

Утвержден

ВЕРМ.00118-01-ЛУ

ПС «Купол-СКЗИ для Linux»

Руководство оператора

ВЕРМ.00118-01 34 01

Листов 29

Инд. № подл.	Подпись и дата	Взам. инд. №	Инд. № дудл.	Подпись и дата

2019

Литера О₁

АННОТАЦИЯ

Настоящий документ содержит сведения, необходимые для обеспечения процедуры общения оператора с программным средством «Купол-СКЗИ для Linux» ВЕР.00118-01 (далее по тексту – ПС «Купол-СКЗИ для Linux»).

СОДЕРЖАНИЕ

1. Назначение программного средства	4
2. Условия выполнения программного средства	5
3. Выполнение программного средства	6
4. Сообщения оператору	27
Перечень принятых сокращений	28

1. НАЗНАЧЕНИЕ ПРОГРАММНОГО СРЕДСТВА

1.1. Программное средство предназначено для построения защищённых распределённых хранилищ данных.

1.2. ПС «Купол-СКЗИ для Linux» состоит из следующих программ:

- Модуль формирования сетевого имени (initus);
- Модуль генерации контейнеров для связи с оператором РР (gencrtk);
- Модуль изменения пароля (chpin);
- Модуль формирования файла для передачи оператору РР (rsen);
- Модуль проверки и экстракции файла (rrec);
- Модуль записи в РР (areestr);
- Модуль извлечения информации из РР по номеру звена (creestr);
- Модуль сервера РР (rrwserv).

1.3. ПС «Купол-СКЗИ для Linux» выполняет следующие функции:

- хранение данных реестра с выполнением функций резервного копирования;
- приём данных и их запись в реестр;
- формирование и передача данных в соответствии с полученными заявками;
- формирование блока для записи;
- индексирование данных, хранящихся в распределённом реестре;
- передача заявок на поиск в распределённых реестр;
- передача результатов поиска на фронт-сервер в соответствии с поступившими заявками;
- взаимодействие пользователей с инфраструктурой распределённого реестра;
- вывод пользователю результатов поиска в распределённом реестре;
- аудит консенсуса базы данных.

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММНОГО СРЕДСТВА

2.1. ПС «Купол-СКЗИ для Linux» функционирует на ПЭВМ с характеристиками, не ниже следующих:

- процессор Intel Core2 Duo 1,8 ГГц;
- оперативная память 2048 Мбайт;
- жесткий диск 100 Гбайт;
- устройство чтения компакт-дисков;
- сетевая плата Fast Ethernet 100 Мбит/с.

2.1.1. ПС «Купол-СКЗИ для Linux» функционирует в среде ОС СН «Astra Linux 1.6 Special Edition» (Смоленск).

3. ВЫПОЛНЕНИЕ ПРОГРАММНОГО СРЕДСТВА

3.1 Расположение файлов комплекса программ на диске.

Расположение файлов комплекса программ приведены на нижеследующих рисунках.

Корневой каталог

 bin	5 объектов	Вчера
 LMakefiles	8 объектов	Вчера
 src	22 объекта	Вчера
 WMakefiles	8 объектов	Вчера
 VCBUILD.BAT	198 байт	Пн

Рис. 1

Каталог с исполняемыми файлами (после сборки) и файлами реестра













 areestr	190,7 кБ	10:59
 chpin	190,7 кБ	11:00
 creestr	186,6 кБ	11:01
 gencrtk	186,5 кБ	11:01
 initus	186,6 кБ	11:01
 operator	28 байт	Пн
 reestr.ind	1,3 кБ	Пн
 reestr.rus	166,7 кБ	Пн
 rrec	186,5 кБ	11:02
 rrwserv	200,1 кБ	11:02
 rrwserv.cfg	70 байт	Пн
 rsen	186,5 кБ	11:02
 stopserv	8 байт	Вчера

Рис. 2

Каталог с makefiles для linux









	AREESTR.MAK	409 байт	Пн
	CHPIN.MAK	405 байт	Пн
	CREESTR.MAK	413 байт	Пн
	GENCRTK.MAK	413 байт	Пн
	INITUS.MAK	401 байт	Пн
	RREC.MAK	392 байта	Пн
	RRWSERV.MAK	433 байта	Пн
	RSEN.MAK	392 байта	Пн

Рис. 3

Каталог с исходными текстами программ















	areestr.c	12,0 кБ	Пн
	chpin.c	8,9 кБ	Пн
	common.c	9,5 кБ	Пн
	common.h	1,2 кБ	Пн
	creestr.c	8,5 кБ	Пн
	gencrtk.c	15,0 кБ	Пн
	initus.c	6,6 кБ	Пн
	k2.c	47,1 кБ	Пн
	k2.h	1,7 кБ	Пн
	k3.c	8,7 кБ	Пн
	k3.h	839 байт	Пн
	k_t.c	7,9 кБ	Пн
	r1.c	5,6 кБ	Пн
	r1.h	339 байт	Пн

Рис. 4

3.2 Программа «Модуль формирования сетевого имени»

Создает нового пользователя (в том числе оператора распределенного реестра).

Формирует служебные файлы для созданного пользователя

3.2.1 Наименование

initus

3.2.2 Формат вызова

```
./initus PersonalKeyFileName PersonalPIN  
PersonalFileName [RandomString]
```

3.2.2.1 Параметры вызова

- **PersonalKeyFileName (out)** – имя создаваемого файла с закрытым на пароле персональным идентификатором пользователя (может быть связано с именем пользователя, но не должно совпадать с именем файла **PersonalFileName**);
- **PersonalPIN (in)** – пароль (пин-код или метод его ввода, например, чтения из USB-токена) для закрытия персонального идентификатора пользователя;
- **PersonalFileName (in)** – текстовый файл длиной не более 160 байт, в котором размещаются данные пользователя (ФИО, паспортные данные и др.).
Формат не регламентирован;
- **[RandomString] (in)** – («разгонная строка») необязательный параметр для улучшения работы датчика случайных чисел.

3.2.3 Результат вызова

3.2.4 Созданы файлы

- **random.bin** - для дальнейшего использования датчика случайных чисел

- PersonalKeyFile - с закрытым на пароле персональным идентификатором пользователя (фактически – защищенный контейнер для хранения и передачи персонального идентификатора/ключа пользователя).
- NetNameFile - с сетевым именем (в виде 32 символов шестнадцатеричного кода). Первые 8 цифр определяют также имя файла, в котором сетевое имя находится в бинарном формате.

3.2.5 Пример использования

3.2.6 Исходные данные:

- Имя пользователя: «Alisa»
- Имя каталога пользователя: alisa
- Файл с данными пользователя (PersonalFile): alisa.txt

3.2.7 Последовательность действий

Создаём в корневом каталоге подкаталог alisa



Рис. 5

Помещаем в него файл с данными пользователя (PersonalFile): alisa.txt



Рис. 6

В каталоге alisa запускаем командную строку

```
../bin/initus al 1 alisa.txt
```

```

vlad@vb-u:~/Kupol/KupolCore/alisa$ ../bin/initus al 1 alisa.txt
Success Protect Function
Ok Test Random
PersonalKeyFile: al
Successful PersonalKeyFile create!
Creation PersonalKeyFile Time-> 12:05:39 16.08.2019
Network name (full) : 89dbf699a5408ba6eea09a11e77fe1b6
Network name (short): 89dbf699

```

Рис. 7

Содержимое каталога alisa после запуска команды

 random.bin	32 байта	12:05
 initus.log	172 байта	12:05
 alisa.txt.net	32 байта	12:05
 al	96 байт	12:05
 89dbf699.net	16 байт	12:05
 alisa.txt	82 байта	20 июн.

Рис. 8

3.3 Программа «Модуль генерации контейнеров для связи с оператором РР»

3.3.1 Создает сетевой контейнер пользователя на основе сетевого имени пользователя и пароля для закрытия транспортного ключа. Этот пароль далее будет использоваться для защиты контейнера с транспортным ключом. Оператор РР должен иметь ключи всех пользователей, поэтому пользователи могут выработать транспортные ключи самостоятельно и направить их оператору РР, а пароль сообщить оператору отдельно (по смс, письмом или голосом). Либо пользователи высылают оператору РР бинарный файл своего сетевого имени, и оператор РР формирует транспортные ключи пользователей и также отдельно (по другим каналам) сообщает им их пароли. С точки зрения безопасности — это равноценная схема, поскольку пользователи не знают пароля друг друга, а оператор РР является доверенной стороной (доверенным компонентом системы).

3.3.2 Наименование

gencrtk

3.3.3 Формат вызова

```
./gencrtk NetNameFileName NetKeyPIN [SrvPath]
```

3.3.4 Параметры вызова

- NetNameFileName (in) – файл, полученный программой initus длиной 16 байт, содержащий бинарное сетевое имя пользователя (абонента);
- NetKeyPIN (in) – пароль (пин-код или метод его ввода, например, чтения из USB-токена) для закрытия транспортного ключа;
- SrvPath (in) – (необязательный параметр) Путь, куда пишется серверный ключ пользователя. В случае отсутствия серверный ключ формируется в текущем каталоге.

3.3.5 Результат вызова

Созданы файлы

- NetKeyFile – сетевой контейнер пользователя с именем персонального файла пользователя (PersonalFile) и расширением .007 (пишется в каталог пользователя);
- NetKeyFile2 - Серверный ключ пользователя с именем состоящем из первых 8 символов сетевого имени пользователя и расширением .007, пишется в каталог SrvPath (если каталог SrvPath не указан, то файл пишется в каталог пользователя).

3.3.6 Пример использования

3.3.7 Исходные данные:

- NetNameFile - alisa.txt.net
- NetKeyPIN - 11
- SrvPath - ../bin/

3.3.8 Последовательность действий

В каталоге alisa запускаем командную строку

```
../bin/genctrk alisa.txt.net 11 ../bin/
```

```
vlad@vb-u:~/Kupol/KupolCore/alisa$ ../bin/genctrk alisa.txt.net 11 ../bin/
Success Protect Function
Ok Test Random
NetNameFile: alisa.txt.net
NetKeyFile: alisa.txt.007
NetName:89dbf699a5408ba6eea09a11e77fe1b6
NetKeyFile2: ../bin/89dbf699.007
Successful NetKeyFile create!
Creation Time-> 12:35:00 16.08.2019
```

Рис. 9

Содержимое каталога alisa после запуска команды






	random.bin	32 байта	12:35
	genctrk.log	317 байт	12:35
	alisa.txt.007	112 байт	12:35
	initus.log	172 байта	12:05
	alisa.txt.net	32 байта	12:05
	al	96 байт	12:05
	89dbf699.net	16 байт	12:05
	alisa.txt	82 байта	20 июн.

Рис. 10

Содержимое каталога bin после запуска команды



Рис. 11

3.4 Программа «Модуль формирования файла для передачи оператору РР»

Создает подписанный файл, содержащий сообщение пользователя.

3.4.1 Наименование

rseп

3.4.2 Формат вызова

```
./rseп NetKeyFileName NetKeyPIN FileNameToSign  
SignedFileName
```

3.4.3 Параметры вызова

- NetKeyFileName (in)– файл, содержащий сетевой ключ пользователя с расширением (.007), (файл создан программой genctrlk);
- NetKeyPIN (in)– пароль, используемый для подписи отправляемых файлов (задается при создании NetKeyFile программой genctrlk);
- FileNameToSign (in) – файл, содержащий сообщение пользователя;
- SignedFileName (out) – файл, содержащий подписанное пользователем сообщение;

3.4.4 Результат вызова

3.4.5 Создан файл

- SignedFile (out) – файл, содержащий подписанное пользователем сообщение

3.4.6 Пример использования

3.4.7 Исходные данные:

- NetKeyFile (in) - alisa.txt.007
- NetKeyPIN (in)– 11
- FileToSign (in) - letter.txt



Рис. 12

3.4.8 Последовательность действий

В каталоге alisa запускаем командную строку

```
../bin/rsen alisa.txt.007 11 letter.txt lettersign.txt
```

```
vlad@vb-u:~/Kupol/KupolCore/alisa$ ../bin/rsen alisa.txt.007 11 letter.txt lettersign.txt
Success Protect Function
Ok Test Random
Len= 29
NetKeyFile: alisa.txt.007
Successful NetKeyFile read!
Creation NetKeyFile Time: 12:35:00 16.08.2019
Network name: 89dbf699a5408ba6eea09a11e77fe1b6
Length: 064
Ok SignedFile write
Ok SignedFile read
Ok SignedFile check
Registration SignedFile in: 13:16:29 16.08.2019
FileToSign: letter.txt
```

Рис. 13

Содержимое каталога alisa после запуска команды

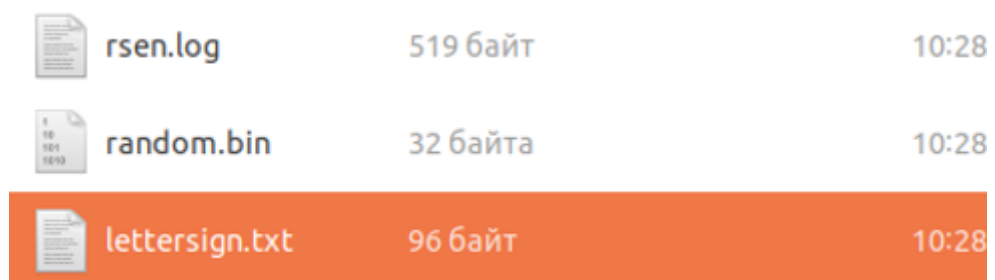


Рис. 14

3.5 Программа «Модуль изменения пароля»

3.5.1 Меняет пароль, установленный на персональный ключ пользователя либо на сетевой ключ пользователя

3.5.2 Наименование

chpin

3.5.3 Формат вызова

```
./chpin -TypeContainer(P - PersonalKey; N - NetKey)  
PersonalKeyFileName/NetKeyFileName UserPIN_old UserPIN_new  
[SrvPath (Only for -N)]
```

3.5.4 Параметры вызова

- TypeContainer (in) – тип ключа:
 - P - персональный ключ пользователя;
 - N - сетевой ключ пользователя;
- PersonalKeyFileName/NetKeyFileName (in/out)– файл, содержащий ключ пользователя (персональный / сетевой);
- UserPIN_old (in) – старый пароль;
- UserPIN_new (in) – новый пароль;
- SrvPath (in) - (только для сетевого ключа пользователя) путь, куда пишется серверный сетевой ключ пользователя;

3.5.5 Результат вызова

3.5.6 Изменен пароль на ключ пользователя

- PersonalKeyFile/NetKeyFile (in/out)– файл, содержащий ключ пользователя (персональный / сетевой);

3.5.7 Пример использования

3.5.8 Смена пароля персонального ключа пользователя

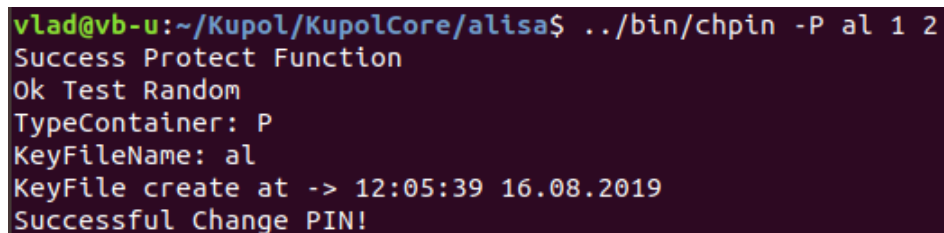
3.5.9 Исходные данные:

- TypeContainer (in) – -P
- PersonalKeyFile/NetKeyFile (in/out) – al
- UserPIN_old (in) – 1;
- UserPIN_new (in) – 2;
- SrvPath (in) (в данном режиме не используется)

3.5.10 Последовательность действий

В каталоге alisa запускаем командную строку

```
../bin/chpin -P al 1 2
```



```
vlad@vb-u:~/Kupol/KupolCore/alisa$ ../bin/chpin -P al 1 2
Success Protect Function
Ok Test Random
TypeContainer: P
KeyFileName: al
KeyFile create at -> 12:05:39 16.08.2019
Successful Change PIN!
```

Рис. 15

3.5.11 Смена пароля сетевого ключа пользователя

3.5.12 Исходные данные:

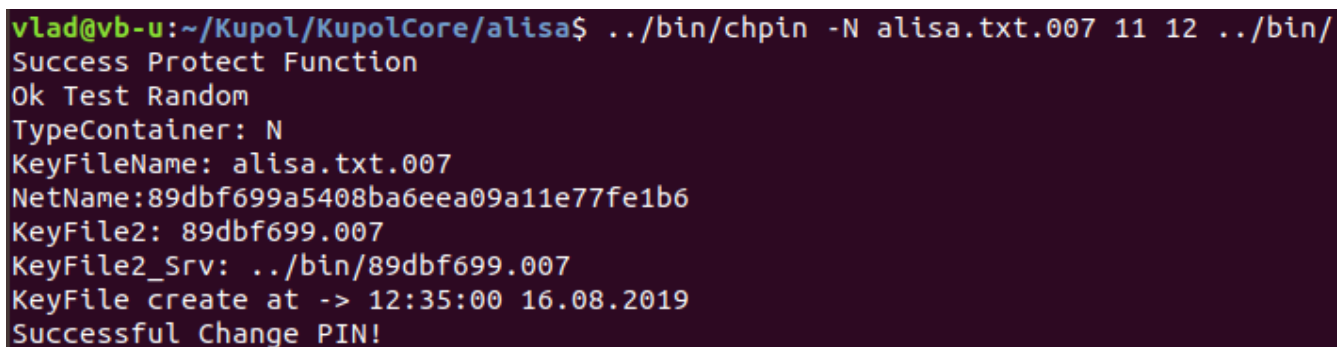
- TypeContainer (in) – -N
- PersonalKeyFile/NetKeyFile (in/out) – alisa.txt.007
- UserPIN_old (in) – 11

- UserPIN_new (in) – 12
- SrvPath (in) - ../bin/

3.5.13 Последовательность действий

В каталоге alisa запускаем командную строку

```
../bin/chpin -N alisa.txt.007 11 12 ../bin/
```



```
vlad@vb-u:~/Kupol/KupolCore/alisa$ ../bin/chpin -N alisa.txt.007 11 12 ../bin/
Success Protect Function
Ok Test Random
TypeContainer: N
KeyFileName: alisa.txt.007
NetName:89dbf699a5408ba6eea09a11e77fe1b6
KeyFile2: 89dbf699.007
KeyFile2_Srv: ../bin/89dbf699.007
KeyFile create at -> 12:35:00 16.08.2019
Successful Change PIN!
```

Рис. 16

3.6 Программа «Модуль записи в РР»

3.6.1 Программа «Модуль записи в РР» вызывается программой «Модуль сервера РР» и предназначена для добавления записей в распределенный реестр. Записи добавляет оператор распределенного реестра. Запускается из каталога bin.

3.6.2 Наименование

areestr

3.6.3 Формат вызова

```
./areestr PersonalKeyFileName(operator)
PersonalPIN(operator) SignedFileName(length <= 32 symbols)
```

3.6.4 Параметры вызова

- PersonalKeyFileName(operator) (in) – персональный ключ оператора распределенного реестра;
- PersonalPIN(operator) (in)– пароль оператора распределенного реестра;
- SignedFileName (in) – файл с сообщением пользователя, подписанный пользователем.

3.6.5 Результат вызова

- В реестр добавляется новая запись о файле SignedFile. Добавление записи в распределенный реестр подразумевает под собой обновление двух файлов (reestr.ind и reestr.rus). Файл reestr.ind – это индексный файл РР, необходимый для поиска записей в реестре. Файл reestr.rus – информационный файл РР, содержащий подписанные пользователем файлы. Если к моменту запуска модуля эти файлы отсутствуют, то они создаются автоматически;
- Формируется квитанция о транзакции (файл с расширением *.kvt).

3.6.6 Пример использования

3.6.7 Исходные данные:

- PersonalKeyFile(operator)– boss
- PersonalPIN(operator) – boss
- SignedFile – lettersign.txt

3.6.8 Последовательность действий

В каталоге bin запускаем командную строку

```
./areestr boss boss lettersign.txt
```

```

vlad@vb-u:~/Kupol/KupolCore/bin$ ./areestr boss boss lettersign.txt
Success Protect Function
Ok Test Random
PersonalKeyFile: boss
SignedFileName : lettersign.txt
SignedFile len = 96
Successful PersonalKeyFile read!
Creation PersonalKeyFile Time: 14:22:27 16.08.2019
Ok OutFile write
Ok OutFileIndex write
Read Len = 96
TNum ok Info ok Imi ok Ok transnum Ok imit
DNum      : 25
DNum(full): 4e438564d8610f0e0000000000000019
TNum      : 04c1b84c6c0373c3b079649e9c7901b0
Sign      : 4ef257d3659d60f5
File      : lettersign.txt
NetName   : 00000000000000000000000000000000
AddTime   : 14:22:47 16.08.2019

```

Рис. 17

3.7 Программа «Модуль извлечения информации из РР по номеру звена»

3.7.1 Читает содержимое записи из распределенного реестра (порядковый номер, добавленный файл, сетевое имя пользователя, время добавления и т.д.).

3.7.2 Наименование

creestr

3.7.3 Формат вызова

```

./creestr PersonalKeyFileName(operator)
PersonalPIN(operator) Num [-x OutDir]

```

3.7.4 Параметры вызова

- PersonalKeyFileName(operator) (in) – персональный ключ оператора распределенного реестра;
- PersonalPIN(operator) (in)– пароль оператора распределенного реестра;
- Num (in) – порядковый номер записи в распределенном реестре;

- -x (in) – флаг, указывающий на необходимость записи данных в файл.

При его отсутствии данные не извлекаются из реестра;

- OutDir (in) – каталог, куда пишется файл содержащий запись распределенного реестра (указывается при наличии флага -x).

3.7.5 Результат вызова

3.7.6 Данные о записи РР и результате валидации файла выводятся в стандартный поток. При наличии флага -x, подписанный файл извлекается из РР в директорию OutDir. При отсутствии параметра OutDir подписанный файл извлекается в текущую директорию. Также формируется квитанция (файл с расширением *.ldf).

3.7.7 Пример использования

3.7.8 Исходные данные:

- PersonalKeyFile(operator)– boss
- PersonalPIN(operator)– boss
- Num (in) – 21
- -x (in) – -x
- OutDir (in) – outf

3.7.9 Последовательность действий

В каталоге bin запускаем командную строку

```
./creestr boss boss 21 -x outf
```

```

vlad@vb-u:~/Kupol/KupolCore/bin$ ./creestr boss boss 25 -x outf
Success Protect Function
Ok Test Random
PersonalKeyFile: boss
Index= 25
File = 00000019
MaxIndex=0026
Extract...
Successful PersonalKeyFile read!
Creation PersonalKeyFile Time: 14:22:27 16.08.2019
Ok OutFileIndex read
167566 0
Read Len = 96
Ok transnum
Ok imit
DNum      : 25
DNum(full): 4e438564d8610f0e0000000000000019
TNum      : 04c1b84c6c0373c3b079649e9c7901b0
Sign      : 4ef257d3659d60f5
File      : lettersign.txt
NetName   : 00000000000000000000000000000000
AddTime   : 14:22:47 16.08.2019
Extracting to outf/lettersign.txt
Ok SignedFile write

```

Рис. 18

Содержимое каталога bin/outf после запуска команды



Рис. 19

3.8 Программа «Модуль проверки и экстракции файла»

3.8.1 Восстанавливает исходное сообщение пользователя из подписанного пользователем файла сообщения.

3.8.2 Наименование

rrec

3.8.3 Формат вызова

```
./rrec NetKeyFileName NetKeyPIN SignedFileName [-x]
```

3.8.4 Параметры вызова

- NetKeyFileName (in) – файл, содержащий сетевой ключ пользователя (либо серверный дубликат ключа - с именем состоящем из первых 8 символов сетевого имени пользователя и расширением .007 (файл создан программой gencrkt));
- NetKeyPIN (in)– пароль сетевого ключа (задается при создании NetKeyFileName программой gencrkt);
- SignedFileName – подписанный файл пользователя;
- -x (in) – флаг, указывающий на необходимость записи данных в файл. При его отсутствии данные не извлекаются из подписанного файла.

3.8.5 Результат вызова

3.8.6 Создан файл

- FileToSign (out) – файл, содержащий исходное сообщение пользователя (файл создается в текущем каталоге);

3.8.7 Пример использования

3.8.8 Исходные данные:

- NetKeyFile (in) – 89dbf699.007
- NetKeyPIN (in) – 12
- SignedFile – lettersign.txt
- -x (in) – -x

3.8.9 Последовательность действий

В каталоге bin запускаем командную строку

```
./rrec 89dbf699.007 12 lettersign.txt -x
```

```

vlad@vb-u:~/Kupol/KupolCore/bin$ ./rrec 89dbf699.007 12 lettersign.txt -x
Success Protect Function
Ok Test Random
Extract...
NetKeyFile: 89dbf699.007
Successful NetKeyFile read!
Creation NetKeyFile Time: 12:35:00 16.08.2019
Network name: 89dbf699a5408ba6eea09a11e77fe1b6
Ok SignedFile read
Length: 064
File Signature: c98a71213cf4c9a6
Calc Signature: c98a71213cf4c9a6
FileToSign valid!
Registration SignedFile in: 13:16:29 16.08.2019
FileToSign: letter.txt
Extracted NetName: 89dbf699a5408ba6eea09a11e77fe1b6
Full validation!
Extracting to letter.txt
Ok FileToSign write

```

Рис. 20

Содержимое каталога bin с исходным сообщением пользователя после запуска команды




 rrec.log	935 байт	18:15
 random.bin	32 байта	18:15
 letter.txt	29 байт	18:15

Рис. 21

3.9 Программа «Модуль сервера PP»

3.9.1 Читает поступившие в каталог in файлы, и добавляет в распределенный реестр (с помощью модуля areestr), подписанные файлы пользователя.

3.9.2 Наименование

rrwserv

3.9.3 Формат вызова (запуск PP)

./rrwserv netKeyPin(user)

3.9.4 Параметры вызова

- netKeyPin(user) (in) – пароль пользователя

3.9.5 Результат вызова

3.9.6 Запущен сервер распределенного реестра

3.9.7 Останов сервера распределенного реестра

Для остановки сервера РР необходимо в каталог `in` поместить файл с именем `stopserv`.

3.9.8 Пример использования

3.9.9 Исходные данные:

- `netKeyPin(user) (in) – 12`

3.9.10 Последовательность действий

В каталоге `bin` запускаем командную строку

```
./rrwserv 12
```



```

vlad@vb-u:~/Kupol/KupolCore/bin$ ./rrwserv 12
Success Protect Function
Ok Test Random
Today : 15:15:59 16-08-2019
Input : in
Answer: in_k
Error : in_err
Keys : keys
Out : outf
System 1: ./areestr boss boss
System 2: ./creestr boss boss
.Processing: 0 bytes Time: 0.000000 sec Speed: 0.000000
.....Processing: 0 bytes Time: 0.000000 sec Speed: 0.000000
.....Processing: 0 bytes Time: 0.000000 sec Speed: 0.000000
Ok SignedFile read
Length: 064
File Signature: c98a71213cf4c9a6
Registration SignedFile in: 13:16:29 16.08.2019
FileNameToSign: letter.txt
Extract Netname: 89dbf699a5408ba6eea09a11e77fe1b6
NetKeyFile: 89dbf699.007
Successful NetKeyFile read!
Creation NetKeyFile Time: 12:35:00 16.08.2019
Network name: 89dbf699a5408ba6eea09a11e77fe1b6
Calc Signature: c98a71213cf4c9a6
File valid!
Full validation!
./areestr boss boss in/lettersign.txt
Success Protect Function
Ok Test Random
PersonalKeyFile: boss
SignedFileName : lettersign.txt
SignedFile len = 96
Successful PersonalKeyFile read!
Creation PersonalKeyFile Time: 14:22:27 16.08.2019
Ok OutFile write
Ok OutFileIndex write
Read Len = 96
TNum ok Info ok Imi ok Ok transnum Ok imit
DNum : 26
DNum(full): 4ef257d3659d60f5000000000000001a
TNum : d624aa67fabb10ad1e05878e6715221b
Sign : 3627e5a4c6c03d32
File : lettersign.txt
NetName : 89dbf699a5408ba6eea09a11e77fe1b6
AddTime : 15:16:04 16.08.2019
Result processing = 0
Copy:cp *.kvt in_k
Del:rm *.kvt

```

Рис. 22

3.9.11 Возвращаемые коды ошибок

- 1 – ошибка тестирования модулей защиты,
- 2 – ошибка формата вызова (неверное количество аргументов),
- 3 – файл идентификатора уже существует или не существует файла реального имени,
- 4 – ошибка формирования случайного числа,
- 5 – ошибка обновления случайного числа,
- 6 – ошибка записи файла пользователя,
- 7 – ошибка контрольного чтения файла пользователя.

3.10 Логгирование работы системы

Каждый модуль ведет протокол своей работы, в котором отражаются все операции совершенные модулем. Протокол работы записывается в файл в текущий каталог.

Имя файла протокола формируется из имени модуля и расширения .log. Например, имя файла протокола работы модуля `initus` будет `initus.log`.

4. СООБЩЕНИЯ ОПЕРАТОРУ

4.1. Сообщения, выдаваемые оператору в процессе установки и работы программы, описаны в разделе 3 настоящего документа.

ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

РР	– распределенный реестр
ПС	– программное средство
ОС	– операционная система
КА	– код аутентификации
ПЭВМ	– персональная электронная вычислительная машина

