КОД безопасности

Аппаратно-программный комплекс шифрования

Континент
Версия 3.9

Руководство администратора

Ввод в эксплуатацию

RU.88338853.501430.022 90 2

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
АПКШ	Аппаратно-программный комплекс шифрования
БД	База данных
ДА	Детектор атак
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
СД	Сервер доступа
СЗИ	Средство защиты информации
СУ	Сетевое устройство (КШ, ДА)
ЦУС	Центр управления сетью
BIOS	Basic Input-Output System
IP	Internet Protocol
PPPoE	Point to Point Protocol over Ethernet
QoS	Quality of Service
OSPF	Open Shortest Path First
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USB	Universal Serial Bus
UTC	Coordinated Universal Time (фр. Temps Universel Coordonné)
VoIP	Voice over IP

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.

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.

Порядок ввода комплекса в эксплуатацию

Ввод комплекса в эксплуатацию состоит из следующих этапов:

1. Инициализация ЦУС (см. стр. **7**).
2. Установка пакета программ администрирования комплекса (см. стр. **11**).
3. Настройка контроля целостности программного обеспечения комплекса (см. стр. **16**).
4. Запуск программы управления (см. стр. **17**).
5. Конфигурирование базы данных журналов, настройка агентов ЦУС и СД (при необходимости аудита, см. [**4**]).
6. Регистрация сетевых устройств, входящих в комплекс (см. стр. **21**).
7. Настройка QoS на внешнем интерфейсе КШ (см. стр. **27**).
8. Инициализация зарегистрированных сетевых устройств (см. стр. **28**).

   Примечание. 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. Перечень протоколов и портов, по которым осуществляется обмен служебными пакетами между компонентами комплекса, приведен на стр. **35**.

9. Ввод в эксплуатацию инициализированных сетевых устройств (см. стр. **30**), настройка параметров журналирования (при необходимости аудита, см. [**4**]).
10. Тестовая эксплуатация комплекса (см. стр. **30**).

Глава 1
Инициализация ЦУС и установка программ администрирования комплекса

Инициализация центра управления сетью

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

Внимание! Если планируется развертывание резервного ЦУС в сегменте сети, отличном от основного ЦУС, резервный ЦУС необходимо инициализировать на статической маршрутизации (см. стр. **24**). Смена типа маршрутизации возможна только после передачи резервному ЦУС конфигурации от активного ЦУС (в ПУ ЦУС резервный ЦУС отобразится со статусом "Подключен").

Для инициализации ЦУС подготовьте:

- клавиатуру и монитор для подключения к системному блоку КШ;
- USB-флеш-накопитель для записи идентификатора администратора комплекса;
- информацию об IP-адресе маршрутизатора по умолчанию, а также выделите IP-адреса для внешнего и внутреннего интерфейса КШ;

  Примечание. Примеры подключения и настройки интерфейсов КШ к действующим локальным сетям приведены в документе [3].

- ключевой блокнот РДП-006 в случае его использования в качестве источника исходной ключевой информации.

  Примечание. В качестве источника исходной ключевой информации используется ПАК "Соболь" или ключевой блокнот РДП-006.

Для инициализации ЦУС:

1. Подключите к системному блоку КШ клавиатуру и монитор.
2. Включите питание монитора и КШ, затем войдите в меню настройки BIOS (BIOS Setup).

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

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

   Пример. Для Москвы нужно вместо UTC+3 установить UTC.

4. Закройте меню настройки BIOS с сохранением внесенных изменений.

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

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

   Внимание! Запрещается использование комплекса с постоянно подключенным идентификатором iButton.

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

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

5. Введите пароль администратора 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 руководстве администратора 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.

6. 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):
   ```

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

   На экране появится запрос на указание внешнего интерфейса КШ, подобный следующему:

   ```
   Обнаруженные интерфейсы:
   Номер  Имя
   1.     em0
   2.     em1
   3.     em2
   4.     tun0
   Укажите номер внешнего интерфейса:
   ```

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

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

   На экране появится запрос:

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

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

   На экране появится запрос:

   ```
   Продолжить (Y/N)?
   ```

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

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

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

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

После определения каждого параметра нажимайте клавишу <Enter>.

На экране появится запрос на указание внутреннего интерфейса КШ с пронумерованным списком доступных интерфейсов, подобный следующему:

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

11. Введите номер соответствующего интерфейса из списка, представленного на экране. Нажмите клавишу <Enter>.

На экране появится запрос:

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

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

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

На экране появится сообщение, подобное следующему:

```
Продолжить (Y/N)?
```

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

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

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

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

На экране появится сообщение, подобное следующему:

```
Адрес маршрутизатора 192.0.2.1
Продолжить (Y/N)?
```

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

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

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

16. Выполните одно из следующих действий:

- при использовании в качестве источника исходной ключевой информации ПАК "Соболь" введите "n" и нажмите клавишу <Enter>. Перейдите к п. **18**;
- при использовании ключевого блокнота РДП-006 введите "y" и нажмите клавишу <Enter>. На экране появится сообщение:

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

17. Вставьте носитель с исходной ключевой информацией и нажмите клавишу <Enter>.

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

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

18. Введите пароль и нажмите клавишу <Enter>.

Примечание. Длина и сложность пароля должны соответствовать политике аутентификации администраторов. По умолчанию длина пароля – не менее 8 символов. Разрешено использование любых символов, кроме кириллицы.

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

На экране появится сообщение:

```
Повторите пароль
```

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

На экране появится сообщение:

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

20. Вставьте чистый носитель и нажмите клавишу <Enter>.

Дождитесь сообщений об успешном сохранении ключей администратора и о завершении процедуры конфигурирования, после которых на экране появится сообщение:

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

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

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 приводится на стр. **34**.

22. Для завершения процедуры инициализации ЦУС введите "0" и нажмите клавишу <Enter>.

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

    После завершения инициализации на экране появится сообщение:

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

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

23. Извлеките носитель из считывающего устройства.

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

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

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

Развертывание рабочего места администратора

Средством удаленного управления ЦУС, а также другими узлами комплекса является программа управления ЦУС, входящая в состав пакета программ администрирования комплекса.

Развертывание РМ администратора ЦУС включает в себя последовательное выполнение трех этапов:

1. Установка программы управления ЦУС (см. ниже).

   Внимание! По умолчанию используется биологический ДСЧ, обеспечивающий защиту информации по классу КС1. В случае необходимости переключения на физический ДСЧ, обеспечивающий защиту информации по классам КС1 и КС2, необходимо изменить настройки криптопровайдера "Код безопасности CSP" (см. стр. 38). При использовании биологического ДСЧ после перезагрузки компьютера на экране появится сообщение с инструкцией по накоплению энтропии для биологического датчика случайных чисел. Следуя инструкции, нажимайте левой кнопкой мыши на мишень, перемещающуюся по экрану, до завершения процесса накопления энтропии.

2. Настройка контроля целостности программных модулей РМ администратора (см. стр. **16**).
3. Запуск программы управления и подключение к ЦУС (см. стр. **17**).

Состав и варианты размещения пакетов программ администрирования комплекса

В пакет программ администрирования комплекса входят следующие компоненты:

- программа управления ЦУС;
- программа управления агентом ЦУС и СД;
- программа создания ключевого носителя для агента ЦУС и СД;
- конфигуратор БД журналов ЦУС и СД;
- программа просмотра журналов ЦУС и СД;
- программа просмотра отчетов ЦУС;
- программа управления агентом обновлений базы решающих правил СОВ;
- программа управления агентом Роскомнадзор;
- программа копирования ключей.

Регистрационные журналы комплекса хранятся в базе данных на сервере СУБД.

Примечание. При использовании MS SQL Express все его базы данных не могут занимать более 4 Гбайт дискового пространства (ограничение производителя).

Установка пакета программ администрирования комплекса

Внимание! Установку и удаление программ администрирования может выполнить только пользователь, наделенный правами администратора.

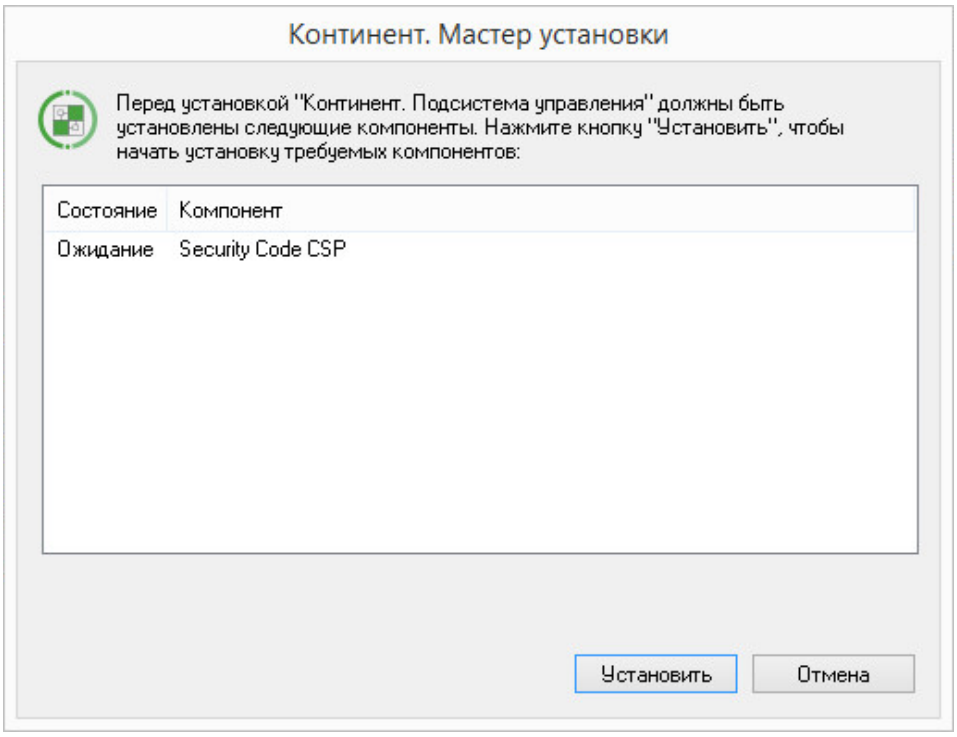
Перед запуском мастера установки завершите работу всех приложений.

Внимание! Если ПО комплекса должно удовлетворять требованиям высокого уровня безопасности, необходимо предварительно установить СЗИ семейства Secret Net Studio .

Для установки программ администрирования:

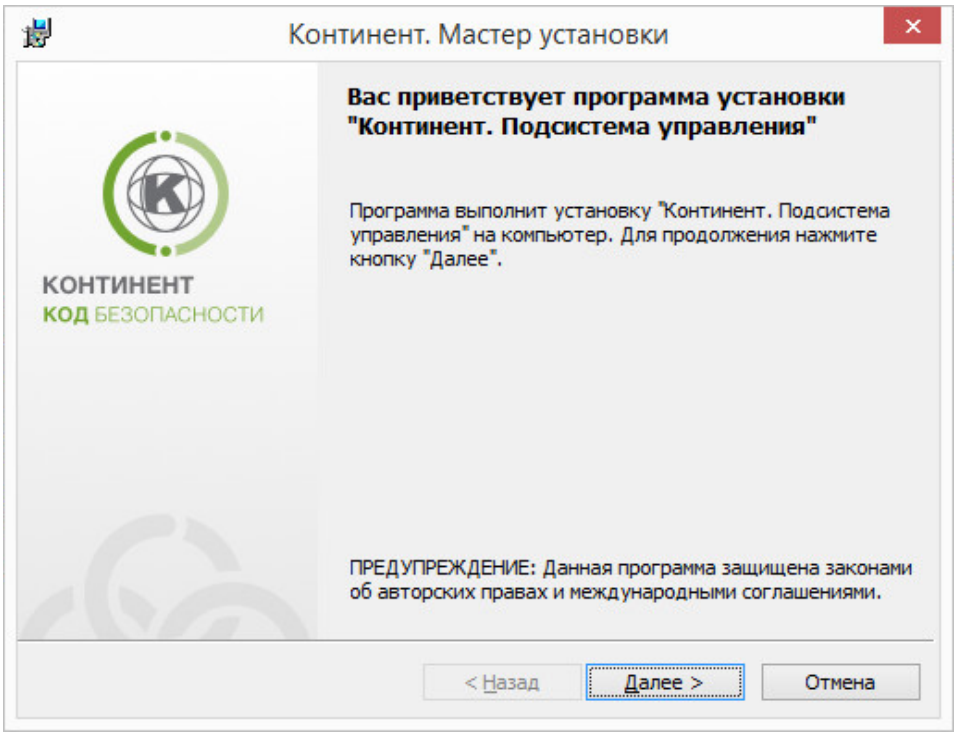
1. Вставьте установочный диск в устройство чтения компакт-дисков.
2. Запустите на исполнение файл \MS\Setup.exe.

   Система будет проанализирована мастером установки, после чего на экране появится окно со списком дополнительных компонентов, которые должны быть установлены до начала установки программ администрирования комплекса.



3. Нажмите кнопку "Установить".

   Начнется поочередная установка компонентов в соответствии с заявленным списком. После ее завершения на экране появится стартовое окно мастера установки ПО администрирования комплекса.

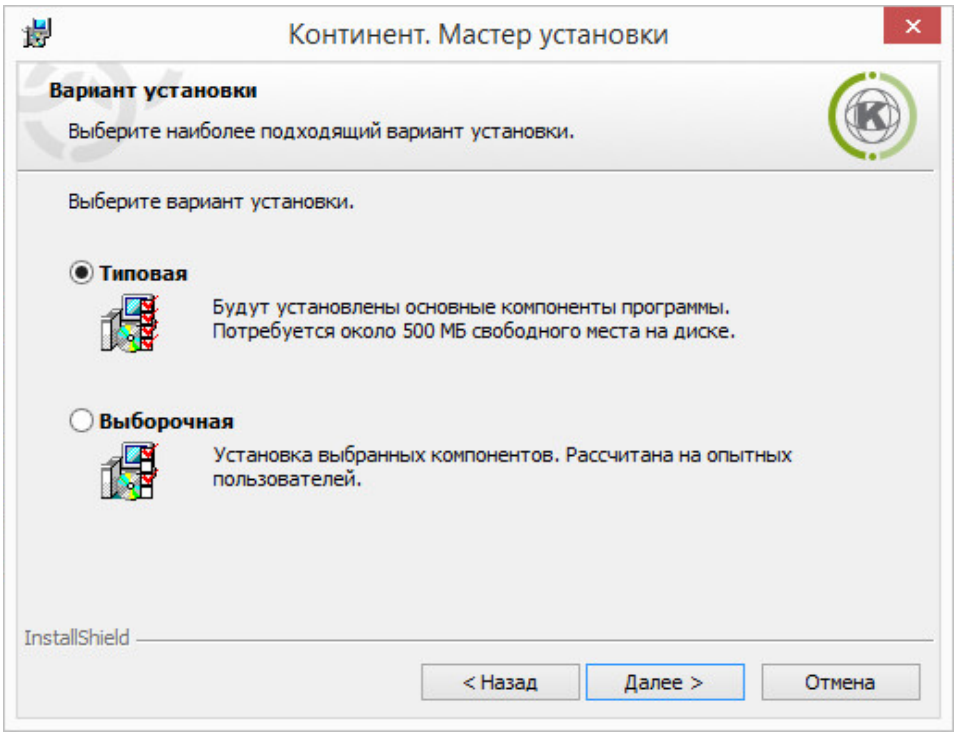


4. Ознакомьтесь с информацией, содержащейся в стартовом окне, и нажмите кнопку "Далее >" для продолжения установки.

   Появится окно с текстом лицензионного соглашения.

5. Ознакомьтесь с содержанием лицензионного соглашения, прочитав его до конца. Если вы не согласны с условиями лицензионного соглашения, откажитесь от продолжения установки, нажав кнопку "Отмена", и подтвердите свой выбор в появившемся на экране окне. Установка завершится. Если вы согласны с условиями лицензионного соглашения, подтвердите свое согласие, поставив отметку в поле "Я принимаю условия лицензионного соглашения" и нажав кнопку "Далее >".

Появится окно выбора варианта установки.



При использовании типового варианта устанавливаются следующие основные компоненты:

- программа управления ЦУС;
- программа копирования ключей;
- программа просмотра журналов;
- агент ЦУС и СД.

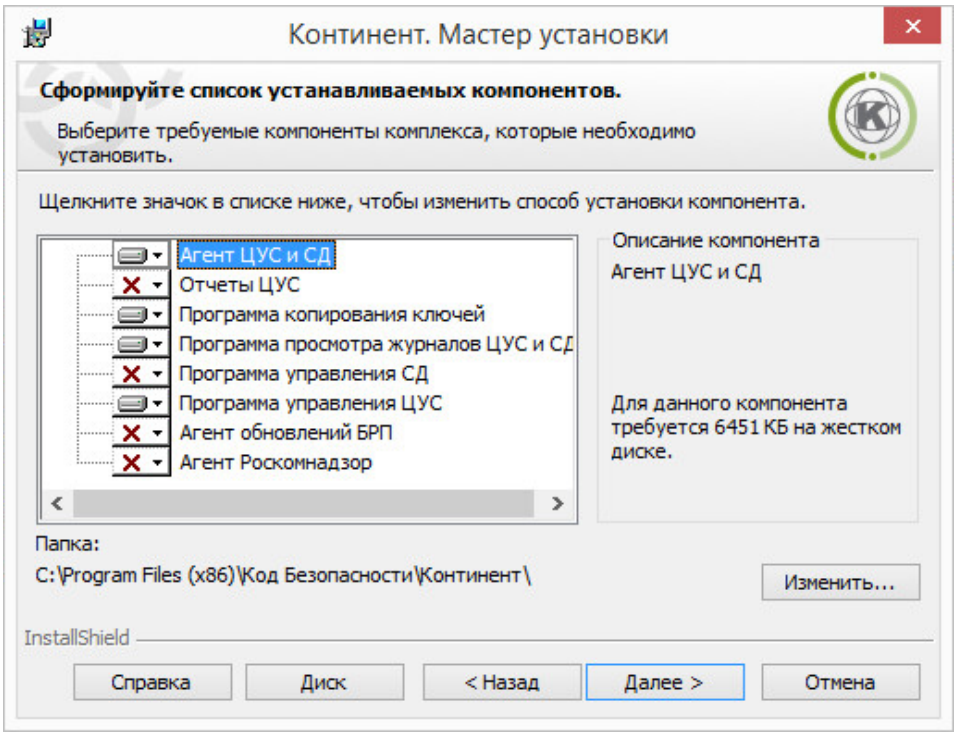
Выборочная установка позволяет выбрать необходимые компоненты из их полного перечня.

Примечание. Компоненты "Программа создания ключевого носителя для агента ЦУС и СД" и "Конфигуратор БД журналов ЦУС и СД" устанавливаются автоматически независимо от выбранного варианта установки.

6. Выберите требуемый вариант установки и нажмите кнопку "Далее >".

   В случае типовой установки перейдите к п. **9**.

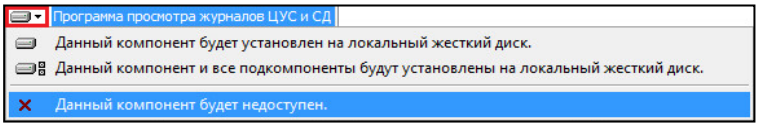
При выборочной установке на экране появится стандартное окно выбора компонентов ПО, которые требуется установить на данный компьютер.



7. Отметьте в списке устанавливаемые компоненты.

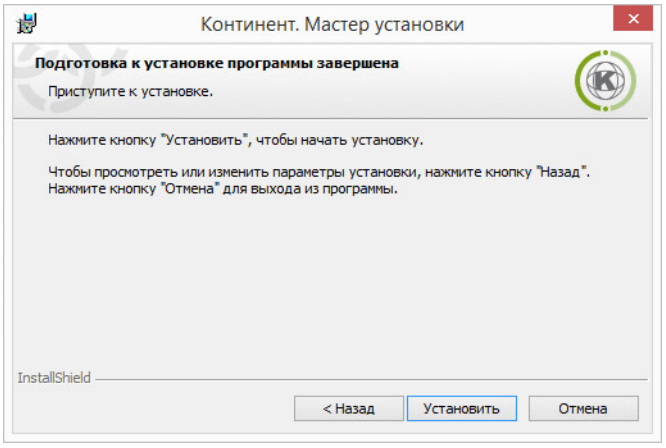
Примечание. Компонент "Программа управления СД" выбирать запрещается.

Для настройки установки компонента нажмите на соответствующую пиктограмму рядом с его названием и в раскрывшемся меню выберите необходимый пункт.



8. При необходимости измените папку установки программ администрирования комплекса. Для этого используйте кнопку "Изменить...". По умолчанию программа установки копирует файлы на системный диск в папку \Program Files (x86)\Код Безопасности\Континент.
9. Для продолжения установки нажмите кнопку "Далее >".

   На экране появится окно проверки выбранных настроек.



Перед началом установки можно проверить и откорректировать выполненные настройки. Для проверки и корректировки настроек используйте кнопки "< Назад" и "Далее >".

10. Для запуска установки нажмите кнопку "Установить".

Программа установки приступит к копированию файлов на жесткий диск компьютера. Ход выполнения процесса копирования отображается на экране.

Примечание. Если программа установки в процессе копирования не обнаружит файл, заявленный в комплекте поставки, на экране появится предупреждающее сообщение с указанием имени отсутствующего файла. Скопируйте еще раз файлы с дистрибутивного диска и повторите установку. Если это не приведет к желаемому результату, обратитесь к поставщику комплекса.

После успешного выполнения процедуры установки на экране появится итоговое информационное окно.

11. Нажмите кнопку "Готово".

На экране появится запрос на перезагрузку компьютера. Перезагрузите компьютер.

После установки программ администрирования комплекса в меню "Программы" главного меню ОС Windows появится программная группа "Код Безопасности".

Настройка контроля целостности программных модулей РМ администратора

После установки программ администрирования комплекса на РМ администратора необходимо настроить контроль целостности программных модулей и среды функционирования. Перечень объектов, подлежащих контролю целостности, приведен в документе "Аппаратно-программный комплекс шифрования "Континент". Версия 3.9. Правила пользования".

Постановка модулей на контроль осуществляется средствами, обеспечивающими контроль целостности ПО и установленными на данном компьютере. Если для контроля целостности используется ПАК "Соболь", постановку программных модулей на контроль следует выполнять в соответствии с описанием процедур, приведенных в руководстве администратора ПАК "Соболь".

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

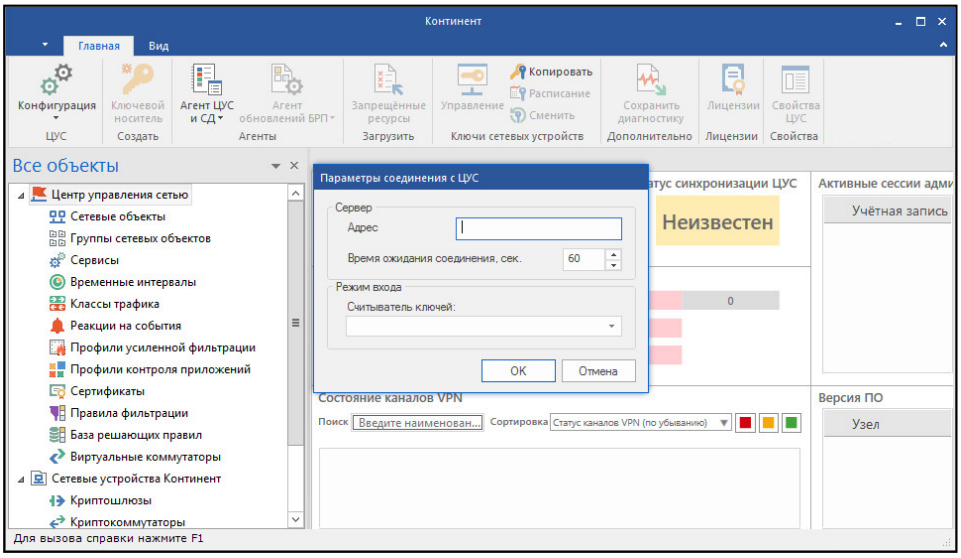
Если при работе с мастером установки программ администрирования комплекса был выбран биологический датчик случайных чисел, при первой генерации ключевой последовательности на экране появится сообщение с инструкцией по накоплению энтропии. Следуя инструкции, нажимайте левой кнопкой мыши на мишень, перемещающуюся по экрану, до завершения процесса накопления энтропии для датчика случайных чисел.

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

Для запуска программы управления:

1. Вставьте внешний носитель с идентификатором администратора комплекса.
2. Активируйте ярлык программы управления на рабочем столе:

На экране появится главное окно ПУ и диалоговое окно "Параметры соединения с ЦУС".



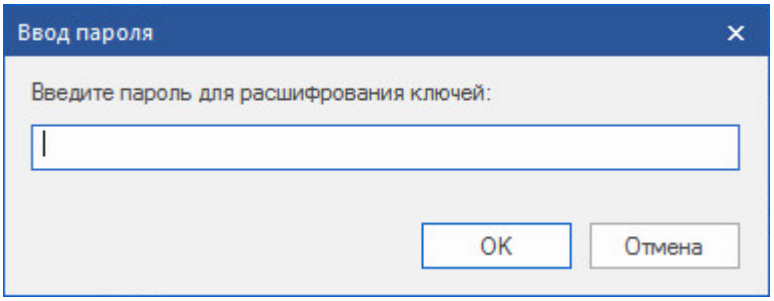
3. Заполните поля этого окна и нажмите кнопку "OK".

Адрес	IP-адрес интерфейса ЦУС, к которому осуществляется подключение
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

На экране появится запрос пароля для расшифрования ключей администратора.

Примечание. Если идентификатор администратора не предъявлен, на экране сначала появится запрос идентификатора. Предъявите идентификатор. Если носитель неисправен или не содержит административного ключа, на экране появится сообщение об ошибке. Закройте окно сообщения и повторите попытку запуска с надлежащим носителем.

Сообщение об ошибке может содержать техническую информацию для разработчиков. При обращении в службу технической поддержки необходимо предоставить снимок экрана с сообщением или полный текст сообщения, включая техническую информацию.



4. Введите пароль и нажмите кнопку "OK".

При успешном чтении служебной информации с идентификатора программа управления установит защищенное соединение с ЦУС и на экране появится окно для регистрации лицензий ЦУС (см. ниже).

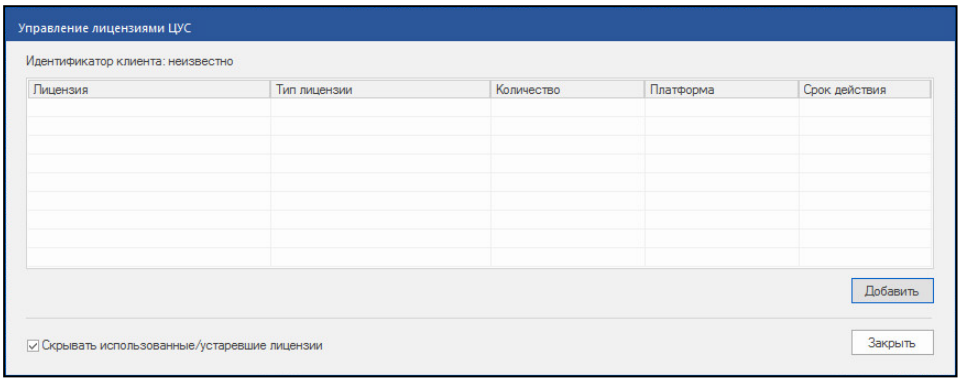
Совет. Если при установлении соединения произошел сбой и на экран выведено сообщение о невозможности соединения с ЦУС, проверьте работоспособность ЦУС и повторите попытку соединения с ним еще раз.

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.



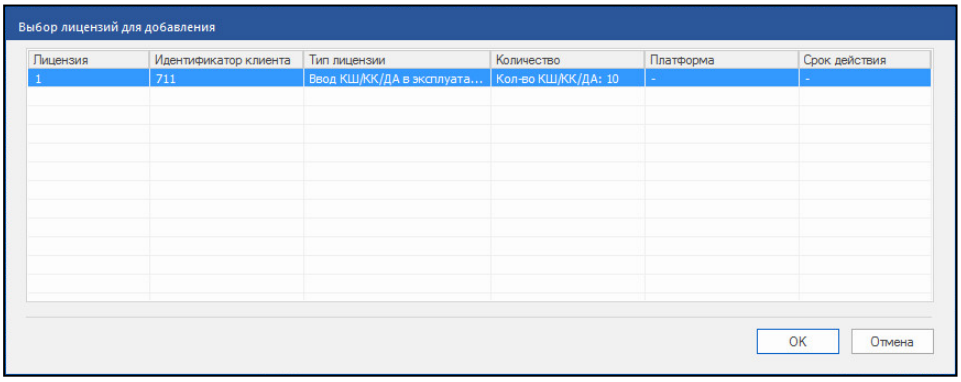
Примечание. Лицензии, зарегистрированные в более ранних версиях комплекса, отображаются в списке с отметкой "Ввод КШ<устройства> в эксплуатацию". При этом действие таких лицензий сохраняется.

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".



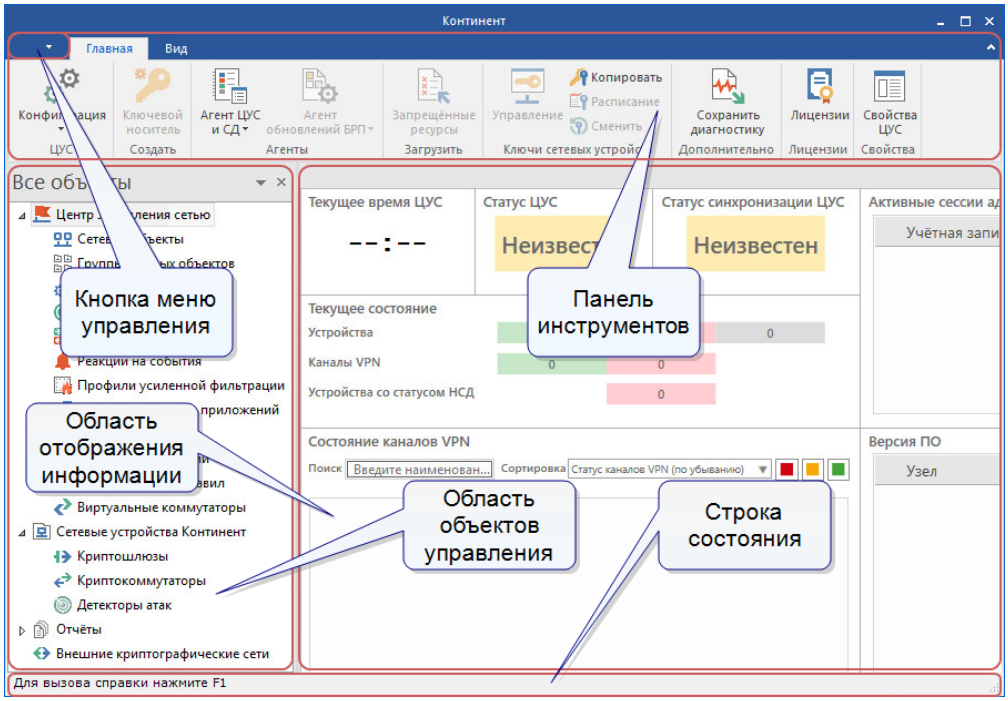
4. Выберите требуемую лицензию и нажмите кнопку "ОК".

   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.

Интерфейс

После запуска ПУ ЦУС и успешной аутентификации на экране отображается главное окно приложения.



Окно ПУ ЦУС содержит следующие основные элементы интерфейса:

Элемент интерфейса	Описание
Панель инструментов	Содержит набор инструментов на нескольких вкладках: • "Главная" — основные инструменты; • "Вид" — настройка отображения элементов интерфейса и ряда объектов ПУ ЦУС. На вкладках расположены функциональные кнопки, предназначенные для запуска часто используемых команд. Состав кнопок зависит от выбора объекта в области объектов управления, а их доступность определяется текущей ситуацией. При наведении курсора мыши на кнопку появляется всплывающая подсказка с дополнительной информацией
Кнопка меню управления	Кнопка предназначена для доступа к меню управления и настроек ПУ ЦУС
Область объектов управления	Содержит список объектов комплекса
Область отображения информации	Содержит информацию выбранного раздела или пункта из списка объектов
Строка состояния	Отображает в реальном времени данные мониторинга

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.

Глава 3
Развертывание сетевого устройства

Регистрация

Регистрация сетевых устройств осуществляется с помощью программы управления после установления соединения с ЦУС и появления на экране основного окна этой программы.

Регистрация СУ выполняется в следующем порядке:

1. Настройка основных параметров СУ в мастере создания нового устройства.

   Примечание. Для поддержки протоколов динамической маршрутизации необходимо предварительно сформировать конфигурационный файл zebra.conf, а также конфигурационные файлы используемых протоколов ospfd.conf, bgpd.conf, ripd.conf (см. стр. 36).

2. Экспорт конфигурации и ключевой информации СУ.

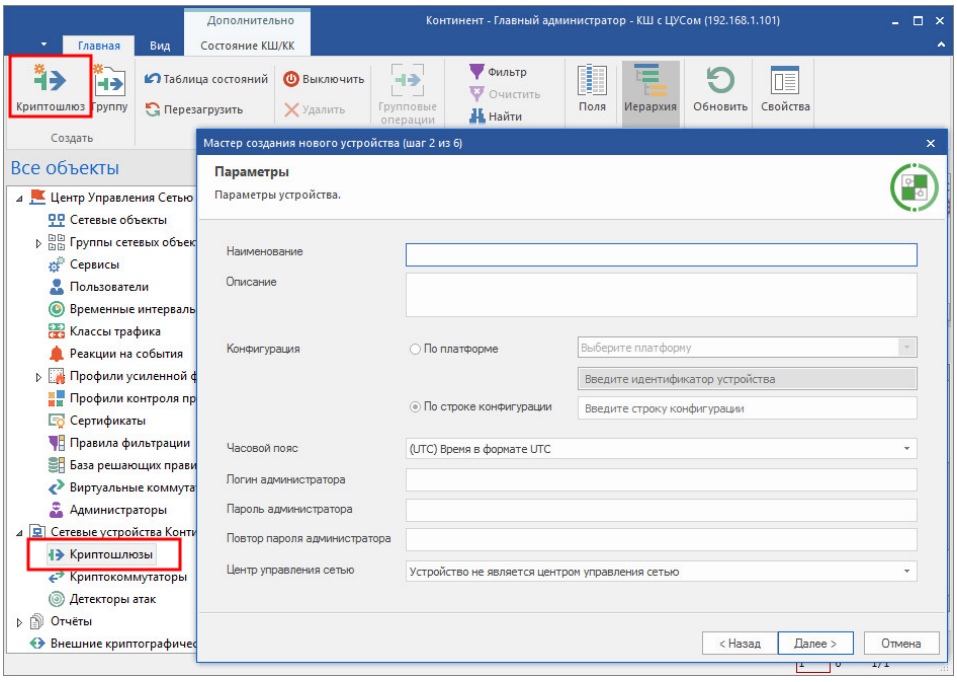
   Примечание. По умолчанию файл конфигурации экспортируется под именем "gate.cfg", а главный ключ и ключ связи с ЦУС упаковываются в файл под именем "keyset".

Перед запуском ПУ ЦУС завершите работу всех приложений и вставьте внешний носитель для экспорта на него файла конфигурации и ключевой информации СУ. В качестве носителя обычно используют USB-флеш-накопитель.

Для регистрации сетевого устройства:

1. В разделе "Сетевые устройства Континент" выберите пункт, соответствующий требуемому типу регистрируемого СУ, и нажмите кнопку с типом устройства на панели инструментов.

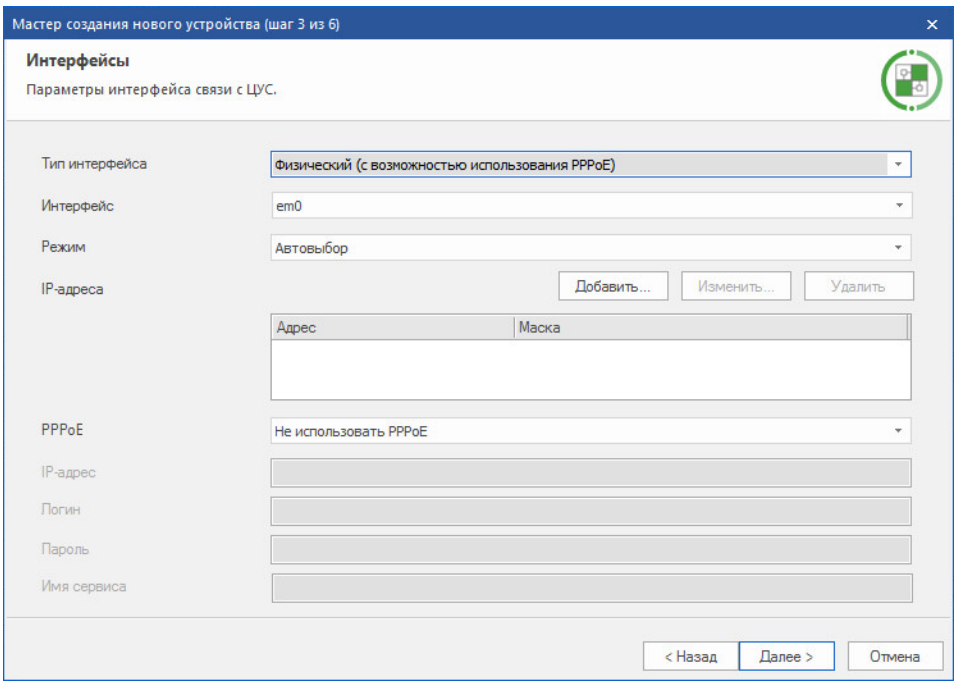
   На экране появится окно мастера создания нового сетевого устройства.



2. Заполните поля и нажмите кнопку "Далее >".

Наименование	Имя сетевого устройства, под которым оно будет зарегистрировано в базе данных ЦУС. Это имя будет определять данное устройство в списке объектов, отображаемом программой управления. Максимальная длина имени — 39 символов
Описание	Дополнительная информация, которая будет отображаться программой управления в списке сетевых устройств. Максимальная длина записи в этом поле — 79 символов
Конфигурация	Конфигурация устройства указывается двумя способами: либо по его идентификатору и типу платформы, либо по строке конфигурации, определяющей аппаратную конфигурацию сетевого устройства. Эти данные указаны в его паспорте
Часовой пояс	Смещение зимнего времени относительно Гринвича в часах для того региона, в котором будет эксплуатироваться данное сетевое устройство
Логин и пароль администратора	Учетные данные локального администратора СУ
Центр управления сетью	Включение/отключение режима управления сетью (только для КШ)

На экране появится окно "Интерфейсы".



3. Выберите тип интерфейса:

- Физический (с возможностью использования PPPoE).
- DialUp (исходящий).
- DialUp (входящий).
- Выделенная линия.

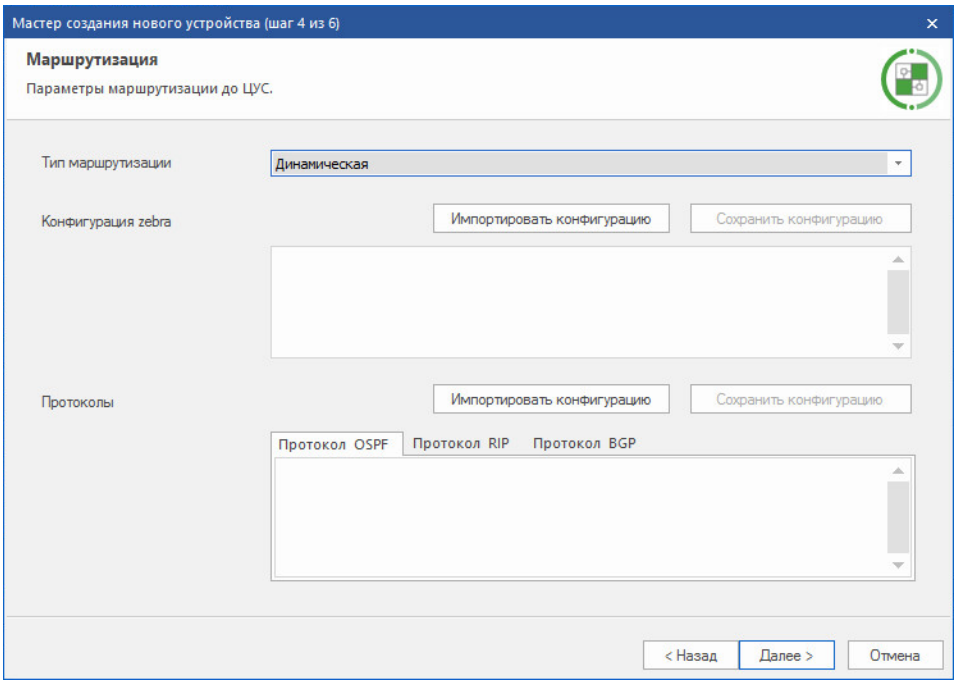
В зависимости от выбора изменятся поля прочих параметров интерфейса.

4. Заполните поля и нажмите кнопку "Далее >".

Примечание. При вводе IP-адреса допустимо указать префикс маски. При этом поле "Маска" заполняется автоматически.

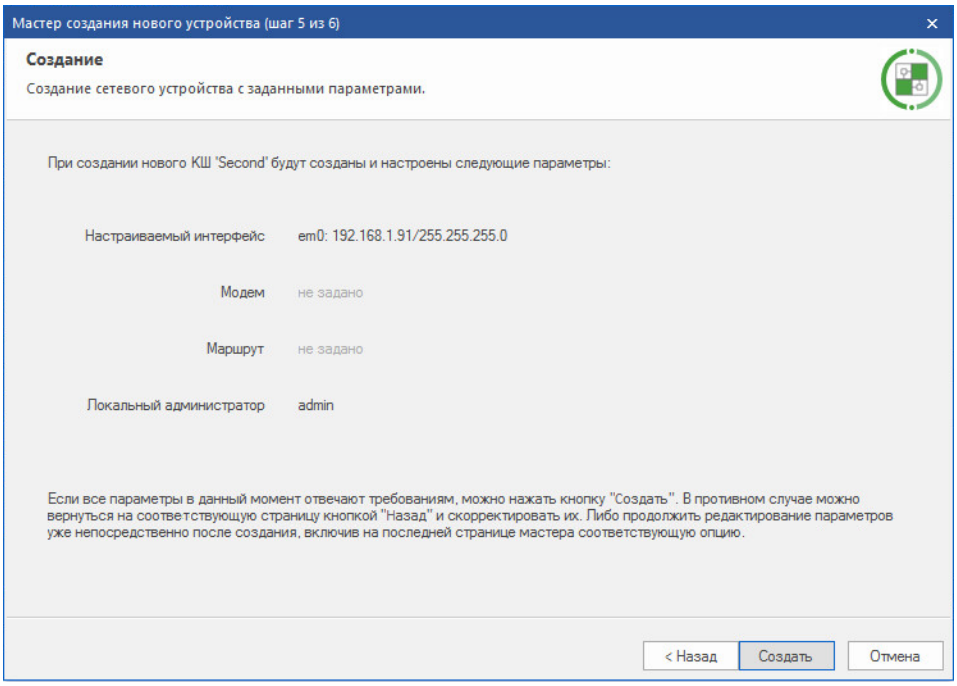
Физический интерфейс	
Интерфейс	Выбор интерфейса, через который осуществляется подключение к ЦУС
Режим	Выбор режима связи
IP-адреса	IP-адреса, назначенные для интерфейса. Для добавления IP-адреса нажмите кнопку "Добавить..." и введите в поля появившегося окна IP-адрес и префикс маски подсети
PPPoE	Использование PPPoE-соединения для подключения к внешним сетям с помощью xDSL-сервисов
IP-адрес	IP-адрес и учетные данные пользователя, зарегистрированного у провайдера
Логин	
Пароль	
Имя сервиса	Имя сервиса (если требуется провайдером)
DialUp	
IP-адрес	IP-адрес и учетные данные пользователя, зарегистрированного у провайдера
Логин	
Пароль	
Скорость	Выбор скорости передачи данных через COM-порт. При подключении модема через USB-порт в данном поле необходимо выбрать значение "USB-модем"
Строка инициализации	Значение строки инициализации модема
Тайм-аут, сек.	Время ожидания соединения в секундах
Номера телефонов (для исходящего режима Dialup)	Список номеров телефонов модемного пула. Для добавления нового номера нажмите кнопку и введите номер телефона в появившееся поле. Для удаления выбранного номера используйте кнопку
Выделенная линия	
IP-адрес	IP-адрес и учетные данные пользователя, зарегистрированного у провайдера
Логин	
Пароль	
Имя сервиса	Имя сервиса (если требуется провайдером)
Скорость	Выбор скорости передачи данных через COM-порт. При подключении через USB-порт в данном поле необходимо выбрать значение "USB-модем"

На экране появится окно "Маршрутизация".



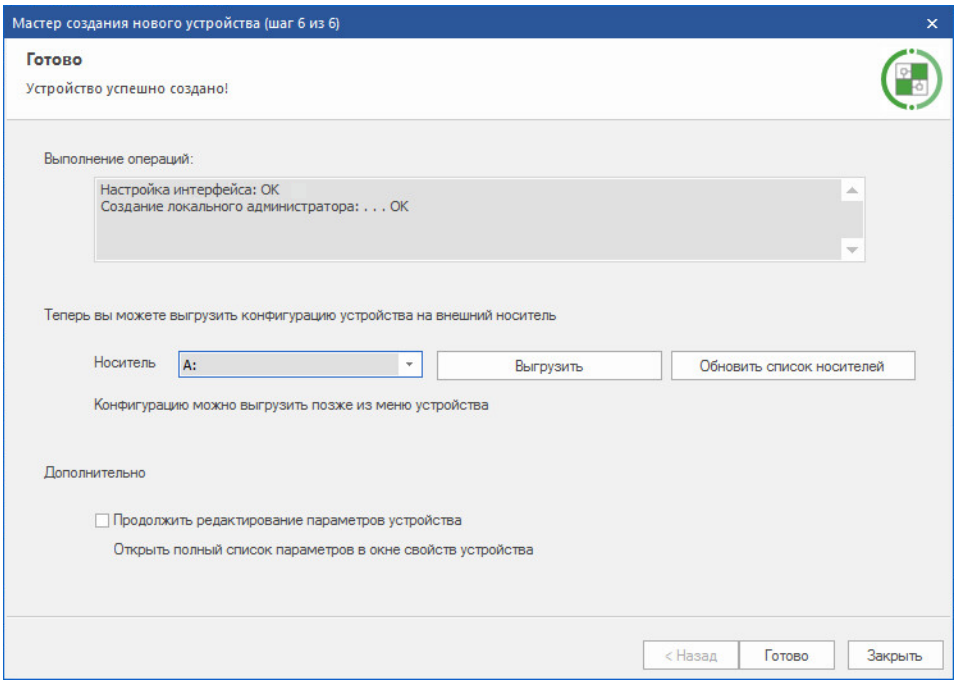
5. Выберите тип маршрутизации, в случае динамической маршрутизации — импортируйте конфигурационные файлы и нажмите кнопку "Далее >".

На экране появится окно "Создание".



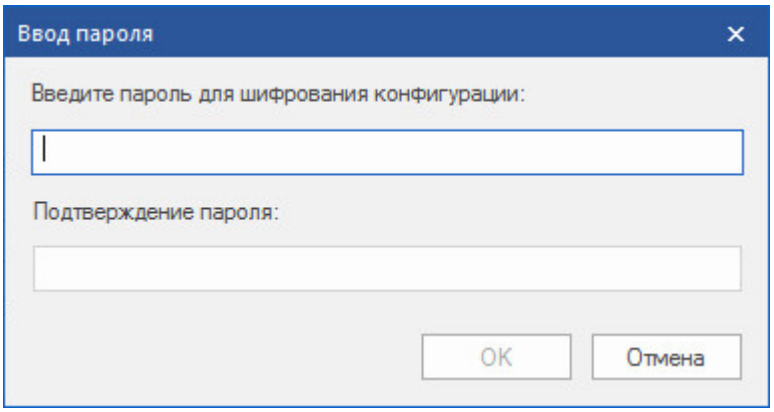
6. Проверьте заданные параметры (для их корректировки используйте клавиши "< Назад" и "Далее >") и нажмите кнопку "Создать".

На экране появится окно завершения работы мастера.



7. После выполнения операций по созданию и настройке параметров СУ выберите из списка требуемый носитель и нажмите кнопку "Выгрузить".

На экране появится окно для ввода пароля.



8. Введите дважды пароль и нажмите кнопку "ОК".

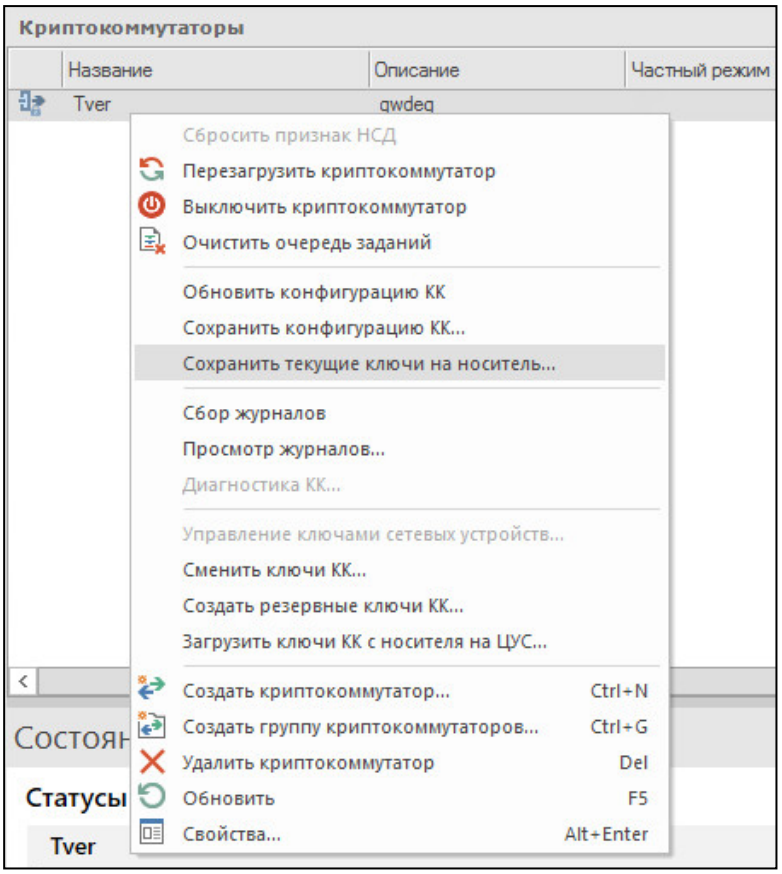
После успешного экспорта конфигурации на экране появится соответствующее информационное окно.

9. Нажмите кнопку "ОК" для возврата к мастеру создания нового СУ, затем нажмите кнопку "Готово".

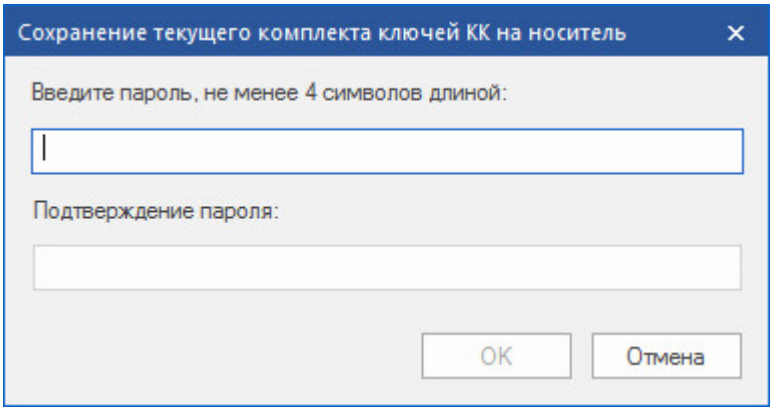
Окно мастера регистрации закроется, а в список сетевых устройств в основном окне программы управления будет добавлен объект с заданными параметрами.

В процессе регистрации сетевого устройства для него будут сгенерированы главный ключ и ключ связи с ЦУС, необходимые для дальнейшей инициализации устройства.

10. Для экспорта ключевой информации вызовите контекстное меню устройства и выберите команду "Сохранить текущие ключи на носитель...".



На экране появится окно для ввода пароля.



11. Введите дважды пароль и нажмите кнопку "ОК".

После успешного экспорта конфигурации на экране появится стандартное окно выбора каталога для хранения ключей СУ.

12. Укажите внешний носитель и нажмите кнопку "ОК".

После успешного экспорта ключевой информации на экране появится соответствующее информационное окно.

13. Нажмите кнопку "ОК" и отсоедините внешний носитель.

Настройка QoS на внешнем интерфейсе КШ

Для надежной передачи служебной информации между КШ комплекса необходимо настроить управление QoS на внешнем интерфейсе каждого КШ.

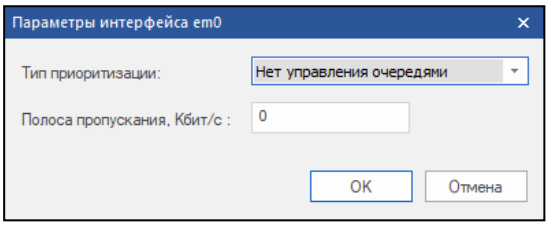
Для настройки QoS на внешнем интерфейсе КШ:

1. В разделе "Сетевые устройства Континент" программы управления ЦУС выберите требуемый КШ и нажмите кнопку "Свойства" на панели инструментов.

   На экране появится окно свойств КШ.

2. Перейдите на вкладку "Управление QoS", выберите в списке внешний интерфейс и нажмите кнопку "Изменить".

   На экране появится окно настройки параметров интерфейса.

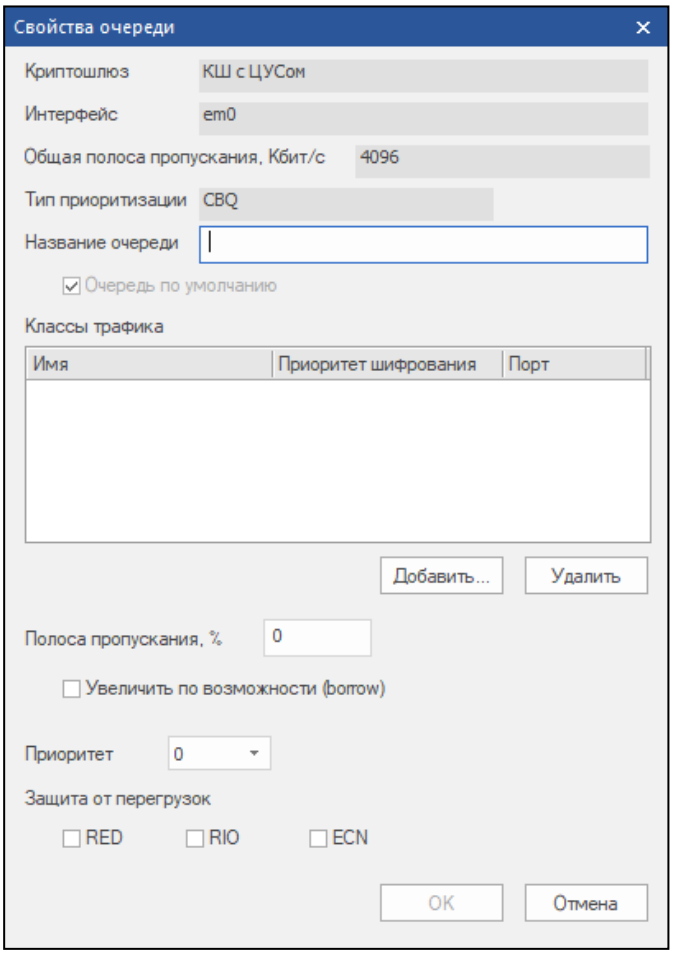


3. Выберите тип приоритизации CBQ, установите полосу пропускания (рекомендуется не менее 4 Мбит/с) и нажмите кнопку "ОК".

   На экране соответственно изменится характеристика управления очередями на выбранном интерфейсе.

4. Нажмите кнопку "Добавить очередь...".

   Появится окно "Свойства очереди".



5. Задайте очередь для служебного трафика:

- заполните поле "Название очереди" (например "служебный");
- нажмите кнопку "Добавить...", выберите класс трафика "Нормальный" и нажмите кнопку "ОК";
- определите полосу пропускания (рекомендуется не менее 1 Мбит/с, то есть 25% для приводимого примера);
- установите приоритет "1";
- нажмите кнопку "ОК".

Примечание. При введении дополнительных классов трафика количество очередей может быть расширено (см. [**1**]).

6. Нажмите кнопку "ОК".

Инициализация сетевого устройства

В ходе инициализации сетевого устройства выполняются следующие операции:

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

Конфигурация сетевого устройства считывается с носителей типа USB-флеш-накопитель. По умолчанию файл конфигурации получает имя "gate.cfg", а главный ключ и ключ связи с ЦУС упаковываются в файл под именем "keyset".

Для инициализации сетевого устройства:

1. Подключите к системному блоку сетевого устройства клавиатуру и монитор.
2. Включите питание сетевого устройства. Дождитесь появления на экране основного окна ПАК "Соболь", в центре которого будет отображаться запрос персонального идентификатора.

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

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

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

   На экране появится меню администратора ПАК "Соболь".
4. Выберите с помощью управляющих клавиш клавиатуры раздел "Общие параметры системы" и убедитесь, что опция "Запрет загрузки с внешних носителей" включена для всех пользователей, опция "Автономный режим работы" отключена.

   Примечание. Все сведения, необходимые администратору для управления работой ПАК "Соболь", содержатся в руководстве администратора "ПАК "Соболь".
   В штатном режиме работы сетевого устройства загрузка ОС с отчуждаемого носителя для всех пользователей должна быть запрещена. Убедитесь, что режим "Запрет загрузки с внешних носителей" включен для всех пользователей.
5. Вернитесь в главное меню, выберите команду "Загрузка операционной системы" и нажмите клавишу <Enter>.

   Дождитесь появления на экране следующего сообщения:

   ```
   Вставьте носитель с конфигурацией и нажмите Enter
   ```
6. Вставьте в USB- разъем внешний носитель с конфигурационной информацией, сохраненной после регистрации сетевого устройства (см. стр. **21**). Дождитесь сообщения на экране об успешном выполнении операции и нажмите клавишу <Enter>.

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

При успешном чтении информации с носителя на экране появится сообщение:

```
Введите пароль
```

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

   После успешной аутентификации и считывания конфигурации на экран выводятся краткие сведения о конфигурации и запрос ключей управления:

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

> **Примечание.** Если конфигурация сетевого устройства и ключи управления записаны на разных носителях, подсоедините требуемый к разъему USB-порта.

8. Нажмите клавишу <Enter>.

   На экране появится сообщение об обнаружении ключевых носителей и их список:

```
Обнаружены следующие ключевые носители:
```

9. Введите номер пункта, соответствующий носителю с требуемым комплектом ключей, и нажмите клавишу <Enter>.

   На экране появится список ключей выбранного комплекта.

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

    На экране появится запрос ввода пароля.

11. Введите пароль и нажмите клавишу <Enter>.

    При правильном вводе пароля на экране появится краткая информация о комплекте ключей и запрос на установку этого комплекта.

> **Примечание.** Если пароль указан неверно, операция загрузки ключей будет отменена. Загрузку ключей можно повторить, используя меню "Настройки безопасности" (см. [1]).

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

    На экране появится следующее сообщение:

```
Ключ установлен как активный
```

    При необходимости дальнейшей настройки параметров сетевого устройства нажмите клавишу <Enter>.

    В противном случае конфигурация будет применена автоматически и на экране появится сообщение:

```
Успешный запуск <Дата, Время>
```

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

13. Извлеките носитель из считывающего устройства и подключите интерфейсы сетевого устройства к сетевым коммуникациям в соответствии с настройкой. Имена интерфейсов указаны на корпусе сетевого устройства рядом с соответствующим разъемом.

> **Внимание!** Для установления соединения ЦУС с инициализированным сетевым устройством в программе управления ЦУС в окне "Свойства сетевого устройства" на вкладке "Общие сведения" установите отметку в поле выключателя "Введен в эксплуатацию".

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

Ввод в эксплуатацию

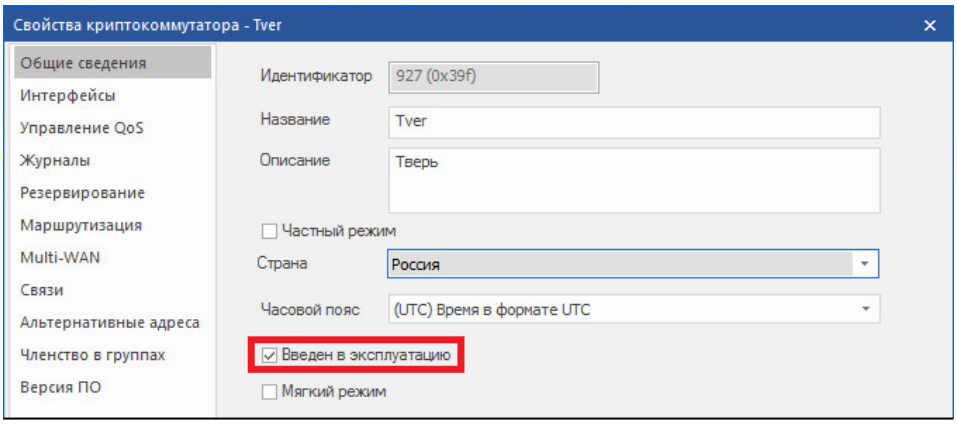
Ввод сетевого устройства в эксплуатацию осуществляется после его инициализации и подключения.

Пока сетевое устройство не введено в эксплуатацию, такое сетевое устройство в программе управления отображается со статусом состояния "Не введен в эксплуатацию".

Для ввода сетевого устройства в эксплуатацию:

1. Вызовите контекстное меню объекта с именем нужного устройства и активируйте команду "Свойства...".

   На экране появится окно настройки свойств данного сетевого устройства.
2. Установите отметку в поле "Введен в эксплуатацию".



3. Нажмите кнопку "OK".

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".

Тестовая эксплуатация комплекса

На этапе настройки коммуникаций комплекса может быть использован мастер для настройки VoIP (см. стр. **40**).

Для настройки комплекса:

1. Создайте для каждого зарегистрированного КШ правило фильтрации, пропускающее любой трафик (см. [**2**]).
2. Проведите опытную эксплуатацию комплекса в течение нескольких дней.
3. Проанализируйте журналы сетевого трафика для каждого КШ:
   - выделите из общего списка пакеты, передача которых в сети разрешена политикой безопасности вашего предприятия;
   - определите для этих пакетов перечень подсетей, протоколов и портов.
4. Создайте необходимые элементы правил и сами правила фильтрации (см. [**2**]).

5. Отключите исходное правило фильтрации. Трафик в сети будет определяться вновь созданными правилами фильтрации.
6. Проведите контрольную эксплуатацию комплекса в течение нескольких дней:
   - контролируйте работу каждого КШ по журналу НСД;
   - при необходимости внесите изменения в список правил фильтрации.

Примечание. Если при контрольной эксплуатации будет нарушена работа какой-либо службы, включите на время отладки работы этой службы мягкий режим работы КШ (см. подраздел "Общие сведения" свойств КШ).

Приложение

Установка ПО с внешнего накопителя

ПО АПКШ "Континент" поставляется на установочном компакт-диске. Если аппаратная платформа не располагает соответствующим приводом, необходимо использовать внешний привод оптических дисков либо создать загрузочный USB-флеш-накопитель.
При использовании USB-флеш-накопителя для установки ПО необходимо, чтобы носитель находился в USB-разъеме до завершения установки, поскольку с этого носителя выполняется загрузка системы.

Запись образа диска сетевого устройства на USB-флеш-накопитель

На компакт- диске "Диск 1", входящем в комплект поставки, в папке \Setup\Continent\FLASH\IMAGES расположены следующие файлы образов дисков:

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

Для записи такого образа диска на USB-флеш-накопитель используют программу FlashGUI.exe. Эта программа находится на этом же компакт-диске в папке Tools.

Для записи образа диска на USB-флеш-накопитель:

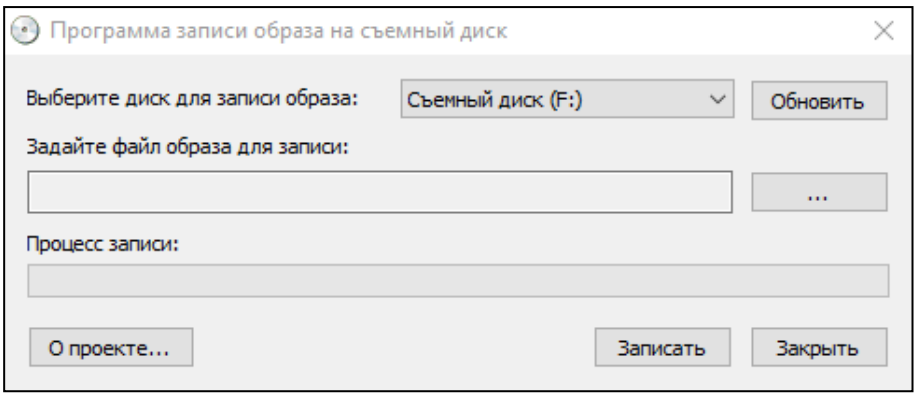
1. Загрузите компьютер с ОС Windows и войдите в систему.
2. Подключите подготовленный USB-носитель.

   После добавления USB-флеш-накопителя в папке "Мой компьютер" появится новый объект с именем "Съемный диск".
3. С компакт-диска из комплекта поставки скопируйте на компьютер программу FlashGUI.exe и образы дисков с ПО.
4. Запустите FlashGUI.exe.

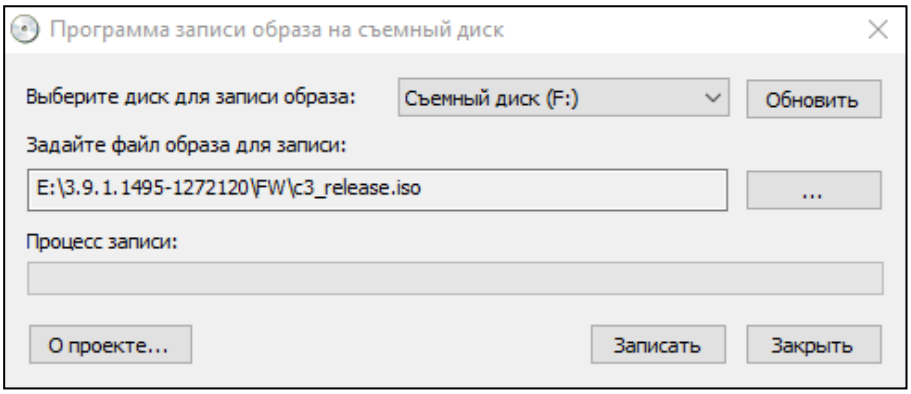
Примечание. Рекомендуется выполнять запуск программы с правами администратора.

На экране отобразится окно программы записи образа на съемный диск.

5. В раскрывающемся списке выберите диск для записи образа.

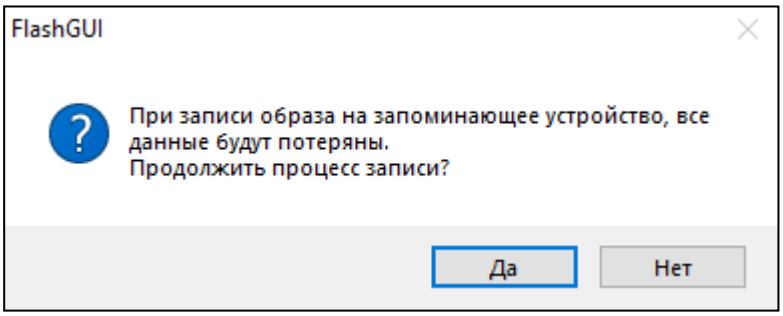


6. Выберите файл образа диска для записи.



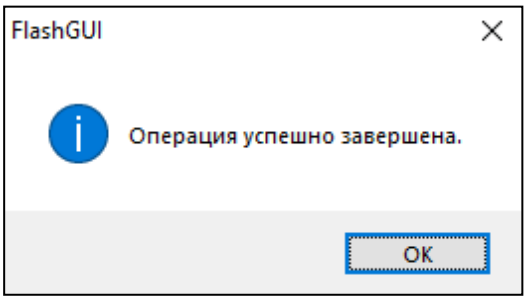
7. Нажмите кнопку "Запись".

   На экране отобразится окно с предупреждением.



8. Нажмите кнопку "Да", чтобы подтвердить запись.

   На экране отобразится оповещение об успешном завершении записи.



9. Нажмите кнопку "ОК", а затем кнопку "Закрыть" для завершения работы с FlashGUI.
10. Извлеките USB-флеш-накопитель из USB-разъема компьютера.

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>.

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

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.1 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)
ip route <адрес/маска> <шлюз>	Определение статического маршрута и маршрута по умолчанию

Табл.2 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

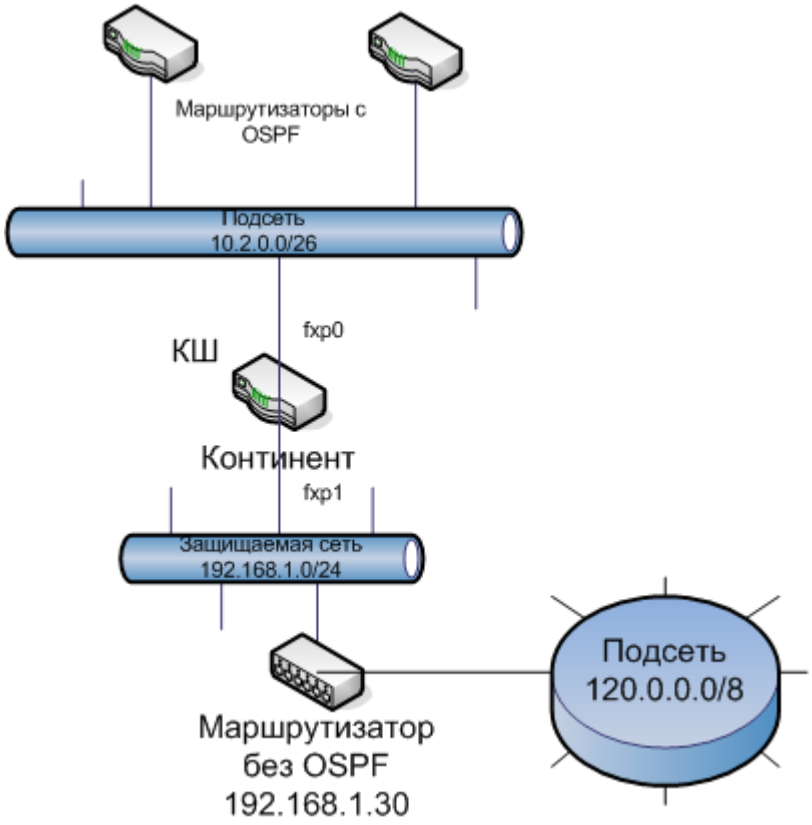
Параметр	Описание
interface <имя>	Определение имени интерфейса, используемого для обмена служебной информацией в процессе OSPF-маршрутизации
ip ospf authentication message-digest	Установка режима аутентификации OSPF-маршрутизатора
ip ospf message-digest-key 1 <алгоритм> <ключ>	Установка аутентификационного 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
```

Смена типа ДСЧ

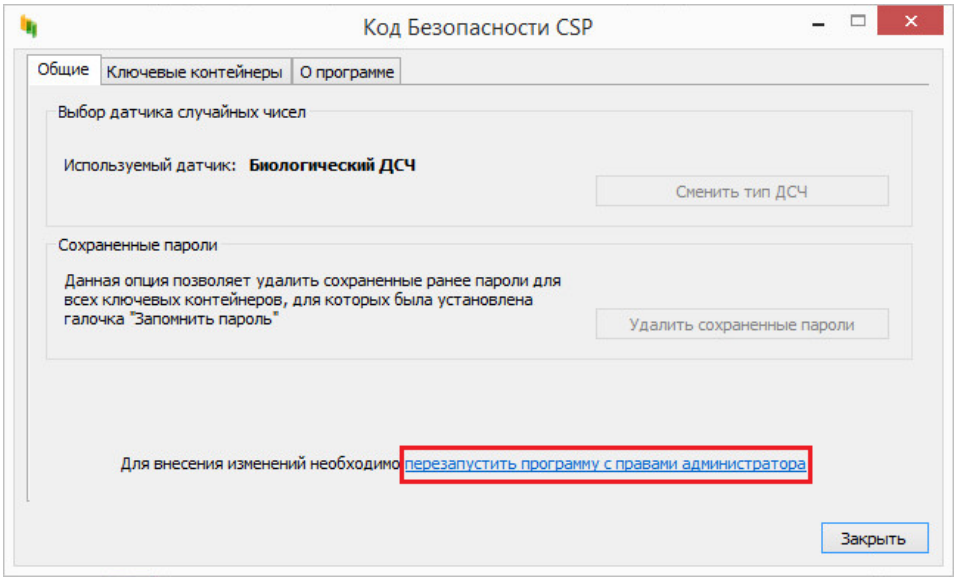
Составной частью программы управления ЦУС является криптопровайдер "Код Безопасности CSP", по умолчанию использующий биологический ДСЧ. При необходимости использования этим криптопровайдером физического ДСЧ на компьютере должны быть установлены плата и ПО ПАК "Соболь".

Внимание! Смена типа ДСЧ доступна только пользователю ОС Windows с правами администратора.

Для выбора типа ДСЧ:

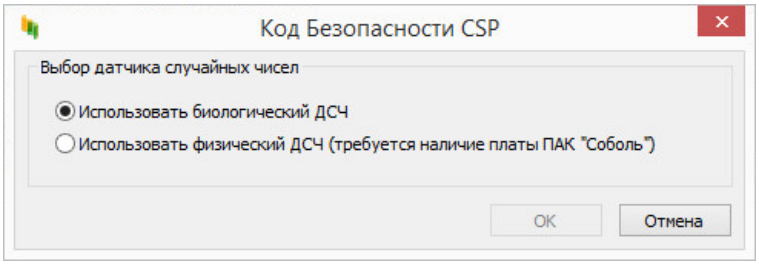
1. Запустите в панели управления ОС Windows элемент "Код Безопасности CSP".

   На экране появится главное окно программы.



2. Нажмите на ссылку "перезапустить программу с правами администратора" и подвердите полномочия в появившемся окне.
3. Нажмите кнопку "Сменить тип ДСЧ", ставшую активной после перезапуска программы.

   На экране появится окно выбора ДСЧ.



4. Выберите требуемый тип ДСЧ и нажмите кнопку "ОК".

   На экране появится запрос на перезагрузку компьютера.

5. Нажмите кнопку "Да".

Расчет контрольных сумм

Для расчета контрольных сумм дистрибутивного диска с использованием программы csum-2012:

1. Вставьте установочный диск в устройство чтения компакт дисков и скопируйте файл csum-2012.exe на жесткий диск компьютера.
2. Вызовите командную строку. Для этого нажмите кнопку "Пуск", в главном меню Windows выберите команду "Выполнить" и в открывшемся окне введите cmd.
3. В окне командной строки введите команду:

   ```
   csum-2012.exe источник > результат
   ```

   где источник – имя диска или каталога для расчета контрольных сумм; результат – полное имя файла для записи полученных результатов.

   Например:

   ```
   E:\csum-2012 D:\ > E:\log.txt
   ```

4. Нажмите клавишу "Enter". Дождитесь окончания процесса. Рассчитанные контрольные суммы будут записаны в указанный файл.

Для вызова дополнительной справки запустите в командной строке программу csum-2012 без указания параметров.

Для расчета контрольных сумм дистрибутивного диска с использованием программы "ФИКС" 2.0.2:

1. Скопируйте папку с программой "ФИКС" 2.0.2 на жесткий диск компьютера.
2. Запустите файл isx_sost.exe.
3. На вкладке "Задание" в группе параметров "Алгоритм КС" установите значение "Уровень-3".
4. В группе параметров "Код" задайте значение параметра "Const" равным 2.
5. Перейдите на вкладку "Настройки" и укажите имя файла результатов и папку для его сохранения.
6. Установите флаг "Фильтровать имена".
7. В строке ниже укажите "csum-2012.exe" чтобы не учитывать при расчете соответствующий файл. Контрольную сумму данного файла не требуется рассчитывать для данной процедуры. В поле "Доп." установить флаг "К" (кроме).
8. Вернитесь на вкладку "Задание".
9. В поле "Контролируемые файлы" выделите папку, в которой содержатся файлы для расчета КС. Нажмите на папке правой кнопкой мыши, выберите пункт "Добавить в проект… – с подкаталогами".
10. В открывшемся окне проверьте наличие добавляемых папок.
11. Нажмите кнопку "Пуск".
12. По завершении работы на экран будет выведен отчет.

Настройка VoIP

Предусмотрена автоматическая настройка криптошлюзов для работы VoIP, которая выполняется на начальном этапе настройки комплекса. В результате настройки:

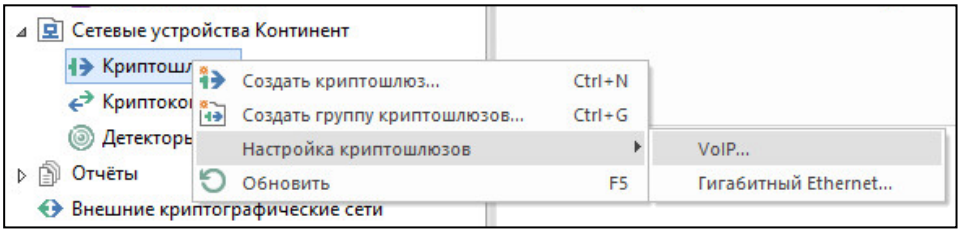
- создаются защищенные сегменты для внутренних интерфейсов КШ;
- создаются правила фильтрации;
- устанавливаются связи между КШ.

Внимание! Если в сети уже были созданы защищенные объекты, правила фильтрации и установлены связи, корректная настройка не гарантируется.

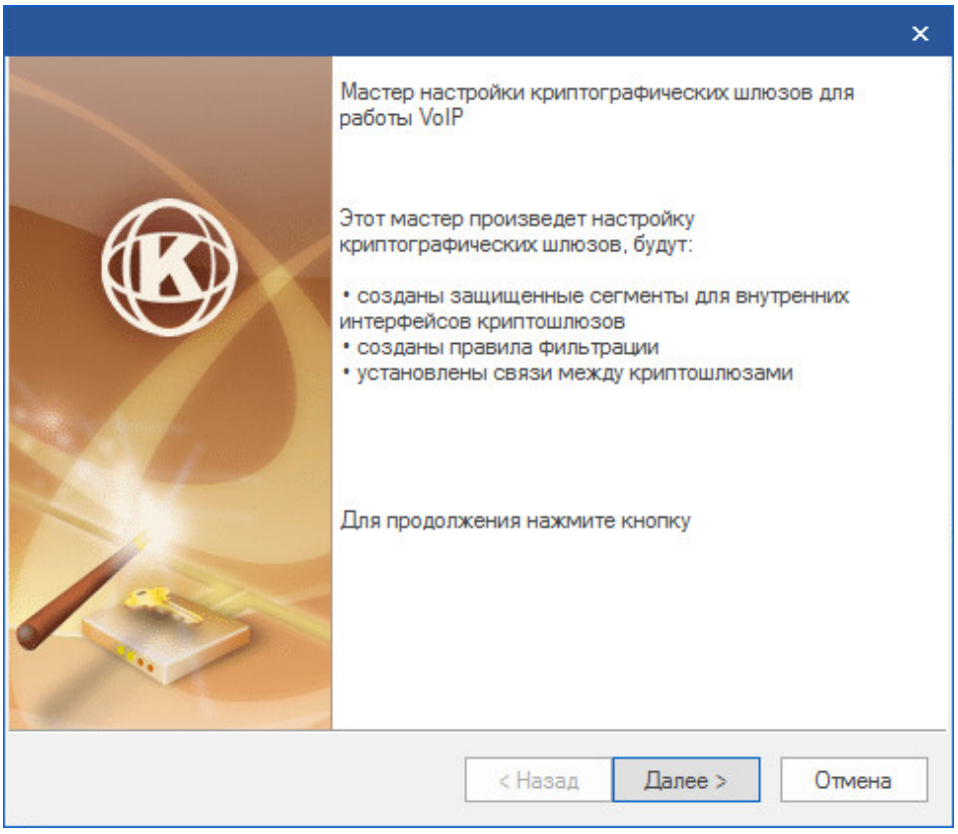
Настройка выполняется с помощью мастера. Для настройки необходимо указать КШ, участвующие в работе VoIP, и схему их подключения (полносвязная матрица или звезда).

Для настройки VoIP:

1. Вызовите контекстное меню подраздела "Криптошлюзы" и выберите в нем "Настройка криптошлюзов | VoIP...".

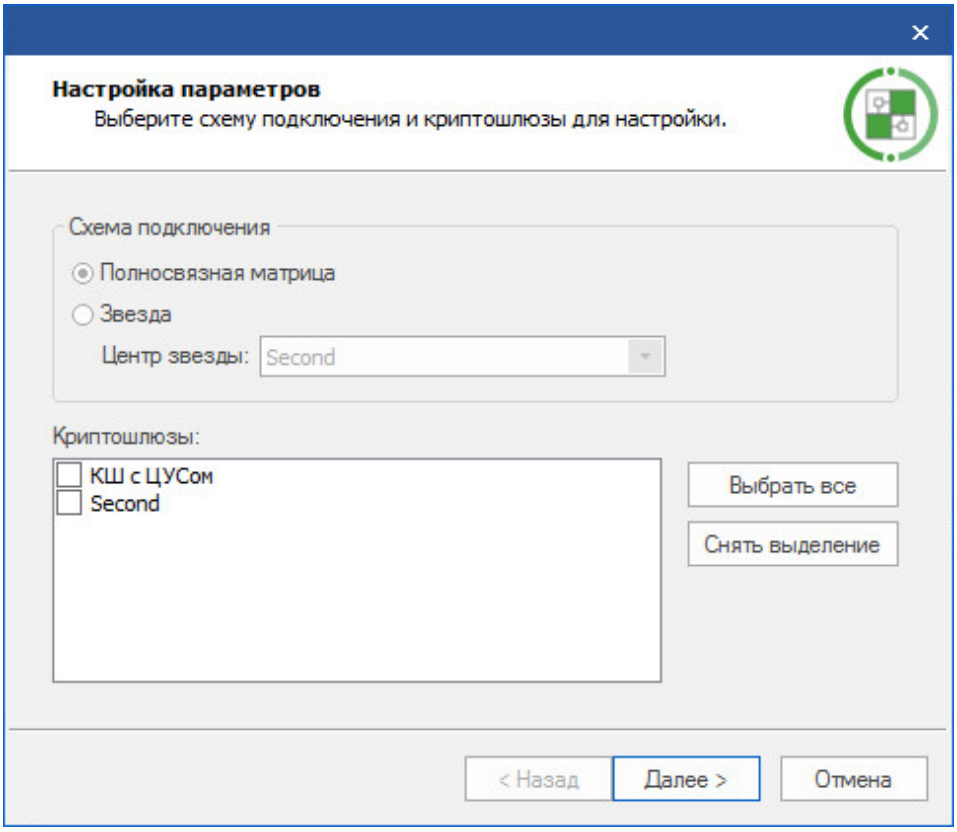


Появится стартовое окно мастера.



2. Нажмите кнопку "Далее >".

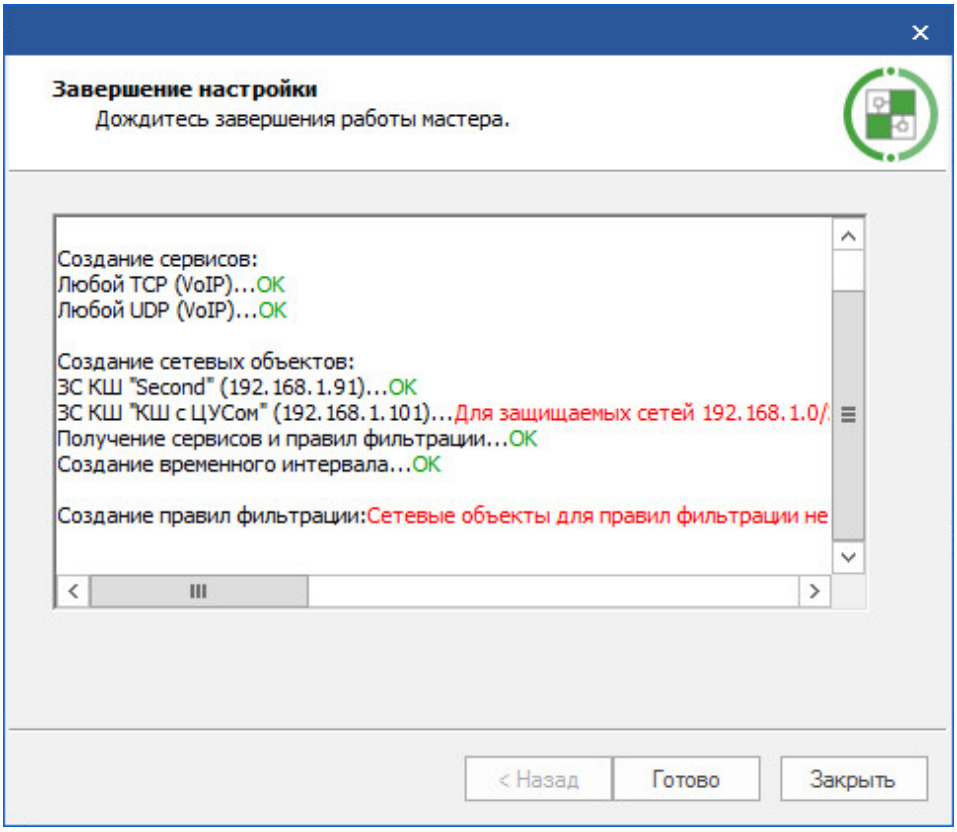
   Появится окно "Настройка параметров".



3. Выберите схему подключения, укажите задействованные КШ и нажмите кнопку "Далее >".

Полносвязная матрица	В списке "Криптошлюзы" отметьте КШ, которые должны участвовать в работе VoIP
Звезда	В поле "Центр звезды" укажите центральный КШ. В списке "Криптошлюзы" отметьте остальные КШ, которые должны участвовать в работе VoIP

Мастер приступит к настройке. Ход настройки отображается в окне "Завершение настройки". При нарушении условий корректной настройки результаты выполнения операций выделяются красным цветом.



4. Дождитесь завершения работы мастера и проанализируйте результаты.
   - Если настройка выполнена успешно, нажмите кнопку "Готово".
   - Если в процессе настройки имели место ошибки, нажмите кнопку "Закрыть", устраните причины их возникновения и повторите процедуру.

Документация

1. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9. Руководство администратора. Управление комплексом.
2. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9. Руководство администратора. Межсетевое экранирование.
3. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9. Руководство администратора. Настройка VPN.
4. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9. Руководство администратора. Аудит.
5. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9. Руководство администратора. Сервер доступа.