ООО Фирма «ИнфоКрипт»

Сервер безопасности (Версия 4.0)
Инструкция по эксплуатации

11485466.72.21.12.189 91

2025

Содержание

1 Введение 4
1.1 Общие положения 4
1.2 Системные требования 4
2 Установка 6
3 Подготовка к работе 7
3.1 Настройка файла CRYSRVxxx.INI 7
3.1.1 Секция [address] 8
3.1.2 Секция [dirs] 9
3.1.3 Секция [keys] 13
3.2 Настройка файла THIS.INI 16
4 Описание операций 22
4.1 Начало работы с ПО «Сервер безопасности» 22
4.2 Окончание работы ПО «Сервер безопасности» 24
4.3 Просмотр параметров работы ПО «Сервер безопасности» 25
4.4 Просмотр статистики работы ПО «Сервер безопасности» 26
4.5 Просмотр состояния работы ПО «Сервер безопасности» 27
4.6 Просмотр протокола работы ПО «Сервер безопасности» 28
4.7 Просмотр справочной информации о ПО «Сервер безопасности» 29

Обозначения и сокращения

В настоящем документе используются следующие обозначения и сокращения:

Обозначение	**Описание**
БОК	База открытых ключей
ЛВС	Локальная вычислительная сеть
НЖМД	Накопитель на жёстком магнитном диске
ОЗУ	Оперативное запоминающее устройство
ПО	Программное обеспечение
СКЗИ	Средство криптографической защиты информации
ЭП	Электронная подпись

1 Введение

1.1 Общие положения

ПО «Сервер безопасности (Версия 4.0)» (далее по тексту «Сервер безопасности») обеспечивает в автоматическом режиме функции шифрования и электронной цифровой подписи данных, расположенных на локальном диске или файловом сервере.

Сервер безопасности предоставляет следующие функциональные возможности:

- Обработка исходящих файлов:
  - формирование ЭП в соответствии с требованиями ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»;
  - зашифрование данных в соответствии с требованиями ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая».
- Обработка входящих файлов:
  - расшифрование данных в соответствии с требованиями ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая»;
  - формирование ЭП в соответствии с требованиями ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».
- Ведение протокола обработки всех исходящих и входящих сообщений;
- Ведение архивов исходящих и входящих документов в расшифрованном виде и с электронной подписью.

Сервер безопасности использует в качестве СКЗИ модуль криптографических библиотек «Бикрипт 5.0».

1.2 Системные требования

Сервер безопасности устанавливается на компьютер, удовлетворяющий следующим аппаратным требованиям:

- процессор не ниже Pentium II;
- НЖМД ёмкостью не менее 1 Гб;
- ОЗУ ёмкостью не менее 1 Гб.

Сервер безопасности должен работать под управлением следующих 64-х битных операционных систем: SberLinux (совместим с ОС RedHat 8.6 и выше) и SberOS (совместим с ОС Debian Linux 12 и выше).

При хранении ключей подписи в электронном идентификаторе Touch Memory необходимj устройство считывания аутентифицирующих носителей ТМ Infocrypt.

Главный ключ и узел замены ПО «Сервер безопасности» должны храниться на съёмном носителе (флеш-накопитель или устройство Touch Memory).

2 Установка

Для того чтобы установить ПО «Сервер безопасности», необходимо выполнить следующие действия:

- создать каталог, в котором должно располагаться ПО «Сервер безопасности»;
- скопировать архив crysrv4.tar.gz в созданный каталог;
- выполнить команду

tar -xvfz crysrv4.tar.gz

Перед первым запуском ПО «Сервер безопасности» необходимо произвести его подготовку к работе, включая настройку параметров в конфигурационных файлах CRSRVxxx.INI и THIS.INI (см. раздел 3). Изменение параметров в данных файлах может осуществляться при помощи текстового редактора, сохраняющего файлы обычном текстовом формате.

3 Подготовка к работе

Для подготовки ПО «Сервер безопасности» к работе необходимо настроить следующие конфигурационные файлы:

- **CRYSRVxxx.INI** для задания параметров обработки электронных документов, рабочих каталогов, из которых поступают в обработку и в которые по результатам обработки помещаются электронные документы, а также каталогов и имен файлов с ключами
- **THIS.INI** для задания параметров работы с конфигурационными файлами CRYSRVxxx.INI, имен LOG-файлов с протоколами работы, и индивидуальных параметров, обеспечивающих работу в одной локальной сети нескольких экземпляров ПО «Сервер безопасности» (агрегатирование)

Конфигурационные файлы должны размещаться в том же каталоге, в котором находится исполняемый модуль ПО «Сервер безопасности» – файл ./CRYSRV.

Точка с запятой в начале строки конфигурационного файла указывает на то, что данная строка игнорируется ПО «Сервер безопасности».

При формировании конфигурационного файла каждая строка (в том числе и последняя) должна оканчиваться символом окончания абзаца.

Необходимо также иметь съёмный носитель (флеш-накопитель или идентификатор Touch Memory), на котором должен храниться ключ подписи оператора ПО «Сервер безопасности», а также главный ключ и узел замены ПО «Сервер безопасности».

3.1 Настройка файла CRYSRVxxx.INI

Сервер поддерживает одновременную работу с несколькими (до 999) конфигурационными файлами CRYSRVxxx.INI, параметры работы с которыми задаются в конфигурационном файле THIS.INI, а символы xxx в имени файла CRYSRVxxx.INI определяют номер соответствующего конфигурационного файла.

Некоторые параметры для конфигурационных файлов CRYSRVxxx.INI могут также копироваться из файла THIS.INI. Для этого в файле CRYSRVxxx.INI в качестве значения параметра должно стоять наименование параметра из файла THIS.INI, а перед ним должен стоять знак $ (см. раздел 3.2).

Конфигурационный файл CRYSRVxxx.INI построен по секционному принципу и состоит из трех секций: [address], [dirs] и [keys].

3.1.1 Секция [address]

В секции [address] задаются ключи шифрования для работы по разным направлениям. Секция может включать в себя одно или несколько полей следующего синтаксиса:

Синтаксис

<маска> = <режим_подписывания>, <количество_ЭП_для_проверки>, <режим_шифрования>, <криптономер>, <признак обработки файлов в формате ZIP>

Параметры:

Параметр	Назначение
<маска>	Маска файлов, предназначенных для передачи данному абоненту-получателю. Если параметр принимает значение «*.*», то считается, что все поступающие файлы предназначены для обработки по данному правилу
<режим_подписывания>	Может принимать значение 0 или 1: 0 – не подписывать файлы при отправке; 1 – подписывать файлы при отправке
<количество ЭП для проверки>	Указывает количество ЭП для проверки входящих документов. Если файл подписан меньшим количеством ЭП, чем задано в параметре, то файл переносится в каталог ошибок NO_SIGN. Если параметр принимает значение 0, то проверка ЭП не производится
<режим_шифрования>	Может принимать значения 0, 1 или 2: 0 – не шифровать поступающие файлы; 1 – шифровать поступающие файлы; 2 – шифровать поступающие файлы со сжатием
<криптономер>	Криптономер абонента-получателя (номер его ключа). Если *<режим_шифрования>* = 0, то параметр игнорируется
<признак обработки файлов в формате ZIP>	Может принимать значения 0 или 1: 0 – обычные файлы; 1 – файлы в формате ZIP

Пример 1:

```
[address]
*.ras =1,2,2,2,0
```

Файлы с расширением RAS из каталога OUT_BANK подписывать и шифровать со сжатием с помощью ключа №2. Файлы с расширением RAS из каталога IN_POST расшифровывать с помощью ключа №2 и проверять две ЭП.

Пример 2:

```
[address]
*.*=1,1,1,2,0
```

Все поступающие файлы из каталога OUT_BANK подписывать ЭП и шифровать с помощью ключа №2. Файлы из каталога IN_POST расшифровывать с помощью ключа №2 и проверять одну ЭП.

Пример 3:

```
[address]
00CA*.*2=1,0,0
```

Файлы, начинающиеся с символов 00CA, из каталога OUT_BANK только подписывать. Файлы, начинающиеся с символов 00CA, из каталога IN_POST принимать, не проверяя ЭП.

3.1.2 Секция [dirs]

В секции [dirs] задается список рабочих каталогов ПО «Сервер безопасности»:

Синтаксис

<параметр>=<путь_к_каталогу>

Параметры:

Параметр	Назначение
OUT_BANK	Из данного каталога Сервером безопасности забираются входящие на обработку файлы из прикладной банковской системы (для подписи и шифрования)
OUT_POST	Можно указывать через запятую множественные выходные каталоги. В данные каталоги помещаются файлы для передачи в почтовую или транспортную систему (зашифрованные и подписанные)
TMP_POST	Необязательный параметр. В данный каталог временно помещаются файлы, находящиеся в процессе передачи в почтовую или транспортную систему. По окончании процесса передачи в TMP_POST файлы автоматически перемещаются в каталог, указанный в параметре OUT_POST. Каталоги, указанные в параметрах TMP_POST и OUT_POST должны располагаться на одном логическом диске или на одном сетевом ресурсе, чтобы обеспечить возможность мгновенного перемещения файлов путем изменения имени (rename)

Параметр	Назначение
IN_POST	Из данного каталога «Сервер безопасности» забирает входящие на обработку файлы из почтовой или транспортной системы для расшифрования и проверки подписи
IN_BANK	Можно указывать через запятую множественные выходные каталоги. В данные каталоги помещаются обработанные файлы для передачи в прикладную банковскую систему (расшифрованные и проверенные)
TMP_BANK	Необязательный параметр. В данный каталог временно помещаются файлы для передачи в прикладную банковскую систему, находящиеся в процессе расшифрования и проверки подписи. По окончании процессов расшифрования и проверки подписи файлы перемещаются в каталог, указанный в параметре IN_BANK. Каталоги, указанные в параметрах TMP_BANK и IN_BANK должны располагаться на одном логическом диске или на одном сетевом ресурсе, чтобы обеспечить возможность мгновенного перемещения файлов путем изменения имени (rename)
BAD_SIGN	В данный каталог помещаются файлы с некорректной ЭП
BAD_CRYP	В данный каталог помещаются все неправильно расшифрованные файлы
BAD_EXT	В данный каталог помещаются файлы с неопознанным расширением
NO_REG	В данный каталог помещаются подписанные файлы с незарегистрированной ЭП
NO_SIGN	В данный каталог помещаются неподписанные файлы или файлы, подписанные недостаточным количеством ЭП в соответствии с параметрами секции [address]
NO_CRYP	В данный каталог помещаются незашифрованные файлы, которые в соответствии с параметрами секции [address] должны быть зашифрованы
MY_BAD_CRYP	В данный каталог следует помещать полученные квитанции о неправильном расшифровании файлов абонентом получателя
MY_BAD_SIGN	В данный каталог следует помещать квитанции о некорректной ЭП при расшифровании абонентом принятого файла
MY_NO_REG	В данный каталог следует помещать квитанции о

Параметр	Назначение
	незарегистрированной ЭП при проверке абонентом подписи принятого файла
MY_NO_SIGN	В данный каталог следует помещать квитанции об отсутствии ЭП при проверке абонентом подписи принятого файла
ARHIV_IN	В данном каталоге ведется архив входящих файлов, поступивших на обработку (после операций шифрования и формирования ЭП). Если данный путь не указан, то архивирование входящих файлов не производится
ARHIV_OUT	В данном каталоге ведется архив исходящих файлов, поступивших на обработку (до операций шифрования и формирования ЭП). Если данный путь не указан, то архивирование исходящих файлов не производится

Пример:

```
[dirs]
; Секция [dirs]
; В этой секции задаются имена рабочих директорий криптосервера
;-----------------------------------------------------
; Архивные директории для входящих/исходящих документов
;-----------------------------------------------------
ARHIV_IN  = "arhiv_in"
ARHIV_OUT = "arhiv_out"

;-----------------------------------------------------
; Директории для неверно принятых документов
;-----------------------------------------------------
BAD_CRYP  = "BAD/bad_cryp"
BAD_EXT   = "BAD/bad_ext"
BAD_SIGN  = "BAD/bad_sign"

NO_CRYP     = "BAD/no_cryp"
NO_REG      = "BAD/no_reg"
NO_SIGN     = "BAD/no_sign"

;-----------------------------------------------------
; Директории для пересылаемых в почтовую/банковскую программу
; out_bank - подписать/зашифровать
; out_post - переложить из out_bank
;-----------------------------------------------------
OUT_BANK    = "out_bank"

OUT_POST    = "out_post/out_post, out_post/out_post2, out_post/out_post3"
;TMP_POST       = out_post/tmp

;-----------------------------------------------------
; Директории для принимаемых из почтовой/банковской программы
; in_post - расшифровать/проверить
; in_bank - переложить из in_post
;-----------------------------------------------------
IN_POST   = "in_post"
IN_BANK   = "in_bank/in_bank"
TMP_BANK  = "in_bank/tmp"

;-----------------------------------------------------
; Директории для неверно сформированных документов
; которые вернулись от криптосервера получателя
;-----------------------------------------------------
MY_BAD_CRYP = "BAD/mb_cryp"
MY_BAD_SIGN = "BAD/mb_sign"
MY_NO_REG   = "BAD/mn_reg"
MY_NO_SIGN  = "BAD/mn_sign"
```

Рисунок 1 – Примерное содержание секции [dirs]

Примечание 1

Если имя каталога задать в кавычках, то можно использовать пробелы в имени, например: OUT_BANK = "out bank". При отсутствии кавычек пробелы в имени каталога удаляются.

Примечание 2

Если задать каталог, к которому у данного пользователя нет доступа, то будет выдано сообщение об ошибке.

Примечание 3

Разбор спорных ситуаций в процессе эксплуатации производится на основе анализа содержимого и ЭП файлов, хранящихся в архивах обработанных документов. Вследствие этого должны быть предприняты меры по защите информации, хранящейся в архивных каталогах, от физического уничтожения (жесткое ограничение доступа, резервное копирование, ведение архивов на носителях, исключающих модификацию, и т.п.).

3.1.3 Секция [keys]

В секции [keys] задаются параметры, указывающие каталоги и файлы содержащие ключевую информацию.

Синтаксис

<параметр>=<значение>

Параметры:

Параметр	Назначение
FLAG_X509	Определяет наличие или отсутствие режима проверки X.509 сертификатов: 1 – режим проверки X.509 сертификатов включен. Недействительны параметры: PUB_1_SIGN, PUB_2_SIGN, ADM_SIGN, KEY_CRY, а также параметры *<режим_шифрования>*, *<криптономер>* и *<признак обработки файлов в формате ZIP>* из секции [address] (см. п. 3.1.1). 0 – режим проверки X.509 сертификатов выключен (включен режим проверки по БОК). Недействительны параметры: CHECK_DATE, DETACHED_EXT, CRL_PATH, CRL_CERT_PATH и TRUSTED_CERT_PATH
CHECK_DATE	Указывает дату, на которую проверяется ЭП. Если параметр не задан, используется текущая дата
DETACHED_EXT	Указывает разделённые точкой возможные расширения имени файла для откреплённой ЭП (например, .p7s.sgn.sig). Точка в начале обязательна. Если указано несколько расширений имени файла, то будет

Параметр	Назначение
	обработан первый встреченный файл с первым (вторым и т.д.) расширением, а остальные файлы будут игнорироваться. Если параметр не задан, проверяется прикреплённая ЭП
CRL_PATH	Указывает маску файлов для списков отозванных сертификатов. Если параметр не задан, проверка по спискам отозванных сертификатов не производится
CRL_CERT_PATH	Необязательный параметр. Указывает маску файлов для сертификатов проверки списков отозванных сертификатов. Если параметр не задан, проверка по спискам отозванных сертификатов не производится
TRUSTED_CERT_PATH	Указывает маску файлов для доверенных сертификатов (в том числе p7b сертификатов)
KEY_CRY	Указывает путь к файлу, в котором размещаются сетевые ключи шифрования. В каталоге должны находиться только файлы с ключами шифрования
PUB_1_SIGN	Указывает полный путь к файлу справочника действующих ключей проверки ЭП
PUB_2_SIGN	Указывает полный путь к файлу справочника выводимых из действия ключей проверки ЭП
ADM_SIGN	Необязательный параметр. Указывает полный путь к БОК администраторов криптоключей. С использованием указанной базы производится контроль целостности справочников открытых ключей, указанных в параметрах PUB_1_SIGN и PUB_2_SIGN. В случае нарушения контроля целостности справочников «Сервер безопасности» прекращает работу. В случае отсутствия параметра контроль целостности справочников не производится
SIGN_DELETE	Определяет действие с файлами, содержащими ЭП, в процессе проверки: YES – при перекладывании входящего документа в выходной каталог удаляет подпись, если она была верна; NO – подпись не удаляется, и документ в выходном каталоге будет таким же, как в архиве, т.е. с подписью

Пример:

```
[keys]
; Работа с сертификатами X.509 на приём документов
;
; flag_x509 = 1 включает режим проверки X.509 сертификатов
; flag_x509 = 0 выключает режим проверки X.509 сертификатов (режим БОК)
;
; если задать FLAG_X509 = 1
; в этом режиме недействительны параметры:
; PUB_1_SIGN
; PUB_2_SIGN
; ADM_SIGN
; KEY_CRY
; а также параметры C,D,E (см [address] выше) так как шифрование X.509 не поддерживается
;
; если задать FLAG_X509=0
; тогда недействительны эти 5 параметров:
; CHECK_DATE
; DETACHED_EXT
; CRL_PATH
; CRL_CERT_PATH
; TRUSTED_CERT_PATH

FLAG_X509 = 0

; проверка ЭП для этой даты DD.MM.YYYY (если не задать, то для текущей даты)
;CHECK_DATE                    = 10.10.2029

; расширение для откреплённой ЭП, точка в начале обязательна
; (если не задать, то прикреплённая ЭП)
;DETACHED_EXT           = .p7s.sgn.sig

; маска файлов для стоп-листов
; (если не задать, то не будем проверять по стоп-листам)
; если задать $CRL_FILENAME то будет взято из this.ini CRL_FILENAME=
; CRL_PATH                      = crl\*.crl
;CRL_PATH                       = $CRL_FILENAME

; маска файлов для сертификатов проверки CRL
; (если не задать, то не будем проверять стоп-листы)
; если задать $CERT_TRUSTPATH то будет взято из this.ini CERT_TRUSTPATH=
;CRL_CERT_PATH          = crl\*.cer
;CRL_CERT_PATH          = $CERT_TRUSTPATH

; маска файлов для доверенных сертификатов (в том числе p7b сертификатов)
; если задать $CERT_TRUSTPATH то будет взято из this.ini CERT_TRUSTPATH=
;TRUSTED_CERT_PATH      = crl\*.cer
;TRUSTED_CERT_PATH   = $CERT_TRUSTPATH
;
;              К Л Ю Ч И   П О Д П И С И
; Файл с рабочими открытыми ключами для проверки подписи
PUB_1_SIGN = "sign.dat"
; Файл выводимыми из обращения ключами для проверки подписи
;PUB_2_SIGN = sign2.dat
; Файл с открытыми ключами для проверки подписи администратора
;ADM_SIGN = sign.adm
;           К Л Ю Ч И   Ш И Ф Р О В А Н И Я
; Директория где хранятся ключи шифрования
; они шифрованы на главном ключе
; для экспортной версии данный параметр игнорируется

KEY_CRY = "kl020001.nkl"
```

Рисунок 2 – Примерное содержание секции [keys]

3.2 Настройка файла THIS.INI

В конфигурационном файле THIS.INI указываются параметры работы ПО «Сервер безопасности», такие как период ожидания, ключи ЭП, файл журнала и т.п. Действие параметров данного файла распространяется на все конфигурации, обслуживаемые ПО «Сервер безопасности».

Синтаксис

<параметр>=<значение>

Параметры:

Параметр	Назначение
RUN_MODE	Определяет режим работы ПО «Сервер безопасности» по обслуживанию конфигурационных файлов CRSRVxxx.INI и может принимать следующие значения: AUTO – Сервер безопасности осуществляет непрерывную циклическую работу по обслуживанию конфигурационных файлов CRSRVxxx.INI, обрабатывая их последовательно. ONE – Сервер безопасности обрабатывает для каждого конфигурационного файла CRSRVxxx.INI все поступившие к моменту обработки файлы и уведомления, после чего выводит сообщение «работа завершена» и останавливается. EXIT – Сервер безопасности обрабатывает для каждого конфигурационного файла CRSRVxxx.INI все поступившие к моменту обработки файлы и уведомления, после чего прекращает свою работу
GK_DB3	Определяет место хранения Главного ключа. Может принимать следующие значения: <путь_к_файлу> – Главный ключ (файл GK.DB3) считывается только со съёмного носителя из заданного файла. TMDRV – Главный ключ читается из устройства Touch Memory. При этом значение параметра UZ_DB3 игнорируется

Параметр	Назначение
UZ_DB3	Определяет путь к файлу Узла замены. Узел замены (файл UZ.DB3) считывается только со съёмного носителя
SIGN_KEY	Параметр определяет носитель ключа подписи оператора. Может принимать следующие значения: <путь_к_файлу> – Ключ подписи считывается только со съёмного носителя. После знака равенства следует указать полное имя файла на съёмном носителе с ключом подписи оператора. TMDRV – Ключ подписи оператора считывается из устройства Touch Memory
PASSWORD	Определяет пароль секретного ключа на диске (файл a:\sign_XXXX.key). Является обязательным параметром, если не задан параметр MASK_KEY. Значение параметра – любая комбинация букв и цифр, 6 символов
MASK_KEY	Определяет полный путь к файлу с мастер-ключом администратора (файл с «шумом»)
RECEIVE_ONLY	Определяет режим работы ПО «Сервер безопасности» «только на прием». При активации режима обрабатываются только входящие документы, устройство Touch Memory или съёмный носитель с ключом подписи оператора не запрашиваются
SCAN_TIME	Данный параметр действует, если нет файлов в очереди на обработку. Определяет время в секундах между последовательными циклами опроса входных каталогов, задаваемых параметрами OUT_BANK и IN_POST (см. раздел 3.1.2). Принимает значения от 0 до 30000. При значении близком к нулю существенно увеличивается нагрузка на файл-сервер. Не действует при значениях EXIT и ONE параметра RUN_MODE
SCREEN_SAVER	Задает число секунд, после которого включается функция сохранения экрана. Может принимать значения от 0 до 9999
WAIT_TIME	Задает временную задержку в секундах между поступлением файла на обработку во входные для ПО «Сервер безопасности» каталоги и началом его обработки Сервером безопасности для разрешения возможных конфликтов. Может принимать значения от 0 до 30000.

Параметр	Назначение
	Не действует при значениях EXIT и ONE параметра RUN_MODE
LOG_FILE	В процессе работы ПО «Сервер безопасности» предусмотрено ведение протокола. Данный параметр определяет полное имя файла с протоколом. Файл с протоколом должен размещаться на жестком диске компьютера, на котором установлен Сервер безопасности
ERR_LOG	Определяет имя файла с протоколом сообщений об ошибках приема типа BAD_CRYP, NO_CRYP и т. д., а также о принятии сообщений об ошибках передачи типа MY_BAD_CRYP и др., на которые указанно в конфигурационном файле CRSRVxxx.INI. Для получения списка событий необходимо отфильтровать события в журнале по источнику «SbCrySrv»
OVERWRITE	Определяет поведение ПО «Сервер безопасности» при приеме в обработку файлов с одинаковыми именами. Может принимать следующие значения: YES – при попытке создать файл с именем уже существующего файла старый файл удаляется, и на его месте создается новый. NO – при попытке создать файл с именем уже существующего файла Сервер безопасности останавливает свою работу
TEMP	Определяет каталог, используемый ПО «Сервер безопасности» для создания временных файлов. Данный каталог должен располагаться на локальном диске или на виртуальном диске. В последнем случае ёмкость виртуального диска должна как минимум втрое +10K превышать размер самого большого файла, принимаемого к обработке системой. При работе в режиме агрегатирования можно, но необязательно задавать одинаковые значения параметра TEMP для разных Серверов безопасности, работающих в одной локальной вычислительной сети (ЛВС)
FILE_LOCK	Для исключения проблем с агрегатированием на файлах большой длины (например, более 10 мегабайт) задает режим создания дополнительного файла в рабочем каталоге с именем *.lock.tmp, где расширение .lock.tmp добавляется автоматически. Первый

Параметр	Назначение
	Сервер безопасности создает этот файл, и если второй Сервер безопасности его видит, он соответствующий файл не обрабатывает. После обработки файла файл с именем *.lock.tmp удаляется. Если задать параметр FILE_LOCK=.mylock, то файл будет создаваться с именем *.mylock. Если параметр FILE_LOCK отсутствует или FILE_LOCK= (т. е. без указания расширения файла), то lock файл создаваться не будет
NAME	Определяет уникальный номер Сервера безопасности в данной ЛВС. Используется при работе Сервера безопасности в режиме агрегатирования (работе нескольких Серверов безопасности в одной ЛВС). Может принимать значения от 0 до 999
PKCS_FILENAME	Параметр необходим для включения работы с сертификатами X.509. После знака равенства следует указать полное имя файла с сертификатом владельца ЭП в формате X.509. Сертификат при этом прикрепляется к ЭП. ЭП и сертификат записываются в отдельный файл *.p7s. Если для проверки подписи будут использоваться различные сертификаты, следует указать маску *.cer. В этом случае выбор сертификата пользователя производится на основании предъявленного ключа подписи. Если значение параметра не задано, ЭП формируется в формате Бикрипт
CRL_FILENAME	После знака равенства следует указать полное имя файла со списком отозванных сертификатов. Если будут использоваться несколько списков отозванных сертификатов, следует указать маску *.crl. Если значение параметра не задано, сертификаты пользователя не проверяются по списку отозванных сертификатов
CERT_TRUSTPATH	После знака равенства следует указать полное имя каталога, где находятся сертификаты УЦ для проверки сертификатов пользователя и списков отозванных сертификатов, а также маску имени файла *.cer

Параметр	Назначение
MAX_FILES	Определяет количество файлов, обрабатываемых в рамках сессии работы с каждой конфигурацией. Может принимать значения от 1 до 1000. При отсутствии параметра в конфигурационном файле значение по умолчанию равно 1000
X, Y	Параметры определяют размеры окна в символах. Минимальные размеры 50x15, размеры по умолчанию 80x25
MAX_ARCHIV	Определяет максимальное количество файлов в архивном каталоге (ARHIV_IN и ARHIV_OUT). При превышении этого количества создаётся дополнительный подкаталог hXX_mXX_sXX (часы, минуты, секунды). Может принимать значения от 10 до 100000. Если значение параметра не задано, дополнительный подкаталоги в каталогах ARHIV_IN и ARHIV_OUT создаваться не будут

Пример:

```
RUN_MODE = AUTO

;SIGN_KEY = TMDRV
SIGN_KEY = "sign.key"

MASK_KEY = "mask.key"

;PASSWORD = 123abc

;SCAN_TIME = 3

WAIT_TIME = 0

LOG_FILE = "log.log"

;ERR_LOG  = "err.log"

;RECEIVE_ONLY=YES

TEMP = "temp"

NAME = 1

GK_DB3 = "gk.db3"
UZ_DB3 = "uz.db3"
PRND_DB3 = "prnd.db3"
;UZ_DB3 = tmdrv
;GK_DB3 = tmdrv
;PRND_DB3 = tmdrv

OVERWRITE = yes

SCREEN_SAVER = 1000

;NET_DOWN_ACTION = exit

;PKCS_FILENAME="crserv\TestCA.cer"

;CRL_FILENAME="crl\00CA2565.crl"

;CERT_TRUSTPATH="uc_cert\*.cer"

PKCS_FILENAME = "crl/client.cer"
;CRL_FILENAME="crl\CRYPTO-PRO Test Center 2(1).crl"
CERT_TRUSTPATH = "crl/certnew.cer"

MAX_FILES=1000

X = 150
Y = 50

MAX_ARHIV=1000
```

Рисунок 3 – Примерное содержание файла THIS.INI

4 Описание операций

4.1 Начало работы с ПО «Сервер безопасности»

Для начала работы с программой ПО «Сервер безопасности» необходимо запустить приложение ./CRYSRV.

Если главный ключ и узел замены хранятся на съёмном носителе, необходимо подключить этот носитель.

Если ключ датчика случайных чисел не был создан ранее, необходимо при появлении соответствующего сообщения (см. Рисунок 4) следует нажать кнопку **Ok** для продолжения работы или кнопку **Отмена** для прекращения работы с программой ПО «Сервер безопасности».

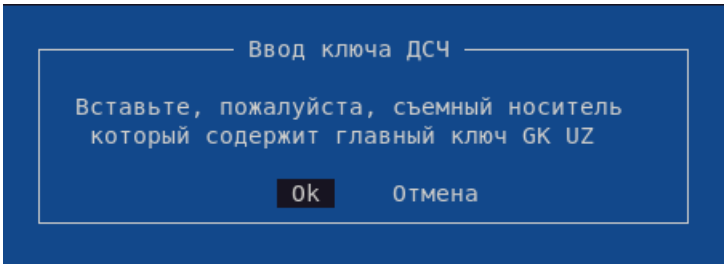

Рисунок 4 – Сообщение о необходимости предъявить носитель главного ключа

В открывшемся окне с сообщением о порядке создания ключа ДСЧ (см. Рисунок 5) следует нажать кнопку **Ok** для продолжения работы или кнопку **Отмена** для прекращения работы с программой ПО «Сервер безопасности».

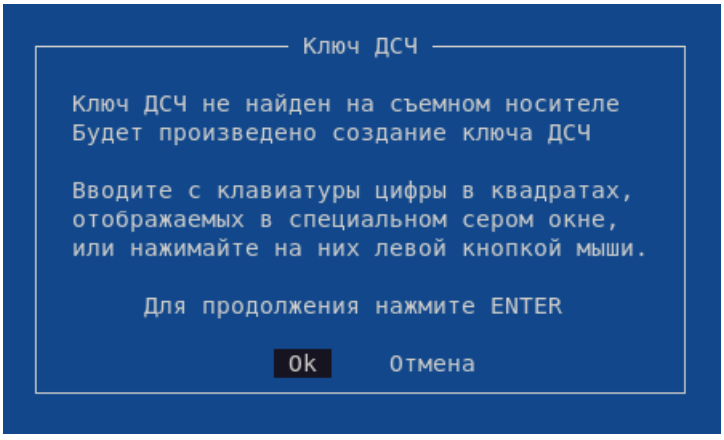

Рисунок 5 – Сообщение о порядке создания ключа ДСЧ

В открывшемся окне инициализации ДСЧ (см. Рисунок 6) необходимо перемещать указатель мыши в пределах этого окна, многократно меняя направление движения по горизонтальной оси. Когда необходимое количество данных будет получено, окно закроется

и будет создан файл с вектором инициализации ПДСЧ.

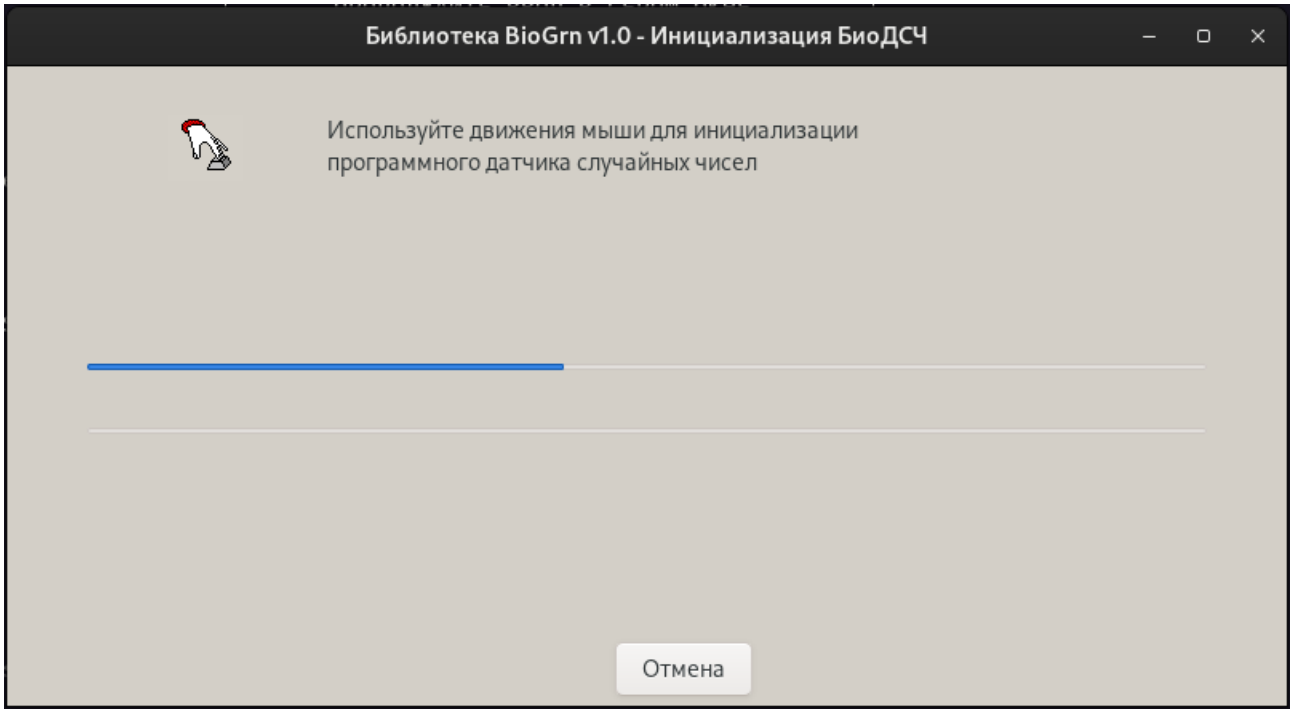

Рисунок 6 – Окно инициализации ПДСЧ

4.2 Окончание работы ПО «Сервер безопасности»

Для окончания работы с программой «Сервер безопасности» следует нажать клавишу F9.

В появившемся окне (см. Рисунок 7) следует нажать кнопку **Выйти** для прекращения работы или кнопку **Продолжить работу** для продолжения работы с программой ПО «Сервер безопасности».

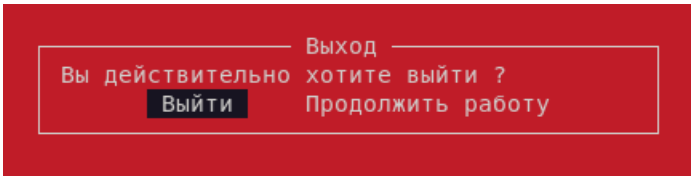

Рисунок 7 Окно выхода из ПО «Сервер безопасности»

4.3 Просмотр параметров работы ПО «Сервер безопасности»

Для того чтобы просмотреть основные параметры работы ПО «Сервер безопасности», содержащихся в конфигурационных файлах CRYSRVxxx.INI и THIS.INI, следует нажать клавишу F2 (см. Рисунок 8).

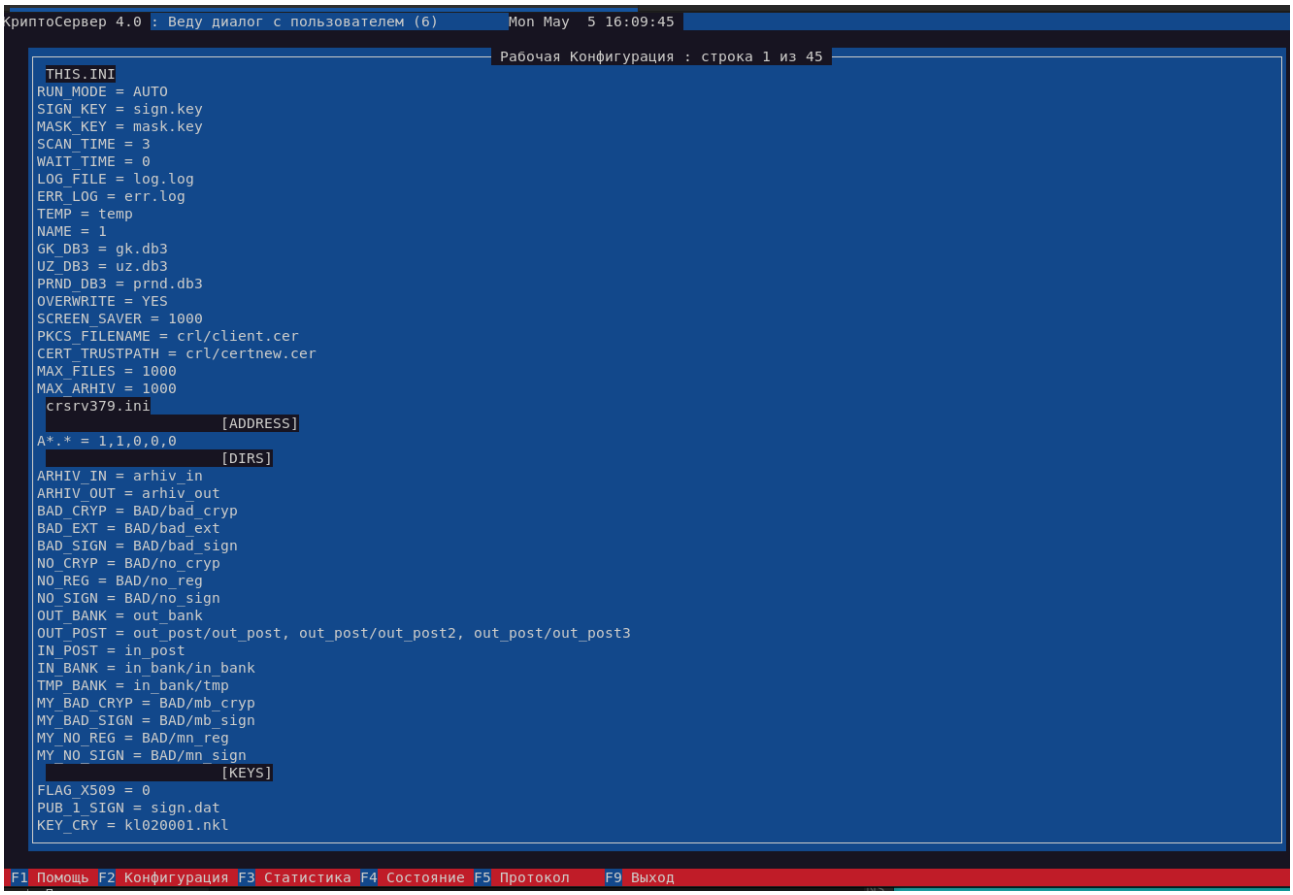

Рисунок 8 – Основные параметры работы ПО «Сервер безопасности»

4.4 Просмотр статистики работы ПО «Сервер безопасности»

Для того чтобы просмотреть статистические данные работы ПО «Сервер безопасности», следует нажать клавишу F3 (см. Рисунок 9).

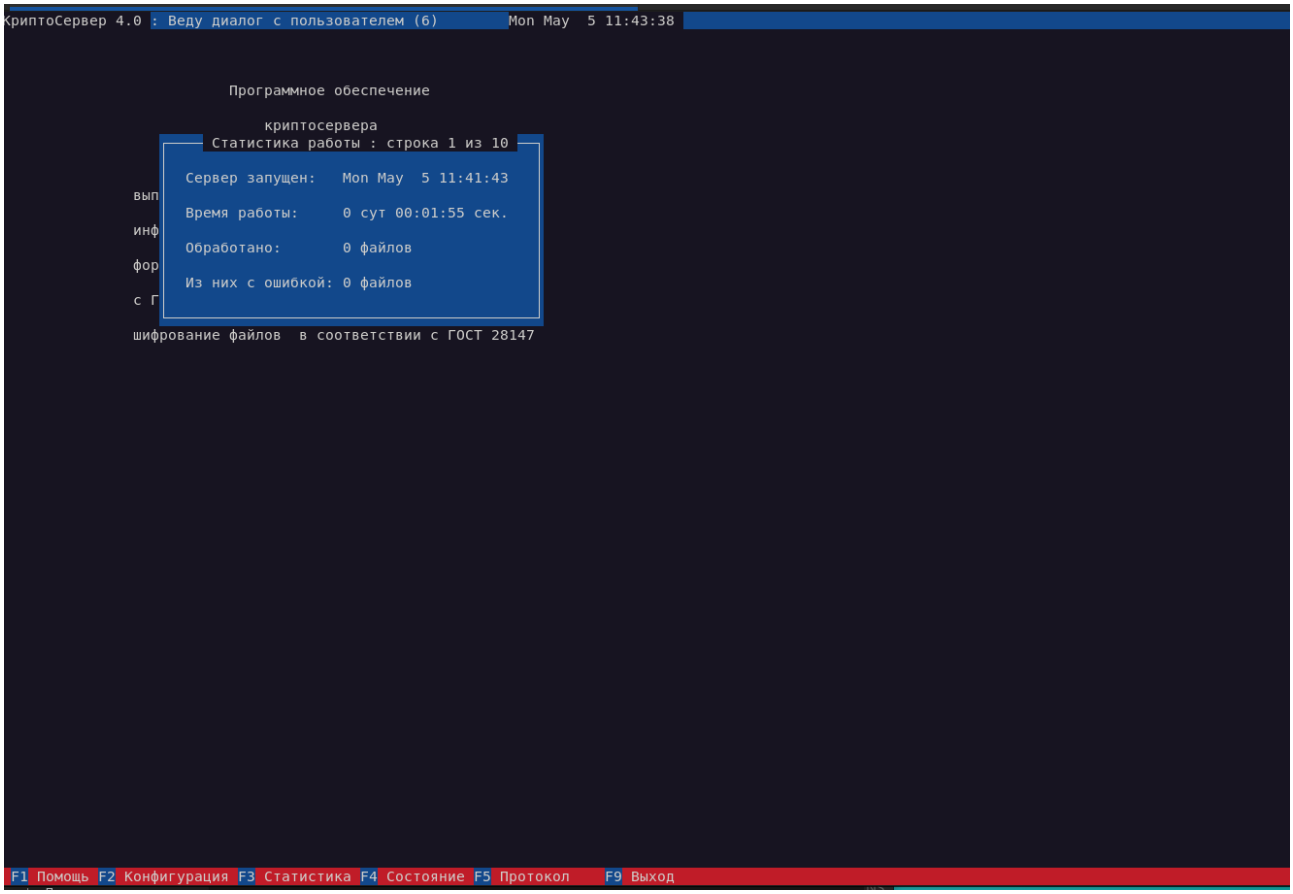

Рисунок 9 – Статистика работы ПО «Сервер безопасности»

4.5 Просмотр состояния работы ПО «Сервер безопасности»

Для того чтобы просмотреть состояние работы ПО «Сервер безопасности», следует нажать клавишу F4 (см. Рисунок 10).

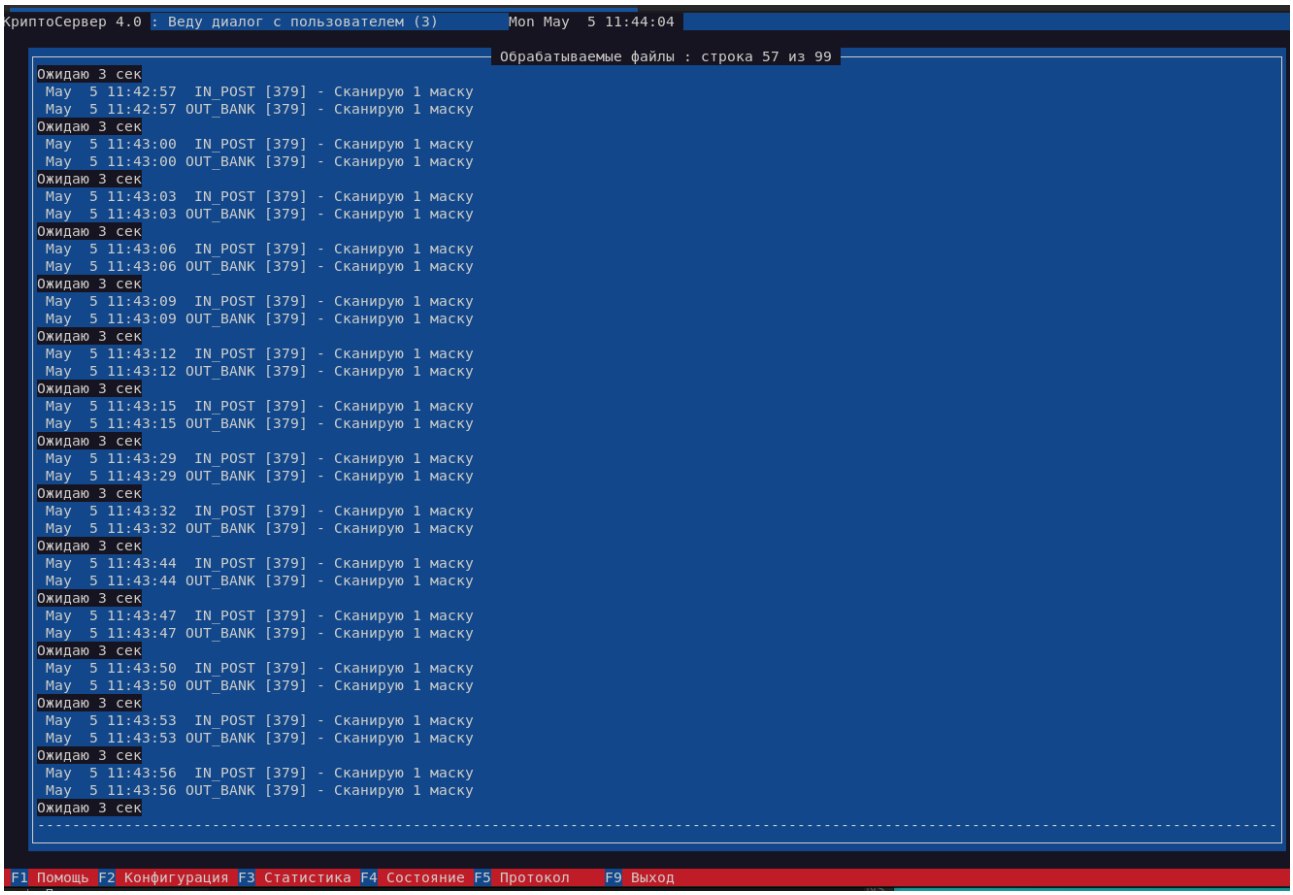

Рисунок 10 – ПО «Сервер безопасности» в режиме работы AUTO

4.6 Просмотр протокола работы ПО «Сервер безопасности»

Для того чтобы просмотреть протокол работы ПО «Сервер безопасности», следует нажать клавишу F5 (см. Рисунок 11).

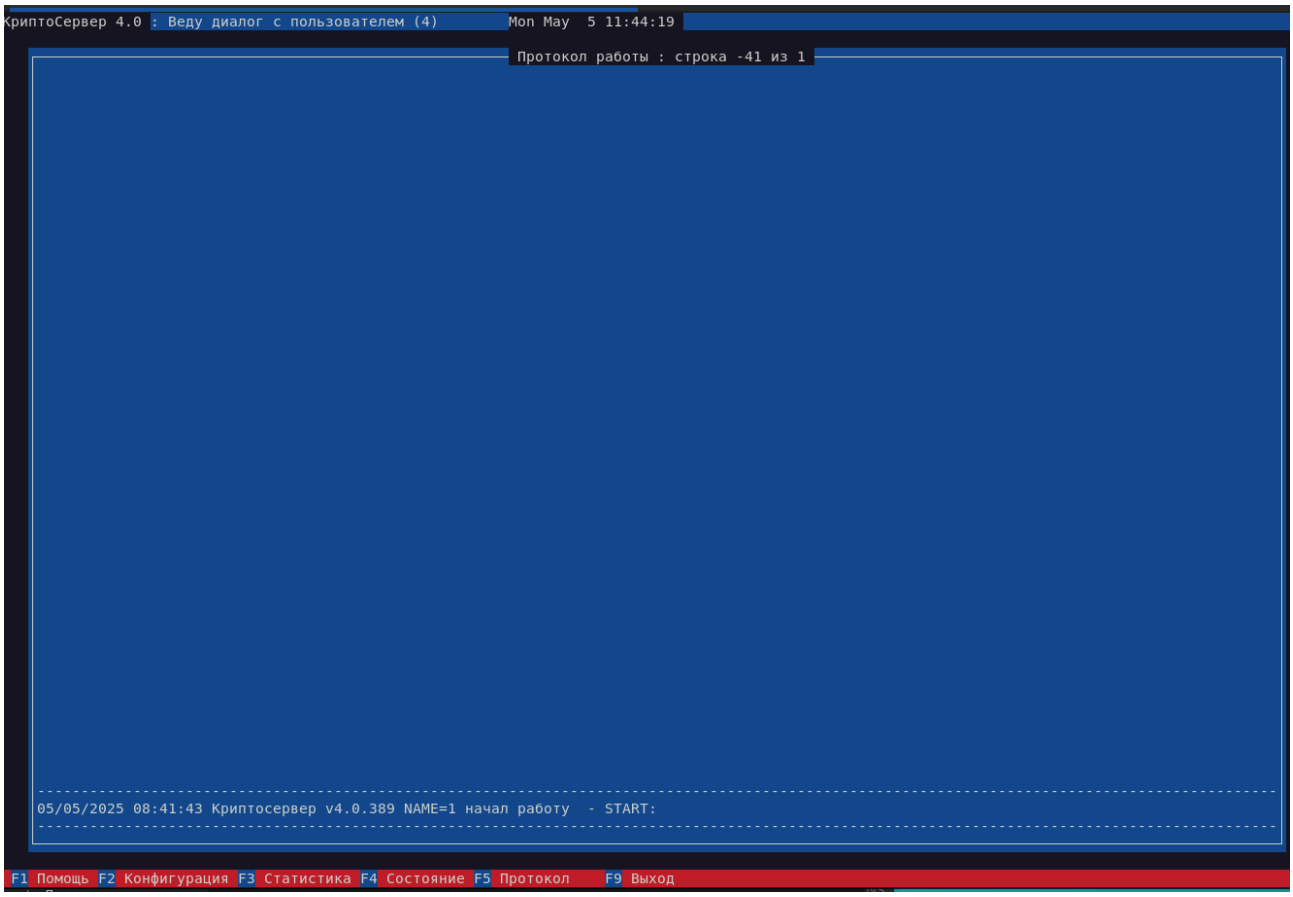

Рисунок 11 – Протокол работы ПО «Сервер безопасности»

4.7 Просмотр справочной информации о ПО «Сервер безопасности»

Для того чтобы просмотреть информации о ПО «Сервер безопасности», следует нажать клавишу F1 (см. Рисунок 12).

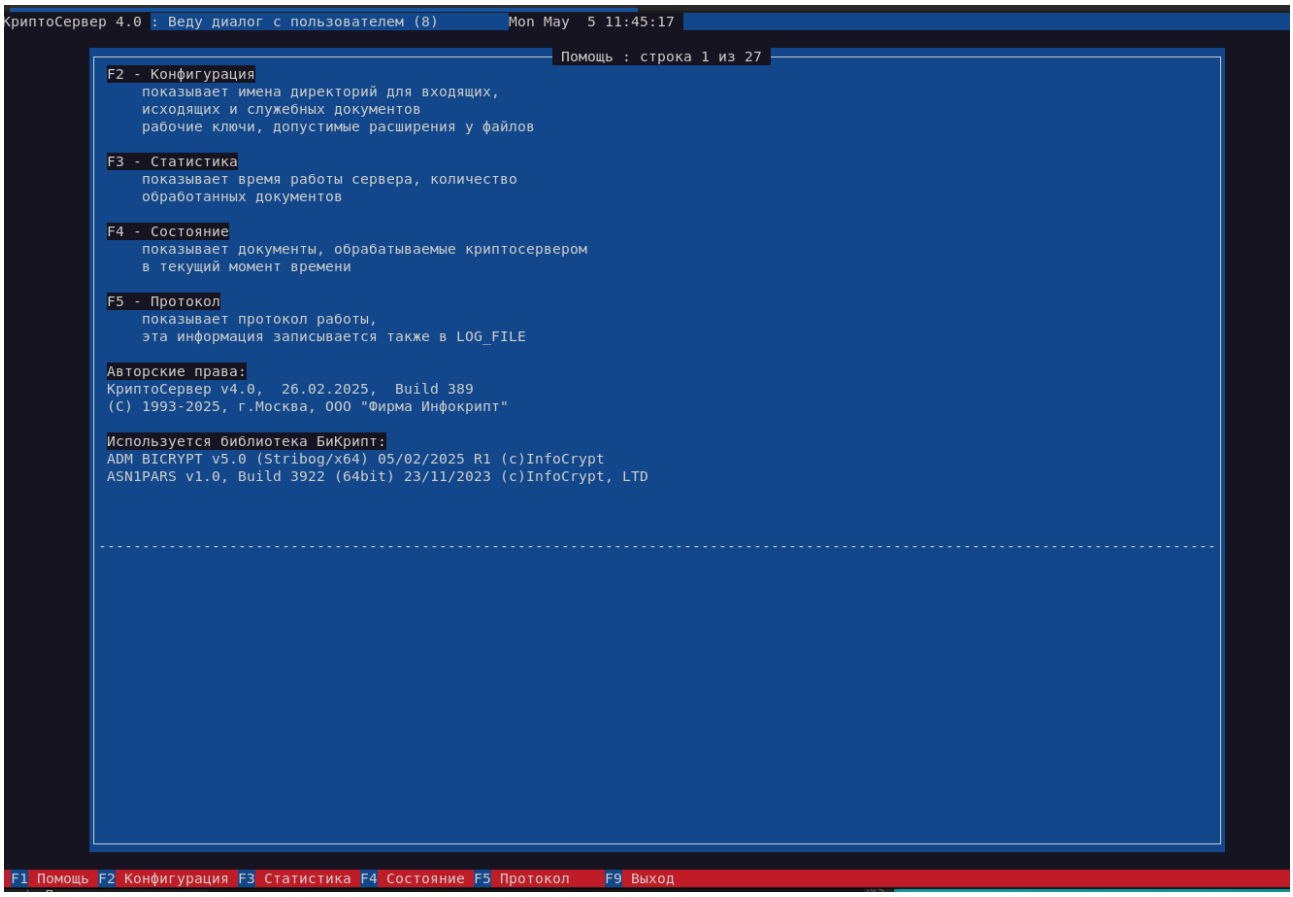

Рисунок 12 – Справочная информация о ПО «Сервер безопасности»

Лист регистрации изменений

№№ п/п	Дата	Описание изменения, основание для внесения изменения	Автор
1			
2			
3			