

Утвержден

ВЕРМ.00119-01-ЛУ

ПС «Купол-СКЗИ для Windows»

Руководство оператора

ВЕРМ.00119-01 34 01

*Листов 24*

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

2019

Литера О<sub>1</sub>

## АННОТАЦИЯ

Настоящий документ содержит сведения, необходимые для обеспечения процедуры общения оператора с программным средством «Купол-СКЗИ для Windows» ВЕР.00119-01 (далее по тексту – ПС «Купол-СКЗИ для Windows»).

## СОДЕРЖАНИЕ

Аннотация	2
Содержание	3
1. Назначение программного средства	4
3. Выполнение программного средства	6
3.1. Загрузка и настройка	6
3.2. Запуск	6
3.3. Работа с ПС «Купол-СКЗИ для Windows»	7
3.4. Программа «Пользовательский интерфейс»	8
3.5. Программа «Модуль формирования сетевого имени»	8
3.6. Программа «Модуль генерации контейнеров для связи с оператором PP»	10
3.7. Программа «Модуль формирования файла для передачи оператору PP»	12
3.8. Программа «Модуль изменения пароля»	14
3.9. Программа «Модуль записи в PP»	15
3.10. Программа «Модуль сервера PP»	16
3.11. Программа «Модуль извлечения информации из PP по номеру звена»	19
3.12. Программа «Модуль проверки и экстракции файла»	20
4. Сообщения оператору	22
Перечень принятых сокращений	23

## 1. НАЗНАЧЕНИЕ ПРОГРАММНОГО СРЕДСТВА

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

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

- Пользовательский интерфейс;
- 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 (rwserv).

1.3. ПС «Купол-СКЗИ для Windows» 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 Windows» 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.

2.2. ПС «Купол-СКЗИ для Windows» функционирует в среде ОС Windows 10 со встроенными и дополнительными интегрируемыми механизмами обеспечения безопасности, реализуемыми средством защиты информации «Secure Pack Rus версия 3.0 (исполнение б)».

### 3. ВЫПОЛНЕНИЕ ПРОГРАММНОГО СРЕДСТВА

#### 3.1. Загрузка и настройка

3.1.1. Установка и настройка ПС «Купол-СКЗИ для Windows» выполняется в соответствии с документом ВЕМР.00119-01 99 01 Инструкция по загрузке и настройке.

#### 3.2. Запуск

3.2.1. Запуск ПС «Купол-СКЗИ для Windows» осуществляется с помощью двойного нажатия клавиши «мыши» на ярлык «Купол-СКЗИ», расположенный на рабочем столе.

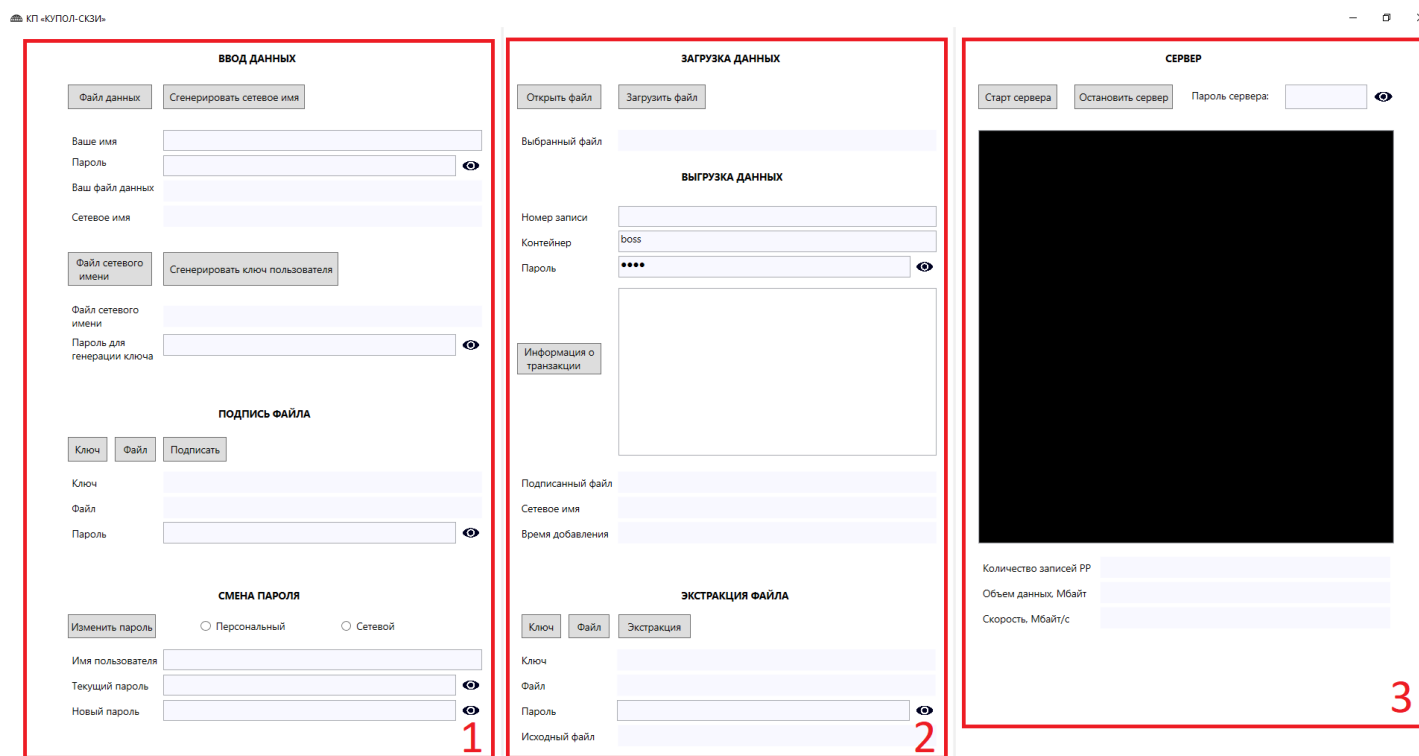
Ярлык «Купол-СКЗИ»



Рис. 1

3.2.2. После запуска на экране отобразится главное окно программы «Пользовательский интерфейс» (рис. 2). Главное окно программы позволяет производить вызовы остальных компонентов комплекса, а также предоставляет пользователю необходимую информацию в удобном для просмотра виде.

## Главное окно программы ПС «Купол-СКЗИ для Windows»



© АО «Концерн ГРАНИТ», 2019

Рис. 2

### 3.3. Работа с ПС «Купол-СКЗИ для Windows»

#### 3.3.1. Описание интерфейса

3.3.1.1. Работа оператора с ПС «Купол-СКЗИ для Windows» производится через графический интерфейс программы «Пользовательский интерфейс».

Главное окно программы «Пользовательский интерфейс» состоит из трех функциональных областей:

- зоны ввода данных, подписи файла и смены пароля (см. рис. 2, область 1);
- зоны загрузки, выгрузки данных, экстракции файла (см. рис. 2, область 2);
- зона сервера (см. рис. 2, область 3).

#### 3.3.2 Работа датчика случайных чисел

3.3.2.1 Запуск каждого модуля начинается с тестирования датчика случайных чисел. Если сгенерированное число не удовлетворяет требованиям, будет выдано соответствующее сообщение (рис.3).

Сообщение об ошибке генерации случайного числа.

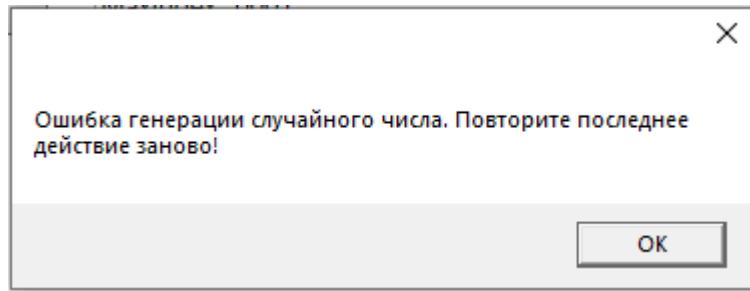


Рис. 3

Для продолжения работы с системой необходимо повторить последнее действие (заново запустить соответствующий модуль).

### 3.4. Программа «Пользовательский интерфейс»

3.4.1. Программа «Пользовательский интерфейс» реализует графический интерфейс оператора.

3.4.2. Описание запуска программы «Пользовательский интерфейс» представлено в п.3.2 данного документа.

3.4.3. Описание графического интерфейса представлено в п. 3.3 данного документа.

### 3.5. Программа «Модуль формирования сетевого имени»

3.5.1. Программа генерирует файл с сетевым именем пользователя (также формируется файл, в котором сетевое имя хранится в бинарном формате) на основе пароля и файла с цифровыми данными пользователя, а также файл, закрытый на пароле персональным идентификатором пользователя (фактически защищенный контейнер для хранения и передачи персонального идентификатора/ключа пользователя).

3.5.2. Перед запуском программы необходимо заполнить пользовательские данные (имя, пароль и пользовательский файл данных). Пользовательский файл необходимо добавить, нажав кнопку «Файл данных» (рис.4). В настоящее время



формат не регламентирован. Это может быть любой файл с цифровой информацией, описывающей пользователя реестра (ФИО, паспортные данные и т.д.)

Кнопка «Файл данных»

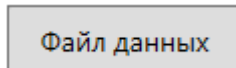


Рис. 4

3.5.3. Запуск программы Модуль формирования сетевого имени осуществляется с помощью кнопки «Сгенерировать сетевое имя» (рис. 5).

Кнопка «Сгенерировать сетевое имя»

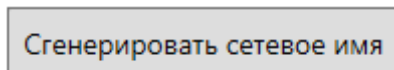


Рис. 5

3.5.4. После запуска программы «Модуль формирования сетевого имени» на экране появится сетевое имя пользователя (рис. 6).

Программа «Модуль формирования сетевого имени»

#### ВВОД ДАННЫХ

Файл данных	Сгенерировать сетевое имя
Ваше имя	<input type="text" value="Ivan"/>
Пароль	<input type="password" value="..."/>
Ваш файл данных	<input type="text" value="ivan.txt"/>
Сетевое имя	<input type="text" value="ceabaac962feb870dd689e4691e8bca0"/>

Рис. 6

3.5.5. Если пользователь с таким именем уже существует, выдается сообщение об ошибке (рис. 7).

## Сообщение об ошибке

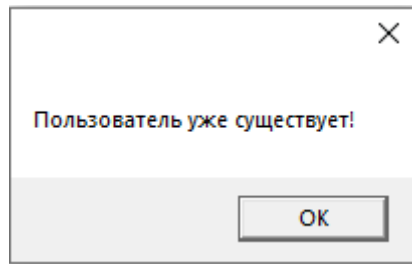


Рис. 7

## 3.6. Программа «Модуль генерации контейнеров для связи с оператором РР»

3.6.1. Программа «Модуль генерации контейнеров для связи с оператором РР» формирует 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).

3.6.2. Перед запуском программы необходимо заполнить пользовательские данные (файл сетевого имени и пароль). Файл сетевого имени добавляется автоматически в интерфейсе после того, как завершила работу программа «Модуль формирования сетевого имени». Если необходимо подключить другой файл с сетевым именем, то необходимо нажать кнопку «Файл сетевого имени» (рис.8) и добавить нужный файл.

## Кнопка «Файл сетевого имени»

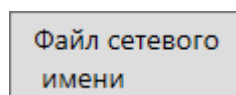


Рис. 8

3.6.3. Запуск программы осуществляется с помощью кнопки «Сгенерировать ключ пользователя» (рис. 9).

Кнопка «Сгенерировать ключ пользователя»

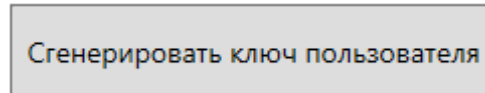


Рис. 9

3.6.4. После запуска программы отобразится сообщение об успешной генерации сетевого ключа (рис. 10).

Программа «Модуль генерации контейнеров для связи с оператором РР»

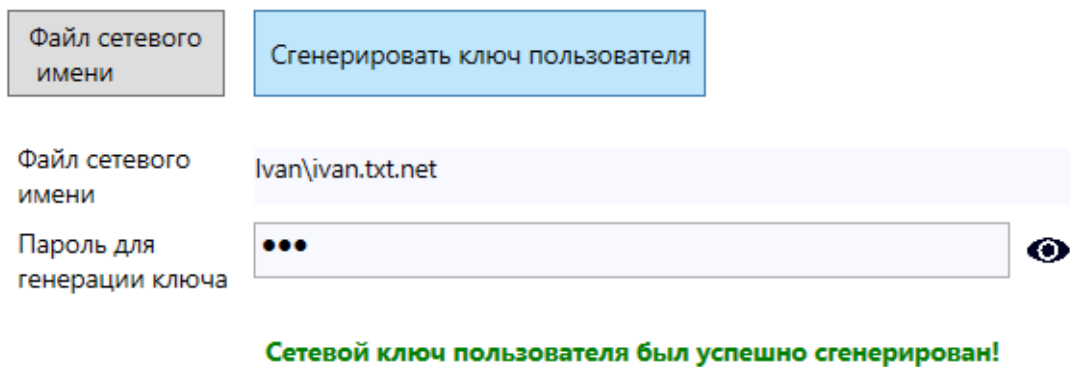


Рис. 10

3.6.5. Если пользователь попытается повторно сгенерировать ключ, он получит сообщение об этом (рис.11).

Сообщение о повторной генерации сетевого ключа

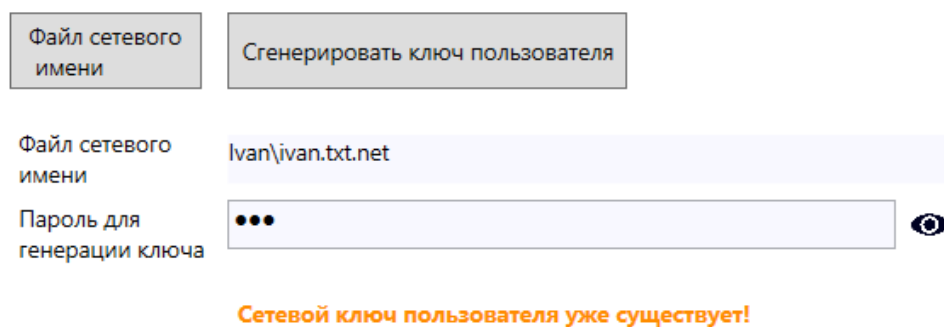


Рис. 11

### 3.7. Программа «Модуль формирования файла для передачи оператору РР»

3.7.1. Программа используется пользователем для подписания файла и его подготовки к дальнейшей отправке в РР.

3.7.2. Перед запуском программы необходимо заполнить пользовательские данные (сетевой контейнер и пароль), а также файл для подписи. Файл с сетевым контейнером добавляется автоматически в интерфейс после того, как завершила работу программа «Модуль генерации контейнеров для связи с оператором РР». Если необходимо подключить другой файл с сетевым контейнером, то необходимо нажать кнопку «Ключ» (рис.12) и добавить нужный файл.

Кнопка «Ключ»

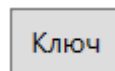


Рис. 12

Аналогично выбирается файл, который необходимо подписать. Для этого необходимо нажать кнопку «Файл» (рис.13) и выбрать нужный файл. Имя файла не должно превышать 31 символ.

Кнопка «Файл»

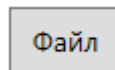


Рис. 13

3.7.3. Запуск программы осуществляется с помощью кнопки «Подписать» (рис. 14).

Кнопка «Подписать»

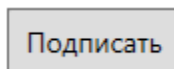



Рис. 14

3.7.4. После запуска программы отобразится сообщение об успешной подписи файла (рис.15).

## Программа «Модуль формирования файла для передачи оператору РР»

## ПОДПИСЬ ФАЙЛА


Ключ	Иван\ivan.txt.007
Файл	kremlin.jpg
Пароль	●●● 

**Файл был успешно подписан!**

Рис. 15

3.7.5. Если пароль был набран неправильно, то выводится сообщение об ошибке (рис.16).

## Сообщение об ошибке «Неверная пара ключ-пароль!»


Ключ	Иван\ivan.txt.007
Файл	kremlin.jpg
Пароль	<input type="password"/> 

**Неверная пара ключ-пароль!**

Рис. 16

3.7.6. Если файл уже был подписан, то об этом выдается соответствующее сообщение (рис.17).

## Сообщение об уже сформированном файле

Ключ	Иван\ivan.txt.007
Файл	kremlin.jpg
Пароль	●●● 

**Файл уже был подписан ранее!**

Рис. 17

### 3.8. Программа «Модуль изменения пароля»

3.8.1. Программа позволяет менять пароль как для персонального, так и сетевого контейнеров.

3.8.2. Перед запуском необходимо убедиться, что пользователь, для которого необходимо изменить пароль, существует. Если он не существует, выдается сообщение с соответствующим содержанием (рис. 18).

Сообщение об отсутствии указанного пользователя

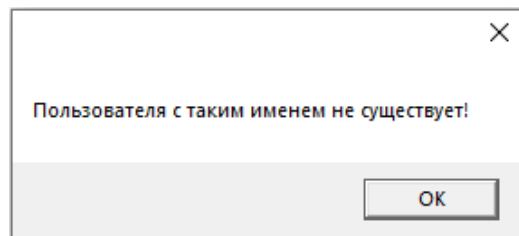


Рис. 18

3.8.3. Также перед запуском программы необходимо выбрать тип ключа и ввести текущий и новый пароль.

3.8.4. Запуск программы осуществляется с помощью кнопки «Изменить пароль» (рис. 19).

Кнопка «Изменить пароль»

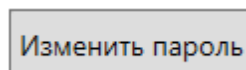


Рис. 19

3.8.5. После запуска программы отобразится сообщение об успешной смене пароля (рис.20).

## Программа «Модуль изменения пароля»

**СМЕНА ПАРОЛЯ**

      Персональный       Сетевой

Имя пользователя

Текущий пароль

Новый пароль

**Сетевой ключ пользователя был успешно изменен!**

Рис. 20

3.8.6. Если текущий пароль был набран неправильно, то выдается сообщение об ошибке (рис.21).

## Сообщение об ошибке «Неправильный текущий пароль»

**СМЕНА ПАРОЛЯ**

      Персональный       Сетевой

Имя пользователя

Текущий пароль

Новый пароль

**Неправильный текущий пароль!**

Рис. 21

## 3.9. Программа «Модуль записи в РР»

3.9.1. Программа «Модуль записи в РР» вызывается программой «Модуль сервера РР» и предназначена для добавления записей в распределенный реестр. Записи добавляет оператор распределенного реестра. 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.

### 3.10. Программа «Модуль сервера РР»

3.10.1. Программа «Модуль сервера РР» обрабатывает запросы пользователей, а также вызывает сервер записи в РР.

3.10.2. Перед запуском необходимо заполнить поле «Пароль сервера» в зоне «Сервер» (заполняется в интерфейсе автоматически после подписания файла), а также в зоне «Загрузка данных» выбрать файл для добавления в реестр. Для этого необходимо нажать кнопку «Открыть файл» (рис.22).

#### Блок «Загрузка данных»

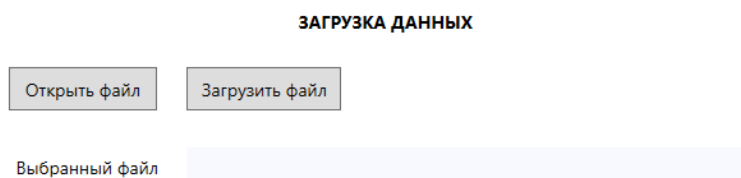


Рис. 22

3.10.3. Запуск программы осуществляется с помощью кнопки «Старт сервера» (рис. 23).

#### Кнопка «Старт сервера»

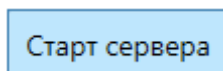


Рис. 23

3.10.4. После запуска программы в окне сервера начнут появляться сообщения об обработке данных (рис.24).



## Окно сервера

```
Starting server...
Success Protect Function
Ok Test Random
Today : 16:36:18 21-08-2019
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
```

Рис. 24

3.10.5. Для добавления файла в реестр необходимо нажать кнопку «Загрузить файл» (рис.25).

## Кнопка «Загрузить файл»

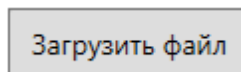


Рис. 25

После нажатия данной кнопки в окне сервера появится информация о прошедшей транзакции (рис.26).

## Окно сервера в момент добавления файла в РР

```
Full validation!
areestr boss boss in\kremlin.drr
Success Protect Function
Ok Test Random
PersonalKeyFile: boss
SignedFileName : kremlin.drr
SignedFile len = 163534
Successful PersonalKeyFile read!
Creation PersonalKeyFile Time: 14:29:42 21.08.2019
Ok OutFile write
Ok OutFileIndex write
Read Len = 163534
TNum ok Info ok lmi ok Ok transnum Ok imit
DNum : 2
DNum(full): f90f7588221e9fac0000000000000002
TNum : 863dbc6ecf0ffa07610ce696fbe81927
Sign : de86f0737398a2d6
File : kremlin.drr
NetName : 6b0ac74cc808b3f0343c8b0b95384bb8
AddTime : 14:50:45 21.08.2019
Result processing = 0
Copy:copy *.kvt in_k
00000002.kvt
'€@īEa@ÿ@д@*@ÿ: 1.
Del:del *.kvt
.Processing: 163502 bytes Time: 0.983000 sec Speed: 166329.609375
.....Processing: 163502 bytes Time: 0.983000 sec Speed: 166329.609375
```

Рис. 26

Также обновятся данные о количестве записей в РР, скорости и размере файла (рис. 27).

### Информация о состоянии реестра

Количество записей РР	3
Объем данных, Мбайт	0,155928
Скорость, Мбайт/с	0,158624

Рис. 27

3.10.6. Для остановки сервера необходимо нажать кнопку «Остановить сервер» (рис.28).

### Кнопка «Остановить сервер»

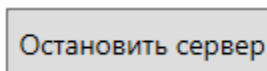


Рис. 28

В этом случае в окне сервера появится запись «Server stopped!».

3.10.7. В случае запуска сервера РР с неверным паролем в окне сервера должно появиться сообщение об ошибке «Error NetKeyFile read» (рис.29).

### Сообщение о невозможности чтения сетевого контейнера пользователя

```
Starting server...
Success Protect Function
Ok Test Random
Today : 16:42:58 21-08-2019
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
....Ok SignedFile read
Length: 163502
File Signature: 8e59f508b7c729a9
Registration SignedFile in: 16:30:24 21.08.2019
FileNameToSign: Ivan\kremlin.jpg
Extract Netname: ceabaac962feb870dd689e4691e8bca0
NetKeyFile: ceabaac9.007
Error NetKeyFile read
Processing: 163502 bytes Time: 0.000000 sec Speed: 0.000000
.....Processing: 163502 bytes Time: 0.000000 sec Speed: 0.000000
```

Рис. 29

### 3.11. Программа «Модуль извлечения информации из РР по номеру звена»

3.11.1. Программа «Модуль извлечения информации из РР по номеру звена» предназначена для получения данных о транзакции (порядковый номер, добавленный файл, сетевое имя пользователя, время добавления и т.д.).

3.11.2. Перед началом работы необходимо ввести номер записи, информацию о которой необходимо получить. (нумерация начинается с нуля, поэтому максимальный номер записи на единицу меньше количества записей в реестре, указанного в нижней части зоны «Сервер»). Также необходимо ввести имя персонального контейнера оператора РР и пароль от него.

3.11.3. Для запуска программы необходимо нажать кнопку «Информация о транзакции» (рис.30).

Кнопка «Информация о транзакции»

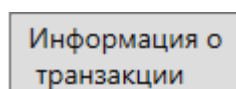


Рис. 30

3.11.4. Если запись с таким номером отсутствует, то выдается сообщение об ошибке (рис.31).

Сообщение об отсутствии транзакции

**ВЫГРУЗКА ДАННЫХ**

Номер записи	<input type="text"/>
Контейнер	<input type="text" value="boss"/>
Пароль	<input type="password" value="••••"/>
<input type="button" value="Информация о транзакции"/>	<div style="border: 1px solid gray; height: 100px; width: 100%;"></div>
Подписанный файл	<input type="text"/>
Сетевое имя	<input type="text"/>
Время добавления	<input type="text"/>


**Транзакция с таким номером не существует!**

Рис. 31

3.11.5. При успешном запуске будет сформирована квитанция с информацией о записи в реестре (подписанный файл, сетевое имя отправителя, время добавления и др.). Также выводится сообщение «Файл успешно извлечен из реестра!» (рис.32).

### Квитанция с информацией о записи в РР

**ВЫГРУЗКА ДАННЫХ**

Номер записи	<input type="text" value="0"/>
Контейнер	<input type="text" value="boss"/>
Пароль	<input type="password" value="••••"/> 
Информация о транзакции	<pre>Success Protect Function Ok Test Random PersonalKeyFile: boss Index= 00 File = 00000000 MaxIndex=0001 Extract... Successful PersonalKeyFile read! Creation PersonalKeyFile Time: 12:15:35 21.08.2019 Ok OutFileIndex read 163603 163603 Read Len = 163535</pre>
Подписанный файл	<input type="text" value="outf\kremlin.drr.001"/>
Сетевое имя	<input type="text" value="f6552369c89e56d7c81911f5ad294a2d"/>
Время добавления	<input type="text" value="13:23:09 21.08.2019"/>

**Файл успешно извлечен из реестра!**

Рис. 32

Пользователь может убедиться в том, что сетевое имя пользователя у извлеченного файла соответствует сетевому имени пользователя, который подписал исходный файл.

## 3.12. Программа «Модуль проверки и экстракции файла»

3.12.1. Программа предназначена для получения исходного файла на основе пароля и сетевого контейнера пользователя.

3.12.2. Перед началом работы необходимо заполнить поля «Ключ», «Файл» и «Пароль» в зоне «Экстракция файла» (если они не были заполнены ранее). Для этого необходимо нажать кнопки «Ключ» и «Файл», и выбрать соответствующие файлы, а также ввести пароль от сетевого контейнера пользователя.

3.12.3. Для запуска программы необходимо нажать кнопку «Экстракция» (рис.33).

## Кнопка «Экстракция»

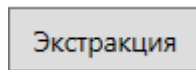



Рис. 33

3.12.4. При успешном запуске будут получены данные о местонахождении извлеченного файла (рис.34).

## Информация об извлеченном файле

**ЭКСТРАКЦИЯ ФАЙЛА**

Ключ	Файл	Экстракция
Ключ	f6552369.007	
Файл	outf\kremlin.drr.001	
Пароль	<input type="password"/> 	
Исходный файл	Derek\kremlin.jpg.001	

**Исходный файл успешно получен!**


Рис. 34

Пользователь может убедиться в том, что извлеченный из РР файл полностью соответствует файлу, который был туда записан ранее.

3.12.5. В случае, если был введен неверный пароль сетевого контейнера, выводится соответствующее сообщение (рис.35).

## Сообщение об неверном пароле

**ЭКСТРАКЦИЯ ФАЙЛА**

Ключ	Файл	Экстракция
Ключ	f6552369.007	
Файл	outf\kremlin.drr.001	
Пароль	<input type="password"/> 	
Исходный файл	Derek\kremlin.jpg.001	

**Неверный пароль пользователя!**

Рис. 35

#### 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

