



**КОД**  
безопасности

Программный комплекс

**Континент-СОА**

**Версия 4**

**Руководство администратора**

Ввод в эксплуатацию



© Компания "Код Безопасности", 2021. Все права защищены.

Все авторские права на эксплуатационную документацию защищены.

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

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

Почтовый адрес: **115127, Россия, Москва, а/я 66**  
**ООО "Код Безопасности"**

Телефон: **8 495 982-30-20**

E-mail: **info@securitycode.ru**

Web: **https://www.securitycode.ru**

# Оглавление

<b>Список сокращений</b> .....	<b>4</b>
<b>Введение</b> .....	<b>5</b>
<b>Общие сведения</b> .....	<b>6</b>
Назначение и основные функции комплекса .....	6
Порядок ввода комплекса в эксплуатацию .....	7
<b>Развертывание узла безопасности с ЦУС</b> .....	<b>8</b>
Вход в систему локального управления .....	8
Инициализация ЦУС .....	9
Настройка системного времени .....	10
Создание сертификатов .....	11
Настройка центра управления сетью .....	12
<b>Развертывание рабочего места администратора</b> .....	<b>15</b>
Установка Менеджера конфигурации .....	15
Настройка РМ администратора .....	17
Подготовка к запуску Менеджера конфигурации .....	18
Запуск Менеджера конфигурации .....	18
Инициализация программного ДСЧ .....	19
Подключение к ЦУС .....	19
Интерфейс Менеджера конфигурации .....	20
<b>Развертывание узла безопасности с резервным ЦУС</b> .....	<b>22</b>
Инициализация резервного ЦУС .....	22
Настройка системного времени .....	23
Создание сертификатов .....	24
Создание резервного ЦУС на активном ЦУС .....	26
Подключение УБ с резервным ЦУС к активному ЦУС .....	26
Установка конфигурации УБ с резервным ЦУС на активный ЦУС .....	27
Синхронизация резервного ЦУС с активным .....	28
<b>Развертывание узла безопасности</b> .....	<b>29</b>
Выпуск сертификата управления .....	29
Создание УБ и экспорт его конфигурации .....	31
Инициализация узла безопасности .....	32
Настройка узла безопасности .....	33
Установка конфигурации УБ в ЦУС .....	34
<b>Старт комплекса и процедура проверки его работоспособности</b> .....	<b>36</b>
Проверка корректности старта .....	36
Проверка работоспособности .....	36
<b>Приложение</b> .....	<b>39</b>
Подключение к УБ через последовательный порт .....	39
Смена пароля для входа в меню установки BIOS .....	41
Смена кода загрузчика .....	42
Обозначение сетевых интерфейсов .....	42
<b>Документация</b> .....	<b>43</b>

## Список сокращений

БД	База данных
БРП	База решающих правил
ДА	Детектор атак
ДСЧ	Датчик случайных чисел
МК	Менеджер конфигурации
ОС	Операционная система
ПБД	Панель быстрого доступа
ПК	Программный комплекс
ПО	Программное обеспечение
РМ	Рабочее место
СОВ	Система обнаружения вторжений (компьютерных атак)
УБ	Узел безопасности
УЦ	Удостоверяющий центр
ЦУС	Центр управления сетью
CSP	Cryptography Service Provider
DNS	Domain Name System
HTTPS	HyperText Transfer Protocol Secure
IP	Internet Protocol
MMC	Microsoft Management Console
NTP	Network Time Protocol
USB	Universal Serial Bus
UTC	Coordinated Universal Time

# Введение

Документ предназначен для администраторов изделия "Программный комплекс "Континент-СОА". Версия 4" RU.АМБС.58.29.12.008 (далее — комплекс). В нем содержатся сведения, необходимые администраторам для ввода комплекса в эксплуатацию.

Дополнительные сведения, необходимые администратору комплекса, содержатся в документах [1], [2].

**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](mailto:support@securitycode.ru).

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

# Глава 1

## Общие сведения

### Назначение и основные функции комплекса

Средство обнаружения атак (далее — система обнаружения вторжений) входит в состав комплекса "Континент. Версия 4" и предназначено для обнаружения и противодействия основным угрозам безопасности информации (носителей информации), возникающим при преднамеренном несанкционированном доступе или специальном воздействии со стороны:

- внешних нарушителей, действующих из информационно-коммуникационных сетей, в том числе сетей международного информационного обмена;
- внутренних нарушителей, обладающих правами и полномочиями на доступ к информации в информационной системе.

В состав комплекса входят следующие программные компоненты — "Узел безопасности" и "Менеджер конфигурации".

УБ представляет собой программное средство, устанавливаемое на специализированную аппаратную платформу, обеспечивающее взаимодействие между узлами сети с соблюдением требований информационной безопасности.

Вместе с УБ устанавливаются или активируются следующие дополнительные программные модули:

- "Центр управления сетью", предназначенный для настройки и централизованного управления всеми УБ комплекса, а также для мониторинга и аудита их состояния в ходе эксплуатации комплекса.
- "Детектор атак", обеспечивающий обнаружение основных угроз безопасности информации, относящихся к вторжениям (компьютерным атакам).

Менеджер конфигурации представляет собой программное средство, устанавливаемое на одном или нескольких компьютерах (РМ администратора) и предназначенное для удаленного управления функционированием ЦУС.

Управление функционированием компонентов комплекса преимущественно централизованное с возможностью локального внесения изменений в конфигурацию компонента на каждом УБ.

Функционирование каждого компонента УБ зависит от наличия соответствующего типа лицензии:

- рабочая лицензия на компонент (набор функций);
- демонстрационная лицензия на компонент (набор функций);
- лицензия на обновление программного обеспечения компонента.

Комплекс реализует следующие функции:

- контроль работы УБ в режиме реального времени;
- регистрация событий управления и работы СОВ;
- возможность обновления БРП по расписанию;
- возможность создания пользовательских решающих правил СОВ;
- возможность группировки и выборочной установки решающих правил СОВ на ДА;
- подготовка и отправка отчетов о работе ДА;
- оповещение администратора о наступлении событий.

## Порядок ввода комплекса в эксплуатацию

Ввод комплекса в эксплуатацию состоит из следующих этапов:

1. Развертывание УБ с ЦУС (см. стр. **8**).
2. Развертывание РМ администратора (см. стр. **15**).
3. При необходимости развертывание УБ с резервным ЦУС (см. стр. **22**).
4. Развертывание УБ (см. стр. **29**).

**Примечание.** Рекомендуется ввод комплекса в эксплуатацию завершить процедурой обновления ПО, БРП (см. [1]).

## Глава 2

# Развертывание узла безопасности с ЦУС

Развертывание узла безопасности с ЦУС выполняют после установки операционной системы в следующей последовательности:

1. Вход в систему локального управления (см. ниже).

**Примечание.** В целях безопасности рекомендуется сменить пароль для входа в меню настройки BIOS (см. стр. 41).

2. Инициализация ЦУС (см. стр. 9).
3. Настройка системного времени (см. стр. 23).
4. Создание корневого сертификата и сертификата управления ЦУС (см. стр. 11).
5. Настройка ЦУС и применение локальной политики (см. стр. 12).

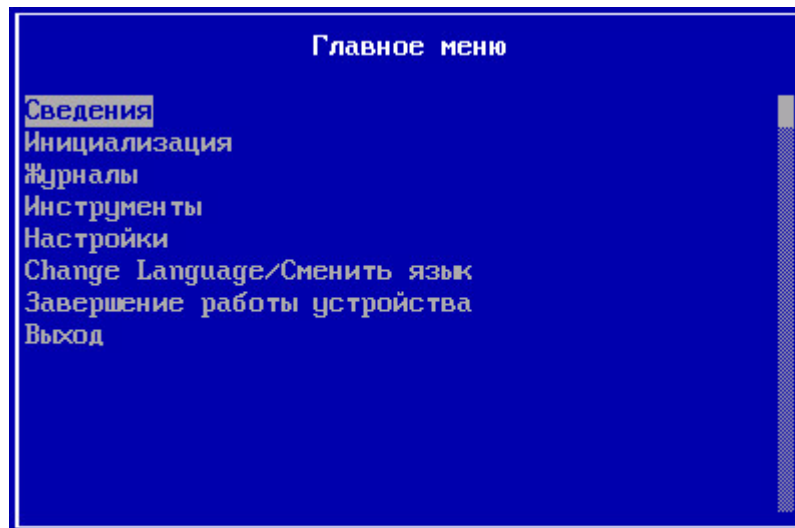
**Примечание.** Рекомендуется сменить код загрузчика для предотвращения возможности изменений параметров загрузки ПО (см. стр. 42).

## Вход в систему локального управления

**Для входа в систему:**

1. Подключите к УБ клавиатуру и монитор или ноутбук (см. стр. 39).
2. Включите питание УБ.

На экране после загрузки ОС появится главное меню локального управления УБ.



Для перемещения между пунктами меню используйте клавиши клавиатуры:

- <Enter> — выбор текущего пункта меню;
- <↑> — перемещение на одну строку вверх;
- <↓> — перемещение на одну строку вниз;
- <Page Up> — перемещение в начало списка;
- <Page Down> — перемещение в конец списка;
- <Esc> — возврат в предыдущее меню.



Администратору доступны следующие типы окон:

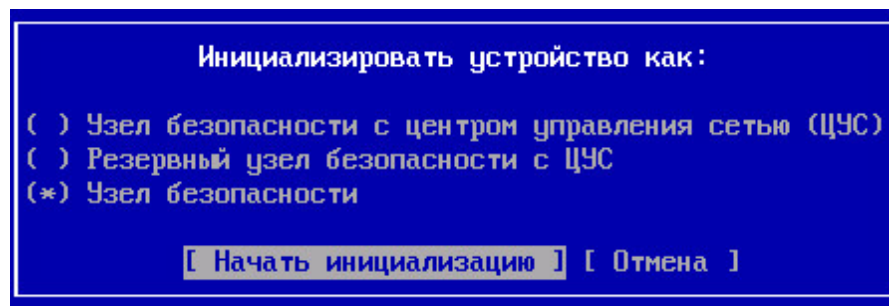
Тип окна	Способ переключения
Окно с меню локального управления	<Alt> + <F1>
Окно с лог-сообщениями об установлении связи с ЦУС, а также о локальных изменениях в конфигурации УБ	<Alt> + <F6>
Окно с лог-сообщениями о процессах подключения к ЦУС (только в ЦУС)	<Alt> + <F8>

## Инициализация ЦУС

### Для инициализации ЦУС:

1. В главном меню локального управления выберите пункт "Инициализация" и нажмите клавишу <Enter>.

На экране появится окно выбора инициализируемого компонента.

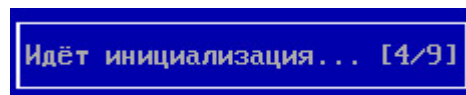


2. Выберите "Узел безопасности с центром управления сетью (ЦУС)" и нажмите клавишу <Enter>.

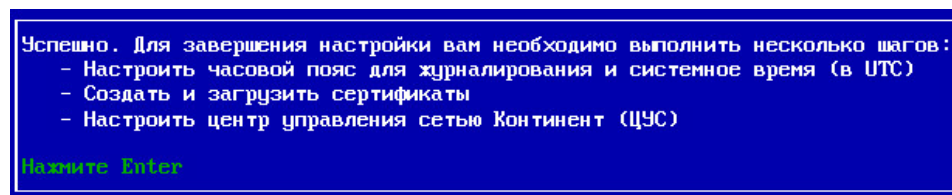
На экране появится запрос на очистку локальных журналов.

3. При необходимости очистки журналов выберите "Да" в окне запроса и нажмите клавишу <Enter>.

Начнется инициализация УБ.

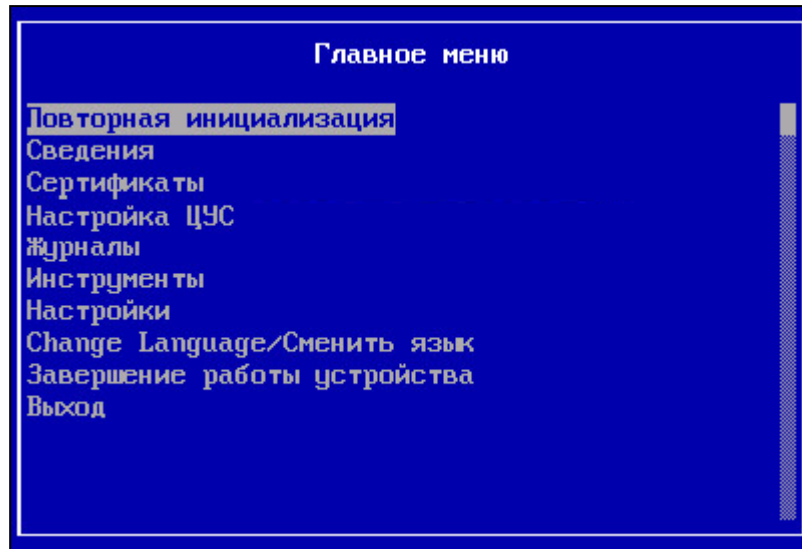


Дождитесь сообщения об успешном завершении инициализации.



4. Нажмите клавишу <Enter>.

Выполнится возврат в главное меню локального управления. При этом в результате инициализации содержание меню будет изменено.

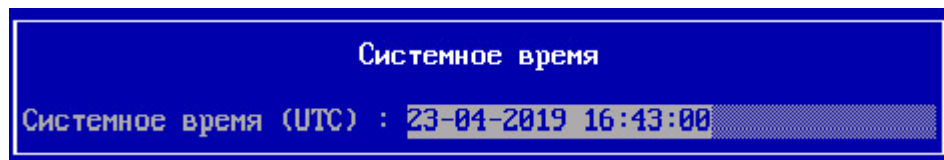


## Настройка системного времени

Перед созданием сертификатов необходимо настроить системное время для правильной синхронизации элементов комплекса.

### Для настройки системного времени:

1. В главном меню выберите пункт "Настройки" и нажмите клавишу <Enter>. На экране появится окно "Меню настроек".
2. Выберите пункт "Системное время" и нажмите клавишу <Enter>. На экране появится окно "Настройка времени".
3. Выберите пункт "Ручная установка времени" и нажмите клавишу <Enter>. На экране появится окно "Системное время".



4. Введите текущее время в формате UTC+0 и нажмите клавишу <Enter>.

**Пример.** Для Москвы нужно вместо UTC+3 установить UTC. То есть если в Москве в данный момент время 13:32, установить нужно время 10:32.

Установится системное время на узле с соответствующим оповещением на экране.

5. Нажмите клавишу <Enter>.

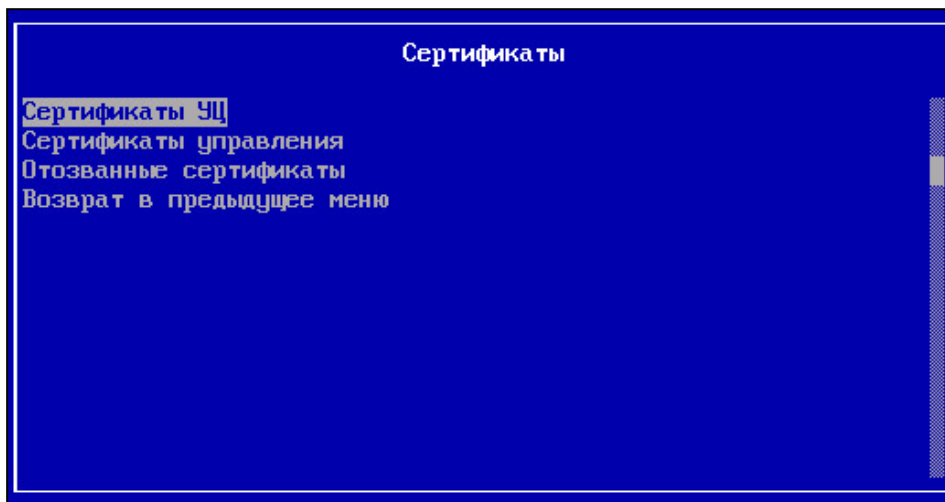
## Создание сертификатов

На этапе развертывания ЦУС средствами локального управления создаются корневой сертификат и сертификат управления ЦУС.

### Для входа в меню "Сертификаты":

В главном меню локального управления выберите пункт "Сертификаты" и нажмите клавишу <Enter>.

На экране появится окно "Сертификаты".



### Для создания корневого сертификата:

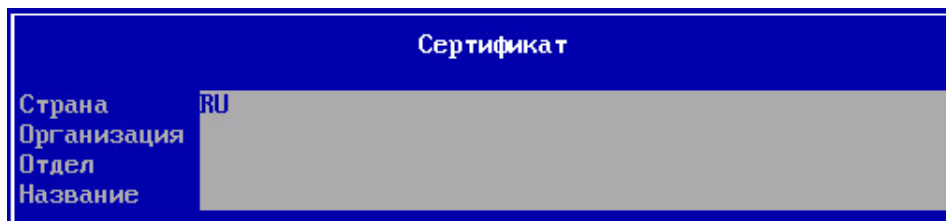
1. Выберите в меню "Сертификаты" пункт "Сертификаты УЦ" и нажмите клавишу <Enter>.

На экране появится окно "Сертификаты УЦ".

**Примечание.** Для взаимодействия с сервером обновлений в комплексе предустановлен сертификат "Доверенный издатель КБ". Для использования в других целях он не предназначен.

2. Для создания корневого сертификата нажмите клавишу <F2>.  
На экране появится окно "Выпуск сертификата".
3. Выберите пункт "Выпуск корневого сертификата" и нажмите клавишу <Enter>.

На экране появится окно "Сертификат".



4. Заполните поля "Организация", "Отдел", "Название" и нажмите клавишу <Enter>.

**Примечание.** Для перемещения используйте стандартные клавиши: <↑>, <↓>, <Tab>, <Page Down>, <Page Up>, <Home>, <End>.

На экране появится сообщение об успешном создании сертификата.

5. Нажмите клавишу <Enter>.  
Выполнится возврат в окно "Выпуск сертификата".

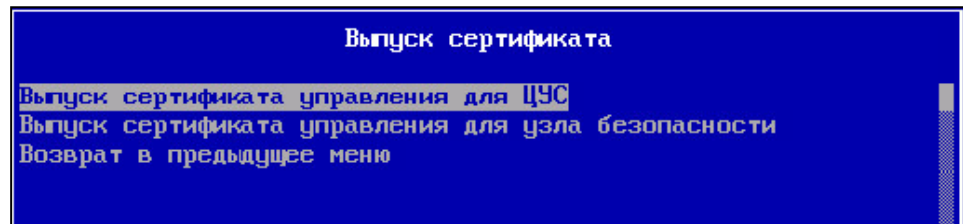
6. Нажмите клавишу <Esc>.  
Выполнится возврат в окно "Сертификаты УЦ". В окне отобразится созданный корневой сертификат.
7. Нажмите клавишу <Esc>.  
Выполнится возврат в меню "Сертификаты".

#### Для создания сертификата управления:

1. Выберите в меню "Сертификаты" пункт "Сертификаты управления" и нажмите клавишу <Enter>.  
На экране появится окно "Сертификаты управления".

**Примечание.** При создании первого сертификата список будет пустым.

2. Нажмите клавишу <F2>.  
На экране появится меню "Выпуск сертификата".

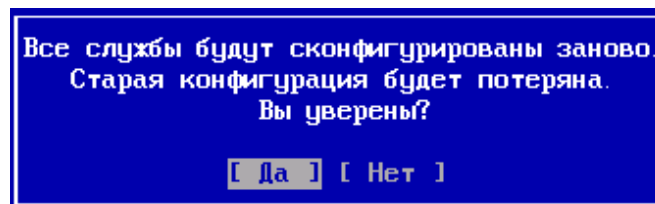


3. Выберите пункт "Выпуск сертификата управления для ЦУС" и нажмите клавишу <Enter>.  
На экране появится окно "Сертификат".
4. Заполните поля "Организация", "Отдел", "Название" и нажмите клавишу <Enter>.  
На экране появится список созданных корневых сертификатов.
5. Выберите корневой сертификат, созданный в предыдущей процедуре, и нажмите клавишу <Enter>.  
На экране появится сообщение об успешном создании сертификата.
6. Нажмите клавишу <Enter>.  
Выполнится возврат в окно "Выпуск сертификата".
7. Нажмите клавишу <Esc>.  
Выполнится возврат в окно "Сертификаты управления". В окне отобразится созданный сертификат управления ЦУС.
8. Нажмите клавишу <Esc>.  
Выполнится возврат в меню "Сертификаты".

## Настройка центра управления сетью

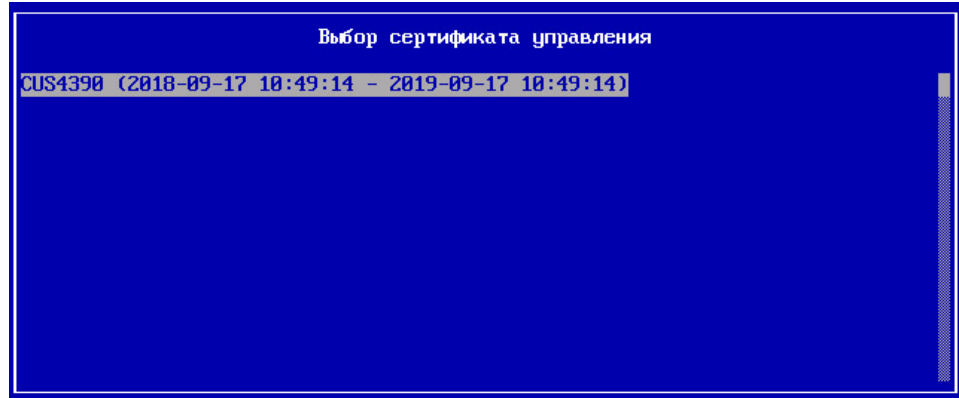
#### Для настройки ЦУС:

1. В главном меню локального управления выберите пункт "Настройка ЦУС" и нажмите клавишу <Enter>.  
На экране появится предупреждение о необходимости конфигурирования служб и запрос на продолжение процедуры.



2. Выберите "Да" и нажмите клавишу <Enter>.

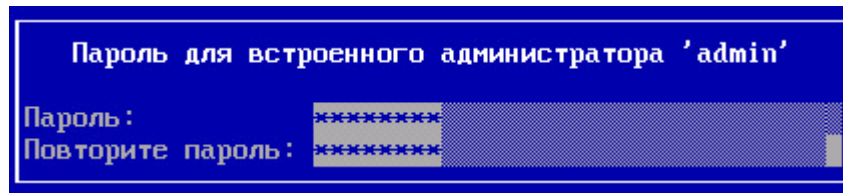
На экране появится окно выбора сертификата управления.



3. Выберите в списке сертификат управления ЦУС (см. стр. 11) и нажмите клавишу <Enter>.

На экране появится окно ввода пароля главного администратора.

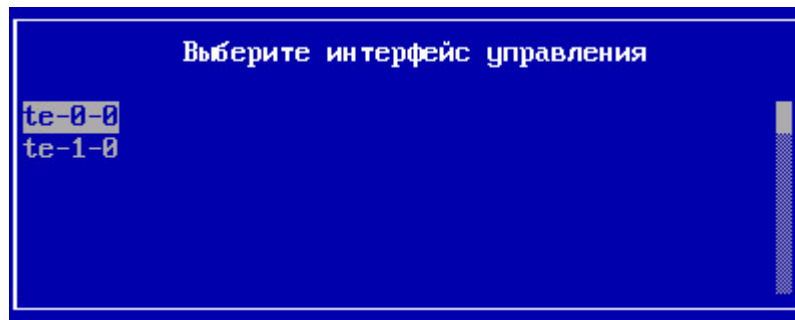
4. Введите дважды пароль главного администратора и нажмите клавишу <Enter>.



**Примечание.** Пароль должен содержать не менее 8 символов. Пароль должен содержать как минимум одну заглавную и одну строчную букву латинского алфавита. Кириллица в обоих регистрах запрещена. Пароль должен содержать как минимум одну цифру и один из следующих специальных символов:

! " # \$ % & ' ( ) \* + , - . / : ; < \ > ? @ [ \ ] ^ \_ ` { | } ~

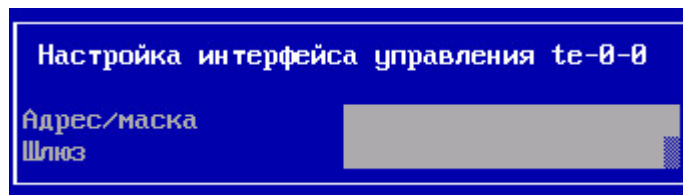
После успешного ввода пароля на экране появится окно для выбора интерфейса управления.



Разъяснение обозначения интерфейсов описывается на стр. 42

5. Выберите интерфейс, через который осуществляется подключение к РМ администратора, и нажмите клавишу <Enter>.

На экране появится окно настройки интерфейса управления.

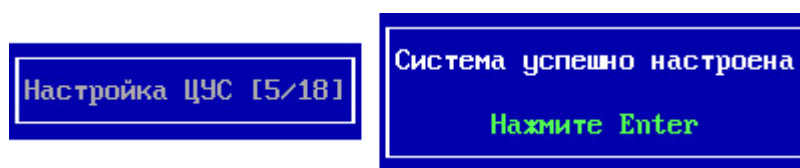


6. Введите IP-адрес ЦУС с указанием префикса маски подсети и IP-адрес шлюза (если необходимо), затем нажмите клавишу <Enter>.

На экране появится запрос на применение указанных настроек.

7. Для применения настроек выберите "Да" и нажмите клавишу <Enter>.

Начнется последовательное выполнение процессов настройки ЦУС, после чего на экране появится сообщение об успешном завершении настройки.



8. Нажмите клавишу <Enter>.

После завершения настройки выполнится возврат в главное меню для выполнения процедуры аутентификации пользователя.

**Внимание!** В случае сбоя при настройке ЦУС обратитесь к событиям, отраженным в системном журнале, для выяснения причины сбоя.

После устранения причины сбоя выполните команду повторной инициализации в меню "Инструменты", перезагрузите ЦУС и заново выполните процедуры настройки времени и создания сертификатов.

**Примечание.** При инициализации ЦУС создается демолицензия с нулевым ID клиента, которая позволяет использовать возможности комплекса в ограниченный период времени — 14 дней. Демолицензия не позволяет использовать расширенный контроль приложений, Web/FTP фильтры. Кроме того, количество подключений к СД ограничено двумя. По завершении срока действия демолицензии возможности эксплуатации комплекса будут значительно ограничены. Для установки рабочей лицензии необходимо установить ПО МК (см. ниже) и загрузить лицензию в репозиторий (см. [4], раздел "Управление лицензиями").

## Глава 3

# Развертывание рабочего места администратора

ПО "Менеджер конфигурации", входящее в состав комплекса, является средством удаленного управления ЦУС, а также другими узлами комплекса.

Развертывание РМ администратора включает в себя последовательное выполнение трех этапов:

1. Установка МК и криптопровайдера CSP (см. ниже).
2. Настройка РМ администратора (см. стр. 17).
3. Настройка системы мониторинга и аудита (см. [2]).

**Примечание.** Использование и управление системой мониторинга и аудита комплекса осуществляется на любом хосте в защищаемой сети после соответствующей настройки.

## Установка Менеджера конфигурации

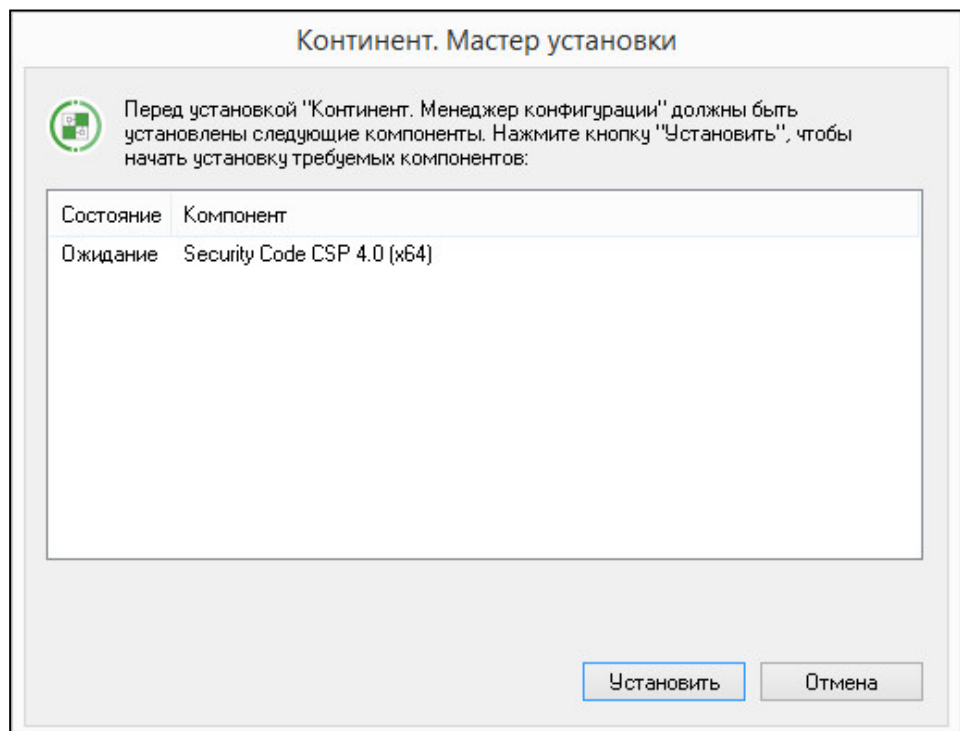
Установку и удаление МК и CSP может выполнить только пользователь, наделенный правами локального администратора данного компьютера.

Перед запуском программы установки завершите работу всех приложений.

### Для установки МК:

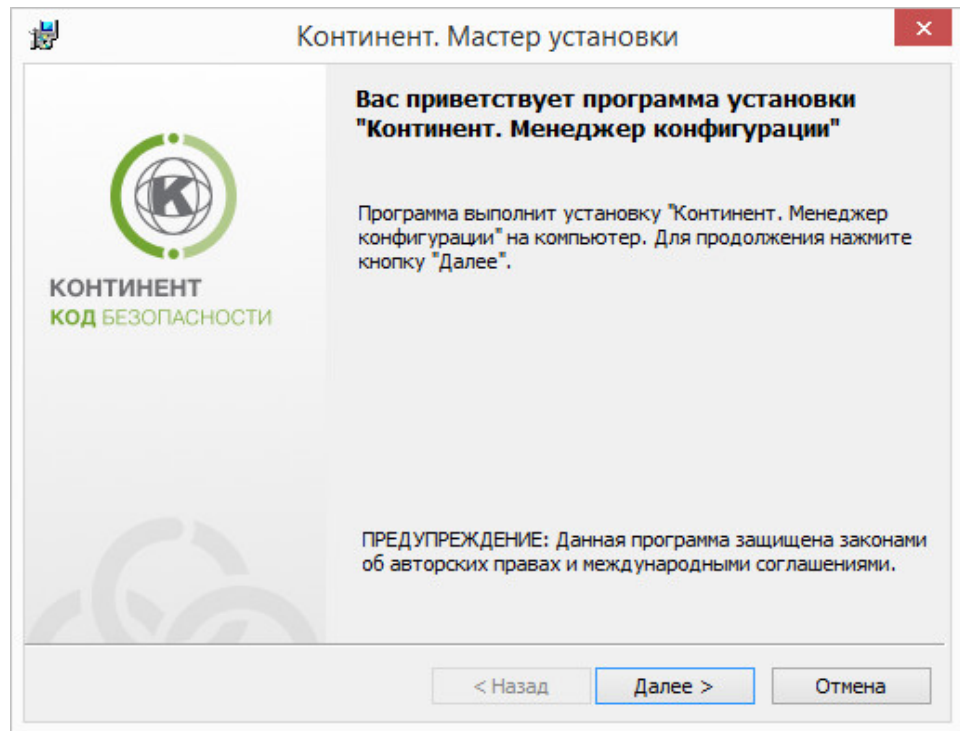
1. Запустите на исполнение:
  - файл \Setup\Continent\MS\Rus\x86\Setup.exe — для 32-разрядной ОС;
  - файл \Setup\Continent\MS\Rus\x64\Setup.exe — для 64-разрядной ОС.

На экране появится окно со списком дополнительных компонентов, которые должны быть установлены до начала установки МК.



2. Нажмите кнопку "Установить".

После завершения установки дополнительных компонентов на экране появится стартовое окно программы установки МК.



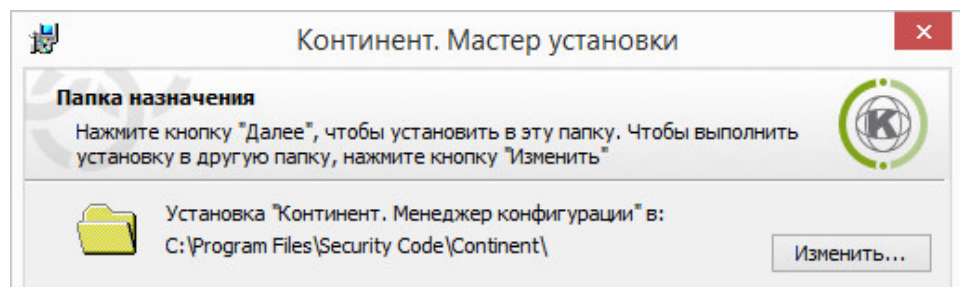
3. Ознакомьтесь с информацией, содержащейся в стартовом окне, и нажмите кнопку "Далее >" для продолжения установки.

Появится окно с текстом лицензионного соглашения.

4. Изучите содержание лицензионного соглашения, прочитав его до конца. Если вы согласны с условиями лицензионного соглашения, установите отметку в поле "Я принимаю условия лицензионного соглашения", затем нажмите кнопку "Далее >".

На экране появится окно "Папка назначения" для определения папки установки программы "Континент. Менеджер конфигурации".

5. При необходимости измените папку установки и нажмите кнопку "Далее >". Для выбора папки используйте кнопку "Изменить...".



По умолчанию программа установки копирует файлы на системный диск в папку ..\Program Files\Security Code\Continent.

6. Для продолжения установки нажмите кнопку "Далее >".

На экране появится финальное окно мастера установки МК.

**Примечание.** Для корректировки параметров установки используйте кнопку "< Назад".



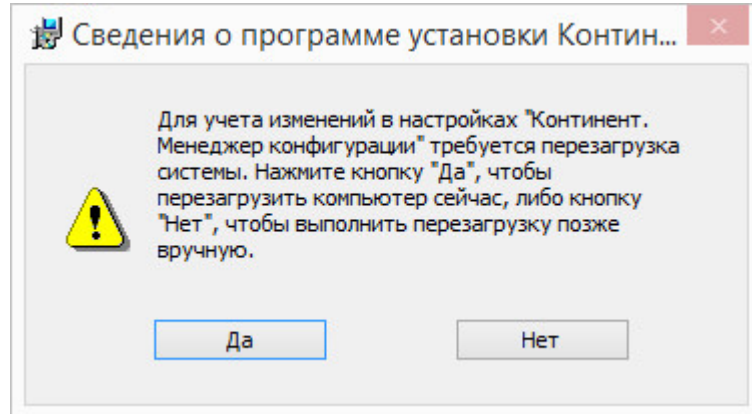
7. Для начала установки программы нажмите кнопку "Установить".

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

**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 установочного диска и повторите установку. Если это не приведет к желаемому результату, обратитесь к поставщику комплекса.

После установки МК на экране появится информационное окно об успешной установке приложения.

8. Для завершения установки нажмите кнопку "Готово". При этом появится окно с предложением перезагрузить компьютер.



9. Перезагрузите компьютер.

После перезагрузки на рабочем столе появится ярлык МК, а в меню "Пуск" ОС Windows появится группа "Код Безопасности" с командами — "Менеджер конфигурации", "Код Безопасности CSP" и "Восстановление Код Безопасности CSP".

## Настройка РМ администратора

Первый запуск МК включает в себя последовательное выполнение следующих этапов:

1. Подготовка к запуску МК (см. ниже).
2. Запуск МК (см. стр. 18).
3. Инициализация программного ДСЧ (см. стр. 19).
4. Подключение к ЦУС (см. стр. 19).

При последующих запусках МК сразу отображается окно подключения к ЦУС с автоматически заполненными полями IP-адреса ЦУС, к которому было выполнено последнее подключение МК, и учетной записи администратора, осуществившего последнее подключение.

## Подготовка к запуску Менеджера конфигурации

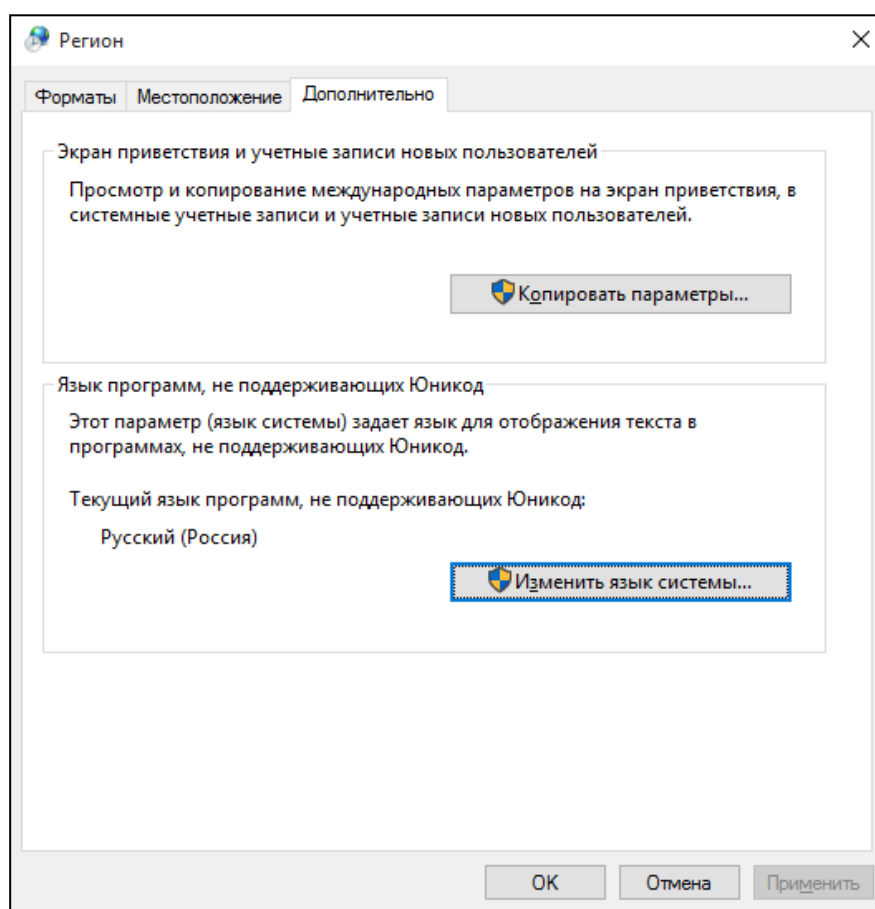
Перед запуском МК необходимо проверить региональные настройки ОС. В случае установленного по умолчанию английского языка для программ, не поддерживающих Юникод, попытка подключения к ЦУС завершится появлением сообщения об ошибке.

### Для проверки региональных настроек ОС:

1. Откройте раздел "Панель управления | Часы, язык и регион | Региональные стандарты".
2. Перейдите на вкладку "Дополнительно". Если в области "Язык программ, не поддерживающих Юникод" не установлен русский язык — нажмите кнопку "Изменить язык системы".

**Примечание.** Если отображается запрос на ввод пароля администратора или его подтверждение, укажите пароль или предоставьте подтверждение.

3. Выберите язык "Русский (Россия)" и нажмите кнопку "ОК".

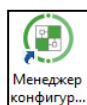


4. Выполните перезагрузку ОС.

## Запуск Менеджера конфигурации

### Для запуска Менеджера конфигурации:

- Активируйте на рабочем столе ярлык МК.



На экране появится главное окно Менеджера конфигурации (см. стр. 20).


## Инициализация программного ДСЧ

При первом после установки запуске МК в его главном окне появится информационное сообщение о необходимости инициализации биологического ДСЧ.

### Для инициализации ДСЧ:

1. Нажмите ссылку "здесь" для начала процесса инициализации ДСЧ и, следуя инструкции, нажимайте мишень, перемещающуюся по экрану, левой кнопкой мыши до завершения процесса накопления энтропии.

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

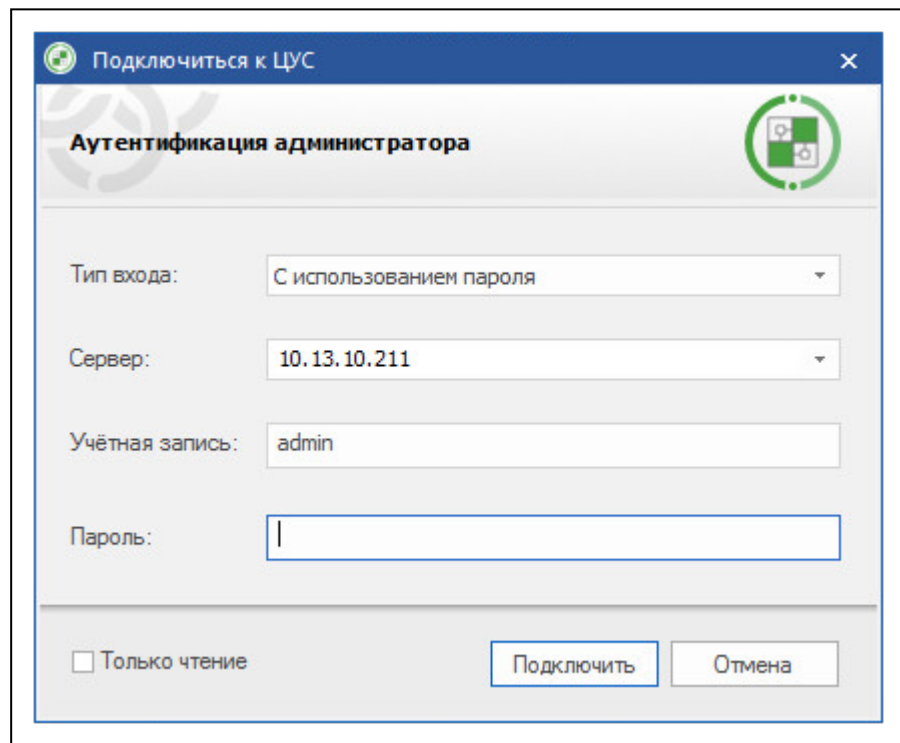
2. После завершения процесса накопления энтропии нажмите кнопку установления соединения с ЦУС  в левом верхнем углу МК.

## Подключение к ЦУС

### Для подключения к ЦУС:

1. Запустите Менеджер конфигурации (см. выше).

На экране появится диалог подключения администратора к ЦУС.



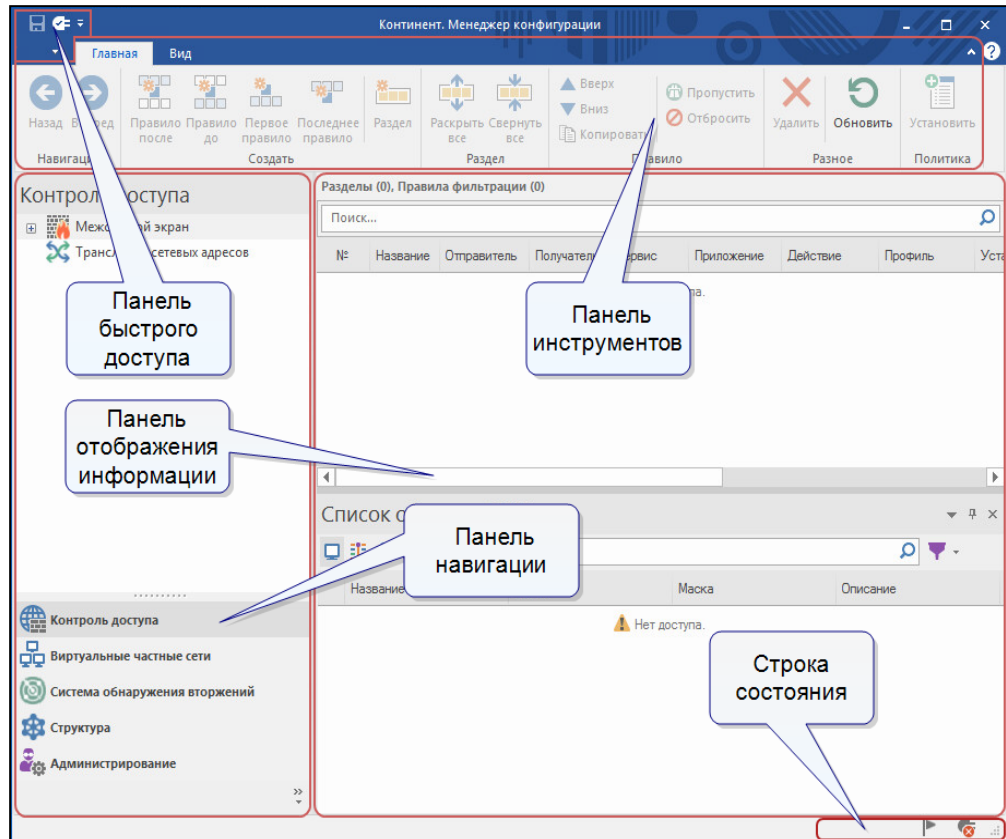
2. В поле "Тип входа" выберите значение "С использованием пароля" и при первом запуске МК в поле "Сервер" введите IP-адрес ЦУС, к которому осуществляется подключение.

- Введите имя и пароль администратора в поля "Учетная запись" и "Пароль". Нажмите кнопку "Подключить".









После подключения к ЦУС на экране в главном окне МК появится информация о текущем состоянии комплекса.

## Интерфейс Менеджера конфигурации

После запуска МК на экране отображается главное окно приложения.



Окно "Менеджер конфигурации" содержит следующие основные элементы интерфейса:

Элемент интерфейса	Описание
<b>Панель инструментов</b>	<p>Содержит набор инструментов и две вкладки:</p> <ul style="list-style-type: none"> <li>• "Главная" — отображение панели инструментов;</li> <li>• "Вид" — настройка отображения элементов окна Менеджера конфигурации.</li> </ul> <p>Инструменты — это функциональные кнопки, предназначенные для запуска часто используемых команд. Состав кнопок зависит от выбора подраздела на панели навигации, а их доступность определяется текущей ситуацией. При наведении курсора мыши на кнопку появляется всплывающая подсказка с дополнительной информацией</p>
<b>Панель быстрого доступа</b>	<p>Предназначена для быстрого доступа к часто используемым командам. Содержит настраиваемые кнопки:</p> <ul style="list-style-type: none"> <li>•  — сохранение текущей конфигурации;</li> <li>•  — установка политики безопасности;</li> <li>•  — настройка подключений к ЦУС;</li> <li>•  — установка соединения с ЦУС;</li> <li>•  — настройка панели быстрого доступа;</li> <li>•  — вызов меню команд быстрого доступа</li> </ul>
<b>Панель навигации</b>	<p>Содержит следующие разделы:</p> <ul style="list-style-type: none"> <li>• "Контроль доступа" — управление правилами фильтрации и трансляции трафика;</li> <li>• "Виртуальные частные сети" — создание и настройка VPN;</li> <li>• "Система обнаружения вторжений" — настройка параметров системы обнаружения и предупреждения вторжений;</li> <li>• "Структура" — управление параметрами УБ комплекса;</li> <li>• "Администрирование" — управление сервисными функциями (работа с сертификатами, резервными копиями, управление лицензиями, обновлением и др.)</li> </ul>
<b>Панель отображения информации</b>	<p>Предназначена для отображения информации выбранного раздела панели навигации</p>
<b>Строка состояния</b>	<p>Содержит следующие данные:</p> <ul style="list-style-type: none"> <li>• число выполняемых задач и кнопка вызова центра уведомлений , содержащего информацию о выполняемых задачах и ссылку на переход к общему списку задач (см. раздел "Администрирование");</li> <li>• пиктограмма состояния соединения с ЦУС (при установленном соединении — с именем учетной записи авторизованного администратора, к примеру  admin)</li> </ul>

## Глава 4

# Развертывание узла безопасности с резервным ЦУС

Развертывание узла безопасности с резервным ЦУС (также по тексту резервного ЦУС) выполняются в следующей последовательности:

**Примечание.** В целях безопасности рекомендуется сменить пароль для входа в меню настройки BIOS (см. стр. 41).

1. Инициализация резервного ЦУС (см. стр. 22).
2. Установка системного времени (см. стр. 23).
3. Создание сертификата управления ЦУС (см. стр. 24).
4. Создание резервного ЦУС активного ЦУС (см. стр. 26).
5. Настройка резервного ЦУС и применение локальной политики (см. стр. 26).

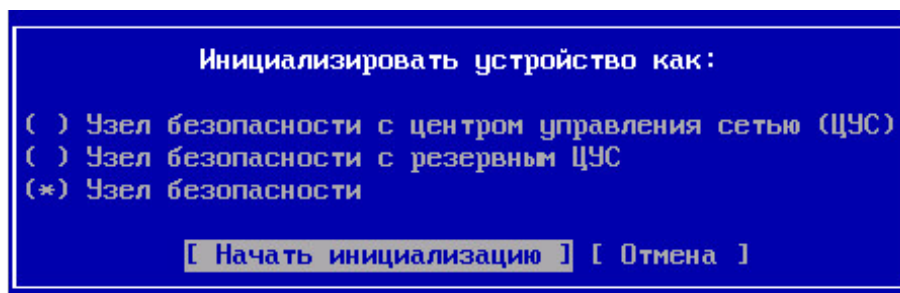
**Примечание.** Рекомендуется сменить код загрузчика для предотвращения возможности изменений параметров загрузки ПО (см. стр. 42).

## Инициализация резервного ЦУС

**Для инициализации резервного ЦУС:**

1. В главном меню локального управления УБ с резервным ЦУС выберите пункт "Инициализация" и нажмите клавишу <Enter>.

На экране появится окно выбора инициализируемого компонента.



2. Выберите пункт "Узел безопасности с резервным ЦУС" и нажмите клавишу <Enter>.

На экране появится запрос на очистку локальных журналов.

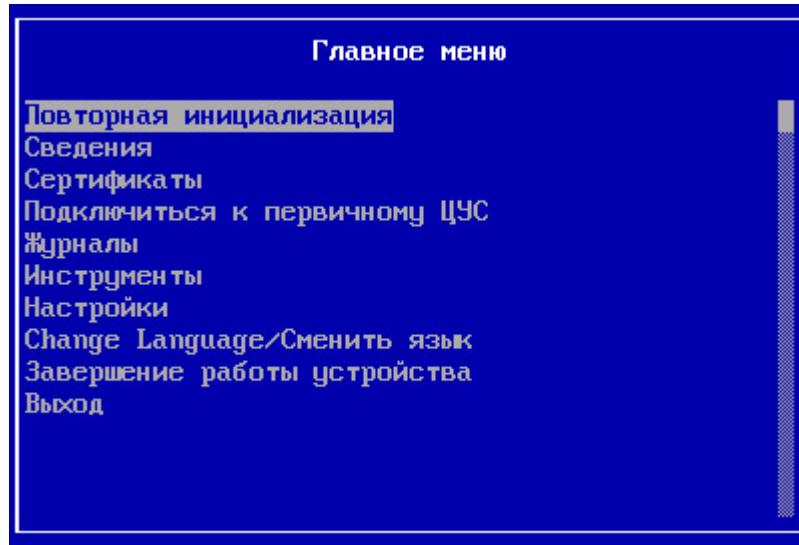
3. При необходимости очистки журналов выберите "Да" в окне запроса и нажмите клавишу <Enter>.

Начнется инициализация УБ.

Дождитесь сообщения об успешном завершении инициализации.

4. Нажмите клавишу <Enter>.

Выполнится возврат в главное меню локального управления. При этом в результате инициализации содержание меню будет изменено.

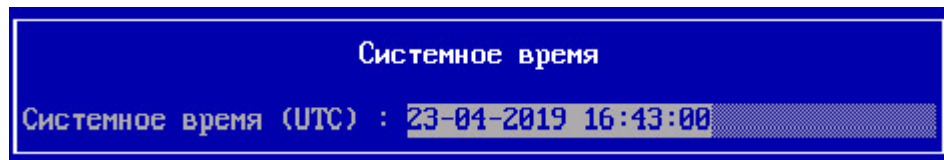


## Настройка системного времени

Перед созданием сертификатов необходимо настроить системное время для правильной синхронизации элементов комплекса.

**Для настройки системного времени:**

1. В главном меню выберите пункт "Настройки" и нажмите клавишу <Enter>. На экране появится окно "Меню настроек".
2. Выберите пункт "Системное время" и нажмите клавишу <Enter>. На экране появится окно "Настройка времени".
3. Выберите пункт "Ручная установка времени" и нажмите клавишу <Enter>. На экране появится окно "Системное время".



4. Введите текущее время в формате UTC+0 и нажмите клавишу <Enter>.

**Пример.** Для Москвы нужно вместо UTC+3 установить UTC. То есть если в Москве в данный момент время 13:32, установить нужно время 10:32.

Установится системное время на узле с соответствующим оповещением на экране.

5. Нажмите клавишу <Enter>.

## Создание сертификатов

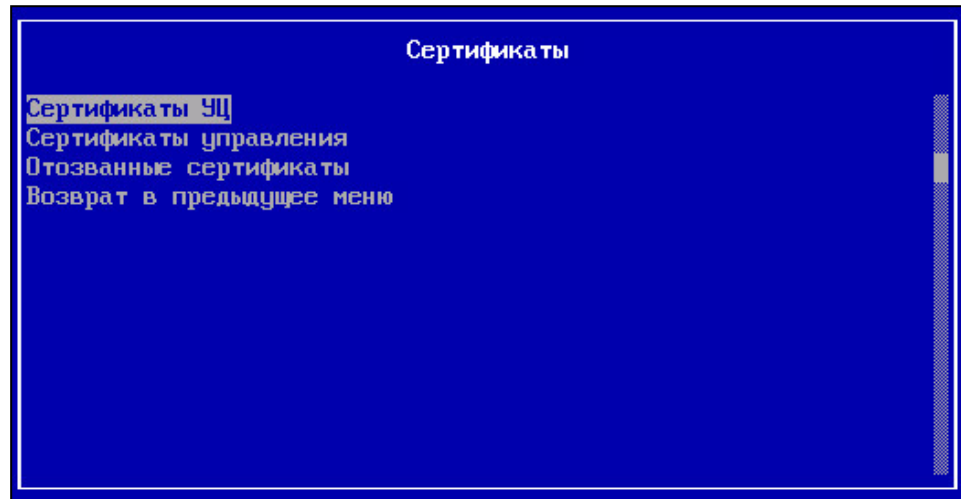
На этапе развертывания резервного ЦУС средствами локального управления создается только сертификат управления.

### Создание запроса на выпуск сертификата

#### Для входа в меню "Сертификаты":

- в главном меню локального управления выберите пункт "Сертификаты" и нажмите клавишу <Enter>.

На экране появится окно "Сертификаты".



#### Для создания запроса на выпуск сертификата управления:

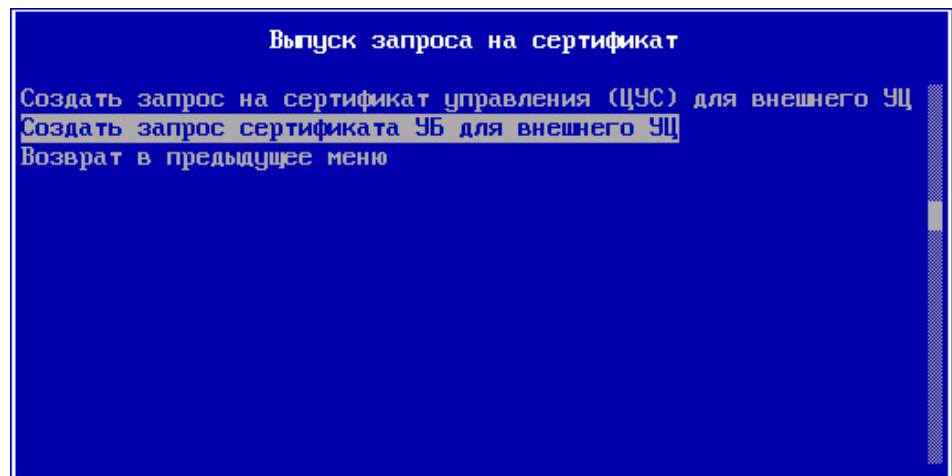
1. Выберите в меню "Сертификаты" пункт "Сертификаты управления" и нажмите клавишу <Enter>.

На экране появится окно "Сертификаты управления".

**Примечание.** При создании первого сертификата список будет пустым.

2. Нажмите клавишу <F4>.

На экране появится меню "Выпуск запроса на сертификат".



3. Выберите пункт "Создать запрос на сертификат управления (ЦУС) для внешнего УЦ" и нажмите клавишу <Enter>.

На экране появится окно с предложением подключить USB-флеш-накопитель.

4. Подключите USB-флеш-накопитель и нажмите клавишу <Enter>.

На экране появится окно "Сертификат".



5. Заполните поля "Организация", "Отдел", "Название" и нажмите клавишу <Enter>.  
На экране появится сообщение об успешной записи запроса на внешний носитель.
6. Нажмите клавишу <Enter>.  
Выполнится возврат в окно "Выпуск запроса на сертификат".
7. Нажмите клавишу <Esc>.  
Выполнится возврат в окно "Сертификаты управления". Созданный запрос будет отображен в списке.
8. Нажмите клавишу <Esc>.  
Выполнится возврат в окно "Сертификаты".
9. Нажмите клавишу <Esc>.  
Выполнится возврат в главное меню локального управления.

### **Выпуск сертификата управления резервного ЦУС на активном ЦУС**

#### **Для создания сертификата средствами локального управления:**

1. В главном меню локального управления ЦУС выберите пункт "Сертификаты" и нажмите клавишу <Enter>.  
На экране появится меню "Сертификаты".
  2. Выберите пункт "Сертификаты управления" и нажмите клавишу <Enter>.  
На экране появится список сертификатов управления ЦУС.
  3. Нажмите клавишу <F2>.  
На экране появится окно "Выпуск сертификата".
  4. Выберите пункт "Выпуск сертификата управления для узла безопасности" и нажмите клавишу <Enter>.  
На экране появится окно с вопросом о наличии запроса на сертификат.
  5. Вставьте внешний носитель с файлом запроса, выберите "Да" и нажмите клавишу <Enter>.  
На экране появится окно со списком файлов, обнаруженных на внешнем носителе.
- Примечание.** По умолчанию имя файла запроса на сертификат имеет формат: continent-XX.req, где XX — ID узла безопасности.
6. Выберите нужный файл запроса и нажмите клавишу <Enter>.  
На экране появится окно выбора корневого сертификата.
  7. Выберите нужный корневой сертификат и нажмите клавишу <Enter>.  
Будет создан файл сертификата управления для резервного ЦУС, после чего появится сообщение об успешном создании сертификата.
  8. Нажмите клавишу <Enter>.  
Произойдет возврат к окну "Выпуск сертификата".
  9. Выберите пункт "Возврат в предыдущее меню" и нажмите клавишу <Enter>.  
Будет выполнен возврат в окно "Сертификаты управления". В списке появится новый сертификат, созданный на основании запроса.

## Создание резервного ЦУС на активном ЦУС

**Для создания резервного ЦУС средствами локального управления активного ЦУС:**

1. В главном меню локального управления активного ЦУС выберите пункт "Инструменты" и нажмите клавишу <Enter>.
 

На экране появится "Меню инструменты".
2. Выберите пункт "Создать узел безопасности с резервным ЦУС" и нажмите клавишу <Enter>.
 

На экране появится окно с предложением подключить USB-флеш-накопитель (если не был подключен ранее).
3. Подключите USB-флеш-накопитель и нажмите клавишу <Enter>.
 

На экране появится окно с запросом серийного номера УБ с резервным ЦУС.
4. Укажите серийный номер и нажмите клавишу <Enter>.
 

На экране появится окно выбора сертификата управления для резервного ЦУС.
5. Выберите созданный ранее сертификат и нажмите клавишу <Enter>.
 

Будет начата операция создания резервного ЦУС.

Идет создание узла безопасности

После окончания операции будет выведено сообщение об успешном создании УБ. В USB-флеш-накопитель будет записан файл конфигурации созданного УБ с резервным ЦУС.

6. Нажмите клавишу <Enter>.
 

Будет произведен возврат в "Меню инструменты".
7. Нажмите клавишу <Esc>.
 

Будет произведен возврат в главное меню локального управления.

## Подключение УБ с резервным ЦУС к активному ЦУС

Перед началом процедуры подготовьте внешний носитель с конфигурационным файлом gate-XX.json, где XX — серийный номер УБ.

1. В главном меню локального управления УБ с резервным ЦУС выберите пункт "Подключиться к первичному ЦУС".
 

На экране появится предупреждение о необходимости конфигурирования служб и запрос на продолжение процедуры.

Все службы будут сконфигурированы заново.  
Старая конфигурация будет потеряна.  
Вы уверены?

[ Да ] [ Нет ]

2. Выберите "Да" и нажмите клавишу <Enter>.
 

На экране появится окно с предложением подключить USB-флеш-накопитель (если не был подключен ранее).
3. Подключите USB-флеш-накопитель с сохраненной ранее конфигурацией и нажмите клавишу <Enter>.
 

На экране появится окно со списком файлов, обнаруженных на внешнем носителе.

4. Выберите требуемый файл конфигурации с расширением .json и нажмите клавишу <Enter>.
 

На экране появится окно выбора интерфейса управления УБ со списком интерфейсов данного узла.
5. Выберите интерфейс, используемый для подключения к ЦУС, и нажмите клавишу <Enter>.
 

На экране появится окно настройки интерфейса управления УБ.
6. Введите его IP-адрес с маской, а также IP-адрес шлюза и нажмите клавишу <Enter>.
 

На экране появится информационное окно о применении настроек.
7. Выберите "Да" и нажмите клавишу <Enter>.
 

Начнется настройка УБ, после чего на экране появится сообщение об успешном завершении операции.
8. Нажмите клавишу <Enter>.

## Установка конфигурации УБ с резервным ЦУС на активный ЦУС

**Примечание.** Если в МК появилось информационное окно о перехвате управления из-за локального управления ЦУС, то установите соединение с ЦУС заново.

### Для установки конфигурации УБ:

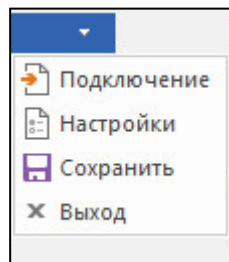
1. Откройте МК и перейдите в раздел "Структура".
 

В правой части окна отобразится список УБ комплекса.

**Примечание.** Если в списке у подключаемого УБ с резервным ЦУС не указана локальная версия конфигурации, нажмите кнопку "Обновить" на панели инструментов.
2. Выберите в списке подключаемый УБ и нажмите кнопку "Подтвердить изменения" на панели инструментов.
 

Появится окно с запросом о подтверждении локальных изменений конфигурации УБ.
3. Нажмите кнопку "Да".
 

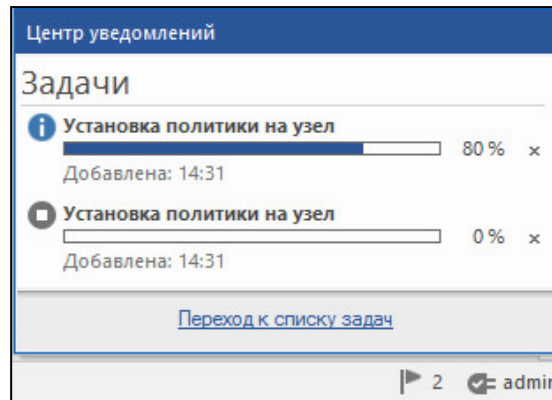
Система внесет изменения в конфигурацию ЦУС, сохранит ее в БД, после чего появится окно с сообщением об успешном завершении операции.
4. Нажмите кнопку "ОК".
5. Для сохранения выполненных настроек в автозагружаемую конфигурацию в окне Менеджера конфигурации в левом верхнем углу нажмите на раскрывающийся список и выберите пункт "Сохранить".



6. Нажмите кнопку "Установить" на панели инструментов.
 

Откроется окно для установки политик узлам комплекса.
7. В окне установки политики выберите УБ с резервным ЦУС, поставив отметку слева от названия. Нажмите кнопку "ОК".
 

Сформируется задача по установке политики на выбранный узел, после чего на экране отобразится центр уведомлений, на котором можно в реальном времени наблюдать степень выполнения поставленных задач.



8. Дождитесь окончания процесса.

## Синхронизация резервного ЦУС с активным

1. Откройте МК и перейдите в раздел "Структура".  
В правой части окна отобразится список УБ комплекса.
2. Выберите в списке подключаемый УБ, вызовите контекстное меню и выберите пункт "Резервирование — Синхронизировать ЦУС".  
Отобразится запрос на подтверждение выполнения полной синхронизации ЦУС.
3. Выберите "Да" и нажмите клавишу <Enter>.  
Будет начат процесс синхронизации, о чем свидетельствует прогресс-бар на экране.  
После окончания процесса в столбце "Состояние" для УБ с резервным ЦУС будет указан статус "Синхронизирован".

## Глава 5

# Развертывание узла безопасности

Для развертывания УБ рекомендуется выполнить следующие этапы:

1. Выпуск сертификата управления (см. ниже).
2. Создание УБ и экспорт его конфигурации (см. стр. 31).
3. Инициализация УБ (см. стр. 32).
4. Настройка УБ (см. стр. 33).
5. Установка конфигурации УБ в ЦУС (см. стр. 34).

**Внимание!** Этапы 1, 2, 4 выполняются централизованно с помощью МК, этап 3 — локально на УБ. Пропуск 4-го этапа и переход к эксплуатации УБ приведет к необходимости повторной инициализации и перенастройки УБ.

Процедуру развертывания УБ рекомендуется завершить сменой кода загрузчика для предотвращения возможности изменений параметров загрузки ПО (см. стр. 42).

## Выпуск сертификата управления

Для начала процедуры необходимо знать идентификатор инициализируемого УБ, указанный на его корпусе, и приготовить внешний носитель для экспорта на него файлов, которые требуются на УБ для настройки подключения к ЦУС:

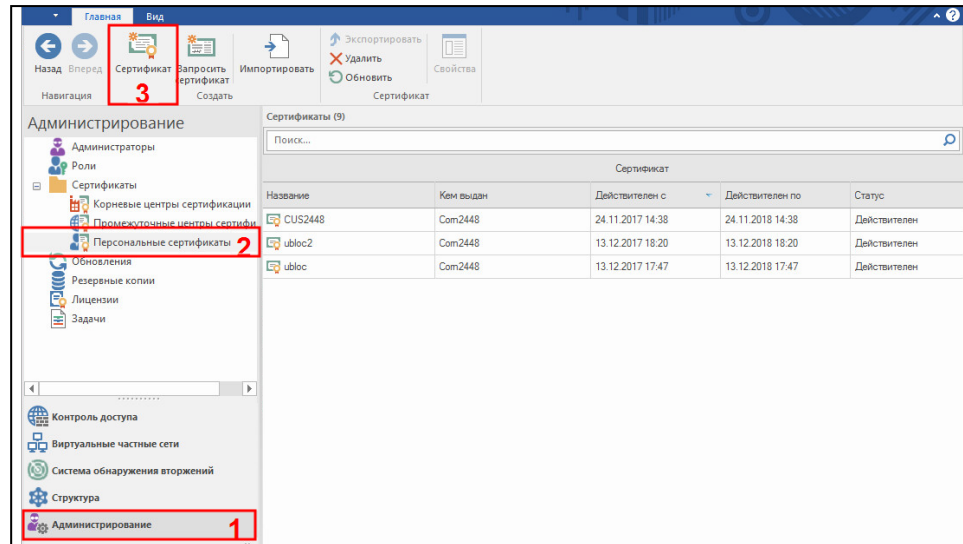
- файл сертификата управления УБ;
- запрос на сертификат управления УБ;
- контейнер закрытого ключа УБ;
- конфигурационный файл УБ.

**Внимание!** Не рекомендуется использовать внешний носитель, на котором хранятся другие контейнеры закрытых ключей.


### Для создания сертификата в Менеджере конфигурации:

1. Перейдите в раздел "Администрирование" на панели навигации МК.
2. В списке сертификатов выберите "Персональные сертификаты".  
В правой части экрана появится список установленных персональных сертификатов.

### 3. Нажмите кнопку "Сертификат" на панели инструментов.



На экране появится окно "Сертификат".

4. В поле "Тип сертификата" выберите пункт "Узел безопасности", затем заполните поля областей "Данные о владельце сертификата" и "Назначение ключа".
5. В области "Дополнительно" выберите созданный при настройке ЦУС корневой сертификат, установите требуемый срок действия сертификата управления.
6. Нажмите кнопку , выберите корневой каталог внешнего носителя для записи файлов, а также укажите их общее название и нажмите кнопку "Сохранить".
7. Нажмите кнопку "Создать сертификат".

На экране появится окно для ввода пароля на доступ к контейнеру.

- Введите дважды пароль и нажмите кнопку "ОК".

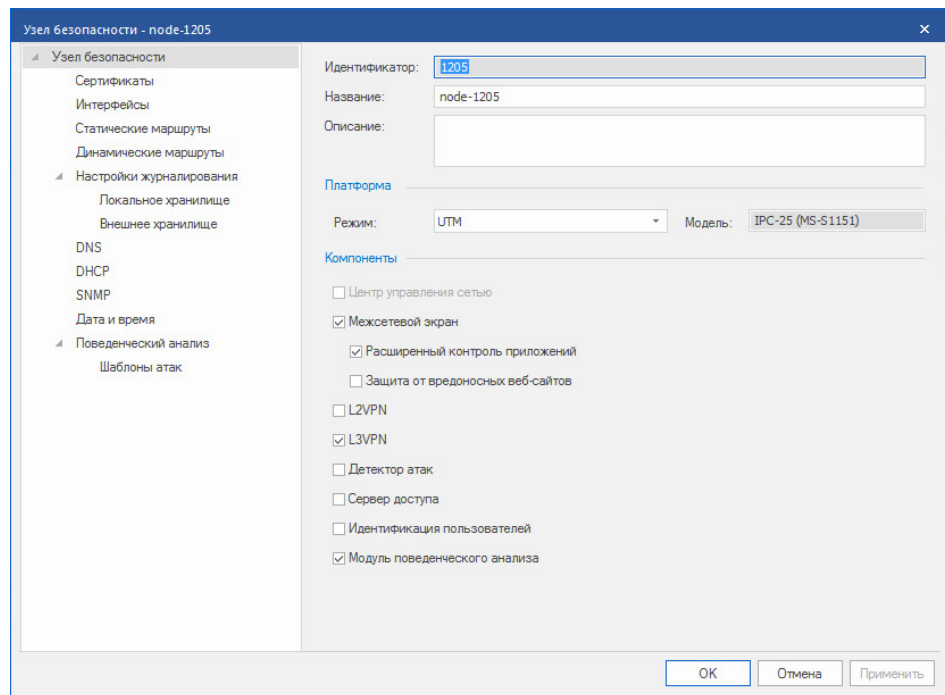
Файл сертификата управления УБ, запрос на него и ключевой контейнер создадутся и экспортируются на внешний носитель, после чего данные сертификата отобразятся в списке на экране.



## Создание УБ и экспорт его конфигурации

**Для создания УБ и экспорта конфигурационного файла в Менеджере конфигурации:**

**Внимание!** Перед созданием УБ в структуре МК убедитесь в наличии сетевого доступа от ЦУС до УБ.

- Откройте МК и перейдите в раздел "Структура".
- Нажмите кнопку "Узел безопасности" на панели инструментов.  
На экране появится окно "Узел безопасности".



- Выберите в левой части окна в разделе "Узел безопасности" пункт "Сертификаты".  
На экране появится список установленных сертификатов.
- В области серверных сертификатов нажмите кнопку добавления нового сертификата .
- На экране появится окно "Сертификаты".
- Выберите в списке сертификат управления, созданный в ходе предыдущей процедуры.  
Сертификат узла безопасности отобразится в списке на экране.
- В области корневых сертификатов нажмите кнопку добавления нового сертификата .
- На экране появится окно "Сертификаты".
- Выберите в списке корневой сертификат (см. стр. 11) и нажмите кнопку "ОК".

**Примечание.** Для обновления ПО в комплексе предустановлен сертификат "Доверенный издатель КБ". Для использования в других целях он не предназначен.

Корневой сертификат отобразится в списке на экране.

- Нажмите кнопку "ОК".

Созданный узел безопасности отобразится в списке на экране.

9. Вставьте внешний носитель в USB-разъем для записи на него конфигурационного файла.
10. Выберите в списке созданный УБ и на панели инструментов МК нажмите кнопку "Экспортировать".  
Система выполнит автосохранение конфигурации ЦУС и на экране появится стандартное окно для сохранения файла.
11. Укажите нужный путь и имя файла, затем нажмите кнопку "Сохранить".

**Примечание.** По умолчанию имя конфигурационного файла, предлагаемого системой для записи на внешний носитель, имеет вид `gate_XX.json`, где `XX` — серийный номер УБ.

Будет создан конфигурационный файл УБ. Дождитесь сообщения об успешном завершении процесса записи.

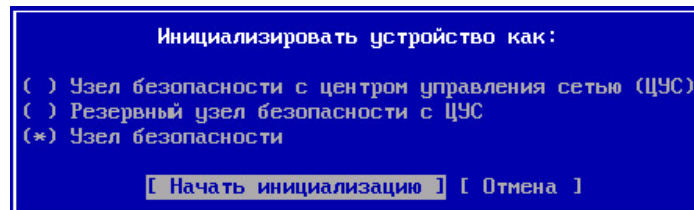
## Инициализация узла безопасности

**Примечание.** В целях безопасности рекомендуется сменить пароль на вход в меню настройки BIOS (см. стр. 39).

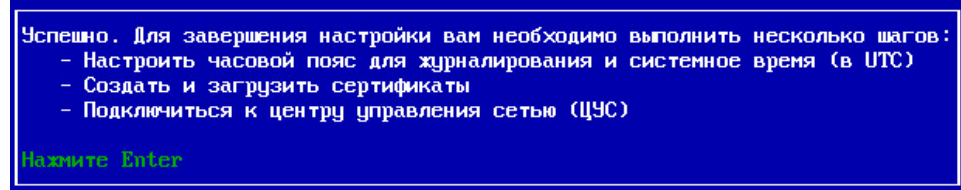
### Для инициализации УБ:

1. Осуществите вход в главное меню локального управления УБ (см. стр. 8), выберите пункт "Инициализация" и нажмите клавишу <Enter>.

На экране появится окно выбора инициализируемого компонента.



2. Выберите "Узел безопасности" и нажмите клавишу <Enter>.  
На экране появится запрос на очистку локальных журналов.
3. Выберите "Да" в окне запроса и нажмите клавишу <Enter>.  
Начнется инициализация УБ. Дождитесь сообщения об успешном завершении процесса.



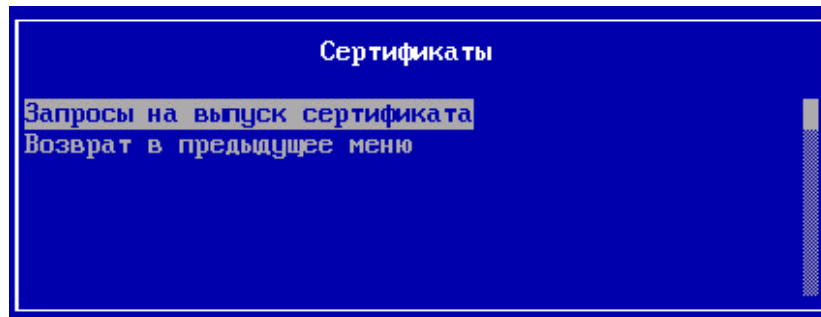
4. Нажмите клавишу <Enter>.  
Выполнится возврат в главное меню локального управления.

### Для импорта контейнера закрытого ключа УБ:

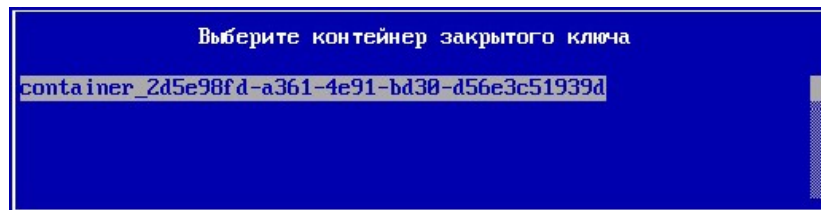
1. В главном меню выберите пункт "Сертификаты" и нажмите клавишу <Enter>.

На экране появится меню "Сертификаты".





2. Выберите пункт "Запросы на выпуск сертификата" и нажмите клавишу <Enter>. На экране появится окно "Запросы на выпуск сертификата".
3. Вставьте внешний носитель в USB-разъем и нажмите клавишу <F5> для импорта запроса на сертификат. На экране появится окно выбора файла запроса.
4. Выберите нужный файл с расширением .req и нажмите клавишу <Enter>. На экране появится окно выбора контейнера закрытого ключа.



5. Выберите нужный контейнер и нажмите клавишу <Enter>. На экране появится окно ввода пароля.
6. Введите пароль и нажмите клавишу <Enter>. Выполнится импорт файла запроса сертификата и ключевой информации, после чего на экране появится сообщение об успешном завершении операции.
7. Нажмите клавишу <Esc> для возврата в меню "Запросы на выпуск сертификата".

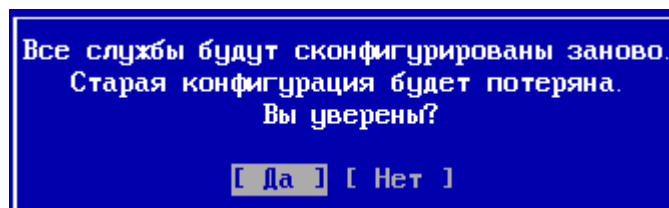
## Настройка узла безопасности

### Для настройки УБ и подключения к ЦУС:

Перед началом процедуры подготовьте внешний носитель с конфигурационным файлом gate-XX.json, где XX — серийный номер УБ.

1. Настройте системное время (см. стр. 23).
2. Вставьте внешний носитель с конфигурационным файлом и файлами сертификата в свободный порт USB.
3. В главном меню локального управления УБ выберите пункт "Подключиться к ЦУС" и нажмите клавишу <Enter>.

На экране появится предупреждение.



4. Выберите "Да" и нажмите клавишу <Enter>.

На экране появится окно со списком файлов, обнаруженных на внешнем носителе.

5. Выберите требуемый файл конфигурации с расширением .json и нажмите клавишу <Enter>.

На экране появится окно выбора интерфейса управления УБ со списком интерфейсов данного узла.

6. Выберите интерфейс, используемый для подключения к ЦУС, и нажмите клавишу <Enter>.

На экране появится окно настройки интерфейса управления УБ.

7. Введите его IP-адрес с маской, а также IP-адрес шлюза (если необходимо) и нажмите клавишу <Enter>.

На экране появится информационное окно о применении настроек.

8. Выберите "Да" и нажмите клавишу <Enter>.

Начнется настройка УБ, после чего на экране появится сообщение об успешном завершении операции.

9. Нажмите клавишу <Enter>.

## Установка конфигурации УБ в ЦУС

**Примечание.** Если в МК появилось информационное окно о перехвате управления из-за локального управления ЦУС, то установите соединение с ЦУС заново. Подробная информация о смене варианта управления ЦУС приведена в [1].

### Для установки конфигурации УБ:

1. Откройте МК и перейдите в раздел "Структура".

В правой части окна отобразится список УБ комплекса.

**Примечание.** Если в списке у подключаемого УБ не указана локальная версия конфигурации, нажмите кнопку "Обновить" на панели инструментов.

2. Выберите в списке подключаемый УБ и нажмите кнопку "Подтвердить изменения" на панели инструментов.

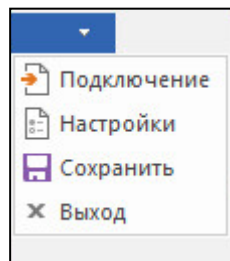
Появится окно с запросом о подтверждении локальных изменений конфигурации УБ.

3. Нажмите кнопку "Да".

Система внесет изменения в конфигурацию ЦУС, сохранит ее в БД, после чего появится окно с сообщением об успешном завершении операции.

4. Нажмите кнопку "ОК".

5. Для сохранения выполненных настроек в автозагружаемую конфигурацию в окне Менеджера конфигурации в левом верхнем углу нажмите на раскрывающийся список и выберите пункт "Сохранить".

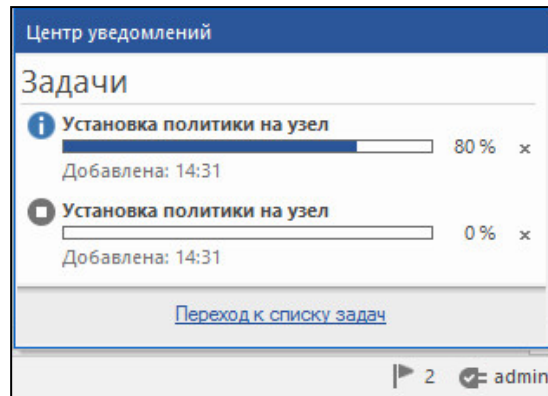


6. Нажмите кнопку "Установить" на панели инструментов.

Откроется окно для установки политик узлам комплекса.

7. В окне установки политики выберите УБ, поставив отметку слева от названия. Далее нажмите кнопку "ОК".

Сформируется задача по установке политики на выбранный узел, после чего на экране отобразится центр уведомлений, на котором можно в реальном времени наблюдать степень выполнения поставленных задач.



## Глава 6

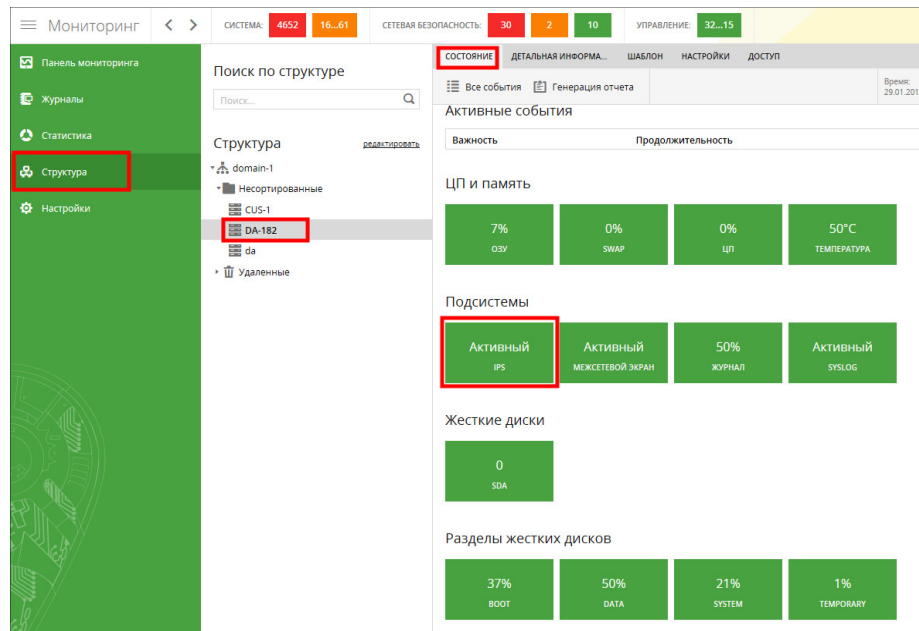
# Старт комплекса и процедура проверки его работоспособности

## Проверка корректности старта

### Для проверки корректности старта комплекса:

1. Включите питание платформы. Дождитесь окончания загрузки.
2. Запустите Менеджер конфигурации (см. стр. 18).
3. Подключитесь к ЦУС (см. стр. 19).
4. Перейдите в раздел "Структура" и в панели инструментов нажмите кнопку "Мониторинг".
5. Введите имя и пароль администратора и нажмите кнопку "ОК".
6. Перейдите в раздел "Структура".
7. В дереве объектов выберите проверяемый узел.

В рабочей области отобразятся сведения о состоянии выбранного узла.



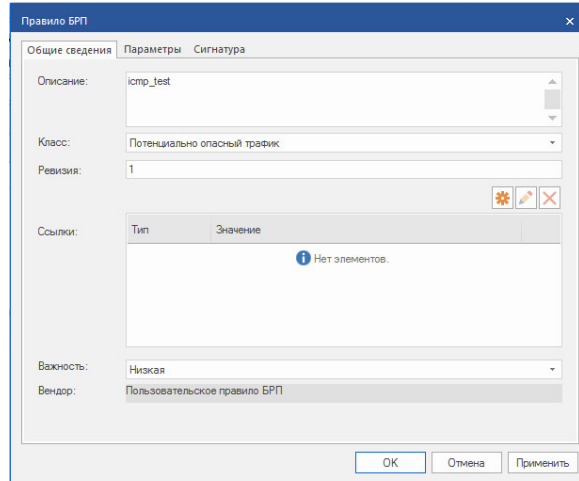
Старт комплекса корректен, если на вкладке "Состояние" подсистема "IPS" имеет статус "Активный".

## Проверка работоспособности

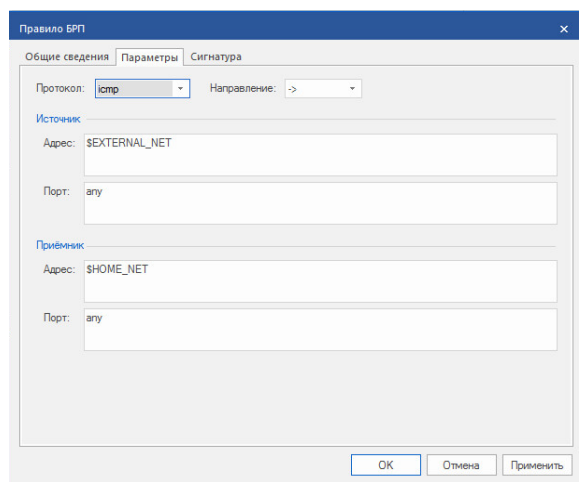
Для проверки работоспособности комплекса необходимо использовать две рабочие станции, между которыми передается трафик. Содержимое трафика проверяется COA. Отправка трафика должна осуществляться с рабочей станции с установленной операционной системой семейства Linux. Для проверки используется утилита hping3.

### Для проверки работоспособности:

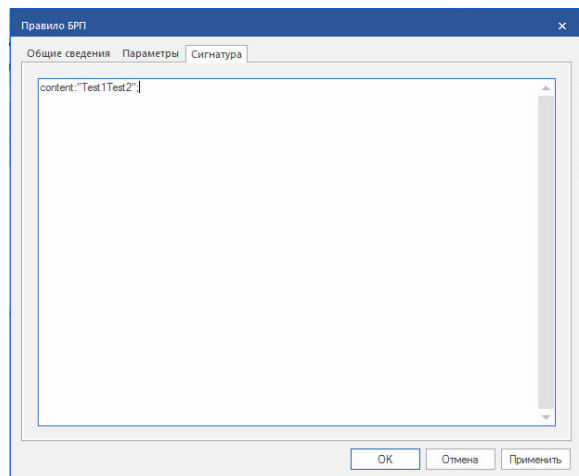
1. Запустите Менеджер конфигурации (см. стр. 18).
2. Подключитесь к ЦУС (см. стр. 19).
3. В панели навигации перейдите в подраздел "Система обнаружения вторжений | База решающих правил | Пользовательские правила".
4. Создайте новое пользовательское правило БРП.







5. На вкладке "Параметры" укажите протокол icmр и его направление. Введите адреса источника и получателя трафика.



6. На вкладке "Сигнатура" укажите строку для поиска в пакете (например "Test1Test2").



7. Нажмите кнопку "ОК".  
Новое правило отобразится в списке правил.
8. Выделите правило.
9. Нажмите кнопку  **Оповещать**, чтобы установить соответствующее действие.

Профили COB		
Оптимальный н...	Полный набор	Рекомендованн...
 Оповещать	 Оповещать	 Оповещать

10. Перейдите в раздел "Структура". Установите политику на ДА (см. стр. 34).

11. На рабочей станции, осуществляющей отправку трафика, запустите утилиту hping3 с параметрами:

```
hping3 -1 XXX.XXX.XXX.XXX -e Text
```

где:

Параметр	Описание
<b>-1</b>	Режим icmp
<b>XXX.XXX.XXX.XXX</b>	IP-адрес рабочей станции-получателя
<b>-e</b>	Параметр, добавляющий текстовую последовательность
<b>Text</b>	Последовательность, которая будет искаться в пакете

Пример запуска:

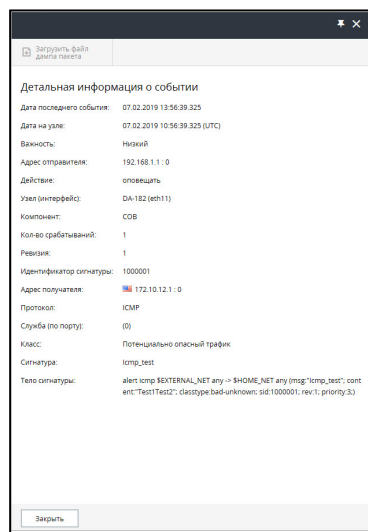
```
hping3 -1 172.10.12.1 -e Test1Test2
```

12. Перейдите в МК.

13. Перейдите в раздел "Структура" и в панели инструментов нажмите кнопку "Мониторинг".

14. Перейдите в раздел "Журналы" на вкладку "Сетевая безопасность".

При успешном обнаружении в пакете заданной текстовой последовательности в списке событий отобразится запись о тестовом событии.



# Приложение

## Подключение к УБ через последовательный порт

**Внимание!** Комплекс допускает подключение через последовательный порт только к меню локального управления.

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

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

**Внимание!** Последовательный порт может быть отключен в BIOS платформы. Включить Serial порт можно зайдя в BIOS устройства (обычно надо изменить значения параметров Serial Port и Serial Port Console Redirection на Enabled во вкладке Advanced).

Вставьте один конец кабеля в 9-контактный разъем последовательного порта на ноутбуке, другой конец кабеля вставьте в разъем последовательного порта RJ-45, расположенный на фронтальной панели сетевого устройства.

На ноутбуке запустите программу эмуляции терминала и в ее настройках укажите следующие значения параметров:

Параметр	Значение
Порт	Укажите значение, определяемое автоматически в диспетчере устройств ноутбука
Скорость	115200
Тип подключения	serial
Количество бит в информационном пакете	8
Без проверки бита на четность	да
Количество стоп-битов	1
Тип кодировки	UTF-8
Функциональные клавиши и клавиатура	Linux

Подключитесь к последовательному порту с выбранными параметрами. Если локальное меню не отобразилось, нажмите клавишу <Esc>, а затем <Enter>.

**Внимание!** При подключении к последовательному порту во время включения или перезагрузки платформы может возникать проблема с некорректным отображением кириллицы.

Предустановленный на платформе программно-аппаратный комплекс "Соболь" некорректно отображает русский язык в консольном меню. Для избежания возникновения проблемы необходимо предварительно локально настроить в ПАК "Соболь" параметры входа.

Параметр "Время ожидания автоматического входа в систему" не должен быть равен нулю. Данный параметр отвечает за интервал, через который начинается загрузка операционной системы. Значение "0" означает, что автоматическая загрузка операционной системы отключена. По умолчанию значение данного параметра равно 5 секундам.

При подключении через последовательный порт необходимо входить в меню ПАК "Соболь" в пользовательском режиме (не прислоняя идентификатор к считывателю), загрузка ОС начнется автоматически по истечении времени ожидания автоматического входа в систему.

Если вход в меню ПАК "Соболь" будет осуществлен в пользовательском режиме, но параметр "Время ожидания автоматического входа в систему" будет иметь значение "0", то автоматическая загрузка ОС не начнется. Необходимо приложить

идентификатор к считывателю. По окончании анимации тестирования датчика случайных чисел загрузится некорректно отображающаяся ПАК "Соболь" информация об идентификаторе. Нужно нажать клавишу <Enter>, а после смены изображения на экране нажать клавишу <Enter> еще раз для начала загрузки операционной системы.

В случае если вход в меню ПАК "Соболь" был осуществлен в административном режиме (с прислоненным к считывателю идентификатором), то автоматическая загрузка ОС не начнется. В этом случае требуется нажать клавишу <Enter>, а после смены изображения на экране нажать клавишу <Enter> еще раз для начала загрузки операционной системы.

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

#### **Для управления подключениями в главном меню локального управления УБ:**

1. В главном меню локального управления УБ выберите пункт "Настройки" и нажмите клавишу <Enter>.

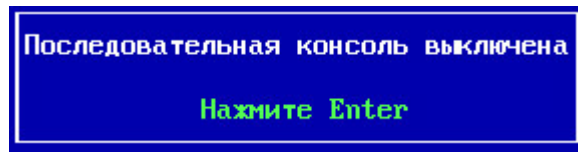
На экране появится окно "Меню настроек".

2. Выберите пункт "Последовательная консоль" и нажмите клавишу <Enter>.

На экране появится окно "Настройки последовательной консоли".

3. Для запрета подключения через консольный порт выберите пункт "Выключить последовательную консоль" и нажмите клавишу <Enter>.

На экране появится сообщение о выключении последовательной консоли.

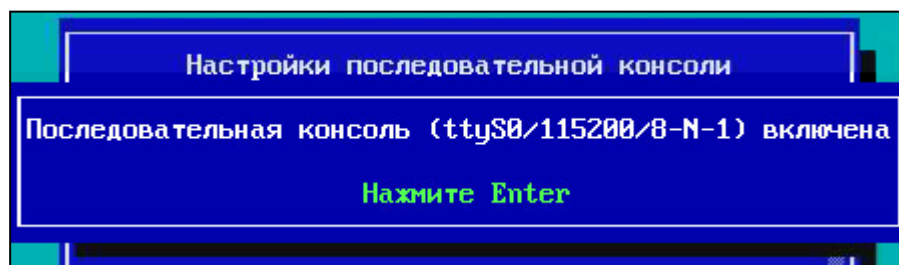


4. Нажмите клавишу <Enter>.

Наименование пункта в меню настроек последовательной консоли будет изменено на противоположное.

5. Для разрешения подключения через консольный порт выберите пункт "Включить последовательную консоль" и нажмите клавишу <Enter>.

На экране появится сообщение о включении последовательной консоли, содержащее информацию о рекомендуемой скорости передачи и количестве бит в информационном пакете.



6. Нажмите клавишу <Enter>.

Наименование пункта в меню настроек последовательной консоли будет изменено на противоположное.

#### **Для управления подключениями в меню настройки BIOS:**

**Примечание.** Для перемещения между вкладками и пунктами меню настройки BIOS используйте управляющие клавиши клавиатуры, для выбора пункта или смены его состояния — клавишу <Enter>.

1. Включите питание УБ и войдите в меню установки BIOS.



**Примечание.** Как правило, для входа в меню используется клавиша <Del>, на некоторых платформах — <F1>, <F2>.

На экране появится окно запроса пароля.

2. Введите текущий пароль для входа в меню установки BIOS (по умолчанию — 123456) и нажмите клавишу <Enter>.

На экране появится меню установки BIOS. Вид и содержание меню зависит от типа платформы УБ и установленной на ней версии BIOS. Описание далее приведено для BIOS version LN010AISC.003. Меню других версий BIOS может иметь незначительные отличия.

3. Перейдите на вкладку расширенных настроек (Advanced), выберите пункт управления консольным портом (Serial Port Console Redirection).
4. Для разрешения подключения через консольный порт параметр "Console Redirection" должен быть в состоянии "Enable".
5. Для запрета подключения через консольный порт параметр "Console Redirection" должен быть в состоянии "Disable".
6. Для просмотра параметров подключения через консольный порт выберите пункт "Console Redirection Settings".

**Примечание.** Не рекомендуется вносить изменения в параметры подключения через консольный порт.

7. Закройте меню настройки BIOS с сохранением внесенных изменений.  
Узел безопасности перезагрузится.

## Смена пароля для входа в меню установки BIOS

### Для смены пароля:

1. Подключите к УБ клавиатуру и монитор.
2. Включите питание УБ и войдите в меню установки BIOS.

**Примечание.** Как правило, для входа в меню используется клавиша <Del>, на некоторых платформах — <F1>, <F2>.

На экране появится окно запроса пароля.

3. Введите текущий пароль для входа в меню установки BIOS (по умолчанию — 123456) и нажмите клавишу <Enter>.

На экране появится меню установки BIOS. Вид и содержание меню зависит от типа платформы сетевого устройства.

4. Перейдите на вкладку смены пароля (обычно — "Security"), выберите пункт пароля администратора и нажмите клавишу <Enter>.

На экране появится окно запроса текущего пароля.

5. Введите текущий пароль для входа в меню установки BIOS и нажмите клавишу <Enter>.

На экране появится окно запроса нового пароля.

6. Введите новый пароль для входа в меню установки BIOS и нажмите клавишу <Enter>.

На экране появится окно подтверждения нового пароля.

7. Введите новый пароль для входа в меню установки BIOS и нажмите клавишу <Enter>.

8. Закройте меню настройки BIOS с сохранением внесенных изменений.  
Узел безопасности перезагрузится.

## Смена кода загрузчика

### Для смены кода загрузчика:

1. В главном меню УБ выберите пункт "Настройки" и нажмите клавишу <Enter>.
1. Осуществите вход в главное меню локального управления УБ (см. стр. 8), выберите пункт "Настройки" и нажмите клавишу <Enter>. На экране появится окно "Меню настроек".
2. Выберите пункт "Настройки загрузчика" и нажмите клавишу <Enter>. На экране появится окно для ввода текущего кода загрузчика.
3. Введите код загрузчика (по умолчанию — Boot-4.Y) и нажмите клавишу <Enter>. На экране появится окно для ввода нового кода загрузчика.
4. Введите дважды новый код загрузчика и нажмите клавишу <Enter>. Будет выполнено обновление БД УБ и на экране появится информационное окно об успешном завершении операции.
5. Нажмите клавишу <Enter> для возврата в меню настроек.

## Обозначение сетевых интерфейсов

Обозначения сетевых интерфейсов в комплексе имеют следующий вид:

**<пропускная способность>-<шина>-<адаптер>**

где

- **<пропускная способность>** — буквенный префикс, показывающий максимальную пропускную способность этого адаптера в соответствии с таблицей ниже:

Префикс	Пропускная способность
ge	1 Гбит/с
te	10 Гбит/с
qe	40 Гбит/с

- **<шина>** — адрес устройства на материнской плате аппаратной платформы (0, 1, 2...);
- **<адаптер>** — номер адаптера в модуле (0–3), если модуль содержит несколько адаптеров.

**Примеры:**

te-0-0

qe-1-1

## Документация

1. Программный комплекс "Континент-СОА". Версия 4. Руководство администратора. Обнаружение вторжений.
2. Программный комплекс "Континент-СОА". Версия 4. Руководство администратора. Мониторинг и аудит.