КОД безопасности

Аппаратно-программный комплекс шифрования

Континент
Версия 3.9

Руководство администратора

Управление комплексом

RU.88338853.501430.022 90 3

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

Оглавление

Список сокращений

АП	Абонентский пункт
АС	Автономная система
АПКШ	Аппаратно-программный комплекс шифрования
БД	База данных
ДСЧ	Датчик случайных чисел
КШ	Криптографический шлюз
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
ПУ	Программа управления
РКН	Роскомнадзор
РМ	Рабочее место
СЗИ	Средство защиты информации
СУ	Сетевое устройство (КШ, ДА)
ЦУС	Центр управления сетью
BGP	Border Gateway Protocol
BIOS	Basic Input-Output System
DNS	Domain Name System
ICMP	Internet Control Message Protocol
IP	Internet Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
OSPF	Open Shortest Path First
TCP	Transmission Control Protocol
ToS	Type of Service
UDP	User Datagram Protocol
USB	Universal Serial Bus
VTY	VirtualTeletYpe

Введение

Документ предназначен для администраторов изделия "Аппаратно-программный комплекс шифрования "Континент" Версия 3.9" (далее — АПКШ "Континент", комплекс). В нем содержатся сведения, необходимые администраторам для ввода комплекса в эксплуатацию, централизованного управления сетевыми устройствами, а также для локального управления отдельными компонентами комплекса.

Дополнительные сведения, необходимые администратору комплекса, содержатся в [**1**]–[**5**].

Сайт в интернете. Информация о продуктах компании "Код Безопасности" представлена на сайте https://www.securitycode.ru.

Служба технической поддержки. Связаться со службой технической поддержки можно по телефону 8 800 505-30-20 или по электронной почте support@securitycode.ru.

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно в авторизованных учебных центрах. Список учебных центров и условия обучения представлены на сайте компании — https://www.securitycode.ru. Связаться с представителем компании по вопросам организации обучения можно по электронной почте education@securitycode.ru.

Глава 1
Локальное управление сетевым устройством

Запуск и перезагрузка сетевого устройства

В этом подразделе представлена процедура запуска сетевого устройства, находящегося в эксплуатации. Процедура запуска сетевого устройства при его первом включении приведена в [**2**].

Для перезагрузки устройства достаточно нажать комбинацию клавиш <Ctrl> + <Alt> + <Del>.

Включение и перезагрузку устройства можно выполнить дистанционно, с помощью программы управления ЦУС (см. стр. **42**).

Для запуска сетевого устройства:

1. Включите питание сетевого устройства. На экране появится основное окно ПАК "Соболь", в центре которого будет отображаться запрос персонального идентификатора.
2. Приложите персональный идентификатор администратора ПАК "Соболь" к считывателю.

   После считывания информации из идентификатора в зависимости от настроек ПАК "Соболь" на экране может появиться запрос пароля. В этом случае введите пароль администратора ПАК "Соболь".
3. Нажмите клавишу <Enter>.

   На экране появится главное меню администратора ПАК "Соболь".

Примечание. Все сведения, необходимые администратору для управления работой ПАК "Соболь", содержатся в руководстве администратора ПАК "Соболь".

4. Выберите в меню пункт "Загрузка операционной системы" и нажмите клавишу <Enter>.

   После успешной проверки целостности файлов программного обеспечения средствами ПАК "Соболь" начнется загрузка операционной системы.

   По окончании загрузки операционной системы на экране появится сообщение:

```
Нажмите Enter для настройки параметров
```

Сообщение актуально в течение 5 секунд. Для выполнения настроек перед запуском сетевого устройства нажмите клавишу <Enter> и в открывшемся главном меню сетевого устройства выберите нужный пункт (см. стр. **10**). После выполнения настроек вернитесь в главное меню и выберите пункт "Выход".

5. По завершении настройки или по истечении 5 секунд конфигурация комплекса будет загружена и на экране появится сообщение:

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

С этого момента сетевое устройство переходит в рабочий режим.

Интерфейс системы локального управления

Для пользователя при локальном управлении СУ доступны следующие типы окон:

Тип окна	Способ переключения
Окно с главным меню	<Alt> + <F1>
Окно с дополнительным меню (требуется аутентификация локального администратора, см. стр. **25**)	<Alt> + <F2>

Во всех окнах допустим переход в режим чтения отображаемой информации на экране при нажатии клавиши <Scroll Lock>. В этом режиме используются следующие клавиши клавиатуры:

- < ↑> — для перемещения на одну строку вверх;
- < ↓> — для перемещения на одну строку вниз;
- <Page Up> — для перемещения на одну страницу вверх;
- <Page Down> — для перемещения на одну страницу вниз;
- <Home> — для перемещения в конец списка;
- <End> — для перемещения в начало списка;
- <Scroll Lock> — для возврата в режим управления.

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. на стр. **101**.

При локальном управлении изменение настроек сетевого устройства, находящегося в рабочем режиме, невозможно.

Для перехода к режиму настройки сетевого устройства:

1. Выключите питание сетевого устройства. Подключите к системному блоку сетевого устройства клавиатуру и монитор.
2. Осуществите запуск сетевого устройства (см. стр. **8**). При появлении на экране сообщения "Нажмите Enter для настройки параметров" нажмите клавишу <Enter>.

Примечание. 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, подобное следующему:

```
1: Завершение работы
2: Перезагрузка
3: Управление конфигурацией
4: Настройка безопасности
5: Настройка ДА <функция недоступна>
7: Тестирование
0: Выход
Выберите пункт меню (0–7):
```

Примечание. На выбор команды меню дается одна минута, после чего осуществляется автоматическое завершение процедуры настройки и переход устройства в рабочий режим.

Настройка сетевого устройства

Для перехода к меню управления СУ:

- В главном меню локального управления СУ введите номер команды "Управление конфигурацией" и нажмите клавишу <Enter>.

  На экране появится меню управления СУ, подобное следующему:

```
1: Сохранение конфигурации
2: Загрузка конфигурации
3: Изменение адреса активного ЦУС
4: Настройка PPP-соединений
5: Настройка шифрования
6: Настройка фрагментации
7: Настройка коммутации
8: Настройка отладочного журнала
9: Настройка доступа удаленного терминала
0: Выход
Выберите пункт меню (0 - 10):
```

Создание резервной копии конфигурации сетевого устройства

Резервную копию конфигурации сетевого устройства сохраняют в зашифрованном виде на внешнем носителе в файле gate.cfg. В качестве внешнего носителя используют USB-флеш-накопитель.

Для создания резервной копии:

1. Перейдите к меню управления сетевым устройством (см. стр. **10**).
2. Введите в строке ввода номер команды "Сохранение конфигурации" и нажмите клавишу <Enter>.

   На экране появится сообщение:

```
Введите пароль
```

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

   Внимание! Длина пароля – не менее 5 символов.

   На экране появится сообщение:

```
Повторите пароль
```

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

   На экране появится сообщение:

```
Вставьте носитель для записи конфигурации и нажмите Enter
```

5. Вставьте USB-флеш-накопитель для создания резервной копии, дождитесь сообщений на экране о подключении носителя к системе и нажмите клавишу <Enter>.

   Дождитесь информационного сообщения о сохранении конфигурации.

Загрузка резервной копии конфигурации сетевого устройства

Для загрузки конфигурации сетевого устройства подготовьте внешний носитель с конфигурационным файлом gate.cfg.

Для загрузки резервной копии:

1. Перейдите к меню управления сетевым устройством (см. стр. **10**).
2. Введите в строке ввода номер команды "Загрузка конфигурации" и нажмите клавишу <Enter>.

   На экране появится сообщение:

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

3. Вставьте USB-флеш-накопитель для создания резервной копии, дождитесь сообщений на экране о подключении носителя к системе и нажмите клавишу <Enter>.

   На экране появится сообщение:

   ```
   Введите пароль
   ```

4. Введите пароль и нажмите клавишу <Enter>.

   Дождитесь информационного сообщения о загрузке конфигурации.

Изменение адреса подключения к ЦУС

Данную процедуру выполняют для ликвидации нештатной ситуации, когда по каким-либо причинам связь между сетевым устройством и ЦУС установить не удалось.

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 задать адрес сетевого устройства централизованно в программе управления ЦУС ([**6**]).

Изменение внешнего адреса возможно только при отключенном режиме динамической маршрутизации.

Для изменения адреса подключения к ЦУС:

1. Перейдите к меню управления (см. [**6**]).
2. Введите в строке ввода номер команды "Изменение адреса активного ЦУС" и нажмите клавишу <Enter>.

   На экране появится запрос на ввод нового IP-адреса ЦУС.

3. Введите IP-адрес и нажмите клавишу <Enter>.

   На экране появится меню управления.

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

Настройка параметров шифратора

Для шифратора КШ при локальном управлении предусмотрены следующие настройки:

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

  Включение или отключение режима шифрования трафика к парному сетевому устройству зависит от принадлежности адреса источника — входит он в диапазон адресов глобальной сети интернет ("белый" адрес) или в диапазон адресов, назначаемых для внутренних сетей ("серый" адрес). При включенном режиме, если адрес источника "белый", трафик, передаваемый в защищаемую сеть парного сетевого устройства, зашифровываться не будет. При отключенном режиме такой трафик будет зашифровываться.

- Разрешение или запрет дефрагментации пакетов до фильтра.

  Дефрагментация пакетов в КШ 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 пакетного фильтра".

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

- Задание числа потоков шифрования.

  На КШ трафик при шифровании распределяется по потокам. При наличии свободных ресурсов процессора целесообразно повысить количество потоков для повышения производительности шифрования. Данная настройка актуальна для платформ IPC-1000 и выше.

  По умолчанию число потоков определяется шифратором автоматически.

Для настройки шифратора:

> **Внимание!** Если сетевое устройство находится в кластере, описанные ниже настройки должны быть выполнены на каждом устройстве, входящем в состав кластера.

1. Перейдите к меню управления сетевого устройства (см. стр. **10**).
2. Введите в строке ввода номер команды "Настройка шифрования" и нажмите клавишу <Enter>.

   На экране появится меню:

```
1: Включение/Отключение режима шифрования трафика на
основе адреса источника
2: Разрешение/Запрет дефрагментации пакетов до пакетного
фильтра
3: Запрет/Разрешение распределения пакетов с учетом
соединений
4: Задание числа потоков шифрования
0: Выход
Выберите пункт меню (0 – 4):
```

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

Для первых трех команд статус параметра в меню на экране изменится.

При выборе задания числа потоков шифрования на экране появится запрос:

```
Задайте число потоков шифрования (1-32):
```

4. Введите нужное значение и нажмите клавишу <Enter>.

Настройка STUN

Данная настройка выполняется 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. **10**).
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 фильтрации протоколов на криптокоммутаторе

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. **10**).
2. Введите в строке ввода номер команды "Настройка коммутации" и нажмите клавишу <Enter>.

   На экране появится меню настроек коммутации.

```
1: Показать текущие настройки коммутации
2: Разрешить прохождение LACP-пакетов
3: Разрешить прохождение STP-пакетов
4: Разрешить прохождение пакетов Port-Based access control
по 802.1x
5: Разрешить прохождение Pause-пакетов для flow control
6: Включить Jumbo frame на портах коммутации
0: Выход
Выберите пункт меню (0 – 5):
```

Примечание. Криптокоммутаторы версии 3.7 не поддерживают Jumbo frame. При включении этой настройки на КК, у которого есть парная связь с КК версии 3.7, возможны проблемы с передачей данных.

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

   На экране отобразятся текущие настройки.

```
Прохождение пакетов LACP запрещено
Прохождение пакетов STP запрещено
Прохождение пакетов 802.1 запрещено
Прохождение Pause пакетов запрещено
```

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).

Настройка дистанционного доступа по протоколу SSH

Дистанционный доступ разрешается только в рамках текущей сессии, после перезагрузки сетевого устройства все параметры по дистанционному доступу будут сброшены.

Для настройки дистанционного доступа к локальному управлению сетевым устройством:

1. Перейдите к меню управления сетевым устройством (см. стр. **10**).
2. Введите в строке ввода номер команды "Настройка доступа удаленного терминала" и нажмите клавишу <Enter>.

   На экране появится меню настроек SSH.

```
1: Включить сервис удаленного терминала
2: Установить адрес принимающего соединения
3: Изменить порт принимающего соединения
4: Список разрешенных IP-адресов
0: Выход
Выберите пункт меню (0 – 4):
```

3. Введите в строке ввода номер команды "Установить адрес принимающего соединения" и нажмите клавишу <Enter>.

   На экране появится запрос IP-адреса.
4. Введите требуемый IP-адрес интерфейса, через который будет осуществляться дистанционный доступ, и нажмите клавишу <Enter>.

   На экране появится меню настроек SSH, в котором строка установления адреса принимающего соединения дополнится введенным IP-адресом.
5. Введите в строке ввода номер команды "Изменить порт принимающего соединения" и нажмите клавишу <Enter>.

   На экране появится запрос порта.
6. Введите в строке ввода номер используемого порта и нажмите клавишу <Enter>.

   Примечание. Для доступа по протоколу SSH обычно используется 22-й TCP-порт.

   На экране появится меню настроек SSH, в котором строка изменения порта принимающего соединения дополнится введенным номером порта.
7. Введите в строке ввода номер команды "Список разрешенных IP-адресов" и нажмите клавишу <Enter>.

   На экране появится окно формирования списка.
8. Для добавления IP-адреса нажмите клавишу <F2>, введите требуемый IP-адрес и нажмите клавишу <Enter>.
9. Для редактирования IP-адреса перейдите на него, используя курсоры клавиатуры, нажмите клавишу <Enter>, внесите требуемые изменения и нажмите клавишу <Enter>.
10. Для удаления IP-адреса перейдите на него, используя курсоры клавиатуры, нажмите клавишу <F8> и подтвердите операцию удаления, выбрав команду "Да" и нажав клавишу <Enter>.
11. После формирования списка IP-адресов, которым будет разрешен доступ к удаленному управлению устройством, нажмите клавишу <Esc>.
12. Для возвращения к меню управления сетевым устройством введите "0" и нажмите клавишу <Enter>.

Настройка безопасности

Переход к меню "Настройки безопасности"

Для перехода к меню "Настройки безопасности":

1. Перейдите к режиму настройки сетевого устройства (см. стр. **9**).
2. В главном меню введите в строке ввода номер команды "Настройки безопасности" и нажмите клавишу <Enter>.

   На экране появится меню "Настройки безопасности".

   Внимание! Состав меню и доступность функций зависит от типа установленных на аппаратной платформе программных компонентов. Ниже представлено стандартное меню "Настройки безопасности" КШ с ЦУС.

```
1: Регистрация нового администратора
2: Ограничение управления
3: Обновление исходной ключевой информации
4: Смена ключей КШ
5: Загрузка ключей с носителя (функция недоступна)
6: Удаление криптографической информации
7: Включение привязки маршрутизаторов к MAC-адресам
8: Ограничение числа соединений с одного IP-адреса
9: Очистка журналов ЦУС
10: Настройка параметров локальной сигнализации НСД
11: Разрешение прохождения пакетов с IP-опциями
12: Включение программного контроля целостности
0: Выход
Выберите пункт меню (0 - 12):
```

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

   Описание процедур приводится в последующих разделах.
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 (см. стр. **37**) появится новая запись "Добавленный с консоли администратор".

Для регистрации администратора:

1. Перейдите к меню настройки безопасности (см. стр. **16**).
2. Введите в строке ввода номер команды "Регистрация нового администратора" и нажмите клавишу <Enter>. На экране появится сообщение:

```
Введите пароль ключа администратора ЦУС
```

3. Введите пароль и нажмите клавишу <Enter>.

   Примечание. Длина и сложность пароля задаются политикой аутентификации администраторов (см. стр. 37). По умолчанию длина пароля не менее 4 символов. Разрешено использование любых символов, кроме кириллицы.

   Запомните пароль. Этот пароль будет использован для шифрования административного ключа и в дальнейшем понадобится для подключения программы управления к ЦУС.

   На экране появится сообщение:

   ```
   Повторите пароль
   ```

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

   На экране появится сообщение:

   ```
   Вставьте носитель для записи ключа администратора ЦУС и
   нажмите Enter
   ```

5. Предъявите носитель и нажмите клавишу <Enter>.

   После успешной записи информации на экране появится меню настройки безопасности.

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

Ограничение управления ЦУС

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

Для включения режима ограничения управления с интерфейса:

1. Перейдите к меню настройки безопасности (см. стр. 16).
2. Введите в строке ввода номер команды ограничения управления 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 настройки разрешения управления:

   ```
   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: <список интерфейсов>
   Введите название интерфейса, с которого будет разрешено управление:
   ```

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

   На экране появится сообщение:

   ```
   Добавлено разрешение управления с интерфейса <наименование интерфейса>
   ```

   Затем на экране появится меню настройки разрешения управления.

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. **16**).
2. Введите в строке ввода номер команды ограничения управления и нажмите клавишу <Enter>.

   На экране появится меню ограничения управления.

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

   На экране появится меню настройки разрешения управления.

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 с указанием префикса маски и нажмите клавишу <Enter>.

   На экране появится сообщение:

   ```
   Продолжить? (Y/N)
   ```

6. Для ввода другого IP-адреса введите "n", нажмите клавишу <Enter> и перейдите к п. **5**.
7. Для продолжения работы введите "y" и нажмите клавишу <Enter>.

   На экране появится сообщение:

   ```
   Добавлено разрешение управления с IP-адреса <адрес>
   ```

   Затем на экране появится меню настройки разрешения управления.

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

Для просмотра списка разрешений:

1. Перейдите к меню настройки безопасности (см. стр. **16**).
2. Введите в строке ввода номер команды ограничения управления и нажмите клавишу <Enter>.

   На экране появится меню ограничения управления.

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. **16**).
2. Введите в строке ввода номер команды ограничения управления и нажмите клавишу <Enter>.

   На экране появится меню ограничения управления.
3. Введите в строке ввода номер команды "Очистить список разрешений управления" и нажмите клавишу <Enter>.

   На экране появится меню настройки безопасности.
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-диск (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 к меню настройки безопасности КШ с ЦУС (см. стр. **16**).
2. Введите в строке ввода номер команды "Обновление исходной ключевой информации" и нажмите клавишу <Enter>.

   На экране появится запрос:

   ```
   Использовать внешний носитель для инициализации? (Y/N)
   ```
3. Введите "Y" и нажмите клавишу <Enter>.
4. 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
   ```
5. 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.

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

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 ([6]).

Для смены ключей на КШ с ЦУС:

1. Перейдите к меню настройки безопасности (см. стр. **16**).
2. Введите в строке ввода номер команды "Смена ключей 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.

Загрузка ключей

Данную процедуру выполняют для загрузки ключа. Ключ представляет собой пару: главный ключ КШ и ключ связи с ЦУС.

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

Для загрузки ключа на сетевое устройство:

1. Перейдите к меню настройки безопасности (см. стр. **16**).
2. Введите в строке ввода номер команды "Загрузка ключей с носителя" и нажмите клавишу <Enter>.

   На экране появится меню загрузки ключа.
3. Введите номер варианта "Загрузить активный ключ" и нажмите клавишу <Enter>.

   На экране появится сообщение, подобное следующему:

   ```
   Уже имеется активный ключ, установленный на КШ. Заменить?
   (Y/N):
   ```
4. Введите "Y" и нажмите клавишу <Enter>.

   Примечание. Если в ходе эксплуатации комплекса на сетевое устройство были присланы ключи с ЦУС, то будет предложено их использование. Для их использования предъявите ключевой носитель сетевого устройства, введите "Y" и нажмите клавишу <Enter>.

   На экране появится сообщение о необходимости предъявления носителя с ключами.
5. Предъявите носитель с ключами и нажмите клавишу <Enter>.

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

   Примечание. 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.

7. Введите "1" и нажмите клавишу <Enter>.
   - Если носителем является USB-флеш-накопитель, начнется загрузка ключа.
   - Если носителем является Рутокен, появится список ключей, входящих в комплект.

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

     Начнется загрузка ключа.

   После успешной загрузки появится сообщение:

   ```
   Ключ установлен как активный
   ```

   На экране появится меню "Настройки безопасности".

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. **16**).
2. Введите в строке ввода номер команды "Удаление криптографической информации" и нажмите клавишу <Enter>.

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

   ```
   ВНИМАНИЕ! После этой операции понадобится повторная
   <загрузка конфигурации>/<инициализация ЦУС>!
   Продолжить? (Y/N):
   ```

3. Наберите "y" 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. [**2**]).
   - Для КШ с ЦУС перейдите к выполнению п. **7** процедуры инициализации КШ с ЦУС (см. [**2**]).

Примечание. Если требуется отложить инициализацию, выключите компьютер.

Привязка аппаратных адресов маршрутизаторов

Данная функция позволяет запретить на сетевом устройстве действие протокола ARP и осуществлять маршрутизацию по MAC-адресам маршрутизаторов. Такой подход обеспечивает защиту от сетевых атак типа ARP-spoofing.

При использовании этой функции в случае замены маршрутизатора (сетевых карт узлов, выполняющих функции маршрутизатора) необходимо выполнить принудительное обновление зафиксированных в конфигурации сетевого устройства аппаратных адресов.

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

Включение контроля аппаратных адресов

Для фиксации аппаратных адресов:

1. Перейдите к меню настройки безопасности (см. стр. **16**).
2. Введите в строке ввода номер команды "Включение привязки 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 ввести "n", MAC-адрес маршрутизатора будет определен автоматически.

   На экране появится сообщение:

   ```
   Введите MAC-адрес:
   ```

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

   Примечание. При использовании нескольких маршрутизаторов повторите выполнение пп. **3, 4** для каждого маршрутизатора.

   На экране появится сообщение:

   ```
   ARP кэш сохранен
   ```

   Затем на экране появится меню настройки безопасности. 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. **16**).
2. Введите в строке ввода номер команды "Отключить привязку маршрутизаторов или обновить их адреса" и нажмите клавишу <Enter>.

   На экране появится меню настройки привязки:

   ```
   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 FF:FF:FF:FF:FF:FF и нажмите клавишу <Enter>.

Примечание. При использовании нескольких маршрутизаторов повторите выполнение пп. **4, 5** для каждого маршрутизатора.

На экране появится сообщение:

```
ARP кэш сохранен
```

Затем на экране появится меню настройки привязки.

6. Введите в строке ввода "0" и нажмите клавишу <Enter>.

На экране появится меню настройки безопасности.

7. 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. **16**).
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 меню настройки привязки.

4. Введите в строке ввода "0" и нажмите клавишу <Enter>.

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

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

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. [**3**]).

Для ограничения числа соединений:

1. Перейдите к меню настройки безопасности (см. стр. **16**).
2. Введите в строке ввода номер команды "Ограничение числа 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 меню настройки безопасности.

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. **16**).
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 меню настройки безопасности.
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. **16**).
2. Введите в строке ввода номер команды "Настройка параметров 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. **16**).
2. Введите в строке ввода номер команды "Разрешение прохождения пакетов с IP-опциями" и нажмите клавишу <Enter>.

   На экране появится сообщение:

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

   Затем на экране появится меню настройки безопасности, в котором содержание команды настройки режима прохождения пакетов с IP-опциями изменится на противоположное.
3. Перейдите к настройке следующего параметра или выйдите из меню.

Для выключения режима:

1. Перейдите к меню настройки безопасности (см. стр. **16**).
2. Введите в строке ввода номер команды "Запрет прохождения пакетов с IP-опциями" и нажмите клавишу <Enter>.

   На экране появится сообщение:

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

   Затем на экране появится меню настройки безопасности, в котором содержание команды настройки режима прохождения пакетов с IP-опциями изменится на противоположное.
3. 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 ЦУС (см. стр. **49**).

Для включения/выключения режима:

1. Перейдите к меню настройки безопасности (см. стр. **16**).
2. Введите в строке ввода номер команды "Включение/ отключение программного контроля целостности" и нажмите клавишу <Enter>.

   На экране появится меню настройки безопасности.
3. Перейдите к настройке следующего параметра или выйдите из меню.

Дополнительные возможности

Команды дополнительного меню

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

Для перехода к дополнительному меню:

1. У сетевого устройства в рабочем режиме 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. стр. **37**).

   На экране появится дополнительное меню (см. Табл.1).

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.1 Команды дополнительного меню

Команда	Описание
Сведения об устройстве	Отображает на экране следующие сведения: • тип аппаратной платформы; • версия, контрольная сумма и конфигурация ПО; • идентификатор СУ; • статус мягкого режима (вкл/выкл); • ввод в эксплуатацию (да/нет). Если устройство входит в состав кластера, отображается статус – основной/резервный. Дополнительные сведения для ЦУС: • режим работы ЦУС в кластере (активный/пассивный); • дата и время последнего изменения БД ЦУС
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 с возможностью сохранения информации в файл и экспорта его на внешний носитель информации
Список правил NAT	Отображает на экране список всех правил NAT с возможностью сохранения информации в файл и экспорта его на внешний носитель информации
Вывести полный список интерфейсов	Отображает на экране список всех интерфейсов с возможностью сохранения информации в файл и экспорта его на внешний носитель информации
Вывести таблицы маршрутизации	Отображает на экране таблицы маршрутизации для протоколов IPv4 и IPv6 с возможностью сохранения информации в файл и экспорта его на внешний носитель информации
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 (см. Табл.2)
Перезагрузить	Запускает перезагрузку сетевого устройства
Выключить	Выключает электропитание сетевого устройства
Выход	Закрывает дополнительное меню

Табл.2 Команды меню "Диагностика"

Команда	Описание
Загруженность ЦП	Отображает на экране информацию о загруженности каждого процессора
Использование памяти	Отображает на экране общий, используемый 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

Команда	Описание
Выполнить traceroute*	Запускает на компьютере команду traceroute и отображает на экране результаты выполнения этой команды. Укажите IP-адрес, маршрут к которому требуется определить
Выполнить arp/ndp	Отображает на экране содержимое ARP- и NDP-кеша с возможностью сохранения результатов в файл и экспорта его на внешний носитель информации
Сведения о сетевых соединениях	Отображает на экране сведения об открытых сетевых соединениях с возможностью сохранения информации в файл и экспорта его на внешний носитель информации
Сведения о работе шифратора	Статистическая информация о работе шифратора с возможностью ее сохранения в файл и экспорта его на внешний носитель информации
Просмотр дампа сетевого трафика	Отображает на экране информацию о сетевом трафике. Для запуска команды задайте имя тестируемого интерфейса, фильтр в формате команды tcpdump и количество пакетов для просмотра. Есть возможность сохранения результатов в файл и экспорта его на внешний носитель информации. Для сетевого устройства, выведенного из эксплуатации, предусмотрено сохранение информации в двоичном коде для последующего просмотра в специализированном приложении
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. Файл отчета получит имя debug_report_DDMMYYYY_HHMMSS.dump, где DDMMYYYY_HHMMSS - дата и время его создания
Сохранить отладочные журналы	Выгрузка информации системных журналов на USB-флеш-накопитель в файл syslog
Командная строка	Переход в режим командной строки (Continent Shell). Выход по команде exit
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.

Автоматическое 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 автовыключения:

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.

Глава 2
Программа управления ЦУС

Централизованное управление сетевыми устройствами осуществляется с помощью программы управления, устанавливаемой на одном или нескольких компьютерах, находящихся в защищенном сегменте сети (РМ администратора). Программа управления устанавливает защищенное соединение с ЦУС и позволяет в диалоговом режиме контролировать все сетевые устройства, а также редактировать данные, содержащиеся в базе данных ЦУС. Работа программы управления возможна только при предъявлении идентификатора администратора комплекса.

Внимание! Для корректной работы с ключевыми носителями Рутокен, Рутокен ЭЦП в настройках ОС Windows необходимо запустить системную службу "Смарт-карты", предварительно установив тип запуска – "Авто".

Запуск программы

При запуске ПУ ЦУС осуществляется аутентификация администратора. Аутентификация выполняется в соответствии с политикой, заданной по умолчанию или измененной главным администратором комплекса (настройка параметров политики аутентификации приводится на стр. **37**).

Для запуска программы управления:

1. Активируйте на рабочем столе ярлык программы управления ЦУС или нажмите на панели задач кнопку "Пуск" и активируйте в главном меню Windows команду "Программы | Код Безопасности | Континент 3.9 | Программа управления ЦУС (ПУ ЦУС)".

   На экране появится запрос идентификатора администратора.

2. Предъявите идентификатор администратора.

   На экране появится запрос пароля для расшифровки ключей администратора.

3. Введите пароль и нажмите кнопку "ОК".

   При успешном чтении служебной информации с идентификатора программа управления установит защищенное соединение с ЦУС и агентом, загрузит данные, необходимые для ее работы, и отобразит на экране главное окно (см. стр. **28**).

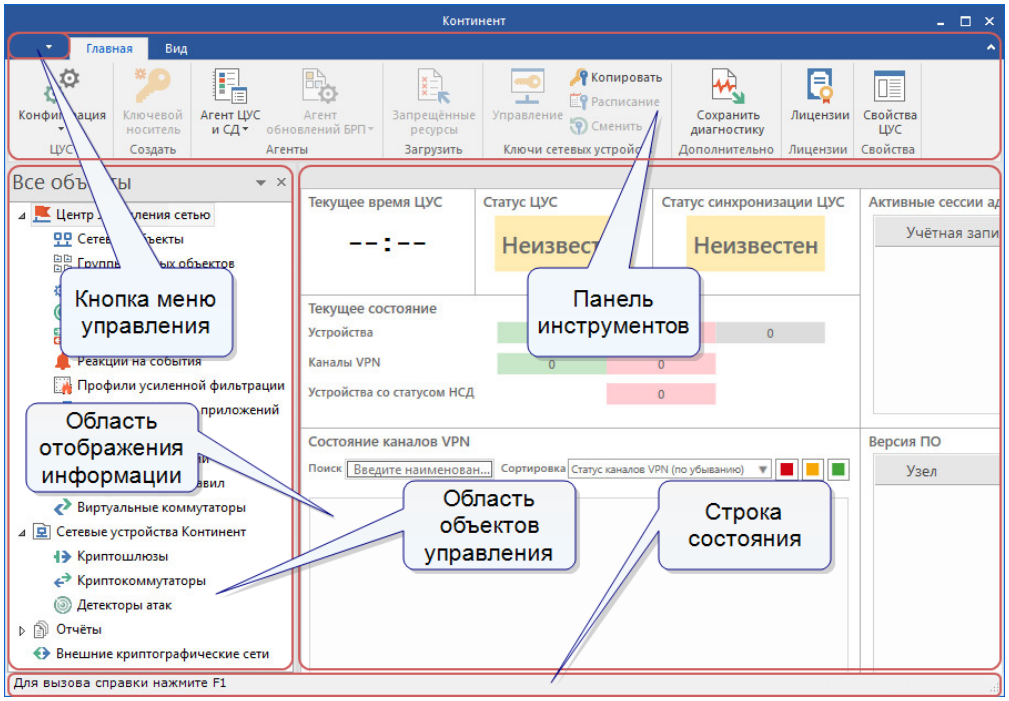
   Если носитель испорчен или не содержит административного ключа, соединение с ЦУС установлено не будет и на экране появится сообщение об ошибке. В этом случае закройте окно сообщения и повторите процедуру запуска с надлежащим носителем.

   Совет. Если при установлении соединения произошел сбой и на экран выведено сообщение о невозможности соединения с ЦУС, проверьте работоспособность ЦУС и повторите попытку соединения с ним еще раз. Сообщение об ошибке может содержать техническую информацию для разработчиков. При обращении в службу технической поддержки необходимо представить снимок экрана с сообщением или полный текст сообщения, включая техническую информацию.

Интерфейс программы

Главное окно

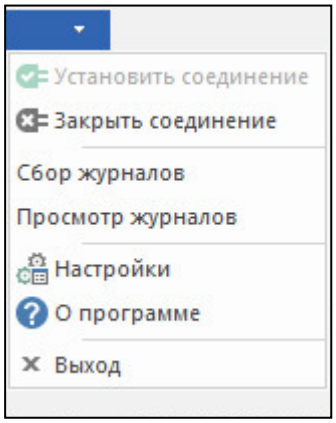
После того как соединение программы управления с ЦУС успешно установлено и необходимые данные из базы данных ЦУС загружены, на экране появится главное окно программы управления.



В главном окне отображаются характеристики зарегистрированных объектов, а также сведения об их текущем состоянии.

В верхней части главного окна на модульной ленте расположена панель инструментов. Она представляет собой набор функциональных кнопок, предназначенных для вызова часто выполняемых задач. Статус "доступности" и тип кнопок изменяется в зависимости от ситуации (активный раздел меню, наличие элементов, права пользователя и т. п.), в которой в данный момент ведется работа. Каждая кнопка имеет название на русском языке, поясняющее ее функционал. При наведении курсора мыши на кнопку появится всплывающая подсказка, содержащая дополнительную информацию о выполняемой команде.

В левом верхнем углу панели управления расположена кнопка вызова меню управления. В нем присутствуют команды управления соединением с ЦУС, работы с журналами, настройки текущего соединения с ЦУС и общая информация о версии ПУ ЦУС.



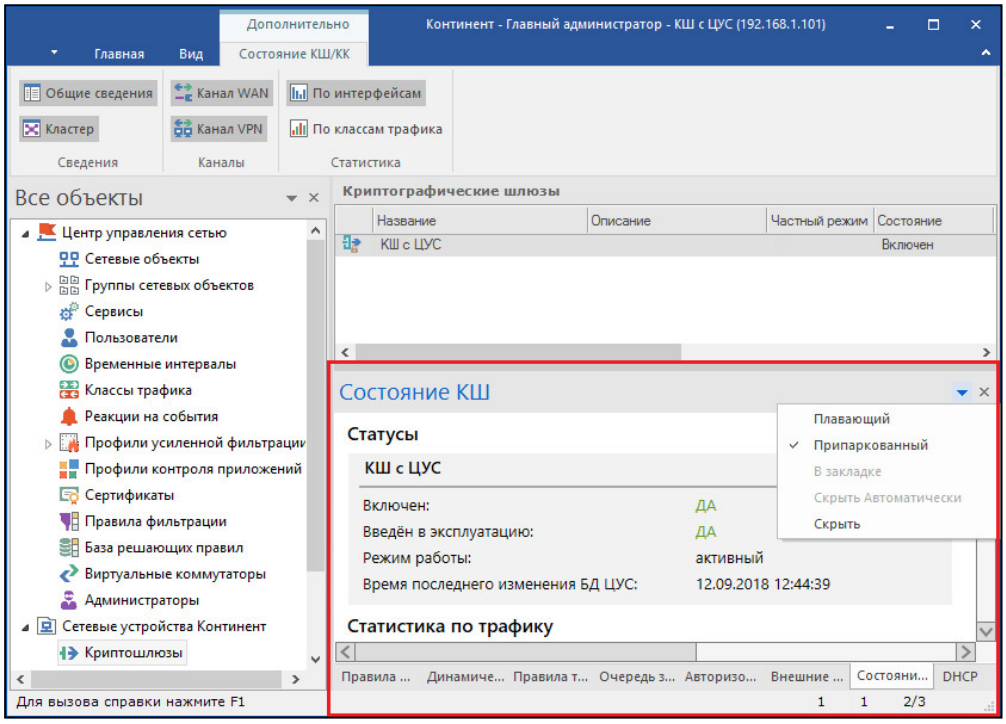
Выбор отображаемой в главном окне информации осуществляется в области объектов управления. По умолчанию область объектов расположена в левой части главного окна. В ней отображается иерархический список объектов, часть которых сгруппирована по тематическим разделам. Список объектов управления ЦУС представлен в Табл.3. Также в отдельные разделы выделены сетевые устройства Континент (см. стр. **42**), отчеты (см. [**5**]) и внешние криптографические сети (см. [**4**]).

В правой части главного окна ПУ ЦУС расположена область отображения информации активного объекта управления. Данная область может содержать как

совокупность структурированных данных, представляемых в виде списков, таблиц и графиков, так и различные функциональные элементы (дополнительные кнопки, активные поля и т. п.). Табличные данные часто имеют свое контекстное меню, вызываемое щелчком правой кнопки мыши, часть команд которого дублирует команды панели инструментов. Для сортировки отображаемой информации по возрастанию/убыванию одного из параметров нажмите на соответствующий заголовок столбца. Двойной щелчок левой кнопки мыши обычно приводит к вызову свойств элемента, аналогично нажатию кнопки "Свойства" на панели инструментов.

Сведения о некоторых выбранных объектах отображаются на вкладках дополнительного окна. По умолчанию дополнительное окно расположено в нижней части области отображения информации.

Примечание. Некоторые активные вкладки дополнительного окна создают дополнительные вкладки на панели инструментов, на которых расположены наборы соответствующих функциональных кнопок, предназначенных для вызова часто выполняемых задач.



Управление объектами осуществляют с помощью кнопок панели инструментов, а также команд контекстного меню.

Внизу главного окна расположена строка состояния, в которой можно в реальном времени посмотреть количество случаев НСД, проблемных кластеров и сетевых устройств Континент.

Табл.3 Объекты раздела "Центр управления сетью"

Объект	Описание
Сетевые объекты	Содержат списки соответствующих элементов правил фильтрации IP-пакетов и трансляции сетевых адресов (см. [**3**])
Группы сетевых объектов	
Сервисы	
Временные интервалы	
Пользователи	Список зарегистрированных пользователей и групп пользователей. Группы пользователей используют в правилах фильтрации IP-пакетов и трансляции сетевых адресов для более тонкой настройки доступа сотрудников к ресурсам

Объект	Описание
Классы трафика	Справочник классов трафика (используются для гибкого управления трафиком)
Реакции на события	Список автоматических реакций агента ЦУС на события
Профили усиленной фильтрации	Список профилей, используемых для дополнительной фильтрации трафика на уровне прикладных протоколов (см. [**3**])
Профили контроля приложений	
Сертификаты	Список собственных сертификатов открытых ключей, зарегистрированных в комплексе. Эти сертификаты предназначены для установления защищенного соединения с внешними криптографическими сетями
Правила фильтрации	Список всех правил фильтрации IP-пакетов, установленных администратором (см. [**3**])
База решающих правил	Список групп загруженных в БД ЦУС решающих правил
Виртуальные коммутаторы	Список виртуальных коммутаторов, используемых для управления криптографической коммутируемой сетью (см. [**4**])
Администраторы	Список учетных записей администраторов комплекса (см. стр. **37**)

Настройка интерфейса

Настройка интерфейса программы управления ЦУС осуществляется с помощью технологии drag- and- drop, кнопок управления областями и вкладками дополнительного окна. Часть этих функций представлена в виде кнопок на вкладке "Вид" панели инструментов.

В правом верхнем углу области объектов управления и вкладок дополнительного окна находятся кнопки управления, с помощью которых можно настроить их отображение:

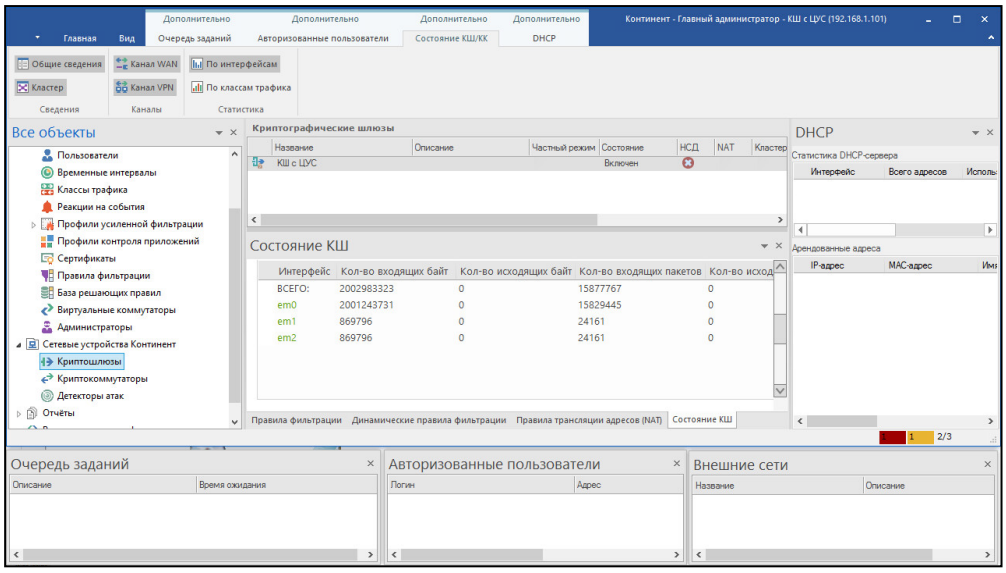
Кнопка/ команда меню	Описание действия
	Вызов меню управления
Плавающий	Отображение в виде дополнительного окна Windows, которое можно переместить или изменить размеры стандартными средствами. Для управления окном также используется контекстное меню заголовка окна, дублирующее стандартное меню управления. Быстрый переход в припаркованный режим осуществляется двойным щелчком мыши по заголовку окна
Припаркованный	Отображение в определенной части области отображения информации (вверху, внизу или по бокам). Этот вариант используется по умолчанию
 или Скрыть	Активная вкладка или область перестает отображаться до смены объекта управления ЦУС

Местоположение границ областей и вкладок можно изменять с помощью мыши.

Область объектов управления и каждую вкладку дополнительного окна можно переместить в отдельную область (припаркованный режим) или окно (плавающий режим), используя технологию drag-and-drop. Контактными зонами являются заголовок области и название вкладки. При перемещении на экране отображаются дополнительные кнопки автоматической пристыковки к нижней, верхней или боковой стороне области отображения информации.

Примечание. Местоположение обособленных вкладок сохраняется для каждого типа объектов

управления.



Для перевода в припаркованный режим по технологии drag-and-drop:

- Наведите курсор мыши на контактную зону вкладки, области или окна и нажмите левую кнопку мыши. Не отпуская кнопку, осуществите перенос к требуемой точке автоматической пристыковки. Отпустите кнопку мыши.

Для перевода в плавающий режим по технологии drag-and-drop:

- Наведите курсор мыши на контактную зону вкладки, области или окна и нажмите левую кнопку мыши. Не отпуская кнопку, осуществите перенос в требуемое место экрана. Отпустите кнопку мыши.

Для возврата обособленной вкладки в дополнительное окно:

- Наведите курсор мыши на контактную зону вкладки и нажмите левую кнопку мыши. Не отпуская кнопку, осуществите перенос к значку ❐ в центре дополнительного окна. Отпустите кнопку мыши.

Для возврата к первоначальным настройкам:

- Нажмите кнопку "Восстановить представления по умолчанию" на вкладке "Вид" панели инструментов, затем нажмите кнопку "Да" на появившемся окне подтверждения. Осуществите перезапуск программы управления ЦУС.

Для быстрого вызова области объектов управления:

- Перейдите на вкладку "Вид" панели инструментов и нажмите кнопку "Объекты управления".

Для быстрого перехода к вкладке:

- Перейдите на вкладку "Вид" панели инструментов и нажмите кнопку выбора вкладки. Установите отметку в соответствующем поле.

Управление таблицами

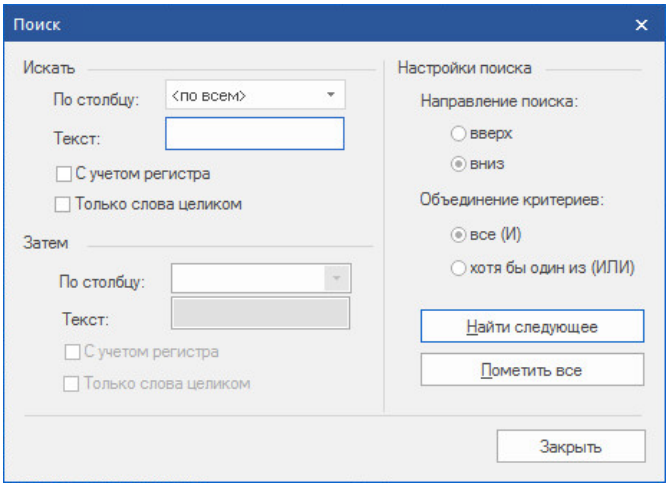
Сведения о выбранном объекте управления обычно представлены в области отображения информации в табличном виде. Программа управления снабжена удобным инструментарием для работы с таблицами:

- поиск нужной записи;
- отбор (фильтрация);
- сортировка записей;
- перемещение столбцов;
- выбор отображаемых полей.

Для поиска нужной записи:

1. Нажмите на панели инструментов кнопку "Найти" или в контекстном меню таблицы выберите пункт "Поиск...".

   На экране появится окно "Поиск".

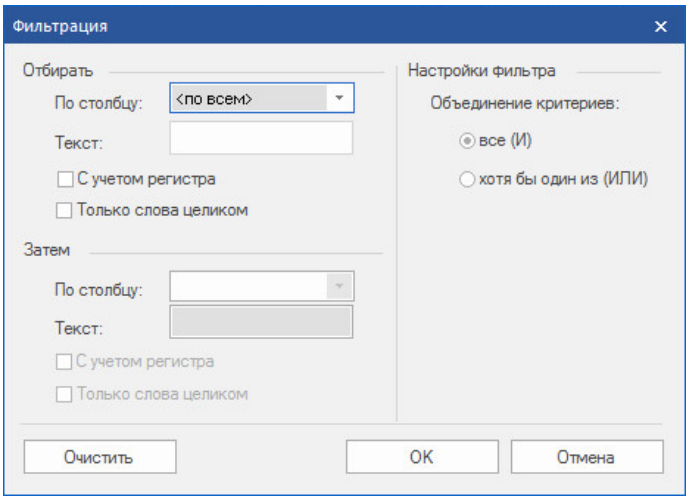


2. В полях окна укажите условия поиска.
3. Для поиска нужных записей нажмите одну из кнопок:
   - "Найти следующее" — для поиска очередной записи, удовлетворяющей заданным условиям;
   - "Пометить все" — для выделения всех записей, удовлетворяющих заданным условиям.
4. Нажмите кнопку "Закрыть" после завершения процедуры поиска.

Для фильтрации записей:

1. Нажмите на панели инструментов кнопку "Фильтр" или в контекстном меню таблицы выберите пункт "Фильтрация списка...".

   На экране появится окно "Фильтрация".



2. Определите критерии отбора.
3. Нажмите кнопку "OK" для выполнения фильтрации.

   Окно закроется, а в таблице будут отображены только те записи, которые удовлетворяют заданным условиям отбора.
4. Для отключения фильтрации нажмите на панели инструментов кнопку "Очистить".

Для сортировки записей:

- Наведите курсор мыши на заголовок столбца и нажмите левую кнопку мыши.

Список будет отсортирован по данному полю в алфавитном порядке. Повторное нажатие кнопки мыши изменяет порядок сортировки. Текущее направление сортировки обозначается значками и соответственно.

Для перемещения столбцов:

- Наведите курсор мыши на заголовок перемещаемого столбца и нажмите левую кнопку мыши. Не отпуская кнопку, перетащите поле в нужное место. Отпустите кнопку. Столбец займет указанное место.

Настройка программы

Настройка программы осуществляется с помощью команд меню "ЦУС" и заключается в настройке параметров соединения с ЦУС и агентом, а также в выборе режима идентификации администратора.

Настройка параметров соединения с ЦУС

Внимание! Чтобы измененные параметры вступили в силу, необходимо разорвать соединение программы управления с ЦУС и заново установить его.

Для настройки параметров соединения с ЦУС:

1. В контекстном меню раздела "Центр управления сетью" выберите пункт "Параметры соединения с ЦУС...".

   На экране появится одноименное окно.

2. Заполните поля окна:

IP-адрес	IP-адрес того интерфейса ЦУС, который подключен к сегменту сети, содержащему данный компьютер
Время ожидания соединения, сек.	Время ожидания соединения в секундах (от 10 до 600 сек.)
Считыватель ключей	Устройство для считывания ключа администратора ЦУС. Список содержит названия тех устройств идентификации, драйверы которых установлены на компьютере

3. Нажмите кнопку "ОК".

Настройка параметров соединения с агентом

Для настройки параметров соединения с агентом:

1. В контекстном меню раздела "Центр управления сетью" выберите пункт "Параметры соединения с агентом ЦУС и СД...".

   На экране появится одноименное окно.

2. Заполните поля окна:

IP-адрес	IP-адрес компьютера, на котором установлен агент. Если агент и программа управления установлены на одном и том же компьютере — IP-адрес данного компьютера или 127.0.0.1
Время ожидания соединения, сек.	Время ожидания соединения в секундах (от 10 до 600 сек.)

3. Нажмите кнопку "ОК".

Программа управления устанавливает соединение с агентом автоматически каждый раз, когда это необходимо, поэтому никакие дополнительные действия после изменения параметров соединения не требуются.

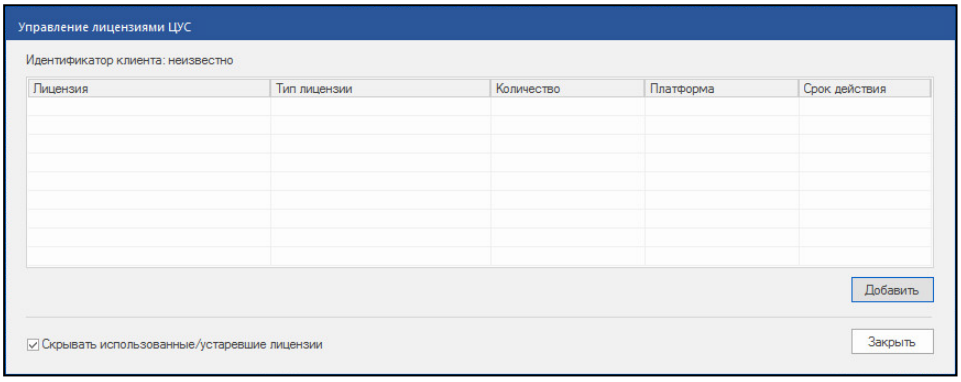
Дальнейшие действия по настройке соединения с агентом описаны в [**5**].

Управление лицензиями

Ограничения на параметры ЦУС определяются приобретенными лицензиями. Управление лицензиями осуществляют в ПУ ЦУС.

Для добавления лицензии:

1. При отсутствии лицензий при запуске ПУ ЦУС окно "Управление лицензиями ЦУС" появляется автоматически после прохождения процедуры аутентификации. Это окно также можно вызвать посредством кнопки "Лицензии" на панели инструментов при выборе раздела "Центр управления сетью" в области навигации ПУ ЦУС.



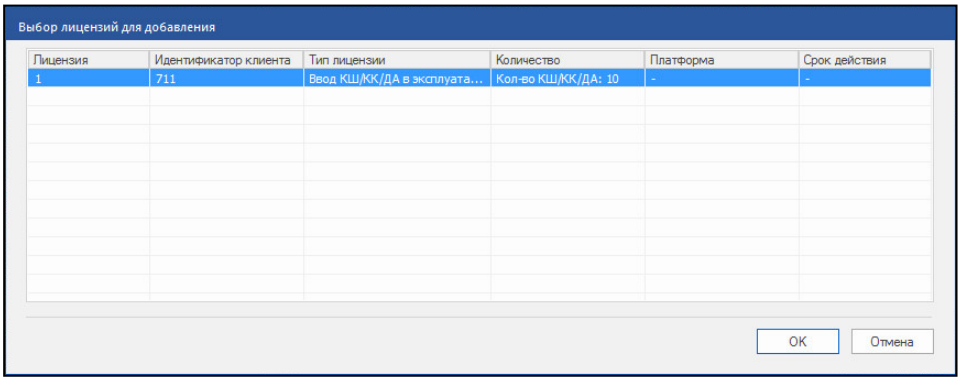
Примечание. Лицензии, зарегистрированные в более ранних версиях комплекса, отображаются в списке с отметкой "Ввод КШ<устройства> в эксплуатацию". При этом действие таких лицензий сохраняется.

2. Для добавления лицензии нажмите кнопку "Добавить".

   Появится окно ОС Windows для открытия файла.

3. Укажите местонахождение и имя файла лицензии и нажмите кнопку "Открыть".

   Появится окно "Выбор лицензий для добавления".



4. Выберите требуемую лицензию и нажмите кнопку "ОК".

   При успешном добавлении лицензии ее серийный номер и краткая характеристика появится в списке зарегистрированных лицензий. При ошибке на экране появляется соответствующее сообщение.

5. Нажмите кнопку "Закрыть" для выхода в главное окно ПУ ЦУС.

Завершение работы

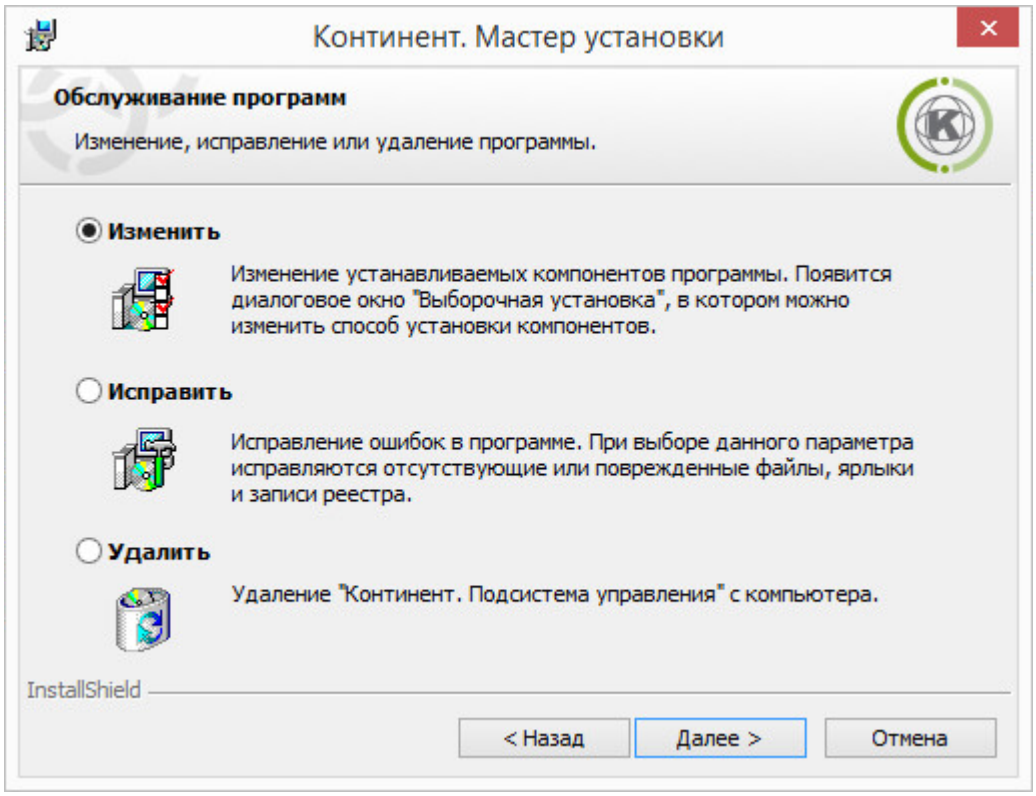
Для завершения работы с ПУ ЦУС активируйте в меню управления команду "Выход". При этом защищенное управляющее соединение программы с ЦУС будет разорвано, а основное окно программы исчезнет с экрана.

Переустановка, исправление и удаление

Перед выполнением обновления, переустановки или удаления (далее — обслуживания) обязательно завершите работу программы управления, иначе появится сообщение с предложением закрыть программу управления в ходе установки.

Обслуживание агента, установленного с программой управления на одном компьютере, осуществляется автоматически при выполнении этих процедур над программой управления.

Обслуживание ПУ ЦУС выполняют аналогично процедуре установки ПУ ЦУС, приведенной в [**2**]. Вместо окна выбора варианта установки будет отображено окно обслуживания программы:



Для обслуживания ПУ ЦУС:

1. Установите отметку в требуемом поле и нажмите "Далее >".
2. Выполните дальнейшие пункты процедуры установки подсистемы управления.

Примечание. Удалить ПУ ЦУС можно также средствами ОС Windows.

Глава 3
Организация работы администраторов комплекса

Политика аутентификации администраторов

Параметрами политики аутентификации администраторов при запуске ПУ ЦУС являются:

- минимальная длина пароля;
- количество неудачных попыток входа до блокировки;
- время блокировки при превышении количества неудачных попыток входа;
- контроль слабых паролей (т. е. пароль должен содержать буквы верхнего и нижнего регистра, цифры и специальные символы, при этом любой символ не должен повторяться более 2 раз).

Настройка параметров выполняется главным администратором комплекса. Остальным администраторам параметры политики доступны только для просмотра.

Внимание! Политика аутентификации распространяется на вход в локальное меню сетевого устройства.

Для просмотра и настройки политики аутентификации:

1. В области объектов управления ПУ ЦУС вызовите контекстное меню раздела "Центр управления сетью" и выберите пункт "Свойства".

   Появится окно "Свойства ЦУС".

2. Выберите пункт "Политика аутентификации".

   В правой части окна отобразятся значения параметров политики аутентификации.

3. Установите значения параметров и нажмите кнопку "ОК".

Управление учетными записями администраторов

После установки комплекс будет содержать только одну учетную запись администратора ЦУС — "Встроенный администратор". Этой учетной записи присвоена роль "Главный администратор", обеспечивающая полные права на администрирование комплекса.

Идентификатор администратора, предназначенный для идентификации главного администратора, создается при инициализации ЦУС. Идентификатор содержит служебную информацию, необходимую для запуска программы управления.

Помимо учетных записей администраторов ЦУС можно создавать учетные записи локальных администраторов сетевых устройств комплекса. Этот тип учетной записи обладает полными правами на локальное управление набором сетевых устройств, включая опциональное удаленное управление по протоколу SSH.

Главный администратор может назначать других администраторов, наделенных ограниченными правами на администрирование комплекса. Список ролей администраторов и соответствующих им прав представлен на стр. **90**. При добавлении новой учетной записи создается идентификатор данного администратора.

Для просмотра списка зарегистрированных администраторов:

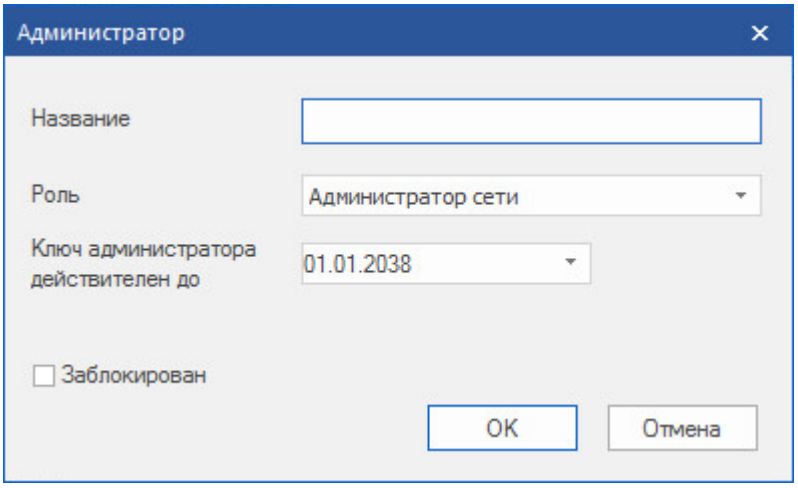
- Выберите в области объектов управления пункт "Центр управления сетью | Администраторы".

В области отображения информации появится список зарегистрированных администраторов.

Для создания учетной записи администратора ЦУС:

1. Выберите в области объектов управления пункт "Центр управления сетью | Администраторы" и нажмите кнопку "Администратор" на панели управления.

На экране появится одноименное окно.



2. Заполните поля и нажмите кнопку "OK".

Название	Имя администратора (не более 59 символов)
Роль	Наименование роли. Роль определяет права администратора на администрирование системы. Список ролей и соответствующих им прав представлен на стр. **90**
Ключ администратора действителен до	Срок действия данной учетной записи. Максимальный срок действия учетной записи — до 01.01.2038
Заблокирован	При наличии отметки запуск программы управления и агента данным администратором невозможен

На экране появится запрос пароля для шифрования ключа администратора.

3. Введите пароль и нажмите кнопку "OK".

На экране появится окно "Параметры соединения".

4. Выберите в раскрывающемся списке чистый носитель для сохранения административного ключа и нажмите кнопку "OK".

В случае если нужный носитель не был подключен, подключите его и нажмите кнопку  .

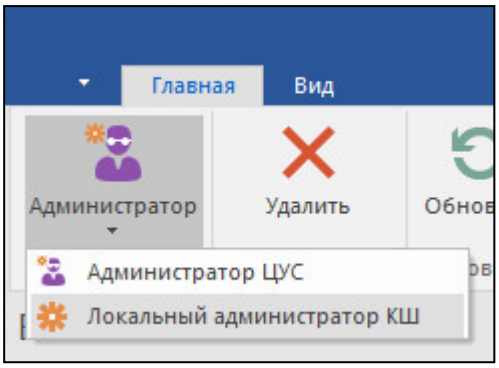
Примечание. Список содержит названия тех устройств идентификации, драйверы которых установлены на компьютере.

После успешного завершения записи ключевой информации на носитель список администраторов на экране дополнится соответствующей записью.

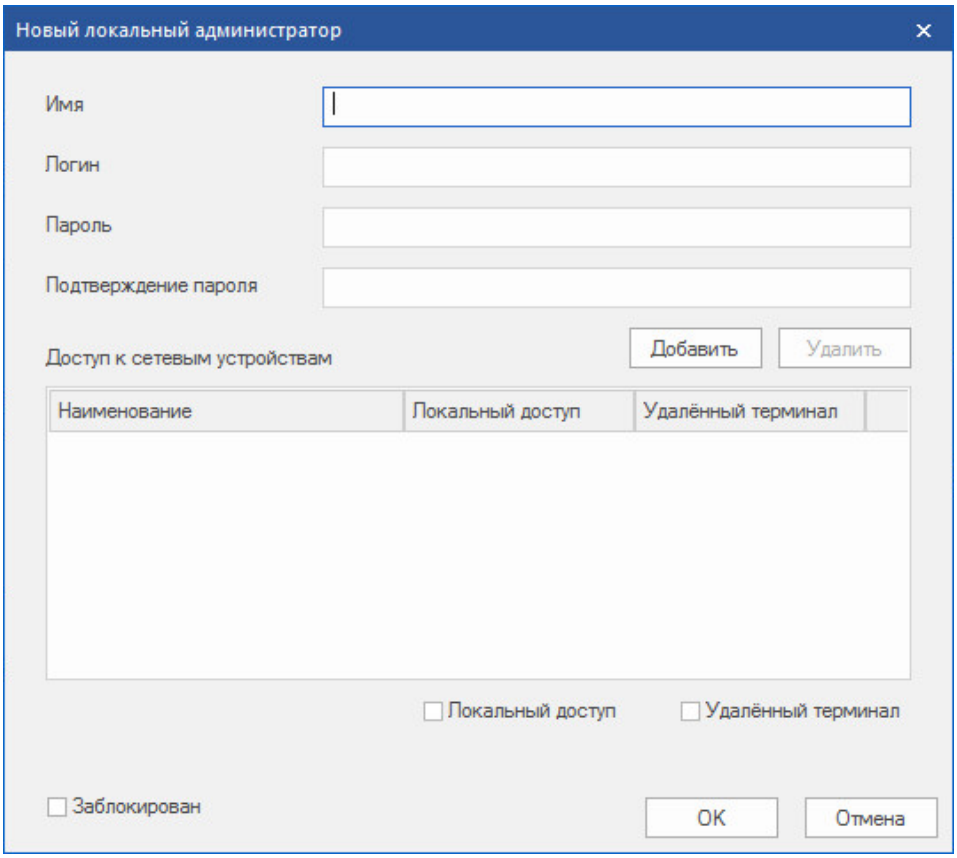
Для создания учетной записи локального администратора КШ:

1. Выберите в области объектов управления пункт "Центр управления сетью | Администраторы" и в раскрывающемся списке кнопки "Администратор" на

панели управления выберите команду "Локальный администратор КШ".



На экране появится окно создания новой учетной записи.



2. Заполните поля и нажмите кнопку "OK".

Имя	Имя администратора (не более 59 символов)
Логин	Имя учетной записи администратора, содержащее буквы латинского алфавита в нижнем регистре, цифры или символы -_
Пароль Подтверждение пароля	Пароль длиной не менее 6 символов, содержащий знаки как минимум двух из трех категорий: • буквы латинского алфавита; • цифры от 0 до 9; • символы !@$%&?
Доступ к сетевым устройствам	Список сетевых устройств, к управлению которыми имеет доступ администратор. Для добавления сетевых устройств нажмите кнопку "Добавить", затем, используя клавиши "Ctrl" и "Shift", выберите требуемое в списке устройств и нажмите кнопку "OK". Для удаления сетевого устройства выберите его в списке и нажмите кнопку "Удалить"

Локальный доступ	При наличии отметки администратору разрешен доступ к локальному управлению устройством
Удаленный терминал	При наличии отметки администратору разрешен доступ к удаленному управлению устройством по протоколу SSH
Заблокирован	При наличии отметки запуск программ управления администратором невозможен

После успешного выполнения операции на экране список учетных записей администраторов дополнится соответствующей записью.

Для управления учетной записью администратора:

Примечание. Если в системе зарегистрирован единственный действующий администратор с правами главного администратора, изменить, блокировать или удалить его учетную запись невозможно.

1. Выберите в списке нужную учетную запись администратора.
2. Для изменения нажмите на панели инструментов кнопку "Свойства", внесите изменения в параметрах учетной записи и нажмите кнопку "ОК".
3. Для блокировки нажмите на панели инструментов кнопку "Свойства", установите отметку в поле "Заблокирован" и нажмите кнопку "ОК".
4. Для удаления нажмите на панели инструментов кнопку "Удалить" и нажмите кнопку "Да" в появившемся окне подтверждения.

Смена административного ключа

Смена ключей осуществляется периодически в соответствии с требованиями политики безопасности предприятия, а также при утере носителя с административным ключом.

При записи административного ключа на новый носитель старый административный ключ становится недействительным.

Для смены ключа:

1. Выберите в списке необходимую учетную запись администратора.
2. Вызовите контекстное меню и активируйте команду "Сменить ключ".

   На экране появится запрос для подтверждения обновления ключа.
3. Нажмите кнопку "Да".

   На экране появится окно для ввода пароля.
4. Введите пароль для шифрования ключей и нажмите кнопку "ОК".

   На экране появится окно для определения параметров соединения.
5. Выберите в раскрывающемся списке носитель для сохранения нового административного ключа.

   В случае если нужный носитель не был подключен, подключите его и нажмите кнопку  .

   После успешного завершения записи ключевой информации на носитель на экране появится соответствующее информационное сообщение. Закройте окно сообщения.

Копирование административного ключа

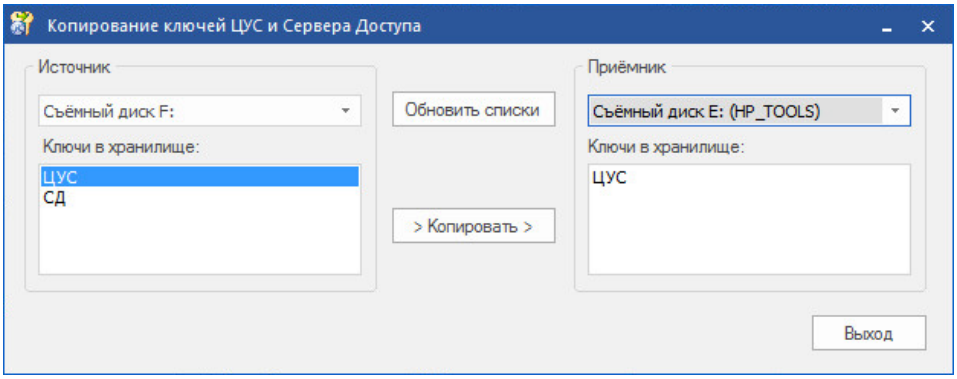
Данная процедура позволяет создать дубликат административного ключа, с помощью которого осуществляется идентификация администратора. Программа копирования ключей является одним из компонентов подсистемы управления и устанавливается на компьютер с установочного диска совместно с другими компонентами.

Примечание. Ключевой носитель может содержать только один ключ ЦУС.

Для копирования ключа:

1. Предъявите носитель с ключом и носитель для записи дубликата.
2. Нажмите на панели задач кнопку "Пуск" и выберите в главном меню Windows пункт "Программы | Код Безопасности | Программа копирования ключей".

   На экране появится окно "Копирование ключей ЦУС и сервера доступа".



3. Выберите из раскрывающихся списков:
   - в группе полей "Источник" — название устройства, с которого будет копироваться ключ;
   - в группе полей "Приемник" — название устройства, на которое будет копироваться ключ.

   Примечание. Списки содержат названия тех устройств идентификации, драйверы которых установлены на компьютере. Для обновления списков используйте кнопку "Обновить списки".

   В поле "Ключи в хранилище" отобразится список ключей, хранящихся на данном носителе.
4. В поле "Ключи в хранилище" группы полей "Источник" выберите ключи для копирования и нажмите кнопку "> Копировать >".

   Выбранные ключи будут скопированы на новый носитель, и список скопированных ключей отобразится в поле "Ключи в хранилище" группы полей "Приемник".
5. Закройте окно программы с помощью кнопки "Выход".

Глава 4
Централизованное управление сетевыми устройствами

Управление сетевым устройством

Развертывание сетевого устройства описано в [**2**]. Дальнейшее управление устройством возможно как локально, с ограниченным функционалом, так и с помощью программы управления, с полным набором настроек.

Ввод сетевого устройства в эксплуатацию осуществляется после его инициализации и подключения. Вывод из эксплуатации требуется для выполнения некоторых настроек.

Пока сетевое устройство не введено в эксплуатацию, для него не могут быть установлены парные связи. При этом в программе управления такое сетевое устройство отображается с соответствующим статусом.

Программа управления позволяет дистанционно проводить перезагрузку и выключение сетевых устройств. Перезагрузка автоматически выполняется при обнаружении сбоев в работе программного обеспечения сетевого устройства.

Для ввода сетевого устройства в эксплуатацию/вывода сетевого устройства из эксплуатации:

1. В контекстном меню объекта с именем нужного устройства выберите пункт "Свойства...".

   На экране появится окно настройки свойств данного сетевого устройства.
2. Установите/удалите отметку в поле "Введен в эксплуатацию".
3. Нажмите кнопку "ОК".

Примечание. Данную операцию можно выполнить для группы сетевых устройств. Для этого выделите группу в списке, вызовите контекстное меню и выберите команду "Ввести в эксплуатацию" или "Вывести из эксплуатации".

Для удаления сетевого устройства:

Внимание! Запрещено удалять криптографический шлюз, на котором находится ЦУС.

1. Выберите в области объектов управления тип устройства, затем выберите в списке справа требуемый объект и нажмите на панели инструментов кнопку "Удалить".

   На экране появится запрос на подтверждение удаления.
2. Нажмите кнопку "Да" в окне запроса.

   На экране появится окно "Режимы удаления криптошлюза".

   Примечание. Окно отображается только в том случае, если существуют сетевые объекты, привязанные (см. [**6**]) к данному сетевому устройству. Если такие объекты отсутствуют, то сетевое устройство будет удалено сразу после подтверждения запроса.
3. Выберите режим удаления и нажмите кнопку "ОК".

Удалить объекты	Удаляет сетевые устройства, а также все сетевые объекты, привязанные к этому сетевому устройству
Снять привязку к объектам	Удаляет сетевое устройство. Сетевые объекты данного сетевого устройства сохраняются

Для перезагрузки сетевого устройства:

1. Выберите в области объектов управления тип устройства и нажмите кнопку "Перезагрузить" на панели инструментов.

Примечание. Возможен множественный выбор объектов.

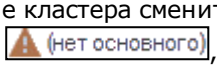
На экране появится запрос на перезагрузку сетевого устройства.

2. Нажмите кнопку "Да".

Для перезагрузки сетевых устройств в составе кластера резервирования:

1. Выберите в области объектов управления кластер и нажмите кнопку "Перезагрузить" на панели инструментов.

   На экране появится запрос на перезагрузку сетевого устройства.

2. Нажмите кнопку "Да".
3. Когда состояние кластера сменится на предупреждение об отсутствии в сети основного узла 

, нажмите кнопку "Перезагрузить" на панели инструментов.

   На экране появится запрос на перезагрузку сетевого устройства.

4. Нажмите кнопку "Да".

При перезагрузке сетевого устройства осуществляется проверка целостности файлов программного обеспечения и загрузочных секторов. Сведения о нарушении целостности этих объектов помещаются в журнал НСД данного сетевого устройства.

Для выключения сетевого устройства:

Внимание! После выключения сетевого устройства защищаемый им сегмент сети отключается от общей сети и связь с внешними и сторонними абонентами из этого сегмента становится невозможной.

1. Выберите в области объектов управления тип устройства и в контекстном меню требуемого объекта выберите пункт "Выключить <сетевое устройство>".

   Примечание. Возможен множественный выбор объектов.

   На экране появится запрос на выключение устройства.

2. Нажмите кнопку "Да".

Для обновления конфигурации сетевого устройства:

Примечание. Обновление конфигурации сетевого устройства требуется для согласования взаимодействия ЦУС с устройством в случае возникновения сбоев в работе программного обеспечения.

- Выберите в области объектов управления тип устройства, вызовите контекстное меню требуемого объекта и выберите пункт "Обновить конфигурацию...".

  По этой команде все настройки сетевого устройства будут приведены в соответствие настройкам, хранящимся в базе данных ЦУС. В течение интервала времени до обновления конфигурации на сетевом устройстве это сетевое устройство будет отображаться в списке с индикатором  .

Миграция на новую аппаратную платформу

При необходимости можно заменить аппаратную платформу ЦУС или сетевого устройства, например, более производительной.

Для проведения работ, связанных с переходом на новую аппаратную платформу, отличающуюся количеством и типами сетевых адаптеров от исходной, необходимо предварительно связаться со службой технической поддержки компании "Код Безопасности" и получить соответствующие инструкции.

Внимание! Самостоятельная замена аппаратной платформы запрещена.

Просмотр сведений о ПО сетевого устройства

В программе управления ЦУС можно просмотреть следующие сведения о ПО, установленном на сетевом устройстве:

- состояние программного обеспечения — наличие в БД ЦУС обновления ПО, готового для установки на данное сетевое устройство;
- текущая версия программного обеспечения, установленного на сетевом устройстве;
- контрольная сумма установленного программного обеспечения;
- аппаратная платформа;
- статус автозагрузки сетевого устройства (отключена или включена).

Примечание. Настройка автозагрузки сетевого устройства выполняется при локальном управлении средствами ПАК "Соболь".

Для просмотра сведений о сетевом устройстве:

1. Выберите в области объектов управления тип устройства, затем в списке справа выберите требуемый объект и нажмите кнопку "Свойства" на панели инструментов.

   На экране появится окно настройки свойств данного сетевого устройства.

2. Перейдите на вкладку "Версия ПО".

   На вкладке отобразятся сведения о сетевом устройстве.

Примечание. В нижней части вкладки расположена группа полей "Время загрузки ПО", предназначенная для загрузки файла обновления на данное сетевое устройство" (см. стр. 87).

Управление группой сетевых устройств

Сетевые устройства комплекса одного типа можно группировать и выполнять одновременную настройку ряда параметров.

Группа сетевых устройств

Для удобства управления сетевыми устройствами одного типа их можно объединять в группы. Посредством контекстного меню группы сетевых устройств выполняются следующие операции:

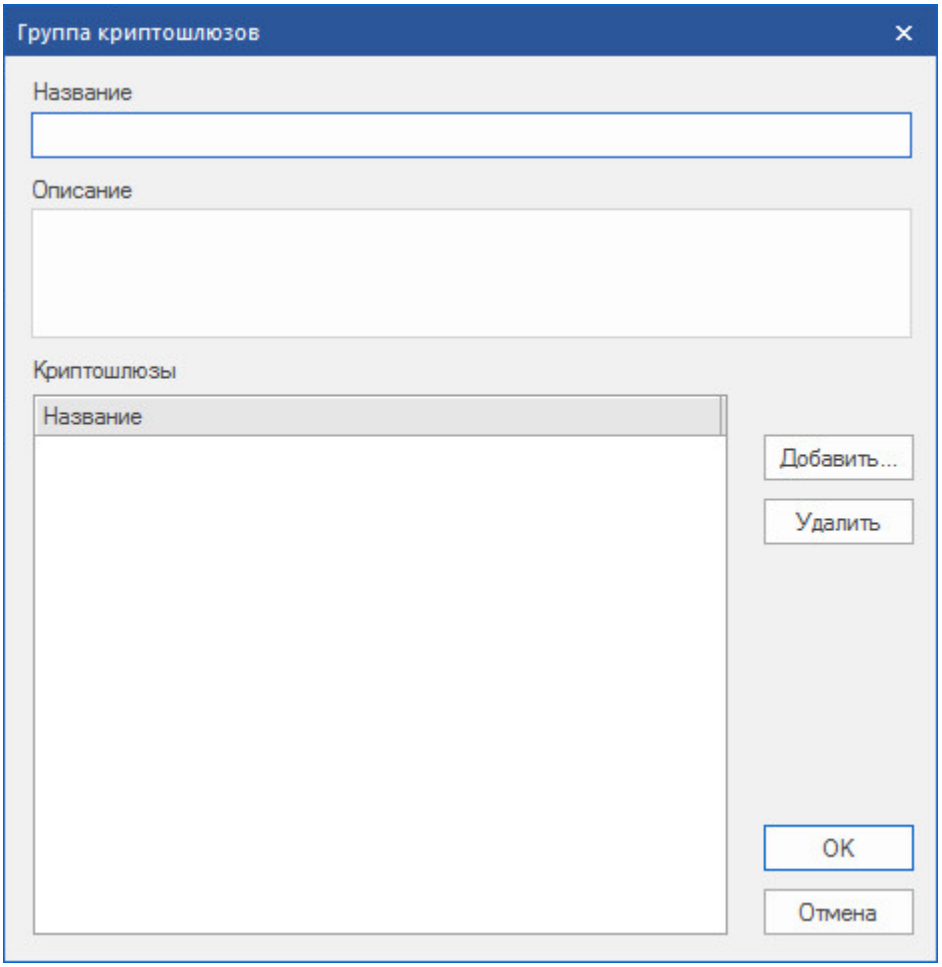
- Создание еще одной группы (см. ниже).
- Удаление группы (см. стр. 46).
- Смена ключей парной связи всех устройств группы (см. стр. 45).
- Просмотр свойств группы (см. стр. 45).

Управление составом сетевых устройств в группах осуществляется как в свойствах группы (см. стр. 45), так и в свойствах сетевого устройства (см. стр. 46).

Для создания группы сетевых устройств:

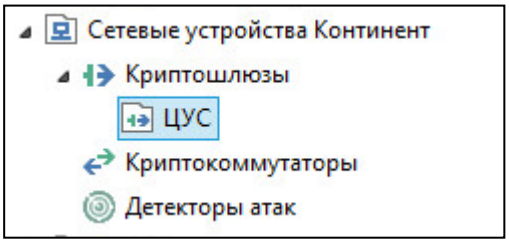
1. Выберите в области объектов управления требуемый тип устройства, затем нажмите кнопку создания группы сетевых устройств  на панели инструментов.

   На экране появится окно создания группы сетевых устройств.



2. Заполните поле названия и при необходимости описания группы.
3. Сформируйте список сетевых устройств группы, используя кнопки "Добавить..." и "Удалить".
4. Нажмите кнопку "ОК".

   На экране в области объектов управления появится новая группа сетевых устройств.



Для просмотра свойств группы сетевых устройств:

- Вызовите в области объектов управления контекстное меню группы сетевых устройств и выберите команду "Свойства...".

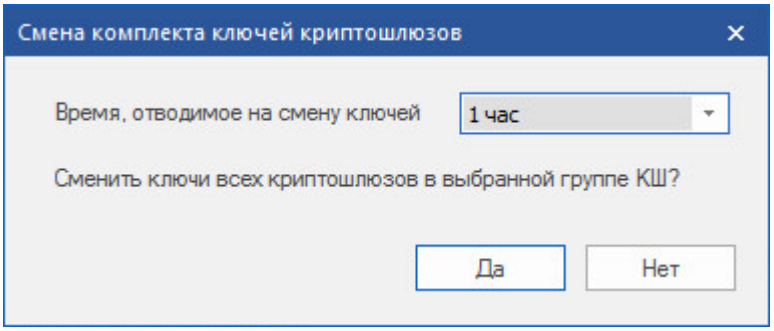
  На экране появится окно свойств группы <сетевых устройств> (см. выше).

Для смены ключей парной связи всех устройств группы:

Внимание! Запрещена групповая смена ключей в группе, в которой находится ЦУС.

1. Вызовите в области объектов управления контекстное меню группы сетевых устройств и выберите команду смены ключей.

   На экране появится окно смены комплекта ключей сетевых устройств.



2. Выберите время, отводимое на смену ключей, и нажмите кнопку "Да".

Для удаления группы сетевых устройств:

1. Вызовите в области объектов управления контекстное меню группы сетевых устройств и выберите команду ее удаления.

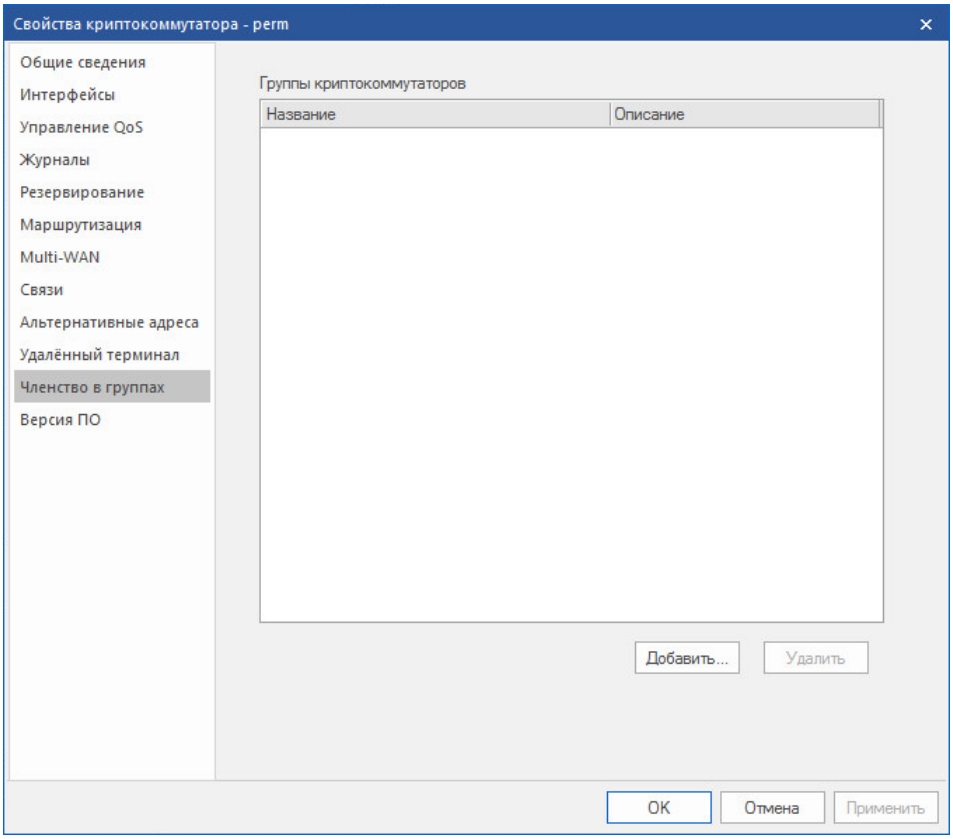
   На экране появится запрос на подтверждение удаления.
2. Нажмите кнопку "Да" в окне запроса.

Для управления размещением сетевого устройства в группах:

Примечание. Добавить сетевое устройство можно также в окне свойств группы (см. выше).

1. Выберите в области объектов управления требуемый тип устройства, затем в списке справа выберите требуемый объект и нажмите кнопку "Свойства" на панели инструментов.

   На экране появится окно свойств, открытое на вкладке "Общие сведения".
2. Перейдите на вкладку "Членство в группах".



   На экране появится список групп, в которых состоит сетевое устройство.
3. Для добавления устройства в состав группы нажмите кнопку "Добавить..." и выберите требуемую в списке имеющихся групп.

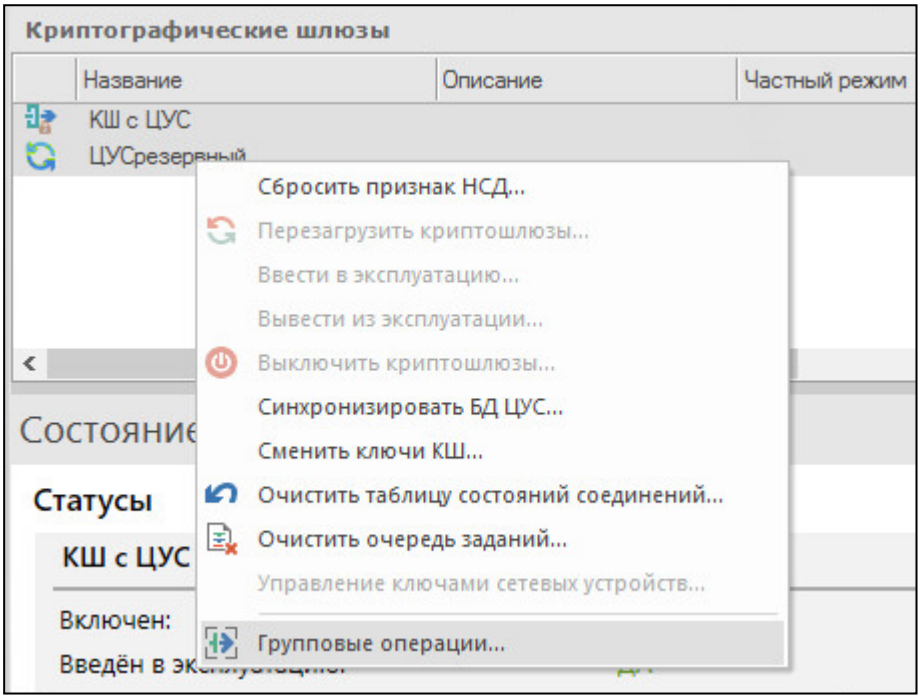
4. Для удаления устройства из состава группы выберите требуемую группу в списке и нажмите кнопку "Удалить".

Групповая настройка сетевых устройств

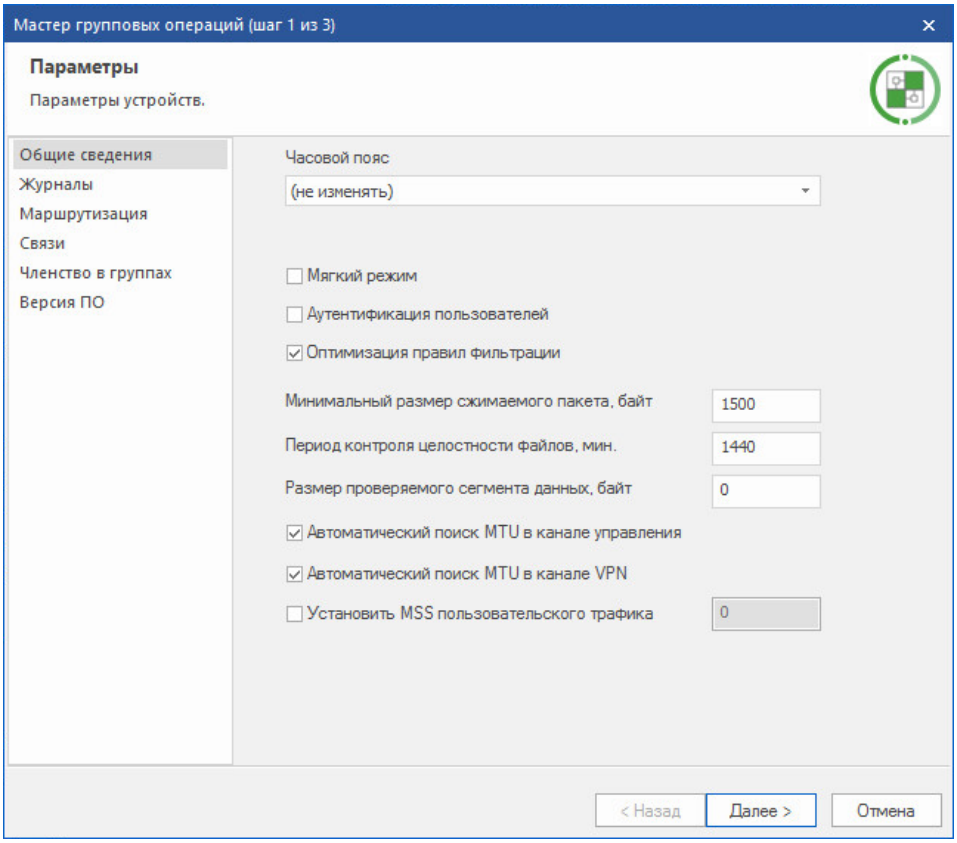
Настройку ряда параметров сетевых устройств можно выполнить сразу для группы сетевых устройств одного типа.

Для групповой настройки сетевых устройств:

1. Выберите в области объектов управления требуемый тип устройства, затем в списке справа выберите группу объектов, используя клавиши "Ctrl", "Shift" и управляющие клавиши клавиатуры или мышь. Вызовите контекстное меню и выберите команду "Групповые операции...".



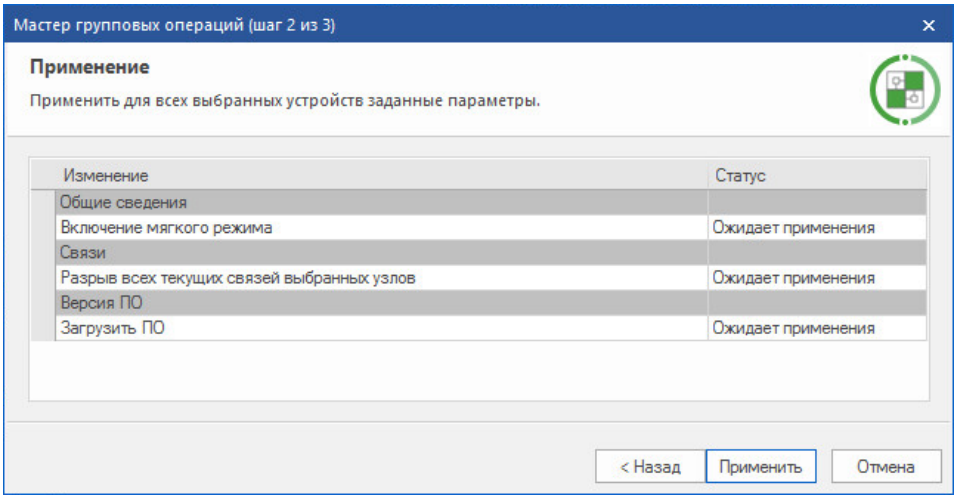
На экране появится окно мастера групповых операций, открытое на вкладке "Общие сведения".



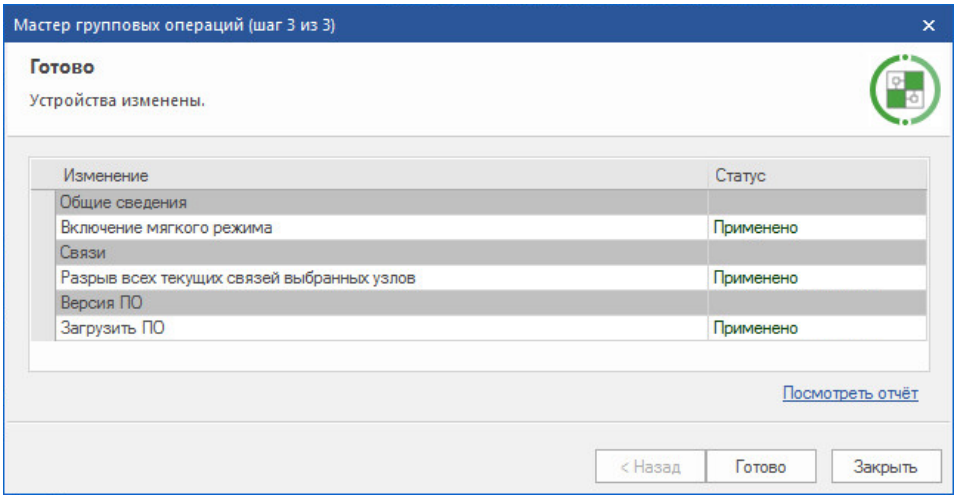
2. Проведите настройку требуемых параметров и нажмите кнопку "Далее>".

Вкладка	**Описание параметров**
Общие сведения	Стр. **49**
Журналы	Документ [**5**]
Членство в группах	Стр. **46**
Версия ПО	Стр. **86**

На экране появится окно "Применение" мастера групповых операций.



3. Проверьте список планируемых изменений и нажмите кнопку "Применить".
На экране появится завершающее окно мастера групповых операций.



4. При необходимости посмотреть и сохранить отчет нажмите ссылку "Посмотреть отчет".

   На экране появится окно приложения для просмотра текстовых документов с открытым в нем файлом отчета.

5. Для выхода из мастера групповых операций нажмите кнопку "Готово" или "Закрыть".

Настройка общих параметров сетевого устройства

Настройку общих параметров выполняют в окне свойств сетевого устройства.

Для настройки общих параметров:

1. Выберите в области объектов управления тип устройства, затем в списке справа выберите требуемый объект и нажмите кнопку "Свойства" на панели инструментов.

   На экране появится окно свойств сетевого устройства, открытое на вкладке "Общие сведения".

2. Внесите необходимые изменения в поля вкладки и нажмите кнопку "ОК".

Идентификатор	Информационное поле, отображающее заводской идентификационный номер сетевого устройства. Изменению средствами ПУ ЦУС не подлежит
Название	Имя сетевого устройства, под которым оно зарегистрировано в базе данных ЦУС и значится в списке объектов, отображаемом программой управления. Максимальная длина имени — 39 символов
Описание	Дополнительные сведения. Максимальная длина записи в этом поле — 79 символов
Частный режим	Установка отметки включает частный режим работы
Страна	Страна местонахождения устройства
Часовой пояс	Смещение часовой зоны региона, в котором эксплуатируется сетевое устройство, от UTC
Введен в эксплуатацию	При наличии отметки ЦУС устанавливает управляющее соединение с данным сетевым устройством, при отсутствии отметки — не устанавливает. Для КШ, на котором находится ЦУС, выключатель заблокирован
Мягкий режим	Установка отметки включает мягкий режим работы КШ, который предназначен для настройки устройства. В этом режиме нарушения правил фильтрации регистрируются в журнале НСД, однако IP-пакеты, не удовлетворяющие правилам фильтрации, не отбрасываются

Аутентификация пользователей	Только для КШ. При наличии отметки выполняется процедура аутентификации пользователей на данном КШ
Оптимизация правил фильтрации	Только для КШ. При наличии отметки ЦУС оптимизирует список правил фильтрации, загружаемых на сетевое устройство
Программный криптоускоритель	Установка отметки включает программный криптоускоритель при наличии соответствующей лицензии
Минимальный размер сжимаемого пакета	Размер IP-пакета в байтах, при превышении которого IP-пакеты подвергаются сжатию, если режим сжатия для данного сетевого устройства включен (см. [**6**]). IP-пакеты меньшего размера сжатию не подвергаются
Период контроля целостности файлов, мин.	Периодичность в минутах, с которой на сетевом устройстве осуществляется проверка целостности объектов, заданных шаблонами контроля целостности. Проверка осуществляется средствами программного обеспечения сетевого устройства. Сведения о результатах проверки сохраняются в журналах регистрации
Размер проверяемого сегмента данных	Только для КШ. Объем проверяемых данных в байтах, относящихся к одному соединению. В зависимости от задаваемого значения может составлять от доли пакета до нескольких пакетов
Автоматический поиск MTU в канале управления	Включение/отключение режима принудительной установки флага DF (Don't fragment) в канале управления. По умолчанию режим включен
Автоматический поиск MTU в канале VPN	Включение/отключение режима принудительной установки флага DF (Don't fragment) в канале VPN. По умолчанию режим включен
MSS пользовательского трафика	"Не менять" — значение MSS устанавливается автоматически. "Установить" — ввод вручную значения из диапазона 536-1408

Глава 5
Управление пользователями

Управление списком пользователей

Для вызова списка:

- В области объектов управления программы управления выберите пункт "Центр управления сетью | Пользователи".

  В правой части окна отобразится список зарегистрированных пользователей.

Список пользователей отображается в форме таблицы, каждая строка которой соответствует одной учетной записи. Список полей, отображаемых в списке, и их описание представлены в таблице ниже.

Табл.4 Поля списка пользователей

Поле	Описание
Имя	Имя пользователя, зарегистрированное в комплексе
Описание	Произвольный текстовый комментарий
Логин	Имя пользователя для идентификации с помощью программы "Клиент аутентификации пользователя"
Заблокирован	При наличии отметки учетная запись пользователя заблокирована

Для регистрации пользователя:

1. Выполните одно из следующих действий:
   - в контекстном меню в любом месте списка пользователей выберите пункт "Создать пользователя";
   - нажмите на панели инструментов кнопку "Пользователь".

   На экране появится окно "Пользователь".
2. Настройте параметры учетной записи и нажмите кнопку "OK".

Имя	Имя пользователя, отображаемое в списке пользователей
Описание	Дополнительные сведения (необязательный параметр)
Логин	Имя пользователя для идентификации с помощью программы "Клиент аутентификации пользователя"
Пароль	Пароль пользователя для аутентификации с помощью программы "Клиент аутентификации пользователя". Пароль должен удовлетворять требованиям политики аутентификации администраторов (см. стр. **37**)
Подтверждение пароля	
Заблокирован	Установка отметки блокирует учетную запись без удаления ее из списка

Вкладка "Членство в группах" предназначена для просмотра списка групп, в которые входит пользователь. Для редактирования этого списка используйте кнопки "Добавить..." и "Удалить", расположенные справа от него.

Для изменения параметров учетной записи:

1. Выберите нужную учетную запись и выполните одно из следующих действий:
   - активируйте в контекстном меню команду "Свойства...";
   - нажмите на панели инструментов кнопку "Свойства".

   На экране появится окно "Пользователь".

2. Настройте и сохраните параметры учетной записи. Порядок настройки параметров см. выше.

Для удаления пользователя:

- Выберите одну или несколько учетных записей в списке и нажмите кнопку "Удалить" на панели инструментов (либо клавишу <Delete>). Для выбора нескольких элементов используйте клавиши <Shift> и <Ctrl>.

Для создания группы пользователей:

1. Выполните одно из следующих действий:
   - в контекстном меню списка пользователей выберите пункт "Создать группу пользователей...";
   - нажмите на панели инструментов кнопку "Группа пользователей".

   На экране появится окно "Группа пользователей".
2. Настройте параметры группы и нажмите кнопку "ОК".

Название	Наименование группы
Описание	Дополнительные сведения (необязательный параметр)
Размещение*	Наименование зарегистрированного сетевого объекта, с которым будет связана группа
Пользователи	Список пользователей, входящих в данную группу. Для формирования списка используйте кнопки "Добавить..." и "Удалить"

Примечание. Группе пользователей с помощью правил фильтрации IP-пакетов и правил трансляции сетевых адресов предоставляют доступ к определенным сетевым ресурсам или трафику. Доступ, предоставляемый этой группе, действует только на компьютерах, относящихся к связанному с группой сетевому объекту.

В области объектов управления в разделе "Пользователи" появится пункт с названием созданной группы. При выборе этого пункта в области отображения информации отобразится список пользователей, входящих в группу.

Для изменения параметров группы пользователей:

1. Выберите в области объектов управления группу пользователей и в контекстном меню группы выберите пункт "Свойства...".

   На экране появится окно "Группа пользователей".
2. Настройте и сохраните параметры группы (см. выше).

Для удаления группы пользователей:

- Выберите в области объектов управления группу пользователей и в контекстном меню группы выберите пункт "Удалить группу пользователей..." (либо нажмите клавишу <Delete>).

Глава 6
Управление криптографическими ключами

Управление осуществляется по однолетней схеме распределения ключей (см. [**1**]).

Однолетняя схема распределения ключей

Генерацию ключей и их распределение по узлам сети выполняют в соответствии с общим порядком ввода комплекса в эксплуатацию.

По истечении срока действия ключей необходимо осуществить смену ключей (см. ниже). Кроме того, смену ключей выполняют в случае их компрометации.

При выполнении операций смены ключей, описанных в данном разделе, не рекомендуется производить каких-либо действий по управлению сетевым устройством до завершения синхронизации с БД ЦУС.

Общий порядок смены ключей

Смену ключей шифрования осуществляют периодически в соответствии с принятым планом смены ключей, а также в случае компрометации ключей.

Примечание. Смена ключей на КШ с ЦУС средствами ПУ ЦУС невозможна. Главный ключ и ключ связи с ЦУС меняется на КШ с ЦУС средствами локального управления (см. стр. **20**).

Общий порядок смены ключей:

1. Обновление исходной ключевой информации. Выполняют до истечения срока действия ключа сетевого устройства исходя из оперативности процедуры рассылки ключевого материала локальным администраторам. Исходную ключевую информацию загружают на ЦУС средствами локального управления (см. стр. **19**).
2. Генерация нового ключевого материала для сетевого устройства (см. стр. **54**). Ключи нумеруют и учитывают в журнале выпуска ключей. Для каждого сетевого устройства выпускают несколько комплектов ключей. Срок действия каждого ключа — один год.

   Примечание. Ключевой материал используют для смены следующих ключей сетевого устройства:
   - главный ключ сетевого устройства;
   - ключ связи с ЦУС.
3. Рассылка сгенерированного ключевого материала локальным администраторам средствами спецсвязи.
4. Смена ключей сетевых устройств средствами программы управления ЦУС и локального управления сетевыми устройствами (см. стр. **54**).

   Примечание. На данном этапе выполняется смена следующих ключей сетевого устройства:
   - главный ключ сетевого устройства;
   - ключ связи с ЦУС.
5. Смена ключей парной связи сетевых устройств (см. стр. **55**).

Порядок действий при смене ключей в зависимости от требуемой процедуры представлен в таблице ниже.

Табл.5 Порядок действий при смене ключей

Причина	Действия
Компрометация исходной ключевой информации или окончание срока действия ключей	Выполните пп. **1-5** общего порядка смены ключей

Причина	Действия
Компрометация ключевого материала сетевого устройства	Выполните пп. **2-5** общего порядка смены ключей
Компрометация ключей одного или нескольких сетевых устройств	Выполните пп. **4, 5** общего порядка смены ключей

Генерация ключевого материала

Ключевой материал создают средствами ПУ ЦУС.

Для генерации ключевого материала:

1. В области объектов управления выберите тип сетевых устройств, вызовите контекстное меню требуемого сетевого устройства и выберите пункт "Создать резервный комплект ключей…".

   На экране появится окно ввода пароля. Этот пароль служит для защиты ключевого материала от несанкционированного доступа.

2. Введите пароль (не менее 4 символов, удовлетворяющий требованиям политики аутентификации администраторов (см. стр. **37**)), подтвердите его и нажмите кнопку "ОК".

   На экране появится окно выбора каталога, предназначенного для сохранения ключевого материала.

3. Выберите каталог и нажмите кнопку "Сохранить".

   Резервный ключевой материал будет сохранен в файле keyset. На экране появится сообщение "Резервный комплект ключей сохранен".

4. Закройте сообщение, нажав кнопку "ОК".

Смена ключей сетевого устройства

Автоматическая смена ключей сетевого устройства

Автоматическая смена ключей выполняется в соответствии с заданным расписанием.

Для настройки расписания:

1. В контекстном меню раздела "Центр управления сетью" выберите пункт "Настройка смены ключей сетевых устройств по расписанию…".

   На экране появится соответствующее окно.

2. Установите значения параметров:

Автоматически менять ключи на всех сетевых устройствах	Установка отметки включает режим автоматической смены ключей
Начиная с	Начало действия расписания
Повторять смену ключей через	Период времени, через который выполняется автоматическая смена ключей
Время, отводимое на смену ключей	Период времени, отведенный на смену ключей
Блокировать трафик через сетевые устройства с истекшим сроком действия ключей	При наличии отметки зашифрованный трафик через сетевые устройства, у которых истек срок действия ключей, блокируется

3. Нажмите кнопку "ОК".

Примечание. Не рекомендуется устанавливать длительный период времени, отводимый на смену ключей. Во время смены ключей управление сетевым устройством средствами централизованного управления невозможно.

Принудительная смена ключей сетевого устройства

Для смены ключей сетевого устройства:

1. Выберите в списке нужное сетевое устройство и в контекстном меню выберите пункт смены ключей.

   Примечание. Возможен множественный выбор объектов.

   На экране появится окно смены комплекта ключей.
2. Укажите время, отводимое на смену ключей, и нажмите кнопку "Да".

Для смены ключей группы сетевых устройств:

1. Выберите в области объектов управления группу сетевых устройств и в контекстном меню выберите пункт "Сменить ключи всех устройств в группе...".

   Примечание. Возможен множественный выбор объектов.

   На экране появится окно смены комплекта ключей сетевых устройств.
2. Укажите время, отводимое на смену ключей, и нажмите кнопку "Да".

Для смены ключей всех сетевых устройств:

1. В контекстном меню раздела "Центр управления сетью" выберите пункт "Сменить ключи всех сетевых устройств...".

   На экране появится окно смены комплекта ключей сетевых устройств.
2. Укажите время, отводимое на смену ключей, и нажмите кнопку "Да".

Смена ключей парных связей КШ

При смене ключей парных связей КШ защищенные соединения, установленные на старых ключах, автоматически разрываются и затем создаются уже на новых ключах. В результате кратковременного разрыва соединения возможны потери трафика.

Для смены ключей парной связи:

1. В области объектов управления, в подразделе "Сетевые устройства Континент | Криптошлюзы"выберите сетевое устройство.
2. В контекстном меню сетевого устройства выберите пункт "Сменить все ключи парных связей КШ...".

   Примечание. Команда "Сменить все ключи парных связей КШ" недоступна при пустом списке связанных сетевых устройств.

   На экране появится запрос на подтверждение смены ключей.
3. Нажмите кнопку "Да".

   На экране появится сообщение "Ключи парной связи изменены".
4. Закройте сообщение, нажав кнопку "ОК".

Запись ключей сетевого устройства на носитель

Данная операция выполняется для последующей инициализации сетевого устройства комплекса.

Для записи ключей:

1. Предъявите носитель для записи ключей.
2. В основном окне программы управления в контекстном меню зарегистрированного сетевого устройства активируйте команду "Сохранить текущие ключи на носитель...".

   На экране появится окно назначения пароля.
3. Введите и подтвердите пароль.

   Внимание! Пароль должен удовлетворять требованиям политики аутентификации

администраторов (см. стр. 37). В противном случае кнопка "ОК" в окне назначения пароля будет неактивной.

На экране появится окно выбора каталога хранения ключей.

4. Укажите в качестве каталога предъявленный носитель.

   В результате успешной записи ключей на носитель появится сообщение "Текущие ключи сетевого устройства сохранены".

Глава 7
Организация связи со сторонними криптографическими сетями

Общий порядок организации связи

Для организации связи со сторонней криптографической сетью, управляемой другим ЦУС, необходимо выполнить следующие действия:

1. Регистрация внешней сети средствами программы управления (см.стр. **59**).
2. Обмен сертификатами открытых ключей.
   - Создание и экспорт сертификата собственной сети (см.стр. **58**).
   - Импорт сертификата сторонней сети (см.стр. **60**).
3. Обмен файлами конфигурации разрешенных к доступу ресурсов.
   - Создание и экспорт файла конфигурации разрешенных к доступу ресурсов собственной сети (см. стр. **60**).
   - Импорт файла конфигурации разрешенных к доступу ресурсов сторонней сети (см.стр. **60**).
4. Создание межсетевого ключа (см. стр. **60**).
5. Настройка парной связи между КШ (см. [**4**]).
6. Создание правил фильтрации для информационного обмена между сетями (см. [**3**]).

Внимание!

- Связь со сторонней криптографической сетью не может быть установлена, если хотя бы на одном из связываемых ЦУС включен режим изолированной сети.
- Для установки соединения между КШ, принадлежащими разным криптографическим сетям, хотя бы один из этих КШ должен обладать однозначно идентифицируемым статическим IP-адресом.
- Загрузка конфигурации внешней сети при совпадении идентификаторов КШ в домашней и внешней сети невозможна.

Инфраструктура открытых ключей

Собственная инфраструктура открытых ключей предназначена для установки защищенного соединения с внешней криптографической сетью.

Удостоверяющим центром является ЦУС. Здесь выполняются генерация ключевой пары и издание сертификата открытого ключа, а также их хранение.

Для вызова списка сертификатов:

- В области объектов управления ПУ ЦУС выберите пункт "Центр управления сетью | Сертификаты".

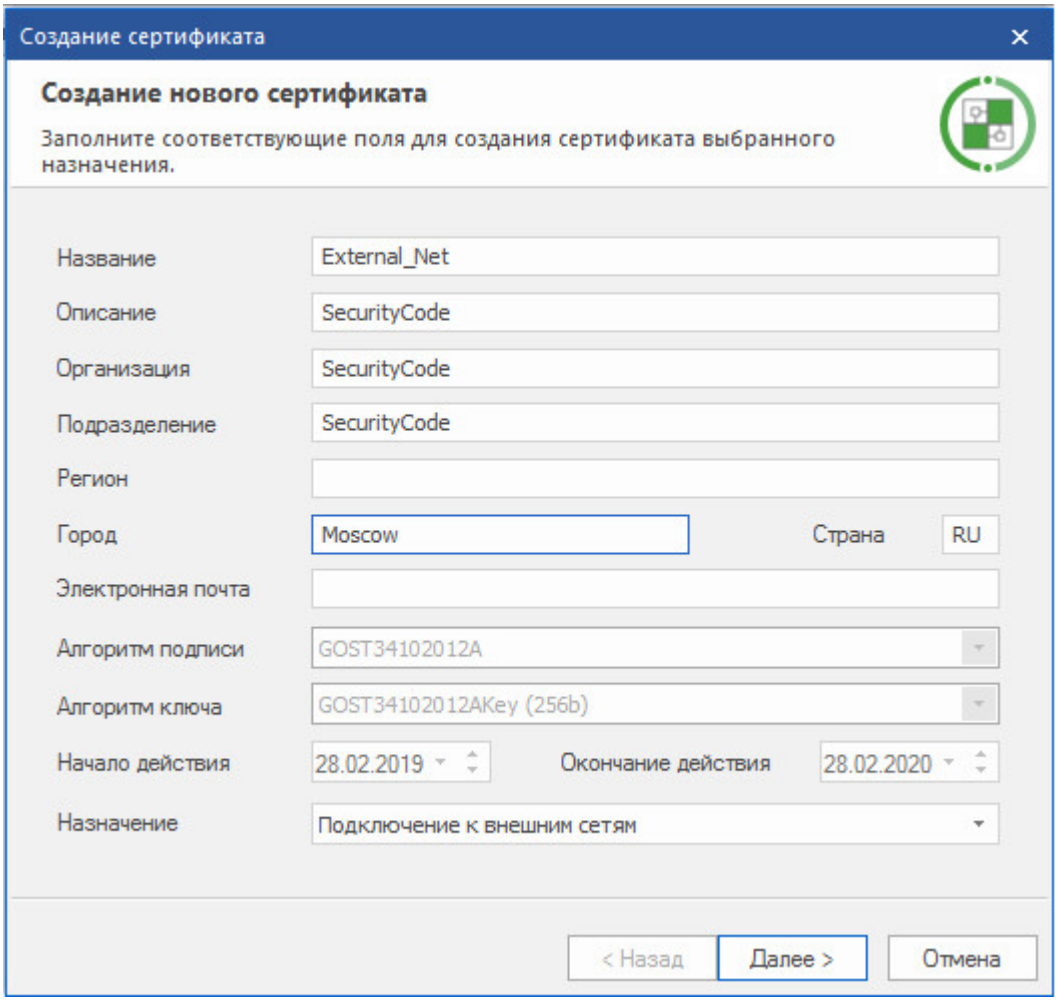
  В правой части окна отобразится список сертификатов, содержащий следующие поля:
  - серийный номер;
  - субъект;
  - издатель;
  - назначение;
  - привязка;
  - алгоритм подписи;
  - алгоритм ключа;

- срок действия.

Для создания сертификата:

1. Вызовите контекстное меню в любом месте списка сертификатов и активируйте команду "Создать сертификат" или нажмите одноименную кнопку на панели инструментов.

   На экране появится окно "Создание сертификата".



2. Заполните поля параметров и нажмите кнопку "ОК".

Название	Наименование сертификата открытого ключа
Описание	Дополнительная текстовая информация
Организация	Наименование организации, издавшей сертификат
Подразделение	Наименование подразделения, издавшего сертификат
Регион	Почтовые атрибуты организации, издавшей сертификат
Город	
Страна	
Электронная почта	
Алгоритм подписи	Используемый алгоритм для подписи сертификата
Алгоритм ключа	Используемый алгоритм для создания ключевой информации сертификата
Начало/конец действия	Срок действия сертификата
Назначение	Предназначение сертификата

В поле "Назначение" выберите значение "Подключение к внешним сетям" и нажмите кнопку "Далее".

На экране появится окно "Привязка сертификата".

В окне отображается привязка создаваемого сертификата к домашней сети.

3. Нажмите кнопку "Готово".

   Окно мастера закроется и в списке сертификатов появится вновь созданный сертификат.

Для просмотра сертификата:

- Выберите нужную запись в списке и нажмите кнопку "Свойства" на панели инструментов.

  На экране появится окно просмотра свойств сертификатов.

Для удаления сертификата:

- Выберите одну или несколько записей в списке и нажмите кнопку "Удалить" на панели инструментов (либо клавишу <Delete>). Для выбора нескольких элементов используйте клавиши <Shift> и <Ctrl>.

Управление внешними сетями

Перечень сторонних криптографических сетей отображается в окне "Внешние криптографические сети". Управление внешними сетями выполняют в этом окне.

Для вызова списка внешних сетей:

1. В левой части окна программы управления выберите раздел "Внешние криптографические сети".

   В правой части окна отобразится список зарегистрированных внешних сетей.

Табл.6 Перечень полей списка внешних сетей

Поле	Описание
Название	Наименование внешней криптографической сети
Описание	Дополнительная текстовая информация

2. Для просмотра подробных сведений о внешней сети раскройте в левой части окна раздел "Внешние криптографические сети" и далее раскройте вложенную папку с нужным названием.

   На экране отобразится список, содержащих всю необходимую информацию для работы с данной сетью.

3. Для просмотра содержимого папки выберите ее в списке.

   В правой части окна отобразится содержимое папки.

Для регистрации внешней сети:

1. Вызовите контекстное меню в любом месте списка внешних сетей и выберите пункт "Создать внешнюю криптографическую сеть" или нажмите одноименную кнопку на панели инструментов.

   На экране появится окно "Внешняя криптографическая сеть".

2. Заполните поля окна и нажмите кнопку "ОК".

Название	Наименование внешней криптографической сети
Описание	Дополнительная текстовая информация

Для редактирования внешней сети:

1. Выберите запись в списке и в контекстном меню выберите пункт "Свойства" или нажмите одноименную кнопку (

) на панели инструментов.

На экране появится окно "Внешняя криптографическая сеть".

2. Заполните поля окна и нажмите кнопку "ОК".

Название	Наименование внешней криптографической сети
Описание	Дополнительная текстовая информация

Для импорта сертификата внешней сети:

1. Выберите запись в списке сертификатов и в контекстном меню выберите пункт "Импортировать сертификат...".

   На экране появится окно выбора файла.

2. Выберите файл сертификата (*.cer) и нажмите кнопку "Далее". После окончания импорта нажмите кнопку "ОК".

Для импорта конфигурации разрешенных к доступу ресурсов:

1. Выберите запись в списке и в контекстном меню выберите пункт "Импортировать конфигурацию внешней сети...".

   На экране появится окно открытия файла.

2. Выберите файл конфигурации (*.nc) и нажмите кнопку "ОК".

Для экспорта конфигурации разрешенных к доступу ресурсов:

1. Выберите запись в списке и в контекстном меню выберите пункт "Экспортировать конфигурацию для внешней сети...".

   На экране появится окно "Экспорт конфигурации для внешней сети".

2. Заполните поля окна и нажмите кнопку "ОК".

Сертификат своей сети	Наименование сертификата собственной сети, предназначенного для создания электронной подписи файла конфигурации
Сертификат внешней сети	Наименование сертификата внешней сети для зашифровывания файла конфигурации
Сетевые объекты и криптошлюзы, доступные для внешней сети	Перечень сетевых объектов собственной сети, к которым разрешен доступ из данной внешней сети. Для формирования списка используйте кнопки "Добавить..." и "Удалить"
Имя файла для сохранения экспортируемой конфигурации	Полное имя файла конфигурации ресурсов собственной сети, разрешенных для доступа из сторонней сети

Для удаления внешней сети:

- Выберите одну или несколько записей в списке и нажмите кнопку  на панели инструментов (клавишу <Delete>). Для выбора нескольких элементов используйте клавиши <Shift> и <Ctrl>.

Управление межсетевыми ключами

Межсетевой ключ используется для генерации ключей парной связи КШ. Для создания межсетевого ключа необходимо заранее издать сертификат собственной сети и импортировать сертификат сторонней сети, с которой устанавливается связь.

Примечание. Межсетевой ключ используется для генерации не более 256 ключей парной связи КШ.

Срок действия ключа парной связи КШ (как с узлом своей сети, так и с узлом внешней криптографической сети) составляет 12 месяцев, если количество циклов запуска КШ не превысило 70 раз. По истечении срока действия ЦУС

автоматически генерирует новые ключи парной связи КШ при наличии активного и действующего межсетевого ключа.

Примечание. Ключи парной связи генерируются при формировании списка связанных сетевых устройств в свойствах криптошлюза (до нажатия кнопки "ОК").

Для вызова списка межсетевых ключей:

- В левой части окна программы управления выберите раздел "Внешние криптографические сети | <Наименование нужной сети>| Межсетевые ключи".

  В правой части окна отобразится список межсетевых ключей для данной внешней сети.

Табл.7 Перечень полей списка межсетевых ключей

Поле	Описание
Пиктограмма ключа	Пиктографическое обозначение состояния межсетевого ключа (см. Табл.8)
Действителен с	Дата и время начала срока действия межсетевого ключа
Действителен по	Дата и время окончания срока действия межсетевого ключа. Дополнительные отметки: ! — до окончания срока действия осталось меньше месяца; !! — до окончания срока действия осталось меньше недели
Сертификат своей сети	Наименование сертификата домашней сети, использованного для создания данного межсетевого ключа
Сертификат внешней сети	Наименование сертификата внешней сети, использованного для создания данного межсетевого ключа
Хэш ключа	Результат хэширования ключа
Ресурс ключа	Оставшееся время жизни ключа в процентах в зависимости от интенсивности использования его производных – ключей парной связи

Табл.8 Пиктографические обозначения состояния межсетевого ключа

Пиктограмма	Описание
	Активный межсетевой ключ. Этот ключ используется для генерации ключей парной связи КШ. Только один ключ из списка может быть активен
	Неактивный действительный межсетевой ключ
	Недействительный межсетевой ключ

Для создания межсетевого ключа:

1. Вызовите контекстное меню в любом месте списка межсетевых ключей и выберите пункт "Создать межсетевой ключ" или нажмите одноименную кнопку на панели инструментов ().

   На экране появится окно "Межсетевой ключ".

2. Заполните поля окно и нажмите кнопку "ОК".

Сертификат своей сети	Наименование сертификата собственной сети, использованного для создания данного межсетевого ключа
Сертификат внешней сети	Наименование сертификата внешней сети, использованного для создания данного межсетевого ключа

Для активирования межсетевого ключа:

- В контекстном меню записи выберите пункт "Активировать" или нажмите кнопку на панели инструментов ().

  Пиктограмма выбранного ключа примет вид  .

Для удаления межсетевого ключа:

- Выберите одну или несколько записей в списке и нажмите кнопку  на панели инструментов (клавишу <Delete>). Для выбора нескольких элементов используйте клавиши <Shift> и <Ctrl>.

Внимание! Для поддержания корректной работы комплекса со сторонней криптографической сетью не рекомендуется удалять активный межсетевой ключ. Если по каким-либо причинам произошло его ошибочное удаление, необходимо повторно выполнить все действия в соответствии с общим порядком организации связи (см. стр. 57), используя новые сертификаты.

Примечание. Срок действия межсетевого ключа заканчивается в момент истечения срока действия одного из сертификатов, на которых он сгенерирован. Для поддержания корректной работы комплекса со сторонней криптографической сетью необходимо поддерживать актуальность сертификатов домашней и внешней сетей.

Глава 8
Агент Роскомнадзора

Агент предназначен для автоматической загрузки в БД ЦУС сведений о запрещенных ресурсах единого реестра Роскомнадзора. Для получения агентом сведений о запрещенных ресурсах используется веб-сервис портала Роскомнадзора.

Примечание. Сведения о запрещенных ресурсах могут быть загружены в ручном режиме без использования агента (см. стр. 101).

Установка агента

Агент Роскомнадзора устанавливают как компонент, входящий в состав подсистемы управления.

Компьютер, на который устанавливают агент, должен удовлетворять следующим требованиям:

- На компьютере установлены компоненты ОС Windows, обеспечивающие доступ к порталу Роскомнадзора по сетевым протоколам TCP/IP.
- Поддерживается связь агента с ЦУС по зашифрованному каналу для передачи сведений о запрещенных ресурсах в БД ЦУС.
- На компьютере установлено программное обеспечение криптопровайдера "КриптоПро CSP".
- В хранилище локального компьютера установлены сертификат пользователя (устанавливается в раздел "Личное"), корневой сертификат и сертификат Роскомнадзора (устанавливаются в раздел "Доверенные корневые центры сертификации").

  Примечание. При создании запроса на получение сертификата средствами "КриптоПро CSP" формируется закрытый ключ. Для хранения ключевой информации используется внешний носитель.

Для установки агента:

1. Выполните процедуру установки ПУ ЦУС (см. [**2**]).

   Вид установки — "Выборочная". Устанавливаемый компонент — "Агент Роскомнадзора".
2. После завершения процедуры установки перезагрузите компьютер.

   На экране появится сообщение с инструкцией по накоплению энтропии для биологического датчика случайных чисел, если она не была накоплена ранее.
3. Нажмите кнопку "ОК" в окне сообщения и, следуя инструкции, нажимайте на мишень, перемещающуюся по экрану, до завершения процесса накопления энтропии.

   Внимание! Непопадание в мишень может привести к понижению уровня накопленной энтропии и необходимости повторного выполнения данной операции.

   После завершения операции накопления энтропии на экране появится окно настройки параметров агента.
4. Укажите значения параметров или откажитесь от настройки нажатием кнопки "Отмена".

   Настройку параметров можно выполнить позже (см. стр. 65).
5. После настройки параметров нажмите кнопку "ОК".

   Окно настройки параметров агента закроется.

После завершения процедуры установки на компьютере будут установлены агент и программа управления агентом, а группа приложений "Код

Безопасности" дополнится ярлыком "Программа управления агентом Роскомнадзора".

При запуске программа размещает свою пиктограмму в панели задач Windows. Цвет пиктограммы указывает на состояние агента:

	Зеленый	Агент запущен
	Красный	Агент остановлен

После установки, а также после настройки параметров агент находится в состоянии "остановлен".

Программа управления агентом Роскомнадзора

Программа используется для настройки и локального управления агентом Роскомнадзора.

После завершения процедуры установки агента программа изначально находится во включенном состоянии в пользовательском режиме. При этом агент находится в состоянии "остановлен".

Для управления агентом используются команды контекстного меню пиктограммы программы  в панели задач (см. ниже). В пользовательском режиме доступна только часть этих команд, для полного функционала программы необходимо запустить ее в меню "Программы" главного меню Windows от имени администратора.

При выходе из программы управления пиктограмма из панели задач удаляется и вызов контекстного меню становится невозможным. При этом агент, если он был запущен, продолжает свою работу в соответствии с заданными настройками.

Команды управления агентом Роскомнадзора

Ниже в таблице приведены все команды программы управления агентом Роскомнадзора.

Название команды	**Описание**
Запустить агент	Осуществляет запуск агента
Остановить агент	Осуществляет остановку агента
Параметры агента…	Открывает окно настройки параметров агента
Удалить сохраненный пароль к ЦУС	Удаляет сохраненный пароль доступа к ключам ЦУС. При выполнении команды "Запустить агент" потребуется ввести пароль
Отключить уведомления об ошибках	Отключает/включает вывод всплывающих сообщений об ошибках в работе агента
Журнал приложений системы	Вызывает на экран журнал событий ОС Windows
О программе…	Открывает окно, содержащее сведения о номере версии программы управления агентом, а также сведения об авторских правах на программный продукт
Выход	Осуществляет выход из программы управления агентом и удаляет пиктограмму с панели задач. **Внимание!** При удалении пиктограммы агент не выключается

Настройка параметров агента

Внимание! Для изменения параметров агента его необходимо запустить в меню "Программы" главного меню Windows от имени администратора.

Для настройки параметров агента:

1. Вызовите контекстное меню пиктограммы программы управления агентом и выберите команду "Параметры агента".

   На экране появится окно настройки параметров.

2. Укажите требуемые значения параметров.

Параметр	Описание
Служба выгрузки	
URL службы выгрузки	Адрес страницы на портале Роскомнадзора для получения выгрузки
Путь хранения последней выгрузки	Папка локального компьютера, в которую агент сохраняет выгрузку Роскомнадзора для последующей передачи в ЦУС
Период опроса службы выгрузки	Периодичность опроса агентом портала Роскомнадзора
Подключения к ЦУС	
Адрес	IP-адрес для подключения агента к ЦУС
Тип ключевого носителя	Тип съемного носителя, на котором хранятся ключи связи с ЦУС. Возможные значения: дисковод и USB-флеш-накопитель
Прокси HTTP	
Адрес Порт	Адрес и порт прокси-сервера для подключения агента к порталу Роскомнадзора
Логин Пароль	Аутентификационные данные, используемые при подключении к порталу Роскомнадзора через прокси-сервер
Сертификат	
Сертификат	Сертификат, предъявляемый агентом при обращении в Роскомнадзор. Хранится в хранилище локального компьютера
Оператор связи	
Наименование	Полное наименование оператора связи
ИНН	ИНН оператора связи (10 цифр для юридических лиц)
ОГРН	ОГРН оператора связи (13 цифр для юридических лиц)
E-mail	Электронный адрес технического специалиста, ответственного за использование механизма получения выгрузки; может использоваться для оперативной обратной связи в случае возникновения технических вопросов или проблем (необязательное поле)

3. Нажмите кнопку "ОК".

   Окно настройки параметров закроется.

Примечание. После изменения параметров, если агент был запущен, он переходит в состояние "остановлен". Для продолжения работы агент необходимо запустить (см. ниже).

Запуск агента

Перед запуском агента подготовьте носитель с дубликатом административного ключа (создание дубликата административного ключа см. стр. **40**).

Для запуск агента:

1. Вставьте носитель с дубликатом административного ключа.
2. Вызовите контекстное меню пиктограммы программы управления агентом и выберите команду "Запустить".

   На экране появится запрос на ввод административного пароля.

   Примечание. Запрос не появится, если при предыдущем запуске агента в запросе на ввод пароля была установлена отметка в поле "Сохранить пароль".
3. Введите пароль администратора.

   Если необходимо сохранить пароль, установите отметку в поле "Сохранить пароль".
4. Нажмите кнопку "ОК".

   Агент будет запущен и пиктограмма программы управления агентом изменит цвет с красного на зеленый.

Сообщения об ошибках

Ошибки подключения агента к веб- сервису портала Роскомнадзора регистрируются в журнале событий ОС Windows в разделе Windows Logs/Application.

Для просмотра событий:

1. Вызовите контекстное меню программы управления агентом и выберите команду "Журнал приложений системы".

   Откроется журнал.
2. Перейдите в раздел Windows Logs/Application.

Ниже приведено описание событий, связанных с ошибками подключения агента к веб-сервису портала Роскомнадзора.

Событие	Описание
Event ID: 4. Network connection fail to RKN-service. Error: HTTP error: 408 HTTP/1.1 408 Request Time-out, <html>Your request timed out. Please retry the request	Данная ошибка вызвана невозможностью подключения к сервису Роскомнадзора. Это может быть связано как с нарушением сетевого соединения на стороне пользователя, так и недоступностью сервиса со стороны Роскомнадзора. В зависимости от установленного в параметрах агента периода опроса службы выгрузки попытка подключения будет выполнена позже
Event ID: 7. Verify sign fail. Error: Невозможно построить цепочку доверенных сертификатов	Причиной ошибки является недействительный сертификат. Недействительным может быть как один из сертификатов, загружаемых пользователем, так и сертификат, присылаемый со стороны Роскомнадзора при подключении
Event ID: 9. Service wait result, a112a3375b80b156726829cd69ef95002	Событие, описывающее подключение к сервису. С шестнадцатеричным номером, указанным в описании события, можно обратиться в Роскомнадзор и получить список, если он не был загружен по каким-либо причинам из сервиса

Глава 9
Обеспечение отказоустойчивости комплекса

Резервное копирование и восстановление конфигурации ЦУС

Резервное копирование конфигурации ЦУС

В комплексе предусмотрена возможность резервного копирования конфигурации ЦУС. Резервная копия позволяет быстро восстановить работу сети при выходе из строя штатного ЦУС.

Существуют два способа создания резервной копии:

- автоматически агентом ЦУС и СД в соответствии с заданным расписанием;
- принудительно администратором.

Автоматическое создание резервной копии

Агент сохраняет резервную копию конфигурации ЦУС в папку, которую можно указать средствами локального управления агентом (см. [**5**]). По умолчанию это папка %PUBLIC%\Documents\Continent3\<имя_базы данных>. Имя файла резервной копии Save_at_yy_mm_dd-hh_mm.dat. Всего в данной папке одновременно может храниться от 2 до 365 последних файлов резервных копий (в зависимости от настроек ЦУС; по умолчанию — 30).

Имеются два типа расписания работы агента:

- периодическое;
- еженедельное.

Периодическое расписание определяет интервал времени, через который агент выполняет свои функции. Еженедельное расписание определяет точное время действия агента по дням недели. Можно определить расписание работы агента любым из этих методов.

Для настройки расписания:

1. Вызовите окно настройки агента. Для этого в меню "ЦУС" активируйте команду "Настройки агента ЦУС и СД".
2. Выберите вкладку "Сохранение конфигурации ЦУС".
3. Выберите тип расписания и определите его параметры:

Периодическое расписание	Включает режим работы, при котором запуск процесса осуществляется через равные промежутки времени. Продолжительность промежутка задается количеством минут или часов. Режим начинает действовать с момента наступления определенной даты и времени. Чтобы указать другой момент начала действия режима, активируйте ссылку с текущим значением даты и времени и в появившемся на экране окне введите нужные значения. Способы выбора и редактирования значений в этом окне аналогичны стандартным способам, принятым в ОС Windows для установки даты и времени

Еженедельное расписание	Включает режим работы, при котором запуск процесса осуществляется в моменты времени, заданные специальным расписанием. Расписание представлено в виде таблицы, разделенной, для оптимального отображения, на две части. В столбцах таблицы перечислены дни недели, а в строках — часы и минуты с шагом 30 минут. Выбор времени запуска процесса осуществляется посредством установки отметки в соответствующей ячейке таблицы. Для установки отметки поместите указатель в ячейку и нажмите левую кнопку мыши. Повторное нажатие кнопки приводит к удалению отметки. Действие расписания повторяется еженедельно

4. Нажмите кнопку "ОК".

Агент будет автоматически создавать резервную копию конфигурации ЦУС в соответствии с заданным расписанием.

Принудительное создание резервной копии

Принудительное создание резервной копии конфигурации ЦУС рекомендуется выполнять всякий раз после внесения очередного изменения в настройки комплекса.

Примечание. Используйте для хранения резервной копии специально выделенный и защищенный жесткий диск.

Принудительное создание резервной копии конфигурации при локальном управлении ЦУС выполняется аналогично процедуре для сетевого устройства (см. стр. **10**). В ходе процедуры будет предложен выбор между обычным сохранением конфигурации ЦУС и сохранением для техподдержки. Второй вариант не сохраняет параметры сетевых интерфейсов всех КШ комплекса и предназначен только для отсылки в службу технической поддержки (см. стр. **7**) для решения сложных проблем с работоспособностью комплекса.

Для принудительного создания резервной копии ЦУС посредством ПУ ЦУС:

1. В области объектов управления вызовите контекстное меню раздела "Центр управления сетью" и выберите пункт "Сохранить файл конфигурации ЦУС...".

   На экране появится окно задания пароля для зашифрования файла конфигурации ЦУС.

2. Введите и подтвердите пароль.

   Внимание! При задании пароля должны выполняться требования, предъявляемые к паролям в соответствии с политикой аутентификации администраторов (см. стр. **37**).

   Нажмите кнопку "ОК".

   На экране появится окно ОС Windows для сохранения файла.

3. Выберите папку и укажите имя файла для создания резервной копии.

   Внимание! Имя файла резервной копии не должно содержать кириллических символов.

4. Нажмите кнопку "Сохранить".

   Файл будет создан и зашифрован, а на экране появится сообщение об успешном завершении записи.

5. Закройте окно сообщения.

Восстановление конфигурации ЦУС из резервной копии

Способ восстановления конфигурации ЦУС зависит от текущей работоспособности комплекса.

Для загрузки конфигурации ЦУС подготовьте носитель с файлом резервной копии ncc.cfg или Save_ at_ <дата и время>.dat.

Для восстановления конфигурации ЦУС посредством ПУ ЦУС:

1. В области объектов управления вызовите контекстное меню раздела "Центр управления сетью" и выберите пункт "Загрузить файл конфигурации ЦУС...".

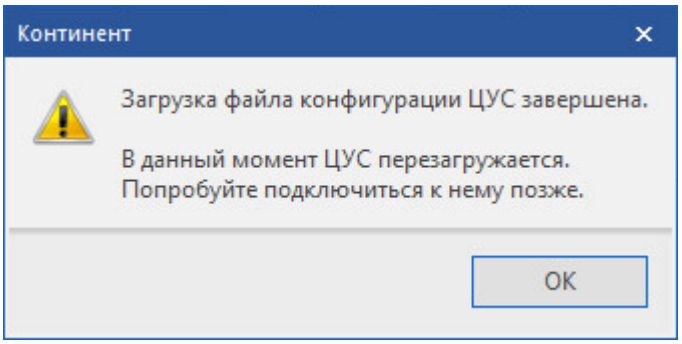
   На экране появится окно открытия файла.

2. Выберите нужную папку и укажите имя файла резервной копии. Нажмите кнопку "Открыть".

   На экране появится окно ввода пароля.

3. Введите и подтвердите пароль.

   На экране появится сообщение о перезагрузке ЦУС.



4. Нажмите кнопку "OK".
5. Нажмите кнопку вызова меню управления в левом верхнем углу панели управления и выберите команду "Установить соединение".

Для восстановления конфигурации при локальном управлении ЦУС:

1. В главном меню управления введите номер команды "Управление конфигурацией" и нажмите клавишу <Enter>.

   На экране появится список команд управления конфигурацией ЦУС.

2. Введите в строке ввода номер команды "Переинициализировать ЦУС" и нажмите клавишу <Enter>.

   На экране появится сообщение:

```
Провести начальную конфигурацию ЦУС? (Y/N):
```

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

   На экране появится сообщение:

```
Начальная конфигурация ЦУС
Инициализировать ЦУС с использованием файла конфигурации?
(Y/N):
```

4. Предъявите носитель с файлом конфигурации ЦУС, введите "y" и нажмите клавишу <Enter>.
5. Перейдите к выполнению п. **7** процедуры инициализации ЦУС (см. стр. **77**).

Для восстановления конфигурации вышедшего из строя ЦУС:

1. Выполните установку ПО "Континент" на ЦУС (см. стр. **83**).

   Примечание. При установке ПО ЦУС необходимо указать идентификатор вышедшего из строя КШ. В противном случае корректная работа нового КШ с восстановленной базой данных ЦУС невозможна.

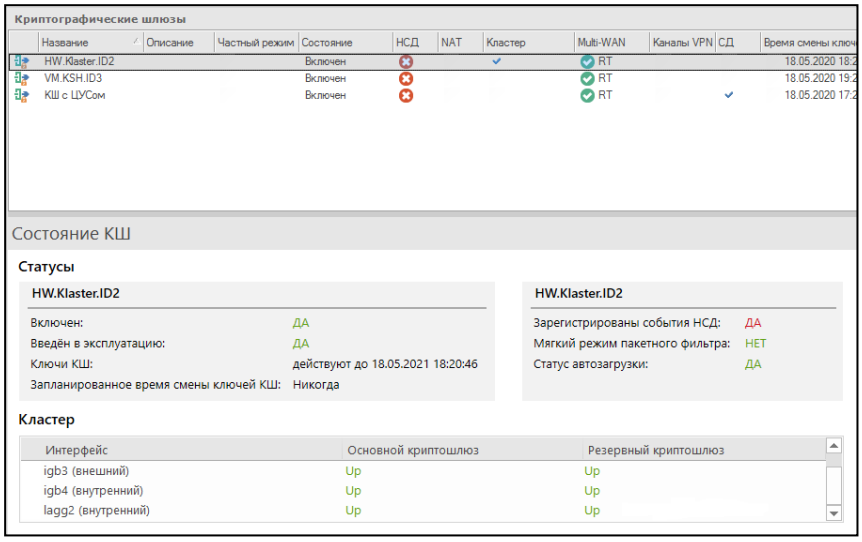
2. Выполните инициализацию ЦУС с использованием файла конфигурации (см. стр. **77**).

Управление кластером

Условия функционирования кластера

Кластер обеспечивает аппаратное резервирование сетевого устройства и автоматическое переключение канала связи с основного устройства на резервное при выходе основного из строя.

Сетевое устройство и его резервное сетевое устройство отображаются в ПУ ЦУС как единый объект.



Примечание. Возможность аппаратного резервирования отсутствует у КШ, подключенных к телефонным линиям с помощью модема.

- ДА;

Для корректной работы кластера необходимо соблюдать следующие условия:

- Оба устройства, образующие кластер, должны иметь одинаковые аппаратные платформы, а также одинаковое ПО одной и той же версии.

  Примечание. Для формирования кластера, не входящего в комплект поставки изделия, обратитесь в службу технической поддержки поставщика комплекса.

- Среда передачи пакетов, к которой подключены интерфейсы обоих устройств кластера, должна допускать наличие одинаковых IP- и MAC-адресов. Это требование относится как к внешним, так и к внутренним сетям комплекса.
- Интерфейсы резервирования обоих устройств кластера запрещено подключать к тем сетям, к которым подключены внешние и внутренние интерфейсы этих устройств. Для подключения интерфейсов резервирования необходимо использовать либо отдельную сеть, либо прямое подключение друг к другу.

Создание кластера

Создание кластера выполняют в следующей последовательности:

1. Регистрация сетевого устройства.
2. Настройка интерфейсов резервирования.
3. Включение режима резервирования.
4. Запись конфигурации и ключей сетевого устройства на отчуждаемый носитель.
5. Инициализация резервного устройства.
6. Ввод кластера в эксплуатацию.

Необходимо заранее подготовить два носителя: один — для записи конфигурации основного устройства, другой — для записи конфигурации резервного устройства.

Ключи сетевого устройства можно записать либо на те же носители, на которых записана конфигурация, либо на отдельный носитель.

Для корректной работы кластера необходимо в настройках ПАК "Соболь" указать следующие значения параметра "Автоматический вход в систему":

- для основного устройства — 5 сек.;
- для резервного устройства — 20 сек.

Шаг 1. Регистрация устройств кластера

Регистрацию основного сетевого устройства выполняют только в том случае, если оно вводится в эксплуатацию впервые. Описание процедуры регистрации устройств приведено в [**2**].

Шаг 2. Настройка интерфейсов резервирования

Настройку интерфейсов основного сетевого устройства выполняют с помощью программы управления ЦУС. Имеется возможность использовать несколько интерфейсов резервирования.

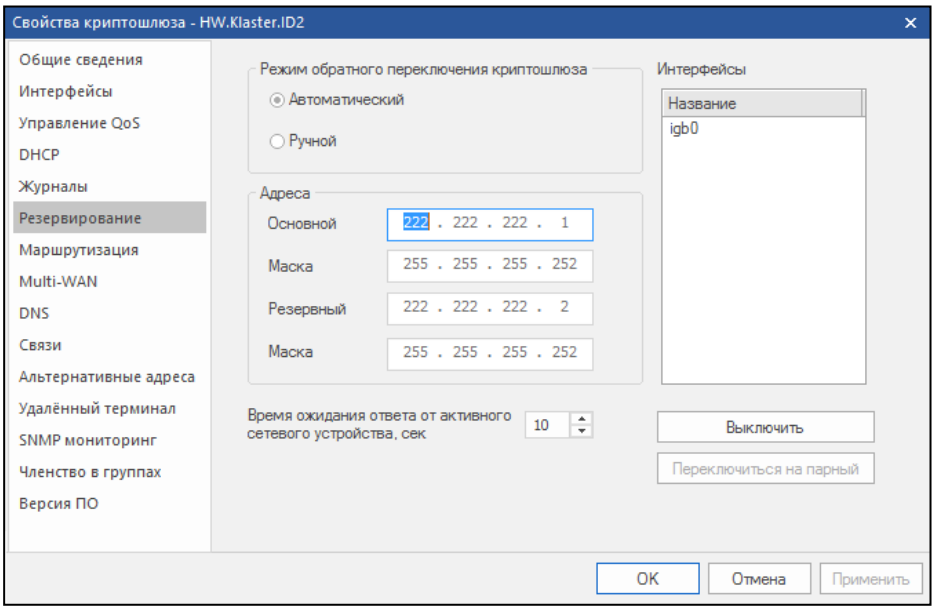
Описание настройки интерфейсов приведено в [**6**]. При выборе типа интерфейса укажите значение "Резервирование".

Шаг 3. Включение режима резервирования

Включение режима резервирования выполняют с помощью программы управления ЦУС.

Для включения режима резервирования:

1. Вызовите на экран окно настройки параметров сетевого устройства и перейдите к вкладке "Резервирование".
2. Нажмите кнопку "Включить". Поля параметров резервирования активируются.



3. Заполните поля параметров и нажмите кнопку "OK".

Интерфейсы	Перечень интерфейсов, у которых параметр "Тип" имеет значение "Резервирование"
Режим обратного переключения устройства	Порядок обратного переключения канала связи с резервного устройства на основное (возврат в состояние "как было"): • Автоматический — переключение осуществляется автоматически; • Ручной — переключение осуществляет администратор нажатием кнопки "Переключиться на парный"
Адреса	IP-адрес интерфейса резервирования и маска подсети, к которой он подключен, для основного и резервного устройств. Адреса этих интерфейсов должны быть уникальными для данной корпоративной сети и принадлежать одной подсети
Время ожидания ответа от активного сетевого устройства, сек.	Переключение канала связи (с резервного на основной и с основного на резервный) происходит при превышении времени, указанного в данном поле. Допустимые значения: 2-60 (секунд)

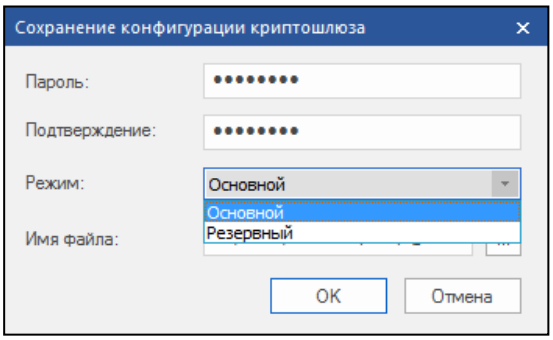
Шаг 4. Запись конфигурации и ключей КШ (КК) на отчуждаемый носитель

Запись конфигурации резервного устройства на носитель выполняют с помощью программы управления (см. [**2**], Глава 3). При записи конфигурации устройства в поле "Режим" выберите значение "Резервный".

Данную процедуру выполняют дважды:

- При записи конфигурации основного устройства в поле "Режим" выберите значение "Основной".
- При записи конфигурации резервного устройства — "Резервный"

Внимание! Конфигурации основного и резервного устройств необходимо записывать на разные носители.



Запись ключей сетевого устройства на носитель выполняют также с помощью программы управления (см. стр. **53**).

Примечание. Ключи и для основного, и для резервного устройства одинаковы. Ключи можно записать либо на тот же носитель, на котором записана конфигурация, либо на отдельный носитель.

Шаг 5. Инициализация резервного устройства

Данную процедуру выполняют средствами локального управления (см. [**2**]).

Внимание! Идентификационные номера основного и резервного устройства должны быть идентичны. Поэтому при установке программного обеспечения на резервный КШ (криптокоммутатор) необходимо указать идентификационный номер основного устройства кластера.

При инициализации резервного устройства используйте носители с соответствующими конфигурацией и ключами. После инициализации резервного устройства дождитесь появления на консоли сообщения "Успешный старт".

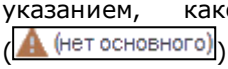
Шаг 6. Ввод кластера в эксплуатацию

Ввод кластера в эксплуатацию выполняют с помощью программы управления ЦУС.

Для ввода кластера в эксплуатацию:

1. Введите устройства кластера в эксплуатацию (см. стр. **42**).
2. Перезагрузите кластер (см. стр. **42**).

Дождитесь отображения рабочего состояния кластера в таблице состояний устройств соответствующего типа.

После этого основное и резервное устройства начнут функционировать в режиме резервирования. При выходе из строя одного из устройств в таблице соответствующих сетевых устройств пиктограмма кластера изменит свой вид с указанием, какое именно устройство перестало функционировать (

).

Добавление и удаление дополнительных интерфейсов резервирования

Внимание! При добавлении и удалении дополнительных интерфейсов резервное устройство должно быть включено.

Для добавления интерфейса резервирования:

1. Настройте интерфейс (см. [**6**]). При выборе типа интерфейса укажите значение "Резервирование".
2. Нажмите кнопку "Применить" в окне "Свойства <устройства>".

   Будет выполнено обновление конфигурации кластера.

Для удаления интерфейса резервирования:

Примечание. Для удаления единственного интерфейса резервирования необходимо предварительно выключить режим резервирования (см. стр. **75**).

1. Откройте окно свойства сетевого устройства и выберите вкладку "Интерфейсы".
2. Выберите удаляемый интерфейс резервирования и в поле "Тип" измените значение "Резервирование" на "Не определен".
3. Нажмите кнопку "Применить".

   Будет выполнено обновление конфигурации кластера.

Изменение адреса на интерфейсах резервирования

При выполнении процедуры изменения адреса на интерфейсе резервирования кластер должен быть введен в эксплуатацию. При этом оба устройства (основное и резервное) должны функционировать в режиме резервирования.

Для изменения адреса на интерфейсе резервирования:

1. Выберите кластер в списке, в контекстном меню выберите пункт "Свойства...".

   На экране появится окно свойств сетевого устройства.
2. Выберите вкладку "Резервирование" и в группе полей "Адреса" внесите необходимые изменения.
3. Нажмите кнопку "Применить".

   Будет выполнено обновление конфигурации кластера.
4. Выполните перезагрузку кластера (см. стр. **42**).

Если по каким-либо причинам при изменении адреса на интерфейсе резервирования резервное устройство кластера было выключено (или находилось

в ремонте), после изменения адреса (см. процедуру выше) необходимо выполнить следующее:

1. Запишите конфигурацию устройства на носитель (см. [**2**]). При записи конфигурации в поле "Режим" выберите значение "Резервный".
2. Выполните средствами локального управления загрузку конфигурации на резервном устройстве (см. [**2**]).

Определение состояния кластера

Сведения о работоспособности кластера отображаются в общей таблице состояния соответствующих сетевых устройств в ПУ ЦУС. Сведения о состоянии каждого устройства кластера представлены в главном окне на странице характеристик кластера.

Для просмотра сведений о состоянии устройства в кластере:

- Выберите в области объектов управления ПУ ЦУС название нужного кластера.

  В главном окне отобразятся характеристики кластера. Текущее состояние устройств, составляющих кластер, отображается в группе полей "Состояние кластера". Состояние устройства может принимать следующие значения:

Включен (Трафик)	Кластер функционирует в нормальном режиме. Данное устройство выполняет роль основного и обрабатывает трафик
Включен	Кластер функционирует в нормальном режиме. Данное устройство выполняет роль резервного и готово к обработке трафика
Активен	В кластере функционирует только данное устройство
Неактивен	Данное устройство в кластере не функционирует
Отключен	У обоих устройств питание отключено

Переключение канала связи в кластере

Существуют два режима переключения канала связи в кластере между основным и резервным устройствами:

- автоматический;
- ручной.

Выбор режима осуществляется в окне "Резервирование". В автоматическом режиме переключение канала связи осуществляется системой самостоятельно. Описание алгоритма автоматического переключения приведено на стр. **70**. При выборе ручного режима переключение канала связи выполняет администратор.

Совет. Если переключение канала связи с резервного устройства на основное не происходит, перезагрузите устройство (см. стр. **42**).

Для переключения канала связи в ручном режиме:

1. Вызовите окно настройки параметров устройства и выберите вкладку "Резервирование".
2. Нажмите кнопку "Переключиться на парный".

   На экране появится окно подтверждения.
3. Нажмите кнопку "Да", затем закройте окно настройки, нажав кнопку "ОК".

После этого основное устройство начнет функционировать в активном режиме, а в окне объектов программы управления пиктограмма данного устройства будет отображать состояние "включено".

Примечание. В связи с особенностью механизма взаимодействия механизмов LACP, протокола STP и модели реализации кластера, при использовании агрегированных интерфейсов увеличивается время переключения в кластере.

Выключение режима резервирования

Внимание! Выключение режима резервирования у работающего кластера запрещено.

Для выключения режима:

1. Выключите электропитание у резервного устройства.
2. Вызовите на экран окно настройки параметров устройства и выберите вкладку "Резервирование".
3. Нажмите кнопку "Выключить", а затем "Применить".
4. Закройте окно настройки, нажав кнопку "ОК".

После этого основное устройство будет автоматически перезагружено, а режим резервирования выключен.

Нештатные ситуации при работе кластера

В таблице представлено описание нештатных ситуаций при работе кластера резервирования, а также причины возникновения таких ситуаций и способы устранения их последствий.

Кластер*	Трафик	Сообщение в журнале НСД	Причина	Действие
✔ (нет резервного)	Есть	—	Отключено электропитание резервного устройства	Подключить электропитание
			Отсутствует соединение резервного устройства с основным через интерфейс резервирования	Восстановить работоспособность интерфейса резервирования
✔ (резервный)	Есть	Неправильный номер пакета**	Отключено электропитание основного устройства	Подключить электропитание
			У основного устройства нарушено подсоединение и внешнего интерфейса, и интерфейса резервирования	1. Восстановить подсоединение интерфейсов. 2. Разорвать и заново установить парную связь
✔	Нет	Неправильный номер пакета	У одного или обоих устройств было нарушено и затем восстановлено подсоединение внешнего интерфейса и интерфейса резервирования	Разорвать и заново установить парную связь

* Этот параметр отображается в общей таблице состояния устройства и отчетах о состоянии проблемных кластеров (см. [**5**]).

** Сообщения в журнале НСД появляются после подсоединения интерфейсов.

Во всех случаях, когда разрешить нештатные ситуации не удалось, следует обращаться в службу технической поддержки поставщика комплекса.

Восстановление работы кластера после ремонта основного устройства

Если основное устройство кластера было отправлено в ремонт, после возвращения устройства из ремонта подключите его к сетевым коммуникациям, включите питание и дождитесь загрузки. При необходимости средствами

локального управления выполните процедуру повторной инициализации устройства для загрузки последней сохраненной конфигурации (см. стр. **11**).

Чтобы убедиться в возобновлении работы кластера, проверьте прохождение IP-пакетов в другие защищаемые сети. Для проверки можно использовать команду ping (см. стр. **100**).

Если работоспособность кластера не восстановлена (IP-пакеты не проходят в другие защищаемые сети), проверьте наличие соединения резервного устройства с основным через интерфейс резервирования. При исправном соединении выполните действия в следующей последовательности:

1. Выключите резервное устройство (см. стр. **42**).
2. Выполните процедуру обновления конфигурации основного устройства (см. стр. **43**).
3. Выполните процедуру смены ключей устройства для основного устройства (см. стр. **55**).
4. Средствами локального управления выполните загрузку ключей для данного сетевого устройства (см. стр. **20**). При загрузке используйте ключевой носитель с хранящимися на нем комплектами ключей для данного сетевого устройства. В ходе процедуры загрузки укажите вариант "Загрузить активный ключ".
5. После загрузки конфигурации основного устройства включите резервное устройство (см. стр. **8**).

Резервирование ЦУС

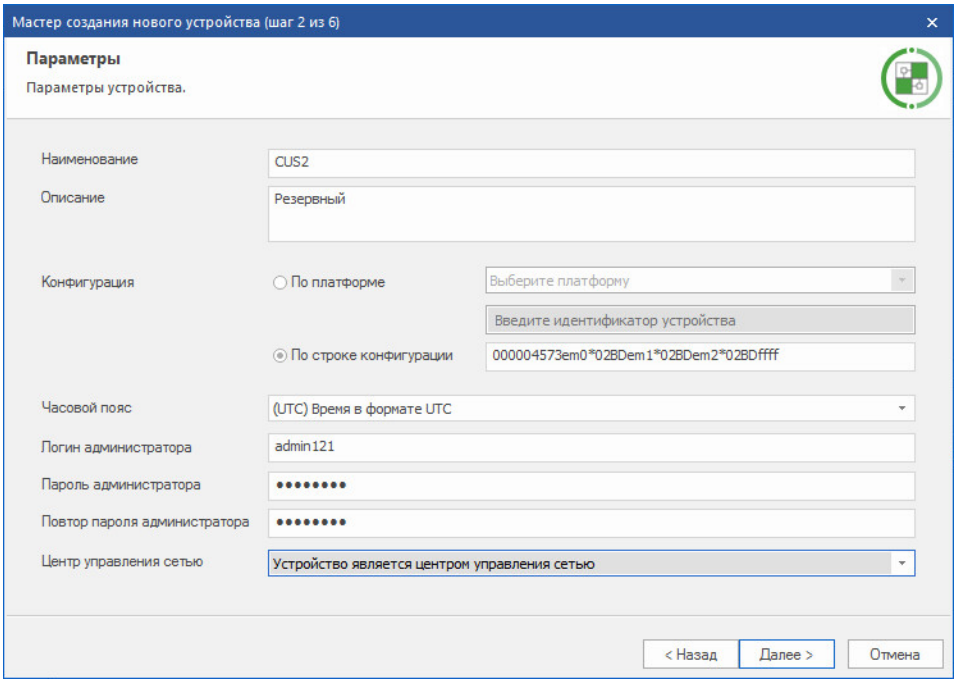
Для достижения отказоустойчивости ЦУС может состоять из нескольких сетевых устройств с ПО ЦУС. Устройства могут быть выполнены на разных платформах, однако рекомендуется устанавливать ПО ЦУС на платформы одной модели. По территориальному расположению и количеству устройств с ПО ЦУС ограничений нет. ЦУС состоит из одного устройства в активном режиме, осуществляющего управление сетью, и одного или нескольких устройств в пассивном режиме, находящихся в режиме ожидания.

Внимание! При резервировании ЦУС не рекомендуется устанавливать парные связи на КШ с ЦУС.

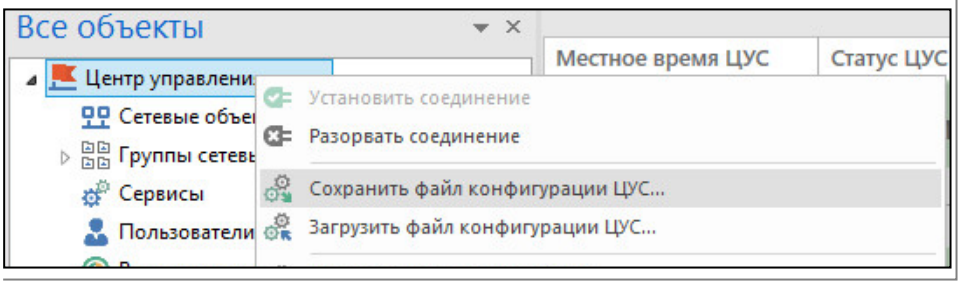
Переключение в активный режим осуществляет администратор централизованно через ПУ ЦУС или локально на КШ с ЦУС (см. стр. **80**).

Резервирование ЦУС выполняют в следующей последовательности:

1. Регистрация резервных КШ с ЦУС в ПУ ЦУС (см. [**2**], раздел "Развертывание сетевого устройства"). В параметрах устройства отмечаем, что оно является ЦУС.



Внимание! На заключительном шаге работы мастера создания нового устройства не нужно выгружать конфигурацию устройства на внешний носитель. Данную процедуру необходимо выполнить из контекстного меню раздела "Центр управления сетью" области объектов управления, не меняя название файла конфигурации ncc.cfg, предлагаемое по умолчанию.



2. Инициализация резервных платформ центра управления сетью (см. стр. **77**).
3. Настройка синхронизации БД ЦУС (см. стр. **79**).
4. Ввод резервных КШ с ЦУС в эксплуатацию (см. стр. **42**).

Инициализация резервных платформ центра управления сетью

Конфигурация ЦУС считывается с носителей типа USB-флеш-накопитель. По умолчанию файл конфигурации ЦУС получает имя "ncc.cfg".

Для инициализации ЦУС:

1. Подключите к системному блоку КШ клавиатуру и монитор.
2. Включите питание монитора и КШ.

   На экране появится основное окно ПАК "Соболь", в центре которого будет отображаться запрос персонального идентификатора.
3. Не дожидаясь автоматической загрузки КШ, аккуратно приложите персональный идентификатор администратора ПАК "Соболь" к считывателю.

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

   На экране появится меню администратора ПАК "Соболь".

Примечание. Все сведения, необходимые администратору для управления работой ПАК "Соболь", содержатся в эксплуатационной документации ПАК "Соболь".

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.

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

   Начнется проверка целостности файлов установленного программного обеспечения средствами ПАК "Соболь" и далее будет выполнена загрузка операционной системы.

   Дождитесь появления на экране сообщения о выборе варианта дальнейших действий, подобного следующему:

```
Криптографический шлюз с ЦУС "Континент"
Конфигурация: ЦУС
Начальная конфигурация ЦУС
Инициализировать ЦУС с использованием файла конфигурации?
(Y/N):
```

6. Вставьте внешний носитель с файлом конфигурации ncc.cfg, введите "y" и нажмите клавишу <Enter>.

   На экране появится список обнаруженных на носителе файлов конфигурации, подобный следующему:

```
1.     ncc.cfg
Введите номер файла содержащего конфигурацию ЦУС:
```

7. Введите номер, соответствующий требуемому файлу. Нажмите клавишу <Enter>.

   На экране появится запрос на создание учетной записи локального администратора:

```
Создать учетную запись локального администратора? (Y/N)
```

8. При необходимости создать учетную запись локального администратора введите "y", нажмите клавишу <Enter> и последовательно введите его учетные данные.

   Примечание. Если в импортированной конфигурации ЦУС имелись данные об учетной записи локального администратора, запрос учетных данных будет опущен.

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

```
Конфигурация ЦУС завершена
```

   На экране появится главное меню ЦУС, подобное следующему:

```
1: Завершение работы
2: Перезагрузка
3: Управление конфигурацией
4: Настройка безопасности
5: Настройка СД <функция недоступна>
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. на стр. **100**.

9. Для завершения процедуры инициализации устройства введите "0" и нажмите клавишу <Enter>.

   Если в течение 5 секунд после появления последнего сообщения клавиша <Enter> нажата не будет, ПО 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.

10. Извлеките носитель из считывающего устройства.

    Загрузка ПО ЦУС осуществится автоматически. С этого момента устройство готово к работе.

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

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

Синхронизация БД ЦУС

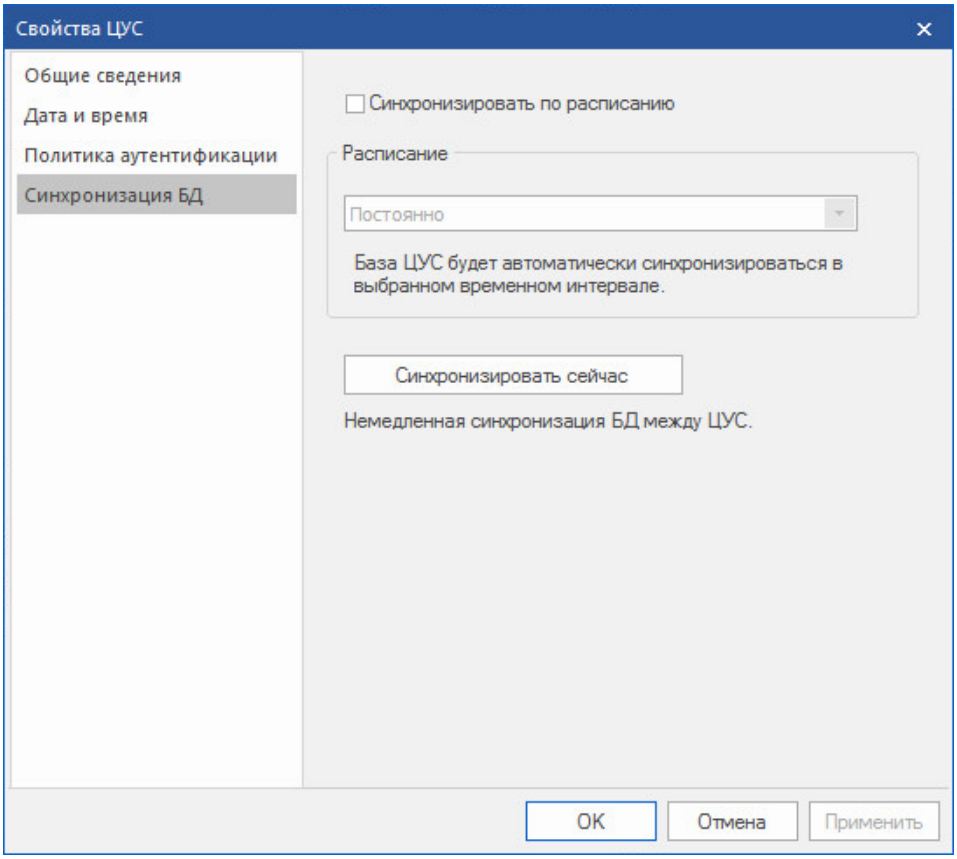
Для поддержания актуальной базы данных на всех платформах ЦУС между КШ с ЦУС должна производиться периодическая синхронизация, которая может осуществляться как периодически как по расписанию, через определенный интервал времени, так и по команде администратора.

Для настройки автоматической синхронизации БД ЦУС:

Внимание! Перед настройкой автоматической синхронизация БД ЦУС при необходимости сформируйте временной интервал, в течение которого она будет происходить (см. [**3**], параграф "Временной интервал"). По умолчанию имеется только один временной интервал "Постоянно", означающий формат "24/7".

1. Вызовите контекстное меню раздела "Центр управления сетью" области объектов управления и активируйте команду "Свойства...".

   На экране появится окно настройки свойств ЦУС.



2. Для включения периодической автоматической синхронизации установите отметку в поле "Синхронизировать по расписанию" и выберите требуемый временной интервал в области "Расписание".

   Внимание! Автоматическая синхронизация БД ЦУС сопровождается автоматической перезагрузкой пассивных КШ с ПО ЦУС после каждого изменения конфигурации комплекса.

3. Нажмите кнопку "ОК" в окне "Свойства ЦУС".

Для принудительной синхронизации БД ЦУС:

Внимание! Принудительная синхронизация БД ЦУС сопровождается перезагрузкой КШ с ПО ЦУС, БД которых будет обновлена.

1. Для принудительной синхронизации пассивных устройств ЦУС вызовите контекстное меню раздела "Центр управления сетью" области объектов управления, активируйте команду "Свойства...", нажмите кнопку "Синхронизировать сейчас", а затем подтвердите операцию, нажав кнопку "ОК" в появившемся окне подтверждения.

   На экране появится окно настройки свойств ЦУС.

2. Для принудительной синхронизации одного или нескольких пассивных устройств выберите их в списке криптошлюзов, вызовите контекстное меню и выберите "Синхронизировать БД ЦУС", а затем подтвердите операцию, нажав кнопку "ОК" в появившемся окне подтверждения.

Смена режима работы КШ с ЦУС

Переключение в активный режим осуществляет администратор централизованно через ПУ ЦУС или локально на КШ с ЦУС.

Для переключения КШ с ЦУС в активный режим при локальном управлении:

1. В главном меню (см. стр. **9**) введите номер команды "Управление конфигурацией" и нажмите клавишу <Enter>.

   На экране появится меню управления КШ.

2. Введите номер команды "Перевести ЦУС в активный режим" и нажмите клавишу <Enter>.

   В меню управления КШ данная команда дополнится текстом "<функция недоступна>".

3. Выйдите из режима настройки параметров, введя номер команды "Выход" и нажав клавишу <Enter>.

   На экране появится сообщение:

   ```
   Режим работы ЦУС: Активный
   Дата и время изменения БД ЦУС (UTC): <Дата, Время>
   ```

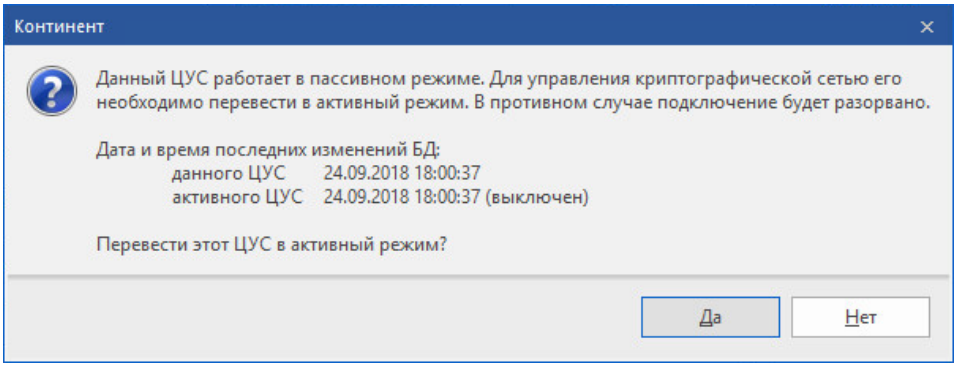
4. Дождитесь загрузки конфигурации комплекса и появления сообщения:

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

Для переключения КШ с ЦУС в активный режим при централизованном управлении:

1. В ПУ ЦУС осуществите подключение к пассивному КШ с ЦУС (см. стр. **34**) и пройдите процедуру аутентификации (см. стр. **28**).

   На экране появится информационное окно.



2. Нажмите кнопку "Да".

   ПУ ЦУС подключится к БД ЦУС, все КШ с ЦУС при этом примут состояние "Отключен".

3. Осуществите процедуру принудительной синхронизации БД ЦУС.

Глава 10
Обновление ПО комплекса

Общий порядок действий

Выполнение процедуры обновления программного обеспечения накладывает определенные ограничения на управление комплексом в штатном режиме и поэтому должно быть завершено в минимально допустимые сроки.

Примечание. Учетные данные и идентификаторы администраторов сетевых устройств комплекса на отчуждаемых носителях в ходе процедуры обновления не изменяются.

Обновление программного обеспечения комплекса выполняется в следующем порядке:

1. Подготовка к обновлению программного обеспечения комплекса (см. ниже).
2. Обновление ПО ЦУС, ПУ ЦУС (см. стр. **83**).
3. Установка лицензии на обновление ПО комплекса (см. стр. **35**).
4. В случае изменения системы журналирования — создание новой базы данных журналов и соответствующая настройка программного компонента "Конфигуратор БД журналов ЦУС" (см. [**5**], параграф "Конфигуратор").
5. Обновление ПО прочих сетевых устройств комплекса (см. стр. **85**).
6. Проверка работоспособности комплекса. В случае выявления сбоев рекомендуется провести процедуру смены ключей парной связи сетевых устройств комплекса (см. стр. **55**).

Внимание! Данная процедура приводится для обновления ПО комплекса версии 3.7.5 и выше. Для обновления с более старых версий ПО рекомендуется обратиться в службу технической поддержки.

После обновления ПО ЦУС совместная работа ЦУС с сетевыми устройствами необновленных версий имеет следующие особенности:

- На сетевых устройствах необновленных версий сохраняется работоспособность функций, настроенных до обновления ПО ЦУС.
- На сетевых устройствах необновленных версий настройка новых функций обновленного ПО ЦУС недоступна.
- Не рекомендуется вносить изменения в настройки сетевых устройств необновленных версий. Если изменения необходимы, их следует выполнить до обновления ПО ЦУС или после обновления ПО сетевого устройства.
- На сетевом устройстве не рекомендуется создавать и изменять правила фильтрации и трансляции до обновления ПО сетевого устройства.
- Не рекомендуется создавать сетевые объекты и привязывать их к сетевым устройствам необновленных версий.
- Для сетевых устройств необновленных версий сохраняется возможность переустановки парных связей.
- Возможность смены ключей сетевого устройства в случае их компрометации или истечения срока действия сохраняется.

Подготовка к обновлению программного обеспечения

Перед обновлением ПО комплекса необходимо выполнить следующие подготовительные действия:

1. Документирование всех настроек комплекса (идентификационные номера сетевых устройств, IP-адреса интерфейсов, структура сети, действующие правила фильтрации и маршрутизации). Эти данные могут понадобиться в случае неудачной загрузки конфигурации из резервной копии.

2. Проверка сроков действия ключей КШ. Ключи с истекшим сроком действия необходимо сменить (см. стр. **53**). В противном случае после обновления работоспособность сети будет нарушена.
3. При использовании однолетней схемы хранения ключей — сохранение ключей сетевых устройств на внешние носители (см. стр. **53**).

   Примечание. Данная схема является базовой и присутствует на всех версиях комплекса. Начиная с версии 3.7 введена альтернативная усиленная трехлетняя схема хранения ключей.
4. Проверка правил фильтрации и трансляции (см. [**3**]). Правила, использующие сервис IPv6-ICMP, требуется удалить или скорректировать, чтобы исключить применение в них данного сервиса.
5. Резервное копирование конфигурации ЦУС (см. стр. **67**).

Обновление ПО ЦУС, ПУ ЦУС

При обновлении ПО ЦУС используется резервная копия (файл конфигурации), сохраненная при подготовке к обновлению и соответствующая более ранней версии ПО.

Для обновления ПО ЦУС:

1. Выполните установку ПО "Континент" на ЦУС (см. ниже).
2. Выполните инициализацию ЦУС с использованием файла конфигурации (см. стр. **77**).
3. На АРМ администратора удалите программу управления ЦУС старой версии (см. стр. **36**).

   После удаления программы управления перезагрузите компьютер.
4. На АРМ администратора установите программу управления ЦУС новой версии (см. [**2**]).
5. Запустите программу управления ЦУС и подключитесь к ЦУС (см. стр. **28**).

Установка ПО "Континент"

АПКШ "Континент" поставляется на установочном компакт-диске с ПО. Если аппаратная платформа не располагает соответствующим приводом, необходимо использовать внешний привод оптических дисков.

Для установки программного обеспечения:

1. Подключите к системному блоку сетевого устройства клавиатуру, монитор и при необходимости внешний привод оптических дисков.
2. Вставьте входящий в комплект поставки CD/DVD-ROM в привод компакт-дисков. Затем включите питание сетевого устройства.

   На экране появится окно ПАК "Соболь", в центре которого будет отображаться запрос персонального идентификатора:

   ```
   Предъявите персональный идентификатор
   ```
3. Не дожидаясь автоматической загрузки сетевого устройства, приложите персональный идентификатор администратора ПАК "Соболь" к считывателю.

   Совет. При автоматической загрузке сетевого устройства установка программного обеспечения невозможна. В этом случае перезагрузите устройство и повторите процедуру.

   После успешного считывания информации из идентификатора на экране появится запрос пароля.
4. Введите пароль администратора, назначенный вами при смене пароля или указанный в паспорте сетевого устройства (п. 2.2, графа "Пароль администратора по умолчанию").

   Совет. Если для администратора не задан пароль по умолчанию, для продолжения работы нажмите клавишу <Enter>.

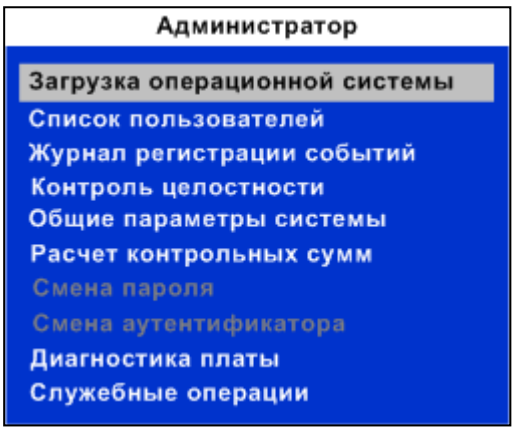
На экране появится предупреждение, подобное следующему:

```
"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".

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

   На экране появится меню администратора:



Внимание! 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 руководстве администратора ПАК "Соболь".

6. 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 сначала. 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]:
```

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

   На экране появится предупреждение:

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

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

   На экране появится предупреждение:

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

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

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.

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

На экране появится запрос:

```
Введите идентификатор:
```

11. Введите идентификационный номер сетевого устройства и нажмите клавишу <Enter>.

Примечания:

- Идентификационный номер указан в п. 2.2 паспорта сетевого устройства и на его задней панели.
- При установке или обновлении ПО резервного сетевого устройства введите идентификационный номер основного сетевого устройства кластера. Идентификационные номера основного и резервного сетевых устройств должны быть идентичны.

На экране появятся строка конфигурации данного сетевого устройства и запрос на указание аппаратной платформы.

12. Введите номер варианта используемой аппаратной платформы и нажмите клавишу <Enter>. Тип шасси аппаратной платформы указан в п. 1.2.1 паспорта сетевого устройства.

Начнется копирование файлов, запись данных в память ПАК "Соболь" и постановка файлов на контроль целостности. При успешном завершении процессов на экране появится сообщение:

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

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

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.

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

13. Для загрузки ОС и инициализации устройства выберите с помощью управляющих клавиш клавиатуры в меню администратора команду "Загрузка операционной системы" и нажмите клавишу <Enter>.

14. Перейдите к выполнению п. **7** процедуры инициализации ЦУС (см. [**2**]).

Обновление программного обеспечения сетевых устройств

Для обновления ПО сетевых устройств используется файл обновления update_all_release.tar, входящий в состав установочного компакт-диска комплекса.

Внимание! Версия обновления ПО сетевого устройства должна соответствовать версии обновленного ПО ЦУС.

При обновлении ПО сетевого устройства последовательно выполняют следующие процедуры:

1. Удаление предыдущей версии файла обновления ПО.

2. Загрузка файла обновления на ЦУС.
3. Загрузка файла обновления на сетевое устройство.
4. Обновление файлов сетевых устройств.

Внимание! При обновлении ПО кластера:
- Основное и резервное устройства кластера должны находиться в рабочем режиме.
- Параметр "Режим обратного переключения" устройств кластера должен иметь значение "Автоматический" (см. стр. 70).

Удаление предыдущей версии файла обновления ПО

Для удаления:

1. В контекстном меню раздела "Центр управления сетью" выберите пункт "Свойства...".

   На экране появится окно "Свойства ЦУС".
2. Нажмите кнопку "Удалить ПО", если она активна. Если кнопка недоступна, значит файл последнего обновления уже удален.

   На экране появится запрос для подтверждения операции удаления ПО.
3. Нажмите кнопку "Да" для удаления текущей версии ПО.

Загрузка файла обновления на ЦУС

Описанную ниже процедуру используют для загрузки файла обновления update_all_release.tar для последующей загрузки на сетевые устройства комплекса.

Для загрузки файла обновления на ЦУС:

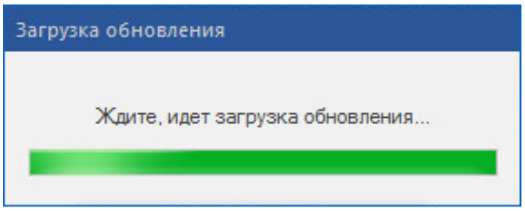
1. В контекстном меню раздела "Центр управления сетью" выберите пункт "Свойства...".

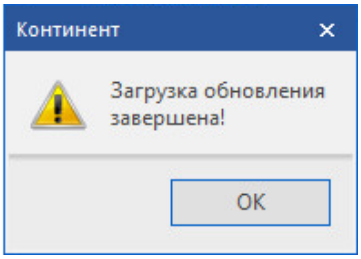
   На экране появится окно "Свойства ЦУС".
2. Нажмите кнопку "Загрузить ПО".

   На экране появится окно открытия файла.
3. Откройте нужную папку, укажите файл обновления и нажмите кнопку "Открыть".

   Примечание. При обновлении посредством компакт-диска с дистрибутивом ПО файл обновления находится в папке ...\Setup\Continent\UPDATE\.

   Файл обновления будет скопирован на жесткий диск КШ с ЦУС. По окончании процесса копирования на экран будет выведено соответствующее сообщение.





4. Нажмите кнопку "ОК", чтобы закрыть сообщение.

   В поле "Текущая версия" окна свойств ЦУС будет показан номер версии ПО, содержащегося в файле обновления.
5. Нажмите кнопку "ОК" для закрытия окна "Свойства ЦУС".

Загрузка файла обновления на сетевое устройство

Для загрузки файла обновления на сетевое устройство:

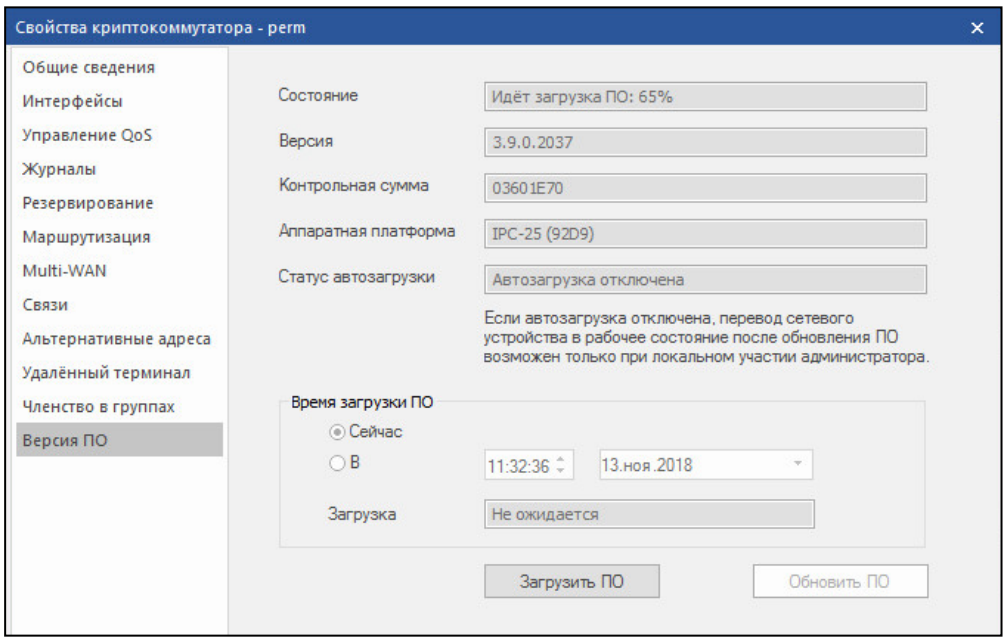
1. В контекстном меню сетевого устройства выберите пункт "Свойства...".

   На экране появится окно свойств сетевого устройства.
2. Выберите вкладку "Версия ПО".
3. В группе полей "Время загрузки ПО" укажите нужное время и нажмите кнопку "Загрузить ПО".

   Примечание. При установке отметки в поле "Сейчас" загрузка файла обновления на устройство выполняется немедленно после закрытия окна.

   Задание на загрузку файла обновления на сетевое устройство будет передано в ЦУС, а на экране появится сообщение об этом.
4. Закройте окно сообщения для возврата в окно свойств сетевого устройства.
5. Нажмите кнопку "ОК", чтобы закрыть окно свойств сетевого устройства.

В указанное время файл обновления будет загружен на сетевое устройство, а в поле "Состояние" вкладки "Версия ПО" свойств сетевого устройства станет доступной кнопка "Обновить ПО". В ходе загрузки в поле "Состояние" будет отображаться прогресс загрузки ПО. После окончания загрузки в поле "Состояние" будет отображена версия ПО обновления.



Обновление файлов сетевых устройств

Приведенную ниже процедуру выполняют после загрузки на сетевые устройства файла обновления update_all_release.tar.

Для обновления:

1. В контекстном меню сетевого устройства выберите пункт "Свойства...".

   На экране появится окно свойств сетевого устройства.
2. Выберите вкладку "Версия ПО" и нажмите кнопку "Обновить ПО" для выполнения процедуры обновления в текущий момент.

   Примечание. При необходимости отложить проведение процедуры обновления в группе полей "Время загрузки ПО" укажите нужное время и нажмите кнопку "Обновить ПО". На экране появится подтверждение о проведении обновления в указанный срок.
3. Закройте окно сообщения для возврата в окно свойств сетевого устройства.
4. Нажмите кнопку "ОК" для закрытия окна свойств сетевого устройства.

В указанное время система приступит к обновлению ПО. В процессе обновления автоматически выполняется перезагрузка сетевого устройства. Изменение версии ПО по окончании процесса обновления можно увидеть в ПУ ЦУС:

- в окне свойств сетевого устройства на вкладке "Версия ПО";
- при выборе папки ЦУС на панели навигации в области "Версия ПО".

Приложение

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
TCP/22	Передача данных SSH	РМ / СУ
TCP/4444	Передача сообщений. ПУ ЦУС, активный и пассивный 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. Активный ЦУС / пассивный ЦУС. Пассивный ЦУС / активный ЦУС. Агент ЦУС и СД / ЦУС. ЦУС / агент ЦУС и СД. Аент ЦУС и СД / ЦУС. Агент обновлений БРП / ЦУС. ЦУС / агент обновлений БРП. Агент РКН / ЦУС. ЦУС / агент РКН
TCP/4445	Передача обновлений ПО	ПУ ЦУС / ЦУС
	Обмен сообщениями. ПУ ЦУС устанавливает подключение со случайного порта из диапазона 1024-65535 на порт ЦУС 4445. ЦУС отвечает на тот порт, с которого было обращение	ПУ ЦУС / агент ЦУС и СД. Агент ЦУС и СД / ПУ ЦУС
TCP/4446	Аутентификация 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	Клиент аутентификации / ЦУС. ЦУС / Клиент аутентификации
TCP/5100	Передача сообщений	ЦУС / КШ
	Обмен сообщениями в кластере. Узел кластера обращается к парному со случайного порта из диапазона 10000-65535 на порт 5100. Парный отвечает на тот порт, с которого было обращение	Основной КШ / резервный КШ. Резервный КШ / основной КШ
TCP/5101	Обмен сообщениями (для узлов версии 3.7 и ниже). КШ устанавливает подключение со случайного порта 10000-65535 на порт ЦУС 5101. ЦУС отвечает на тот порт, с которого было обращение	КШ / ЦУС. ЦУС / КШ
TCP/5103	Передача файлов. КШ устанавливает подключение со случайного порта 10000-65535 на порт ЦУС 5103. ЦУС отвечает на тот порт, с которого было обращение	ЦУС / КШ. КШ / ЦУС
TCP/5109	Связь ЦУС с узлами (для узлов версии 3.9 и выше)	ЦУС / СУ.
UDP/123	Передача данных синхронизации NTP	ЦУС / внешний NTP-сервер
UDP/161	Передача данных SNMP	РМ администратора / СУ
UDP/5101	Передача сообщений от КШ к ЦУС (для узлов версии 3.7 и ниже). КШ обращается с порта 5100 на порт ЦУС 5101. ЦУС отвечает с порта 5101 на порт 5100	КШ / ЦУС. ЦУС / КШ

Протокол/ порт	Описание	Источник/получатель
UDP/5106 UDP/5107	Поддержка работы КШ за NAT-узлом. В зависимости от используемых классов трафика, КШ отправляют пакеты с портов 10000-10031 на порты ЦУС 5106-5107	КШ / ЦУС
UDP/5109	Связь ЦУС с узлами (для узлов версии 3.9 и выше)	ЦУС / СУ. СУ / ЦУС
UDP/5557	Обмен сообщениями об активности между КШ в кластере (с порта 5557 на порт 5557)	Основной КШ / резервный КШ. Резервный КШ / основной КШ
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. ЦУС / СУ

Права пользователей на администрирование комплекса

("+" — элемент управления доступен, "–" — элемент управления недоступен)

Элемент управления программы управления ЦУС	Роль пользователя			
	Главный администратор	Администратор сети	Администратор ключей	Аудитор
Управление настройками комплекса				
Изменение списка сетевых объектов и групп сетевых объектов	+	+	–	–
Изменение списка сервисов и групп сервисов	+	+	–	–
Управление учетными записями пользователей	+	+	–	–
Изменение классов трафика	+	+	–	–
Изменение временных интервалов	+	+	–	–
Изменение реакций на события	+ (создание, удаление, изменение)	+ (создание, удаление, изменение)	–	+ (изменение)
Изменение профилей усиленной фильтрации	+	+	–	–
Изменение профилей контроля приложений	+	+	–	–
Изменение списка сертификатов	+ (создание, удаление, импорт)	+ (создание, удаление, импорт)	+ (импорт)	–
Изменение настроек виртуальных коммутаторов	+	+	–	–
Изменение списка администраторов комплекса	+ (создание, удаление, изменение, просмотр)	–	–	+ (просмотр)

Элемент управления программы управления ЦУС	Роль пользователя			
	Главный администратор	Администратор сети	Администратор ключей	Аудитор
Изменение списка локальных администраторов сетевых устройств	+	–	–	–
Управление настройками комплекса — Правила фильтрации				
Просмотр правил фильтрации	+	+	–	+
Изменение правил фильтрации	+	+	–	–
Управление доступом локальных администраторов				
Доступ к устройству по SNMP	+	–	–	–
Доступ к локальному меню команд устройства по SSH	+	–	–	–
Доступ к локальному меню команд устройства с консоли	+	–	–	–
Управление настройками сетевого устройства				
Сбросить признак НСД	+	+	–	+
Перезагрузить сетевое устройство	+	+	–	–
Выключить сетевое устройство	+	+	–	–
Очистить таблицу состояний соединений	+	+	–	–
Синхронизировать БД ЦУС (для резервного ЦУС)	+	+	–	–
Обновить конфигурацию	+	+	–	–
Сохранить конфигурацию…	+	+	–	–
Сохранить текущие ключи на носитель	+	–	+	–
Сбор журналов	+	+	+	+
Просмотр журналов	+	+	+	+
Диагностика сетевого устройства	+	+	–	–
Управление ключами сетевых устройств	+	–	+	–
Сменить ключи устройства	+	–	+	–
Создать резервный комплект ключей сетевого устройства	+	–	+	–
Загрузить ключи сетевого устройства с носителя на ЦУС	+	–	+	–
Сменить все ключи парных связей сетевого устройства	+	–	+	–
Создать сетевое устройство/группу сетевых устройств	+	+	–	–
Удалить сетевое устройство/группу сетевых устройств	+	+	–	–

Элемент управления программы управления ЦУС	Роль пользователя			
	Главный администратор	Администратор сети	Администратор ключей	Аудитор
Свойства сетевого устройства — Общие				
Название	+	+	–	–
Описание	+	+	–	–
Часовой пояс	+	+	–	–
Введен в эксплуатацию	+	+	–	–
Мягкий режим	+	+	–	–
Аутентификация пользователей	+	–	–	–
Оптимизация правил фильтрации	+	+	–	–
Минимальный размер сжимаемого пакета	+	+	–	–
Период контроля целостности файлов	+	+	–	–
Изменить настройки поиска MTU	+	+	–	–
Изменить минимальный MSS	+	+	–	–
Свойства сетевого устройства — Интерфейсы	+	+	–	–
Свойства сетевого устройства — Управление QOS	+	+	–	–
Свойства сетевого устройства — DHCP	+	+	–	–
Свойства сетевого устройства — Журналы	+	–	–	+
Свойства сетевого устройства — Резервирование	+	+	–	–
Свойства сетевого устройства — Маршрутизация	+	+	–	–
Свойства сетевого устройства — Multi-WAN	+	+	–	–
Свойства сетевого устройства — DNS	+	+	–	–
Свойства сетевого устройства — Связи	+	–	+	–
Свойства сетевого устройства — Альтернативные адреса	+	+	–	–
Свойства сетевого устройства — Удаленный терминал	+	–	–	–

Элемент управления программы управления ЦУС	Роль пользователя			
	Главный администратор	Администратор сети	Администратор ключей	Аудитор
Свойства сетевого устройства — SNMP мониторинг	+	–	–	–
Свойства сетевого устройства — Членство в группах	+	+	–	–
Настройки ДА				
Изменение параметров ДА	+	+	–	–
Изменение списка регистрируемых приложений	+	+	–	–
Настройки ЦУС				
Сохранить / загрузить файл конфигурации	+	+	–	–
Создание ключевого носителя агента	+	–	–	+
Параметры соединения с агентом ЦУС и СД	+	+	+	+
Настройка агента ЦУС и СД	+	–	–	+
Настройка агента обновлений БРП	+	+	–	–
Загрузить файл обновлений БРП	+	+	–	–
Загрузить файл РКН	+	+	–	–
Управление ключами сетевых устройств	+	–	+	–
Копировани ключей ЦУС и сервера доступа	+	+	+	+
Настройка смены ключей устройств по расписанию	+	–	+	–
Смена ключей всех сетевых устройств	+	–	+	–
Сохранить диагностический файл БД ЦУС	+	+	–	–
Управление списком лицензий	+	+	+	+
Свойства ЦУС — Общие сведения				
Управление версией ПО	+	+	–	–
Смена режима управления ключевой информацией	+	+	+	–
Максимальные размеры журналов	+	–	–	–
Включение режима изолированной сети	+	–	–	–
Свойства ЦУС — Дата и время	+ (локальное, через NTP)	+ (локальное)	–	–
Свойства ЦУС — Политика аутентификации	+	–	–	–

Элемент управления программы управления ЦУС	Роль пользователя			
	Главный администратор	Администратор сети	Администратор ключей	Аудитор
Настройки программы управления				
Параметры соединения с ЦУС	+	+	+	+
Очередь заданий сетевого устройства				
Просмотр очереди заданий	+	+	–	–
Удаление задания из очереди	+	+	–	–
Очистить очередь заданий	+	+	–	–
Управление настройками внешних крипто-графических сетей				
Создание внешней сети	+	+	–	–
Удаление внешней сети	+	+	–	–
Импорт сертификата внешней сети	+	+	+	–
Создание сертификата для внешней сети	+	+	–	–
Импорт конфигурации внешней сети	+	+	–	–
Экспорт конфигурации для внешней сети	+	+	–	–
Создание межсетевого ключа	+	–	–	–
Активация межсетевого ключа	+	–	–	–

Формат и примеры конфигурационных файлов

Для создания конфигурационных файлов можно использовать любой текстовый редактор, например "Блокнот".

В конфигурационных файлах должны быть определены:

- маршруты по умолчанию;
- статические маршруты, которые должны быть загружены в таблицу маршрутизации.

В конце конфигурационных файлов должна быть пустая строка.

Формат конфигурационного файла OSPF

В таблицах ниже представлены основные параметры конфигурационных файлов, используемые для настройки динамической маршрутизации.

Табл.9 Формат файла zebra.conf

Параметр	Описание
hostname <имя хоста>	Установка имени хоста
log stdout	Установка режима протоколирования на консоль
log file/var/zebra.log	Экспорт журналов событий динамической маршрутизации из КШ на USB-флеш-накопитель (локально)

Параметр	Описание
ip route <адрес/маска> <шлюз>	Определение статического маршрута и маршрута по умолчанию

Табл.10 Формат файла ospfd.conf

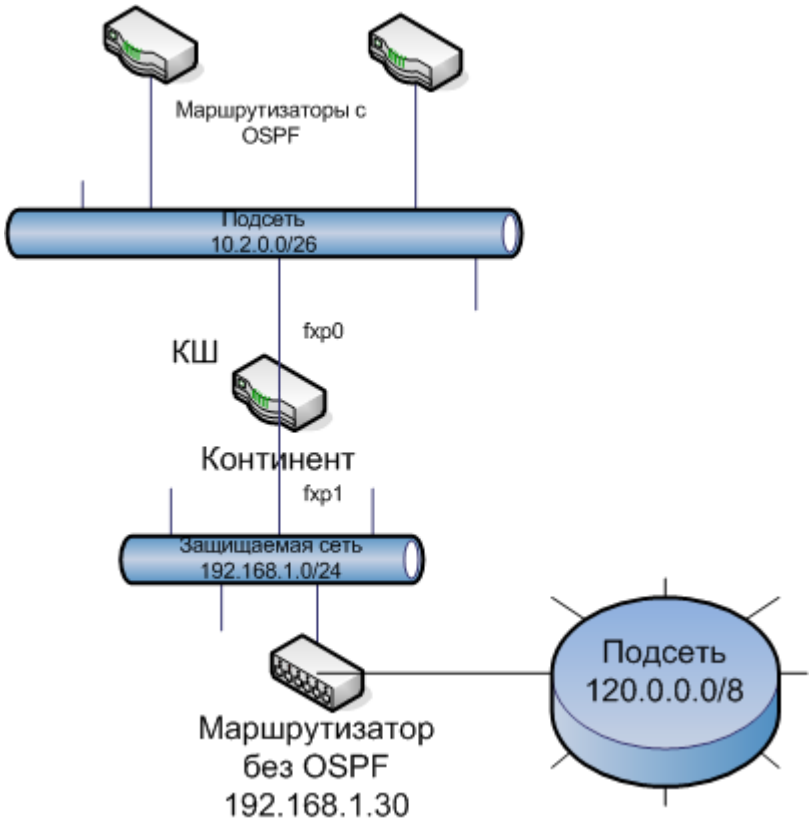
Параметр	Описание
router ospf	Включение OSPF-процесса
network <адрес/маска> area <номер>	Определение диапазона адресов интерфейсов, которые используются для обмена служебной информацией в процессе OSPF-маршрутизации
interface <имя>	Определение имени интерфейса, используемого для обмена служебной информацией в процессе OSPF-маршрутизации
ip ospf authentication message-digest	Установка режима аутентификации OSPF-маршрутизатора
ip ospf message-digest-key 1 <алгоритм> <ключ>	Установка аутентификационного ключа OSPF-маршрутизатора. Использовать указанный алгоритм и ключ (ключ может достигать длины 16 символов)

Примеры конфигурационных файлов

Данный пример иллюстрирует создание конфигурационных файлов для КШ в типовой схеме включения, показанной на рисунке ниже.

Защищаемая сеть 192.168.1.0/24 (например, территориальный филиал какой-либо организации) для связи с другим удаленным филиалом (на рисунке не показан) использует подсеть 10.2.0.0/26 с маршрутизаторами, поддерживающими OSPF.

В состав защищаемой сети входит подсеть 120.0.0.0/8. Для связи с подсетью используется маршрутизатор без OSPF (192.168.1.30).



Для того чтобы обеспечить динамическую маршрутизацию при прохождении трафика между подсетью 120.0.0.0/8 и другим удаленным филиалом, на КШ должна быть выполнена настройка динамической маршрутизации.

Для приведенной выше схемы конфигурационные файлы имеют следующий вид:

zebra.conf

```
hostname continent
log stdout
# статический маршрут в подсеть
ip route 120.0.0.0/8 192.168.1.30
```

ospfd.conf

```
log stdout
router ospf
network 10.2.0.0/26 area 0.0.0.1
area 0.0.0.1 authentication message-digest
# разрешается анонсирование статических маршрутов
redistribute static
interface em0
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 1234567890
```

Формат конфигурационного файла BGP

В таблицах ниже представлены основные параметры конфигурационных файлов, используемые для настройки динамической маршрутизации по протоколу BGP.

Табл.11 Формат файла zebra.conf

Параметр	Описание
hostname <имя хоста>	Установка имени хоста

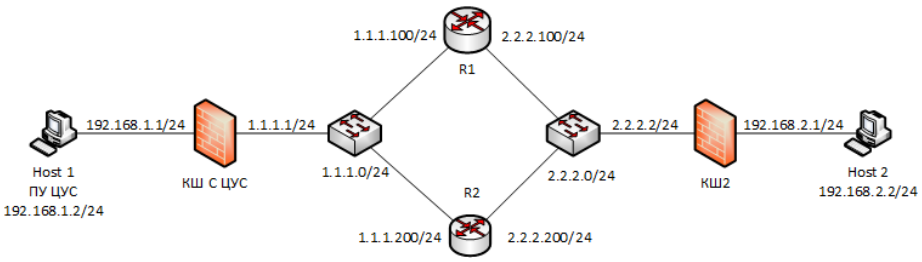
Параметр	Описание
interface <имя>	Установка интерфейса
ip forwarding	Включение пересылки IP-пакетов
line vty	Включение режима конфигурирования интерфейса VTY
exec-timeout <минуты секунды>	Установка времени ожидания подключения по VTY
log stdout	Установка режима протоколирования на консоль
log file /var/zebra.log	Экспорт журналов событий динамической маршрутизации из КШ на USB-флеш-накопитель (локально)

Табл.12 Формат файла bgpd.conf

Параметр	Описание
hostname <имя хоста>	Установка имени хоста
router bgp <имя АС>	Включение BGP-процесса для АС
bgp router-id <идентификатор>	Установка ID роутера
bgp log-neighbor-changes	Включение регистрации изменений состояния BGP-соседей
no synchronization	Отключение синхронизации маршрутов
network <IP-диапазон>	Объявление сети для всех соседей
neighbor <IP-адрес> remote-as <имя АС>	Создание соседа
neighbor <IP-адрес> weight <величина>	Указание веса соседа (больший приоритет имеет сосед с большим весом)
log stdout	Установка режима протоколирования на консоль
log file /var/bgp.log	Экспорт журналов событий динамической маршрутизации из КШ на USB-флеш-накопитель (локально)

Примеры конфигурационных файлов

Данный пример иллюстрирует создание конфигурационных файлов для КШ в типовой схеме включения, показанной на рисунке ниже.



Для приведенной выше схемы конфигурационные файлы имеют следующий вид:

zebra.conf для Host 1

```
hostname CUS
interface em0
```

```
ip forwarding
line vty
exec-timeout 0 0
log stdout
log file /var/bgp.log
```

bgpd.conf для Host 1

```
hostname CUS
router bgp 10
bgp router-id 1.1.1.1
bgp log-neighbor-changes
no synchronization
network 1.1.1.0/24
neighbor 1.1.1.100 remote-as 100
neighbor 1.1.1.100 weight 2000
neighbor 1.1.1.200 remote-as 200
neighbor 1.1.1.200 weight 1000
log stdout
log file /var/bgp.log
```

zebra.conf для Host 2

```
hostname CGW2
interface em0
ip forwarding
line vty
exec-timeout 0 0
log stdout
log file /var/bgp.log
```

bgpd.conf для Host 2

```
hostname CGW2
router bgp 20
bgp router-id 2.2.2.2
bgp log-neighbor-changes
no synchronization
network 2.2.2.0/24
neighbor 2.2.2.100 remote-as 100
neighbor 2.2.2.100 weight 2000
neighbor 2.2.2.200 remote-as 200
neighbor 2.2.2.200 weight 1000
log stdout
log file /var/bgp.log
```

Диагностика сетевого устройства

Средствами ПУ ЦУС можно выполнить диагностику работы сетевого устройства. Результаты диагностики представляются в виде следующих отчетов:

Отчет	Описание
Ресурсы сетевого устройства	Информация о загруженности каждого процессора. Общий и свободный объем оперативной памяти. Общий объем жесткого диска, а также объем используемого и свободного пространства. Максимальные и текущие объемы журналов
arp/ndp	Содержимое ARP- и NDP-кеша
ping*	Результаты выполнения команды ping
traceroute*	Результаты выполнения команды traceroute

Отчет	Описание
tcpdump	Информация о сетевом трафике выбранного интерфейса с возможностью применения фильтра в формате tcpdump. Отчет выводится в окне в виде текстового файла. Для сетевого устройства, выведенного из эксплуатации, предусмотрено сохранение отчета в двоичном коде для последующего просмотра специализированным приложением
Таблица состояний (только для КШ)	Количество установленных соединений с возможностью раздельного просмотра сессий IPv4 и IPv6. При просмотре сессий могут быть использованы фильтр и функция поиска
Сетевые соединения	Сведения об открытых сетевых соединениях
Шифратор (только для КШ)	Статистическая информация о работе шифратора
Технологический отчет	Технологический отчет, выгружаемый на отчуждаемый носитель для отправки в службу поддержки
Пропущенные пакеты (только для ДА)	Сведения о количестве пропущенных пакетов

*Для выполнения команд ping и traceroute на устройстве автоматически создаются временные правила фильтрации, разрешающие прохождение соответствующих пакетов.

Для формирования отчета:

1. Выберите в списке сетевое устройство, и в контекстном меню устройства выберите пункт "Диагностика".

   На экране появится окно "Диагностика".

2. Выберите вкладку отчета, настройте при необходимости его параметры и нажмите кнопку "Выполнить".

   В зависимости от выбранного отчета результат будет выведен в окне "Диагностика сетевого устройства" или сохранен в соответствии с заданными настройками.

Внимание! При формировании нескольких отчетов задания по их подготовке и отображению ставятся в очередь с выводом на экран соответствующего предупреждения. Формирование каждого следующего отчета начинается только после завершения предыдущего. Поэтому не рекомендуется закрывать окно диагностики до вывода на экран очередного отчета, так как при закрытии окна формируемый отчет не сохраняется.

Сохранение базы данных ЦУС

В случае возникновения проблем, связанных с функционированием комплекса, может потребоваться передача копии БД ЦУС в службу технической поддержки.

В этом случае необходимо создать копию БД ЦУС. Файл копии не содержит конфиденциальной информации и предназначен исключительно для анализа в службе технической поддержки.

Внимание! Запрещается загрузка файла копии базы данных в БД ЦУС.

Для сохранения копии БД ЦУС:

1. В контекстном меню раздела "Центр управления сетью" выберите пункт "Сохранить диагностический файл БД ЦУС...".

   На экране появится окно задания пароля.

2. Введите и подтвердите пароль.

   На экране появится окно сохранения файла.

3. Укажите путь сохранения файла копии БД ЦУС, при необходимости измените имя и нажмите кнопку "ОК".

   Примечание. Копия БД ЦУС сохраняется в виде файла с расширением *.support_cfg.

Файл копии БД ЦУС будет сохранен, на экране появится окно об успешном завершении операции.

4. Нажмите кнопку "ОК" и передайте файл и пароль в службу технической поддержки (см. стр. **7**).

Аппаратное тестирование сетевого устройства

Аппаратное тестирование может выполняться в ходе инициализации сетевого устройства и при последующей настройке его параметров средствами локального управления.

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, подобное следующему:

```
Тестирование
1: Тестирование диска
2: Тестирование процессора
3: Тестирование памяти
4: Тестирование сетевых интерфейсов
5: Общий тест
0: Выход
Выберите пункт меню (0-5):
```

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

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

Тестируемый объект	Описание тестирования
Диск	Проверка наличия сбойных секторов жесткого диска
Процессор	Проверка работы процессора. Необходимо задать время тестирования – от 1 до 99 минут
Память	Проверка оперативной памяти
Сеть/сетевые интерфейсы	Проверка работы сетевых интерфейсов. Перед запуском теста необходимо присоединить сетевые интерфейсы к общему коммутатору и соединить оптические интерфейсы в пары
Общий	Последовательное выполнение всех перечисленных выше тестов с предварительным выполнением соответствующих дополнительных действий
Команды, доступные из раздела "Диагностика платы" ПАК "Соболь"	
Память ПАК "Соболь"	Тестирование памяти ПАК "Соболь" на чтение и запись
Датчик случайных чисел	Проверка работоспособности датчика случайных чисел ПАК "Соболь"

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

   Будет выполнен возврат в меню выбора теста.

4. Для выхода из режима тестирования введите номер команды "Выход" и нажмите клавишу <Enter>.

Загрузка сведений о запрещенных ресурсах

Порядок получения сведений о запрещенных ресурсах единого реестра приведен на портале Роскомнадзора по адресу http://vigruzki.rkn.gov.ru/.

Сведения (выгрузка) представляют собой xml-файл, который должен быть загружен в БД ЦУС.

Загрузка файла в БД ЦУС может быть выполнена вручную средствами ПУ ЦУС или автоматически агентом Роскомнадзора (о настройке и работе агента см. стр. **63**).

Для загрузки файла вручную:

1. В контекстном меню раздела "Центр управления сетью" выберите пункт "Загрузить файл реестра запрещенных ресурсов".

   На экране появится окно выбора файла.

2. Укажите файл выгрузки и нажмите в окне кнопку "Открыть".

   Сведения о запрещенных ресурсах будут загружены в БД ЦУС.

Для просмотра сведений о запрещенных ресурсах в БД ЦУС:

- В списке объектов ПУ ЦУС выберите подраздел "Центр Управления Сетью | Группы сетевых объектов | Реестр запрещенных ресурсов".

  В главном окне отобразится список запрещенных ресурсов. В дополнительном окне отобразится список правил фильтрации, в которых используется группа сетевых объектов "Реестр запрещенных ресурсов".

  Примечание. Если такие правила фильтрации не создавались, список в дополнительном окне будет пустым.

Группа "Реестр запрещенных ресурсов" удалению и редактированию не подлежит.

Звуковые сообщения о работе сетевого устройства

При отсутствии монитора работа сетевого устройства контролируется с помощью звуковых сигналов.

Табл.13 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.14 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.15 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.16 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 на USB-флеш-накопителе. Была нарушена целостность файлов	Подключите к сетевому устройству монитор, войдите с правами администратора в ПАК и устраните ошибку

Табл.17 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

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-адрес сервера, 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. [**6**]).
4. Подключите КШ к сетевым коммуникациям и выполните его инициализацию (см. [**2**]).

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. стр. **44**).
2. Выведите КШ из эксплуатации. Для этого на вкладке "Общие сведения" удалите отметку из поля "Введен в эксплуатацию". При этом осуществится разрыв управляющего соединения ЦУС с КШ.
3. Зарегистрируйте новый PPP-интерфейс (см. [**6**]).
4. Сохраните конфигурацию данного КШ на носитель (см. [**1**]).
5. Подключите модем к выбранной телефонной линии (см. документацию на используемый модем).
6. Выполните инициализацию данного КШ, используя носитель с сохраненной конфигурацией (см. [**2**]).
7. Введите КШ в эксплуатацию. Для этого в программе управления в окне свойств 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". Версия 3.9. Руководство администратора. Принципы функционирования комплекса.
2. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9. Руководство администратора. Ввод в эксплуатацию.
3. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9. Руководство администратора. Межсетевое экранирование.
4. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9. Руководство администратора. Настройка VPN.
5. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9. Руководство администратора. Аудит.
6. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9. Руководство администратора. Сетевые функции.