, и сравнит их с эталонными. Если суммы совпадут, то программа выдаст сообщение, что контрольные суммы проверены успешно.

Если будет обнаружено несовпадение, то программа укажет файл, где имеет место ошибка контрольной суммы. В таком случае программное обеспечение *требует* обязательной замены.

Проверку целостности ПО АРМ ГК необходимо выполнять каждый раз при запуске АРМ ГК или периодически.

Периодичность проверки зависит от условий эксплуатации и определяется **политикой безопасности** эксплуатирующей организации.

### 3. Генерация ключевого носителя с мастер-ключом

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

Программа «Генерация мастер-ключа» (**MASTERKEY**) выполняет генерацию мастер-ключа и другой информации, необходимой для генерации сетевых наборов ключей парной связи, с последующей записью их на ключевой носитель КНМК.

После запуска программы **MASTERKEY** на экран будет выведено окно Изготовление мастер-ключа (Рис. 1).

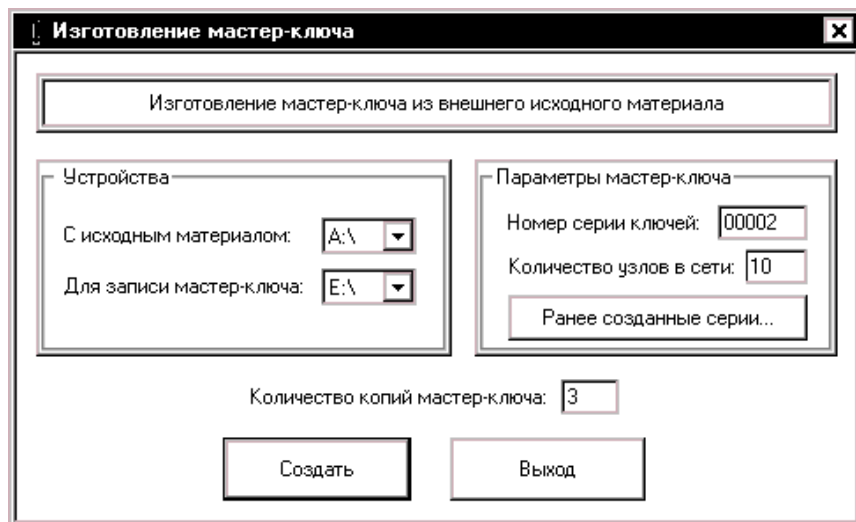


Рис. 1

Передвижение по полям и нажатие кнопок в окне Изготовление мастер-ключа и в других окнах программ АРМ ГК можно выполнять с помощью 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.

Процесс создания мастер-ключа запускается нажатием кнопки **Создать**.

Выйти из программы можно в любой момент нажатием кнопки **Выход**.

#### Группа **Устройства**

Поле **С исходным материалом** содержит список устройств со сменными носителями, с которых может быть считан исходный материал для формирования мастер-ключа. Из данного списка необходимо выбрать устройство, используемое оператором для считывания исходной информации.

Поле **Для записи мастер-ключа** содержит список устройств со сменными носителями для записи мастер-ключа. Из данного списка необходимо выбрать устройство, используемое оператором для записи мастер-ключа.

#### Группа **Параметры мастер-ключа**

В поле **Номер серии ключей** по умолчанию содержится следующий за последним использованным номер серии мастер-ключа (пятизначное десятичное число). Номер автоматически увеличивается 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 не изготавливались. Это 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 возможной компрометации ключей и подразумевает создание резервных ключевых носителей. Подробно принципы выбора данного значения изложены в Разделе 1.3.

Список **Ранее созданные серии ключей**, вызываемый по кнопке с аналогичным названием, необходим для учета и контроля уже созданных серий ключей. Серии ключей и дополнительная информация о них сохраняются в файле **series.lst**.

В поле **Количество копий мастер-ключа** необходимо ввести желаемое количество копий мастер-ключа заданной серии. Копии мастер-ключа необходимы для восстановления мастер-ключа заданной серии при физическом нарушении сменного носителя, на котором записан мастер-ключ (см. раздел 1.2.3).

Для генерации мастер-ключа необходима инициализация программно-клавиатурного датчика случайных чисел (ПКДСЧ). Инициализация ПКДСЧ запускается нажатием кнопки **Создать** (Рис. 1). Следуя инструкции по инициализации ПКДСЧ, представленной в окне Инициализация ПКДСЧ (Рис. 2), необходимо либо тридцать один раз устанавливать курсор мыши на маленькое желтое окно, появляющееся на экране ПЭВМ (Рис. 2), и нажимать левую кнопку мыши, либо вводить с клавиатуры указанный в желтом окне символ (с учетом регистра) соответствующее число раз.

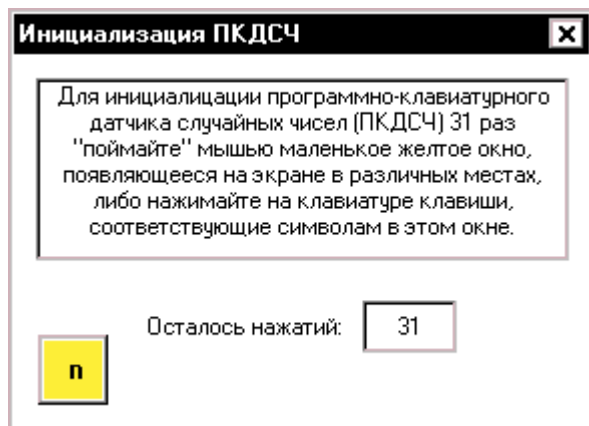


Рис. 2

В поле **Осталось нажатий** окна (Рис. 2) отображается, сколько нажатий осталось сделать пользователю до завершения процесса инициализации ПКДСЧ. До тех пор, пока инициализация ПКДСЧ не будет закончена, генерация мастер-ключа не начнется. При успешном завершении процесса инициализации ПКДСЧ программа выдаст соответствующее сообщение.

При инициализации ПКДСЧ возможны следующие ошибочные ситуации.

1. Пользователем была нажата на клавиатуре клавиша, не соответствующая символу, отображаемому в маленьком желтом окошке (Рис. 2), или им не был учтен регистр буквы. В таком случае счетчик инициализации ПКДСЧ (содержимое поля **Осталось нажатий**) увеличивается на единицу, т.е. после одного неверного нажатия клавиши вводится штраф в виде двух верных.
2. Пользователем было закрыто окно Инициализация ПКДСЧ.  
В таком случае выдается сообщение о том, что ПКДСЧ не проинициализирован. Необходимо заново запустить процесс инициализации ПКДСЧ нажатием кнопки **Создать** (Рис. 1).

После успешного завершения процесса инициализации ПКДСЧ можно приступить непосредственно к изготовлению мастер-ключа.

После заполнения описанных выше полей окна Изготовление мастер-ключа выдается запрос (Рис. 3).

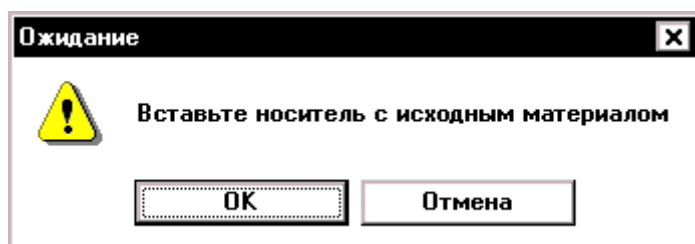


Рис. 3

После нажатия кнопки **ОК** начинается процесс изготовления мастер-ключа.

При успешном завершении генерации мастер-ключа будет выдано сообщение (Рис. 4).

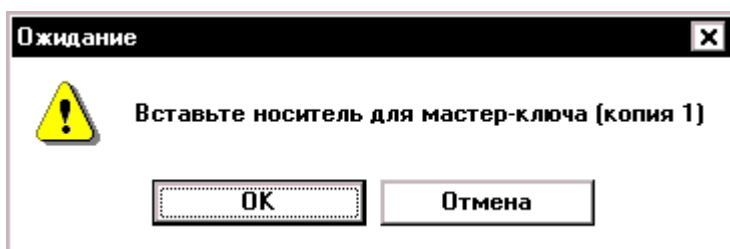


Рис. 4

В процессе генерации мастер-ключа возможно возникновение следующих ошибочных ситуаций.

1. Устройство со сменным носителем, содержащим исходный материал (на Рис. 1- устройство А), не готово для считывания информации. Программа выдаст сообщение об ошибочной ситуации. Необходимо подготовить данное устройство и снова запустить процесс создания мастер-ключа нажатием кнопки **Создать** (Рис. 1).
2. Носитель для считывания не содержит исходный материал для формирования мастер-ключа или исходный материал был испорчен. Программа выдаст сообщение об ошибочной ситуации. Необходимо подготовить носитель, содержащий исходный материал и снова запустить процесс создания мастер-ключа нажатием кнопки **Создать**.

Далее для записи мастер-ключа необходимо вставить сменный носитель в заданное устройство (на Рис. 1 - устройство Е) и нажать кнопку **ОК**.

При успешном завершении записи мастер-ключа выдается соответствующее сообщение.

В процессе записи мастер-ключа возможно возникновение следующих ошибочных ситуаций.

1. Устройство со сменным носителем, предназначенным для хранения мастер-ключа, не готово для записи мастер-ключа. Программа выдаст сообщение об ошибочной ситуации и запрос на повтор операции записи. Необходимо подготовить устройство для записи.
2. Носитель для записи содержит какую-либо информацию. Перед формированием ключевого носителя КНМК программой производится анализ содержимого носителя для записи. Запись ключевой информации на носитель не производится, если на нем содержится исходный материал или иная информация. Программа выдаст соответствующее сообщение и запрос на повтор операции записи.

Если нет необходимости в создании ключей другой серии, то выйти из программы можно нажатием кнопки **Выход** (см. Рис. 1). Если же есть такая необходимость, то процесс генерации следующего мастер-ключа аналогичен уже рассмотренному процессу генерации мастер-ключа и запускается нажатием кнопки **Создать**.

*Замечание.* Для генерации мастер-ключа следующей серии инициализация ПКДСЧ не требуется. Она необходима только при повторном запуске программы **MASTERKEY**.

## 4. Генерация ключевых носителей с сетевыми наборами ключей парной связи

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

Программа «Генерация ключей абонентов» (**GENKWIN**) выполняет генерацию сетевых наборов ключей парной связи и формирует ключевые носители КНПС.

После запуска программы **GENKWIN** на экран будет выведено окно Ввод мастер-ключа (Рис. 5).

Для генерации сетевых наборов ключей парной связи необходим ввод мастер-ключа и некоторой другой информации с ключевого носителя КНМК.

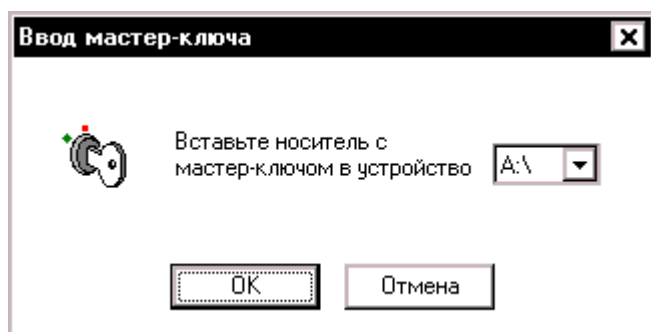


Рис. 5

Поле **Устройство** содержит список устройств со сменными носителями, с которых могут быть считаны мастер-ключ и дополнительная информация. Из данного списка необходимо выбрать устройство, используемое оператором для считывания мастер-ключа.

После успешного завершения процесса ввода мастер-ключа и дополнительной информации можно приступить непосредственно к изготовлению сетевых наборов ключей парной связи. Окно **Создание ключей абонентов** представлено на Рис. 6.

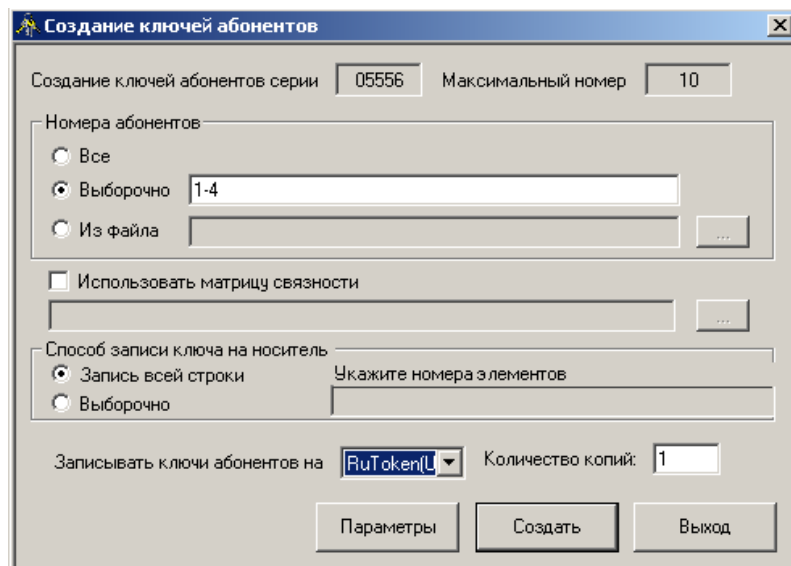


Рис. 6

При вводе мастер-ключа возможны следующие ошибочные ситуации.

1. Устройство со сменным носителем, содержащее мастер-ключ и дополнительную информацию (на Рис. 5 - устройство A), не готово для считывания информации. Программа выдаст сообщение об ошибочной ситуации. Необходимо подготовить данное устройство и ввести информацию нажатием кнопки **ОК**.

2. 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 носитель, содержащий данную информацию, и ввести ее нажатием кнопки **ОК**.

В окне (Рис. 6) «Записывать ключи абонентов на» выбирается носитель, куда будет выполнена запись ключевой информации, а непосредственно процесс создания ключей запускается нажатием кнопки **Создать**.

Выйти из программы можно в любой момент нажатием кнопки **Выход**.

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

Рассмотрим другие поля, отображенные на рис. Рис. 6.

Поле **Создание ключей абонентов серии** содержит номер серии сетевых наборов ключей парной связи. Номер серии считывается из файла **num\_m** ключевого носителя КНМК на этапе ввода мастер-ключа и, соответственно, равен номеру серии мастер-ключа.

Поле **Максимальный номер** содержит число абонентов, которые будут обмениваться информацией в сети связи. Число абонентов считывается из файла **num\_m** ключевого носителя КНМК на этапе ввода мастер-ключа.

Группа **Номера абонентов** 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 бы хотел создать сетевые наборы ключей парной связи, в порядке, задаваемым списком.  
Например: 1, 2, 3-5, 10 или 1, 4, 7, 9
- **из файла** - оператору необходимо ввести имя файла, в котором записаны номера абонентов, для которых он бы хотел создать сетевые наборы ключей парной связи, и полный путь к нему. Файл должен быть создан заранее в любом текстовом редакторе (кроме Microsoft Word) и содержать список абонентов.

*Замечание.* Список абонентов задается аналогично списку в поле **выборочно**, при переносе элемента списка на новую строку запятая после последнего элемента данной строки **НЕ** ставится.

Например: 1, 2  
5, 9

Поле **Использовать матрицу связности** является необязательным. Данное поле 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. С помощью "матрицы связности" можно запретить запись некоторых ключей на КНПС, что сделает невозможным работу владельца КНПС с некоторыми «соседями» по криптографической сети. Файл с матрицей связности должен быть заранее подготовлен с помощью любого текстового редактора (кроме Microsoft Word).

Описание разрешенных и запрещенных взаимных связей абонентов криптографической сети формируется в нем с помощью следующего набора правил.

1. Файл описания "матрицы связности" состоит из одной или нескольких секций. Каждая секция описывает связи одного абонента.
2. Секция начинается со строки, которая содержит номер абонента в квадратных скобках. Например, [ 15 ].
3. За начальной строкой секции могут следовать несколько строк с описанием связей данного абонента. Правила формирования описателей связей абонента приведены ниже.
4. В файле может быть задана одна специальная секция [ \* ], в которой описываются связи всех абонентов, явно не указанных в остальных секциях.
5. В файле описания "матрицы связности" действуют два правила умолчания.

Первое. Если для абонента не задана секция с описанием связей и отсутствует секция [ \* ], то для него *разрешены* связи со всеми абонентами криптографической сети.

Второе. Если задана пустая (не содержащая ни одного описателя связей) секция, то все связи такого абонента *запрещены*.

Правила формирования описателей связей абонента.

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

*Замечание.* Описатель связей абонента обрабатывается в следующем порядке. 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. Таким образом, итоговое разрешение или запрещение связи с каждым абонентом формируется в результате обработки всех элементов описателя. Соответственно, 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. 6) содержит список устройств со сменными носителями для записи сетевых наборов ключей парной связи абонентов. Из данного списка необходимо выбрать используемое оператором для записи сетевых наборов ключей парной связи устройство (на Рис. 6) - устройство RuToken(USB)).

При выбранном устройстве RuToken или EToken пользователю становится доступна кнопка «параметры», позволяющая настроить параметры паролей данных устройств, как показано на Рис. 7.

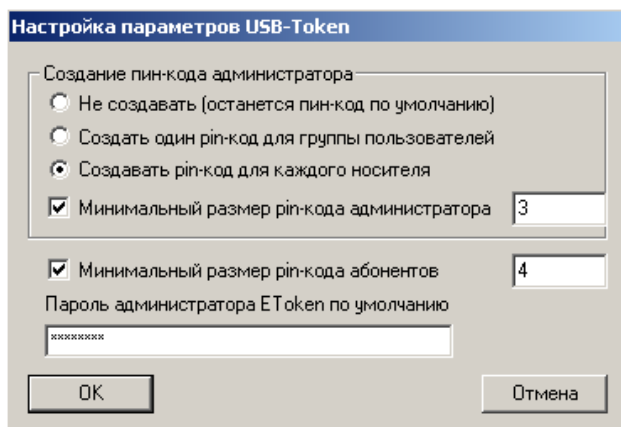


Рис. 7

Группа «Создание пин-кода администратора» содержит набор полей, предназначенных для настроек пин-кода администратора, который будет записан на носитель во время записи ключевой информации.

При выбранном поле «Не создавать» запись пароля администратора не будет выполняться, и останется пароль по умолчанию. При использовании АРМ ГК по уровням защищенности КС2, КС3 пароль администратора обязателен!

Для носителя EToken функция пароля администратора по умолчанию не предусмотрена, отсюда данный пароль следует ввести в соответствующее окно (Рис. 7). Пароль администратора EToken, который в дальнейшем будет использоваться как «пароль по умолчанию» возможно задать средствами форматирования носителя EToken.

Внимание! Отсутствие данного пароля может привести к тому, что создание ключей пользователей и их запись на EToken станут невозможными.

Если в качестве ключевого носителя выбран носитель RuToken, то окно «пароль администратора EToken по умолчанию» становится недоступным, так как чистый отформатированный носитель RuToken имеет стандартный пин-код администратора по умолчанию.

При выбранном поле «Создать один пин-код для группы пользователей» сохраняется один пароль администратора, введенный перед сеансом записи ключевой информации (например, если создаются ключи для нескольких абонентов).

При выбранном поле «Создать пин-код для каждого носителя» АРМ ГК каждый раз требует ввод нового пароля администратора перед записью информации на носитель.

При выделенном окне «минимальный размер пин-кода администратора» (Рис. 7) после ввода пароля администратора система проверяет: удовлетворяет ли введенный пароль указанным требованиям. Если нет, то потребуется ввод другого пароля.

Аналогичная процедура проверки выполняется для пароля абонента, при выделенном окне «минимальный размер пин-кода абонента».

В поле **Количество копий** (Рис. 6) необходимо ввести желаемое количество копий сетевых наборов ключей парной связи заданной серии для каждого абонента. Копии 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).

Группа «Способ записи ключа на носитель» (Рис. 6) содержит набор полей, предназначенных для определения способа записи ключевой информации.

При выделенном окне «Запись всей строки» выполняется запись всей ключевой строки сетевой таблицы, соответствующей криптографическому номеру узла.

При выделенном окне «выборочно» следует указать те номера элементов строки, которые следует записать на носитель. Способ задания элементов аналогичен способу указания номеров абонентов (например: 1, 2, 3-5, 10 или 1, 4, 7, 9).

*Примечание.* Выборочный способ записи элементов ключевой строки доступен только для ключевых носителей RuToken и EToken.

Процесс создания сетевых наборов ключей парной связи запускается нажатием кнопки **Создать** (Рис. 6).

После правильного заполнения полей и успешного завершения генерации сетевых наборов ключей парной связи будет выдано сообщение, отображенное на Рис. 8 при использовании обычных ключевых носителей, или на Рис. 9 при использовании носителей RuToken или EToken.

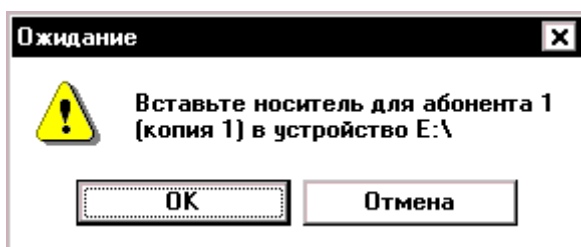
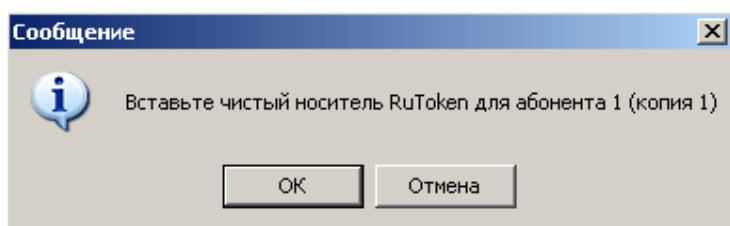


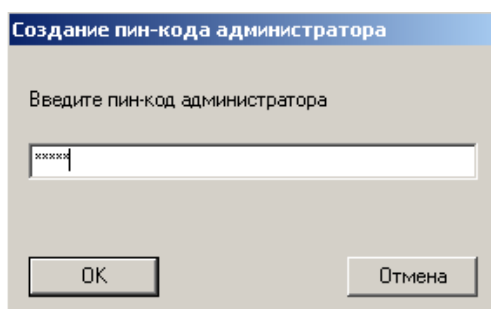
Рис. 8



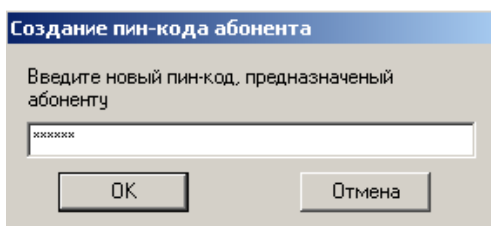
**Рис. 9**  
(сообщение при записи ключевой информации на RuToken)

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

При записи ключевой информации на RuToken или EToken потребуется ввод пароля администратора (Рис. 10), если в настройках носителей указано создание пин-кода администратора, а затем ввод пароля абонента (Рис. 11), после чего будет выполнено сохранение ключевой информации на носитель.



**Рис. 10**  
Создание пин-кода администратора



**Рис. 11**  
Создание пин-кода абонента

Пароль администратора потребуется вводить один раз, если в настройках носителя выбрано создание одного пин-кода для группы пользователей, либо потребуется ввод перед каждой копией, если выбрано создание пин-кода для каждого носителя.

Ввод пин-кода абонента требуется всегда перед созданием каждой копии ключа.

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

1. Поля выбора **Номера абонентов** (Рис. 6):

• Поле **выборочно**

- Неверно задан список абонентов (узлов). Список абонентов включает номера абонентов, превышающие максимальный номер. Программа выдаст соответствующее сообщение. Необходимо ввести номера абонентов с учетом количества абонентов (максимального размера).
- 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**
    - 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.
  3. Поля выбора способа записи ключевой информации
    - При выделенном окне «выборочно» неверно задан список элементов ключевой строки, либо он пуст. Правило заполнения списка элементов аналогично правилу заполнения списка абонентов (узлов).
  4. Ошибки ввода паролей носителей RuToken или EToken.
    - Введенный пароль администратора не соответствует параметрам настройки, длина введенного пароля меньше указанного значения. Требуется либо ввести пароль, удовлетворяющий параметрам настройки, либо в настройках изменить минимальную длину пароля администратора.
    - Введенный пин-код абонента не соответствует параметрам настройки, длина введенного пароля меньше указанного значения. Требуется либо ввести пароль, удовлетворяющий параметрам настройки, либо в настройках изменить минимальную длину пин-кода абонента.
    - Пароли администратора и пользователя EToken удовлетворяют требованиям, указанным в настройках ПО АРМ ГК, но (как минимум) один из них не может быть записан на носитель. Причина: у носителя EToken имеется встроенная функция допустимой «сложности» пароля. В данном случае требуется либо ввести более «сложный» пароль, либо отформатировать носитель с изменением значений данной функции.

При успешном завершении записи ключей парной связи для каждого абонента выдается соответствующее сообщение.

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

1. Устройство со сменным носителем, предназначенным для записи сетевых наборов ключей парной связи, не готово для записи. Программа выдаст сообщение об ошибочной ситуации. Необходимо подготовить устройство для записи.
2. Носитель для записи содержит какую-либо информацию. Перед формированием ключевых носителей КНПС программой производится анализ содержимого носителя для записи. Запись ключевой информации на носитель не производится, если на нем содержится ранее записанная ключевая или иная информация, а также если у носителей RuToken и EToken уже установлены пароли, отличные от паролей по умолчанию. Программа выдаст соответствующее сообщение.

Процесс изготовления сетевых наборов ключей парной связи абонентов протоколируется в файле **journal.txt**. Данный файл может быть просмотрен с помощью любого текстового редактора.

## 5. Копирование ключевых носителей КНМК и КНПС

Для обеспечения надежности хранения ключевой информации на ключевых носителях КНМК и КНПС в связи с высоким риском физической порчи носителей необходимо создание дополнительных копий ключевых носителей на рабочем месте оператора АРМ ГК.

Программа «**Копирование ключевых носителей**» (СОРУКЕУ) выполняет копирование ключевых носителей КНМК и КНПС.

После запуска программы СОРУКЕУ на экран будет выведено окно Копирование ключевых носителей (Рис. 12).

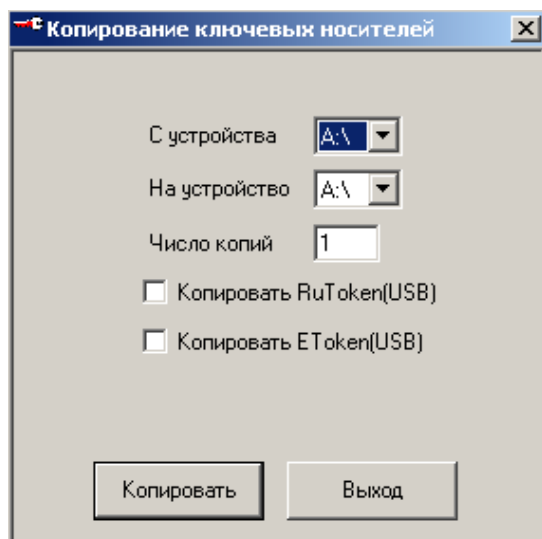


Рис. 12

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

Выйти из программы можно в любой момент нажатием кнопки **Выход**.

Поле **С устройства** содержит список устройств со сменными носителями. Из данного списка необходимо выбрать устройство, сменный носитель которого является исходным для копирования (на Рис. 12 - устройство A).

Поле **На устройство** содержит список устройств со сменными носителями. Из данного списка необходимо выбрать устройство, сменный носитель которого будет использоваться оператором для копирования на него информации, содержащийся на исходном для копирования носителе (на Рис. 12 - устройство A).

При выделенном поле «Копировать RuToken(USB)» или «копировать EToken(USB)» (Рис. 12) будет выполнено создание копии соответствующего ключевого носителя.

*Примечание.* Функций копирования ключевой информации с обычного носителя на Ru(E)Token и наоборот не предусмотрено.

В поле **Число копий** необходимо ввести желаемое количество копий ключевого носителя.

После заполнения описанных выше полей окна **Копирование ключевых носителей** и нажатия кнопки **Копировать** (Рис. 12) необходимо вставить исходный для копирования носитель в выбранное устройство.

Если выбрано копирование носителя Ru(E)Token, то программа потребует ввод всех паролей носителя, как показано на Рис. 13.

Вставьте носитель USB-Token

Введите пароль администратора  
xxxxxx

Введите пароль пользователя  
xxxxxx

Пароль администратора по умолчанию  
xxxxxx

ОК Отмена

**Рис. 13**

*Примечание.* Окно «Пароль администратора по умолчанию» используется только в случае копирования носителя EToken.

Программа выполнит временное сохранение содержимого исходного для копирования носителя в оперативную память и запросит устройство, на сменный носитель которого будет скопирована информация с исходного для копирования носителя.

При успешном завершении копирования ключевого носителя выдается соответствующее сообщение.

В процессе копирования ключевого носителя возможно возникновение следующих ошибочных ситуаций.

1. Устройство со сменным носителем, являющимся исходным для копирования, не готово для считывания информации с него. Программа выдаст сообщение об ошибочной ситуации. Необходимо подготовить устройство для считывания.
2. Устройство со сменным носителем, на который будет записываться информация с исходного носителя, не готово для записи. Программа выдаст сообщение об ошибочной ситуации. Необходимо подготовить устройство для записи.
3. Материал ключевого носителя был испорчен. Программа выдаст сообщение об ошибочной ситуации.
4. Носитель для копирования содержит информацию, отличную от состава ключевой информации КНМК и КНПС. Перед копированием ключевого носителя производится анализ содержимого ключевого носителя и определение типа ключевой информации. Копирование информации ключевого носителя не производится, если на нем содержится информация, отличная от ключевой информации КНМК и КНПС. Программа выдаст соответствующее сообщение.

## 6. Генерация ключевого носителя с исходным материалом

Программа «Генерация исходного материала» (**GENSRC**) выполняет генерацию исходного материала и формирует ключевые носители КНИМ.

После запуска программы **GENSRC** на экран будет выведено окно **Создание исходного материала с помощью ПКДСЧ** (Рис. 14).

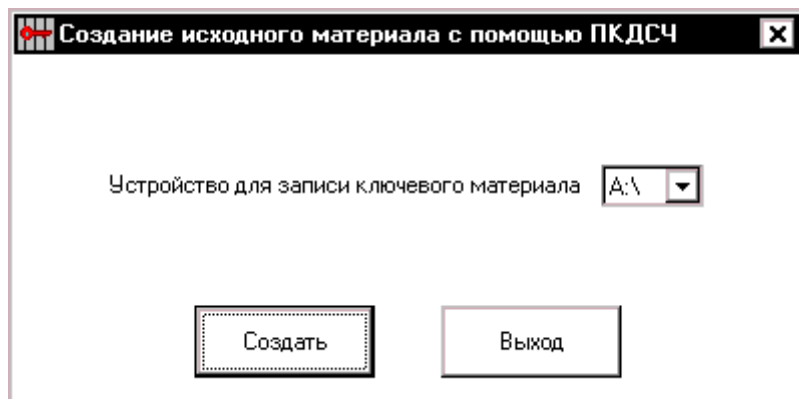


Рис. 14

Процесс создания исходного материала запускается нажатием кнопки **Создать**.

Выйти из программы можно в любой момент нажатием кнопки **Выход**.

Поле **Устройство для записи ключевого материала** содержит список устройств со сменными носителями. Из данного списка необходимо выбрать устройство, на сменный носитель которого будет записан исходный материал.

После заполнения поля окна **Создание исходного материала с помощью ПКДСЧ** и нажатия кнопки **Создать** (Рис. 14) необходимо проинициализировать ПКДСЧ.

Инициализация ПКДСЧ и возможные ошибочные ситуации описаны в разделе 3. Генерация ключевого носителя с мастер-ключом.

После успешного завершения процесса инициализации ПКДСЧ можно приступить непосредственно к генерации исходного материала. Необходимо вставить чистый носитель в устройство для записи исходного материала.

При успешном завершении процесса генерации исходного материала и записи его на сменный носитель программа выдаст соответствующее сообщение.

В процессе записи исходного материала возможно возникновение следующих ошибочных ситуаций.

1. Устройство со сменным носителем, на который будет записан исходный материал, не готово для записи. Программа выдаст сообщение об ошибочной ситуации. Необходимо подготовить устройство для записи.
2. Носитель для записи содержит какую-либо информацию. Перед формированием ключевых носителей КНИМ программой производится анализ содержимого носителя для записи. Запись исходного материала на носитель не производится, если на нем содержится ранее записанная ключевая или иная информация. Программа выдаст соответствующее сообщение.

## 7. Уничтожение ключевой информации на КНПС

В случае вывода по какой-либо причине абонента с заданным номером из криптографической сети, необходимо уничтожение одного или нескольких ключей парной связи по заданному направлению на рабочем месте оператора АРМ ГК.

Программа «**Стирание ключа**» (**CLEARKEY**) выполняет уничтожение ключей парной связи по заданному направлению.

После запуска программы **CLEARKEY** на экран будет выведено окно Уничтожение ключей по направлениям (Рис. 15).

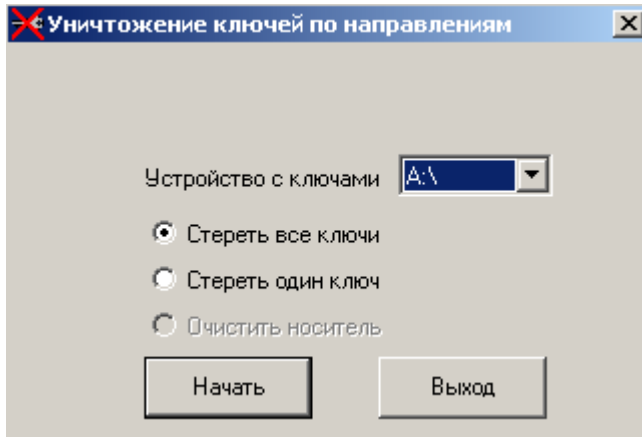


Рис. 15

В данной версии программы предусмотрены три операции:

- уничтожение одного ключа парной связи;
- уничтожение всех ключей в случае компрометации ключевой информации;
- очистка ключевой информации с носителя и перевод его в исходное состояние (функция доступна только для работы с носителем RuToken и EToken).

Поле **Устройство с ключами** содержит список устройств со сменными носителями. Из данного списка необходимо выбрать устройство, сменный носитель которого является ключевым носителем КНПС и с которого будет удален один или все ключи парной связи по заданному направлению.

Процесс уничтожения ключей запускается при нажатии кнопки **Начать**.

Выйти из программы можно в любой момент нажатием кнопки **Выход**.

После заполнения поля окна Уничтожение ключей по направлениям, выбора способа уничтожения ключей и нажатия кнопки **Начать** (Рис. 15) необходимо вставить ключевой носитель КНПС в выбранное устройство.

Если требуется уничтожить информацию на носителе RuToken или EToken, то потребуется ввод пароля абонента (Рис. 16).

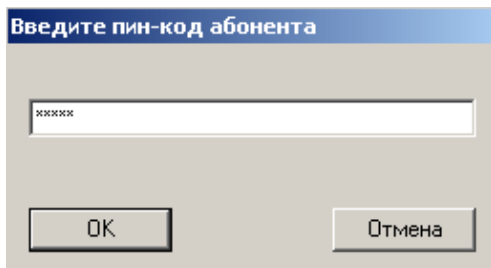


Рис. 16

При уничтожении одного ключа парной связи программа выдаст информацию об обнаруженном ею КНПС (серия, номер, размер сети), и на экран будет выведено окно Стирание ключа на ключевом носителе (Рис. 17).

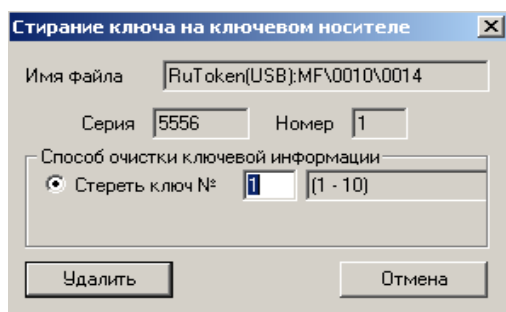


Рис. 17

Процесс уничтожения ключа парной связи по заданному направлению запускается нажатием кнопки **Стереть**.

Выйти из программы можно в любой момент нажатием кнопки **Отмена**.

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

Поле **Серия** содержит серию сетевых наборов ключей парной связи. Данное поле заполняется программой автоматически после считывания информации с ключевого носителя 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 ключевого носителя 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. Далее показан диапазон возможных направлений уничтожения связи.

После того как будет заполнено поле **Стереть ключ** в окне Стирание ключа на ключевом носителе (Рис. 17) и нажата кнопка **Удалить**, будет выдан дополнительный запрос о необходимости удаления ключа с ключевого носителя КНПС (данная операция является необратимой) и после подтверждения программа удалит выбранный ключ парной связи для абонента.

В случае успешного удаления выбранного ключа парной связи выдается соответствующее сообщение.

Если требуется стереть все ключи, то при выполнении данной операции программа стирает всю ключевую строку, главный ключ, а также серию и номер абонента.

При необходимости полной очистки носителя RuToken или EToken будут выполнены следующие действия:

- Для носителя RuToken потребуются ввод пароля администратора, далее будет выдано сообщение с целью подтверждения выполнения данной операции и в случае утвердительного ответа будут удалены все ключевые файлы с носителя, а пароли заменены на пароли по умолчанию;
- Для носителя EToken выдается сообщение с целью подтверждения выполнения данной операции и в случае утвердительного ответа выполнится запуск утилиты форматирования EToken. Для успешного запуска утилиты требуется, чтобы утилита «ETFORMAT» была установлена в ту же папку, где находится программа CLEARKEY. Данная утилита является общедоступной и находится на официальном сайте разработчиков EToken.

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

1. Устройство со сменным носителем не готово для считывания информации с него. Программа выдаст сообщение об ошибочной ситуации. Необходимо подготовить устройство для удаления ключа парной связи.
2. При выполнении операций удаления ключей парной связи материал ключевого носителя КНПС испорчен или содержит недопустимую информацию. Программа выдаст сообщение об ошибочной ситуации.
3. В поле **Стереть ключ** было введено значение, не являющиеся числом, или число, выходящее из диапазона возможных направлений уничтожения связи. Программа выдаст сообщение об ошибочной ситуации.
4. Неверно введен пароль абонента при стирании ключевой информации с носителя RuToken или EToken. Программа выдаст сообщение об ошибочной ситуации.
5. Неверно введен пароль администратора при полной очистке информации с носителя RuToken. Программа выдаст сообщение об ошибочной ситуации.
6. Невозможно запустить утилиту форматирования EToken. Программа выдаст сообщение об ошибочной ситуации.

## 8. Ведение журнала работы АРМ ГК

В ходе работы с ПО АРМ ГК, предусмотрено обязательное автоматическое ведение журнала в электронном виде. Данный журнал предназначен для хранения сведений о создании и копировании 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. Просмотреть данный файл возможно с помощью любого стандартного в ОС Windows текстового редактора (например «WordPad»). Ниже приведен пример фрагмента журнала.

```
10-08-2007 13:22 Создан исходный материал на основе ПКДСЧ
10-08-2007 13:23 Создан мастер-ключ серии 2, число абонентов 10
10-08-2007 13:24 Созданы ключи серии 1 для абонента 1 (число копий: 1)
10-08-2007 13:24 Созданы ключи серии 1 для абонента 2 (число копий: 2)
10-08-2007 13:25 Скопированы ключи серии 1 с номером абонента 2
10-08-2007 13:26 Удаление ключа с КНПС серии 1 для абонента 2, стерт ключ 5
10-08-2007 13:47 Созданы ключи серии 1 для абонента 1
Ключи сохранены на носителях RuToken (число копий: 1)
10-08-2007 13:48 Созданы ключи серии 1 для абонента 1 (число копий: 1)
```

## 9. Состав ключевой информации

### 9.1. Состав ключевой дискеты (флеш-диска) КНМК

После выполнения программы **MASTERKEY** для каждой серии ключей парной связи ключевая дискета КНМК содержит четыре файла:

1. **gkm.key** – мастер-ключ оператора;
2. **uz.db3** - узел замены;
3. **random.ini** – начальное заполнение программного датчика случайных чисел (256 бит);
4. **num\_m** – файл, содержащий номер серии ключей парной связи и количество узлов в сети связи.

### 9.2. Состав ключевой дискеты (флеш-диска) КНПС

После выполнения программы **GENKWIN** для каждой серии ключей парной связи ключевая дискета КНПС содержит пять файлов:

1. **gk.db3** - главный ключ;
2. **uz.db3** - узел замены;
3. **random.ini** - начальное заполнение программного датчика случайных чисел (256 бит).

Директория **КМ\_К** содержит два файла:

4. **kis\_1** - сетевой набор ключей парной связи;
5. **ckd** - ключ шифрования сетевого набора ключей парной связи.

### 9.3. Состав ключевой дискеты (флеш-диска) КНИМ

После выполнения программы **GENSRC** ключевая дискета КНИМ содержит два файла:

1. **uz.db3** - узел замены;
2. **gk.db3** - главный ключ.

### 9.4. Состав ключевого носителя RuToken, содержащего КНПС

После выполнения программы **GENKWIN** носитель RuToken содержит папку с адресом 0010, в которой содержится:

1. 0011 – узел замены;
2. 0012 – главный ключ;
3. 0013 - начальное заполнение программного датчика случайных чисел (256 бит);
4. 0014 – сетевой набор ключей парной связи;
5. 0015 – способ записи ключевой строки (полная или разреженная строка);
6. 0016 – серия ключа, номер абонента и максимально возможное значение абонентов (служебный файл).

### 9.5. Состав ключевого носителя EToken, содержащего КНПС

После выполнения программы **GENKWIN** в корневой папке с адресом f00b создается папка с адресом ffe0, которая содержит:

1. ffe1- узел замены;
2. ffe2 – главный ключ;
3. ffe3 - начальное заполнение программного датчика случайных чисел (256 бит);
4. ffe4 – сетевой набор ключей парной связи;
5. ffe5 - способ записи ключевой строки (полная или разреженная строка).