КОД БЕЗОПАСНОСТИ

Аппаратно-программный комплекс шифрования

Континент
Версия 3.7

Руководство администратора

Локальное управление сетевыми устройствами

RU.88338853.501430.006 96 2 1

© Компания "Код Безопасности", 2017. Все права защищены.

Все авторские права на эксплуатационную документацию защищены.

Этот документ входит в комплект поставки изделия. На него распространяются все условия лицензионного соглашения. Без специального письменного разрешения компании "Код Безопасности" этот документ или его часть в печатном или электронном виде не могут быть подвергнуты копированию и передаче третьим лицам с коммерческой целью.

Информация, содержащаяся в этом документе, может быть изменена разработчиком без специального уведомления, что не является нарушением обязательств по отношению к пользователю со стороны компании "Код Безопасности".

Почтовый адрес:	**115127, Россия, Москва, а/я 66** **ООО "Код Безопасности"**
Телефон:	**8 495 982-30-20**
E-mail:	**info@securitycode.ru**
Web:	**http://www.securitycode.ru**

Оглавление

Введение ... **5**

Общие операции ... **6**
- Запуск сетевого устройства ... 6
- Администрирование ПАК "Соболь" ... 6
- Перезагрузка сетевого устройства ... 7
- Выключение сетевого устройства ... 7

Установка ПО и инициализация сетевого устройства ... **8**
- Установка программного обеспечения ... 8
- Инициализация и подключение ЦУС ... 12
- Инициализация и подключение сетевого устройства ... 16
- Инициализация сервера доступа ... 18
- Переустановка программного обеспечения ... 20
- Восстановление программного обеспечения ... 20

Настройка сетевого устройства ... **22**
- Переход к режиму настройки сетевого устройства ... 22
- Управление сетевым устройством ... 23
  - Переход к меню "Управление" ... 23
  - Создание резервной копии конфигурации сетевого устройства ... 23
  - Повторная инициализация сетевого устройства ... 24
  - Изменение внешнего адреса сетевого устройства ... 25
  - Изменение внешнего адреса ЦУС ... 26
  - Настройка системы управления SNMP ... 27
  - Настройка модемного подключения КШ ... 29
  - Настройки фрагментации пакетов ... 31
  - Настройка параметров шифратора ... 32
  - Настройка STUN ... 33
  - Настройки коммутации ... 34
- Настройки безопасности ... 35
  - Переход к меню "Настройки безопасности" ... 35
  - Регистрация нового администратора ... 36
  - Изменение пароля администратора ... 36
  - Ограничение управления ЦУС и СД ... 37
  - Обновление исходной ключевой информации ... 39
  - Загрузка ключей ... 39
  - Смена ключей на КШ с ЦУС ... 41
  - Просмотр информации о загруженных ключах ... 41
  - Удаление криптографической информации ... 41
  - Ограничение числа соединений ... 42
  - Очистка журналов ЦУС ... 42
  - Настройка параметров локальной сигнализации о НСД ... 43
  - Режим прохождения пакетов с IP-опциями ... 43
  - Привязка аппаратных адресов маршрутизаторов ... 43
  - Управление режимом контроля целостности ... 45
- Настройка сервера доступа ... 45
  - Переход к меню "Настройка СД" ... 45
  - Повторная инициализация сервера доступа ... 46
  - Создание идентификатора администратора ... 46
  - Управление лицензиями ... 47
  - Восстановление базы данных ... 49

Дополнительные возможности ... **50**
- Команды дополнительного меню ... 50
- Корректное выключение питания сетевого устройства ... 52
- Подключение к сетевому устройству через последовательный порт ... 52

Приложение ... **54**
- Аппаратное тестирование сетевого устройства ... 54

Запись образа диска сетевого устройства на USB-флеш-накопитель 55
Программа FlashGUI.exe 55
Программа Flash.exe 56
Протоколы и порты 57
Подключение КШ к действующим локальным сетям 59
Подключение ЦУС 60
Подключение КШ 61
Звуковые сообщения о работе сетевого устройства 61
Показания индикаторов аппаратной платформы 62
Индикаторы сетевых интерфейсов 62
Индикатор ошибки BIOS 63
Особенности эксплуатации КШ с модемным подключением 63
Рекомендуемый порядок подключения КШ к коммутируемой линии 63
Изменение типа телефонной линии при модемном подключении 64
Документация **65**

Введение

Данный документ предназначен для администраторов изделия "Аппаратно-программный комплекс шифрования "Континент". Версия 3.7" RU.88338853.501430.006 (далее — комплекс). В нем содержатся сведения, необходимые администраторам для локального управления сетевыми устройствами.

Приступая к изучению данного руководства, необходимо предварительно ознакомиться с [**1**], а также [**5**] (при использовании сервера доступа).

Сайт в Интернете. Если у вас есть доступ в Интернет, вы можете посетить сайт компании "Код Безопасности" (http://www.securitycode.ru/) или связаться с представителями компании по электронной почте (support@securitycode.ru).

Служба технической поддержки. Связаться со службой технической поддержки можно по телефону 8-495-982-30-20 или по электронной почте support@securitycode.ru. Страница службы технической поддержки на сайте компании "Код Безопасности": http://www.securitycode.ru/products/technical-support/.

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно в авторизованных учебных центрах. Перечень учебных центров и условия обучения представлены на сайте компании http://www.securitycode.ru/company/education/training-courses/. Связаться с представителем компании по вопросам организации обучения можно по электронной почте (education@securitycode.ru).

Общие операции

Для настройки сетевого устройства средствами локального управления к нему необходимо подключить клавиатуру и монитор. При необходимости вместо клавиатуры и монитора к сетевому устройству можно подключить компьютер или ноутбук, имеющий в своем составе последовательный порт. Подробнее о подключении через последовательный порт см. стр.**52**.

Сетевое устройство можно эксплуатировать без монитора. В этом случае работа сетевого устройства контролируется подачей звуковых сигналов. Соответствие звуковых сигналов сообщениям и действия оператора по этим сигналам см. стр.**61**.

Запуск сетевого устройства

В этом разделе представлена процедура запуска сетевого устройства, находящегося в эксплуатации. Процедуру запуска сетевого устройства при первом включении см. стр.**16**.

Для запуска сетевого устройства:

1. Включите питание сетевого устройства. При каждой загрузке сетевого устройства средствами ПАК "Соболь" выполняется контроль целостности файлов программного обеспечения.

   При отсутствии ошибок осуществляется автоматическая загрузка ОС, которая завершается выводом на экран перечня установленного программного обеспечения. После этого подается соответствующий звуковой сигнал, сигнализирующий о готовности сетевого устройства к работе.

   При обнаружении ошибки подается звуковой сигнал о необходимых в данной ситуации действиях оператора.

   Соответствие звуковых сигналов сообщениям и действия оператора по этим сигналам см. стр.**61**.
2. Действуйте в соответствии со звуковыми сообщениями сетевого устройства.

Администрирование ПАК "Соболь"

При получении сообщения сетевого устройства о необходимости вмешательства специалиста (см. стр.**61**) необходимо войти с правами администратора в ПАК "Соболь" и устранить ошибку.

Для администрирования ПАК "Соболь":

1. Выключите питание сетевого устройства. Подключите к системному блоку сетевого устройства клавиатуру и монитор.
2. Включите питание сетевого устройства. На экране появится основное окно ПАК "Соболь", в центре которого будет отображаться запрос персонального идентификатора.

   Не дожидаясь автоматической загрузки сетевого устройства, аккуратно приложите персональный идентификатор администратора к считывателю.

   Если в течение определенного промежутка времени идентификатор предъявлен не будет, сетевое устройство автоматически продолжит загрузку операционной системы. Время ожидания устанавливается администратором при настройке параметров ПАК "Соболь".

   После успешного считывания информации из идентификатора на экране появится меню администратора.

   Все сведения, необходимые администратору для управления работой ПАК "Соболь", содержатся в документе "Программно- аппаратный комплекс "Соболь". Версия 3.0. Руководство администратора" из комплекта поставки сетевого устройства.

Перезагрузка сетевого устройства

Перезагрузка выполняется при обнаружении сбоев в работе программного обеспечения сетевого устройства, а также при проведении инициализации сетевого устройства или администрировании ПАК "Соболь".

Для перезагрузки сетевого устройства:

1. Подключите к сетевому устройству клавиатуру.
2. Одновременно нажмите клавиши <Ctrl>+<Alt>+<Del>.

   Сетевое устройство будет перезагружено.

Для перезагрузки сетевого устройства из главного меню:

1. В главном меню (см. стр. **18**) введите в строке ввода номер команды "Перезагрузить" и нажмите клавишу <Enter>.

   Появится запрос для подтверждения выбранной команды.
2. Введите "Y" и нажмите клавишу <Enter>.

   Сетевое устройство будет перезагружено.

Для перезагрузки сетевого устройства из дополнительного меню:

1. Перейдите к дополнительному меню (см. стр.**50**).
2. В дополнительном меню введите в строке ввода номер команды "Перезагрузить" и нажмите клавишу <Enter>.

   Появится запрос для подтверждения выбранной команды.
3. Введите "Y" и нажмите клавишу <Enter>.

   Сетевое устройство будет перезагружено.

Выключение сетевого устройства

Выключение выполняют при смене источника питания или перемещении сетевого устройства на новое место, а также при проведении инициализации сетевого устройства или администрировании ПАК "Соболь".

Выключение сетевого устройства с помощью кнопки выключения питания, расположенной на корпусе устройства, можно выполнить только на аппаратных платформах MS9297, MS92E3, 92D9 и MS-S021. Выключение устройства на других платформах выполняют следующими средствами:

- в режиме настройки сетевого устройства — из главного меню (см. стр.**22**);
- в режиме функционирования сетевого устройства — из дополнительного меню (см. стр.**50**).

Для выключения сетевого устройства из главного меню:

1. В главном меню введите в строке ввода номер команды "Выключить" и нажмите клавишу <Enter>.

   Появится запрос для подтверждения выбранной команды.
2. Введите "Y" и нажмите клавишу <Enter>.

   Сетевое устройство будет выключено.

Для выключения сетевого устройства из дополнительного меню:

1. Перейдите к дополнительному меню (см. стр.**50**).
2. В дополнительном меню введите в строке ввода номер команды "Выключить" и нажмите клавишу <Enter>.

   Появится запрос для подтверждения выбранной команды.
3. Введите "Y" и нажмите клавишу <Enter>.

   Сетевое устройство будет выключено.

Установка ПО и инициализация сетевого устройства

ЦУС является программным обеспечением, установленным на одном из КШ комплекса. Локальное управление таким КШ имеет некоторые отличия.

Сервер доступа является программным обеспечением, устанавливаемым на КШ, и его наличие зависит от условий поставки.

Установка программного обеспечения

Обычно сетевые устройства поставляются с уже установленным программным обеспечением. В этом случае установку ПО выполнять не требуется.

Установку программного обеспечения на сетевое устройство выполняют при вводе комплекса в эксплуатацию (при поставке ПО на отчуждаемом носителе).

Программное обеспечение сетевого устройства может поставляться на носителях следующих типов:

- CD-ROM;
- USB-флеш-накопитель.

Сетевое устройство может поставляться в корпусе формфактора mini-ITX, не имеющего в своем составе привода CD-ROM. В этом случае все операции по установке программного обеспечения выполняются с использованием USB-флеш-накопителя или USB-CD-привода.

Программное обеспечение сетевого устройства может быть скопировано с CD-ROM на USB-флеш-накопитель с помощью специальной программы (см. стр.**55**).

При использовании USB-флеш-накопителя для установки ПО необходимо, чтобы носитель присутствовал в считывателе до завершения установки, поскольку с этого носителя выполняется загрузка системы.

Если выполняется установка ПО ЦУС, процедура его инициализации начнется автоматически сразу после завершения процедуры установки (см. стр.**12**).

Внимание! При установке ПО параметр BIOS, определяющий порядок опроса устройств для загрузки ОС, должен быть настроен в соответствии с данными, представленными в таблице.

Табл.1 Порядок опроса устройств для загрузки ОС

Носитель	Порядок опроса
CD-ROM	1) CD-ROM; 2) жесткий диск
USB-флеш-накопитель	1) USB-флеш-накопитель; 2) жесткий диск

Для установки программного обеспечения на сетевое устройство:

1. Подключите к системному блоку сетевого устройства клавиатуру и монитор.
2. Включите питание сетевого устройства и войдите в меню установки BIOS (BIOS Setup).

   Совет. Способ входа в меню BIOS отображается на экране на начальной стадии загрузки компьютера. Как правило, для входа в меню используют клавиши <F1>, <F2> или <Del>.

   На экране появится перечень настроек. Вид меню настройки зависит от марки и версии BIOS.
3. Выполните следующие действия:
   - укажите нужный порядок опроса устройств для загрузки ОС в соответствии с используемым носителем (см. Табл.1);
   - установите системное время в соответствии с текущей датой и текущим временем по Гринвичу (при установке ПО ЦУС).

Пример. Для Москвы текущее время нужно уменьшить на три часа.

4. Вставьте входящий в комплект поставки CD-ROM в привод компакт-дисков или подсоедините USB-флеш-накопитель к USB-порту. Затем закройте меню настройки BIOS с сохранением внесенных изменений.

   Компьютер перезагрузится, и на экране появится основное окно ПАК "Соболь", в центре которого будет отображаться запрос персонального идентификатора, подобный следующему:

   ```
   Прислоните и удерживайте персональный идентификатор
   ```

5. Не дожидаясь автоматической загрузки сетевого устройства, аккуратно приложите персональный идентификатор администратора ПАК "Соболь" к считывателю.

   Совет. Если выполнена автоматическая загрузка сетевого устройства, установка программного обеспечения невозможна. В этом случае перезагрузите КШ и повторите процедуру.

   После успешного считывания информации из идентификатора на экране появится запрос пароля.

6. Введите пароль администратора ПАК "Соболь".

   На экране появится предупреждение, подобное следующему:

   ```
   "Внимание: Изменились параметры основного загрузочного
   диска. Возможно, производится загрузка с внешнего
   носителя. Сохранить новые параметры основного загрузочного
   диска? (Да/Нет)"
   ```

   Примечание. Если загрузка ПО осуществляется с USB-флеш-накопителя и вход в ПАК "Соболь" выполнил не администратор, а пользователь, для которого установлен запрет загрузки ОС с внешних носителей, на экране появится сообщение: "Параметры основного загрузочного диска были изменены. Загрузка запрещена". При нажатии любой клавиши выдается сообщение: "Компьютер заблокирован".

7. Введите "Да" и нажмите клавишу <Enter>.

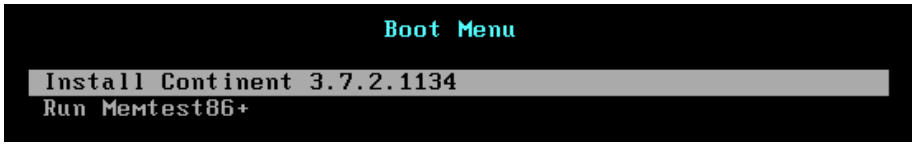
   На экране появится меню администратора, подобное изображенному ниже (для ПАК "Соболь" вер. 3.0).

   Внимание! Нажмите клавишу <F1>. На экране появится окно с параметрами ПАК "Соболь". Выберите в меню администратора команду "Общие параметры системы" и установите для параметра "Автономный режим работы" значение "Нет".

   Подробные сведения о работе с ПАК "Соболь" содержатся в документе "Программно-аппаратный комплекс "Соболь". Версия 3.0. Руководство администратора" из комплекта поставки КШ.

8. Нажмите клавишу <Enter>.

   На экране появится меню.



Пункт меню "Run Memtest86+" предназначен для запуска цикличного теста оперативной памяти. Для запуска теста нажмите клавишу <Enter>. Для остановки теста используйте клавишу <Esc>.

9. Для продолжения процедуры установки выберите пункт "Install Continent" и нажмите клавишу <Enter>.

   Начнется загрузка ОС с предъявленного носителя.

   Примечание. Если на любом этапе установки произошла программная или аппаратная ошибка, осуществляется аварийная автоматическая перезагрузка сетевого устройства, которая **не** сопровождается предупреждающими сообщениями. В этом случае рекомендуется повторить процедуру, начиная с п. 4. При повторном возникновении ошибки необходимо обратиться в службу технической поддержки предприятия-изготовителя.

   По окончании загрузки ОС на экране появится меню:

```
1: Установка
2: Восстановление
3: Тестирование
Выберите номер варианта [1...3]:
```

   Пункт меню "Тестирование" предназначен для выполнения аппаратных тестов сетевого устройства до начала установки ПО. Описание тестов см. стр.**54**.

10. Введите "1" и нажмите клавишу <Enter>.

    На экране появится предупреждение:

```
Установка <<Континент>>
продолжить? (y/n):
```

11. Введите "y" и нажмите клавишу <Enter>.

    На экране появится предупреждение:

```
********** Внимание! **********
ВСЕ данные на жестком диске будут БЕЗВОЗВРАТНО ПОТЕРЯНЫ!
продолжить? (y/n):
```

12. Введите "y" и нажмите клавишу <Enter>.

    На экране появится меню вариантов установки:

```
Выберите вариант установки:
1: Шлюз
2: Шлюз с сервером доступа
3: ЦУС
4: ЦУС с сервером доступа
5: ДА
6: АРМ генерации ключей
7: Коммутатор
Введите номер варианта [1...7]:
```

13. Введите номер нужного варианта и нажмите клавишу <Enter>.

    На экране появится запрос:

```
Введите идентификатор:
```

14. Введите идентификационный номер сетевого усройства и нажмите клавишу <Enter>.

Примечания:

- Идентификационный номер указан в п. 2.2 документа "Аппаратно-программный комплекс шифрования "Континент". Версия 3.7. Криптографический шлюз. Паспорт" и на задней панели системного блока сетевого устройства.
- При установке или обновлении ПО резервного сетевого устройства введите идентификационный номер основного устройства кластера. Идентификационные номера основного и резервного устройств должны быть идентичны.

Внимание! Если запись данных в память ПАК "Соболь" завершится с ошибкой, будет выполнена автоматическая перезагрузка компьютера. В этом случае рекомендуется выполнить инициализацию ПАК "Соболь" и повторить процедуру установки.

После успешной записи данных в память ПАК "Соболь" на экране появятся строка конфигурации данного сетевого устройства и перечень аппаратных платформ.

Внимание! Запишите содержание строки конфигурации в доступном месте. Строку конфигурации потребуется в дальнейшем ввести при регистрации сетевого устройства в ПУ ЦУС. Также строка конфигурации указана в паспорте данного устройства.

15. Введите номер нужной аппаратной платформы и нажмите клавишу <Enter>. Тип шасси аппаратной платформы см. в п. 1.2.1 документа "Аппаратно-программный комплекс шифрования "Континент". Весия 3.7. Криптографический шлюз. Паспорт".

Примечание. Если тип шасси аппаратной платформы IPC в паспорте не указан, введите номер пункта "IPC- <номер> (Другая)". Если наименование аппаратной платформы в списке отсутствует, введите номер пункта "Другая".

Начнется копирование файлов. При успешном завершении установки программного обеспечения на экране появится сообщение:

```
********* Инсталляция произведена успешно *********
```

После чего сразу же осуществится плановая автоматическая перезагрузка компьютера. Во время перезагрузки извлеките носитель с устанавливаемым ПО из привода или отсоедините от USB-порта.

16. Войдите в программу настройки BIOS и установите первоочередной загрузку ОС с жесткого диска. Это обеспечит безошибочную работу комплекса в режиме автозагрузки. Закройте меню настройки BIOS с сохранением внесенных изменений.

Компьютер перезагрузится, и на экране появится основное окно ПАК "Соболь", в центре которого будет отображаться запрос персонального идентификатора.

17. Войдите в меню администратора ПАК "Соболь". Для этого выполните повторно пп. 5–7.

18. Выберите с помощью клавиш со стрелками в меню администратора команду "Настройка общих параметров" и нажмите клавишу <Enter>.

19. В появившемся диалоге выполните следующие действия:

- в поле "Время ожидания автоматического входа в систему (сек.)" укажите время ожидания в секундах (5–40 сек.);
- в поле "Звуковой сигнал" установите значение "Да".

Для этого выберите с помощью клавиш со стрелками нужный пункт и нажмите клавишу <Enter>. Для возврата в меню администратора нажмите клавишу <Esc>.

20. Для загрузки системы выберите с помощью клавиш со стрелками в меню администратора команду "Загрузка операционной системы" и нажмите клавишу <Enter>.

- Если выполняется установка ПО ЦУС, процедура его инициализации начнется автоматически. Перейдите к выполнению п. 7 процедуры инициализации ЦУС (см. стр.**12**).
- В остальных случаях после загрузки операционной системы на экране появится сообщение:

```
Вставьте носитель с конфигурацией и нажмите Enter
```

21. Перейдите к выполнению п. 5 процедуры инициализации сетевого устройства (см. стр. **16**). Если же требуется отложить инициализацию, выключите компьютер (см. стр.**7**).

Инициализация и подключение ЦУС

При инициализации ЦУС выполняют следующие операции:

- подготовка к инициализации;
- настройка сетевых интерфейсов данного КШ;
- загрузка исходной ключевой информации;
- создание идентификатора администратора комплекса;
- настройка дополнительных параметров;
- подключение к сетевым коммуникациям.

В качестве источника исходной ключевой информации может быть использован ПАК "Соболь" или ключевой блокнот РДП-006.

В качестве идентификатора администратора комплекса при инициализации ЦУС могут использоваться устройства типа USB-флеш-накопитель.

При настройке интерфейсов указывают подключаемые к ним сети. Запомните или запишите, какой интерфейс к какой сети необходимо подключить.

Для инициализации ЦУС:

1. Выключите питание КШ. Подключите к системному блоку КШ клавиатуру и монитор.
2. Включите питание КШ и войдите в меню установки BIOS (BIOS Setup).

   Примечание. Способ входа в меню установки BIOS отображается на экране на начальной стадии загрузки компьютера. Как правило, для входа в меню используют клавиши <F2>, <F10>, <Del> или <Alt + S>.

3. Установите в BIOS Setup системное время в соответствии с текущей датой и текущим временем по Гринвичу.

   Пример. Для Москвы текущее время нужно уменьшить на три часа.

4. Закройте меню настройки BIOS с сохранением внесенных изменений.

   Компьютер перезагрузится, и на экране появится основное окно ПАК "Соболь", в центре которого будет отображаться запрос персонального идентификатора.

   Не дожидаясь автоматической загрузки КШ, аккуратно приложите персональный идентификатор администратора к считывателю.

   Если в течение определенного промежутка времени идентификатор не предъявлен, КШ автоматически продолжит загрузку текущей конфигурации. Время ожидания устанавливает администратор при настройке параметров ПАК "Соболь".

   После успешного считывания информации из идентификатора на экране появится запрос пароля.

5. Введите пароль администратора и нажмите клавишу <Enter>.

   На экране появится меню администратора, подобное изображенному ниже (для ПАК "Соболь" вер. 3.0).

Примечание. Все сведения, необходимые администратору для управления работой ПАК "Соболь", содержатся в документе "Программно-аппаратный комплекс "Соболь". Версия 3.0.. Руководство администратора" из комплекта поставки КШ.

В штатном режиме работы КШ загрузка ОС с отчуждаемого носителя для всех пользователей должна быть запрещена. Убедитесь, что режим "Запрет загрузки с внешних носителей" включен для всех пользователей.

6. Выберите с помощью клавиш со стрелками в меню администратора команду "Загрузка операционной системы" и нажмите клавишу <Enter>.

   Дождитесь появления на экране сообщения с пронумерованным списком интерфейсов данного криптографического шлюза, подобного следующему:

```
Криптографический шлюз "Континент"
Конфигурация: ЦУС
Начальная конфигурация ЦУС.
Обнаруженные интерфейсы:
Номер  Имя
1.     em0
2.     em1
3.     em2
4.     tun0
Укажите номер внешнего интерфейса:
```

Примечание. Имена интерфейсов, отображаемые на экране в строке сообщений, соответствуют именам, указанным на корпусе КШ рядом с соответствующим разъемом (кроме tun). Интерфейс tun предназначен для настройки подключения к внешним сетям по протоколу PPPoE.

7. Введите номер, соответствующий внешнему интерфейсу. Например, если к внешней сети подсоединен интерфейс с именем "em0", введите в командной строке "1". Нажмите клавишу <Enter>.

   На экране появится запрос:

```
Введите внешний IP адрес шлюза:
```

8. Введите внешний IP-адрес данного КШ. По этому адресу будут поступать IP-пакеты от внешних и сторонних абонентов. Адрес вводится в формате IPv4 или IPv6 с указанием префикса. Например, 192.0.2.5/24 (для IPv4) или 2345:02BD::5/48 (для IPv6). Нажмите клавишу <Enter>.

   На экране появится запрос:

9. Если допущена ошибка, введите "n" и нажмите клавишу <Enter>. Повторите ввод характеристик внешнего интерфейса.

   Если запись верна, введите "y" и нажмите клавишу <Enter>.

Модемное подключение. Если в п. 7 был указан интерфейс tun, то на экране появится сообщение "Настройка PPPoE" и перечень доступных интерфейсов. Укажите последовательно следующие параметры PPPoE:

- название интерфейса, через который осуществляется подключение;
- имя сервиса;
- имя пользователя;
- пароль.

После определения каждого параметра нажимайте клавишу <Enter>.

На экране появится пронумерованный список внутренних интерфейсов данного криптографического шлюза:

```
  Обнаруженные интерфейсы:
  Номер  Имя
  2.     em1
  3.     em2
Укажите номер внутреннего интерфейса.
Если их несколько — того, к которому подключается АРМ
администратора:
```

10. Введите номер соответствующего интерфейса из списка, представленного на экране. Например, если к локальной сети, в которой находится АРМ администратора, подсоединен интерфейс с именем "em1", введите "2". Если АРМ администратора находится в сети, к которой подсоединен внешний интерфейс (в случае размещения ЦУС в защищенной сети), укажите любой номер из списка. Нажмите клавишу <Enter>.

На экране появится запрос:

```
Введите внутренний IP адрес шлюза:
```

11. Введите IP-адрес данного интерфейса в локальной сети. Адрес вводится с указанием маски (префикса). Например, "10.1.1.200/29". Нажмите клавишу <Enter>.

Примечание. Внутреннему интерфейсу необходимо назначить IP-адрес, даже если подключение защищаемых сетей к этому интерфейсу не предполагается. IP-адрес должен быть уникальным для данной корпоративной сети.

На экране появится сообщение, подобное следующему:

```
Продолжить (y/n)?
```

12. Если допущена ошибка, введите "n" и нажмите клавишу <Enter>. Повторите ввод характеристик внутреннего интерфейса. Если запись верна, введите "y" и нажмите клавишу <Enter>.

После того как параметры интерфейсов определены, на экране появится запрос:

```
Введите адрес маршрутизатора по умолчанию:
```

13. Введите IP-адрес маршрутизатора по умолчанию. Этот маршрутизатор и регистрируемый КШ должны находиться в одной подсети, заданной указанными ранее IP-адресом и маской внешнего интерфейса КШ. Например, "192.0.2.1". Нажмите клавишу <Enter>.

На экране появится сообщение, подобное следующему:

```
Адрес маршрутизатора 192.0.2.1
Продолжить (y/n)?
```

14. Если допущена ошибка, введите "n" и нажмите клавишу <Enter>. Повторите ввод адреса маршрутизатора. Если запись верна, введите "y" и нажмите клавишу <Enter>.

ЦУС сохранит информацию о конфигурации в базе данных, после чего на экране появится сообщение:

```
Использовать внешний носитель для инициализации? (Y/N)
```

15. Выполните одно из следующих действий:

- при использовании в качестве источника исходной ключевой информации ПАК "Соболь" введите "n" и нажмите клавишу <Enter>. Перейдите к п.17;
- при использовании ключевого блокнота РДП-006 введите "y" и нажмите клавишу <Enter>. На экране появится сообщение:

```
Вставьте носитель с исходной ключевой информацией и
нажмите Enter
```

16. Предъявите носитель с исходной ключевой информацией и нажмите клавишу <Enter>.

Исходный ключевой материал будет загружен в ЦУС. По окончании данной операции на экране появится сообщение:

```
Загружена ключевая информация с носителя <наименование
ключевого блокнота>
Введите пароль административного ключа
```

17. Введите пароль и нажмите клавишу <Enter>.

Примечание. Длина и сложность пароля должны соответствовать политике аутентификации администраторов. По умолчанию длина пароля – не менее 4 символов. Разрешено использование любых символов, кроме кириллицы.

Внимание! Запомните пароль. Этот пароль будет использован для шифрования административного ключа и в дальнейшем понадобится для запуска программы управления ЦУС.

На экране появится сообщение:

```
Повторите пароль
```

18. Введите пароль повторно и нажмите клавишу <Enter>.

На экране появится сообщение:

```
Вставьте носитель для записи административного ключа и
нажмите Enter
```

19. Предъявите чистый носитель и нажмите клавишу <Enter>.

Дождитесь сообщения о завершении процедуры конфигурирования и появления главного меню:

```
1: Выключить
2: Перезагрузить
3: Управление
4: Настройки безопасности
5: Настройка ДА <функция недоступна>
6: Настройка СД <функция недоступна>
7: Тестирование
0: Выход
Выберите пункт меню (0-7):
```

Пункт меню "Тестирование" предназначен для выполнения аппаратных тестов сетевого устройства до начала инициализации. Описание тестов см. стр.**54**.

20. Для завершения процедуры инициализации ЦУС введите в строке ввода номер команды "Выход" и нажмите клавишу <Enter>.

Если в течение 5 секунд после появления последнего сообщения клавиша <Enter> нажата не будет, ЦУС автоматически завершит процедуру инициализации.

После завершения инициализации на экране появится сообщение:

```
Успешный запуск <Дата, Время>
```

Примечание. Носитель, содержащий административный ключ, является идентификатором администратора комплекса. Он необходим для запуска программы управления.

21. Извлеките носитель из считывающего устройства.

Загрузка ЦУС осуществится автоматически. С этого момента ЦУС готов к работе.

Примечание. В случае каких-либо нарушений в процедуре инициализации ЦУС повторите процедуру инициализации.

22. Подключите интерфейсы КШ к сетевым коммуникациям в соответствии с настройкой. Имена интерфейсов указаны на корпусе КШ рядом с соответствующим разъемом.

Инициализация и подключение сетевого устройства

При инициализации сетевого устройства выполняют следующие операции:

- загрузка конфигурации сетевого устройства;
- загрузка ключей;
- настройка дополнительных параметров;
- подключение к сетевым коммуникациям.

Конфигурация сетевого устройства может считываться с носителей типа USB-флеш-накопитель.

Для инициализации сетевого устройства:

1. Выключите питание сетевого устройства. Подключите к системному блоку сетевого устройства клавиатуру и монитор.

   Примечание. Если конфигурация сетевого устройства записана на USB-флеш-накопителе, подсоедините его к разъему USB-порта.

2. Включите питание сетевого устройства. На экране появится основное окно ПАК "Соболь", в центре которого будет отображаться запрос персонального идентификатора.

   Не дожидаясь автоматической загрузки сетевого устройства, аккуратно приложите персональный идентификатор администратора к считывателю.

   Если в течение определенного промежутка времени идентификатор не предъявлен, сетевое устройство автоматически продолжит загрузку текущей конфигурации. Время ожидания устанавливает администратор при настройке параметров ПАК "Соболь".

   После успешного считывания информации из идентификатора на экране появится запрос пароля.

3. Введите пароль администратора и нажмите клавишу <Enter>.

   На экране появится меню администратора, подобное изображенному ниже (для ПАК "Соболь" вер. 3.0).

Примечание. Все сведения, необходимые администратору для управления работой ПАК "Соболь", содержатся в документе "Программно-аппаратный комплекс "Соболь". Версия 3.0. Руководство администратора" из комплекта поставки сетевого устройства.

В штатном режиме работы сетевого устройства загрузка ОС с отчуждаемого носителя для всех пользователей должна быть запрещена. Убедитесь, что режим "Запрет загрузки с внешних носителей" включен для всех пользователей.

4. Выберите с помощью клавиш со стрелками в меню администратора команду "Загрузка операционной системы" и нажмите клавишу <Enter>.

   Дождитесь появления на экране следующего сообщения:

   ```
   Вставьте носитель с конфигурацией и нажмите Enter
   ```

5. Предъявите носитель с конфигурационной информацией, сохраненной после регистрации сетевого устройства в базе данных ЦУС (см. [**1**]). Нажмите клавишу <Enter>.

   Если носитель не предъявлен, на нем отсутствуют нужные файлы или файлы повреждены, на экране появится сообщение об ошибке и предложение повторить инициализацию.

   При успешном чтении информации с носителя на экране появится сообщение:

   ```
   Введите пароль
   ```

6. Введите пароль, заданный при записи конфигурации на носитель, и нажмите клавишу <Enter>.

   На экране появится меню загрузки ключей.

   ```
   1: Загрузить активный ключ
   2: Загрузить резервный ключ
   0: Отмена
   Выберите вариант загрузки ключа:
   ```

7. Если загрузка ключей не требуется, введите номер пункта "Отмена" и нажмите клавишу <Enter>.

   На экране появится главное меню. Перейдите к п. 15.

   Если выполняется первичная инициализация, введите номер пункта "Загрузить активный ключ" и нажмите клавишу <Enter>.

   Если ранее инициализация этого сетевого устройства уже проводилась и на сетевом устройстве загружены ключи, то на экране появится следующее сообщение:

   ```
   Уже имеются ключи, установленные на устройстве.
   Осуществить замену ключей? (y/n)
   ```

8. Если замена ключей не требуется, введите "n" и нажмите клавишу <Enter>. На экране появится главное меню. Перейдите к выполнению п. 15.

   Если требуется замена ключей, введите "y" и нажмите клавишу <Enter>. На экране появится сообщение:

   ```
   Вставьте носитель с ключами и нажмите Enter
   ```

9. Вставьте носитель с ключами и нажмите клавишу <Enter>.

   На экране появится список обнаруженных на носителе комплектов ключей.

   Примечание. Если на предъявленном носителе хранятся ключи, записанные средствами ПУ ЦУС для базовой схемы распределения ключей, список будет представлен одним комплектом, содержащим один ключ. Комплекты используются для трехлетней схемы хранения ключей (подробнее о схемах хранения ключей и управлении ключами см. [**1**], [**9**]).

10. Введите номер пункта, соответствующий нужному комплекту ключей, и нажмите клавишу <Enter>.

    На экране появится список ключей выбранного комплекта.

11. Введите номер пункта, соответствующий нужному ключу, и нажмите клавишу <Enter>.

На экране появится запрос ввода пароля.

12. Введите пароль и нажмите клавишу <Enter>.

При правильном вводе пароля на экране появятся сведения о комплекте ключей и запрос на установку данного комплекта.

13. Введите "Y" (без кавычек) и нажмите клавишу <Enter>.

Будет выполнена загрузка ключей и на экране появится сообщение:

```
Ключ установлен как активный
Наажмите Enter для настройки параметров
```

Примечание. Если пароль указан неверно, операция загрузки ключей будет отменена. Загрузку ключей можно повторить, используя дополнительное меню "Настройки безопасности" (см. [2]).

14. Нажмите клавишу <Enter>.

Будет выполнена автоматическая настройка конфигурации сетевого устройства и на экране появится главное меню:

```
1: Выключить
2: Перезагрузить
3: Управление
4: Настройки безопасности
5: Настройка ДА <функция недоступна>
6: Настройка СД <функция недоступна>
7: Тестирование
0: Выход
Выберите пункт меню (0-7):
```

Пункт меню "Тестирование" предназначен для выполнения аппаратных тестов сетевого устройства до начала инициализации. Описание тестов см. стр.**54**.

15. Для завершения процедуры инициализации сетевого устройства введите в строке ввода номер команды "Выход" и нажмите клавишу <Enter>.

Если в течение 5 секунд после появления последнего сообщения клавиша <Enter> нажата не будет, сетевое устройство автоматически завершит процедуру инициализации.

После завершения процедуры инициализации на экране появится сообщение:

```
Успешный запуск <Дата, Время>
```

16. Извлеките носитель из считывающего устройства.

Загрузка сетевого устройства осуществится автоматически. С этого момента сетевое устройство готово к работе.

Примечание. В случае каких-либо нарушений в процедуре инициализации сетевого устройства повторите процедуру инициализации.

17. Подключите интерфейсы сетевого устройства к сетевым коммуникациям в соответствии с настройкой. Имена интерфейсов указаны на корпусе сетевого устройства рядом с соответствующим разъемом.

Внимание! Чтобы ЦУС установил соединение с инициализированным сетевым устройством, в программе управления ЦУС в диалоге "Свойства сетевого устройства" на вкладке "Общие сведения" установите отметку в поле выключателя "Введен в эксплуатацию".

Инициализация сервера доступа

Программное обеспечение сервера доступа устанавливается на криптографическом шлюзе вместе с установкой программного обеспечения ЦУС или КШ.

При первичной инициализации сервера доступа создается идентификатор администратора сервера. В качестве идентификатора могут использоваться USB-флеш-накопители.

Для инициализации сервера доступа:

1. Выполните шаги **1– 12** процедуры первичной инициализации криптографического шлюза (см. стр. **16**) или шаги **1– 20** процедуры первичной инициализации ЦУС (см. стр.**12**).

   Дождитесь появления на экране главного меню:

   ```
   1: Выключить
   2: Перезагрузить
   3: Управление
   4: Настройки безопасности
   5: Настройка СД
   6: Тестирование
   0: Выход
   Выберите пункт меню (0-6):
   ```

   Пункт меню "Тестирование" предназначен для выполнения аппаратных тестов сетевого устройства до начала инициализации. Описание тестов см. стр.**54**.

2. В главном меню введите в строке ввода номер команды "Настройка СД" и нажмите клавишу <Enter>.

   На экране появится сообщение:

   ```
   Начальная конфигурация СД (версия <номер версии>)
   Введите пароль ключа администратора СД
   ```

3. Введите пароль и нажмите клавишу <Enter>.

   Примечание. Длина пароля – не менее 8 символов. Разрешено использование любых символов, кроме кириллицы.

   Внимание! Запомните пароль. Этот пароль будет использован для шифрования административного ключа и в дальнейшем понадобится для запуска программы управления сервером доступа.

   На экране появится сообщение:

   ```
   Повторите пароль
   ```

4. Введите пароль повторно и нажмите клавишу <Enter>.

   На экране появится сообщение:

   ```
   Вставьте носитель для записи ключа ПУ СД и нажмите Enter.
   ```

5. Предъявите носитель для записи ключа.

   Примечание. Это идентификатор администратора сервера доступа. Он необходим для установки соединения программы управления с сервером доступа.

   По окончании создания и записи ключа на носитель на экране появится меню конфигурирования сервера доступа:

   ```
   Конфигурирование Сервера Доступа
   1. Переинициализировать СД
   2. Создать ключевой носитель
   3. Изменить лицензии
   4. Восстановить БД СД
   0. Вернуться в основное меню
   Выберите пункт меню:
   ```

   Процедуры настройки сервера доступа см. стр.**45**.

6. Для завершения конфигурирования сервера введите в строке ввода номер команды "Вернуться в основное меню" и нажмите клавишу <Enter>.

7. Для завершения конфигурирования КШ введите в строке ввода номер команды "Выход" и нажмите клавишу <Enter>.

Примечание. Если в течение 1 минуты команда меню не выбрана, осуществляется автоматическое завершение процедуры конфигурирования сервера.

Запуск сервера доступа осуществится автоматически. На экране появится сообщение:

```
Успешный запуск <Дата> <Время>.
```

Извлеките носитель из считывающего устройства. С этого момента сервер доступа готов к работе.

Переустановка программного обеспечения

Переустановку программного обеспечения на сетевом устройстве выполняют в полном соответствии с описанием установки, приведенным в подразделе "Установка программного обеспечения" (см. стр. **8**). При этом следует иметь в виду, что часть настроек, выполненных локально на сетевом устройстве после первичной установки ПО и настройки комплекса, будет утеряна.

Настройки, не сохраняемые после переустановки ПО сетевого устройства:

Настройки	Сетевое устройство
Настройки snmp	Все устройства
Настройки шифратора	КШ, КК
Настройка локальной сигнализации	Все устройства
Включение привязки маршрутизаторов к MAC-адресам	Все устройства
Пароль локального администратора	Все устройства
Настройка прохождения пакетов с IP-опциями	Все устройства
Настройка программного контроля целостности	Все устройства
Настройки коммутации	КК
Ограничение числа соединений с одного IP-адреса	ЦУС
Ограничения управления	ЦУС
Ограничения управления СД	СД
Настройка замены адресов STUN	ЦУС
Фильтры трафика	ДА

Настройки, сохраняемые после повторной установки ПО сетевого устройства:

Настройки	Сетевое устройство
Настройки фрагментации (pMTU, MSS)	Все устройства
Настройка параметров ppp-доступа	Все устройства
Управление сигнатурным/эвристическим анализатором	ДА
Управление обучением	ДА

Восстановление программного обеспечения

Восстановление программного обеспечения на сетевом устройстве выполняют для устранения сбоев в его работе. При этом журналы и настройки сетевого устройства сохраняются.

Перед началом выполнения процедуры восстановления ознакомьтесь с описанием, приведенном в разделе "Установка программного обеспечения" (см. стр. **8**).

Для восстановления программного обеспечения на сетевом устройстве:

1. Выполните пп. **1**–**8** процедуры установки (см. стр.**8**).

   По окончании загрузки ОС на экране появится меню:

   ```
   1: Установка
   2: Восстановление
   3: Тестирование
   Выберите номер варианта [1...3]:
   ```

2. Введите "2" и нажмите клавишу <Enter>.

   На экране появится предупреждение:

   ```
   Обновление/восстановление <<Континент>>
   продолжить? (y/n):
   ```

3. Введите "y" и нажмите клавишу <Enter>.

   Для отказа от обновления введите "n" и нажмите клавишу <Enter>. Начнется перезагрузка КШ.

   На экране появится меню выбора варианта установки:

   ```
   Выберите вариант установки:
   1: Шлюз
   2: Шлюз с сервером доступа
   3: ЦУС
   4: ЦУС с сервером доступа
   5: ДА
   6: АРМ генерации ключей
   7: Коммутатор
   Введите номер варианта [1...7]:
   ```

   Примечание. USB-флеш-накопитель содержит только один вариант установки ПО.

4. Введите номер нужного варианта и нажмите клавишу <Enter>.

   Начнется копирование файлов. При успешном завершении восстановления на экране появится сообщение:

   ```
   ***** Восстановление произведено успешно *****
   ```

   После чего сразу же осуществится автоматическая перезагрузка компьютера. Во время перезагрузки извлеките носитель с устанавливаемым ПО из привода или отсоедините от USB-порта.

Настройка сетевого устройства

Переход к режиму настройки сетевого устройства

Для перехода к режиму настройки:

1. Выключите питание сетевого устройства. Подключите к системному блоку сетевого устройства клавиатуру и монитор.
2. Включите питание сетевого устройства. На экране появится основное окно ПАК "Соболь", в центре которого будет отображаться запрос персонального идентификатора.

   Не дожидаясь автоматической загрузки сетевого устройства, аккуратно приложите персональный идентификатор администратора к считывателю.

   Если в течение определенного промежутка времени идентификатор не предъявлен, сетевое устройство автоматически продолжит загрузку текущей конфигурации. Время ожидания устанавливает администратор при настройке параметров ПАК "Соболь".

   После успешного считывания информации из идентификатора на экране появится запрос пароля.
3. Введите пароль администратора и нажмите клавишу <Enter>.

   На экране появится меню администратора, подобное изображенному ниже (для ПАК "Соболь" вер. 3.0).

Примечание. Все сведения, необходимые администратору для управления работой ПАК "Соболь", содержатся в документе "Программно-аппаратный комплекс "Соболь". Версия 3.0. Руководство администратора" из комплекта поставки сетевого устройства.

В штатном режиме работы сетевого устройства загрузка ОС с отчуждаемого носителя для всех пользователей должна быть запрещена. Убедитесь, что режим "Запрет загрузки с внешних носителей" включен для всех пользователей.

4. Выберите с помощью клавиш со стрелками в меню администратора команду "Загрузка операционной системы" и нажмите клавишу <Enter>.

   По окончании загрузки операционной системы на экране появится сообщение:

```
Нажмите Enter для настройки параметров
```

5. Нажмите клавишу <Enter>.

   Если в течение 5 секунд клавиша <Enter> нажата не будет, сетевое устройство автоматически продолжит загрузку имеющейся конфигурации.

   После нажатия клавиши <Enter> на экране появится главное меню:

```
1: Выключить
2: Перезагрузить
3: Управление
4: Настройки безопасности
5: Настройка ДА <функция недоступна>
6: Настройка СД <функция недоступна>
7: Тестирование
0: Выход
Выберите пункт меню (0-7):
```

6. Введите в строке ввода номер команды меню и нажмите клавишу <Enter>. Затем выполните действия, соответствующие выбранной команде (см. ниже).

Примечание. Если ни одна из команд меню не будет выбрана в течение 1 минуты, осуществляется автоматическое завершение процедуры настройки.

7. Для завершения процедуры настройки введите в строке ввода номер команды "Выход" и нажмите клавишу <Enter>.

   На экране появится сообщение:

```
Успешный запуск <Дата, Время>.
```

   С этого момента сетевое устройство готово к работе.

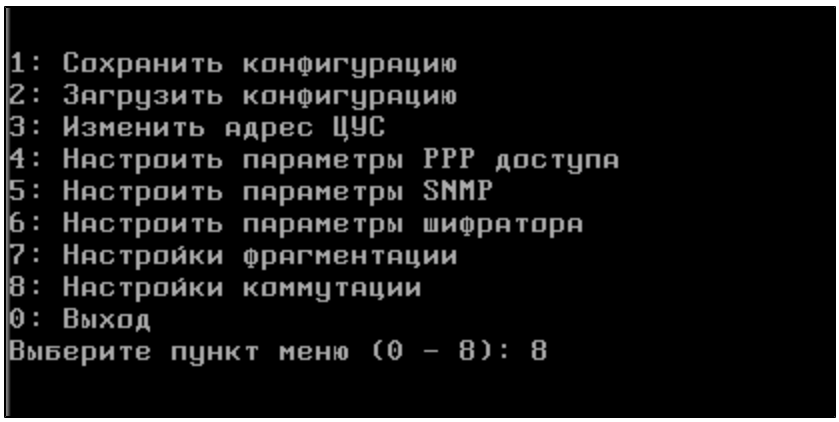
Управление сетевым устройством

Переход к меню "Управление"

Для перехода к меню "Управление":

1. Перейдите к режиму настройки сетевого устройства (см. стр.**22**).
2. В главном меню введите в строке ввода номер команды "Управление" и нажмите клавишу <Enter>.

   На экране появится меню "Управление".



   Внимание! Состав команд меню "Управление" зависит от функционального назначения сетевого устройства — ЦУС, КШ, ДА или КК.

3. Введите номер нужной команды и нажмите клавишу <Enter>.

   Описание процедур см. ниже.

4. Для возврата к главному меню введите в строке ввода номер команды "Выход" и нажмите клавишу <Enter>.

Создание резервной копии конфигурации сетевого устройства

Данная операция позволяет сохранить конфигурацию сетевого устройства в зашифрованном виде на внешнем носителе в файле gate.cfg.

Для создания резервной копии:

1. Предъявите носитель для создания резервной копии.
2. Перейдите к меню управления сетевым устройством (см. стр.**23**).

3. Введите в строке ввода номер команды "Сохранить конфигурацию" и нажмите клавишу <Enter>.

   На экране появится сообщение:

   ```
   Введите пароль
   ```

4. Введите пароль для защиты носителя с конфигурацией и нажмите клавишу <Enter>.

   Внимание! Длина пароля – не менее 5 символов.

   На экране появится сообщение:

   ```
   Повторите пароль
   ```

5. Введите пароль повторно и нажмите клавишу <Enter>.

   Дождитесь возврата в текущее меню.

6. Для завершения процедуры введите в строке ввода номер команды "Выход" и нажмите клавишу <Enter>.

Повторная инициализация сетевого устройства

Повторная инициализация сетевого устройства осуществляется в следующих случаях:

- при обновлении ПО;
- при обнаружении сбоев в работе программного обеспечения.

Процедуры первичной инициализации ЦУС и сетевого устройства см. на стр.**12** и стр.**16**.

При повторной инициализации сетевого устройства выполняют следующие операции:

ЦУС	Сетевое устройство
• Определение параметров сетевых интерфейсов данного сетевого устройства; • загрузка исходной ключевой информации; • создание идентификатора администратора комплекса; • настройка дополнительных параметров (ограничение числа соединений с одного IP-адреса, привязка маршрутизаторов к ARP-адресам и т. д.)	• Загрузка конфигурационной информации; • настройка дополнительных параметров (ограничение числа соединений с одного IP-адреса, привязка маршрутизаторов к ARP-адресам и т. д.)

В качестве носителя исходной ключевой информации и идентификатора администратора комплекса могут использоваться USB-флеш-накопители.

При инициализации сетевого устройства информация о его текущей конфигурации переносится с помощью отчуждаемого носителя (см. [**1**]). Для загрузки конфигурации в сетевое устройство также используются перечисленные выше носители.

Убедитесь в том, что исходная ключевая информация записана на USB-флеш-накопитель.

Для повторной инициализации ЦУС:

1. Перейдите к меню управления сетевым устройством (см. стр.**23**).
2. Введите в строке ввода номер команды "Переинициализировать ЦУС" и нажмите клавишу <Enter>.
3. Далее процедура повторной инициализации ЦУС совпадает с процедурой его первичной инициализации. Перейдите к выполнению п. 7 процедуры инициализации ЦУС (см. стр.**12**).

Примечание. Для того чтобы отказаться от инициализации, нажмите комбинацию клавиш <Ctrl>+<C>. В этом случае осуществится автоматическая загрузка имеющейся конфигурации ЦУС.

Для повторной инициализации сетевого устройства:

1. Выведите сетевое устройство из эксплуатации. Для этого в программе управления ЦУС в диалоге "Свойства сетевого устройства" на вкладке "Общие сведения" удалите отметку из поля "Введен в эксплуатацию" (см. [**1**]). При этом осуществится разрыв управляющего соединения ЦУС с сетевым устройством.
2. Перейдите к меню управления сетевым устройством (см. стр.**23**).
3. Введите в строке ввода номер команды "Загрузить конфигурацию" и нажмите клавишу <Enter>.
4. Далее процедура повторной инициализации сетевого устройства совпадает с процедурой его первичной инициализации. Перейдите к выполнению п. 5 процедуры инициализации сетевого устройства (см. стр.**16**).

Для установления соединения между ЦУС и инициализированным сетевым устройством установите в программе управления ЦУС в диалоге "Свойства сетевого устройства" на вкладке "Общие сведения" отметку в поле "Введен в эксплуатацию".

В случае каких-либо нарушений в процедуре повторной инициализации сетевого устройства повторите эту процедуру еще раз.

Изменение внешнего адреса сетевого устройства

Данную процедуру выполняют для ликвидации нештатной ситуации, когда после изменения внешнего адреса сетевого устройства средствами централизованного управления связь между ЦУС и сетевым устройством установить не удалось.

Предварительно следует изменить внешний адрес централизованно в ПУ ЦУС (см. [**1**]).

Изменение внешнего адреса возможно только при отключенном режиме динамической маршрутизации.

Сетевое устройство

Для изменения внешнего адреса:

1. Перейдите к меню управления сетевым устройством и далее войдите в меню "Настройки безопасности" (см. стр.**35**).
2. Введите в строке ввода номер команды "Изменить внешний адрес" и нажмите клавишу <Enter>.

   На экране появится запрос на ввод нового адреса.
3. Введите новый адрес с указанием маски или префикса (в зависимости от используемого внешним интерфейсом протокола – IPv4 или IPv6) и нажмите клавишу <Enter>.

   На экране появится запрос на ввод адреса маршрутизатора.
4. Введите адрес маршрутизатора и нажмите клавишу <Enter>.

   На экране появится текущее меню.
5. Для завершения процедуры введите в строке ввода номер команды "Выход" и нажмите клавишу <Enter>.

Кластер сетевых устройств

Изменение внешнего адреса в кластере выполняется только на основном сетевом устройстве.

Для изменения внешнего адреса:

1. Выключите резервное сетевое устройство (см. стр.**7**).

2. Перезагрузите основное сетевое устройство (см. стр.**7**).
3. Перейдите к меню управления сетевым устройством и далее войдите в меню "Настройки безопасности" (см. стр.**35**).
4. Введите в строке ввода номер команды "Изменить внешний адрес" и нажмите клавишу <Enter>.

   На экране появится запрос на ввод нового адреса.
5. Введите новый адрес с указанием маски или префикса (в зависимости от используемого внешним интерфейсом протокола – IPv4 или IPv6) и нажмите клавишу <Enter>.

   На экране появится запрос на ввод адреса маршрутизатора.
6. Введите адрес маршрутизатора и нажмите клавишу <Enter>.

   На экране появится текущее меню.
7. В текущем и главном меню введите в строке ввода номер команды "Выход" и нажмите клавишу <Enter>.

   Начнется загрузка сетевого устройства и затем появится сообщение об успешном запуске.
8. Включите резервное сетевое устройство (см. стр.**6**).

   После запуска резервного сетевого устройства на него автоматически с основного сетевого устройства будет передана измененная конфигурация.

Изменение внешнего адреса ЦУС

Данную процедуру выполняют в следующих случаях:

- на КШ с ЦУС – если в результате нештатной ситуации не удалось установить связь между ПУ и ЦУС;
- на КШ – если в результате нештатной ситуации не удалось установить связь между КШ и ЦУС.

Предварительно следует ввести альтернативный внешний адрес ЦУС централизованно в программе управления ЦУС (см. [**1**]).

Изменение внешнего адреса возможно только при отключенном режиме динамической маршрутизации.

Для изменения внешнего адреса ЦУС на КШ с ЦУС:

1. Перейдите к меню управления КШ (см. стр.**23**).
2. Введите в строке ввода номер команды "Изменить внешний адрес КШ с ЦУС" и нажмите клавишу <Enter>.

   На экране появится список альтернативных внешних адресов, введенных ранее средствами централизованного управления.
3. Введите номер нужного адреса и нажмите клавишу <Enter>.

   На экране появится запрос на ввод префикса.
4. Введите префикс для заданного адреса и нажмите клавишу <Enter>.

   На экране появится запрос на ввод адреса маршрутизатора.
5. Введите адрес маршрутизатора и нажмите клавишу <Enter>.

   На экране появится текущее меню.
6. Для завершения процедуры введите в строке ввода номер команды "Выход" и нажмите клавишу <Enter>.

Для изменения адреса ЦУС на КШ:

1. Перейдите к меню управления КШ (см. стр.**23**).
2. Введите в строке ввода номер команды "Изменить адрес ЦУС" и нажмите клавишу <Enter>.

   На экране появится запрос на ввод нового адреса ЦУС.
3. Введите новый адрес ЦУС и нажмите клавишу <Enter>.
4. Для завершения процедуры введите номер команды "Выход".

Настройка системы управления SNMP

Для контроля КШ с помощью средств управления объектами сети по протоколу SNMP в КШ предусмотрен модуль, реализующий сервис SNMP.

Для настройки сервиса SNMP на КШ с помощью локальных средств управления необходимо указать имя community, которое будет являться паролем для доступа к данному сервису, адреса интерфейсов КШ с номерами портов, через которые сервис будет доступен для средств управления сетью.

Имеется возможность рассылки служебных сообщений (traps). Эти сообщения рассылаются при возникновении следующих событий:

- "холодный запуск" (coldStart);
- физическое нарушение связи на интерфейсе (linkDown);
- восстановление связи на интерфейсе (linkUp).

Для рассылки необходимо указать имена community, адреса и номера портов получателей служебных сообщений (traps).

Для настройки системы управления SNMP:

1. Перейдите к меню управления КШ (см. стр.**23**).
2. Введите в строке ввода номер команды "Настроить поддержку SNMP" и нажмите клавишу <Enter>.

   На экране появится строка для ввода служебного параметра "Community name" (имя сообщества), используемого для идентификации отдельных частей сети:

   ```
   Community name:
   ```

3. Введите при необходимости имя сообщества (например "public") или оставьте поле пустым и нажмите клавишу <Enter>.

   На экране появится строка для ввода служебного параметра "Location", используемого для обозначения физического месторасположения КШ:

   ```
   Location:
   ```

4. Введите при необходимости значение параметра (например "Moscow") или оставьте поле пустым и нажмите клавишу <Enter>.

   На экране появится строка для ввода адреса электронной почты лица, ответственного за КШ:

   ```
   e-mail:
   ```

5. Введите при необходимости адрес или оставьте поле пустым и нажмите клавишу <Enter>.

   На экране появится строка для указания источников взаимодействия с системой управления сетью:

   ```
   Источники
   все интерфейсы криптошлюза (Y/N):
   ```

6. Выполните одно из следующих действий:
   - Введите "Y", если источниками информации будут все интерфейсы КШ, и нажмите клавишу <Enter>.

     На экране появится строка для ввода номера порта, который будет использоваться при взаимодействии с системой управления сетью:

     ```
     порт (стандартный – 161):
     ```

     Введите номер порта или оставьте поле пустым для использования порта с номером 161 (по умолчанию) и нажмите клавишу <Enter>.

     На экране появится строка для указания получателей служебных сообщений (traps). Перейдите к выполнению п. 10.
   - Введите "N", если необходимо указать только часть интерфейсов, и нажмите клавишу <Enter>.

На экране появится строка для указания источников взаимодействия с системой управления сетью:

```
Источник 1
IP адрес интерфейса криптошлюза:
```

7. Введите IP-адрес используемого интерфейса КШ и нажмите клавишу <Enter>.

   На экране появится строка для ввода номера порта, который будет использоваться для указанного интерфейса КШ:

   ```
   порт (стандартный – 161):
   ```

8. Введите номер порта или оставьте поле пустым для использования порта с номером 161 (по умолчанию) и нажмите клавишу <Enter>.

   На экране появится строка для указания следующего источника взаимодействия с системой управления сетью:

   ```
   Источник 2 (Y/N):
   ```

9. Выполните одно из следующих действий:
   - Введите "Y", если необходимо указать еще один источник информации, и нажмите клавишу <Enter>. Повторите пп. 7–8.
   - Введите "N", если все источники информации уже определены, и нажмите клавишу <Enter>.

   На экране появится строка для указания получателя служебных сообщений (traps):

   ```
   Получатель traps(Y/N):
   ```

10. Выполните одно из следующих действий:
    - Введите "N", если нет получателей, и нажмите клавишу <Enter>.

      На экране появится текущее меню. Перейдите к выполнению п. 15.
    - Введите "Y", если необходимо указать получателей служебных сообщений (traps), и нажмите клавишу <Enter>.

      На экране появится строка для ввода имени сообщества, в котором находится получатель:

      ```
      Community name:
      ```

11. Введите при необходимости имя сообщества или оставьте поле пустым и нажмите клавишу <Enter>.

    На экране появится строка для ввода IP-адреса получателя:

    ```
    IP-адрес:
    ```

12. Введите IP-адрес получателя и нажмите клавишу <Enter>.

    На экране появится строка для ввода номера порта, который будет использоваться при передаче служебных сообщений:

    ```
    порт (стандартный – 162):
    ```

13. Введите номер порта или оставьте поле пустым для использования порта с номером 162 (по умолчанию) и нажмите клавишу <Enter>.

    На экране появится строка для указания следующего получателя служебных сообщений (traps):

    ```
    Получатель traps 2 (Y/N):
    ```

14. Выполните одно из следующих действий:
    - Введите "Y", если необходимо указать еще одного получателя, и нажмите клавишу <Enter>. Повторите пп. 11–13.
    - Введите "N", если все получатели определены, и нажмите клавишу <Enter>.

      На экране появится текущее меню.

15. Перейдите к настройке следующего параметра или выйдите из меню.

Настройка модемного подключения КШ

Данную процедуру выполняют для ликвидации нештатной ситуации, когда после настройки модемного подключения средствами централизованного управления связь между ЦУС и КШ установить не удалось.

Предварительно следует настроить модемное подключение централизованно в ПУ ЦУС (см. [**1**]).

Модемное подключение не предусмотрено для ЦУС и КШ с установленным сервером доступа. Данная настройка для этих КШ недоступна.

Переход к меню "Настройка параметров PPP-доступа"

Для перехода к меню:

1. Перейдите к меню управления КШ (см. стр.**23**).
2. Введите в строке ввода номер команды "Настроить параметры PPP доступа" и нажмите клавишу <Enter>. На экране появится меню:

```
1: Модем для выделенной линии
2: Входящие модемные звонки
3: Исходящие модемные звонки
4: PPPoE
0: Выход
Выберите режим работы PPP (0-4):
```

3. Введите номер команды и нажмите клавишу <Enter>.

Коммутируемая линия

Для настройки модемного подключения:

1. Введите в строке ввода нужный номер одной из следующих команд:
   - Входящие модемные звонки.
   - Исходящие модемные звонки.

   Нажмите клавишу <Enter>. На экране появится сообщение:

```
Задан режим <название режима> модемных звонков
Скорость порта (0 для USB модема):
```

2. Введите нужное значение скорости передачи данных через COM-порт (например, 19200, 38400, 57600, 115200) и нажмите клавишу <Enter>.

   Пояснение. При использовании USB-порта укажите значение "0".

   На экране появится сообщение:

```
Имя пользователя:
```

3. Введите имя пользователя и нажмите клавишу <Enter>.

   На экране появится сообщение:

```
Пароль:
```

4. Введите пароль и нажмите клавишу <Enter>.

   На экране появится сообщение:

```
Строка инициализации модема:
```

5. Введите значение строки инициализации модема (например "ATS6=0") и нажмите клавишу <Enter>.

   Если задан режим входящих модемных звонков, на экране появится текущее меню. Перейдите к п. 7.

   Если задан режим исходящих модемных звонков, на экране появится сообщение:

```
Номер для дозвона (пустой - прекратить ввод):
```

6. Введите номер телефона модемного пула и нажмите клавишу <Enter>. На экране появится это же сообщение для ввода следующего номера. Введите нужные номера. После ввода каждого номера нажимайте клавишу <Enter>. Для перехода к следующему шагу нажмите клавишу <Enter> без ввода номера.

   На экране появится текущее меню.

7. Перейдите к настройке следующего параметра или выйдите из меню.

Выделенная линия

При использовании выделенной линии необходимо выполнить настройку модема заранее, до подключения его к КШ.

Для настройки модемного подключения:

1. Введите в строке ввода номер команды "Модем для выделенной линии" и нажмите клавишу <Enter>.

   На экране появится сообщение:

   ```
   Задан режим выделенной линии
   Скорость порта:
   ```

2. Введите нужное значение скорости передачи данных через COM-порт (например, 19200, 38400, 57600, 115200) и нажмите клавишу <Enter>.

   Примечание. Значения скоростей передачи данных для модемов на обоих концах соединения должны быть одинаковыми.

   На экране появится сообщение:

   ```
   Имя пользователя:
   ```

3. Введите имя пользователя и нажмите клавишу <Enter>.

   На экране появится сообщение:

   ```
   Пароль:
   ```

4. Введите пароль и нажмите клавишу <Enter>.

   На экране появится текущее меню.

5. Перейдите к настройке следующего параметра или выйдите из меню.

Исходящий PPPoE

Для настройки модемного подключения:

1. Введите в строке ввода номер команды "PPPoE" и нажмите клавишу <Enter>.

   На экране появится сообщение:

   ```
   Задан режим PPPoE
   Доступные интерфейсы: <перечень интерфейсов>
   Название интерфейса, через который осуществляется
   подключение:
   ```

2. Введите название интерфейса и нажмите клавишу <Enter>.

   На экране появится сообщение:

   ```
   Имя сервиса:
   ```

3. Введите имя сервиса и нажмите клавишу <Enter>.

   На экране появится сообщение:

   ```
   Имя пользователя:
   ```

4. Введите имя пользователя и нажмите клавишу <Enter>.

   На экране появится сообщение:

   ```
   Пароль:
   ```

5. Введите пароль и нажмите клавишу <Enter>.

   На экране появится текущее меню.

6. Перейдите к настройке следующего параметра или выйдите из меню.

Настройки фрагментации пакетов

В рамках механизмов фрагментации передаваемых пакетов на сетевом устройстве предусмотрены следующие настройки:

- принудительная установка флага DF (Don't fragment);
- задание значения MSS.

Принудительная установка флага DF выполняется раздельно на канале управления и каналах VPN. По умолчанию после установки ПО и инициализации сетевого устройства принудительная установка флага DF для канала управления и VPN-каналов включена.

Внимание! Настройки фрагментации пакетов выполняют централизованно средствами ПУ ЦУС. Приведенные ниже процедуры настройки рекомендуется применять в тех случаях, когда по каким-либо причинам настройку нельзя выполнить централизованно.

Для настройки фрагментации пакетов:

1. Перейдите к меню управления сетевым устройством (см. стр.**23**).
2. Введите в строке ввода номер команды "Настройки фрагментации" и нажмите клавишу <Enter>.

   На экране появится меню настроек фрагментации.

```
1: Показать текущие настройки фрагментации
2: Блокировать фрагментированный трафик
3: Настройки path MTU канала управления
4: Настройки path MTU канала VPN
5: Настройки MSS
0: Выход
Выберите пункт меню (0 – 5):
```

   Внимание! Пункт меню "Блокировать фрагментированный трафик" используется только применительно к криптографическому шлюзу.
3. Для настройки фрагментации или выхода из меню введите номер нужной команды и нажмите клавишу <Enter>.

Для просмотра текущего состояния настроек фрагментации:

1. В меню настроек фрагментации введите номер команды "Показать текущие настройки фрагментации" и нажмите клавишу <Enter>.

   На экране будут отображены значения текущих настроек фрагментации:

```
Поиск MTU для канала управления включен
Поиск MTU для VPN каналов включен
MSS пользовательского трафика не изменяется
```

   Примечание. "Поиск MTU для <название канала> включен"— флаг DF на IP-пакеты ставится; "Поиск MTU для <название канала> выключен" — флаг DF на IP-пакеты не ставится.
2. Для настройки фрагментации или выхода из меню введите номер нужной команды и нажмите клавишу <Enter>.

Для блокирования/разблокирования фрагментированного трафика:

- В меню настроек фрагментации введите номер команды "Блокировать/Разблокировать фрагментированный трафик" и нажмите клавишу <Enter>.

  Будет включен соответствующий режим и наименование команды в меню настроек будет изменено на противоположное.

Для включения/отключения принудительной установки флага DF:

1. В меню настроек фрагментации введите номер команды "Настройки path MTU..." для канала управления или VPN-каналов и нажмите клавишу <Enter>.

На экране появится меню с командами включения и отключения режима для выбранного канала.

```
1: Включить автоматический поиск MTU для VPN
2: Отключить автоматический поиск MTU для VPN
0: Выход
Выберите пункт меню (0 – 2):
```

2. Введите номер нужной команды и нажмите клавишу <Enter>.

   Будет выполнено включение/отключение режима принудительной установки флага DF.

Примечание. Для проверки результата выполнения команды используйте команду "Показать текущие настройки фрагментации".

3. Для возврата в меню настроек фрагментации введите номер команды "Выход" и нажмите клавишу <Enter>.

Для настройки MSS:

1. В меню настроек фрагментации введите номер команды "Настройки MSS" и нажмите клавишу <Enter>.

   На экране появится меню настройки MSS.

```
1: Показать значение TCP MSS
2: Установить значение TCP MSS
3: Не изменять MSS пользовательского трафика
0: Выход
Выберите пункт меню (0 – 3):
```

Команда	Описание
Показать значение TCP MSS	Вывод на экран текущего значения MSS. **Внимание!** После установки ПО и инициализации сетевого устройства по умолчанию установлено значение "MSS пользовательского трафика не изменяется"
Установить значение TCP MSS	Ввод вручную значения из диапазона 536–1408
Не изменять MSS пользовательского трафика	Значение MSS устанавливается автоматически
Выход	Возврат в меню настроек фрагментации

2. Введите номер нужной команды и нажмите клавишу <Enter>.

Настройка параметров шифратора

Для шифратора предусмотрены следующие настройки:

- Отключение и включение ускоренного режима шифрования.

  При запуске КШ автоматически включается ускоренный режим шифрования (не для всех платформ). Если КШ используется исключительно как межсетевой экран (функция шифрования трафика не используется), отключение ускоренного режима шифрования может привести к увеличению призводительности криптошлюза.

  Отключение ускоренного режима шифрования доступно только на тех платформах, для которых данный режим поддерживается.

- Включение и отключение режима шифрования трафика на основе адреса источника.

  Включение или отключение режима шифрования трафика к парному КШ зависит от того – принадлежит адрес источника к диапазону адресов глобальной сети Интернет ("белый" адрес) или входит в диапазон адресов, назначаемых для внутренних сетей ("серый" адрес). При включенном режиме, если адрес источника "белый", трафик, передаваемый в

защищаемую сеть парного КШ, шифроваться не будет. При отключенном режиме такой трафик будет шифроваться.

- Разрешение или запрет дефрагментации пакетов до фильтра.

  Дефрагментация пакетов в КШ и КК может выполняться на входе или на выходе фильтра. Для предупреждения перегрузки фильтра в случае длительного поступления на его вход фрагментированных пакетов рекомендуется установить режим, в котором дефрагментация пакетов будет выполняться до применения фильтра. Такой режим устанавливают командой "Разрешить дефрагментацию пакетов до фильтра".

  Для переключения в режим, в котором дефрагментация выполняется после фильтра, необходимо использовать команду "Запретить дефрагментацию пакетов до фильтра".

  По умолчанию установлен режим дефрагментации пакетов после фильтра.

- Разрешение или запрет распределения пакетов с учетом соединений.

  Данная настройка позволяет распределять пакеты между ядрами: пакеты с одинаковыми значениями MAC- адресов источника/получателя обрабатываются одними и теми же ядрами. Такой режим позволяет повысить производительность в тех случаях, когда трафик содержит большое количество пакетов с разными адресами источника/получателя.

  По умолчанию для КШ распределение пакетов разрешено, для КК – запрещено.

Для настройки шифратора:

1. Перейдите к меню управления КШ (см. стр.**23**).
2. Введите в строке ввода номер команды "Настроить параметры шифратора" и нажмите клавишу <Enter>.

   На экране появится меню:

```
1: Отключить/Включить ускоренный режим шифрования
2: Включить/Отключить режим шифрования трафика на
основе адреса источника
3: Разрешить/Запретить дефрагментацию пакетов до
пакетного фильтра
4: Запретить/Разрешить распределение пакетов с учетом
соединений
0: Выход
Выберите пункт меню (0 – 4):
```

   Примечание. Если на данной платформе ускоренный режим шифрования не поддерживается, появится сообщение об отсутствии параметров для настройки.

3. Введите номер нужной команды и нажмите клавишу <Enter>.

   Появится сообщение:

```
Установка параметров шифратора произведена. КШ будет
перезагружен.
```

   Дождитесь перезагрузки устройства.

Внимание! Если описанные выше настройки выполняются в кластере, они должны быть выполнены на каждом устройстве, входящем в его состав.

Настройка STUN

Данная настройка выполняется на КШ с ЦУС в том случае, когда необходимо установить парную связь между криптошлюзом (криптошлюзами), расположенным за Hide NAT или Symmetric NAT, и криптошлюзом, расположенным за обычным NAT и доступным для КШ с ЦУС без трансляции адресов. В этом случае для установления между ними парной связи необходимо на КШ с ЦУС задать правило замены адресов.

Правило записывается в следующем виде:

<ID>:<IP-адрес>

где

- ID – идентификационный номер КШ, расположенного за обычным NAT;
- IP-адрес – преобразованный после NAT IP-адрес КШ с данным идентификационным номером.

Если в сети имеется несколько КШ, доступных для КШ с ЦУС без трансляции адресов, правило задается для каждого из них. Совокупность правил составляет таблицу замены адресов.

Внимание! Не рекомендуется включать в состав таблицы криптошлюзы, работающие в режиме Multi-WAN. Работоспособность VPN-каналов таких КШ не гарантируется.

Для просмотра и настройки замены адресов:

1. Перейдите к меню управления сетевым устройством (см. стр.**23**).
2. Введите в строке ввода номер команды "Настройка замены адресов STUN" и нажмите клавишу <Enter>.

   Примечание. Команда доступна только на КШ с ЦУС.

   На экране появится меню.

```
1: Показать таблицу замены адресов
2: Изменить таблицу замены адресов
3: Очистить таблицу замены адресов
0: Выход
Выберите пункт меню (0 – 3):
```

Для просмотра таблицы:

1. Введите номер команды "Показать таблицу замены адресов" и нажмите клавишу <Enter>.

   На экране появится список заданных правил. Каждая строка списка соответствует правилу, заданному для КШ за обычным NAT.

   Примечание. Если правила не задавались, на экране появится соответствующее сообщение.

2. После просмотра правил введите номер нужной команды меню и нажмите клавишу <Enter>.

Для изменения таблицы:

1. Введите номер команды "Изменить таблицу замены адресов" и нажмите клавишу <Enter>.

   На экране появится список правил, разделенных пробелом. Если правила не задавались, на экране появится строка ввода.

2. Внесите необходимые изменения в правила или введите новые правила, разделяя их пробелом, и нажмите клавишу <Enter>.
3. Выйдите из меню и выполните загрузку устройства.

   Правила вступят в силу после загрузки устройства.

Для очистки таблицы:

1. Введите номер команды "Очистить таблицу замены адресов" и нажмите клавишу <Enter>.

   На экране появится сообщение об очистке таблицы.

2. Выйдите из меню и выполните загрузку устройства.

Настройки коммутации

Приведенные ниже настройки предназначены для запрета или разрешения прохождения через криптокоммутатор пакетов следующих протоколов:

- LACP;
- STP;
- 802.1X для Port-based access control;

- Pause-пакеты.

По умолчанию после ввода криптокоммутатора в эксплуатацию прохождение пакетов указанных протоколов запрещено.

Для просмотра текущих настроек коммутации:

1. Перейдите к меню управления сетевым устройством (см. стр.**23**).
2. Введите в строке ввода номер команды "Настройки коммутации" и нажмите клавишу <Enter>.

   На экране появится меню настроек коммутации.

```
1: Показать текущие настройки коммутации
2: Запретить прохождение LACP-пакетов
3: Запретить прохождение STP-пакетов
4; Запретить прохождение пакетов Port-Based access control
по 802.1x
5; Запретить прохождение Pause-пакетов для flow control
0: Выход
Выберите пункт меню (0 – 5):
```

3. Введите в строке ввода номер команды "Показать текущие настройки коммутации" и нажмите клавишу <Enter>.

   На экране отобразятся текущие настройки.

```
Прохождение пакетов LACP разрешено
Прохождение пакетов STP разрешено
Прохождение пакетов 802.1X разрешено
Прохождение Pause пакетов разрешено
```

Для разрешения/запрета прохождения пакетов:

- В меню настроек коммутации введите в строке ввода номер команды для нужного протокола и нажмите клавишу <Enter>.

  Содержание команды в меню изменится на противоположное ("запретить" на "разрешить" и — наоборот).

Настройки безопасности

Переход к меню "Настройки безопасности"

Для перехода к меню "Настройки безопасности":

1. Перейдите к режиму настройки сетевого устройства (см. стр.**22**).
2. В главном меню введите в строке ввода номер команды "Настройки безопасности" и нажмите клавишу <Enter>.

   На экране появится меню "Настройки безопасности".

```
1: Ограничения управления СД <функция недоступна>
2: Задать пароль локального администратора
3: Изменить внешний адрес
4: Криптографические операции
5: Включить привязку маршрутизаторов к MAC адресам
6: Ограничить число соединений с одного IP адреса
7: Настроить параметры локальной сигнализации НСД
8: Разрешить прохождение пакетов с IP опциями
9: Включить программный контроль целостности
0: Выход
Выберите пункт меню (0 – 9): 4
```

Внимание! Состав меню зависит от наличия установленных на КШ компонентов ПО ЦУС и СД.

3. Введите номер нужной команды и нажмите клавишу <Enter>.

   Описание процедур см. ниже.

4. Для возврата к главному меню введите в строке ввода номер команды "Выход" и нажмите клавишу <Enter>.

Регистрация нового администратора

Имеется возможность локальными средствами управления создать на ЦУС новую учетную запись администратора.

Внимание! При создании идентификатора администратора исходная ключевая информация от уполномоченной организации не используется. Рекомендуется этим способом создавать только временный ключ, который затем средствами ПУ ЦУС заменить на постоянный.

В качестве идентификатора администратора комплекса могут использоваться USB-флеш-накопители.

Приготовьте носитель заранее. При записи административного ключа ранее записанные на носитель ключи будут удалены без предупреждения.

После создания учетной записи локальными средствами управления в списке администраторов появится новая запись "Добавленный с консоли администратор" (см. [**1**]).

Для регистрации администратора:

1. Перейдите к меню настройки безопасности (см. стр.**35**).
2. Введите в строке ввода номер команды "Зарегистрировать нового администратора" и нажмите клавишу <Enter>. На экране появится сообщение:

   ```
   Введите пароль административного ключа
   ```

3. Введите пароль и нажмите клавишу <Enter>.

   Примечание. Длина и сложность пароля задаются политикой аутентификации администраторов (см. [**1**]). По умолчанию длина пароля не менее 4 символов. Разрешено использование любых символов, кроме кириллицы.

   Внимание! Запомните пароль. Этот пароль будет использован для шифрования административного ключа и в дальнейшем понадобится для запуска программы управления ЦУС.

   На экране появится сообщение:

   ```
   Повторите пароль
   ```

4. Введите пароль повторно и нажмите клавишу <Enter>.

   На экране появится сообщение:

   ```
   Вставьте носитель для записи административного ключа и
   нажмите Enter
   ```

5. Предъявите носитель и нажмите клавишу <Enter>.

   После успешной записи информации на экране появится текущее меню.

6. Перейдите к настройке следующего параметра или выйдите из меню.

Изменение пароля администратора

Пароль администратора предназначен для ограничения перехода к режиму настройки.

Внимание! При вводе пароля необходимо соблюдать следующие условия:

- длина пароля не менее 8 символов;
- пароль должен содержать буквы верхнего и нижнего регистров, цифры и специальные символы.

Для смены пароля:

1. Перейдите к меню настройки безопасности (см. стр.**35**).
2. Введите в строке ввода номер команды "Задать пароль локального администратора" и нажмите клавишу <Enter>. На экране появится сообщение:

```
Введите пароль локального администратора
```

3. Введите новый пароль и нажмите клавишу <Enter>.

   На экране появится текущее меню.
4. Перейдите к настройке следующего параметра или выйдите из меню.

Ограничение управления ЦУС и СД

Предусмотрено ограничение управления центром управления сетью и сервером доступа со стороны ПУ ЦУС и ПУ СД соответственно. Ограничение заключается в следующем: в настройках безопасности КШ с ЦУС или КШ с СД можно разрешить управление только через определенный внешний интерфейс (или интерфейсы) КШ или с определенного IP-адреса (или IP-адресов). Подключение к ЦУС или СД через другие внешние интерфейсы КШ или с других IP-адресов запрещено.

Если в разрешениях указаны интерфейс и IP-адрес, подключение доступно через указанный интерфейс с любого IP-адреса или с указанного IP-адреса через любой интерфейс.

Если на КШ установлены ЦУС и СД, ограничение действует и для ЦУС, и для СД.

Для включения режима ограничения управления с интерфейса:

1. Перейдите к меню настройки безопасности (см. стр.**35**).
2. Введите в строке ввода номер команды "Ограничения управления" (для КШ с ЦУС/КШ с ЦУС и СД) или "Ограничения управления СД" (для КШ с СД) и нажмите клавишу <Enter>.

   На экране появится меню:

```
1: Вывести список разрешений управления
2: Добавить разрешения управления
3: Очистить список разрешений управления
0: Выход
Выберите пункт меню (0-3):
```

3. Введите в строке ввода номер команды "Добавить разрешения управления" и нажмите клавишу <Enter>.

   На экране появится меню:

```
1: Добавить разрешение управления с интерфейса
2: Добавить разрешение управления с IP-адреса
0: Выход
Выберите пункт меню (0-2):
```

4. Введите в строке ввода номер команды "Добавить разрешение управления с интерфейса" и нажмите клавишу <Enter>.

   На экране появится сообщение:

```
Доступные интерфейсы: <перечень интерфейсов>
Введите название интерфейса, с которого будет разрешено
управление:
```

5. Введите наименование нужного интерфейса из предложенного перечня и нажмите клавишу <Enter>.

   На экране появится сообщение:

```
Управление разрешено с интерфейса <наименование
интерфейса>
```

   Затем на экране появится текущее меню.
6. Перейдите к настройке следующего параметра или выйдите из меню.

Для включения режима ограничения управления с IP-адреса:

1. Перейдите к меню настройки безопасности (см. стр.**35**).
2. Введите в строке ввода номер команды "Ограничение управления" (для КШ с ЦУС/КШ с ЦУС и СД) или "Ограничение управления СД" (для КШ с СД) и нажмите клавишу <Enter>.

   На экране появится меню:

   ```
   1: Вывести список разрешений управления
   2: Добавить разрешения управления
   3: Очистить список разрешений управления
   0: Выход
   Выберите пункт меню (0-3):
   ```

3. Введите в строке ввода номер команды "Добавить разрешения управления" и нажмите клавишу <Enter>.

   На экране появится меню:

   ```
   1: Добавить разрешение управления с интерфейса
   2: Добавить разрешение управления с IP-адреса
   0: Выход
   Выберите пункт меню (0-2):
   ```

4. Введите в строке ввода номер команды "Добавить разрешение управления с IP-адреса" и нажмите клавишу <Enter>.

   На экране появится сообщение:

   ```
   Введите IP-адрес, с которого будет разрешено управление>
   ```

5. Введите IP-адрес или адрес подсети и нажмите клавишу <Enter>.

   На экране появится сообщение:

   ```
   Управление разрешено с адреса <адрес>
   ```

   Затем на экране появится текущее меню.

6. Перейдите к настройке следующего параметра или выйдите из меню.

Для просмотра списка разрешений:

1. Перейдите к меню настройки безопасности (см. стр.**35**).
2. Введите в строке ввода номер команды "Ограничение управления " (для КШ с ЦУС) или "Ограничение управления СД" (для КШ с СД) и нажмите клавишу <Enter>.

   На экране появится меню.

3. Введите в строке ввода номер команды "Вывести список разрешений управления" и нажмите клавишу <Enter>.

   На экране появится список с разрешенными источниками управления.

4. После просмотра списка введите в строке ввода номер нужной команды.

Для отключения режима ограничения:

1. Перейдите к меню настройки безопасности (см. стр.**35**).
2. Введите в строке ввода номер команды "Ограничение управления ЦУС" (для КШ с ЦУС) или "Ограничение управления СД" (для КШ с СД) и нажмите клавишу <Enter>.

   На экране появится меню:

   ```
   1: Вывести список разрешений управления
   2: Добавить разрешения управления
   3: Очистить список разрешений управления
   0: Выход
   Выберите пункт меню (0-3):
   ```

3. Введите в строке ввода номер команды "Очистить список разрешений управления" и нажмите клавишу <Enter>.

   На экране появится текущее меню.

4. Перейдите к настройке следующего параметра или выйдите из меню.

Обновление исходной ключевой информации

Данная процедура предоставляет возможность, используя локальную консоль, обновить исходную ключевую информацию на ЦУС в случае ее плановой замены или компрометации.

Исходная ключевая информация может считываться с носителей следующих типов:

- USB-флеш-накопитель;
- CD-ROM (ключевой блокнот РДП-006);
- ДСЧ платы "Соболь".

Для выполнения процедуры необходимо заранее получить отчуждаемый носитель с новой исходной ключевой информацией.

Для обновления ключевой информации:

1. Перейдите на КШ с ЦУС или на КШ с ЦУС и СД к меню настройки безопасности (см. стр.**35**).
2. Введите в строке ввода номер команды "Обновить исходную ключевую информацию" и нажмите клавишу <Enter>.

   На экране появится запрос:

   ```
   Использовать внешний носитель для инициализации? (Y/N)
   ```

3. Если требуется использовать ДСЧ платы "Соболь", введите "N" и нажмите клавишу <Enter>.

   Начнется обновление ключевой информации и после его завершения появится соответствующее сообщение (см. п. **4**). Перейдите к п. **5**.

   Если требуется использовать внешний носитель, введите "Y" и нажмите клавишу <Enter>.

   На экране появится сообщение:

   ```
   Вставьте носитель с исходной ключевой информацией и
   нажмите Enter
   ```

4. Предъявите носитель с исходной ключевой информацией и нажмите клавишу <Enter>.

   Пояснение. Файл, содержащий новый исходный ключевой материал, копируется на USB-флеш-накопитель до начала процедуры обновления. Если это условие не выполнено, продолжение процедуры обновления невозможно. Извлеките носитель из считывателя, скопируйте на него новый исходный ключевой материал, вставьте носитель в считыватель и повторно нажмите клавишу <Enter>. Если чтение информации не выполняется, повторите процедуру обновления ключевой информации заново.

   Если носитель не предъявлен, на нем отсутствуют нужные файлы или файлы повреждены, на экране появится сообщение об ошибке.

   После успешного считывания информации на экране появится сообщение:

   ```
   Ключевая информация обновлена
   ```

   Затем на экране появится текущее меню.

5. Перейдите к настройке другого параметра или выйдите из меню.

Загрузка ключей

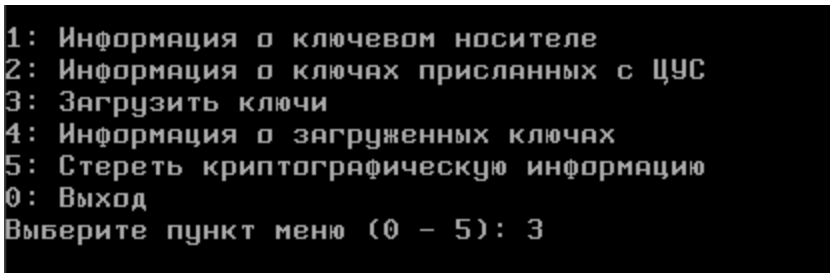
Данную процедуру выполняют для загрузки активного или резервного ключа. Ключ представляет собой пару: главный ключ КШ – ключ связи с ЦУС.

Процедура загрузки ключа выполняется индивидуально для каждого сетевого устройства независимо от используемой схемы распределения ключей (базовой или трехлетней).

Для загрузки ключа на сетевое устройство:

1. Перейдите к меню настройки безопасности (см. стр.**35**).
2. Введите в строке ввода номер команды "Криптографические операции" и нажмите клавишу <Enter>.

   На экране появится меню "Криптографические операции".



3. Введите в строке ввода номер команды "Загрузить ключи" и нажмите клавишу <Enter>.

   На экране появится меню.
4. Введите номер варианта (загрузка активного или резервного ключа) и нажмите клавишу <Enter>.

   На экране появится сообщение:

   Уже имеется активный ключ, установленный на сетевом устройстве. Заменить? (Y/N):
5. Введите Y и нажмите клавишу <Enter>.

   На экране появится сообщение:

   Вставьте носитель с ключами и нажмите Enter.
6. Предъявите носитель с ключами и нажмите клавишу <Enter>.

   В зависимости от предъявленного носителя появится запрос на ввод PIN-кода пользователя (для ТОКЕН_КШ) или пароля (для USB-флеш-накопителя).
7. Введите PIN-код пользователя или пароль, заданный при сохранении ключа на USB-флеш-накопитель, и нажмите клавишу <Enter>.

   Если носитель не предъявлен, на нем отсутствуют нужные файлы или файлы повреждены, на экране появится сообщение об ошибке.

   При успешном чтении информации с носителя на экране появится сообщение об обнаруженном комплекте ключей.
8. Введите 1 и нажмите клавишу <Enter>.
   - Если носителем является USB-флеш-накопитель, начнется загрузка ключа.
   - Если носителем является ТОКЕН_КШ, появится список ключей, входящих в комплект.

     Введите номер пункта, соответствующего загружаемому ключу, и нажмите клавишу <Enter>.

     Начнется загрузка ключа.

   После успешной загрузки появится одно из двух сообщений:

   Ключ установлен как активный

   или

   Ключ установлен как резервный

   На экране появится меню "Настройки безопасности".

Примечание. Загрузка резервных ключей используется только в трехлетней схеме хранения ключей. В случае перехода на резервные ключи при базовой схеме следует устанавливать резервный ключ как активный.

Смена ключей на КШ с ЦУС

Данная процедура позволяет выполнить на КШ с ЦУС смену главного ключа и ключа связи с ЦУС.
Внимание! После смены ключей на КШ с ЦУС необходимо заново сформировать список связанных КШ. Список формируется средствами централизованного управления в ПУ ЦУС (см. [**1**]).

Для смены ключей на КШ с ЦУС:

1. Перейдите к меню настройки безопасности (см. стр.**35**).
2. Введите в строке ввода номер команды "Сменить ключи КШ" и нажмите клавишу <Enter>.

   Будет выполнена смена ключей, и на экране появится сообщение об успешно выполненной операции.
3. Перейдите к настройке другого параметра или выйдите из меню настройки безопасности.

Просмотр информации о загруженных ключах

Для сетевого устройства предусмотрен просмотр сведений о загруженных ключах – основном и резервном. Сведения о каждом из них включают в себя следующую информацию:

- состояние ключа – загружен или не загружен;
- название и серийный номер ключевого носителя, с которого ключ был загружен;
- номер комплекта ключа;
- номер ключа в составе комплекта;
- дата и время истечения срока действия ключа.

Для просмотра информации о загруженных ключах сетевого устройства:

1. Перейдите к меню настройки безопасности (см. стр.**35**).
2. Введите в строке ввода номер команды "Криптографические операции" и нажмите клавишу <Enter>.

   На экране появится меню "Криптографические операции".
3. Введите в строке ввода номер команды "Информация о загруженных ключах " и нажмите клавишу <Enter>.

   На экране появится информация о загруженных ключах.

   Примечание. Если ключ не загружен, информация о нем не приводится.

Удаление криптографической информации

Для сетевого устройства имеется возможность экстренного удаления ключевой информации и файлов конфигурации. Содержимое удаленных файлов конфигурации автоматически затирается на жестком диске сетевого устройства. После удаления требуется повторная инициализация сетевого устройства.

Для удаления криптографической информации:

1. Перейдите к меню настройки безопасности (см. стр.**35**).
2. Введите в строке ввода номер команды "Криптографические операции" и нажмите клавишу <Enter>.

   На экране появится меню "Криптографические операции".
3. Введите в строке ввода номер команды "Стереть криптографическую информацию" и нажмите клавишу <Enter>.

   На экране появится сообщение, содержание которого зависит от установленного или не установленного на сетевом устройстве ПО ЦУС.

```
Наберите yes, если вы хотите удалить криптографическую
информацию
ВНИМАНИЕ! После этой операции понадобится повторная
<загрузка конфигурации>/<инициализация ЦУС>!
Продолжить? (Y/N):
```

4. Наберите yes и нажмите клавишу <Enter>.
   - Для сетевого устройства на экране появится сообщение:

     ```
     Вставьте носитель с конфигурацией и нажмите Enter
     ```

     Перейдите к выполнению п.5 процедуры инициализации сетевого устройства (см. стр.**16**).
   - Для КШ с ЦУС перейдите к выполнению п.6 процедуры инициализации КШ с ЦУС (см. стр.**12**).

Примечание. Если требуется отложить инициализацию, выключите компьютер.

Ограничение числа соединений

Данная процедура предоставляет возможность ограничить число соединений с одного IP-адреса.

Ограничение числа соединений выполняется для тех правил фильтрации, у которых отмечен параметр "Контролировать состояние соединения" (см. [**1**]).

Для ограничения числа соединений:

1. Перейдите к меню настройки безопасности (см. стр.**35**).
2. Введите в строке ввода номер команды "Ограничить число соединений с одного IP-адреса" и нажмите клавишу <Enter>.

   На экране появится сообщение:

   ```
   Максимальное количество соединений (0 — без ограничений)
   ```
3. Введите нужное число и нажмите клавишу <Enter>.

   Примечание. Для открытого трафика учет соединений ведется как по внутреннему, так и по внешнему интерфейсу. В этом случае реальное максимальное количество соединений будет ограничено половиной введенного числа (с округлением в меньшую сторону). Для получения нужного результата введите удвоенное число.

   На экране появится текущее меню.
4. Перейдите к настройке следующего параметра или выйдите из меню.

Очистка журналов ЦУС

Данная процедура позволяет очистить журналы ЦУС и выполняется на ЦУС.

Внимание! Журналы, которые не были переданы агенту ЦУС, будут утрачены.

Для очистки журналов ЦУС:

1. Перейдите к меню настройки безопасности (см. стр.**35**).
2. Введите в строке ввода номер команды "Очистка журналов ЦУС" и нажмите клавишу <Enter>.

   На экране появится запрос:

   ```
   Продолжить? (Y/N)
   ```
3. Введите "Y" и нажмите клавишу <Enter>.

   На экране появится сообщение:

   ```
   Журналы очищены
   ```

   Затем на экране появится текущее меню.
4. Перейдите к настройке следующего параметра или выйдите из меню.

Настройка параметров локальной сигнализации о НСД

Предусмотрено включение и отключение вывода сообщений о НСД. Сообщения могут выводиться на экран монитора, подключенного к сетевому устройству, и воспроизводиться в виде звукового сигнала.

Для настройки параметров сигнализации:

1. Перейдите к меню настройки безопасности (см. стр.**35**).
2. Введите в строке ввода номер команды "Настроить параметры локальной сигнализации НСД" и нажмите клавишу <Enter>.

   Если сигнализация отключена, на экране появится меню:

   ```
   1. Включить вывод на консоль сообщений о НСД (не чаще раза в минуту)
   2. Включить вывод звуковых сообщений о НСД (не чаще раза в минуту)
   0. Выход
   Выберите пункт меню (0-2):
   ```

   Если сигнализация включена, соответствующая команда в меню будет иметь вид "Выключить…".
3. Выберите команду, введите в строке ввода ее номер и нажмите клавишу <Enter>.

   Содержание выбранной команды в меню изменится на противоположное.
4. При необходимости повторите предыдущее действие для другой команды.
5. Для завершения настройки выйдите из меню.

Режим прохождения пакетов с IP-опциями

Некоторые среды (например ОС МСВС) используют поле IP-опций в заголовке IP-пакета в обязательном порядке. Для функционирования комплекса в таких средах предусмотрен режим прохождения пакетов с IP-опциями. По умолчанию этот режим выключен.

Для включения режима:

1. Перейдите к меню настройки безопасности (см. стр.**35**).
2. Введите в строке ввода номер команды "Разрешить прохождение пакетов с IP-опциями" и нажмите клавишу <Enter>.

   На экране появится сообщение:

   ```
   Прохождение пакетов с IP опциями разрешено
   ```

   Затем на экране появится текущее меню.
3. Перейдите к настройке следующего параметра или выйдите из меню.

Для выключения режима:

1. Перейдите к меню настройки безопасности (см. стр.**35**).
2. Введите в строке ввода номер команды "Запретить прохождение пакетов с IP-опциями" и нажмите клавишу <Enter>.

   На экране появится сообщение:

   ```
   Прохождение пакетов с IP опциями запрещено
   ```

   Затем на экране появится текущее меню.
3. Перейдите к настройке следующего параметра или выйдите из меню.

Привязка аппаратных адресов маршрутизаторов

Данная функция позволяет запретить на сетевом устройстве действие протокола ARP и осуществлять маршрутизацию по жестко зафиксированным аппаратным

(MAC) адресам маршрутизаторов. Такой подход обеспечивает защиту от сетевых атак типа ARP-spoofing.

При использовании этой функции в случае замены маршрутизатора (или только его сетевой карты) необходимо выполнить принудительное обновление зафиксированных в конфигурации сетевого устройства аппаратных адресов маршрутизатора.

Примечание. После включения привязки команда меню "Настроить динамическую маршрутизацию" становится недоступной.

Фиксация аппаратных адресов маршрутизаторов

Для фиксации аппаратных адресов маршрутизаторов:

1. Перейдите к меню настройки безопасности (см. стр.**35**).
2. Введите в строке ввода номер команды "Включить привязку маршрутизаторов к MAC-адресам" и нажмите клавишу <Enter>.

   На экране появится сообщение:

   ```
   Маршрутизатор: <IP-адрес маршрутизатора по умолчанию> MAC:
   не установлен (определится динамически)
   MAC-адрес привязки маршрутизатора будет определен
   автоматически. Хотите ввести его вручную? (Y/N)
   ```

3. Введите в строке ввода "y" и нажмите клавишу <Enter>.

   Примечание. Если выбрать "no", MAC-адрес маршрутизатора будет определен автоматически.

   На экране появится сообщение:

   ```
   Введите MAC-адрес:
   ```

4. Введите MAC-адрес в формате 00:00:00:00:00:00 и нажмите клавишу <Enter>.

   Примечание. При использовании нескольких маршрутизаторов повторите выполнение пп. 2–4 для каждого маршрутизатора.

   На экране появится сообщение:

   ```
   ARP кэш сохранен
   ```

   Затем на экране появится текущее меню. Команда меню "Включить привязку маршрутизаторов к MAC-адресам" будет заменена на команду "Отключить привязку маршрутизаторов или обновить их адреса".
5. Перейдите к настройке следующего параметра или выйдите из меню.

Обновление аппаратных адресов маршрутизаторов

Для обновления аппаратных адресов маршрутизаторов:

1. Перейдите к меню настройки безопасности (см. стр.**35**).
2. Введите в строке ввода номер команды "Отключить привязку маршрутизаторов или обновить их адреса" и нажмите клавишу <Enter>.

   На экране появится меню:

   ```
   1. Обновить MAC адреса маршрутизаторов
   2. Отключить привязку MAC адресов маршрутизаторов
   0. Выход
   Выберите пункт меню (0-2):
   ```

3. Введите в строке ввода номер команды "Обновить MAC- адреса маршрутизаторов" и нажмите клавишу <Enter>.

   На экране появится сообщение:

   ```
   Маршрутизатор: <IP-адрес маршрутизатора по умолчанию> MAC:
   <MAC-адрес>
   MAC-адрес привязки маршрутизатора будет определен
   автоматически. Хотите ввести его вручную? (Y/N)
   ```

4. Введите в строке ввода "y" и нажмите клавишу <Enter>.

   На экране появится сообщение:

   ```
   Введите MAC-адрес:
   ```

5. Введите MAC-адрес в формате 00:00:00:00:00:00 и нажмите клавишу <Enter>.

   На экране появится сообщение:

   ```
   ARP кэш сохранен
   ```

   Затем на экране появится текущее меню.

6. Перейдите к настройке следующего параметра или выйдите из меню.

Отключение фиксации аппаратных адресов маршрутизаторов

Для отключения фиксации аппаратных адресов маршрутизаторов:

1. Перейдите к меню настройки безопасности (см. стр.**35**).
2. Введите в строке ввода номер команды "Отключить привязку маршрутизаторов или обновить их адреса" и нажмите клавишу <Enter>.

   На экране появится меню:

   ```
   1. Обновить MAC адреса маршрутизаторов
   2. Отключить привязку MAC адресов маршрутизаторов
   0. Выход
   Выберите пункт меню (0-2):
   ```

3. Введите в строке ввода номер команды "Отключить привязку MAC-адресов" и нажмите клавишу <Enter>.

   На экране появится сообщение:

   ```
   Привязка отключена
   ```

   Затем на экране появится текущее меню. Команда меню "Отключить привязку маршрутизаторов или обновить их адреса" будет заменена на команду "Включить привязку маршрутизаторов к MAC-адресам".

4. Перейдите к настройке следующего параметра или выйдите из меню.

Управление режимом контроля целостности

Режим контроля целостности служит для проверки контрольных сумм файлов ПО сетевого устройства. Проверка контрольных сумм автоматически выполняется при запуске сетевого устройства, а также во время его работы с периодичностью, указанной в программе управления сетью.

Для включения/ выключения режима:

1. Перейдите к меню настройки безопасности (см. стр.**35**).
2. Введите в строке ввода номер команды "Включить/ выключить программный контроль целостности" и нажмите клавишу <Enter>.

   На экране появится текущее меню.

3. Перейдите к настройке следующего параметра или выйдите из меню.

Настройка сервера доступа

Переход к меню "Настройка СД"

Для перехода к меню "Настройка СД":

1. Перейдите к режиму настройки КШ (см. стр.**22**).
2. В главном меню введите в строке ввода номер команды "Настройка СД" и нажмите клавишу <Enter>.

   На экране появится сообщение:

```
Внимание! В случае использования кластера резервирования
необходимо, чтобы резервный КШ был выключен. Для
продолжения нажмите Enter.
```

Примечание. Для ЦУС и СД такое сообщение не выводится. Перейдите к выполнению п. 4.

3. В случае использования кластера резервирования отключите резервный КШ и нажмите клавишу <Enter>.

   На экране появится меню "Настройка СД".

4. Введите номер нужной команды и нажмите клавишу <Enter>.

   Описание процедур см. ниже.

5. Для возврата к главному меню введите в строке ввода номер команды "Вернуться в основное меню" и нажмите клавишу <Enter>.

Повторная инициализация сервера доступа

Повторная инициализация сервера доступа приводит к созданию новой базы данных. Содержимое базы данных может быть восстановлено из резервной копии, поэтому рекомендуется перед инициализацией сервера выполнить резервное копирование его базы данных (см. [**5**]).

После повторной инициализации сервера доступа необходимо заново зарегистрировать лицензии на использование сервера.

Для повторной инициализации сервера:

1. Перейдите к меню конфигурирования сервера доступа (см. стр.**45**).
2. При появлении на экране меню конфигурирования сервера введите в строке ввода номер команды "Переинициализировать СД" и нажмите клавишу <Enter>. На экране появится сообщение:

   ```
   Вы уверены в том, что хотите переинициализировать СД
   (Y/N)?
   ```

3. Введите "y" и нажмите клавишу <Enter>.

   После успешного выполнения операции на экране появится сообщение:

   ```
   Начальная конфигурация СД.
   ```

   Затем на экране вновь появится меню конфигурирования сервера доступа.

Создание идентификатора администратора

Внимание! После создания нового идентификатора администратора старый идентификатор уже не может использоваться для установки соединения программы управления с сервером доступа.

Для создания идентификатора:

1. Перейдите к меню конфигурирования сервера доступа (см. стр.**45**).
2. При появлении на экране меню конфигурирования сервера введите в строке ввода номер команды "Создать ключевой носитель" и нажмите клавишу <Enter>.

   На экране появится сообщение:

   ```
   Вы уверены в том, что хотите создать ключевой носитель для
   ПУ СД (Y/N)?
   ```

3. Введите "y" и нажмите клавишу <Enter>.

   На экране появится сообщение:

   ```
   Введите пароль
   ```

4. Введите пароль и нажмите клавишу <Enter>.

   Примечание. Длина пароля администратора СД не менее 8 символов. Разрешено использование любых символов, кроме кириллицы.

Внимание! Запомните пароль. Этот пароль будет использован для шифрования административного ключа и в дальнейшем понадобится для запуска программы управления сервером доступа.

На экране появится сообщение:

```
Повторите пароль
```

5. Введите пароль повторно и нажмите клавишу <Enter>.

   На экране появится сообщение:

   ```
   Вставьте носитель для записи ключа ПУ СД и нажмите Enter.
   ```

6. Предъявите носитель для записи ключа и нажмите клавишу <Enter>.

   Если носитель не предъявлен, на экране появится сообщение об ошибке, а затем — меню конфигурирования сервера. Повторите создание идентификатора еще раз.

   При успешной записи ключевой информации на носитель на экране вновь появится меню конфигурирования сервера доступа.

Управление лицензиями

Добавление лицензий на использование сервера доступа

При выполнении этой операции добавляются только новые лицензии, т. е. те, которые еще не зарегистрированы на сервере.

Для добавления лицензии:

1. Перейдите к меню конфигурирования сервера доступа (см. стр.**45**).
2. При появлении на экране меню конфигурирования сервера доступа введите в строке ввода номер команды "Изменить лицензии" и нажмите клавишу <Enter>.

   На экране появится меню для работы с лицензиями:

   ```
   Работа с лицензиями
   1. Показать лицензии
   2. Удалить лицензию
   3. Добавить лицензию
   0. Вернуться в основное меню конфигурации СД
   Выберите пункт меню:
   ```

3. Введите в строке ввода номер команды "Добавить лицензию" и нажмите клавишу <Enter>.

   На экране появится сообщение:

   ```
   Введите серийный номер лицензии и нажмите Enter.
   ```

4. Введите серийный номер лицензии и нажмите клавишу <Enter>.

   Если введен неверный серийный номер или номер уже зарегистрированной лицензии, на экране появится сообщение об ошибке. Нажмите клавишу <Enter> и повторите регистрацию лицензии еще раз.

   При успешной регистрации лицензии в базе данных сервера доступа на экране появится сообщение:

   ```
   Лицензия успешно добавлена.
   ```

5. Нажмите клавишу <Enter>.

   На экране вновь появится меню для работы с лицензиями.

6. Для завершения работы с лицензиями введите в строке ввода номер команды "Вернуться в основное меню" и нажмите клавишу <Enter>.

   На экране появится меню конфигурирования сервера доступа.

Примечание. Сведения о лицензиях, зарегистрированных в базе данных сервера доступа, можно получить в программе управления сервером доступа (см. [**5**]).

Удаление лицензий на использование сервера доступа

Для удаления лицензии:

1. Перейдите к меню конфигурирования сервера доступа (см. стр.**45**).
2. При появлении на экране меню конфигурирования сервера доступа введите в строке ввода номер команды "Изменить лицензии" и нажмите клавишу <Enter>.

   На экране появится меню для работы с лицензиями:

   ```
   Работа с лицензиями
   1. Показать лицензии
   2. Удалить лицензию
   3. Добавить лицензию
   0. Вернуться в основное меню конфигурации СД
   Выберите пункт меню:
   ```

3. Введите в строке ввода номер команды "Показать лицензии" и нажмите клавишу <Enter>.

   На экране появятся сведения о зарегистрированных лицензиях на использование сервера доступа. Для каждой лицензии указывается ее порядковый номер, серийный номер, количество клиентов.

4. Запомните порядковый номер лицензии, которую следует удалить, и нажмите клавишу <Enter>.

   На экране вновь появится меню для работы с лицензиями.

5. Введите в строке ввода номер команды "Удалить лицензию" и нажмите клавишу <Enter>.

   На экране появится сообщение:

   ```
   Введите порядковый номер удаляемой лицензии и нажмите
   Enter.
   ```

6. Введите порядковый номер лицензии и нажмите клавишу <Enter>.

   На экране появятся сведения об удаляемой лицензии — ее порядковый номер, серийный номер, количество клиентов, а также следующий запрос:

   ```
   Удалить эту лицензию (Y/N)?
   ```

7. Введите "y" и нажмите клавишу <Enter>.

   При успешном выполнении операции на экране появится сообщение:

   ```
   Лицензия удалена.
   Для возврата в меню работы с лицензиями нажмите Enter.
   ```

8. Нажмите клавишу <Enter>.

   На экране вновь появится меню для работы с лицензиями.

   Примечание. После удаления лицензии порядковые номера оставшихся лицензий изменяются, поэтому при следующем удалении лицензии необходимо опять вывести список лицензий, т. е. выполнить шаги 3–8.

9. Для завершения работы с лицензиями введите в строке ввода номер команды "Вернуться в основное меню" и нажмите клавишу <Enter>.

   На экране появится меню конфигурирования сервера доступа.

Просмотр списка лицензий на использование сервера доступа

Для просмотра списка лицензий:

1. Перейдите к меню конфигурирования сервера доступа (см. стр.**45**).
2. При появлении на экране меню конфигурирования сервера введите в строке ввода номер команды "Изменить лицензии" и нажмите клавишу <Enter>.

   На экране появится меню для работы с лицензиями:

```
Работа с лицензиями
1. Показать лицензии
2. Удалить лицензию
3. Добавить лицензию
0. Вернуться в основное меню конфигурации СД
Выберите пункт меню:
```

3. Введите в строке ввода номер команды "Показать лицензии" и нажмите клавишу <Enter>.

   На экране появятся сведения о зарегистрированных лицензиях на использование сервера доступа. Для каждой лицензии указывается ее порядковый номер, серийный номер, количество клиентов.

4. Нажмите клавишу <Enter>.

   На экране вновь появится меню для работы с лицензиями.

5. Для завершения работы с лицензиями введите в строке ввода номер команды "Вернуться в основное меню" и нажмите клавишу <Enter>.

   На экране появится меню конфигурирования сервера доступа.

Восстановление базы данных

При нарушении работы базы данных имеется возможность восстановить данные, которые не были утрачены.

При восстановлении файлов базы данных автоматически выполняются следующие операции:

- восстановление структуры базы данных;
- удаление неиспользуемых областей базы данных.

Для восстановления базы данных:

1. Перейдите к меню конфигурирования сервера доступа (см. стр.**45**).
2. При появлении на экране меню конфигурирования сервера доступа введите в строке ввода номер команды "Восстановить БД СД" и нажмите клавишу <Enter>.

   На экране появится сообщение:

   ```
   Вы уверены в том, что хотите восстановить БД (Y/N)?
   ```

3. Введите "y" и нажмите клавишу <Enter>.

   В процессе восстановления файлов базы данных на экране появляются сообщения о ходе и результате процесса.

   После успешного завершения процесса восстановления на экране вновь появится меню конфигурирования сервера доступа.

Дополнительные возможности

Команды дополнительного меню

Внимание! Для использования дополнительного меню к системному блоку сетевого устройства заранее должны быть подключены клавиатура и монитор.

Для перехода к дополнительному меню:

1. У работающего сетевого устройства нажмите комбинацию клавиш <ALT+F2>.

   На экране появится запрос на предъявление персонального идентификатора администратора.

2. Предъявите персональный идентификатор и при необходимости введите пароль.

   Количество неудачных попыток предъявления персонального идентификатора и время блокировки задаются политикой аутентификации администраторов (см. [**1**]).

   На экране появится дополнительное меню (см. Табл.2).

3. Введите номер команды и нажмите клавишу <Enter>.

   Выполняйте указания, отображаемые на экране.

4. Для выхода из дополнительного меню нажмите комбинацию клавиш <ALT+F1>.

Табл.2 Команды дополнительного меню

Команда	Описание
Сведения об устройстве	Отображает на экране сведения о версии и конфигурации ПО. Если устройство входит в состав кластера, отображается статус – основной/резервный
Информация о загруженных ключах	Отображает на экране сведения о загруженных ключах (основном и резервном): • наименование и серийный номер носителя, с которого ключ был загружен; • номер комплекта; • номер ключа; • дата истечения срока хранения ключа
Вывести список авторизованных пользователей	Отображает на экране список авторизованных пользователей. Список содержит IP-адреса авторизованных пользователей и время их подключения
Список правил фильтрации	Отображает на экране список всех правил фильтрации
Список правил NAT	Отображает на экране список всех правил NAT
Вывести полный список интерфейсов	Отображает на экране список всех интерфейсов
Вывести таблицы маршрутизации	Отображает на экране таблицу маршрутизации
Просмотр таблицы состояний (keep-state)	Отображает на экране количество установленных соединений с возможностью раздельного просмотра сессий IPv4 и IPv6. При просмотре сессий могут быть использованы фильтр и функция поиска
Диагностика	Выводит на экран меню команд диагностики
Перезагрузить	Запускает перезагрузку сетевого устройства

Команда	Описание
Выключить	Выключает электропитание сетевого устройства
Выход	Закрывает дополнительное меню

Табл.3 Команды меню "Диагностика"

Команда	Описание
Загруженность ЦП	Отображает на экране информацию о загруженности каждого процессора
Использование памяти	Отображает на экране общий и свободный объем оперативной памяти
Использование жесткого диска	Отображает на экране общий объем жесткого диска, а также объем используемого и свободного пространства
Выполнить ping*	Запускает на компьютере команду ping и отображает на экране результаты выполнения этой команды. Укажите IP-адрес, соединение с которым необходимо проверить
Выполнить traceroute*	Запускает на компьютере команду traceroute и отображает на экране результаты выполнения этой команды. Укажите IP-адрес, маршрут к которому требуется определить. Данная функция не работает при значении параметра "Степень сжатия заголовков", равном 2 (см. [**1**])
Выполнить arp/ndp	Отображает на экране содержимое ARP- и NDP-кеша
Сведения о сетевых соединениях	Отображает на экране сведения об открытых сетевых соединениях
Количество пропущенных пакетов	Функция недоступна
Сведения о работе шифратора	Статистическая информация о работе шифратора
Просмотр дампа сетевого трафика	Отображает на экране информацию о сетевом трафике выбранного интерфейса с возможностью применения фильтра в формате tcpdump. Для сетевого устройства, выведенного из эксплуатации, предусмотрено сохранение информации в двоичном коде для последующего просмотра специализированным приложением
Сведения о состоянии журналов	Отображает на экране максимальные и текущие объемы журналов
Сохранить конфигурацию и журналы событий динамической маршрутизации**	Записывает конфигурационные файлы на отчуждаемый носитель
Сохранить технологическую информацию	Выгружает на отчуждаемый носитель технологический отчет для отправки в службу поддержки
Выход	Закрывает меню "Диагностика"

- *Для выполнения команд ping и traceroute на КШ автоматически создаются временные правила фильтрации, разрешающие прохождение соответствующих пакетов.
- **Для сохранения журналов событий в конфигурационном файле для используемых протоколов маршрутизации должна быть включена функция логирования (Log stdout) и указан путь к файлу журнала. Например, для протокола BGP: log file /var/bgpd.log.

Корректное выключение питания сетевого устройства

В АПКШ "Континент" предусмотрено корректное выключение сетевого устройства в автоматическом режиме при работе с источниками бесперебойного питания (ИБП) в случае отключения питания и оставшегося заряда батареи менее 30 %. Поддерживаются модели ИБП APC Smart-UPS 1000 и APS BackUPS ES 525.

Для использования функции корректного выключения:

1. Подсоедините управляющий порт ИБП к USB-разъему сетевого устройства с помощью интерфейсного кабеля, входящего в комплект ИБП.

   Примечание. Подключение управляющего порта ИБП к USB-разъему необходимо выполнять при выключенном сетевом устройстве.

2. Выполните необходимые настройки в соответствии с эксплуатационной документацией фирмы – изготовителя ИБП.

Подключение к сетевому устройству через последовательный порт

Для удобства проведения настроек вместо клавиатуры и монитора к сетевому устройству можно подключить ноутбук.

Подключение выполняют с помощью кабеля RJ-45-DB-9. При этом на ноутбуке должна быть установлена программа эмуляции терминала, например — свободно распространяемый клиент PuTTY.

Внимание! По умолчанию в настройках BIOS сетевого устройства последовательный порт отключен. Для подключения к сетевому устройству необходимо предварительно в настройках BIOS включить поддержку последовательного порта. Для этого войдите в настройки BIOS сетевого устройства и на вкладке Advanced у параметра Console Redirection установите значение Enabled (о входе в меню BIOS см стр.**8**).

Для подключения к сетевому устройству:

1. Вставьте один конец кабеля в 9-контактный разъем последовательного порта на ноутбуке, другой конец кабеля вставьте в разъем последовательного порта RJ-45, расположенный на фронтальной панели сетевого устройства.
2. На ноутбуке запустите программу эмуляции терминала и в ее настройках укажите следующие значения параметров:

Параметр	Значение
Порт	Укажите значение, определяемое автоматически в диспетчере устройств ноутбука
Скорость	115200
Тип подключения	serial
Количество бит в информационном пакете	8
Без проверки бита на четность	
Количество стоп-битов	1

3. Введите команду на подключение.

   Начнется подключение к сетевому устройству и после успешного подключения на экране появится сообщение:

Не предпринимайте никаких действий и дождитесь появления на экране дополнительного меню локального управления (описание дополнительного меню см. стр.**50**).

Для перехода к главному меню:

1. Перезагрузите сетевое устройство. Для этого в дополнительном меню используйте команду "Перезагрузить".

   Начнется перезагрузка сетевого устройства и далее будет выполнено подключение. На экране появится сообщение (см. п.3 предыдущей процедуры).

2. Нажмите клавишу <Enter>.

   На экране появится главное меню локального управления.

Внимание! После завершения работ, выполняемых в рамках подключения через последовательный порт, в настройках BIOS сетевого устройства необходимо отключить поддержку последовательного порта (на вкладке Advanced у параметра Console Redirection установите значение Disabled).

Приложение

Аппаратное тестирование сетевого устройства

Аппаратное тестирование может выполняться в процессе установки ПО сетевого устройства, в ходе инициализации, а также при настройке параметров средствами локального управления сетевым устройством.

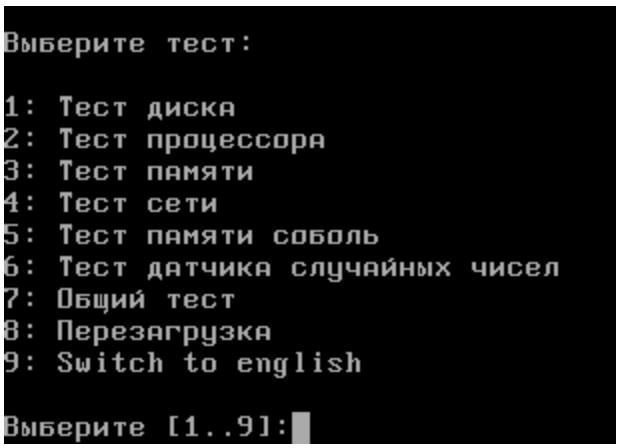
Для аппаратного тестирования применяется набор тестов, с помощью которых проверяются:

- жесткий диск;
- процессор;
- оперативная память;
- память ПАК "Соболь";
- датчик случайных чисел ПАК "Соболь";
- сетевые интерфейсы.

Для запуска теста:

1. Введите в главном локальном меню номер команды "Тестирование" и нажмите клавишу <Enter>.

   На экране появится меню выбора теста.



   - Команда "Перезагрузка" используется для выхода из режима тестирования и продолжения процедуры установки ПО. В режиме инициализации сетевого устройства команда имеет вид: "Выход".
   - Команда "Switch to english" используется для отображения данного меню на английском языке. При отображении меню на английском языке команда имеет вид: "Переключиться на русский". В режиме инициализации сетевого устройства команда не используется.

2. Введите номер команды требуемого теста и нажмите клавишу <Enter>.

   В зависимости от выбранного теста на экране появятся инструкции по выполнению дополнительных действий для проведения теста.

Тест	Описание
Тест диска	Проверка наличия сбойных секторов жесткого диска
Тест процессора	Проверка работы процессора. Необходимо задать время тестирования – от 1 до 99 минут
Тест памяти	Проверка оперативной памяти
Тест сети	Проверка работы сетевых интерфейсов. Перед запуском теста необходимо присоединить сетевые интерфейсы к общему коммутатору и соединить оптические интерфейсы в пары

Тест	Описание
Тест памяти "Соболь"	Тестирование памяти ПАК "Соболь" на чтение и запись
Тест датчика случайных чисел	Проверка работоспособности датчика случайных чисел ПАК "Соболь"
Общий тест	Последовательное выполнение всех перечисленных выше тестов с предварительным выполнением соответствующих дополнительных действий

3. Дождитесь сообщения о завершении теста и нажмите клавишу <Enter>.

   Будет выполнен возврат в меню выбора теста.
4. Для выхода из режима тестирования введите номер команды "Перезагрузка" и нажмите клавишу <Enter>.

Запись образа диска сетевого устройства на USB-флеш-накопитель

В комплект поставляемого с комплексом программного обеспечения входят следующие файлы образов дисков:

cgw_release.flash	ПО для установки сетевого устройства
cgw.aserv_release.flash	ПО для установки КШ с сервером доступа
ncc_release.flash	ПО для установки ЦУС
ncc.aserv_release.flash	ПО для установки ЦУС с сервером доступа
ids_release.flash	ПО для установки детектора атак
csw_release.flash	ПО для установки криптокоммутатора
arm_release.flash	ПО для установки АРМ генерации ключей

Для записи такого образа диска на USB-флеш-накопитель используют программы FlashGUI.exe (с графическим интерфейсом) и Flash.exe (с управлением из командной строки). Эти программы находятся на компакт-диске "Диск 1", входящем в комплект поставки, в папке \Tools\Код Безопасности\ServiceTools. Программы работают в среде Windows 2000 и выше.

Программа FlashGUI.exe

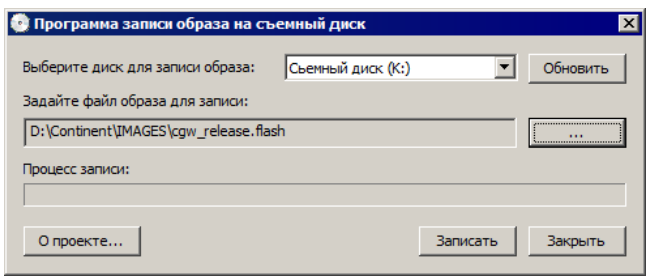
Программа FlashGUI.exe предназначена для копирования образа диска с CD-ROM на USB-флеш-накопитель.

Для записи образа диска на USB-флеш-накопитель:

1. Подсоедините USB-флеш-накопитель к USB-разъему компьютера и дождитесь подключения этого устройства к файловой системе компьютера.

   После добавления USB-флеш-накопителя в папке "Мой компьютер" появится новый объект с именем "Съемный диск".
2. Запустите на исполнение файл FlashGUI.exe.

   На экране появится окно программы записи образа на съемный диск.



3. Введите данные в поля окна и нажмите кнопку "Записать".

Выберите диск для записи образа	Имя USB-флеш-накопителя, на который необходимо записать образ. Для обновления списка используйте кнопку "Обновить"
Задайте файл образа для записи	Полное имя файла нужного образа диска. Для выбора файла в стандартном окне Windows используйте кнопку "..."

Программа приступит к записи образа на USB-флеш-накопитель. Степень выполнения процесса отображается в поле "Процесс записи".

4. Для завершения работы с программой нажмите кнопку "Закрыть".
5. Извлеките USB-флеш-накопитель из USB-разъема компьютера.

Программа Flash.exe

Программа Flash.exe предназначена для копирования образа диска с CD-ROM на USB-флеш-накопитель, а также для просмотра служебной информации о USB-флеш-накопителе.

Для просмотра справочной информации о программе:

1. Активируйте команду "Программы> Стандартные> Командная строка" в главном меню Windows.

   На экране появится окно командной строки.

2. Введите в командной строке полное имя файла программы и нажмите клавишу <Enter>.

   Например: C:\Continent\Tools\Flash.

   В окне командной строки появится описание команд управления программой.

Для просмотра служебной информации о носителе:

1. Подсоедините USB-флеш-накопитель к USB-порту компьютера и дождитесь подключения этого устройства к файловой системе компьютера.

   После добавления USB-флеш-накопителя в папке "Мой компьютер" появится новый объект с именем "Съемный диск".

2. Активируйте команду "Программы> Стандартные> Командная строка" в главном меню Windows.

   На экране появится окно командной строки.

3. Введите в командной строке полное имя файла программы с параметром "map" и нажмите клавишу <Enter>.

   Например: C:\Continent\Tools\Flash map.

   В окне командной строки появится служебная информация о USB-флеш-накопителе.

4. Ознакомьтесь с представленной информацией и закройте окно.

Для записи образа диска на USB-флеш-накопитель:

1. Подсоедините USB-флеш-накопитель к USB-порту компьютера и дождитесь подключения этого устройства к файловой системе компьютера.

   Примечание. Убедитесь, что переключатель защиты от записи, расположенный на корпусе USB-флеш-накопителя, находится в положении, разрешающем запись.

   После добавления USB-флеш-накопителя в список устройств ("Диспетчер устройств") появится новое дисковое устройство, а в папке "Мой компьютер" — новый объект с именем "Съемный диск".

Примечание. Если данный USB- флеш- накопитель уже использовался в качестве идентификатора администратора, обязательно выполните его форматирование, иначе ключевая информация на этот носитель будет записана некорректно. Форматирование осуществляется средствами ОС Windows.

2. Активируйте команду "Программы> Стандартные> Командная строка" в главном меню Windows.

   На экране появится окно командной строки.

3. Введите в командной строке полное имя файла программы Flash.exe с параметрами <имя диска> и <имя файла>, где <имя диска> — буквенное обозначение подключенного USB-флеш-накопителя, <имя файла> — полное имя файла образа диска.

   Например: C:\Continent\Tools\Flash F: D:\Continent\Flash\cgw.aserv_release.flash.

   Примечание. Если имя файла или папки содержит пробелы или специальные символы, весь путь необходимо заключить в двойные кавычки ("").

4. Нажмите клавишу <Enter>.

   В окне командной строки появится служебная информация о USB- флеш-накопителе и запрос для подтверждения операции.

5. Введите "y" и нажмите клавишу <Enter>.

   Программа приступит к записи на носитель указанного образа диска. По окончании этой операции на экран выводится сообщение о результате.

6. Закройте окно командной строки. Перед извлечением USB-флеш-накопителя из USB-порта отключите это устройство средствами Windows.

Протоколы и порты

В данном разделе представлены сведения о протоколах и портах, используемых для связи между компонентами комплекса.

Если на пути зашифрованного трафика находятся межсетевые экраны или другое оборудование, осуществляющее фильтрацию IP- пакетов, необходимо создать для них правила, разрешающие прохождение служебных пакетов комплекса по протоколам и портам, указанным в таблице.

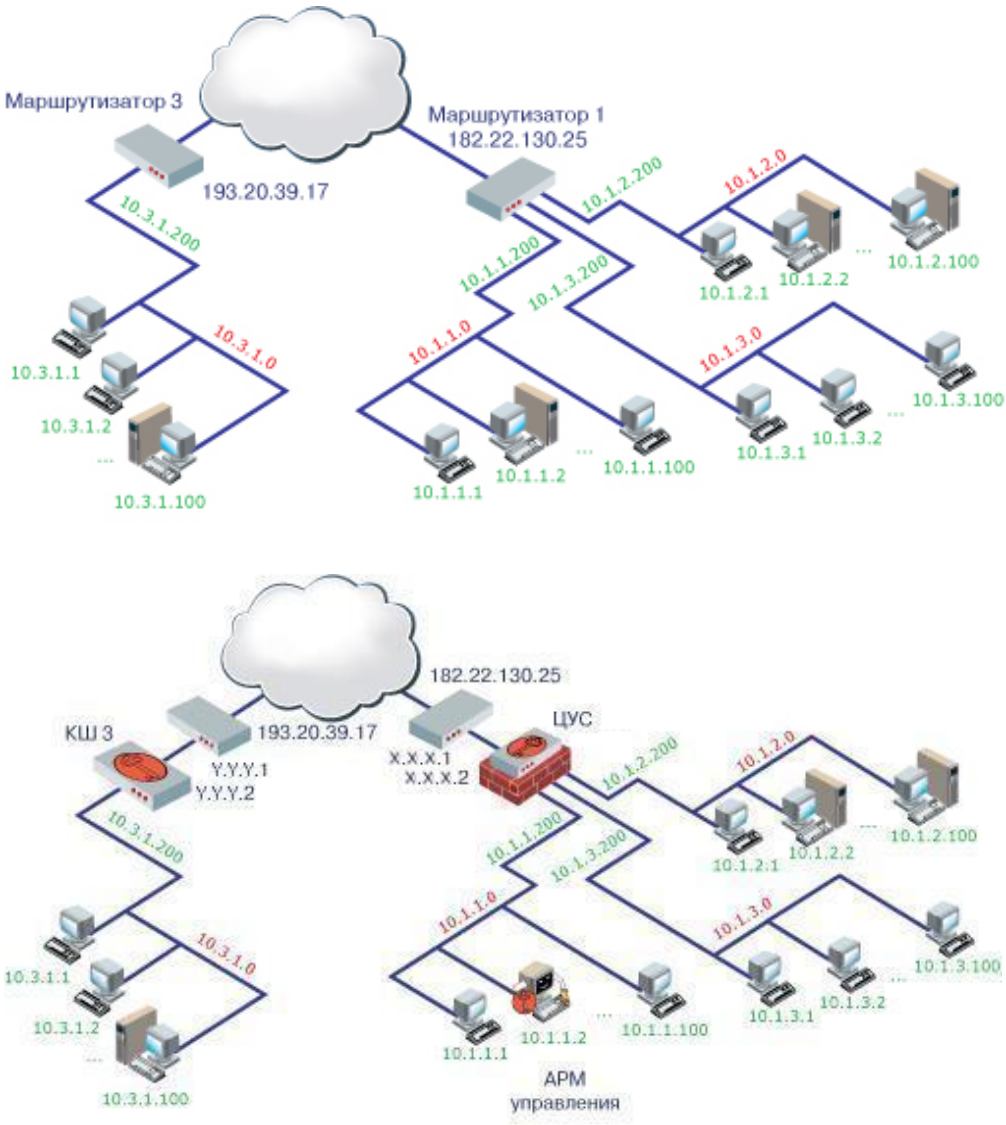
Протокол/ порт	Описание	Источник/получатель	Примечание
TCP/443	Обмен сообщениями между СД и АП. При включенном на АП режиме защищенного соединения "Потоковое подключение (TCP)" или "Подключение через прокси-сервер"	АП / СД. СД / АП	АПКШ "Континент" 3.7
TCP/4431, 1025-65535	Обмен сообщениями между СД и ПУ СД. Обмен сообщениями между агентом ЦУС и СД и СД. ПУ СД и агент ЦУС и СД устанавливают подключение со случайного порта из диапазона 1025-65535 к СД на порт 4431. СД отвечает с порта 4431 на тот порт компьютера с ПУ СД или с агентом ЦУС и СД, с которого пришло подключение	ПУ СД / СД. СД / ПУ СД. Агент ЦУС и СД /СД. СД / агент ЦУС и СД	АПКШ "Континент" 3.2.21 и более поздние версии

Протокол/порт	Описание	Источник/получатель	Примечание
TCP/4444	Передача сообщений от ПУ ЦУС к ЦУС; обмен сообщениями между ЦУС и агентом ЦУС; обмен сообщениями между агентом обновлений БРП и ЦУС. ПУ ЦУС, агент ЦУС и СД, агент обновлений БРП, агент РКН устанавливают подключение со случайного порта 1024-65535 на порт ЦУС 4444. ЦУС отвечает на тот порт, с которого было обращение	ПУ ЦУС / ЦУС. Агент ЦУС и СД / ЦУС. ЦУС / агент ЦУС и СД. Агент обновлений БРП / ЦУС	
TCP/4445	Передача обновлений ПО от ПУ ЦУС к ЦУС и обмен сообщениями между ПУ ЦУС и агентом ЦУС. ПУ ЦУС устанавливает подключение со случайного порта 1024-65535 на порт ЦУС 4445. ЦУС отвечает на тот порт, с которого было обращение	ПУ ЦУС / ЦУС. ПУ ЦУС / агент ЦУС и СД. Агент ЦУС и СД / ПУ ЦУС	АПКШ "Континент" 3.1.18 и более поздние версии
TCP/4446	Аутентификация пользователей в защищенном сегменте сети. Клиент аутентификации устанавливает подключение со случайного порта 1024-65535 на порт ЦУС 4446. ЦУС отвечает на тот порт, с которого было обращение	Компьютер с установленной программой "Клиент аутентификации пользователя" / СУ	АПКШ "Континент" 3.6 и более поздние версии
TCP/5100	Передача сообщений от ЦУС к СУ и обмен сообщениями между СУ в кластере. Узел кластера обращается к парному с порта 10000-65535 на порт 5100. Парный отвечает на тот порт, с которого было обращение	ЦУС / СУ. Основное СУ / резервное СУ. Резервное СУ / основное СУ	АПКШ "Континент" 3.0 и более поздние версии
TCP/5101	Передача сообщений от СУ к ЦУС. Узел устанавливает подключение со случайного порта 10000-65535 на порт ЦУС 5101. ЦУС отвечает на тот порт, с которого было обращение	СУ / ЦУС	АПКШ "Континент" 3.0 и более поздние версии
TCP/5102	Передача файлов от ЦУС к СУ. Узел устанавливает подключение со случайного порта 10000-65535 на порт ЦУС 5102. ЦУС отвечает на тот порт, с которого было обращение	ЦУС / СУ	АПКШ "Континент" версии 3.5

Протокол/ порт	Описание	Источник/получатель	Примечание
TCP/5103	Передача файлов от ЦУС к СУ. Узел устанавливает подключение со случайного порта 10000-65535 на порт ЦУС 5103. ЦУС отвечает на тот порт, с которого было обращение	ЦУС / СУ	АПКШ "Континент" 3.6 и более поздние версии
UDP/5101	Передача сообщений от СУ к ЦУС. Узел обращается с порта 5100 на порт ЦУС 5101. ЦУС отвечает с порта 5101 на порт 5100	СУ (исходящий порт 5100) / ЦУС	АПКШ "Континент" 3.0 и более поздние версии
UDP/5106 UDP/5107	Поддержка работы СУ за NAT. В зависимости от используемых классов трафика, узлы отправляют пакеты с портов 10000-10031 на порты ЦУС 5106-5107	СУ / ЦУС	АПКШ "Континент" 3.6 и более поздние версии
UDP/5557	Передача сообщений об активности между СУ в кластере. Узлы кластера обмениваются пакетами с порта 5557 на порт 5557	Основное СУ / резервное СУ. Резервное СУ / основное СУ	АПКШ "Континент" 3.0 и более поздние версии
UDP/4433	Обмен сообщениями между СД и АП. Номер порта по умолчанию; изменяется в программе управления СД	АП / сервер доступа	АПКШ "Континент" 3.2.21 и более поздние версии
UDP/7500	Обмен сообщениями между СД и АП. Номер порта по умолчанию; изменяется в настройках виртуального адаптера Continent 3 PPP Adapter	Сервер доступа / АП	АПКШ "Континент" 3.2.21 и более поздние версии
UDP/10000	Передача зашифрованного трафика. Узлы обмениваются пакетами с порта 10000 на порт 10000	СУ / СУ. СУ / ЦУС	АПКШ "Континент" 3.5
UDP/10000-10031	Передача зашифрованного трафика. В зависимости от используемых классов трафика, узлы обмениваются пакетами с портов 10000-31 на соответствующие порты 10000-31	СУ / СУ. СУ / ЦУС	АПКШ "Континент" 3.6 и более поздние версии

Подключение КШ к действующим локальным сетям

На рисунке представлен пример организации действующих локальных сетей до и после подключения КШ:



Подключение ЦУС

1. Получите у провайдера два IP-адреса: один для ЦУС и один для маршрутизатора.

   Примечание. Если маршрутизатор расположен в корпоративной сети, определите адреса самостоятельно. На приведенном выше рисунке это IP-адрес X.X.X.1 для маршрутизатора 1 и IP-адрес X.X.X.2 для ЦУС.

2. Выполните инициализацию ЦУС (см. стр.**12**). При этом укажите следующие значения параметров:

Внешний IP-адрес шлюза	IP-адрес ЦУС, определенный в п. 1
Внутренние IP-адреса шлюза	IP-адреса подключенных локальных сетей
Адрес маршрутизатора по умолчанию	IP-адрес маршрутизатора, определенный в п. 1

3. Подключите ЦУС к сетевым коммуникациям, как указано на рисунке выше.
4. Выполните настройку маршрутизатора:
   - назначьте маршрутизатору внутренний IP-адрес, определенный в п. 1;
   - задайте правило маршрутизации, по которому доступ к локальным подсетям осуществляется через маршрутизатор с IP- адресом ЦУС, определенным в п. 1.

5. Перейдите к выполнению следующего пункта ввода комплекса в эксплуатацию (см. [**1**]).

Подключение КШ

1. Получите у провайдера два IP-адреса: один для КШ и один для маршрутизатора.

   Примечание. Если маршрутизатор расположен в корпоративной сети, определите адреса самостоятельно. На приведенном выше рисунке это IP-адрес Y.Y.Y.1 для маршрутизатора 3 и IP-адрес Y.Y.Y.2 для КШ 3.

2. В программе управления зарегистрируйте КШ и запишите конфигурацию на носитель (см. [**1**]). При регистрации укажите следующие значения параметров:

IP-адрес	IP-адрес КШ, определенный в п. 1
IP-адрес внешнего интерфейса	IP-адрес КШ, определенный в п. 1
IP-адреса внутренних интерфейсов	IP-адреса подключаемых локальных сетей
Маршрут по умолчанию	IP-адрес маршрутизатора, определенный в п. 1

3. Выполните инициализацию КШ (см. стр. **16**) и подключите его к сетевым коммуникациям, как указано на рисунке выше.
4. Выполните настройку маршрутизатора:
   - назначьте маршрутизатору внутренний IP-адрес, определенный в п. 1;
   - задайте правило маршрутизации, по которому доступ к локальным подсетям осуществляется через маршрутизатор с IP- адресом КШ, определенным в п. 1.
5. Перейдите к выполнению следующего пункта ввода комплекса в эксплуатацию (см. [**1**]).

Звуковые сообщения о работе сетевого устройства

При каждой загрузке сетевого устройства осуществляется проверка целостности файлов программного обеспечения и загрузочных секторов. Проверка осуществляется средствами ПАК "Соболь". При отсутствии монитора работа сетевого устройства контролируется подачей звуковых сигналов. Соответствие звуковых сигналов сообщениям и действия оператора по этим сигналам приведены ниже.

Табл.4 Информационные сообщения

Сигнал	Причина	Действие
Три коротких слитых вместе высоких сигнала с понижающейся частотой	Необходимо предъявить персональный идентификатор	Прислоните и удерживайте персональный идентификатор
Два коротких высоких сигнала одинаковой частоты	Идентификатор пользователя успешно считан	Нет
Три коротких слитых вместе высоких сигнала с повышающейся частотой	Осуществляется загрузка операционной системы	Нет
Три коротких слитых вместе низких сигнала с понижающейся частотой	Осуществляется перезагрузка компьютера	Нет

Табл.5 Сообщения о неправильном вводе информации

Сигнал	Причина	Действие
Один длинный высокий сигнал	Плохой контакт идентификатора со считывателем или предъявлен неверный персональный идентификатор	Плотнее удерживайте персональный идентификатор или предъявите верный персональный идентификатор

Табл.6 Сообщения о выполняемых действиях

Сигнал	Причина	Действие
Три коротких высоких сигнала, затем один низкий сигнал	Необходима перезагрузка сетевого устройства	Нажмите кнопку Reset
Короткий высокий сигнал, затем длинный низкий сигнал	Необходима перезагрузка сетевого устройства	Нажмите кнопку Reset
Три длинных низких сигнала	Необходима перезагрузка сетевого устройства	Нажмите кнопку Reset

Табл.7 Сообщения о необходимости вмешательства специалиста

Сигнал	Причина	Действие
Сирена из шести сигналов высокой частоты	Нарушена целостность списка пользователей, журнала событий или системных переменных ПАК. Отсутствуют файлы шаблонов для контроля целостности на диске либо неверно указаны пути к файлам с шаблонами в Электронном замке. Была нарушена целостность файлов	Подключите к сетевому устройству монитор, войдите с правами администратора в ПАК и устраните ошибку

Табл.8 Сообщения о фатальной ошибке

Сигнал	Причина	Действие
Шесть коротких высоких сигналов	Не удается определить адрес платы. Тест корректности работы процессора завершился с ошибкой. Чтение флеш-памяти завершилось с ошибкой. Целостность кода нарушена. Ошибка чтения или записи ОЗУ. Нарушена целостность ОЗУ. Не удается выбрать для работы внешний считыватель персонального идентификатора	Произведите инициализацию ПАК "Соболь", измените настройки компьютера или замените плату ПАК "Соболь" на исправную

Показания индикаторов аппаратной платформы

Индикаторы сетевых интерфейсов

Ниже представлена расшифровка показаний светодиодных индикаторов сетевых интерфейсов для аппаратных платформ IPC-25, IPC-100.

Табл.9 Индикатор состояния интерфейса (левый)

Цвет	Описание
Желтый (редкое мигание)	Активный режим, передача данных отсутствует

Цвет	Описание
Желтый (частое мигание)	Активный режим, выполняется передача данных
Зеленый	Режим ожидания

Табл.10 Индикатор типа соединения (правый)

Цвет	Описание
Зеленый	Соединение со скоростью 100 Мбит/с
Оранжевый	Соединение со скоростью 1000 Мбит/с

Индикатор ошибки BIOS

Красный цвет индикатора аппаратной платформы S021 (постоянное свечение или мигание) указывает на повышенную температуру CPU и/или отклонения в работе вентиляторов, системного или CPU.

Значения данных параметров можно уточнить в BIOS: Advanced > H/W Monitor to get information.

Особенности эксплуатации КШ с модемным подключением

Рекомендуемый порядок подключения КШ к коммутируемой линии

Внимание! Сервер удаленного доступа (Remote Access Server — RAS) должен поддерживать аутентификацию стандарта PAP или CHAP. Также этот сервер должен работать в режиме статического выделения IP-адресов RAS-клиентам.

1. Получите у провайдера следующую информацию:
   - статически заданный IP-адрес сервера удаленного доступа;
   - номера телефонов модемного пула;
   - скорость dial-up соединения.

   Пояснение. Если сервер удаленного доступа принадлежит корпоративной сети, выясните IP-адрессервера, номера телефонов и скорость dial-up соединения у представителя вашей организации, ответственного за эксплуатацию сервера. IP-адрес RAS-клиента для КШ назначьте самостоятельно, учитывая, что внутри корпоративной сети все IP-адреса должны быть уникальны.

2. В программе управления зарегистрируйте КШ с модемным подключением и запишите конфигурацию на носитель (см. [**1**]). При регистрации указывайте следующие значения для перечисленных ниже параметров:

Скорость передачи данных через COM-порт для внешнего интерфейса	Скорость, указанная в профиле NVRAM модема (см. документацию на модем, обычно используют 115200 бит/сек.)
Номера телефонов	Номера телефонов модемного пула, полученные у провайдера (см. п. 1)
IP-адреса внутренних интерфейсов	IP-адреса подключаемых локальных сетей

   Пояснение. Настройка самого модема выполняется в соответствии с эксплуатационной документацией, входящей в комплект поставки данного модема.

3. Добавьте для ЦУС маршрут к пулу выделяемых RAS-сервером адресов через адрес RAS-сервера, чтобы подключаемый КШ был доступен для ЦУС (см. [**1**]).
4. Подключите КШ к сетевым коммуникациям и выполните его инициализацию (см. стр.**16**).

Изменение типа телефонной линии при модемном подключении

Модемное подключение криптографического шлюза возможно к телефонным линиям двух типов:

- выделенные телефонные линии;
- коммутируемые телефонные линии.

При изменении типа линии необходимо выполнить повторную инициализацию данного криптографического шлюза.

При использовании выделенной линии необходимо выполнить настройку модема заранее, до подключения его к КШ.

Для смены типа телефонной линии:

1. В программе управления вызовите окно настройки параметров нужного КШ (см. [**1**]).
2. Выведите КШ из эксплуатации. Для этого в окне диалога "Свойства криптошлюза" на вкладке "Общие сведения" удалите отметку из поля "Введен в эксплуатацию". При этом осуществится разрыв управляющего соединения ЦУС с КШ.
3. Перейдите к диалогу "Интерфейсы" и откройте вкладку "PPP".
4. Укажите нужный тип телефонной линии и настройки соединения.
5. Закройте окно "Свойства криптошлюза" с сохранением параметров.
6. Сохраните конфигурацию данного КШ на носитель.
7. Подключите модем к выбранной телефонной линии (см. документацию на используемый модем).
8. Выполните инициализацию данного КШ, используя носитель с сохраненной конфигурацией (см. стр.**16**).
9. Введите КШ в эксплуатацию. Для этого в программе управления в окне диалога "Свойства криптошлюза" на вкладке "Общие сведения" установите отметку в поле "Введен в эксплуатацию". По этой команде ЦУС установит управляющее соединение с КШ на новом ключе, а также обновит все ключи парной связи данного КШ.

Документация

1.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Централизованное управление комплексом
2.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Локальное управление сетевыми устройствами
3.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Аудит
4.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Аутентификация пользователя
5.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Сервер доступа
6.	Аппаратно-программный комплекс шифрования "Континент". Руководство пользователя. Программа мониторинга КШ
7.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Тестирование каналов связи
8.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Обновление программного обеспечения
9.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Автоматизированное рабочее место генерации ключей
10.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Система обнаружения вторжений

Примечание. Набор документов, входящих в комплект поставки, может отличаться от указанного списка.