КОД БЕЗОПАСНОСТИ

Программный комплекс

Континент-СОВ
Версия 4

Руководство администратора

Ввод в эксплуатацию

RU.АМБС.58.29.12.002 90 1

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

IP	Internet Protocol
MMC	Microsoft Management Console
USB	Universal Serial Bus
РМ	Рабочее место
БРП	База решающих правил
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
СКЗИ	Средство криптографической защиты информации
СОВ	Система обнаружения вторжений (компьютерных атак)
УБ	Узел безопасности
ЦУС	Центр управления сетью

Введение

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

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

Служба технической поддержки. Связаться со службой технической поддержки можно по телефону 8-495-982-30-20 или по электронной почте support@securitycode.ru . Страница службы технической поддержки на сайте компании: https://www.securitycode.ru/services/tech-support/.

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

Порядок ввода комплекса в эксплуатацию

Ввод комплекса в эксплуатацию состоит из следующих этапов:

1. Развертывание центра управления сетью и регистрация главного администратора (см. стр. **8**).
2. Развертывание рабочего места главного администратора (см. стр. **15**).
3. Развертывание узла безопасности (см. стр. **26**).
4. Регистрация нового узла безопасности на ЦУС (см. стр. **33**).
5. Формирование и применение политики к узлам безопасности (см. стр. **38**).

Подготовительные работы

Для подготовки к вводу комплекса в эксплуатацию необходимо выполнить следующее:

1. Подготовить согласно паспорту аппаратные платформы для установки и настройки программного обеспечения ЦУС и узлов безопасности.
2. Подготовить USB-флеш-накопитель для передачи служебных файлов между компонентами комплекса.
3. Подготовить рабочее место администратора.

Развертывание Центра управления сетью и регистрация главного администратора

Развертывание ЦУС выполняют в следующей последовательности:

1. Инициализация ЦУС (см. стр. **8**).
2. Настройка системного времени (см. стр. **9**).
3. Создание корневого сертификата, сертификатов администратора и управления ЦУС (см. стр. **10**).
4. Настройка ЦУС и применение локальной политики (см. стр. **12**).

Инициализация Центра управления сетью

Инициализацию ЦУС выполняют на устройстве после установки операционной системы.

Если устройство после установки операционной системы было выключено, включите его и после загрузки ОС дождитесь появления на экране главного меню.

Для инициализации ЦУС:

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

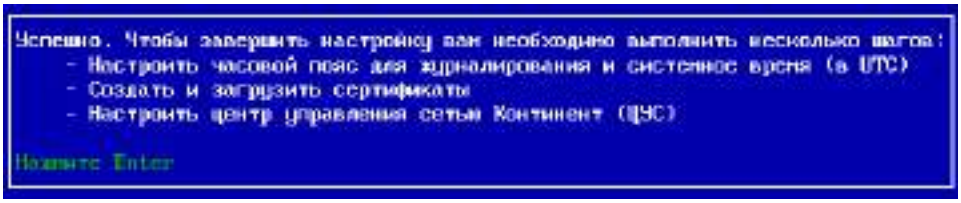
   На экране появится запрос на продолжение процедуры.
2. Выберите "Да" в окне запроса и нажмите клавишу <Enter>.

   На экране появится окно выбора инициализируемого компонента.
3. Выберите "Центр управления сетью Континент (ЦУС)" и нажмите клавишу <Enter>.

   На экране появится запрос на очистку локальных журналов.
4. При необходимости выберите "Да" в окне запроса и нажмите клавишу <Enter>.

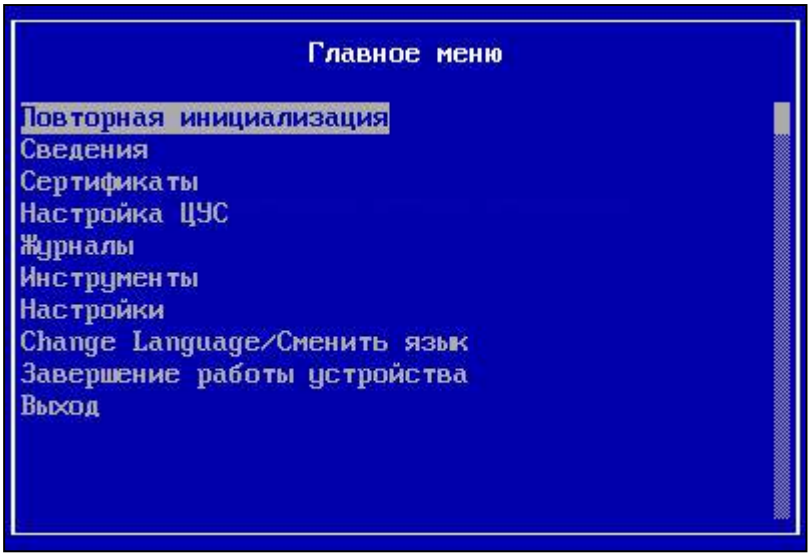
   Начнется сжатие базы данных, после чего будет выполнена инициализация служб контроллера домена.

   Дождитесь сообщения об успешном завершении инициализации.



5. Нажмите клавишу <Enter>.

   Будет выполнен 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.

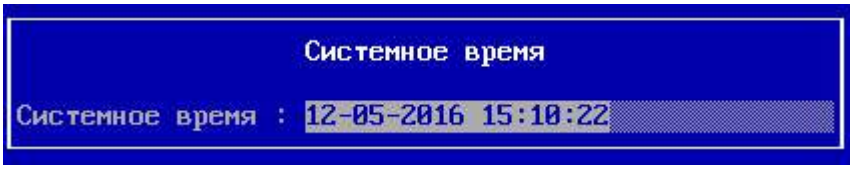
Для настройки системного времени ЦУС:

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".

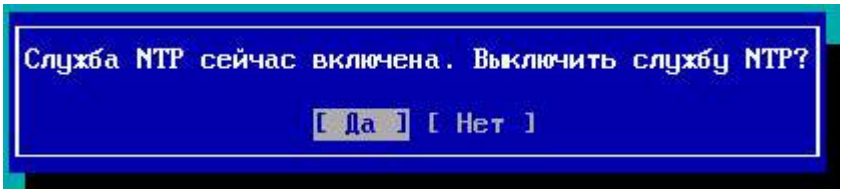


4. Введите текущее время по Гринвичу по предлагаемому шаблону и нажмите клавишу <Enter>.

   Пример. Для Москвы системное время нужно выставить на три часа меньше, чем текущее московское.

   Будет выполнено изменение времени на узле с соответствующим оповещением на экране.
5. Нажмите клавишу <Enter>.

   На экране появится запрос по состоянию службы NTP.



6. Если планируется использовать ЦУС в качестве сервера NTP, выберите пункт "Нет".
7. Нажмите клавишу <Enter>, а затем выберите пункт "Изменить временную зону для дат событий журнала" и нажмите клавишу <Enter>.

   На экране появится окно "Выбор временной зоны".

8. Выберите нужную временную зону и нажмите клавишу <Enter>.

   Будет выполнено изменение часового пояса и возврат в меню настройки времени.

Создание сертификатов

На ЦУС возможно создание следующих сертификатов:

Наименование сертификата	Срок службы	Примечание
Сертификат удостоверяющего центра (УЦ)	5 лет	Он же корневой сертификат
Сертификат управления ЦУС	1 год	
Сертификат узла безопасности	1 год	
Сертификат администратора	1 год	
Сертификат безопасности веб-сервера мониторинга (RSA)	1 год	Доступно после настройки ЦУС только посредством локального управления
Корневой сертификат веб-сервера мониторинга (RSA)	5 лет	

На этапе развертывания ЦУС должны быть созданы корневой сертификат и сертификат управления ЦУС.

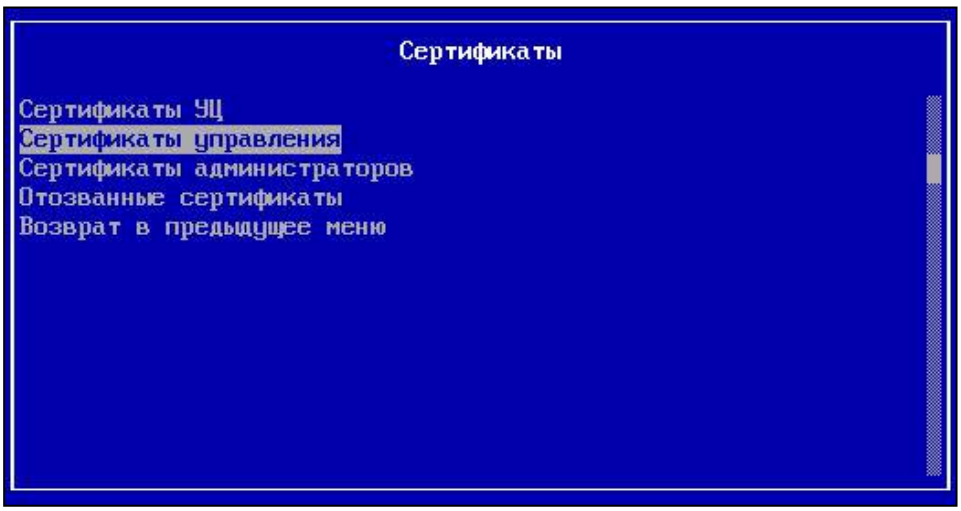
Примечание. После инициализации и настройки ЦУС сертификаты можно будет создавать в Менеджере конфигурации (см. стр. 28).

Для создания сертификатов средствами локального управления используют меню "Сертификаты".

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 обновления ПО в комплексе предустановлены сертификаты "Доверенный издатель КБ" и "Издатель САО КБ Класс 1". Для использования в других целях они не предназначены.

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" и "Название" и нажмите клавишу <Enter>.

   Примечание. Для перемещения по форме используйте стандартные клавиши: <↑>, <↓>, <Page Down>, <Page Up>, <Home>.

   На экране появится сообщение: "Успешно".

5. Нажмите клавишу <Enter>.

   Будет выполнен возврат в окно "Выпуск сертификата".

6. Нажмите клавишу <Esc>.

   Будет выполнен возврат в окно "Сертификаты УЦ". В окне отобразится созданный корневой сертификат.

7. Нажмите клавишу <Esc>.

   Будет выполнен возврат в меню "Сертификаты".

Для создания сертификата управления:

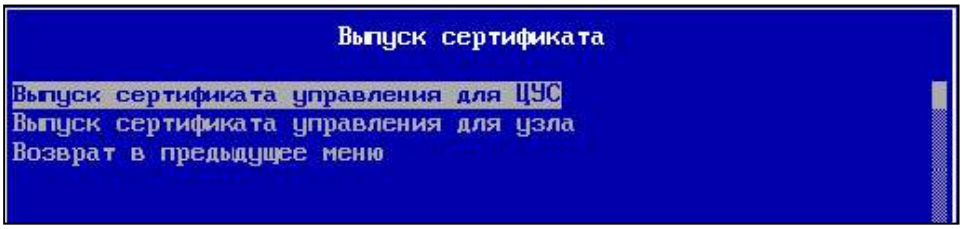
1. Выберите в меню "Сертификаты" пункт "Сертификаты управления" и нажмите клавишу <Enter>.

   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" и "Название" и нажмите клавишу <Enter>.

   На экране появится список созданных корневых сертификатов.

5. Выберите корневой сертификат и нажмите клавишу <Enter>.

На экране появится сообщение: "Успешно".

6. Нажмите клавишу <Enter>.

   Будет выполнен возврат в окно "Выпуск сертификата".

7. Нажмите клавишу <Esc>.

   Будет выполнен возврат в окно "Сертификаты управления". В окне отобразится созданный сертификат управления ЦУС.

8. Нажмите клавишу <Esc>.

   Будет выполнен возврат в меню "Сертификаты".

Для создания сертификата администратора:

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

   На экране появится окно "Сертификаты администраторов".

2. Нажмите клавишу <F2>.

   На экране появится меню "Выпуск сертификата".

3. Выберите пункт "Выпуск сертификата администратора" и нажмите клавишу <Enter>.

   На экране появится окно с вопросом "Есть ли запрос для создания сертификата?".

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

   На экране появится окно с приглашением вставить USB-флеш-накопитель (если не был подключен ранее).

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

   На экране появится окно "Атрибуты идентификации".

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

   На экране появится запрос на ввод пароля к ключевому контейнеру.

7. Введите пароль и нажмите клавишу <Enter>.

   На экране появится окно для ввода названия ключевого контейнера.

8. Введите название контейнера и нажмите клавишу <Enter>.

   Появится сообщение об успешной записи запроса на носитель.

9. Нажмите клавишу <Enter>.

   Появится список созданных корневых сертификатов.

10. Выберите корневой сертификат и нажмите клавишу <Enter>.

    Появится окно с сообщением "Цепочка сертификатов записана на носитель".

11. Нажмите клавишу <Enter>.

    Будет выполнен возврат в окно "Выпуск сертификата".

12. Нажмите клавишу <Esc>.

    Будет выполнен возврат в окно "Сертификаты администраторов". В окне отобразится созданный сертификат администратора.

13. Нажмите клавишу <Esc>.

    Будет выполнен возврат в меню "Сертификаты".

14. Для возврата в главное меню локального управления нажмите клавишу <Esc>.

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 для сервера управления.

3. Выберите в списке сертификат ЦУС, созданный в соответствии с описанием в разделе "Создание сертификатов", и нажмите клавишу <Enter>.

   На экране появится окно задания пароля главного администратора.

4. Задайте пароль главного администратора и нажмите клавишу <Enter>.

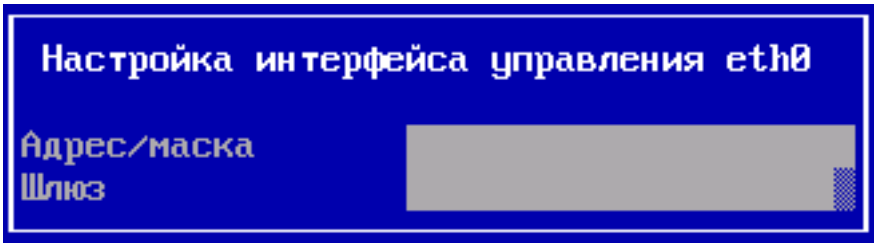
   Примечание. Пароль должен содержать не менее 8 символов, как минимум один из которых должен быть латинской буквой в нижнем регистре. Кириллица в обоих регистрах и латиница в верхнем регистре запрещены. Остальные символы могут быть также цифрами или следующими спецсимволами:

!	@	#	$	%	^	&	*	(	)	_	-	+	;	:	.	,

   Начнется создание узла сети, предустановленных профилей СОВ, а затем на экране появится окно для выбора интерфейса управления.

5. Выберите интерфейс управления, подключенный к РМ администратора, и нажмите клавишу <Enter>.

   На экране появится окно настройки интерфейса управления.



6. Введите адрес с маской и шлюз и нажмите клавишу <Enter>.

   На экране появится запрос на применение указанных настроек.

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

   Начнется последовательное выполнение следующих процессов:

   - инициализация службы сервера домена безопасности;
   - инициализация службы агента управления;
   - применение начальной конфигурации;
   - инициализация служб мониторинга;
   - применение локальных изменений.

   После завершения перечисленных процессов на экране появится журнал инициализации с подробным описанием успешной (неуспешной)инициализации системы.

Примечание. В случае сбоя при настройке ЦУС — выполните команду повторной инициализации в меню "Инструменты", перезагрузите ЦУС и заново проведите процедуры настройки времени и создания сертификатов.

8. Для выхода из журнала нажмите клавишу <Esc>.

   Будет выполнен возврат в главное меню. При этом содержание главного меню изменится и будет содержать следующие пункты:

   - "Сведения";
   - "Вход в систему";
   - "Change Language/Сменить язык";
   - "Завершение работы устройства";
   - "Выход".

Примечание. При инициализации ЦУС создается демолицензия с нулевым ID клиента, которая позволяет использовать все возможности комплекса в ограниченный период времени — 14 дней. По завершении этого срока возможности эксплуатации комплекса будут ограничены. Для загрузки в базу ЦУС имеющихся лицензий см. [1], раздел "Управление лицензиями".

Развертывание и настройка рабочего места главного администратора

Развертывание рабочего места (РМ) главного администратора включает в себя последовательное выполнение двух этапов:

1. Установка на РМ администратора программы управления "Менеджер конфигурации" и подключение к ЦУС (см. ниже).
2. Запуск Менеджера конфигурации (см. стр. **23**).

Программа управления устанавливается на компьютеры, удовлетворяющие следующим системным требованиям:

Операционная система	• Windows Server 2008 R2 Standard; • Windows Server 2012 R2 Standard; • Windows 7 SP1 x64 Enterprise; • Windows 8.1 x64 Enterprise; • Windows 10 x64 Enterprise
Процессор	Pentium IV 2,6ГГц
Оперативная память	2 ГБ
Жесткий диск (свободное место)	20 ГБ (только NTFS,установка на FAT не поддерживается)
Порты (свободные)	• 1 x USB 2.0 — при использовании USB-флеш-накопителя; • 1 x слот PCI — для установки платы ПАК "Соболь"; • 1 x слот PCI-E — для установки платы ПАК "Соболь 3.0"
Сетевой адаптер	Ethernet (1шт.)
Установленное дополнительное ПО	• СКЗИ "Континент TLS VPN Клиент" 1.0.1063; • интернет-браузер следующего типа: ◦ MS Internet Explorer 11.0 и выше; ◦ Google Chrome 55 и выше; ◦ Mozilla Firefox 49.0.2 и выше

Установка Менеджера конфигурации и подключение к ЦУС

Внимание! Установку и удаление Менеджера конфигурации может выполнить только пользователь, наделенный правами локального администратора данного компьютера.

Установку Менеджера конфигурации осуществляют в следующем порядке:

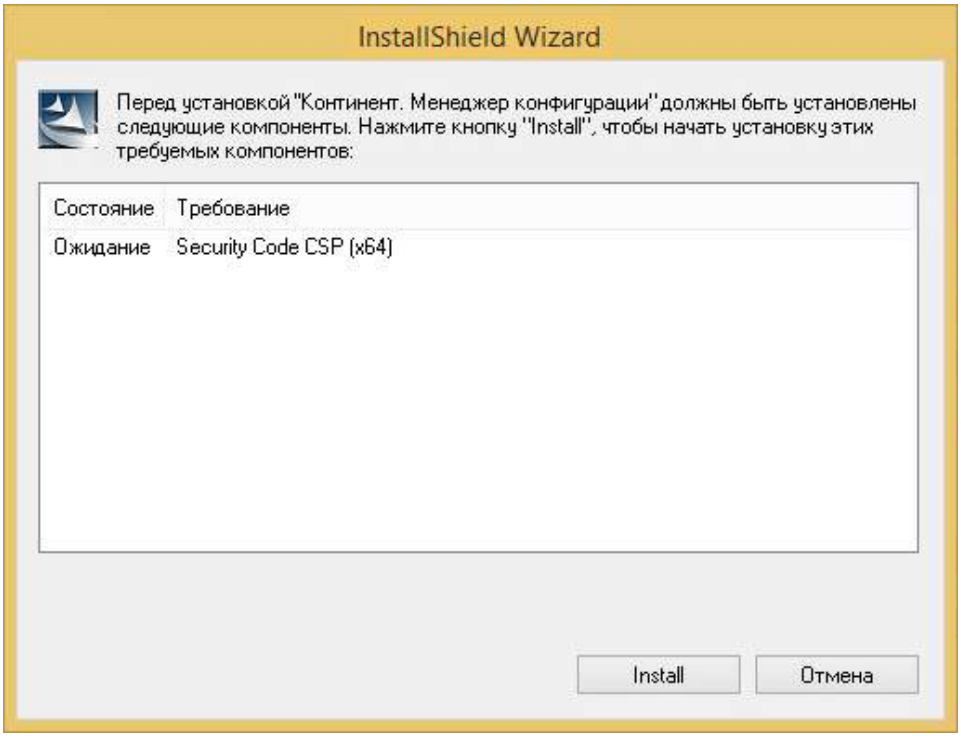
1. Запуск программы установки.
2. Выбор папки установки.
3. Проверка выбранных настроек.
4. Копирование файлов.
5. Завершение установки.

Перед запуском программы установки завершите работу всех приложений.

Шаг 1. Запуск программы установки

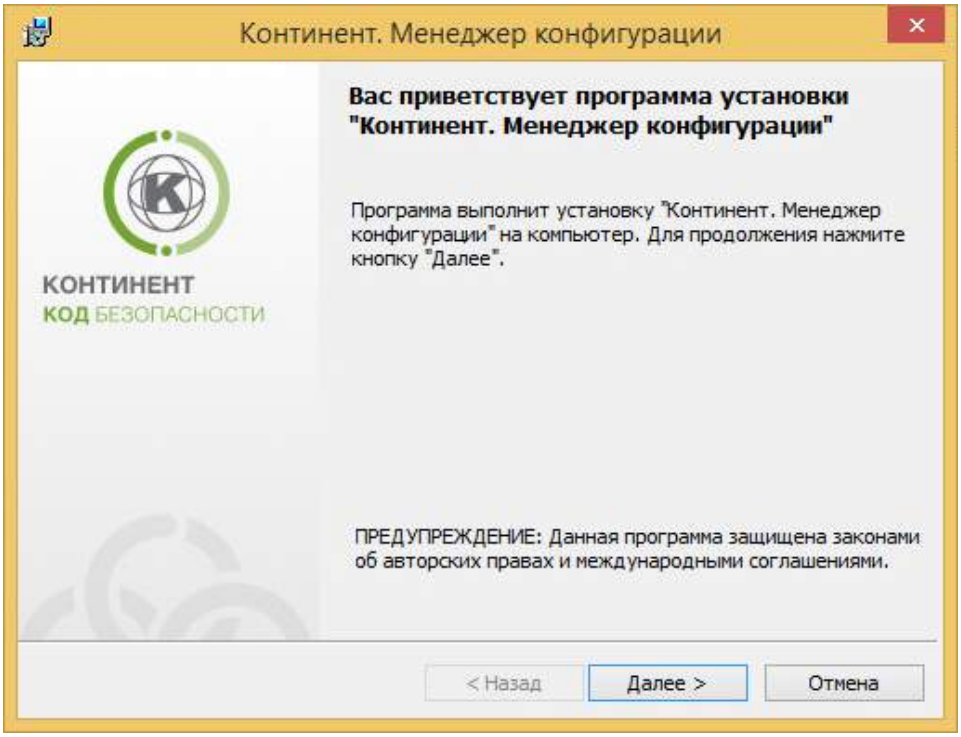
1. Поместите установочный диск в устройство чтения компакт-дисков.
2. Запустите на исполнение файл \Setup\Continent\MS\Rus\x64\Setup.exe.

   На экране появится диалог со списком дополнительных компонентов, которые должны быть установлены до начала установки подсистемы управления.



3. Нажмите кнопку "Install" или "Установить".

   После завершения установки дополнительных компонентов на экране появится стартовый диалог программы установки Менеджера конфигурации.



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

   Появится диалог с текстом лицензионного соглашения.

5. Изучите содержание лицензионного соглашения, прочитав его до конца.

   Если вы согласны с условиями лицензионного соглашения, подтвердите свое согласие, нажав кнопку "Далее >", и перейдите к следующему шагу установки.

Шаг 2. Выбор места установки

На этом шаге программа установки предложит выбрать папку установки для программных файлов.

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

1. При необходимости измените папку установки и нажмите кнопку "Далее >".

   Для выбора папки в стандартном диалоге используйте кнопку "Изменить".

   По умолчанию программа установки копирует файлы на системный диск в папку ..\Program Files\Security Code\Continent.
2. Для продолжения установки нажмите кнопку "Далее >".

Шаг 3. Проверка выбранных настроек

На этом шаге перед началом копирования файлов можно проверить и откорректировать выполненные настройки.

Для проверки и корректировки настроек используйте кнопку "< Назад".

Для начала установки программы нажмите кнопку "Установить". Программа установки приступит к копированию файлов на жесткий диск компьютера.

Шаг 4. Копирование файлов

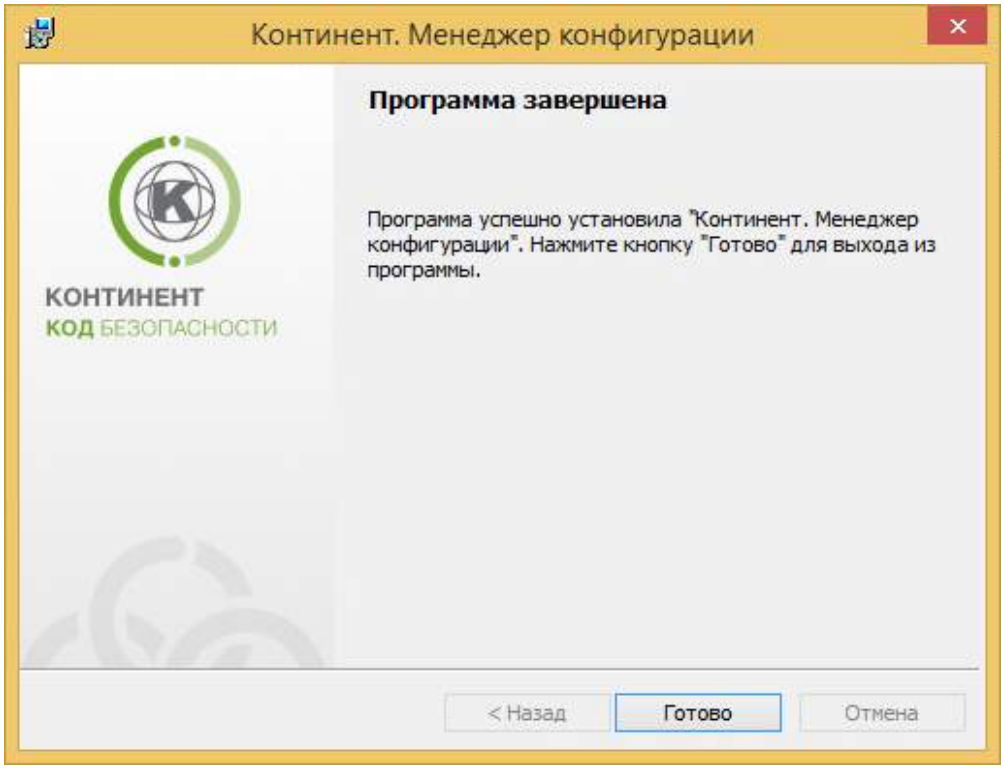
Файлы копируются в папку, выбранную для установки программы (см. шаг 2).

Ход выполнения процесса копирования отображается на экране в специальном окне.

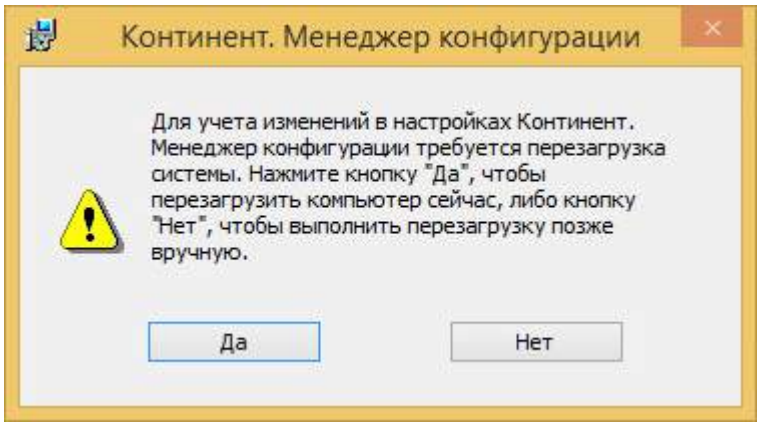
Примечание. Если программа установки в процессе копирования не обнаружит файл, заявленный в комплекте поставки, на экране появится предупреждающее сообщение с указанием имени отсутствующего файла. Скопируйте еще раз файлы с дистрибутивного диска и повторите установку. Если это не приведет к желаемому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

Шаг 5. Завершение установки

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



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



Перезагрузите компьютер.

После перезагрузки на рабочем столе появится ярлык Менеджера конфигурации, а в меню "Программы" главного меню Windows появится группа "Код Безопасности" с командами — "Код Безопасности CSP" и "Менеджер конфигурации".

Настройка мониторинга и аудита

Система мониторинга и аудита комплекса (далее — система) позволяет проводить мониторинг параметров узлов безопасности, входящих в состав комплекса, а также обеспечивает сбор данных по системным событиям и событиям СОВ для их последующего анализа и хранения. Подключение к системе происходит либо с помощью алгоритма ГОСТ Р 34.11-2012, либо с помощью алгоритма RSA (SHA-1). В первом случае необходимо наличие дополнительного ПО СКЗИ "Континент TLS VPN Клиент" 1.0.1063 (далее — TLS-клиент).

Для установки и настройки системы по ГОСТ Р 34.11-2012 необходимо произвести следующие действия:

1. Экспорт сертификатов безопасности (см. ниже).
2. Установка списка отозванных сертификатов (CRL).
3. Установка TLS-клиента и его настройка в соответствии с Руководством по эксплуатации RU.88338853.501430.011 91.

   Внимание! При создании нового подключения в конфигураторе TLS-клиента назовите его по имени сертификата сервера, используемого при настройке ЦУС (далее — "адресмониторинга"), и очистите поле адреса загрузки CRL-сертификата (на шаге 4).

4. Настройка конфигурационного файла Менеджера конфигурации (см. стр. **20**).
5. Запуск системы мониторинга и аудита (см. стр. **21**).

Примечание. При неполадках в подключении TLS-клиента настройте на ЦУС дополнительный сетевой интерфейс и замените адрес получения CRL в настройках профиля соединений TLS-клиента на IP-адрес этого сетевого интерфейса. Например: http://192.168.80.70/cdc.crl

Для установки и настройки системы с помощью алгоритма RSA необходимо произвести следующие действия:

1. Выпуск сертификатов веб-сервера мониторинга (см. стр. **20**).
2. Запуск системы мониторинга и аудита (см. стр. **21**).

Внимание! Подключение с помощью алгоритма RSA не защищено от возможности работы в системе мониторинга стороннего пользователя с правами доступа к РМ по протоколу RDP.

Для подключения системы мониторинга и аудита к Менеджеру конфигурации с помощью алгоритма ГОСТ Р 34.11-2012:

1. Откройте Менеджер конфигурации и перейдите в раздел "Администрирование".
2. В списке сертификатов выберите "Корневые центры сертификации".

   В правой части экрана появится список установленных корневых сертификатов.
3. Выберите действующий корневой сертификат и нажмите кнопку "Свойства" на панели инструментов.

   На экране появится окно "Сертификат".
4. Перейдите на закладку "Состав" и нажмите кнопку "Копировать в файл..." внизу окна.

   На экране появится окно мастера экспорта сертификатов.
5. Нажмите кнопку "Далее" ("Next") внизу окна.

   На экране появится окно выбора формата экспортируемого файла.
6. Выберите любой формат и нажмите кнопку "Далее" ("Next").

   На экране появится окно ввода имени экспортируемого файла.
7. Нажмите кнопку "Обзор" ("Browse").

   На экране появится окно "Сохранение" ("Save").
8. Выберите место для сохранения файла, укажите имя файла и нажмите кнопку "Сохранить" ("Save").

   На экране появится окно с прописанным местом и именем экспортируемого файла.
9. Нажмите кнопки "Далее" ("Next") и "Готово" ("Finish").

   После успешного экспорта корневого сертификата появится соответствующее сообщение.
10. Нажмите кнопку "ОК" в окне сообщения. В списке сертификатов выберите "Персональные сертификаты".

    В правой части экрана появится список установленных персональных сертификатов.
11. Выберите действующий сертификат сервера и нажмите кнопку "Свойства" на панели инструментов.

    На экране появится окно "Сертификат".
12. Повторите пп. **4–9** для экспорта сертификата сервера.
13. Откройте окно интернет- браузера и скачайте CRL- файл по адресу: http://адресмониторинга/cdc.crl

    Примечание 1. В случае если браузеру не удастся открыть эту страницу, замените "адресмониторинга" на IP-адрес или дополнительный адрес сервера комплекса.

    Примечание 2. В случае если скачать CRL-файл не получилось вышеперечисленными способами, это можно сделать из меню "Сертификаты | Отозванные сертификаты | Экспортировать список отозванных сертификатов" при локальном управлении ЦУС, указав корневой сертификат, выбранный в п.**3**.
14. Установите скачанный CRL-файл в хранилище сертификатов Windows, расположенное на локальном компьютере (см. стр. **44**).

    Внимание! Срок действия CRL-файла — 1 месяц.
15. Далее необходимо произвести установку TLS-клиента и его настройку в соответствии с Руководством по эксплуатации RU.88338853.501430.011 91.

Для настройки конфигурационного файла Менеджера конфигурации:

Примечание. Данная процедура производит настройку прямого запуска приложения мониторинга при нажатии кнопки "Мониторинг" на панели инструментов раздела "Структура" Менеджера конфигурации.

1. Используя приложение Проводник Windows, откройте содержимое папки "C:\Users\%username%\AppData\Local\CCM\", где %username% — папка учетной записи пользователя.
2. Откройте файл "CCM.config" с помощью приложения "Блокнот".

   Конфигурационный файл откроется в приложении "Блокнот" для внесения изменений.
3. Найдите в заключительной части файла строку:

   <monitoring url="http://Choose url…
4. Замените содержимое кавычек на IP-адрес или доменное имя ЦУС с обязательным использованием протокола HTTPS. К примеру:

   <monitoring url="https://10.10.10.10"/> или

   <monitoring url="https://srvkdk"/>

   Примечание. Имя ЦУС совпадает с именем сертификата управления ЦУС. При этом требуется соответствующим образом настроить DNS-сервер или дополнить файл hosts.
5. В меню "Файл" приложения "Блокнот" выберите команду "Сохранить", а затем — "Выход".

Для выпуска и установки сертификатов веб-сервера мониторинга:

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

   На экране появится окно "Сертификаты".
2. Выберите в меню "Сертификаты" пункт "Корневые сертификаты веб-сервера мониторинга (RSA)" и нажмите клавишу <Enter>.

   На экране появится окно "Корневые сертификаты веб-сервера мониторинга (RSA)".
3. Для создания корневого сертификата нажмите клавишу <F2>.

   На экране появится окно "Выпуск сертификата".
4. Выберите пункт "Выпуск корневого RSA-сертификата" и нажмите клавишу <Enter>.

   На экране появится окно "Сертификат".
5. Заполните поля "Организация", "Отдел" и "Название" и нажмите клавишу <Enter>.

   Примечание 1. Для перемещения по форме используйте стандартные клавиши: <↑>, <↓>, <Page Down>, <Page Up>, <Home>.

   Примечание 2. По умолчанию название корневого RSA-сертификата: "mon-aes" (без кавычек).

   На экране появится сообщение: "Успешно".
6. Нажмите клавишу <Enter>.

   Будет выполнен возврат в окно "Выпуск сертификата".
7. Выполните возврат в меню "Сертификаты", выберите пункт "Сертификаты безопасности веб-сервера мониторинга (RSA)" и нажмите клавишу <Enter>.

   На экране появится окно "Сертификаты безопасности веб-сервера мониторинга (RSA)".
8. Для создания сертификата управления нажмите клавишу <F2>.

   На экране появится окно "Выпуск сертификата".
9. Выберите пункт "Выпуск сертификата RSA для Web-сервера" и нажмите клавишу <Enter>.

На экране появится окно "Сертификат".

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

> **Примечание.** По умолчанию название корневого RSA-сертификата: "mon-aes" (без кавычек).

> **Внимание!** Название RSA-сертификата для веб-сервера будет использовано как доменное имя ЦУС (далее — "адресмониторинга"). При этом требуется соответствующим образом настроить DNS-сервер или дополнить файл hosts на РМ администратора.

На экране появится окно выбора корневого сертификата.

11. Выберите корневой сертификат и нажмите клавишу <Enter>.

Произойдет выпуск сертификата управления и на экране появится сообщение "Успешно".

12. Нажмите клавишу <Enter>.

На экране появится сообщение с URL-адресом, содержащим доменное имя веб-сервера системы для RSA-доступа.

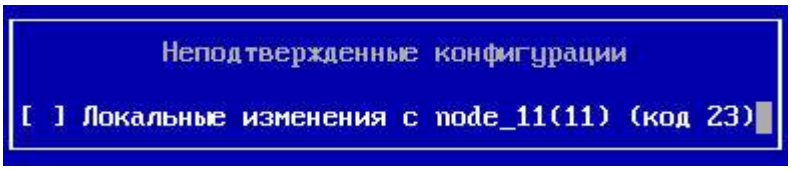
13. Нажмите клавишу <Enter>.

Будет выполнен возврат в окно "Выпуск сертификата".

14. Для применения данных сертификатов перейдите в меню настроек, выберите пункт "Применить локальную политику" и нажмите клавишу <Enter>. Дождитесь успешного завершения операции и появления соответствующего сообщения.

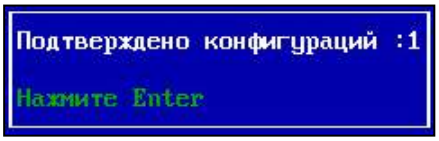
15. Нажмите клавишу <Enter>, выберите пункт "Возврат в главное меню", затем перейдите в меню "Инструменты" и выберите пункт "Подтверждение изменений настроек УБ". Нажмите клавишу <Enter>.

На экране появится окно "Неподтвержденные конфигурации".



16. Установите отметку клавишей <Пробел> и нажмите клавишу <Enter>.

На экране появится сообщение о подтверждении конфигурации.



17. Для возврата в меню "Инструменты" нажмите клавишу <Enter>.

Для запуска системы мониторинга и аудита:

1. В окне веб-браузера (см. стр. **15**) введите "https://адресмониторинга".

   На экране появится окно для аутентификации.

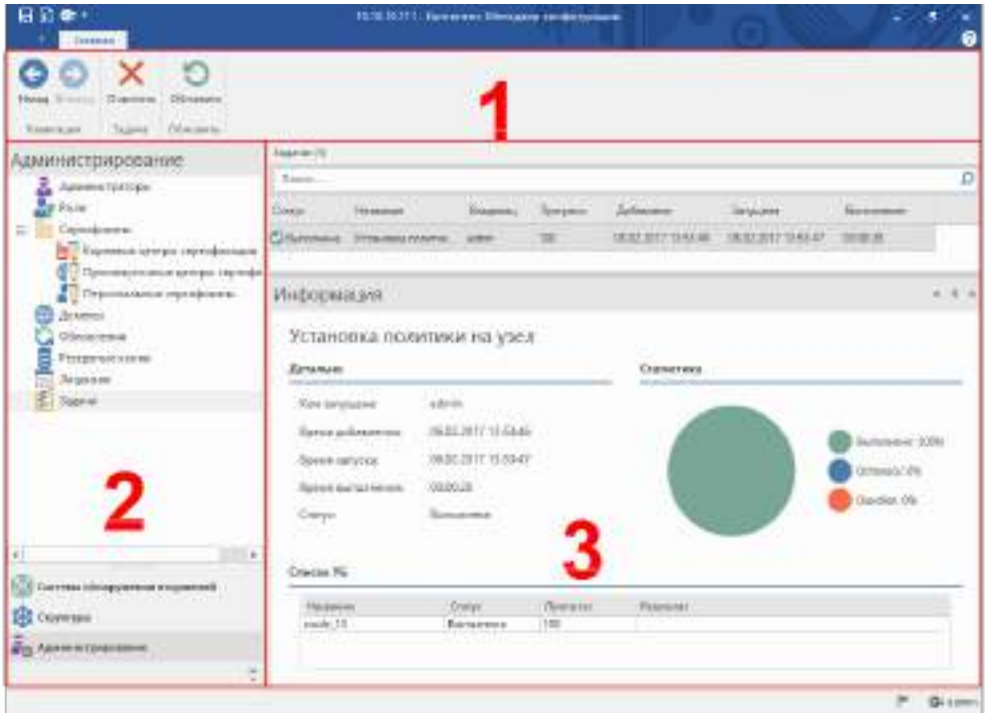
2. Введите имя и пароль администратора (см. стр. **12**) и нажмите кнопку "ОК".

   После успешной аутентификации на экране появится главное окно системы. Руководство по ее использованию приведено в [1].

Интерфейс Менеджера конфигурации

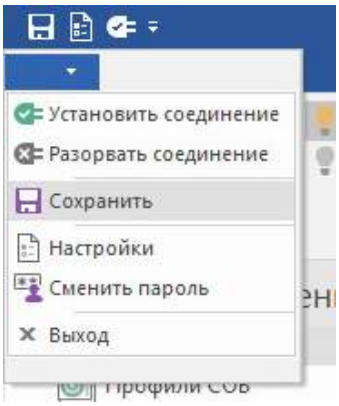
Средством удаленного управления ЦУС, а также другими узлами комплекса является программное обеспечение, входящее в состав комплекса, со специализированным графическим пользовательским интерфейсом.

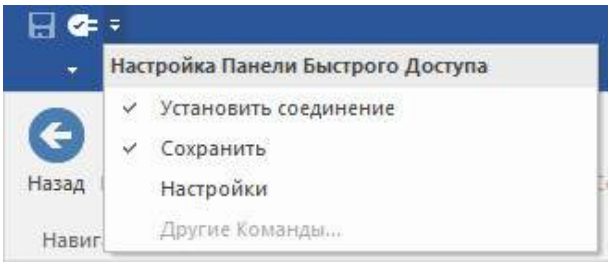
После запуска Менеджера конфигурации и успешной аутентификации (см. стр. **23**) на экране монитора будет отражено главное окно приложения.



В верхней части главного окна расположена панель инструментов (на рисунке — 1-я область). Она представляет собой набор функциональных кнопок, предназначенных для вызова часто выполняемых задач. Статус "доступности" и тип кнопок изменяется в зависимости от ситуации (активный раздел меню, наличие элементов, права пользователя и т. п.), в которой в данный момент ведется работа. Каждая кнопка имеет название на русском языке, поясняющее ее функционал. При наведении курсора мыши на кнопку появится всплывающая подсказка, содержащая дополнительную информацию о выполняемой команде, а также доступное сочетание горячих клавиш для вызова ее функционала с клавиатуры.

Над панелью инструментов в левом верхнем углу расположена панель быстрого доступа, на которой расположены иконки команд основного меню Менеджера конфигурации, а под панелью быстрого доступа — кнопка вызова этого меню.





Справа от панели быстрого доступа расположена иконка ее настройки. Для отображения нужной команды на панели нужно установить соответствующий флажок в раскрытом меню настройки, а для скрытия ненужной команды — снять флажок.

В левой части окна под панелью инструментов отображается список разделов и подразделов главного меню (на рисунке — 2-я область). В его верхней области раскрыт текущий активный раздел и подраздел. Подраздел может иметь свою группу подразделов, в этом случае он сопровождается значком ⊟ в случае уже развернутого списка группы или ⊞ в случае свернутого списка. Соответственно, при нажатии на значок список переходит в альтернативное состояние.

Справа расположена область отображения информации активного подраздела (на рисунке — 3-я область). Данная область может содержать как совокупность структурированных данных, представляемых в виде списков, таблиц и

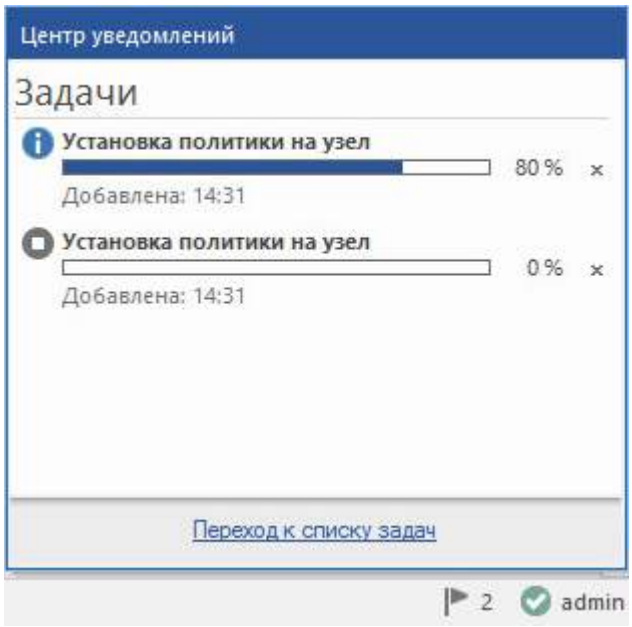
графиков, так и различные функциональные элементы (дополнительные кнопки, активные поля и т. п.). Табличные данные часто имеют свое контекстное меню, вызываемое щелчком правой кнопки мыши, часть команд которого дублирует команды панели инструментов. Двойной щелчок левой кнопки мыши обычно приводит к вызову свойств элемента, аналогично нажатию кнопки "Свойства" на панели инструментов.

Для эффективной работы со структурированными данными реализован принцип выделения (используя клавиши Ctrl/Shift и курсор мыши) и перетаскивания группы выбранных объектов (drag&drop).

Для сортировки отображаемой информации по возрастанию/убыванию одного из параметров нажмите на соответствующий заголовок столбца.

Вверху области отображения информации расположена строка состояния, содержащая сведения о количестве наблюдаемых элементов, а также строка контекстного поиска.

В правом нижнем углу главного окна расположен флажок Центра уведомлений, в котором можно посмотреть прогресс выполнения текущих задач, а также число этих задач (при их наличии). Далее отображается учетная запись текущего администратора, под которым произошла аутентификация в Менеджере конфигурации.



Запуск Менеджера конфигурации

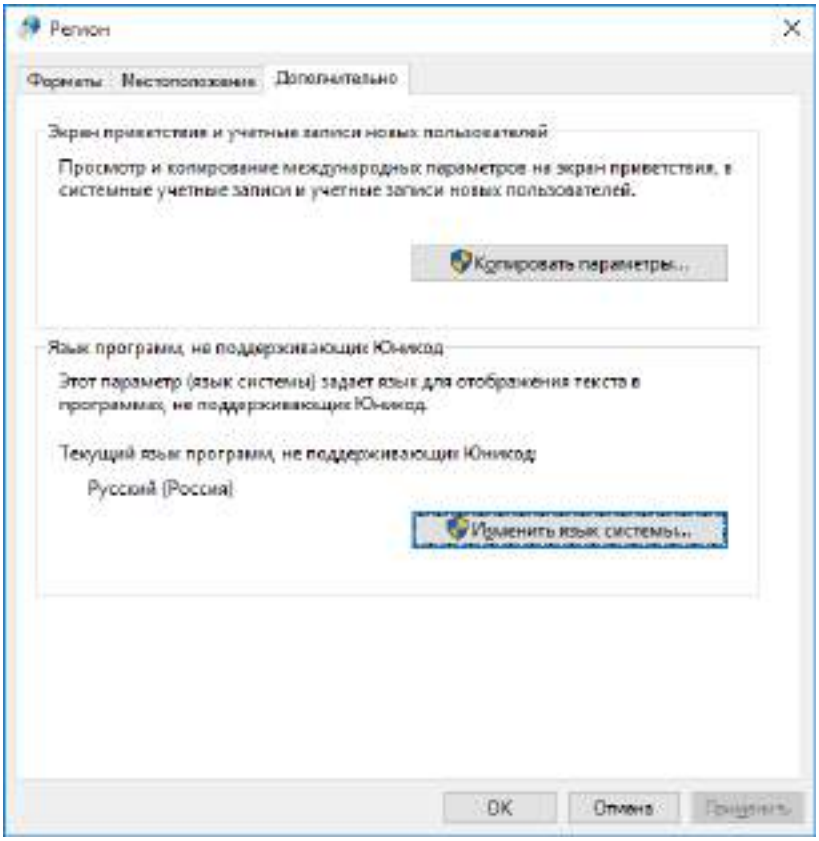
Внимание! Перед запуском Менеджера конфигурации необходимо проверить региональные настройки ОС. В случае установленного по умолчанию английского языка для программ, не поддерживающих Юникод, попытка подключения к ЦУС завершится сообщением об ошибке.

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" установлен не "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 или компьютера.

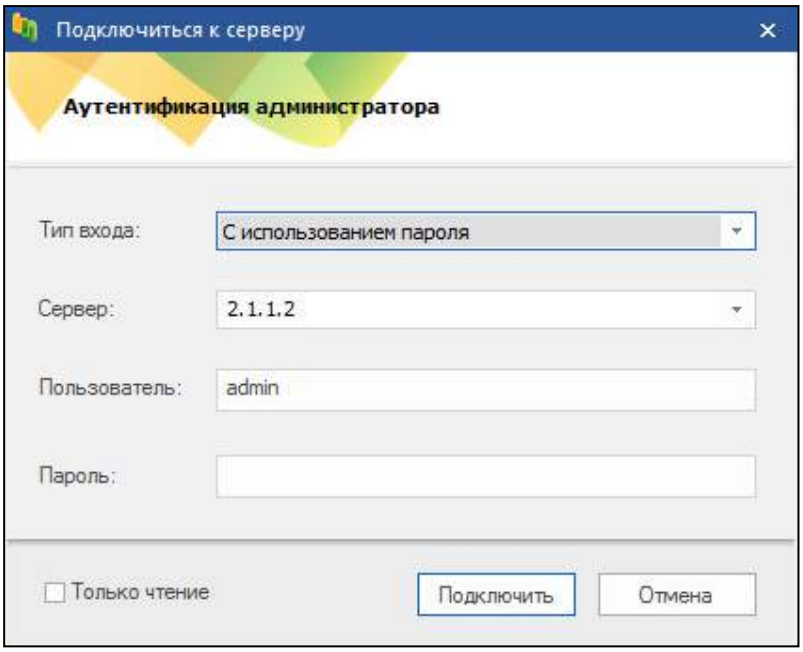
Для запуска Менеджера конфигурации:

1. Активируйте на рабочем столе ярлык Менеджера конфигурации.

Примечание. При первом после установки запуске Менеджера конфигурации в его главном окне может быть отображено информационное сообщение о необходимости выполнить инициализацию биологического датчика случайных чисел (ДСЧ).

Нажмите по ссылке для начала процесса инициализации ДСЧ и следуйте указаниям на экране. Дождитесь завершения процесса накопления энтропии, а затем нажмите кнопку вызова меню настроек в левом верхнем углу Менеджера конфигурации и в раскрывшемся списке выберите команду "Установить соединение".

На экране появятся главное окно Менеджера конфигурации и диалоговое окно "Аутентификация администратора".



2. В окне "Аутентификация администратора" выберите в поле "Тип входа" значение "С использованием пароля" и при первом запуске Менеджера конфигурации в поле "Сервер" введите IP-адрес ЦУС, к которому должно быть выполнено подключение.

   Примечание. Аутентификация главного администратора также возможна по его сертификату, полученному при инициализации ЦУС (см. стр. 12).

   Внимание! Если впоследствии в Менеджере конфигурации были настроены профили подключения к различным ЦУС (см. стр. **45**), то для указания сервера, к которому должно быть выполнено подключение, выберите его из раскрывающегося списка.

3. Укажите имя и пароль администратора ЦУС и нажмите кнопку "Подключить".

   Примечание. Пароль главного администратора задается при инициализации ЦУС.

   Будет выполнено подключение Менеджера конфигурации к ЦУС.

Развертывание узла безопасности

Развертывание узла безопасности выполняют после подготовки аппаратной платформы в следующей последовательности:

1. Установка операционной системы на аппаратную платформу (если не установлена). Процесс установки описан в [3].
2. Инициализация узла безопасности и создание запроса на получение сертификата. Выполняют средствами локального управления УБ (см. ниже).
3. Создание нового узла, выпуск сертификата по запросу, созданному на узле безопасности, и экспорт конфигурации узла. Выполняют с помощью Менеджера конфигурации или средствами локального управления ЦУС (см. стр. **28**).
4. Настройка подключения к ЦУС. Выполняют средствами локального управления узлом безопасности (см. стр. **32**).
5. Регистрация и первичная настройка узла безопасности на ЦУС (см. стр. **33**).

Инициализация узла безопасности и создание запроса на получение сертификата

Данная процедура выполняется средствами локального управления УБ.

Для инициализации УБ:

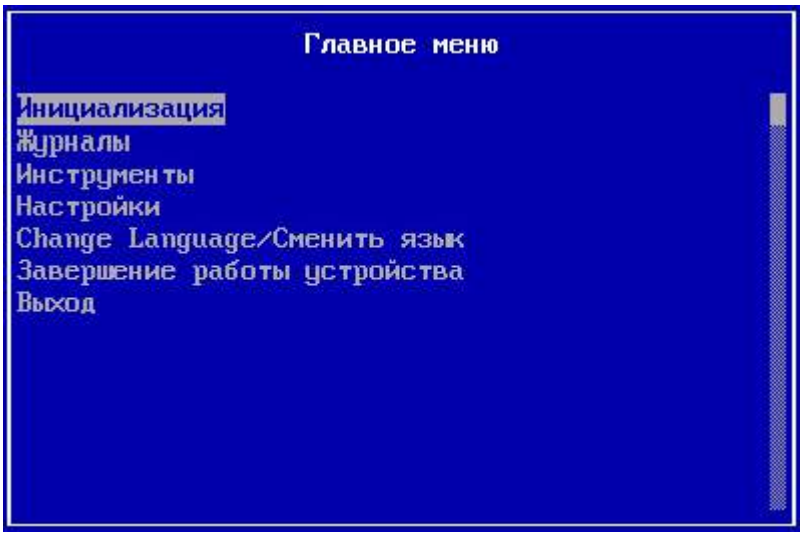
1. Выключите питание сетевого устройства. Подключите к системному блоку сетевого устройства клавиатуру и монитор.
2. Включите питание сетевого устройства.

   На экране появится основное окно ПАК "Соболь", в центре которого будет отображаться запрос персонального идентификатора.
3. Аккуратно приложите персональный идентификатор администратора к считывателю.

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

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

   Начнется загрузка операционной системы и после ее завершения на экране появится главное меню:



6. Выберите пункт "Инициализация" и нажмите клавишу <Enter>.

На экране появится запрос на продолжение процедуры.

7. Выберите "Да" в окне запроса и нажмите клавишу <Enter>.

   На экране появится окно выбора инициализируемого компонента.

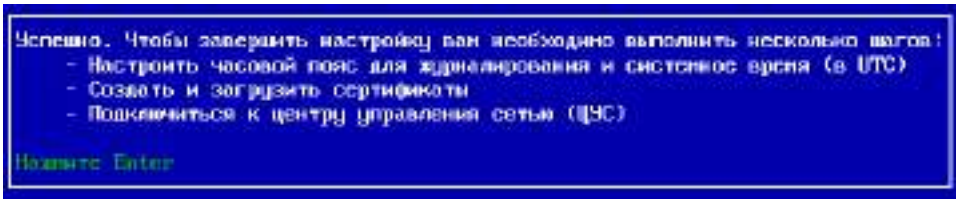
8. Выберите "Узел безопасности" и нажмите клавишу <Enter>.

   На экране появится запрос на очистку локальных журналов.

9. Выберите "Да" в окне запроса и нажмите клавишу <Enter>.

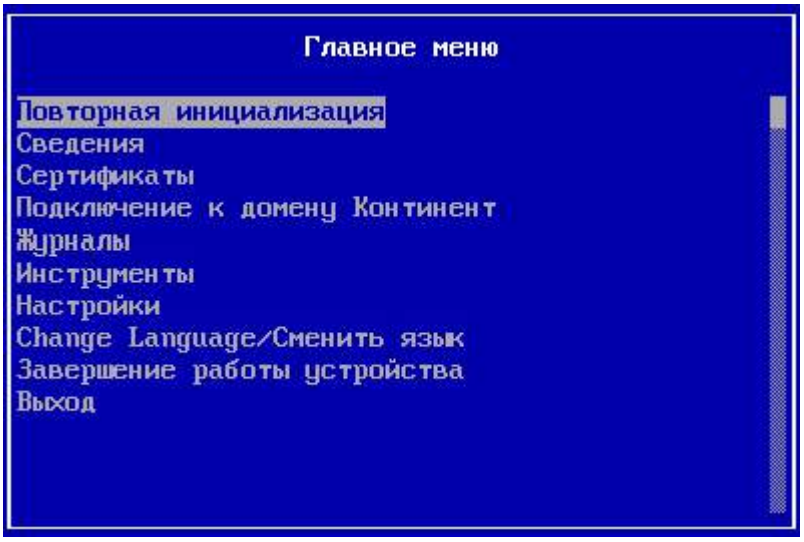
   Начнется сжатие базы данных, после чего будет выполнена инициализация служб сервера конфигурирования.

   Дождитесь сообщения об успешном завершении инициализации.



10. Нажмите клавишу <Enter>.

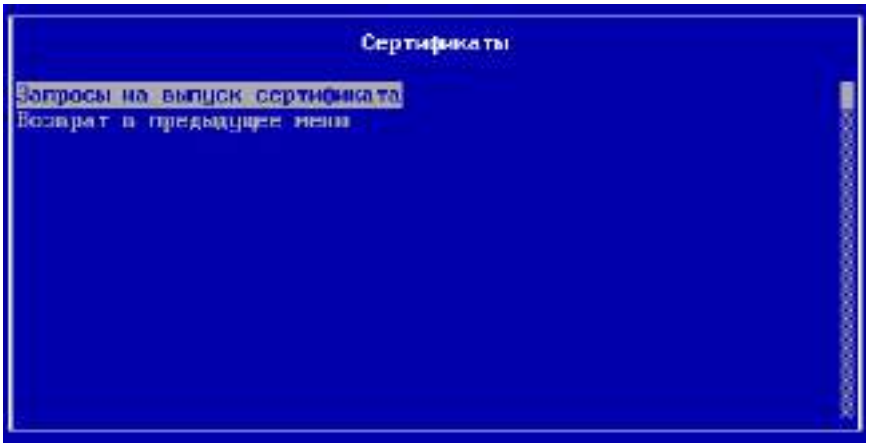
    Будет выполнен возврат в главное меню локального управления. При этом содержание меню изменится.



11. Осуществите настройку системного времени (см. стр. **9**).

12. Выберите пункт "Сертификаты" и нажмите клавишу <Enter>.

    На экране появится меню "Сертификаты".



13. Выберите пункт "Запросы на выпуск сертификата" и нажмите клавишу <Enter>.

    На экране появится окно "Запросы на выпуск сертификата".

14. Вставьте внешний носитель в USB-разъем и нажмите клавишу <F4>.

    На экране появится окно "Сертификат".

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

    Будет выполнена запись файла запроса сертификата на внешний носитель, после чего на экране появится соответствующее сообщение.

16. Нажмите клавишу <Enter> для возврата в меню "Запросы на выпуск сертификата", извлеките внешний носитель и перейдите на ЦУС или РМ администратора для выпуска сертификата управления УБ и формирования конфигурационного файла.

Выпуск сертификата управления и формирование конфигурационного файла

Данную процедуру выполняют на ЦУС в Менеджере конфигурации (см. ниже) или средствами локального управления (см. стр. **31**). Перед началом процедуры необходимо узнать серийный номер инициализируемого сетевого устройства, указанный на его корпусе, и приготовить внешний носитель с файлом запроса continent-XX.req. На этот носитель в результате выполнения процедуры будет записан конфигурационный файл УБ.

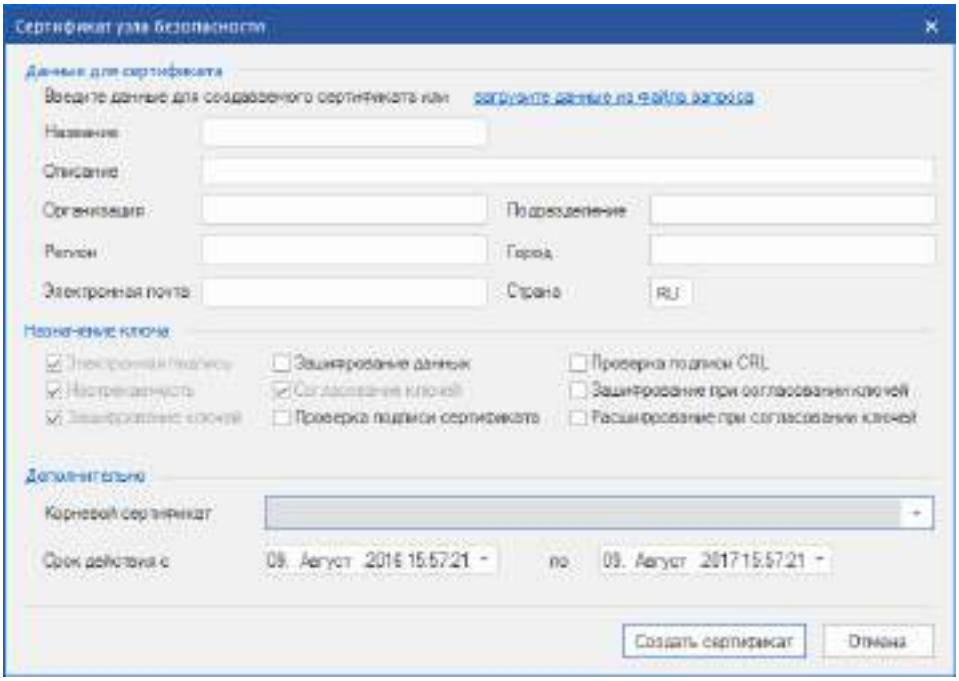
Примечание. Конфигурационный файл потребуется на узле безопасности для настройки подключения к ЦУС.

Для создания сертификата в Менеджере конфигурации:

1. Откройте Менеджер конфигурации и перейдите в раздел "Администрирование".
2. В списке сертификатов выберите "Персональные сертификаты".

   В правой части экрана появится список установленных персональных сертификатов.
3. Нажмите кнопку "Сертификат узла безопасности" на панели инструментов.

   На экране появится окно "Сертификат узла безопасности".



4. Нажмите ссылку "загрузите данные из файла запроса", укажите путь к файлу запроса и нажмите кнопку "Открыть".

   Файл будет считан и на экране заполнятся области данных для сертификата и назначения ключа.

5. В дополнительных параметрах выберите созданный при развертывании ЦУС корневой сертификат, а также установите требуемый срок действия сертификата управления.

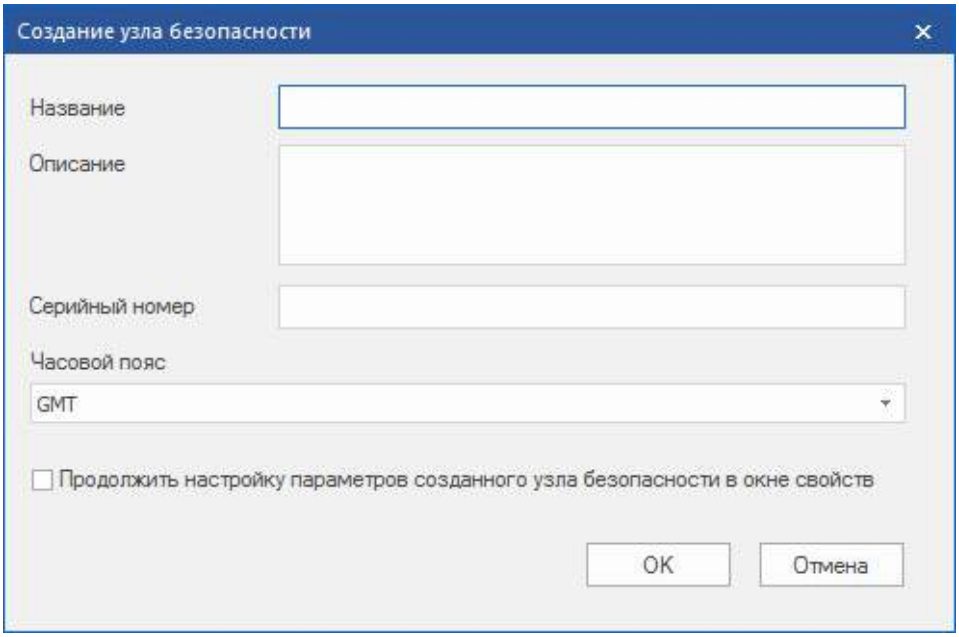
6. Нажмите кнопку "Создать сертификат".

   Будет создан файл сертификата управления для УБ, после чего данные сертификата отобразятся в списке на экране.

Для создания нового УБ и его первичной настройки в Менеджере конфигурации:

1. Откройте Менеджер конфигурации и перейдите в раздел "Структура".
2. Нажмите кнопку "Узел безопасности" на панели инструментов.

   На экране появится окно "Создание узла безопасности".



3. Заполните требуемые поля данных для УБ, укажите часовой пояс, в котором он расположен, установите флажок "Продолжить настройку параметров созданного узла безопасности в окне свойств", а затем нажмите кнопку "ОК".

Внимание! Часовой пояс для всех устройств комплекса должен быть одинаковым! Это необходимо для корректной работы системы журналирования и аудита комплекса.

Примечание. В поле "Название" могут быть использованы только латинские буквы в нижнем регистре, цифры и символы "_-.". Длина названия не может быть более 32 символов. Первым символом может быть только буква или символ "_".

На экране появится окно свойств узла безопасности.

4. Выберите в левой части окна в разделе "Узел безопасности" пункт "Сертификаты".
5. В области серверных сертификатов нажмите кнопку добавления нового сертификата "".

На экране появится окно "Сертификаты".

6. Выберите в списке сертификат управления, созданный в ходе предыдущей процедуры.

Сертификат узла безопасности отобразится в списке на экране.

7. В области корневых сертификатов нажмите кнопку добавления нового сертификата "".

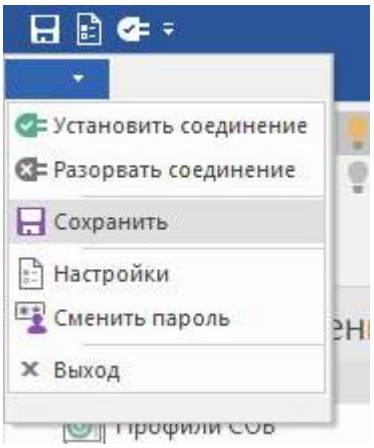
На экране появится окно "Сертификаты".

8. Выберите в списке корневой сертификат и нажмите кнопку "ОК".

Примечание. Для обновления ПО в комплексе предустановлены сертификаты "Доверенный издатель САО КБ" и "Издатель САО КБ Класс 1". Для использования в других целях они не предназначены.

Созданный узел безопасности отобразится в списке на экране.

9. В левом верхнем углу окна Менеджера конфигурации нажмите кнопку вызова меню и выберите пункт "Сохранить".



Для формирования и экспорта конфигурационного файла в Менеджере конфигурации:

1. Вставьте внешний носитель в USB- разъем для записи на него конфигурационного файла.
2. Откройте Менеджер конфигурации и перейдите в раздел "Структура".
3. Нажмите кнопку "Узел безопасности" на панели инструментов.

На экране появится окно "Создание узла безопасности".

4. Вызовите контекстное меню созданного узла безопасности и выберите команду "Экспортировать конфигурацию узла...".

На экране появится стандартное окно для сохранения файла.

5. Укажите нужный путь и имя файла, а 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.

Для создания сертификата средствами локального управления:

Примечание. Если к ЦУС было осуществлено удаленное подключение через Менеджер конфигурации, то после аутентификации появится сообщение о том, что БД заблокирована администратором из Менеджера конфигурации. В этом случае необходимо выбрать пункт "Принудительно захватить блокировку".

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 УБ, после чего произойдет возврат к окну "Выпуск сертификата".

8. 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.

Для создания конфигурационного файла средствами локального управления:

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

   На экране появится меню "Инструменты".

2. Выберите пункт "Создать новый узел безопасности" и нажмите клавишу <Enter>.

На экране появится запрос на ввод ID узла безопасности.

3. Введите ID УБ и нажмите клавишу <Enter>.

   Примечание. ID УБ — серийный номер, указанный на корпусе УБ.

   На экране появится окно выбора сертификата управления для узла безопасности.

4. Выберите сертификат для данного УБ и нажмите клавишу <Enter>.

   Начнется формирование конфигурационного файла для узла безопасности и запись его на внешний носитель. По завершении будет выполнен возврат в меню "Инструменты".

   Примечание. Имя конфигурационного файла, записанного на внешний носитель: gate_XX.json, где XX — ID узла безопасности.

5. Извлеките внешний носитель и перейдите к УБ для настройки подключения к ЦУС.

Настройка подключения к ЦУС

Подключение выполняют на УБ средствами локального управления. Перед началом процедуры приготовьте внешний носитель с конфигурационным файлом gate-XX.json, где XX — серийный номер УБ.

Для настройки подключения:

1. Вставьте внешний носитель с конфигурационным файлом в свободный порт USB.
2. В главном меню локального управления УБ выберите пункт "Подключение к домену "Континент" и нажмите клавишу <Enter>.

   На экране появится предупреждение.

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

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

4. Выберите нужный файл конфигурации и нажмите клавишу <Enter>.

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

5. Выберите используемый для управления интерфейс 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 окно предупреждения о применении настроек.

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

   Начнется применение начальной конфигурации, а затем локальных изменений в настройках УБ. После чего эти изменения будут отправлены на ЦУС, а на экране появится журнал инициализации с описанием успешной инициализации УБ.

8. Для выхода из журнала нажмите клавишу <Esc>.

   Будет выполнен возврат в главное меню. Настройка подключения на УБ завершена.

Примечание. После завершения настройки подключения к ЦУС в Менеджере конфигурации отобразится новый УБ с неустановленным компонентом и локальной версией конфигурации.

Учет изменений и первичная настройка узла безопасности

Заключительную часть процедуры развертывания УБ выполняют на ЦУС. Она заключается в подтверждении политики, пришедшей с подключенного УБ, первичной настройке параметров узла безопасности, а также отправке локальных изменений на вышестоящий ЦУС. Эти действия выполняются в Менеджере конфигурации.

Для регистрации и настройки узла безопасности:

1. Откройте Менеджер конфигурации и перейдите в раздел "Структура".

   В правой части окна отобразится список узлов безопасности, известных ЦУС.

   Примечание. Если в списке у подключаемого узла безопасности не прописана локальная версия конфигурации, нажмите кнопку "Обновить" на панели инструментов.

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

   Появится окно с запросом о подтверждении локальных изменений конфигурации УБ.

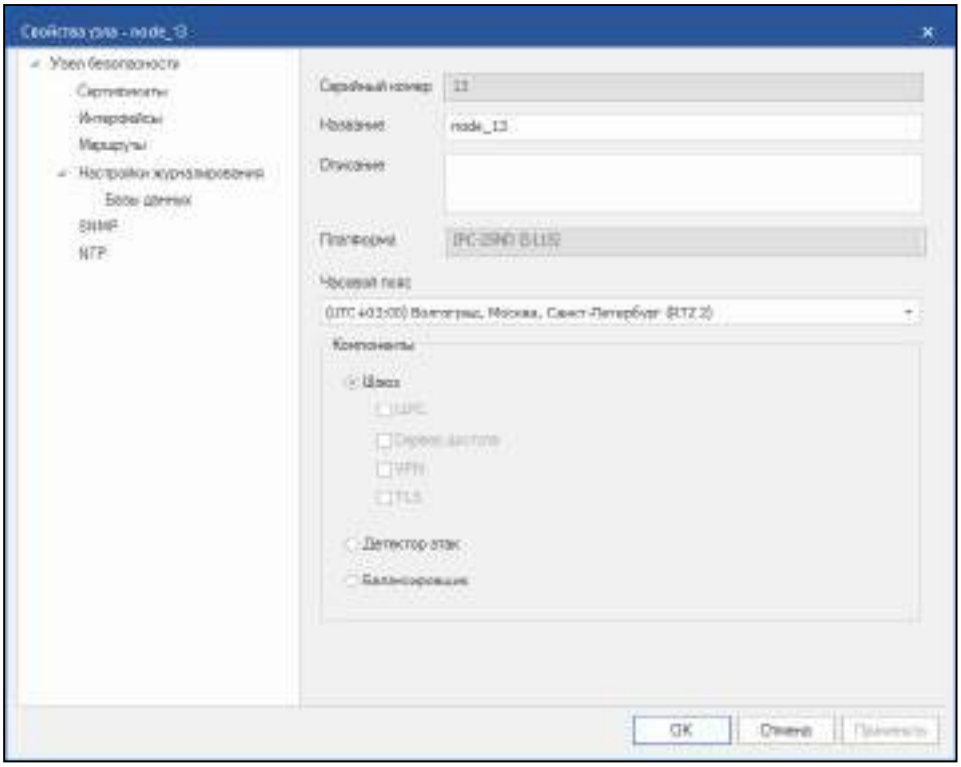
3. Нажмите кнопку "Да".

   Появится окно с сообщением об успешном обновлении конфигурации узла.

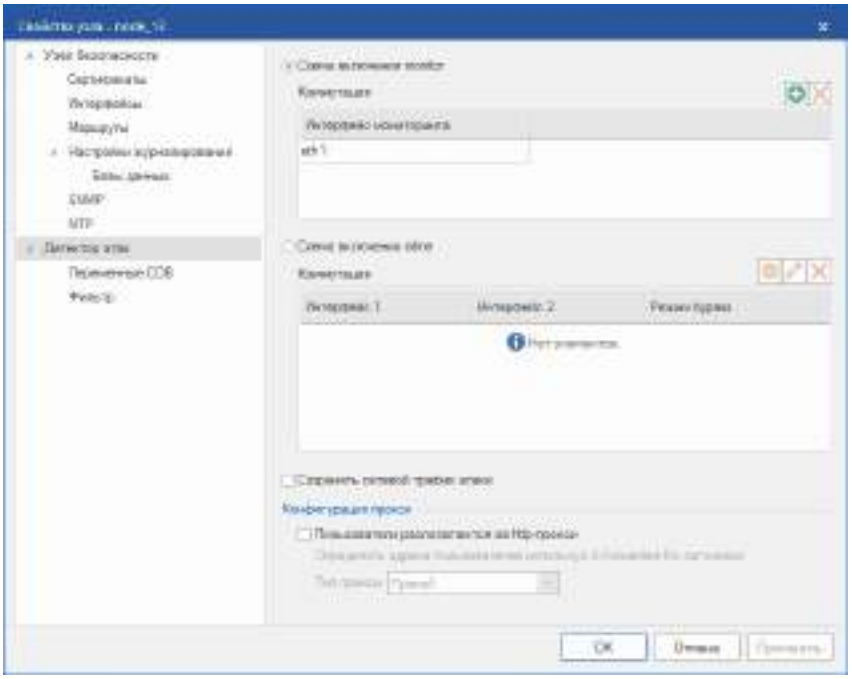
4. Нажмите кнопку "ОК".

   Информация о конфигурации узла безопасности будет добавлена в базу данных домена.

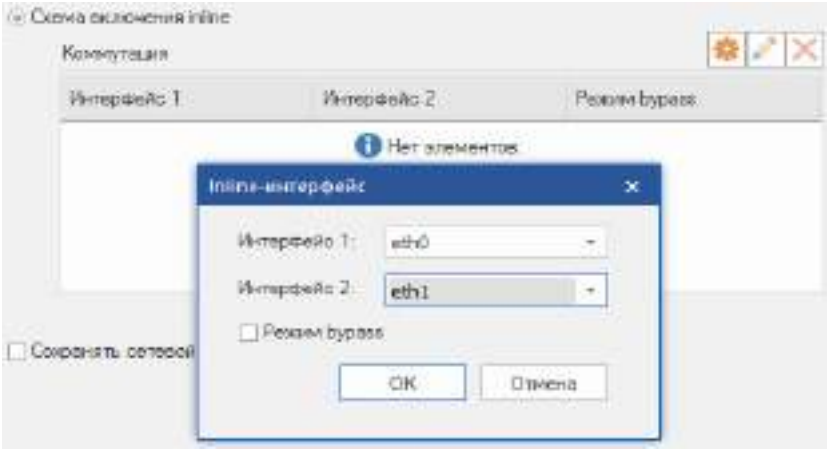
5. Вызовите окно настройки свойств созданного узла.



6. Выберите компонент (детектор атак или балансировщик).
7. Перейдите в меню слева в пункт "Детектор атак".



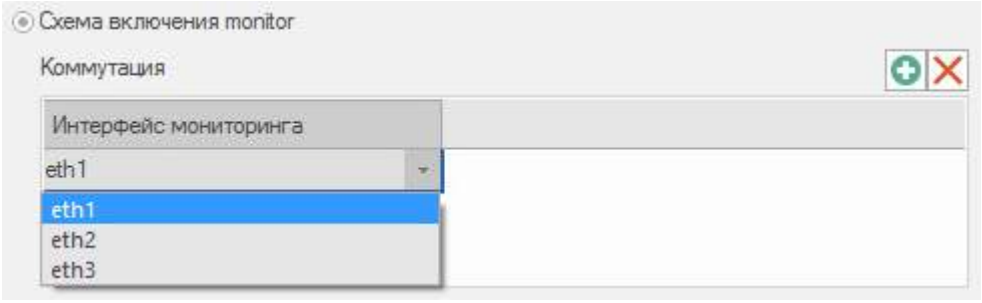
8. В случае если ДА планируется использовать в режиме Monitor, перейдите к п. **14**.
9. Выберите схему включения Inline и в списке "Коммутация" добавьте Inline-интерфейсы. Для этого нажмите кнопку "Добавить" .
   На экране появится окно настройки Inline-интерфейсов.



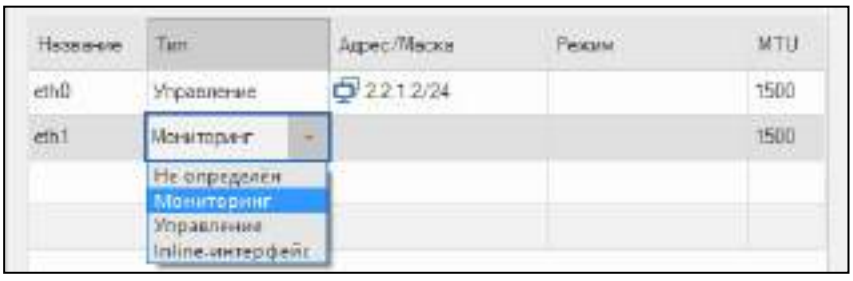
10. Установите соответствие логических и физических Inline-интерфейсов.
11. Установите отметку в поле "Режим bypass" для беспрепятственного прохождения трафика в случае отказа ДА и нажмите кнопку "ОК".

    На экране появится сообщение с уведомлением о назначении Inline-интерфейсов.
12. Нажмите кнопку "Да" в окне сообщения.

    Назначенные интерфейсы появятся в списке "Коммутация".
13. Перейдите к п. **15**.
14. Выберите схему включения Monitor и в списке "Коммутация" добавьте Inline-интерфейсы. Для этого нажмите кнопку "Добавить" и добавьте интерфейс мониторинга, выбрав его из списка.



15. При необходимости установите отметку в поле "Сохранять сетевой трафик атаки".
16. Выберите в свойствах узла безопасности пункт "Интерфейсы" и настройте необходимый тип работы для каждого интерфейса.

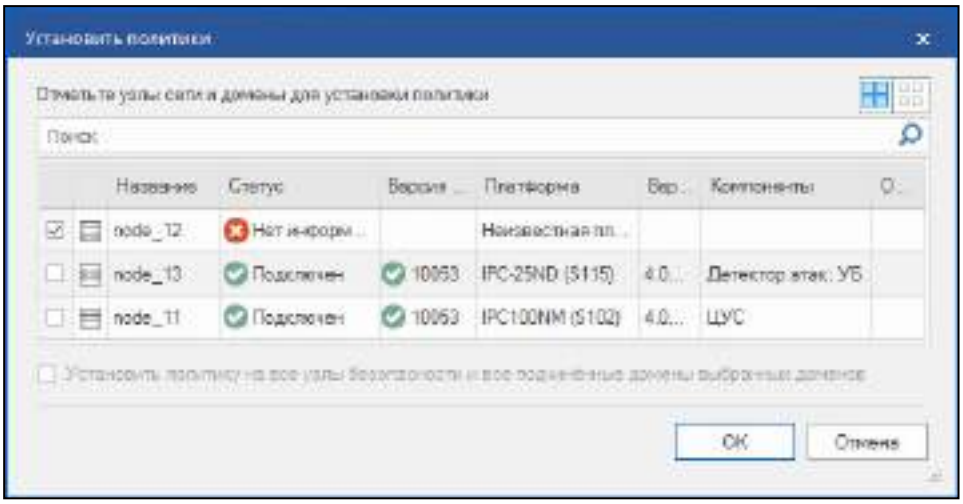


17. Выберите в меню слева пункт "Переменные СОВ" и укажите домашнюю (защищаемую) подсеть (переменная HOME_NET).
18. Нажмите кнопку "ОК".

    Будет осуществлен возврат к списку узлов сети, при этом в строке нового узла сети будут отражены введенные параметры. Например, если выбран компонент "Детектор атак", в столбце "Компоненты" отобразится пункт "Детектор атак; УБ".

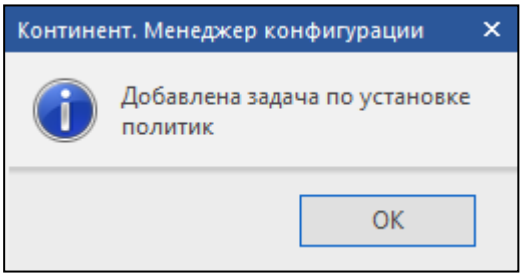
19. В главном окне Менеджера конфигурации нажмите кнопку "Установить политику" на панели инструментов.

Откроется окно для установки политик узлам сети.



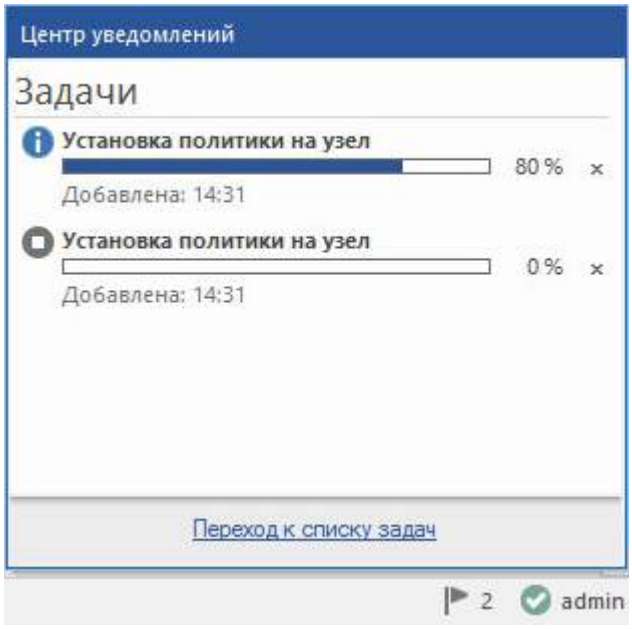
20. В окне установки политики выберите узел сети, для которого следует установить политику, и поставьте отметку слева от названия. Далее нажмите кнопку "ОК".

Конфигурация домена на ЦУС будет изменена в соответствии с указанными настройками, при этом будет поставлена в очередь задача по установке политики на выбранные узлы, после чего на экране появится соответствующее сообщение.



21. Нажмите кнопку "ОК" в окне сообщения.

Примечание. Статус задачи можно увидеть в разделе "Администрирование | Задачи". Для контроля ее выполнения в реальном времени нужно нажать на флажок в нижнем правом углу Менеджера конфигурации. Во всплывающем окне будет показан прогресс выполнения текущих задач.



Формирование и установка политик СОВ

После регистрации в Менеджере конфигурации узлов безопасности необходимо к каждому из них применить соответствующую политику с правилами СОВ. Для применения политики предварительно должны быть созданы профиль (или список профилей) и список правил, входящих в состав политики.

Параметрами профиля являются:

- действие, которое должно быть выполнено системой обнаружения вторжений в результате срабатывания сигнатуры;
- список контролируемых приложений.

Правило, входящее в состав политики, определяет, какой профиль и на каком узле безопасности должен быть применен.

В общем случае для применения политики на каждом из узлов безопасности необходимо выполнить следующее:

1. Создать и настроить профиль или список профилей (см. ниже).

   Примечание. В системе доступны предустановленные профили:
   - Оптимальный набор, содержащий пакет правил, детектирующих угрозы для служб передачи данных, веб-клиентов и веб-серверов.
   - Полный набор, содержащий полный пакет правил.

   Данные профили можно использовать для настройки работы узлов безопасности, но редактировать их нельзя.

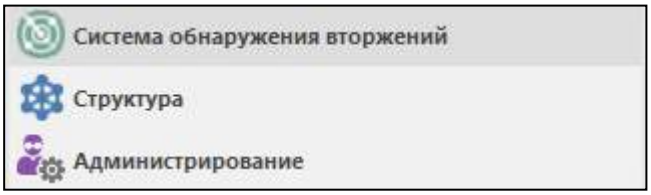
2. Сформировать политику — правило или список правил (см. стр. **41**).
3. Установить политику — применить к зарегистрированным узлам безопасности (см. стр. **42**).

Создание нового профиля

Примечание. Профиль СОВ основывается на базе решающих правил (БРП), хранящейся на ЦУС. Первоначально ЦУС располагает только ограниченной БРП, перед созданием пользовательских профилей рекомендуется провести обновление БРП с диска или из других источников (см. [1], параграф "Обновление БРП").

Для создания профиля:

1. В главном окне Менеджера конфигурации откройте раздел "Система обнаружения вторжений".

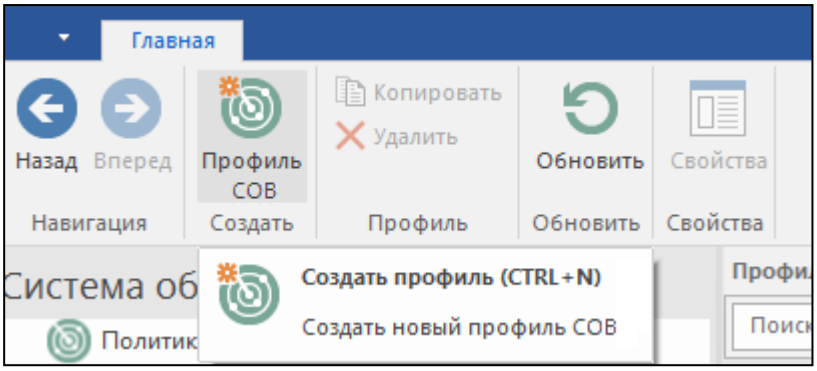
   

2. Перейдите в подраздел "Профили СОВ".

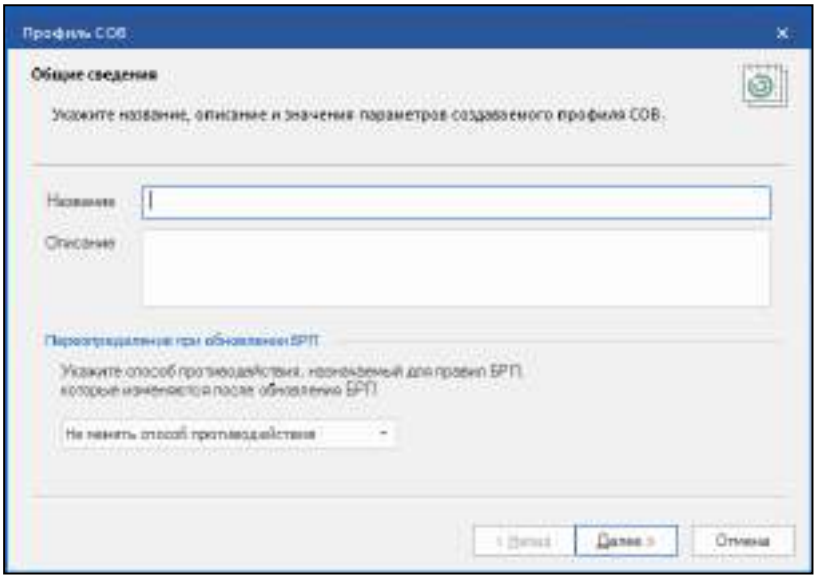
   Справа появится список созданных профилей.

   Примечание. Если профили не создавались, список будет состоять из двух предустановленных профилей — "Оптимальный набор" и "Полный набор".

3. В панели инструментов нажмите кнопку "Профиль СОВ".

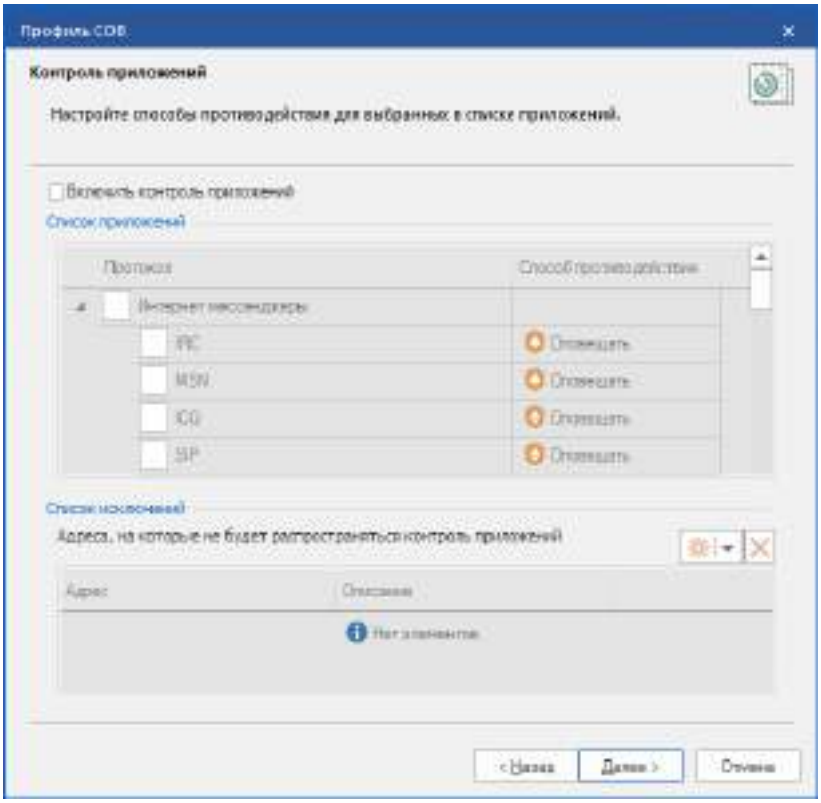


На экране появится диалог сбора общих сведений мастера по настройке профиля СОВ.



4. Заполните поля "Название" и "Описание", укажите способ противодействия и нажмите кнопку "Далее".

   На экране появится диалог контроля приложений.



5. При необходимости контроля трафика определенных приложений установите флажок "Включить контроль приложений", отметьте нужные приложения и выберите для них нужный способ противодействия:
   - "Оповещать";
   - "Блокировать".

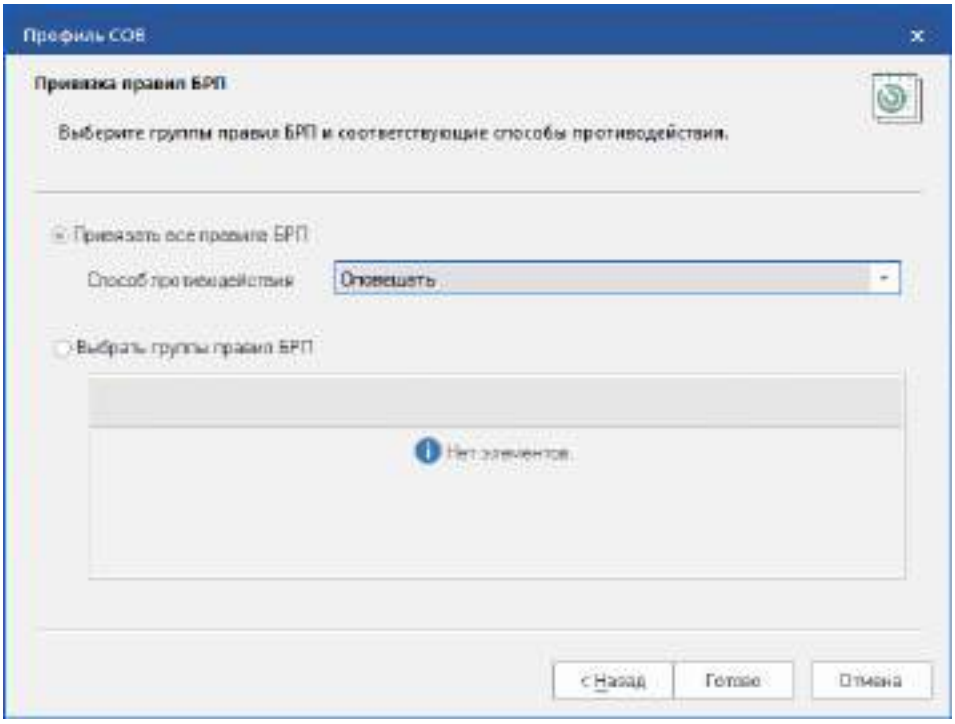
   Примечание. По умолчанию для всех приложений установлено значение "Оповещать".

6. При необходимости настроить список исключений для сетевых объектов, на которые не будет распространятся контроль приложений, нажмите кнопку "Добавить" , выберите тип исключения (одиночный/групповой) и укажите IP-адреса и описания (при необходимости) этих объектов.

   Примечание. Исключение будет действовать как для входящего, так и для исходящего трафика от указанных IP-адресов.

7. Нажмите кнопку "Далее".

   На экране появится диалог привязки правил БРП для установки их способа противодействия по умолчанию .



8. Выберите тип установки привязки (для всех правил или групп правил по отдельности), а затем способы противодействия по умолчанию, для чего в соответствующих полях в правой части экрана выберите нужные значения из раскрывающегося списка. Нажмите кнопку "Готово".

Примечание. Доступны для выбора следующие варианты противодействия:

- "Блокировать" — исключение пакетов данных трафика по сработавшему правилу (только в режиме Inline);
- "Оповещать" — пропуск трафика без изменений, но с оповещением служб мониторинга;
- "Пропустить" — пропуск трафика без изменений и оповещения служб мониторинга;
- "Отключить" — отключение контроля трафика по данному правилу.

В результате будет создан новый профиль, параметры которого отобразятся в списке на экране, а в подразделе "База решающих правил" в таблице со списком решающих правил появится колонка с названием созданного профиля.

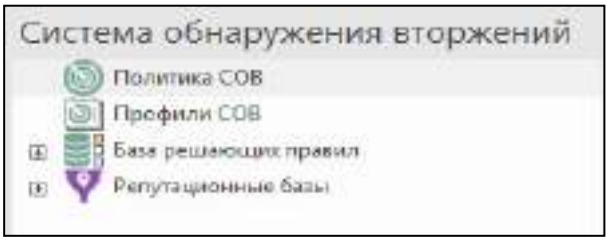
Примечание. Если новая колонка с созданным профилем не появилась — нажмите кнопку "Обновить".

Формирование политики

Для формирования политики создайте правило или список правил.

Для создания правила:

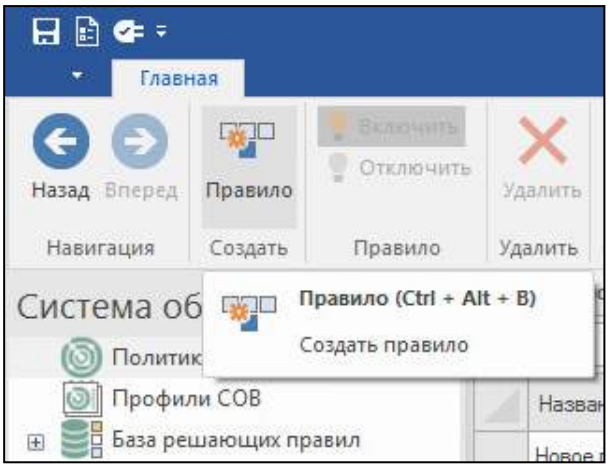
1. В разделе "Система обнаружения вторжений" перейдите на вкладку "Политика СОВ".



Справа отобразится список правил.

Примечание. Если правила не создавались, список будет пустым.

2. Добавьте новое правило. Для этого нажмите в панели инструментов кнопку "Создать правило".



В списке правил появится строка нового правила.

3. Настройте параметры нового правила. Для этого выделите поле в строке правила и укажите нужное значение.

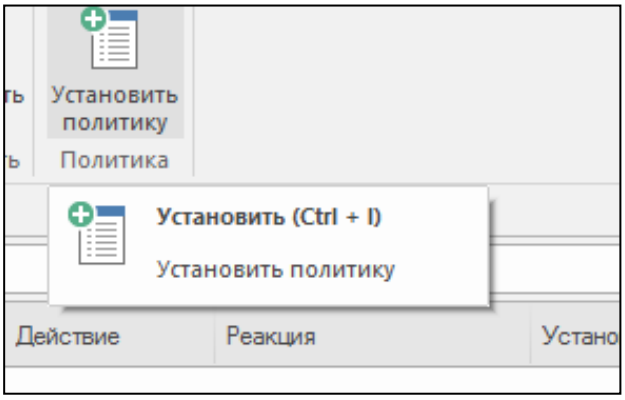
Название	Введите название правила
Профиль СОВ	Выберите профиль из списка
Установить	Выберите из списка ДА, которому должна быть назначена политика
Описание	Введите описание или пояснение к данному правилу

Для добавления другого правила в политику повторите описанную выше процедуру.

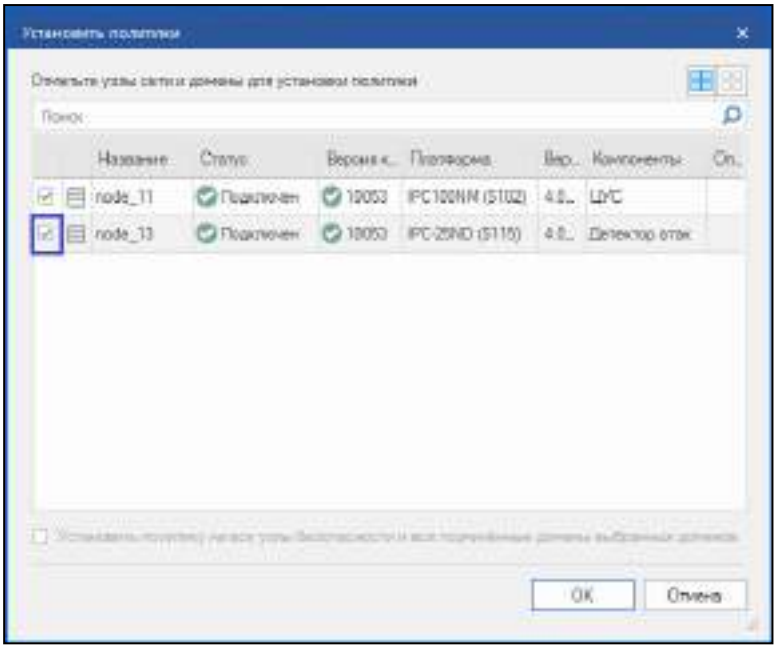
Применение политики

Для применения политики:

1. Нажмите в панели инструментов кнопку "Установить политику".



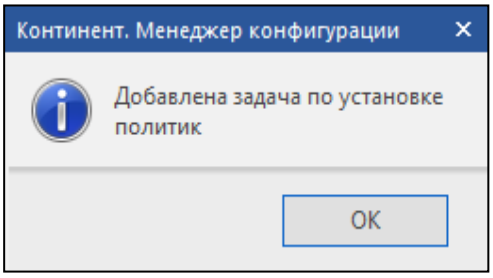
На экране появится окно "Установить политики".



2. Выберите в списке детекторы атак, на которые необходимо установить политику, установите отметку слева от названия и нажмите кнопку "OK".

   Примечание. Можно выделить сразу все узлы (или снять выделение со всех узлов), используя соответствующие кнопки в верхнем правом углу окна.

   Начнется процесс сохранения конфигурации комплекса на ЦУС и добавления в очередь задачи по установке политики на выбранные узлы, после чего на экране появится соответствующее сообщение.



3. Нажмите кнопку "OK" в окне сообщения.

Приложение

Установка CRL-сертификата

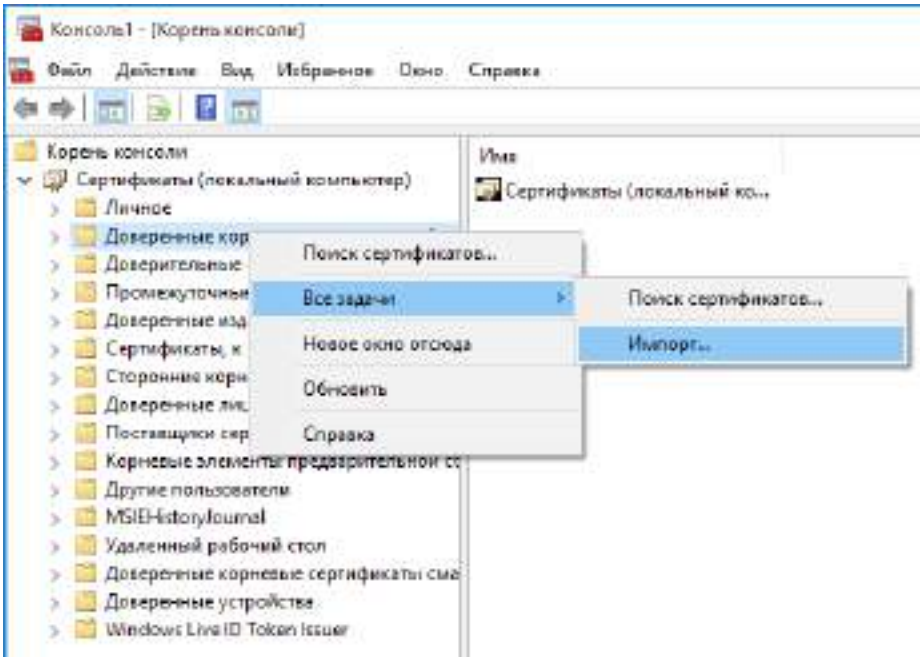
Установку CRL- сертификата в хранилище сертификатов Windows, расположенное на локальном компьютере, можно выполнить в консоли управления Microsoft (MMC). Для этого нужно добавить соответствующую оснастку и осуществить импорт CRL-файла в доверенные корневые центры сертификации.

Для подключения оснастки "Сертификаты" в консоли MMC:

1. Откройте окно команды "Выполнить", нажав сочетание клавиш "Win"+"R".
2. Введите mmc и нажмите клавишу <Enter>. Обратите внимание, что для просмотра сертификатов в хранилище локального компьютера необходимо иметь роль администратора.
3. В меню "Файл" выберите команду "Добавить или удалить оснастку...".
4. В открывшемся диалоговом окне "Добавление или удаление оснасток" в списке доступных оснасток выберите "Сертификаты".
5. Нажмите кнопку "Добавить >".
6. В диалоговом окне "Оснастка диспетчера сертификатов" установите переключатель в положение учетной записи компьютера и нажмите кнопку "Далее".
7. В диалоговом окне "Выбор компьютера" нажмите кнопку "Готово".
8. В диалоговом окне "Добавление или удаление оснасток" нажмите кнопку "ОК".
9. В корне консоли откройте узел "Сертификаты (локальный компьютер)", чтобы просмотреть хранилища сертификатов для данного компьютера.
10. В меню "Файл" выберите команду "Сохранить как...", укажите место сохранения командной консоли для последующих импортов CRL-файлов и нажмите кнопку "Сохранить".

Для импорта CRL-файла:

1. Откройте командную консоль и раскройте дерево сертификатов локального компьютера.
2. Выберите пункт "Доверенные корневые центры сертификации" и вызовите его контекстное меню.
3. Выберите команду "Все задачи | Импорт".



На экране появится окно мастера импорта сертификатов.

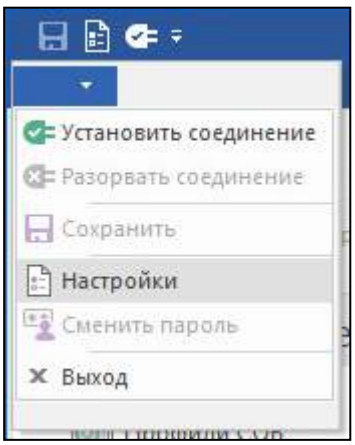
4. Нажмите кнопку "Далее" и в диалоговом окне импортируемого файла нажмите кнопку "Обзор...".
5. В открывшемся диалоге выбора файла укажите тип открываемого сертификата, путь к CRL-файлу, выберите нужный файл и нажмите кнопку "Открыть".
6. В диалоговом окне импортируемого файла нажмите кнопку "Далее".
7. В диалоговом окне выбора хранилища сертификатов укажите автоматический выбор и нажмите кнопку "Далее".
8. В завершающем диалоговом окне мастера импорта сертификатов нажмите кнопку "Готово".

Настройка профилей подключения

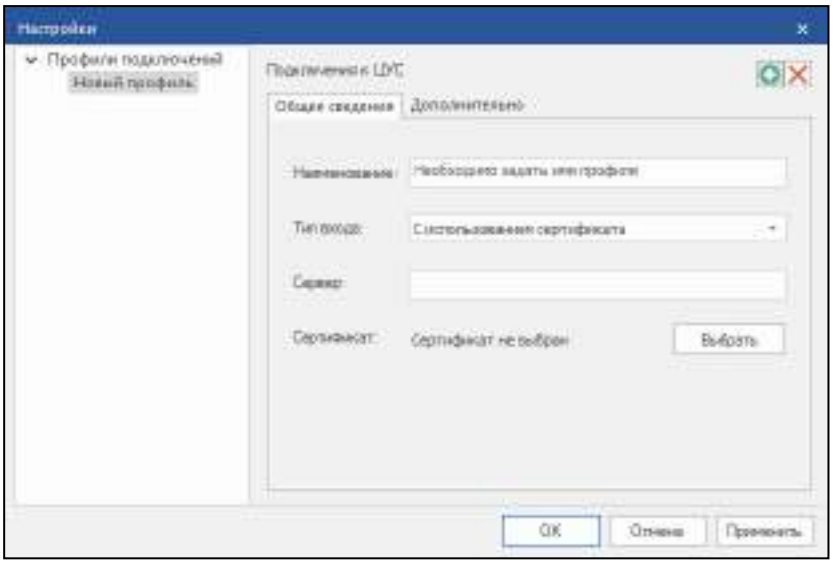
Для подключения Менеджера конфигурации к различным ЦУС необходимо для каждого из них настроить свой профиль подключения.

Для настройки профилей подключения:

1. Запустите Менеджер конфигурации и при появлении окна "Аутентификация администратора" закройте его.
2. В главном окне интерфейса Менеджера конфигурации в строке с закладкой "Главная" разверните контекстное меню и выберите пункт "Настройки".



На экране появится окно "Настройки", предназначенное для настройки профилей подключения к ЦУС.



В левой части окна расположен список профилей подключения к ЦУС.

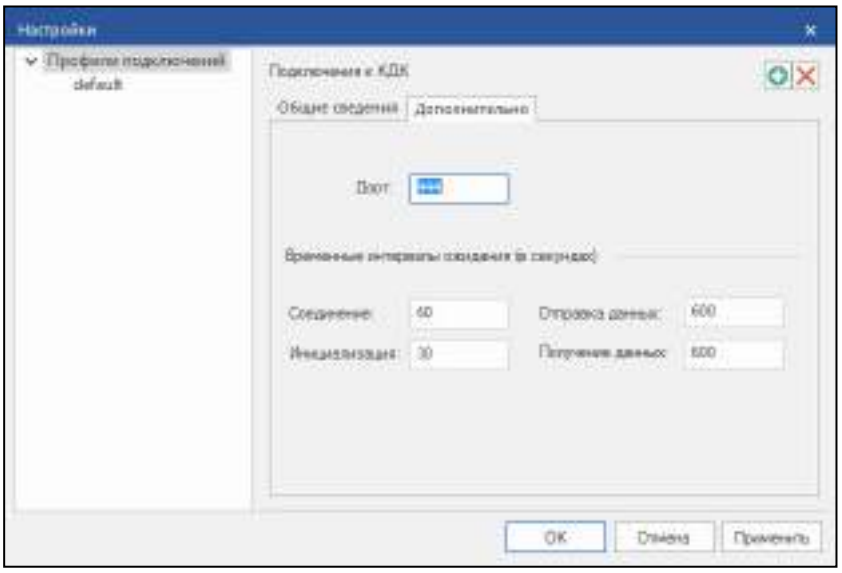
Примечание. Если профили не создавались, список будет пустым.

В правой части окна выполняют настройку параметров профилей.

3. Для создания нового профиля в правой части окна нажмите кнопку "Добавить соединение".

   В левой части окна в списке появится новый профиль подключения .

4. В правой части окна на вкладке "Общие сведения" укажите параметры нового профиля подключения и перейдите на вкладку "Дополнительно".



На вкладке отображаются дополнительные параметры, задаваемые по умолчанию для нового профиля подключения .

5. При необходимости измените значения дополнительных параметров.
6. После настройки параметров профиля подключения нажмите кнопку "Применить", расположенную в нижней части окна.
7. Если необходимо создать другой профиль подключения, нажмите кнопку "Добавить соединение" и выполните его настройку, как описано выше.
8. Закройте окно "Настройки".

Документация

1. Программный комплекс "Континент-СОВ". Версия 4. Руководство администратора. Система обнаружения вторжений.