КОД безопасности

Программный комплекс

Континент-СОА
Версия 4

Руководство администратора

Обнаружение вторжений

RU.АМБС.58.29.12.008 90 2

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

Оглавление

Список сокращений ... **5**

Введение ... **6**

Общие сведения ... **7**
- Назначение и основные функции комплекса ... 7
- Функции ЦУС ... 7
- Описание работы детектора атак ... 8
- Примеры типовых схем использования ДА ... 10
  - Мониторинг трафика ... 10
  - Противодействие обнаруженным вторжениям (атакам) ... 11
- Концепция эксплуатации СОВ ... 11

Администрирование комплекса ... **13**
- Управление ролями администраторов ... 14
  - Просмотр роли ... 14
  - Создание роли ... 15
  - Редактирование роли и назначение ее администраторам ... 17
  - Удаление роли ... 17
- Управление учетными записями ... 17
  - Просмотр учетных записей администратора ... 17
  - Создание учетной записи администратора ... 18
  - Удаление учетной записи администратора ... 20
- Назначение роли администратору ... 21

Аутентификация администраторов ... **22**
- С использованием ПАК "Соболь" ... 23
- С использованием пароля ... 23
- С использованием сертификата ... 24
- Блокировка администратора ... 24
  - Выбор режима работы при локальной аутентификации ... 24
  - Выбор режима работы при аутентификации через Менеджер конфигурации ... 25

Лицензии комплекса ... **26**
- Просмотр лицензий ... 26
- Управление лицензиями ... 27

Управление узлами безопасности ... **29**
- Просмотр свойств ... 29
- Диагностика работы комплекса ... 30
- Сетевые настройки ... 30
  - Настройка IP-адреса ... 31
  - Смена IP-адреса ... 32
  - Настройка DNS ... 33
  - Настройка статической маршрутизации ... 34
  - Настройка ARP-проксирования ... 36
- Настройка дистанционного доступа по протоколу SSH ... 37
  - Настройка SSH-клиента на примере клиентской программы PuTTY ... 38
- Контроль узлов безопасности по протоколу SNMP ... 40
- Управление конфигурацией узла безопасности ... 41
  - Передача сведений об изменении конфигурации ... 41
  - Сохранение конфигурации ЦУС ... 42
- Установка политики ... 43
  - Установка политики ... 43
  - Учет конфигураций узлов ... 44
  - Список задач ... 45
- Перезагрузка и выключение ... 46
- Удаление ... 47

Настройка СОВ ... **48**

Настройка параметров СОВ ... 48
Настройка ДА по схеме Inline (интерфейсы, режим bypass, хранение трафика атаки) ... 51
Настройка ДА по схеме Monitor (интерфейсы и хранение трафика атаки) ... 52
Создание и настройка профиля СОВ ... 52
Создание и настройка правил политики СОВ ... 55
Управление БРП ... 56
Обновление БРП ... 56
Создание пользовательского решающего правила ... 58

Обеспечение отказоустойчивости комплекса ... 61
Резервное копирование и восстановление ... 61
Создание резервной копии ... 61
Восстановление из резервной копии ... 62
Управление резервными копиями ... 64

Обновление программного обеспечения ... 65
Управление репозиторием обновлений ... 65
Обновление ПО УБ ... 67
Обновление Менеджера конфигурации ... 67

Сертификаты безопасности комплекса ... 70
Просмотр сертификатов ... 70
Создание сертификатов ... 71
Создание корневых сертификатов ... 71
Создание сертификатов управления УБ ... 72
Создание сертификатов администратора ... 74
Установка сертификатов администратора ... 75
Смена сертификатов ... 77
Экспорт сертификатов ... 78
Импорт сертификатов и ключей безопасности ... 78
Смена сертификата управления ... 79

Приложение ... 80
Запуск Менеджера конфигурации ... 80
Полномочия встроенных ролей администратора ... 81
Протоколы и порты ... 83
Решающие правила ... 83
Синтаксис правила ... 83
Заголовок правила ... 84
Опции правил ... 85
Управление записью сетевого трафика ... 86
Настройка тайм-аута неактивности ... 86

Документация ... 88

Список сокращений

БД	База данных
БРП	База решающих правил
ДА	Детектор атак
МК	Менеджер конфигурации
МЭ	Межсетевой экран
ОЗУ	Оперативное запоминающее устройство
СОВ	Система обнаружения вторжений (компьютерных атак)
СУ	Стороннее устройство
УБ	Узел безопасности
УК	Узел коммутации
УМ	Узел маршрутизации
ЦУС	Центр управления сетью
DNS	Domain Name System
FTP	File Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IP	Internet Protocol
RPC	Remote Procedure Call
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VPN	Virtual Private Network

Введение

Документ предназначен для администраторов изделия "Программный комплекс "Континент-СОА". Версия 4" RU.АМБС.58.29.12.008 (далее — комплекс, ПК "Континент-СОА"). В нем содержатся сведения, необходимые администраторам для управления системой обнаружения вторжений.

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.

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.

Глава 1
Общие сведения

Назначение и основные функции комплекса

Средство обнаружения атак (далее — система обнаружения вторжений) предназначена для обнаружения основных угроз безопасности информации, относящихся к вторжениям (атакам).

Основным компонентом СОВ является детектор компьютерных атак (детектор атак, ДА), который реализует следующие функции:

- сбор информации о пакетах данных;
- анализ сетевого трафика с использованием сигнатурного и эвристического методов обнаружения вторжений;
- выборочный контроль отдельных объектов сети;
- оповещение ЦУС о своей активности и о событиях, требующих оперативного вмешательства в режиме реального времени;
- противодействие вторжениям в Inline-режиме;
- запись дампа атаки;
- поддержка программного bypass-режима;
- идентификация и аутентификация администратора для управления ДА;
- контроль целостности программного обеспечения и конфигурации ДА;
- регистрация событий, связанных с работой ДА;
- контроль приложений с использованием белого списка IP-адресов (DNS-имен), на которые контроль не распространяется.

Функции ЦУС

В состав комплекса входит ЦУС, который представляет собой программно-аппаратный компонент комплекса, обеспечивающий централизованное управление работой всех подчиненных УБ.

По команде администратора УБ все локальные изменения настроек отправляются на ЦУС, где они встают в очередь на запись в БД ЦУС под своим порядковым номером. После подтверждения администратором ЦУС эти изменения прописываются в БД ЦУС.

Наряду с основными функциями управления узлами ЦУС имеет ряд дополнительных возможностей:

- Использование встроенной в ЦУС системы мониторинга и аудита с доступом из веб-браузера.
- Гибкое управление ролями и учетными записями администраторов с автоматизированным распространением служебной информации на подчиненные узлы.
- Управление СОВ, сертификатами и лицензиями.
- Отдельная БД, хранящая активную конфигурацию ЦУС и всех подчиненных узлов.
- Осуществление мониторинга состояния узлов, запись событий в БД мониторинга и аудита.
- Отсутствие необходимости развертывания отдельной БД для хранения журналов.

Применение ЦУС является самодостаточным решением для управления и мониторинга состояния комплекса с единым центром управления.

Описание работы детектора атак

Детектор атак представляет собой программное средство, предварительно установленное на специализированной аппаратной платформе с архитектурой x64, осуществляющее выявление компьютерных атак на основе анализа сетевого трафика.

Детектор атак контролирует следующие данные о сетевом трафике:

- сетевой адрес отправителя и получателя;
- используемый порт отправителя и получателя;
- значения полей сетевого пакета (флаги);
- аппаратный адрес устройства (при отсутствии сетевого адреса);
- идентификаторы протоколов;
- последовательность команд протоколов;
- размер полей пакета;
- интенсивность трафика;
- содержимое пакета.

ДА может обнаружить следующие классы атак:

- вредоносные командные центры;
- фишинг;
- потенциально опасный трафик;
- криптолокеры;
- предоносное ПО для мобильных приложений;
- бэкдоры;
- эксплойты;
- программы — загрузчики вредоносных файлов;
- потенциально опасные SSL-сертификаты;
- криптомайнеры;
- повышение привилегий;
- шпионское ПО;
- уязвимые приложения;
- веб-атаки;
- рекламное ПО;
- DoS-атаки;
- нарушение политики безопасности;
- шелл-коды;
- сетевые сканеры;
- сетевые черви;
- утечка информации;
- ложные антивирусы.

Анализ данных с целью обнаружения вторжений осуществляется с использованием сигнатурного и эвристического методов.

Метод сигнатурного анализа основан на применении набора решающих правил, предварительно загруженного в базу данных ДА при установке на него политики СОВ, сформированной на ЦУС на основе БРП.

При сигнатурном анализе поддерживаются протоколы следующих уровней:

- сетевого уровня (ICMPv4, ICMPv6, IPv4, IPv6);
- транспортного уровня (TCP, UDP, SCTP);
- канального уровня (PPPoE, PPP);
- прикладного уровня (FTP, HTTP, SMB, SSH, SMTP);

- сеансового уровня (SSL, DCE/RPC).

Эвристический анализ выявления аномалий сетевого трафика может применяться в дополнение к сигнатурному анализу. При этом используются настройки эвристического анализатора, заданные по умолчанию.

При эвристическом анализе поддерживаются протоколы прикладного уровня с возможностью контроля приложений:

- интернет-мессенджеры (Skype, ICQ, Jabber, IRC, SIP, WhatsApp);
- удаленного управления (TeamViewer, RDP, VNC);
- сетевого вещания (Icecast, PPLive, PPStream, Zattoo, SHOUTCast, SopCast, TVAnts, TVUplayer, VeohTV, QQLive);
- со скрытой передачей данных (Tor, Bittorrent, HTTP Application Activesync, RemoteScan);
- процесса туннелирования (IP in IP, GRE, STUN, SSL (в том числе инкапсулированные в HTTP), SSH (в том числе инкапсулированные в HTTP));
- компьютерных игр (Warcraft3, World of Kung Fu, Steam, Halflife2, World of Warcraft, Battlefield, Quake, Thunder/Webthunder);
- поисковых систем, социальных сетей и др. (Google, YouTube, Gmail, Google Maps, FaceBook, Twitter).

События, связанные с работой ДА и обнаружением вторжений, регистрируются в локальных журналах ДА и передаются на ЦУС.

Просмотр событий осуществляется в программе мониторинга. Кроме того, в случае обнаружения вторжения или нарушения безопасности администратору может отсылаться сообщение по электронной почте, а в системе мониторинга визуально отображается событие несанкционированного доступа.

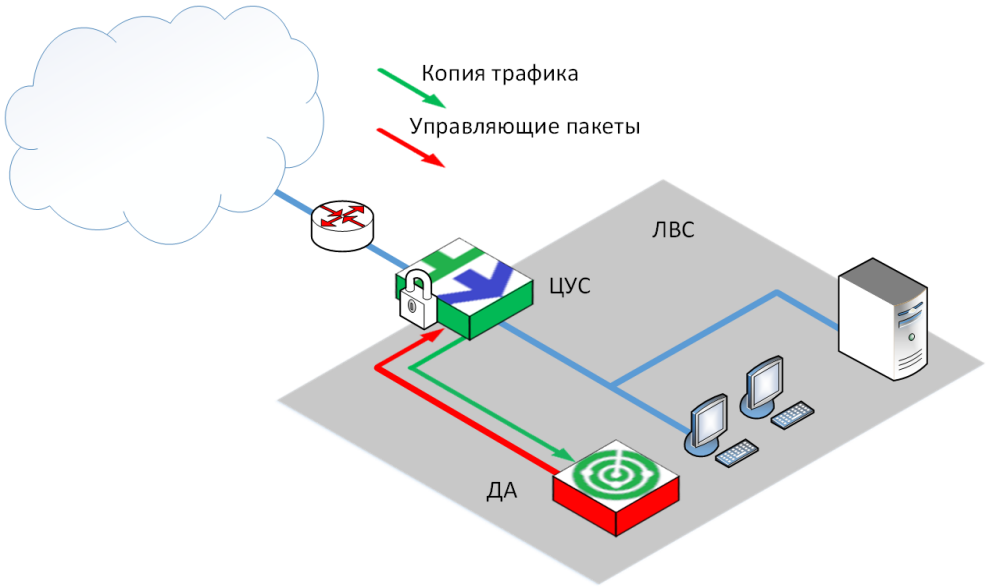
Возможны следующие режимы работы ДА:

- Monitor

  В этом режиме трафик зеркалируется на ДА со SPAN-порта СУ, в роли которого может выступать коммутатор, маршрутизатор или УБ.

  Захват трафика осуществляется с одного или нескольких физических интерфейсов.

  В случае обнаружения атаки ДА фиксирует атаку и отправляет сведения о ней на ЦУС.

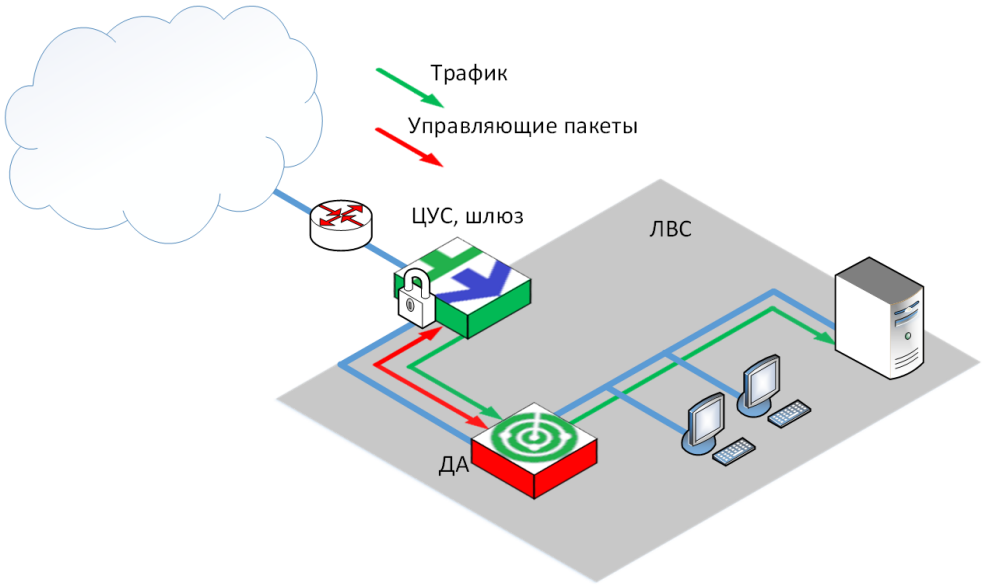


- Inline

  В этом режиме ДА устанавливается "в разрыв" сетевого соединения между сервером интернета и защищаемой сетью. В случае выхода из строя ПО анализатора трафика ДА перейдет в программный Bypass-режим для беспрепятственного прохождения трафика.

Захват трафика, а также отправка обработанного трафика осуществляются с использованием физических интерфейсов. Допускается организация работы с несколькими парами интерфейсов.

В случае обнаружения атаки ДА фиксирует атаку и, если прописано в политике СОВ, сам блокирует вредоносный трафик. Сведения об атаке отправляются в ЦУС.

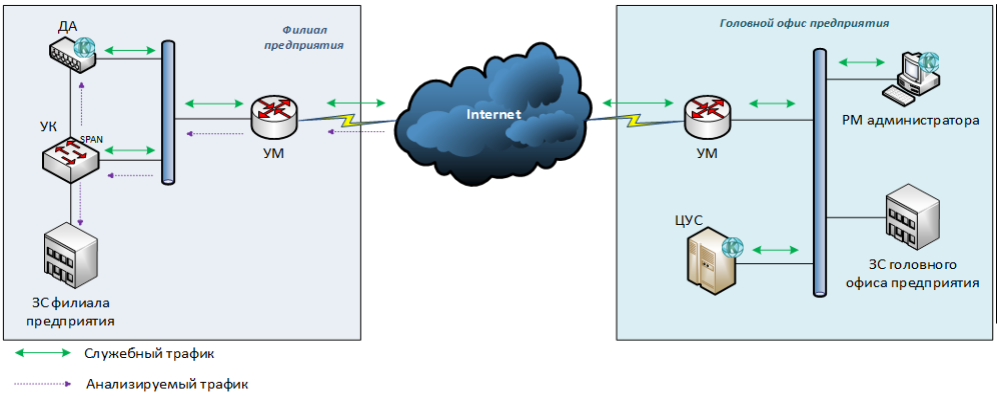


Примеры типовых схем использования ДА

Внимание! Для связи между компонентами комплекса используются заранее определенные протоколы и порты. Если на пути зашифрованного трафика находятся межсетевые экраны или другое оборудование, осуществляющее фильтрацию IP-пакетов, необходимо создать для них правила, разрешающие прохождение служебных пакетов комплекса по протоколам и портам, указанным в Приложении (см. стр. 83).

Мониторинг трафика

Ниже представлена схема использования детектора атак для мониторинга трафика.



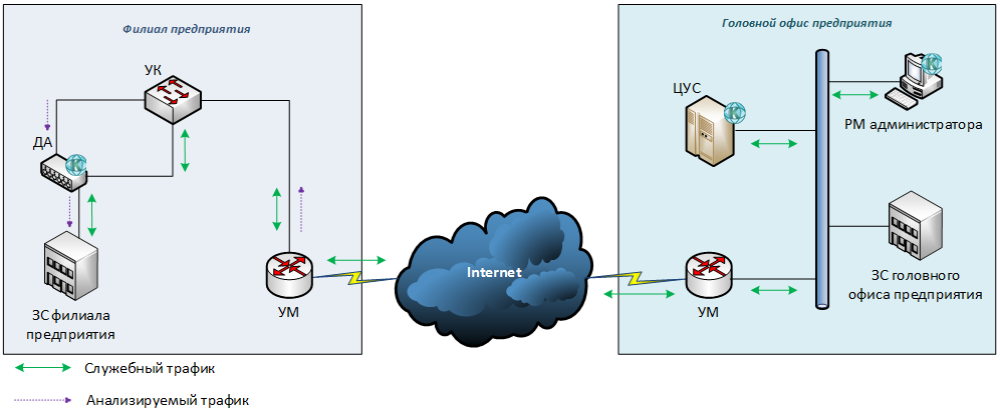
Для развертывания данной схемы требуется инициализация и настройка следующих компонентов:

- ЦУС;
- ДА в режиме Monitor;
- сторонний УК, поддерживающий зеркалирование трафика;
- сторонний пограничный УМ;

- программный компонент "Менеджер конфигурации" на РМ администратора для управления устройствами комплекса с помощью графического интерфейса.

Противодействие обнаруженным вторжениям (атакам)

Ниже представлена схема использования детектора атак для противодействия обнаруженным вторжениям (атакам).



Для развертывания данной схемы требуется инициализация и настройка следующих устройств:

- ЦУС;
- ДА в режиме Inline;
- сторонние пограничные УМ;
- сторонний УК;
- программный компонент "Менеджер конфигурации" на РМ администратора для управления устройствами комплекса с помощью графического интерфейса.

Концепция эксплуатации СОВ

Анализ данных СОВ осуществляется с использованием сигнатурного метода, основанного на применении набора решающих правил. БРП предварительно загружается в ЦУС, а затем определенный набор этих правил привязывается к профилю СОВ. Для применения этого набора правил на ДА администратор формирует правило политики СОВ, содержащее нужный профиль СОВ, и назначает его на этот ДА.

Профиль СОВ также содержит настраиваемый эвристический анализатор для контроля трафика приложений.

Предоставляемый вендорский набор БРП предварительно разбит по группам. Редактирование вендорского правила или набора не предусмотрено. Администратор СОВ имеет возможность создания и редактирования пользовательских решающих правил и их групп. В качестве основы пользовательского правила может выступить любое вендорское правило (см. стр. **60**).

Каждое решающее правило определяет действие (alert — "оповещать", drop — "блокировать", pass — "пропустить"), которое должно быть выполнено при срабатывании сигнатуры атаки, для каждого профиля СОВ в отдельности. Администратор СОВ имеет возможность изменить в решающем правиле или в профиле СОВ тип действия на обнаруженную атаку, но при этом стоит учитывать режим работы ДА, так как в режиме Monitor ДА может только оповещать администратора об обнаруженной угрозе, тогда как в режиме Inline предусматривается возможность использовать любой тип противодействия.

Синтаксис написания решающего правила приведен в Приложении (см. стр. **83**).

Настройка СОВ

Для настройки работы СОВ необходимо выполнить следующие действия:

1. Загрузить в репозиторий лицензию на ДА (см. стр. **26**).
2. Настроить параметры работы ДА по соответствующей схеме включения (см. стр. **48**).
3. Сформировать набор пользовательских решающих правил (см. стр. **58**).
4. Создать и настроить профиль СОВ (см. стр. **52**).
5. Создать правила политики СОВ (см. стр. **55**).
6. Сохранить выполненные настройки (см. стр. **42**).
7. Установить политику на ДА и ЦУС (см. стр. **43**).

Глава 2
Администрирование комплекса

Управление комплексом осуществляют администраторы в соответствии с назначенными им ролями.

Первичная учетная запись администратора создается при инициализации ЦУС и имеет полный набор всех возможных прав на управление ЦУС и входящими в его домен узлами безопасности.

Примечание. Все учетные записи изначально не обладают правом дистанционного доступа к управлению ЦУС по протоколу SSH (см. стр. 37).

В комплексе используются два типа ролей администраторов:

- предустановленная — роль с фиксированным набором привилегий, которую запрещено редактировать или удалять;
- пользовательская — роль с настраиваемым набором привилегий, которую может создавать и редактировать администратор Менеджера конфигурации.

Предусмотрены четыре встроенные роли:

- главный администратор;
- администратор безопасности;
- администратор сети;
- администратор аудита.

Роль администратору может быть назначена одним из двух способов:

- при создании администратора или редактировании его учетной записи;
- при создании или редактировании роли (удобно для расширения доступных привилегий группе администраторов).

Администратору может быть назначено несколько ролей, как встроенных, так и пользовательских. При этом администратор получает привилегию, если она открыта хотя бы в одной из присвоенной ему ролей.

Внимание! При создании или изменении роли или учетной записи администратора происходит автоматическая установка политики на все подключенные узлы домена. Для применения изменений в администрировании ранее отключенных узлов следует установить политику на эти узлы (см. стр. 43) после их включения.

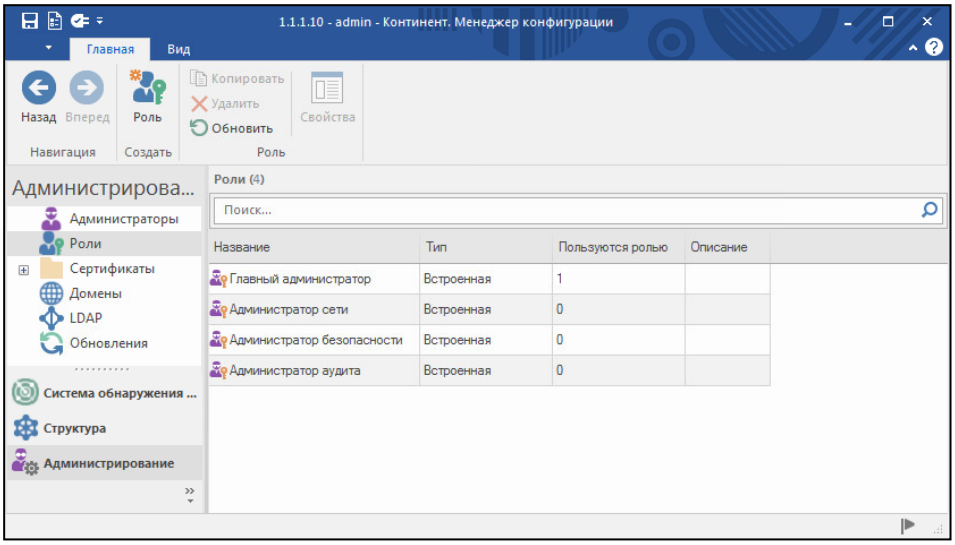
Управление ролями администраторов

Просмотр роли

Для просмотра роли:

1. В Менеджере конфигурации перейдите в раздел "Администрирование" и выберите подраздел "Роли".

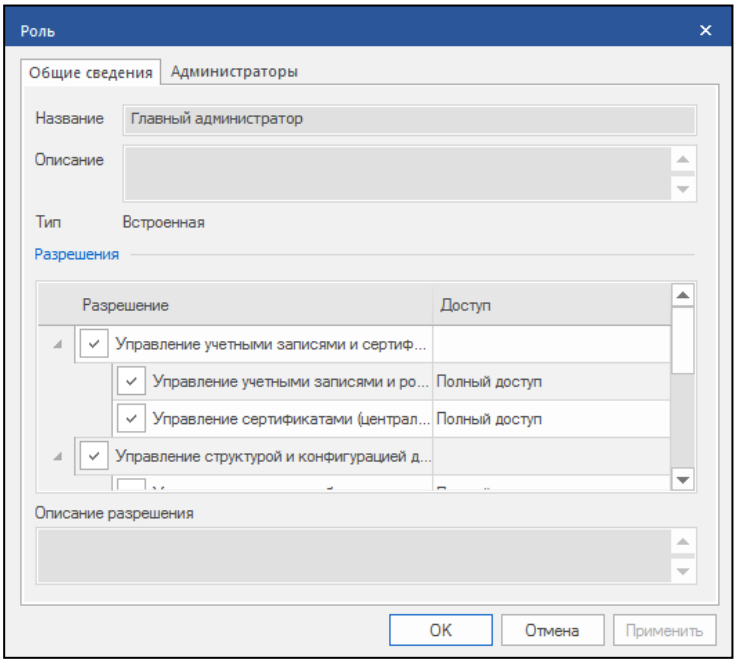
   В правой части окна отобразится список ролей администраторов.



   Для каждой роли указаны тип (встроенная или пользовательская) и количество администраторов, которым назначена данная роль.

2. Для просмотра привилегий какой-либо из ролей выберите ее в списке и нажмите на панели инструментов кнопку "Свойства".

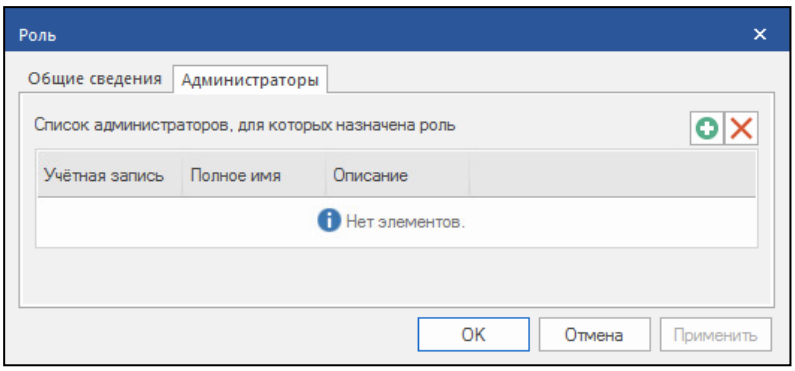
   На экране появится окно "Роль" с описанием привилегий выбранной роли. Окно содержит две вкладки: "Общие сведения" и "Администраторы".



   Вкладка "Общие сведения" предназначена для просмотра и редактирования привилегий данной роли.

Внимание! Редактирование привилегий доступно только для роли типа "пользовательская". Описание редактирования роли см. стр. 17.

3. Для просмотра списка администраторов, которым назначена данная роль, перейдите на вкладку "Администраторы".



На вкладке "Администраторы" предусмотрено назначение данной роли другим администраторам.

4. После просмотра сведений о роли нажмите кнопку "OK" или "Отмена".

Окно "Роль" закроется.

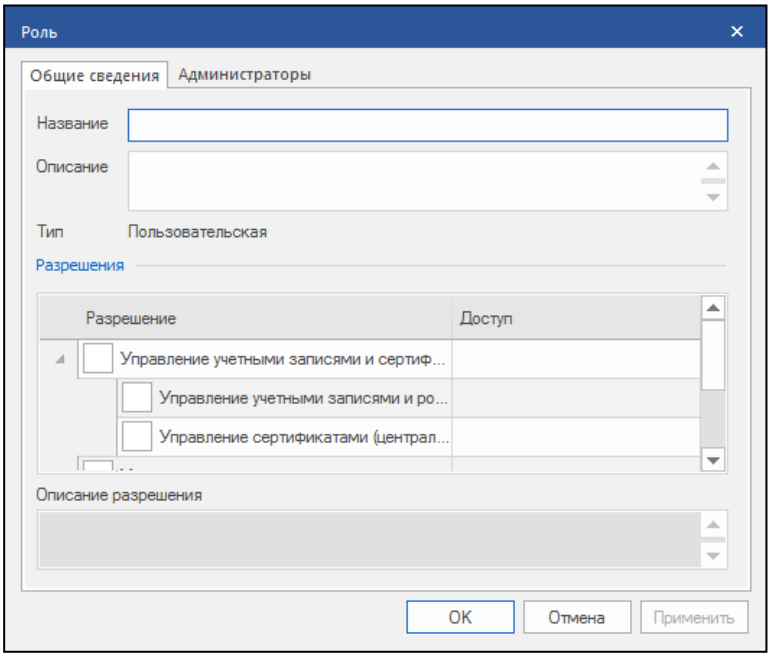
Создание роли

Внимание! При создании роли рекомендуется не присваивать ее сразу администраторам, а предварительно сохранить изменения в конфигурации ЦУС (см. стр. 42).

Для создания новой роли:

1. В Менеджере конфигурации на панели инструментов подраздела "Администрирование/Роли" нажмите кнопку "Роль".

На экране появится окно "Роль".

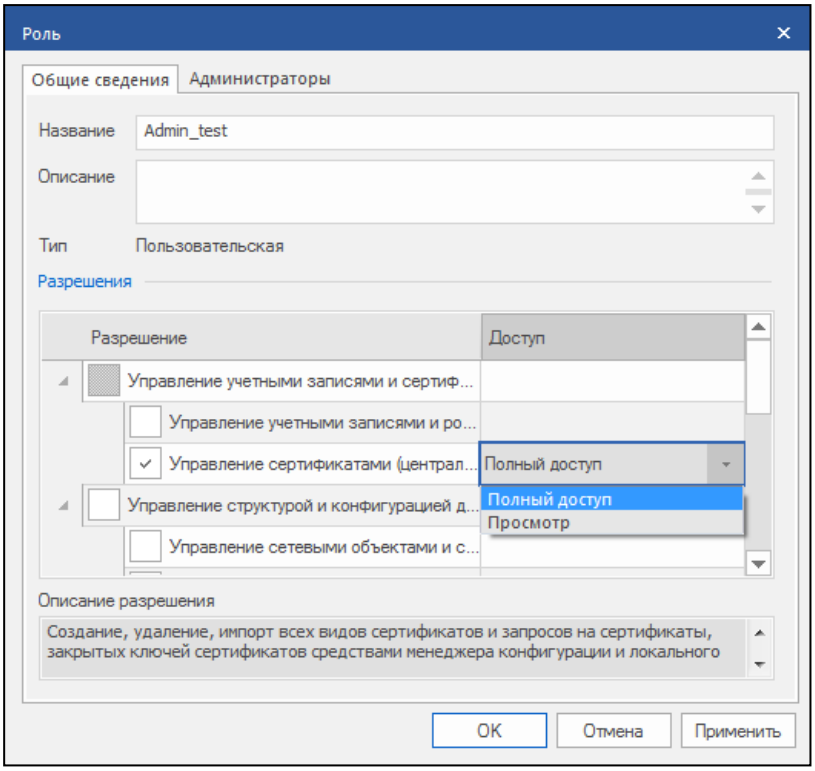


2. Введите название создаваемой роли и краткое описание.

Примечание. Создаваемая роль автоматически становится пользовательской.

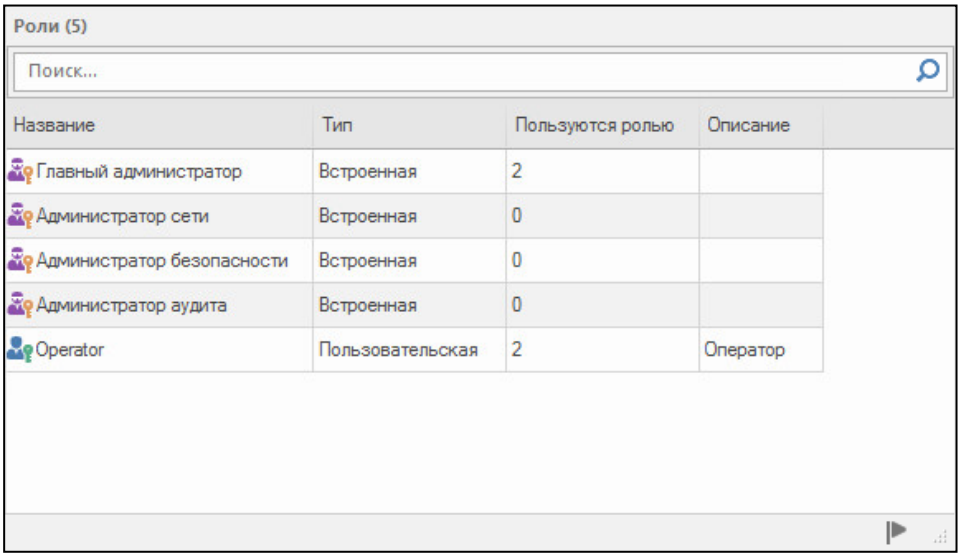
3. Установите отметки у требуемых разрешений и укажите тип доступа: полный доступ или просмотр.

Примечание. Привилегии групп "Локальное управление" и "Мониторинг и диагностика" могут быть предоставлены только при полном уровне доступа.



4. Выполните настройку всех необходимых привилегий и нажмите кнопку "Применить".
5. Для завершения процедуры нажмите кнопку "ОК".

   Окно "Роль" закроется, и в списке появится новая роль. При этом будет сформирована задача по автоматической установке политики на все подключенные узлы домена.



6. Для сохранения изменений в конфигурации ЦУС в левом верхнем углу окна Менеджера конфигурации нажмите на иконку сохранения настроек.

Появится окно сохранения настроек. Дождитесь завершения процесса.

Редактирование роли и назначение ее администраторам

Редактирование роли включает в себя изменение набора привилегий и их доступа. Редактированию подлежат только пользовательские роли. Назначать администраторам можно как пользовательские, так и встроенные роли.

Для редактирования роли:

1. В подразделе "Администрирование/Роли" Менеджера конфигурации выберите роль и на панели инструментов нажмите кнопку "Свойства".

   На экране появится окно "Роли" с описанием привилегий выбранной роли.
2. Внесите необходимые изменения (см. стр. **15**).
3. Если необходимо назначить данную роль кому-либо из администраторов, перейдите на вкладку "Администраторы" и нажмите кнопку  .

   Примечание. Если роль была только что создана, то перед присвоением ее администратору необходимо сохранить изменения в конфигурации ЦУС (см. стр. **42**).

   На экране появится список учетных записей зарегистрированных администраторов.
4. Выберите учетную запись, которой должна быть назначена роль.

   Учетная запись будет добавлена в список администраторов, которым назначена данная роль.
5. Для присвоения роли еще одному администратору повторите п. **4.**
6. В окне "Роль" нажмите кнопку "ОК".

   Параметры роли будут соответствующим образом изменены, после чего будет сформирована задача по автоматической установке политики на все подключенные узлы домена.

Удаление роли

Для удаления роли:

1. В подразделе "Администрирование/Роли" Менеджера конфигурации выберите роль и на панели инструментов нажмите кнопку "Удалить".

   На экране появится окно подтверждения удаления.
2. Нажмите кнопку "Да".

   Выбранная роль будет удалена, после чего будет сформирована задача по автоматической установке политики на все подключенные узлы.

Управление учетными записями

Просмотр учетных записей администратора

Для просмотра параметров учетной записи:

1. В Менеджере конфигурации перейдите в раздел "Администрирование" и выберите подраздел "Администраторы".

   В правой части окна отобразится список администраторов.

   В списке для каждого администратора указываются:

   - учетная запись;
   - домен;
   - полное имя;
   - назначенная роль;
   - описание (необязательно).
2. Для просмотра сведений об учетной записи администратора выберите ее в списке и нажмите на панели инструментов кнопку "Свойства".

На экране появится окно "Администратор", содержащее три вкладки: "Общие сведения", "Аутентификация" и "Роли".

Вкладка	Назначение
Общие сведения	Просмотр и редактирование параметров учетной записи: • имя учетной записи; • полное имя; • описание. Блокирование/разблокирование учетной записи
Аутентификация	Просмотр и задание способа и параметров аутентификации администратора: • аутентификация по паролю учетной записи; • аутентификация по сертификату
Роли	Просмотр и назначение ролей администратору

3. Для просмотра или изменения параметров перейдите на нужную вкладку.

   Описание возможных изменений параметров приведено в последующих подразделах.

4. После просмотра сведений нажмите кнопку "ОК" или "Отмена".

   Окно "Администратор" закроется.

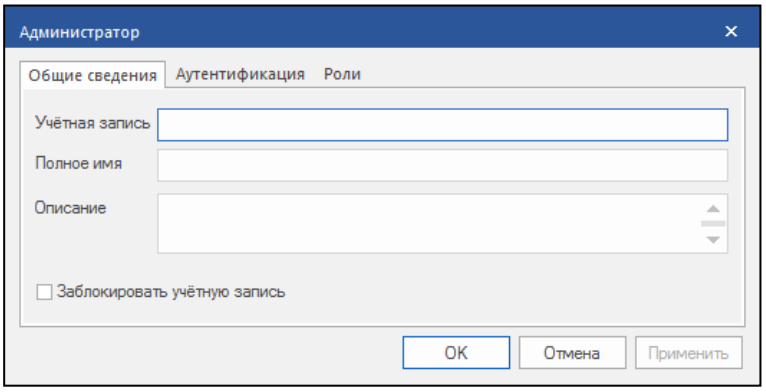
Создание учетной записи администратора

Для создания новой учетной записи администратора:

Внимание! Если для администратора предусматривается тип аутентификации по сертификату, необходимо предварительно выпустить сертификат администратора (см. стр. 74), а затем установить его в личное хранилище сертификатов администратора (см. стр. 75).

1. В Менеджере конфигурации перейдите в подраздел "Администрирование/ Администраторы" и на панели инструментов нажмите кнопку "Администратор".

   На экране появится окно "Администратор", открытое на вкладке "Общие сведения".

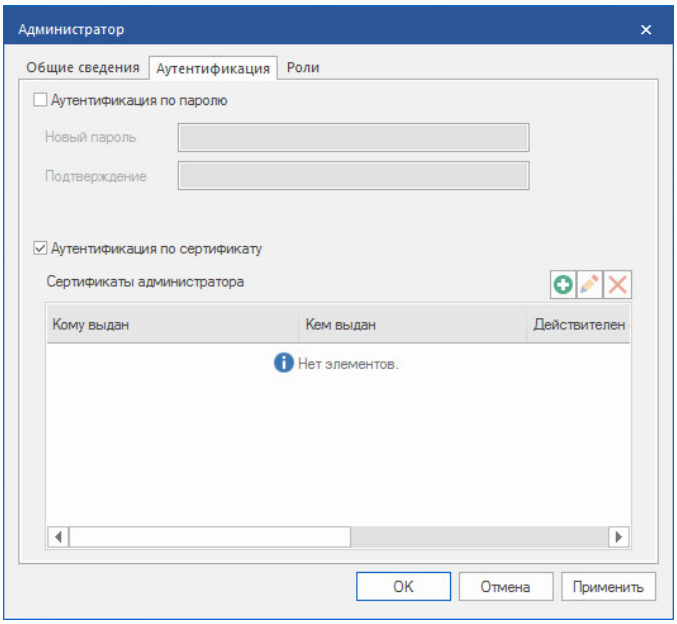


2. Введите имя учетной записи администратора, полное имя и краткое описание и нажмите кнопку "Применить".

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

Внимание! Следующие имена зарезервированы для использования в работе комплекса: "adm", "bin", "daemon", "dhcpd", "ftp", "games", "gopher", "halt", "ips", "lp", "mail", "monit", "nginx", "nobody", "ntp", "nxlog", "operator", "postgres", "quagga", "root", "shutdown", "sshd", "sync", "tcpdump", "uucp", "vcsa", "djdb".

Далее перейдите на вкладку "Аутентификация".



3. Если для администратора предусмотрен тип аутентификации по паролю, установите соответствующий флажок, укажите пароль и нажмите кнопку "Применить".

Примечание. Пароль администратора должен:

- состоять из цифр, латинских букв или следующих спецсимволов:

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

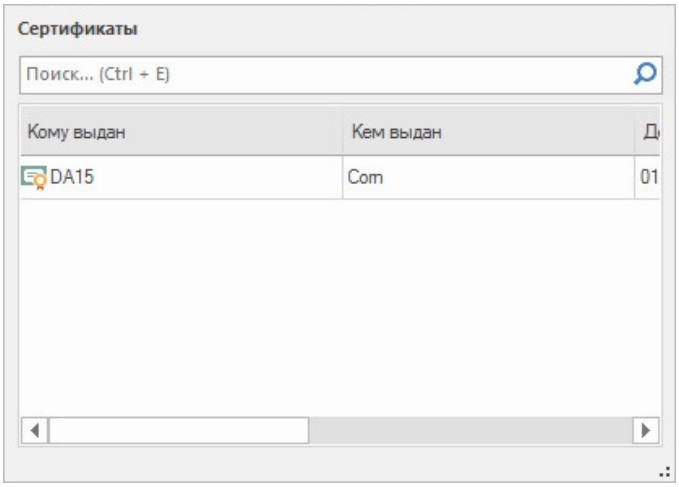
- соответствовать прочим правилам, установленным Политикой безопасности паролей (см. панель инструментов подраздела "Администрирование/Администраторы"). По умолчанию в ней заданы следующие дополнительные требования к паролю:
  - наличие как минимум одной цифры;
  - наличие как минимум одной строчной буквы;
  - запрет повторного использования в пароле подряд идущих 4 символов;
  - длина пароля не может быть меньше 8 символов.

4. Если для администратора не предусмотрен тип аутентификации по сертификату, перейдите к **п. 7**.

5. Установите флажок "Аутентификация по сертификату" и нажмите кнопку  .

На экране появится окно выбора сертификата.

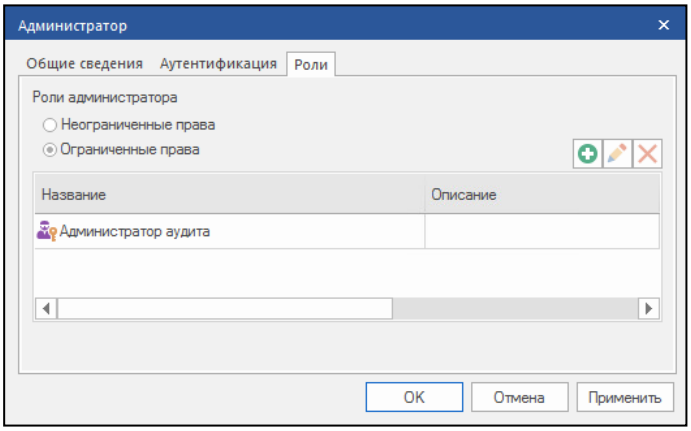
Внимание! При создании администратора с методом аутентификации "Аутентификация по сертификату" также необходимо настроить метод аутентификации "Аутентификацию по паролю". Пароль, должен соответствовать политике безопасности паролей.



6. Выберите требуемый сертификат и нажмите кнопку "Применить".
7. Перейдите на вкладку "Роли".
8. Для назначения роли администратору нажмите кнопку  .

   На экране появится список ролей.
9. Выберите роль в списке.

   Выбранная роль будет добавлена в список на вкладке "Роли".



   При необходимости добавьте другие роли.
10. После добавления ролей нажмите кнопку "ОК", расположенную в нижней части окна "Администратор".

    Окно "Администратор" закроется, и в списке администраторов появится новая учетная запись. При этом будет сформирована задача по автоматической установке политики на все подключенные узлы домена.

Удаление учетной записи администратора

Для удаления учетной записи администратора:

1. В подразделе "Администрирование/Администраторы" Менеджера конфигурации выберите нужную учетную запись администратора и на панели инструментов нажмите кнопку "Удалить".

   На экране появится окно подтверждения удаления.
2. Нажмите кнопку "Да".

   Выбранная учетная запись будет удалена, после чего будет сформирована задача по автоматической установке политики на все подключенные узлы домена.

Назначение роли администратору

Роль администратору может быть назначена одним из двух способов:

- при создании нового администратора или редактировании его учетной записи (см. процедуру создания нового администратора, стр. **18**);
- при создании или редактировании роли.

Для назначения роли при редактировании учетной записи:

1. Откройте список администраторов (см. стр. **17**), выберите учетную запись и нажмите кнопку "Свойства".

   На экране появится окно "Администратор".

2. Перейдите на вкладку "Роли" и добавьте роль (см. пп. **4**, **5** процедуры создания нового администратора, стр. **18**).

3. После добавления роли нажмите кнопку "Применить" в окне "Администратор".

Для назначения роли при ее редактировании:

Примечание. Если роль была только что создана, то перед присвоением ее администратору необходимо сохранить изменения в конфигурации ЦУС (см. стр. **42**).

1. Откройте список ролей (см. стр. **14**), выберите роль и нажмите кнопку "Свойства".

   На экране появится окно "Роль".

2. Перейдите на вкладку "Администраторы" и нажмите кнопку  .

   На экране появится список администраторов.

3. Выберите учетную запись, которой должна быть назначена роль.

   Учетная запись будет добавлена в список администраторов, которым назначена данная роль.

4. В окне "Роль" нажмите кнопку "Применить".

Глава 3
Аутентификация администраторов

Аутентификация администраторов в локальном меню осуществляется либо по имени учетной записи и паролю, либо с помощью ПАК "Соболь".

Аутентификация администраторов в Менеджере конфигурации осуществляется либо по имени учетной записи и паролю, либо по сертификату пользователя.

После прохождения процедуры аутентификации возможен конфликт работы локального и удаленного администратора (см. стр. **24**).

Для запуска процедуры аутентификации при локальном управлении:

1. Включите питание сетевого устройства.

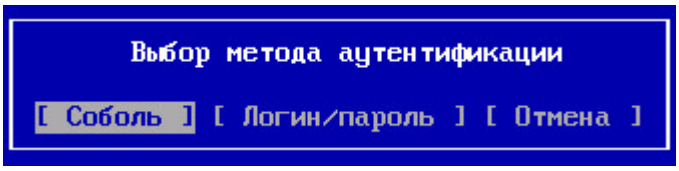
   На экране появится меню администратора, подобное изображенному ниже (для ПАК "Соболь" вер. 3.0).

2. Нажмите клавишу <Enter>.

   Произойдет загрузка ОС, после чего на экране появится главное меню локального управления до прохождения процедуры аутентификации.

3. Выберите пункт "Вход в систему" и нажмите клавишу <Enter>.

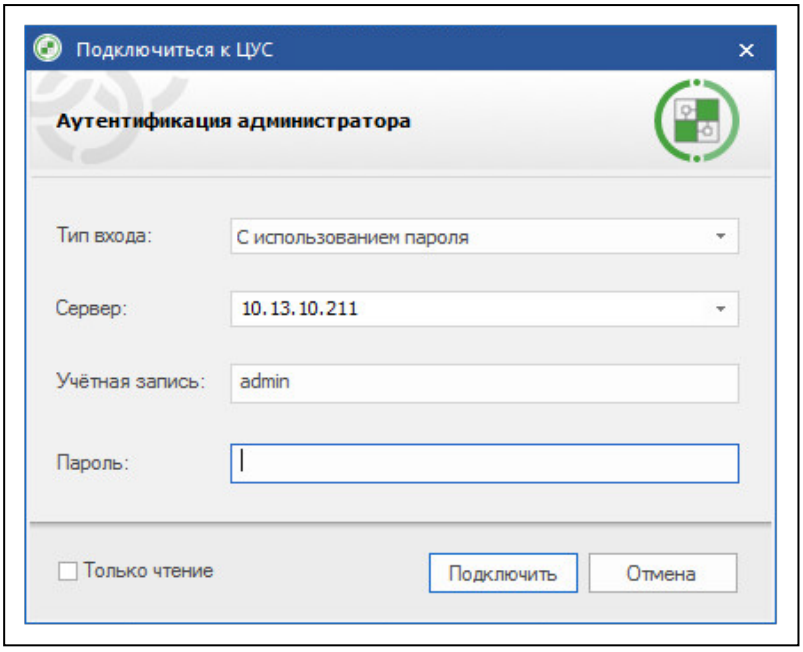
   На экране появится окно "Выбор метода аутентификации".



Для запуска процедуры аутентификации в Менеджере конфигурации:

- Активируйте на рабочем столе ярлык Менеджера конфигурации или, в случае разрыва соединения при работе в программе, нажмите иконку подключения в левом верхнем углу окна Менеджера конфигурации.

На экране появится диалоговое окно подключения к серверу.



С использованием ПАК "Соболь"

Для прохождения процедуры аутентификации при локальном управлении:

1. В окне "Выбор метода аутентификации" выберите пункт "Соболь" и нажмите клавишу <Enter>.

   На экране появится запрос персонального идентификатора, подобный следующему:

   ```
   Предъявите персональный идентификатор...
   ```

2. Аккуратно приложите персональный идентификатор администратора сетевого устройства к считывателю.

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

3. Введите пароль администратора, назначенный вами при смене пароля или указанный в паспорте сетевого устройства (п. 2.2, графа "Пароль администратора по умолчанию").

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

   В случае успешной аутентификации будет выполнен возврат в главное меню локального управления, при этом содержание меню будет функционально дополнено.

С использованием пароля

Для прохождения процедуры аутентификации при локальном управлении:

1. В окне "Выбор метода аутентификации" выберите пункт "Логин/пароль" и нажмите клавишу <Enter>.

   На экране появится окно "Вход в систему".

2. Введите имя учетной записи администратора и ее пароль, используя курсоры клавиатуры для перемещения между строками, и нажмите клавишу <Enter>.

   В случае успешной аутентификации будет выполнен возврат в главное меню локального управления, при этом содержание меню будет функционально дополнено.

Для прохождения процедуры аутентификации в Менеджере конфигурации:

1. В окне аутентификации администратора выберите в поле "Тип входа" значение "С использованием пароля", в поле "Сервер" введите IP-адрес ЦУС, к которому должно быть выполнено подключение, либо выберите из списка ранее вводимых адресов.
2. Укажите имя и пароль администратора ЦУС и нажмите кнопку "Подключить".

   Примечание. Для подключения в режиме чтения установите отметку в соответствующем поле.

   Будет выполнено подключение Менеджера конфигурации к ЦУС.

С использованием сертификата

Примечание. Аутентификация главного администратора возможна по его сертификату, полученному при инициализации ЦУС.

Для прохождения процедуры аутентификации в Менеджере конфигурации:

1. В окне аутентификации администратора выберите в поле "Тип входа" значение "С использованием сертификата", в поле "Сервер" введите IP-адрес ЦУС, к которому должно быть выполнено подключение, либо выберите из списка ранее вводимых адресов.
2. В поле сертификата нажмите кнопку "Выбрать", укажите сертификат администратора ЦУС из списка установленных личных сертификатов и нажмите кнопку "ОК".

   Примечание. Для просмотра сведений о сертификате нажмите на соответствующую ссылку, отображаемую после выбора сертификата.

3. Укажите пароль доступа к ключевому контейнеру в соответствующем поле и нажмите кнопку "Подключить".

   Будет выполнено подключение Менеджера конфигурации к ЦУС.

Блокировка администратора

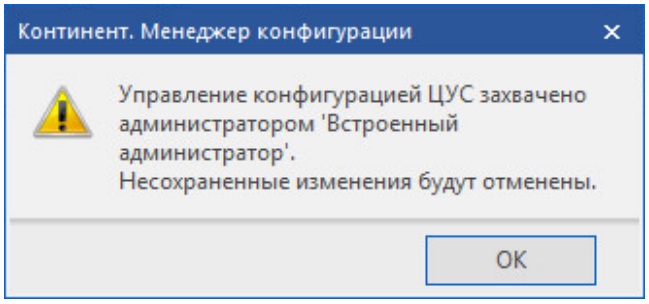
После успешной аутентификации возможна ситуация конфликта управления БД ЦУС локальным администратором и удаленными администраторами через Менеджер конфигурации. В этом случае администратор — инициатор конфликта получит возможность выбора режима работы.

Выбор режима работы при локальной аутентификации

При конфликте администратор получает возможность выбора между двумя режимами работы:

- режим локальных изменений, при котором:
  - недоступно создание сертификатов и запросов на сертификат (при этом можно создавать сертификаты веб-сервера мониторинга);
  - можно применять локальную политику;
  - нельзя подтверждать изменения настроек УБ;
- режим принудительного захвата блокировки (полнофункциональный, изменения в конфигурации ЦУС удаленным администратором при этом теряются).

При выборе режима принудительного захвата блокировки удаленный администратор отключается от управления ЦУС и получает следующее информационное сообщение:



Выбор режима работы при аутентификации через Менеджер конфигурации

При конфликте администратор получает возможность выбора режима работы:

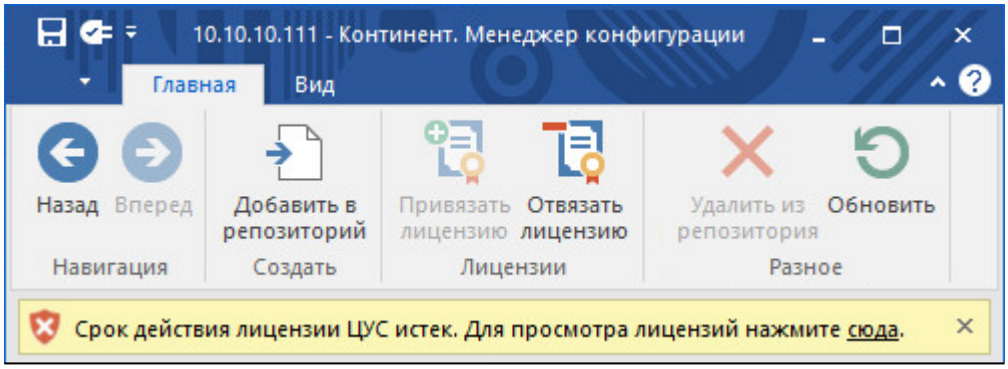
- режим чтения (любое изменение конфигурации запрещено);
- редактирование (идентичен режиму принудительного захвата блокировки, дополнительно отображается информация, какой именно администратор сейчас редактирует конфигурацию ЦУС);
- восстановление (в случае перехвата управления тем же самым администратором — все изменения, сделанные при локальном управлении, передаются в ЦУС для дальнейшей модификации через Менеджер конфигурации);
- сброс (в случае перехвата блокировки тем же самым администратором, идентичен режиму принудительного захвата блокировки).

При выборе любого режима, кроме чтения, локальный администратор переходит в режим локальных изменений.

Глава 4
Лицензии комплекса

Лицензия УБ определяет набор функций, которые можно для него активировать. Без лицензии невозможно применение политик (при этой операции проверяется наличие лицензий в БД ЦУС).

По умолчанию после инициализации узла в базе прописывается демолицензия с нулевым идентификатором клиента, которая позволяет оценить основные возможности комплекса в ограниченный период времени — 14 дней. По истечении этого срока политика перестанет устанавливаться на узел. При сохранении конфигурации или входе в систему по истечении срока демолицензии ЦУС под панелью инструментов МК будет показано соответствующее сообщение:



Отвязанная от УБ лицензия остается в репозитории, ее возможно привязать к другому УБ или удалить (см. стр. **27**).

Просмотр лицензий

Просмотреть сведения об имеющихся на узле безопасности лицензиях можно средствами локального управления или в МК.

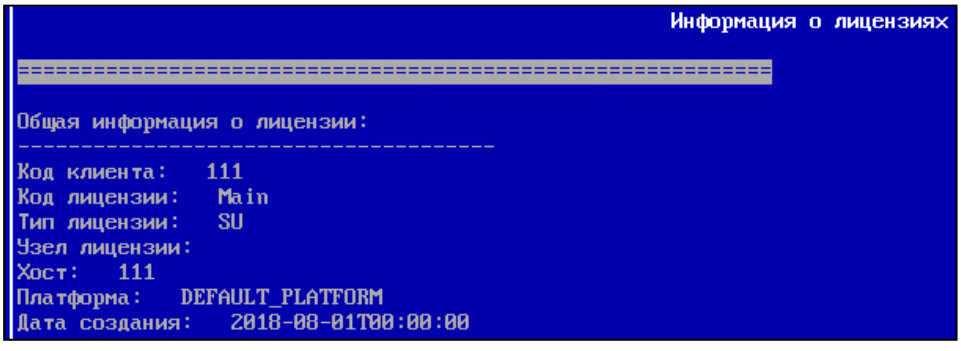
Для просмотра сведений о лицензиях средствами локального управления:

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

   На экране появится окно "Сведения".

2. Выберите пункт "Лицензии" и нажмите клавишу <Enter>.

   Откроется окно просмотра сведений о действующих на узле лицензиях.



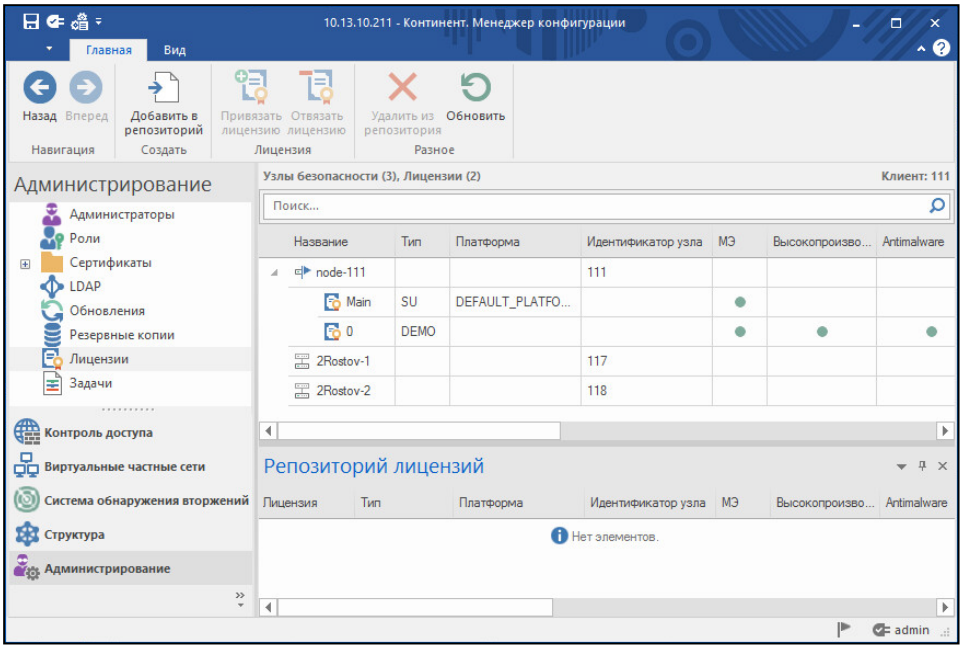
Внимание! Информация о лицензиях отображается только после первой установки политики на этот узел с МК.

3. Для выхода необходимо нажать клавишу <Esc>.

Для просмотра сведений о лицензиях в Менеджере конфигурации:

- Откройте МК, выберите на панели навигации раздел "Администрирование" и в нем — "Лицензии".

  В правой части окна появится таблица зарегистрированных на ЦУС лицензий, сгруппированных по узлам комплекса. В колонках отмечены параметры лицензии, а также компоненты, которые позволяет использовать лицензия. В правом верхнем углу отображается идентификатор клиента, по умолчанию он нулевой. Снизу расположен репозиторий, в котором находятся зарезервированные лицензии.



Управление лицензиями

Операции добавления, привязки, отзыва и удаления лицензий к УБ выполняют в МК.

Для добавления лицензии:

1. На панели навигации МК выберите раздел "Администрирование" и в нем — "Лицензии".
2. На панели инструментов нажмите кнопку "Добавить в репозиторий".

   Появится стандартный диалог открытия файла.
3. Укажите лицензионный файл и нажмите кнопку "Открыть".

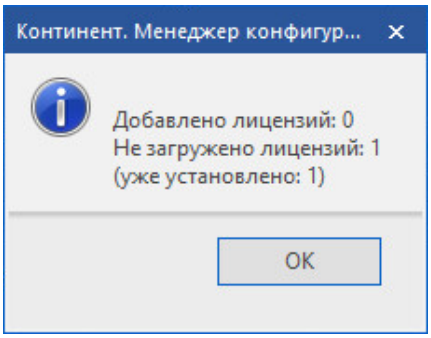
   Лицензии будут загружены из файла, если при этом соблюдены следующие условия:

   - Идентификатор клиента в лицензии совпадает с идентификатором клиента на ЦУС или в базе ЦУС присутствуют только лицензии с нулевым значением идентификатора клиента.
   - Название продукта в лицензии — Continent 4.
   - Срок действия лицензии не истек.

     Примечание. Окончание срока подписки на обновление БРП не означает истечения срока действия бессрочной лицензии УБ.

   - В базе ЦУС нет лицензии с таким же ID лицензии.

По окончании импорта в базу ЦУС будет выдано сообщение о количестве добавленных/незагруженных лицензий и причинах отклонения последних.



Для привязки лицензии к определенному узлу:

Внимание! Привязка лицензии должна быть выполнена до первой выгрузки файла конфигурации УБ и его последующего подключения к ЦУС.

1. Выберите узел в таблице на экране, нажмите кнопку "Привязать лицензию" на панели инструментов.

   Появится окно с доступными для назначения и подходящими по типу и сроку действия лицензиями.
2. Выберите требуемую лицензию. Нажмите кнопку "ОК".

   Совет. Для привязки лицензии удобно пользоваться функцией "drag&drop": перетащить мышью лицензию из репозитория к требуемому УБ.

   Лицензия будет привязана к данному узлу и переместится из репозитория в группу привязанных лицензий при соблюдении следующих условий:
   - Лицензия не просрочена.
   - Тип платформы в лицензии (если он указан) соответствует типу платформы узла назначения.
   - ID узла в лицензии (если он указан) совпадает с ID привязываемого узла.

   Примечание. После привязки лицензии рекомендуется перезапустить МК.

Для отзыва лицензии:

1. Выберите лицензию в таблице на экране, нажмите кнопку "Отвязать лицензию" на панели инструментов.

   Появится окно подтверждения отвязки лицензии.
2. Подтвердите отзыв лицензии, нажав кнопку "Да".

   Совет. Для отзыва лицензии удобно пользоваться функцией "drag&drop": перетащить мышью лицензию от УБ в репозиторий.

   Произойдет отвязка лицензии от определенного узла и она переместится в репозиторий.

Для удаления лицензии:

1. Выберите лицензию в репозитории, нажмите кнопку "Удалить лицензию" на панели инструментов.

   Появится окно подтверждения удаления.
2. Подтвердите удаление лицензии, нажав кнопку "Да".

   Внимание! Удаление привязанных лицензий недоступно, сначала лицензию необходимо отвязать.

   Удаленную лицензию можно повторно загрузить из файла в базу ЦУС.

Глава 5

Управление узлами безопасности

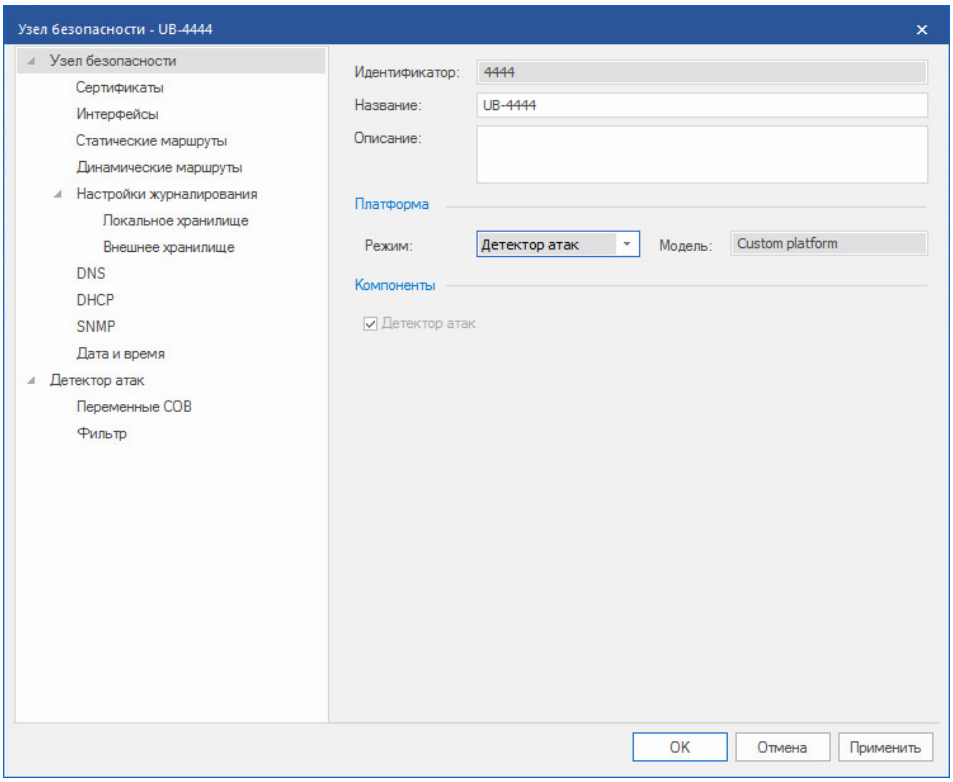
Инициализация, подключение и регистрация узлов безопасности выполняются средствами локального управления и с помощью Менеджера конфигурации (см. [**1**]).
Процедуру развертывания УБ рекомендуется завершить сменой кода загрузчика (пароля в GRUB) для предотвращения возможности изменений параметров загрузки ПО (см. [**1**]).

Просмотр свойств

Для просмотра сведений об устройстве в Менеджере конфигурации:

1. Перейдите в раздел "Структура".
2. В списке узлов безопасности выберите нужный компонент и нажмите кнопку "Свойства" на панели инструментов.

   На экране появится окно "Узел безопасности".

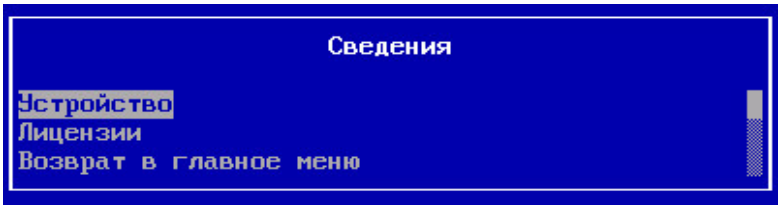


   В левой части окна расположено меню настройки УБ. Сведения по каждому пункту этого меню отображаются в правой части окна.
3. После просмотра нажмите кнопку "ОК" для возврата в раздел "Структура".

Для просмотра сведений об устройстве средствами локального управления:

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

   На экране появится окно "Сведения".



2. Выберите пункт "Устройство" и нажмите клавишу <Enter>.

   Откроется окно просмотра сведений об узле безопасности.

3. Для выхода необходимо нажать клавишу <Esc>.

Диагностика работы комплекса

Для диагностики функционирования комплекса:

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

   На экране появится меню "Инструменты".

2. Выберите пункт "Диагностика" и нажмите клавишу <Enter>.

   На экране появится список возможных форм наблюдения за состоянием аппаратуры комплекса.

Пункт меню	Назначение
Диагностика сети	Диагностика сетевых соединений командами ping, traceroute, arp
Диагностика сетевых интерфейсов	Проверка сетевых интерфейсов сервера
Командная строка	Переход в консольный режим работы при ограниченном наборе доступных команд
Состояние RAID	Проверка состояния RAID-массива
Настройка трассировки коммуникатора	Разрешение или запрет передачи служебных сообщений по взаимодействию УБ и ЦУС в файл с установкой максимального уровня сообщений ("Отладка (Debug)" – "Авария (Emerg)")
Просмотр трассировки коммуникатора	Просмотр списка служебных сообщений с возможностью экспорта списка на внешний носитель
Технологический отчет	Создание технологического отчета для передачи разработчикам ПО и экспорт его на внешний носитель
Возврат в предыдущее меню	Переход в меню "Инструменты"

3. Выберите нужный пункт меню и нажмите клавишу <Enter>.

Сетевые настройки

Настроить сетевые интерфейсы и осуществить иные настройки сети можно в МК или средствами локального управления.

Настройка IP-адреса

Для настройки IP-адреса в Менеджере конфигурации:

1. В разделе "Структура" МК выберите нужный компонент комплекса и вызовите окно настройки свойств.
2. Выберите в левой части окна в разделе "Узел безопасности" пункт "Интерфейсы".

   В правой части окна появится список интерфейсов узла.
3. В окне настройки интерфейсов компонента комплекса выберите строку нужного интерфейса и укажите:
   - назначение;

Тип назначения	Компонент комплекса	Описание применения
Внутренний	Шлюз	Взаимодействие с защищаемой сетью
Внешний	Любой	Взаимодействие с сетью интернет
Мониторинг	ДА	Анализ трафика по схеме включения Monitor
Inline-интерфейс	ДА	Анализ трафика по схеме включения Inline
Синхронизация в кластере	Любой	Синхронизация компонентов кластера

Примечание. Интерфейс управления для передачи служебного трафика между элементами комплекса определяется автоматически.

   - IP-адрес и сетевую маску;
   - величину параметра MTU.

Примечание. Параметр MTU определяет максимальную единицу передачи данных (в байтах) для интерфейса "Управление". По умолчанию установлено значение 1500.

4. После проведения всех необходимых настроек сохраните изменения в конфигурации ЦУС и установите политику на компоненты комплекса с измененными параметрами (см. стр. **41**).

Для настройки IP-адреса при локальном управлении:

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

   На экране появится окно "Меню настроек".
2. Выберите пункт "Сеть" и нажмите клавишу <Enter>.

   На экране появится окно "Сетевые настройки узла".
3. Выберите пункт "Настройка сетевых интерфейсов" и нажмите клавишу <Enter>.

   Появится окно "Сетевые интерфейсы".
4. Выберите сетевой интерфейс для настройки и нажмите клавишу <Enter>.

   Появится окно настройки сетевого интерфейса.

5. Введите IP-адрес и префикс подсети, а также значение MTU и нажмите клавишу <Enter>.

Будет выполнена настройка сетевых параметров выбранного интерфейса, после чего произойдет возврат к окну "Сетевые интерфейсы". При необходимости настройки другого сетевого интерфейса повторите пп. **2, 3**.

6. После проведения всех необходимых настроек отправьте изменения в конфигурации узла в ЦУС и подтвердите их локально или через МК (см. стр. **41**).

Для добавления альтернативного IP-адреса ЦУС (только для УБ):

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

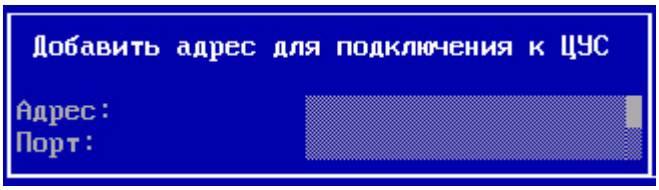
   На экране появится окно "Меню настроек".

2. Выберите пункт "Сеть" и нажмите клавишу <Enter>.

   На экране появится окно "Сетевые настройки узла".

3. Выберите пункт "Добавить адрес для подключения к ЦУС" и нажмите клавишу <Enter>.

4. Введите IP-адрес ЦУС, при необходимости укажите порт и нажмите клавишу <Enter>.



   Будет добавлено альтернативное подключение ДА к ЦУС по новому IP-адресу и произойдет возврат в окно "Сетевые настройки узла".

5. Для применения новых параметров вернитесь в меню настроек, выберите пункт "Применить локальную политику" и нажмите клавишу <Enter>.

   Дождитесь завершения операции и подтвердите изменения в ЦУС локально или через МК (см. стр. **41**).

Смена IP-адреса

Для смены IP-адреса интерфейса управления УБ:

1. На подчиненном узле в главном меню локального управления выберите пункт "Настройки" и нажмите клавишу <Enter>.

   На экране появится окно "Меню настроек".

2. Выберите пункт "Сеть" и нажмите клавишу <Enter>.

   На экране появится окно "Сетевые настройки узла".

3. Выберите пункт "Настройка сетевых интерфейсов" и нажмите клавишу <Enter>.

   Появится окно "Сетевые интерфейсы".

4. Выберите интерфейс управления и нажмите клавишу <Enter>.

   Появится окно настройки сетевого интерфейса.

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

   Будет выполнена настройка сетевых параметров выбранного интерфейса, после чего произойдет возврат к окну "Сетевые интерфейсы".

6. Вернитесь в главное меню, выберите пункт "Инструменты" и нажмите клавишу <Enter>.

   На экране появится окно "Меню инструменты".

7. Выберите пункт "Отправить локальные изменения на ЦУС" и нажмите клавишу <Enter>.

   Данные об измененной конфигурации будут отправлены в ЦУС, дождитесь завершения процесса и появления сообщения "Успешно".

8. Нажмите клавишу <Enter>.

   Будет выполнен возврат в меню "Инструменты".

9. Вернитесь в главное меню, выберите пункт "Завершение работы устройства" и нажмите клавишу <Enter>.

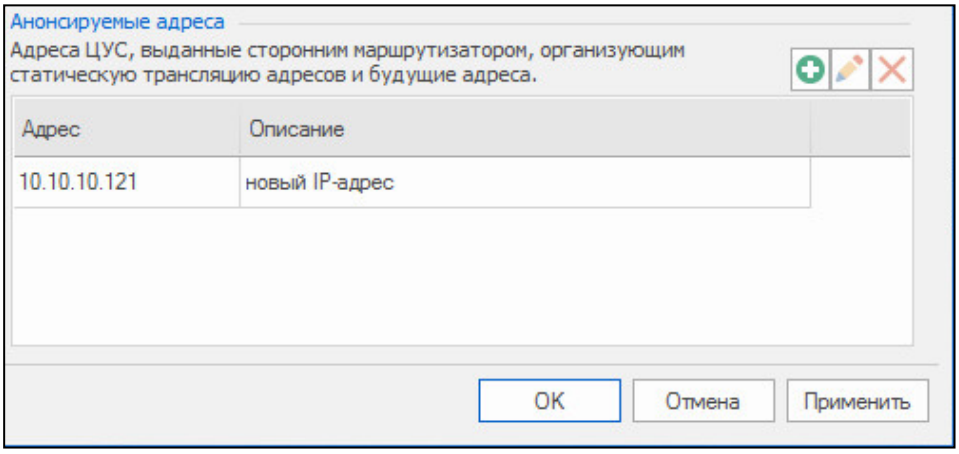
   На экране появится окно "Выключить Континент?".

10. Выберите пункт "Перезагрузка" и нажмите клавишу <Enter>.

11. Подтвердите изменения конфигурации в ЦУС (см. стр. **44**).

Для смены IP-адреса интерфейса управления ЦУС:

1. В разделе "Структура" МК выберите нужный ЦУС и вызовите окно настройки свойств.
2. Выберите в левой части окна в разделе "Узел безопасности" пункт "Интерфейсы".
3. В разделе "Анонсируемые адреса" нажмите кнопку  и добавьте IP-адрес, на который предполагается изменить интерфейс управления ЦУС.



4. Нажмите кнопку "ОК" для сохранения изменений в настройках ЦУС.
5. Установите политику на ЦУС и на все подчиненные узлы.

   Дождитесь выполнения задачи по установке политики.

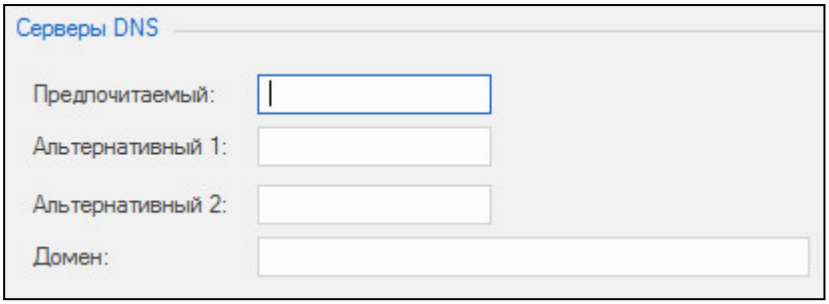
6. Вновь вызовите окно свойств ЦУС, в его интерфейсах замените IP-адрес интерфейса управления и нажмите кнопку "Применить".
7. Если необходимо изменить карту статических маршрутов, выберите в левой части окна в разделе "Узел безопасности" пункт "Маршруты" и сделайте необходимые изменения.
8. Нажмите кнопку "ОК" и установите политику на ЦУС.

Настройка DNS

Для настройки DNS в Менеджере конфигурации:

1. В разделе "Структура" МК выберите нужный ЦУС и вызовите окно настройки свойств.
2. Выберите в левой части окна пункт "DNS".

   В правой части окна появится список серверов DNS.



3. Введите IP-адрес предпочитаемого и, при необходимости, альтернативных DNS-серверов, а также доменное имя локальной системы компонента комплекса, после чего нажмите кнопку "ОК".
4. Сохраните изменения в конфигурации ЦУС и установите на него политику (см. стр. **41**).

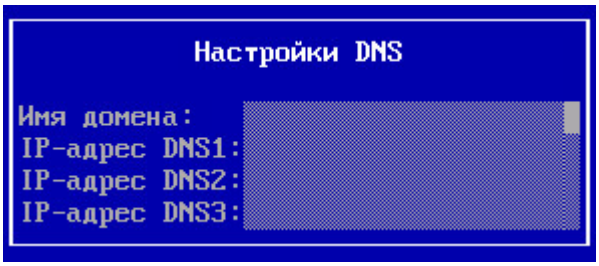
   Дождитесь выполнения задачи по установке политики.

Для настройки DNS при локальном управлении:

1. В меню настроек выберите пункт "Сеть" и нажмите клавишу <Enter>.

   На экране появится окно "Сетевые настройки узла".
2. Выберите пункт "Настройка DNS" и нажмите клавишу <Enter>.

   На экране появится окно "Настройки DNS".



3. Введите доменное имя локальной системы компонента комплекса, IP-адрес предпочитаемого DNS-сервера в поле "IP-адрес DNS1" и, при наличии альтернативного DNS-сервера, укажите его IP-адрес в поле "IP-адрес DNS2", после чего нажмите клавишу <Enter>.

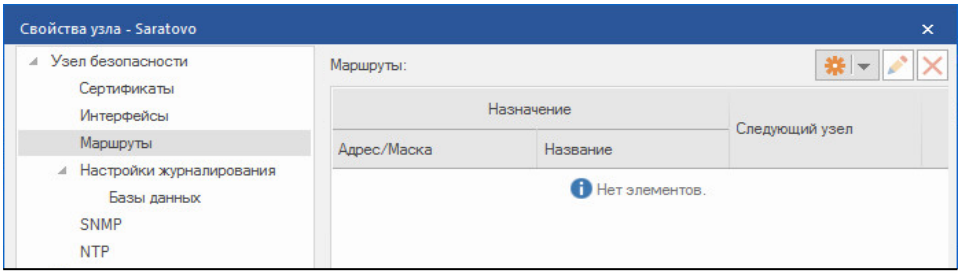
   Примечание. Для перемещения между вводимыми параметрами используйте клавиши курсоров: <↑>, <↓>.
4. Для применения новых параметров вернитесь в меню настроек, выберите пункт "Применить локальную политику" и нажмите клавишу <Enter>.

   Примечание. При изменении локальной конфигурации достаточно одного применения локальной политики после выполнения всех настроек.
5. Подтвердите изменения конфигурации в ЦУС (см. стр. **44**).

Настройка статической маршрутизации

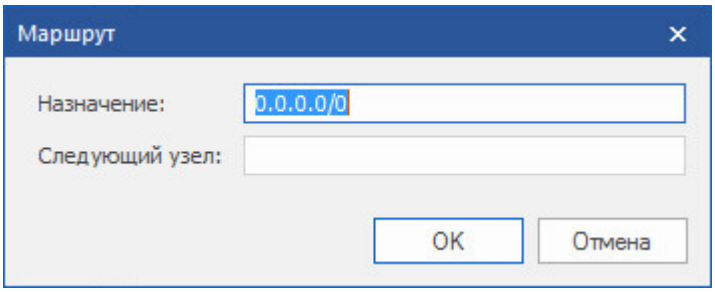
Для настройки таблицы маршрутизации в Менеджере конфигурации:

1. В разделе "Структура" МК выберите нужный ЦУС и вызовите окно настройки свойств.
2. Выберите в левой части окна в разделе "Узел безопасности" пункт "Маршруты".



3. Для добавления нового маршрута нажмите кнопку .

   На экране появится окно "Маршрут".



4. Укажите IP-адреса объекта назначения и шлюза, а затем нажмите кнопку "ОК".

   Список на экране дополнится строкой нового маршрута.

5. Для удаления маршрута нажмите кнопку .

6. После проведения всех необходимых настроек сохраните изменения в конфигурации ЦУС и установите политику на компоненты комплекса с измененными параметрами (см. стр. **41**).

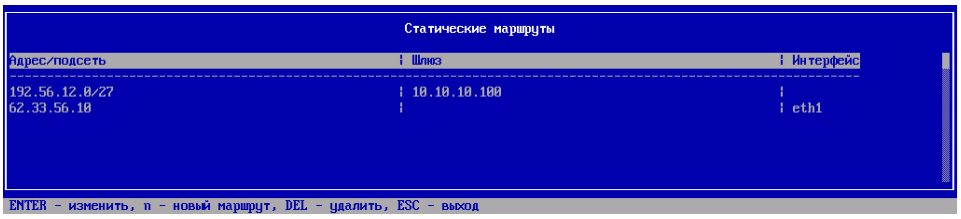
Для настройки статических маршрутов при локальном управлении:

1. В меню настроек выберите пункт "Сеть" и нажмите клавишу <Enter>.

   На экране появится окно "Сетевые настройки узла".

2. Выберите пункт "Настройка статической маршрутизации" и нажмите клавишу <Enter>.

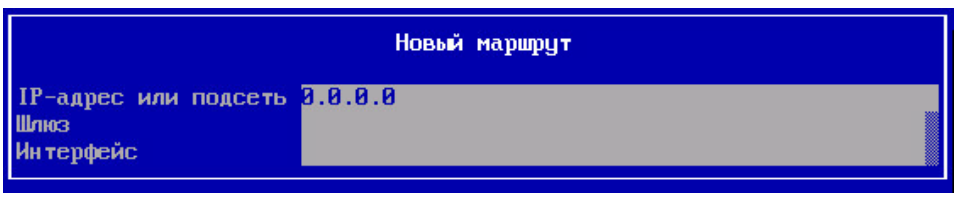
   На экране появится окно "Статические маршруты".



3. Для создания нового маршрута нажмите клавишу "n" .

   Примечание. Для редактирования имеющегося маршрута необходимо выбрать его в списке и нажать клавишу <Enter>, для удаления – клавишу <Del>.

   Появится окно "Новый маршрут".



4. Введите IP-адрес удаленного сетевого объекта или подсети, укажите шлюз, через который будет осуществляться подключение, или интерфейс УБ и нажмите клавишу <Enter>.

   Будет создан новый маршрут и произойдет возврат в окно "Статические маршруты". При необходимости настройки другого сетевого интерфейса повторите пп. **3, 4**.

5. Для применения новых параметров вернитесь в меню настроек, выберите пункт "Применить локальную политику" и нажмите клавишу <Enter>.

   Примечание. При изменении локальной конфигурации достаточно одного применения локальной политики после выполнения всех настроек.

6. Подтвердите изменения конфигурации в ЦУС (см. стр. **44**).

Настройка ARP-проксирования

При настройке правил NAT на шлюзах комплекса может потребоваться организация дополнительного проксирования на узлах безопасности для ответа на ARP-запросы.

Настройку ARP-проксирования можно осуществить только средствами локального управления.

Для настройки ARP-проксирования:

1. В меню настроек выберите пункт "Сеть" и нажмите клавишу <Enter>.

   На экране появится окно "Сетевые настройки узла".

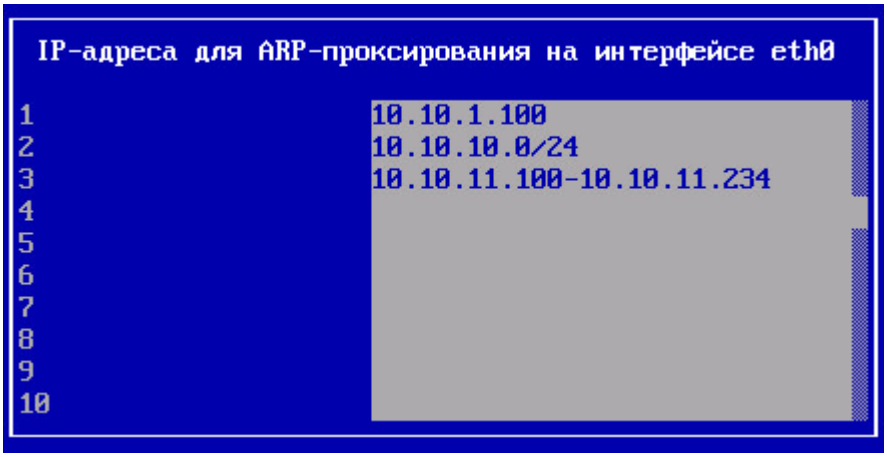
2. Выберите пункт настройки ARP-проксирования и нажмите клавишу <Enter>.

   На экране появится окно "Настройки ARP-прокси".

3. Выберите интерфейс для переадресации на него ARP-запросов и нажмите клавишу <Enter>.

   На экране появится окно со списком IP-адресов для ARP-проксирования на выбранный интерфейс.

4. Введите проксируемые IP-адреса, а также подсети или диапазоны IP-адресов и нажмите клавишу <Enter>.



   Будет выполнено изменение настроек проксирования для выбранного интерфейса, после чего произойдет возврат к окну настроек ARP-проксирования с обновленными данными по количеству используемых адресов или их диапазонов для проксирования.

5. При необходимости настройки другого сетевого интерфейса повторите пп. **3, 4**.

6. Выберите пункт возврата в предыдущее меню и нажмите клавишу <Enter>.

7. Для применения новых параметров выберите пункт "Применить локальную политику" и нажмите клавишу <Enter>.

8. Дождитесь завершения операции и подтвердите изменения в ЦУС локально или через МК (см. стр. **41**).

Для вызова окна настройки в МК:

1. В разделе "Структура" МК выберите нужный УБ и вызовите окно настройки свойств.
2. Выберите в левой части окна в разделе "Узел безопасности" пункт "DHCP".

   В правой части окна отобразится установленный для данного устройства один из трех возможных режимов работы сервиса DHCP:

   - Отключен.
   - Сервер.
   - Ретранслятор.

   Для режима "Сервер" также отображается список профилей. Профиль сервера определяет используемый внутренний интерфейс УБ и пул выделенных IP-адресов.

   Для режима "Ретранслятор" необходимо задать IP-адрес DHCP-сервера и профили ретранслятора. Профиль ретранслятора — это внутренний интерфейс УБ, на котором должен работать сервис, и соответствующие данному интерфейсу параметры ретранслятора. Параметрами ретранслятора являются:

   - идентификатор сервера;
   - Circuit ID;
   - Remote ID.

Настройка дистанционного доступа по протоколу SSH

Для доступа по протоколу SSH необходимо настроить учетную запись администратора и добавить его удаленный IP-адрес в список разрешенных IP-адресов.

Для предоставления администратору права дистанционного доступа:

1. В МК создайте новую роль (см. стр. **15**) и в ней установите отметку напротив привилегии "Дистанционный доступ к локальному меню" группы "Локальное управление".
2. Сохраните изменения в активной конфигурации ЦУС (см. стр. **42**).
3. Для добавления созданной роли выберите нужного администратора или создайте нового (см. стр. **18**).

   Примечание. Для встроенного администратора нет возможности добавления роли, поэтому настроить ему дистанционный доступ невозможно.

4. На закладке "Роли" выбранного администратора добавьте созданную в п. **1** роль и нажмите кнопку "OK".

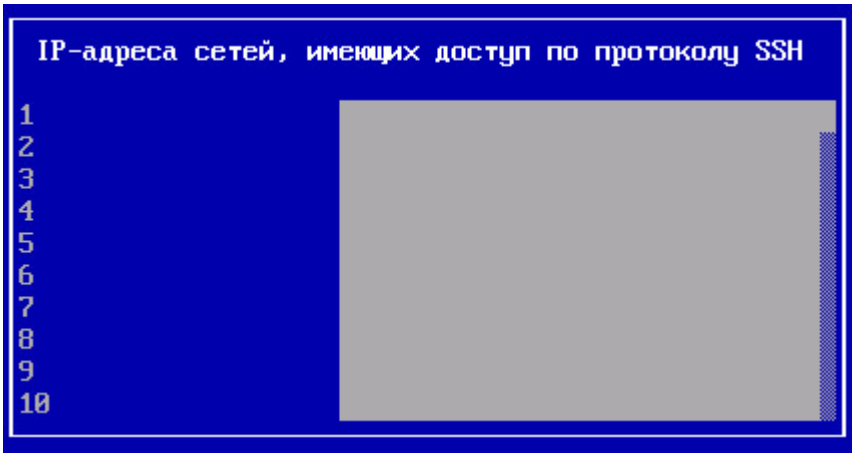
Для формирования списка разрешенных IP-адресов:

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

   На экране появится окно "Меню настроек".
2. Выберите пункт "Сеть" и нажмите клавишу <Enter>.

   На экране появится окно "Сетевые настройки узла".
3. Выберите пункт "Настройка доступа SSH" и нажмите клавишу <Enter>.

   На экране появится окно со списком IP-адресов.



4. Введите требуемый IP-адрес удаленного хоста или подсети с указанием ее префикса в формате xxx.xxx.xxx.xxx[/xx] и нажмите клавишу <Enter>.

   На экране появится информационное окно обновления БД. По окончании процесса на экране появится окно "Сетевые настройки узла".

5. При необходимости добавления еще одного IP-адреса к списку имеющих административный доступ по протоколу SSH повторите действия с п. **3**.

   Примечание. Для удаления IP-адреса перейдите управляющими клавишами клавиатуры к нужной строке списка, удалите требуемый IP-адрес посредством клавиши <Delete> и нажмите клавишу <Enter>.

6. Выберите пункт "Вернуться в предыдущее меню" и нажмите клавишу <Enter>.

   На экране появится окно "Меню настроек".

7. Выберите пункт "Применить локальную политику" и нажмите клавишу <Enter>.

8. Дождитесь появления информационного окна об успешном завершении процесса и нажмите клавишу <Enter>.

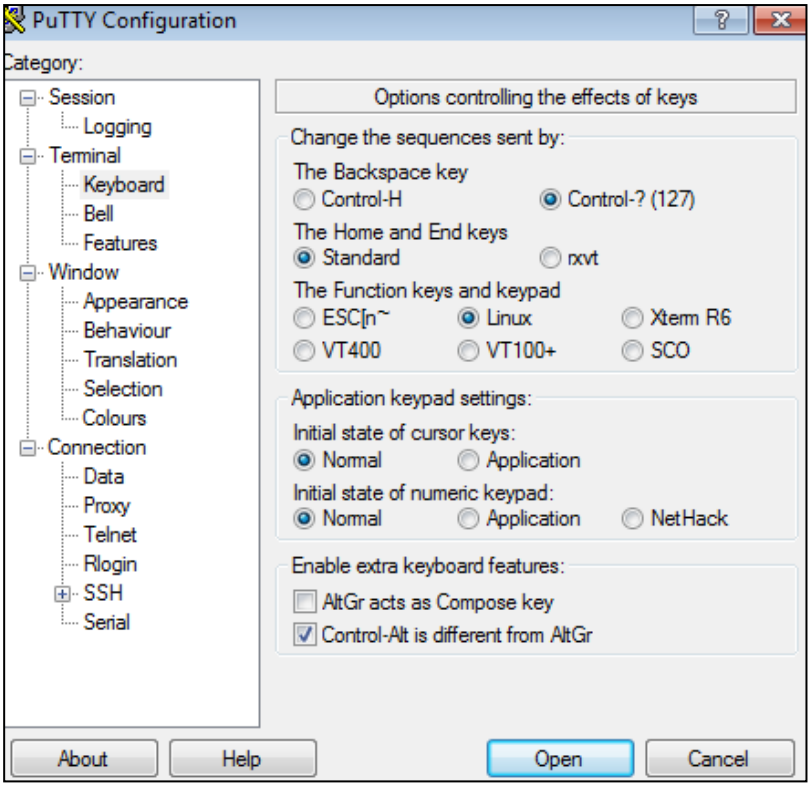
9. Подтвердите изменение конфигурации УБ в МК или в главном меню локального управления ЦУС (см. стр. **44**).

Примечание. Для удаления IP-адреса перейдите управляющими клавишами клавиатуры к нужной строке списка, удалите требуемый IP-адрес подсредством клавиши <Delete> и нажмите клавишу <Enter>.

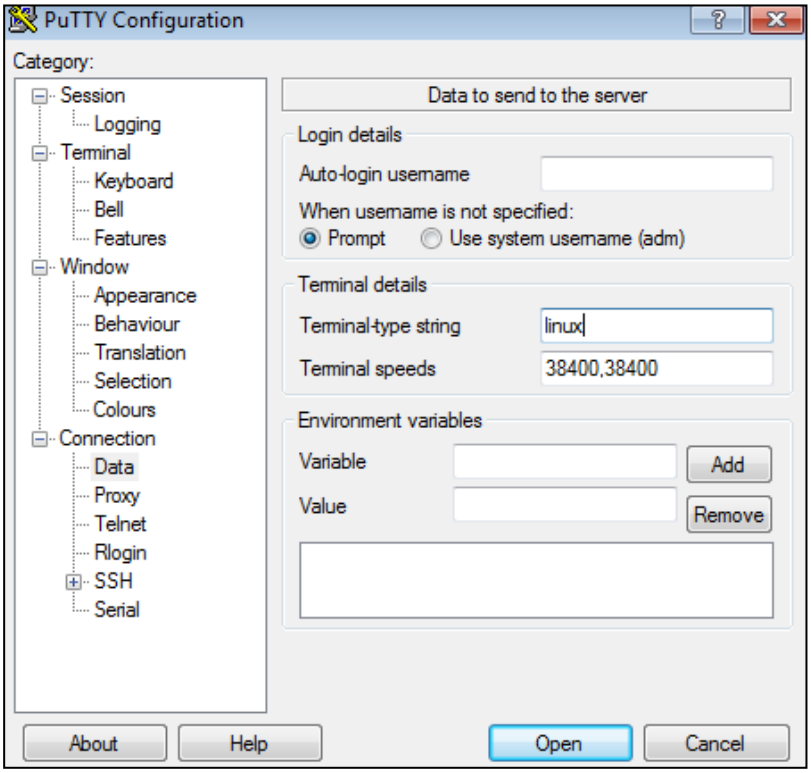
Настройка SSH-клиента на примере клиентской программы PuTTY

Для настройки программы:

1. Запустите программу.
2. Перейдите в подраздел "Terminal (Терминал) | Keyboard (Клавиатура)" в правой части окна конфигурации.



3. В правой части окна в разделе "The function keys and keypad" установите отметку напротив пункта "Linux".
4. Перейдите в подраздел "Connection (Соединение) | Data (Данные)"



5. В правой части окна в разделе "Terminal details" в поле "Terminal-type string" укажите значение "Linux".

Контроль узлов безопасности по протоколу SNMP

Для контроля узлов безопасности и ЦУС комплекса с помощью средств управления объектами сети по протоколу SNMP предусмотрен модуль, реализующий сервис SNMP. Например, можно получать информацию по стандартным OID:

Внимание! SNMP-модуль поддерживает работу только в режиме ответа на запрос (GetRequest).

iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).system(1)	Общесистемная информация
iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).interfaces(2)	Информация об интерфейсах
iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).at(3)	Информация о MAC/IP-адресах на интерфейсах
iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).ip(4)	IP-статистика, роутинг, форвардинг
iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).tcp(6)	Информация о TCP-протоколе
iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).udp(7)	Информация о UDP-протоколе

Соответственно, можно контролировать следующие параметры:

- время работы УБ с момента включения;
- количество полученных/переданных пакетов;
- состояние интерфейсов (Up/Down) и пр.

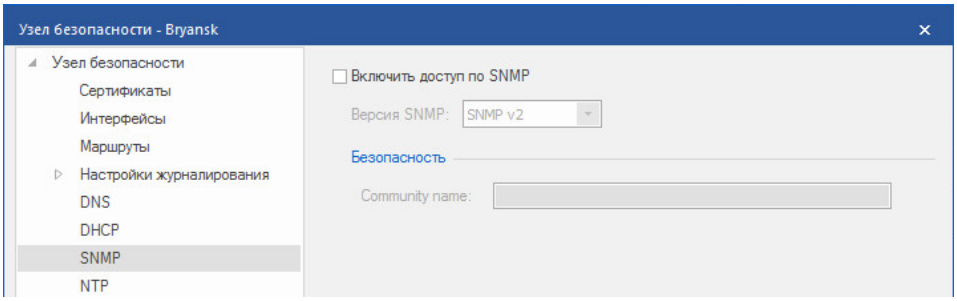
Примечание. При использовании протокола SNMP v3 для настройки SNMP-клиента необходимо в качестве алгоритма аутентификации (Auth Algorithm) использовать MD5, в качестве алгоритма шифрования (Privacy Algorithm) — DES.

Для настройки сервиса SNMP:

1. Откройте МК и перейдите в раздел "Структура".
2. В списке узлов выберите нужный компонент комплекса и нажмите кнопку "Свойства".

   На экране появится окно "Свойства узла".
3. Выберите в левой части окна в разделе "Узел безопасности" пункт "SNMP".

   В правой части окна появятся текущие настройки доступа по протоколу SNMP.



4. Включите доступ по SNMP, выберите версию протокола, укажите авторизационные данные (community name для протокола SNMP v2 или логин и пароль для протокола SNMP v3) и нажмите кнопку "ОК".

   Примечание. Пароль для протокола SNMP v3 должен отвечать требованиям, установленным Политикой безопасности паролей (см. панель инструментов подраздела "Администрирование/Администраторы").

5. Для применения настроек нажмите кнопку "Установить политику" на панели инструментов, отметьте компоненты комплекса с измененными параметрами и нажмите кнопку "ОК".

Управление конфигурацией узла безопасности

При локальном управлении УБ изменения его конфигурации записываются в локальную БД. Затем по команде администратора из меню настроек происходит подтверждение конфигурации и она фиксируется в качестве активной для данного узла. Извещение об изменениях автоматически отсылается в ЦУС, в МК активная конфигурация отображается как локальная до момента подтверждения администратором. Активная локальная конфигурация действует до применения новых локальных изменений или до установки политики из МК.

Передача сведений об изменении конфигурации

После внесения изменений в настройки любого компонента комплекса (включая УБ с ЦУС), например, в его сетевые параметры, необходимо:

- при управлении посредством МК — сохранить изменения в БД ЦУС и установить политику на узлы с измененной конфигурацией (см. стр. **43**);

  Примечание. В случае отсутствия связи между ЦУС и УБ необходимо передать обновленную конфигурацию посредством внешнего носителя (см. стр. **42**).

- при локальном управлении — сохранить конфигурацию в локальной базе данных и передать сведения об изменениях в ЦУС (см. ниже), после чего администратор ЦУС должен подтвердить пришедшие изменения (см. стр. **44**).

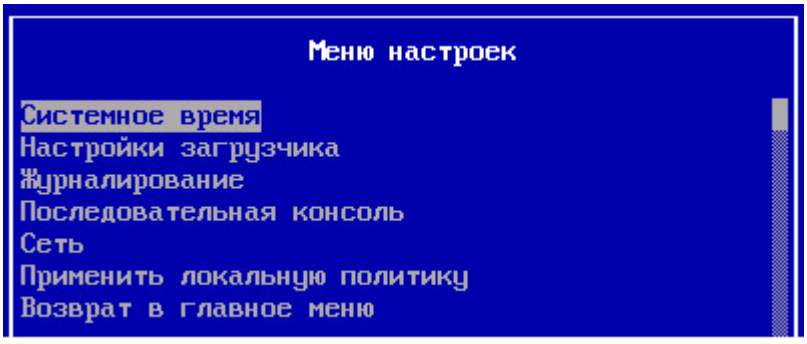
  Примечание. Если администратор ЦУС отменит изменения (см. стр. **44**), то на УБ будет действовать локальная конфигурация. Для ее отмены и возврата к конфигурации, сохраненной в БД ЦУС, необходимо установить политику на УБ (см. стр. **43**).

  Если в процессе изменения конфигурации УБ при локальном управлении его конфигурация была изменена посредством МК, то изменения, пришедшие из МК, перезапишут локальные изменения. В локальном меню можно изменить некоторые настройки узла: адреса на интерфейсах, адреса ЦУС, настройки NTP, настройки DNS, статические маршруты. Эти изменения записываются в локальную базу данных как неподтвержденная конфигурация. Затем изменения применяются к узлу и, если не было обнаружено ошибок, происходит подтверждение конфигурации, она фиксируется в качестве активной для данного узла. Активная конфигурация действует до нового локального изменения или до установки политики из МК. Информация о новой активной конфигурации отправляется в ЦУС и после подтверждения администратором в МК становится активной и в центральной базе данных (базе ЦУС).

Для передачи сведений об изменениях конфигурации посредством локального управления:

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

   На экране появится меню настроек.



2. Выберите пункт "Применить локальную политику" и нажмите клавишу <Enter>.

   Конфигурация узла сохранится в локальной БД. При этом будет создан служебный пакет данных по изменениям в конфигурации УБ, а затем он будет помещен в очередь на запись в базу данных ЦУС с присвоением очередного порядкового номера.

   Дождитесь завершения процесса и появления сообщения "Успешно".

   Примечание. Если на момент применения локальной политики ЦУС будет по каким-либо причинам недоступен, то после восстановления связи необходимо отправить локальные изменения в ЦУС (пункт "Отправить локальные изменения на ЦУС" меню "Инструменты").

3. Нажмите клавишу <Enter>.

   Будет выполнен возврат в меню настроек.

Передача сведений при отсутствии связи

В случае необходимости внесения изменений в конфигурацию УБ при отсутствии связи между ним и ЦУС требуется при локальном управлении ЦУС произвести экспорт конфигурации УБ на внешний носитель, а затем загрузить эту конфигурацию на УБ.

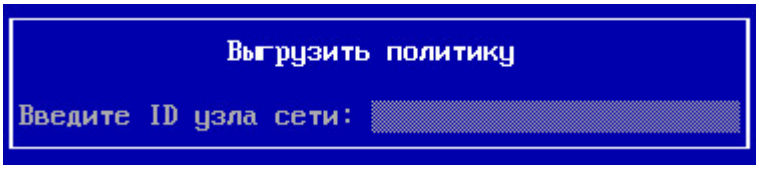
Для выгрузки конфигурации УБ на носитель (только на ЦУС):

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

   На экране появится меню "Инструменты".

2. Выберите пункт "Выгрузить конфигурацию УБ на носитель".

   Появится окно "Выгрузить политику".



3. Вставьте внешний носитель в USB-разъем, введите ID нужного узла сети и нажмите клавишу <Enter>.

   Внимание! Носитель должен быть очищен перед использованием.

   Будет выполнена запись конфигурации УБ на внешний носитель в файл policy.json, после чего появится сообщение о ее успешном завершении.

Для загрузки конфигурации УБ с носителя:

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

   На экране появится меню "Инструменты".

2. Выберите пункт "Загрузить конфигурацию с носителя", вставьте внешний носитель в USB-разъем и нажмите клавишу <Enter>.

   На экране появится стандартный диалог выбора файла.

3. Выберите нужный файл и нажмите клавишу <Enter>.

   Будет запущен процесс установки политики, после чего появится сообщение об успешном завершении процесса.

Сохранение конфигурации ЦУС

Для сохранения настроек:

- В левом верхнем углу окна МК нажмите кнопку вызова меню и выберите пункт "Сохранить".

Примечание. Также к сохранению настроек приводят следующие действия:
- нажатие сочетания клавиш "Ctrl" + "S" на клавиатуре;
- нажатие кнопки на панели быстрого доступа, при ее наличии.

Установка политики

Установка политики

Для применения изменений в конфигурации УБ необходимо установить на него политику. Для установки политики формируется задача, которая будет выполняться в порядке очереди некоторое время, зависящее от объема изменений. При локальном управлении ЦУС можно выставить временные ограничения выполнения задачи. При их превышении задача по установке политики будет завершена с ошибкой, даже если в результате политика будет установлена. По умолчанию действуют следующие нормативы:

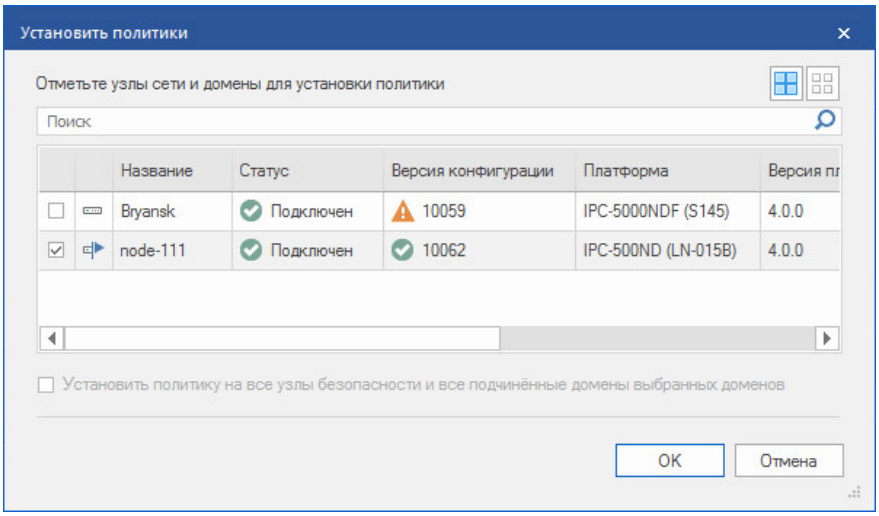
- время от момента формирования задачи до начала ее выполнения — 200 с;
- время, выделяемое на выполнение задачи — 600 с.

Для установки политики:

1. Нажмите комбинацию клавиш <Ctrl>+<I>.

   Примечание. Также вызов окна "Установить политики" можно осуществить с панели инструментов разделов "Структура", "Контроль доступа" и "Виртуальные частные сети", нажав кнопку "Установить".

   На экране появится окно "Установить политики".



2. Установите отметку в поле требуемого УБ и нажмите кнопку "ОК".

   На ЦУС будет сформирована задача по установке политики на указанный УБ.

   Если в данный момент в ЦУС никакие другие задачи не выполняются, начнется выполнение добавленной задачи. При этом в правом нижнем углу главного окна МК рядом со значком появится цифра, соответствующая общему количеству поставленных в очередь и выполняющихся задач.

3. Для просмотра сведений о поставленных задачах нажмите значок .

   В правой части окна отобразится список задач, отсортированный по времени их добавления. Статус "выполнена" будет свидетельствовать о завершении процедуры установки политик.

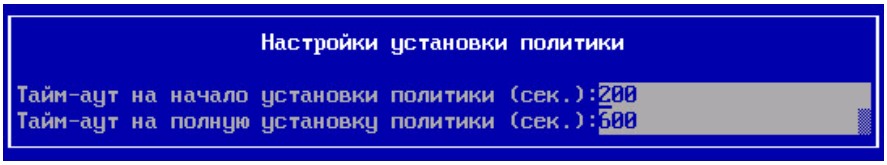
Для настройки времени установки политики:

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

   На экране появится окно "Меню настроек".

2. Выберите пункт "Настройки процесса установки политики" и нажмите клавишу <Enter>.

   На экране появятся текущие настройки.



Примечание. "Тайм-аут на начало установки политики" означает, что если за указанное время политика не начнет устанавливаться, то задача будет завершена с ошибкой.

"Тайм-аут на полную установку политики" означает время, в течение которого система будет ожидать завершения задачи на установку политики. В противном случае задача будет завершена с ошибкой.

3. Осуществите требуемые изменения и нажмите клавишу <Enter>.
4. Дождитесь появления информационного окна об успешном изменении настроек и нажмите клавишу <Enter>.

Учет конфигураций узлов

После изменений в настройках узлов и отправки локальных изменений в ЦУС в МК в поле "Версия конфигурации" для этих узлов числовое значение конфигурации меняется на оповещающий значок . Это означает, что на узле безопасности действует неподтвержденная в БД ЦУС локальная конфигурация.

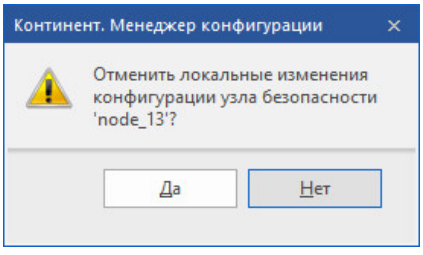
Изменения в настройках подчиненных узлов администратор в МК может подтвердить или отменить.

В МК существуют следующие графические обозначения статуса загруженной на УБ конфигурации:

Пиктограмма	Статус конфигурации	Примечание
	Не подтверждена на ЦУС	Локальные изменения конфигурации УБ ожидают подтверждения в ЦУС
	Не совпадает с имеющейся на ЦУС	В БД ЦУС находится измененная на МК конфигурация УБ, политика на УБ не устанавливалась
	Подтверждена на ЦУС	Загруженная на УБ конфигурация идентична имеющейся в БД ЦУС

Для отмены изменения конфигурации УБ:

1. Откройте МК и перейдите в раздел "Структура".
2. В списке узлов безопасности выберите узел с локальной конфигурацией и нажмите кнопку "Отменить изменения" на панели инструментов, а затем нажмите кнопку "Да" в появившемся окне отмены локальных изменений.



   Оповещающий значок конфигурации изменится на .

3. Для применения настроек установите политику на этот узел безопасности (см. стр. **43**).

   Оповещающий значок изменится на новое числовое значение конфигурации. На узле безопасности будет действовать конфигурация, пришедшая с ЦУС.

Для подтверждения изменения конфигурации УБ в МК:

1. Откройте МК и перейдите в раздел "Структура".
2. В списке узлов безопасности выберите узел с локальной конфигурацией и нажмите кнопку "Подтвердить изменения" на панели инструментов, а затем нажмите кнопку "Да" в появившемся окне подтверждения локальных изменений.

   Примечание. Случаи конфликта конфигураций УБ (merge conflict) разобраны на стр. 41.

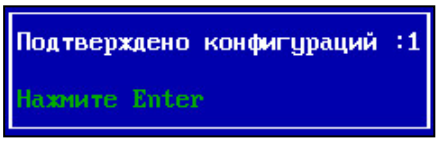
   Пиктограмма статуса изменится на новое числовое значение конфигурации.

Для подтверждения изменения конфигурации УБ в ЦУС посредством локального управления:

1. В меню "Инструменты" главного меню локального управления ЦУС выберите пункт "Подтверждение изменений настроек УБ" и нажмите клавишу <Enter>.

   На экране появится окно "Неподтвержденные конфигурации".
2. Установите отметку клавишей <Пробел> и нажмите клавишу <Enter>.

   На экране появится сообщение о подтверждении конфигурации.

3. Нажмите клавишу <Enter>.

   В БД ЦУС будут внесены изменения в соответствии с полученной от УБ конфигурацией. После чего будет выполнен возврат в меню "Инструменты".
4. Для возврата в главное меню нажмите клавишу <Esc>.

Список задач

При установке политики на узел безопасности формируется соответствующая задача. Если в данный момент никакая другая задача не выполняется, ЦУС приступает к ее выполнению. Если же в данный момент уже выполняется какая-либо задача, вновь сформированная задача регистрируется в системе и становится в очередь.

Сведения обо всех сформированных задачах хранятся в ЦУС в виде списка, в котором отображается следующая информация:

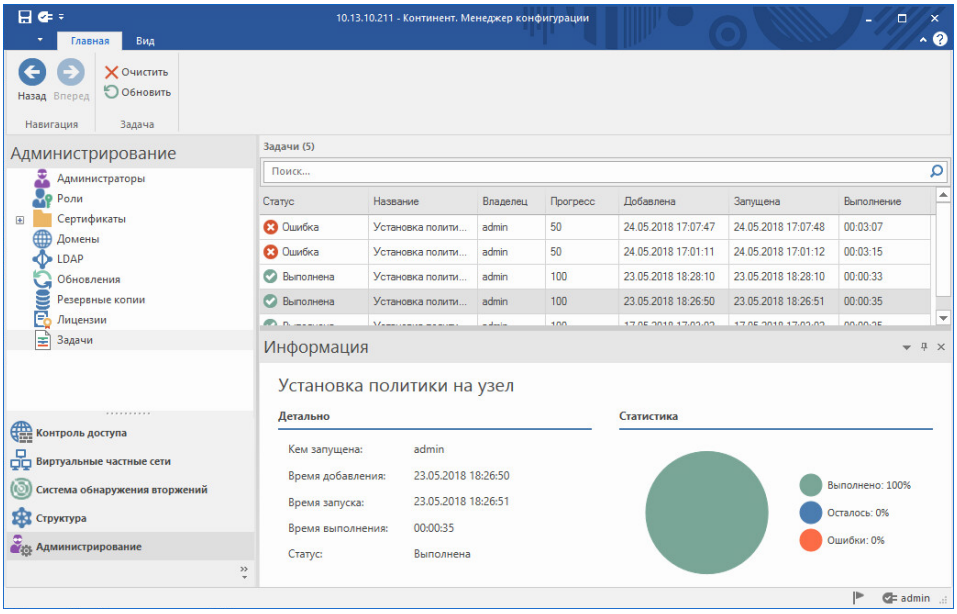
- название задачи;
- логин администратора — инициатора этой задачи;
- статус ("выполнена", "выполняется", "зарегистрирована", "ошибка", "выполнена с предупреждениями");
- прогресс (процент выполнения);
- время добавления задачи в список;
- время начала выполнения;
- время, затраченное на выполнение.

Для просмотра списка задач:

1. Перейдите в раздел "Администрирование" и выберите папку "Задачи".

   В правой части окна отобразится список задач.

   Примечание. Переход к списку задач из любого раздела МК можно выполнить, нажав на значок  , расположенный в правом нижнем углу главного окна, а затем ссылку "Переход к списку задач" в появившемся окне центра уведомлений.



Для отображения в списке статуса задачи используются следующие пиктограммы:

Пиктограмма	Статус	Примечание
	Зарегистрирована	Находится в очереди на выполнение
	Выполняется	Выполняется в данный момент
	Выполнена	Успешно выполнена
	Выполнена с предупреждениями	Операция выполнена несмотря на ошибки, обнаруженные в процессе выполнения
	Ошибка	Выполнена с ошибкой

2. Если задача связана с применением политик к нескольким узлам безопасности, выделите ее в списке.

   В дополнительном окне "Информация", расположенном под списком, отобразятся подробные сведения о выполнении задачи на каждом из узлов.

3. Для очистки списка нажмите на панели инструментов кнопку "Очистить".

   Внимание! Данная операция является необратимой.

   Будут удалены все задачи, кроме задач со статусом "выполняется" или "зарегистрирована".

Перезагрузка и выключение

Перезагрузку и выключение УБ выполняет авторизованный пользователь с правами главного администратора.

Для перезагрузки/выключения УБ в Менеджере конфигурации:

1. В разделе "Структура" МК выделите нужный УБ и нажмите кнопку перезагрузки или завершения работы на панели инструментов.

   На экране появится запрос на подтверждение операции.

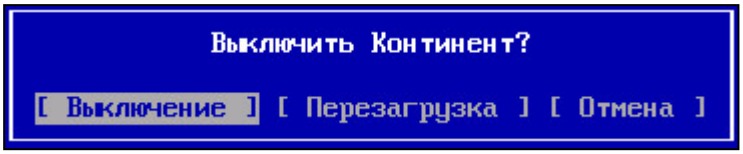
2. Нажмите кнопку "Да".

   В зависимости от выбранного варианта произойдет выключение или перезагрузка УБ.

Для перезагрузки/выключения УБ при локальном управлении:

1. Откройте главное меню локального управления, выберите пункт "Завершение работы устройства" и нажмите клавишу <Enter>.

   На экране появится запрос на выбор операции.



2. Выберите нужную операцию и нажмите клавишу <Enter>.

   В зависимости от выбранного варианта произойдет выключение УБ или начнется его перезагрузка.

Удаление

Для удаления УБ:

1. Откройте МК и в разделе "Структура" выберите в меню пункт "Узлы безопасности".

   В окне отобразится список всех УБ.

2. Выберите необходимый для удаления УБ и на панели инструментов нажмите кнопку "Удалить".

   На экране появится запрос на подтверждение удаления.

3. Нажмите кнопку "Да" в окне запроса, после чего сохраните изменения в конфигурации ЦУС (см. стр. **42**).

4. Для применения конфигурации установите политику на ЦУС (см. стр. **43**).

   Узел безопасности будет удален из БД ЦУС.

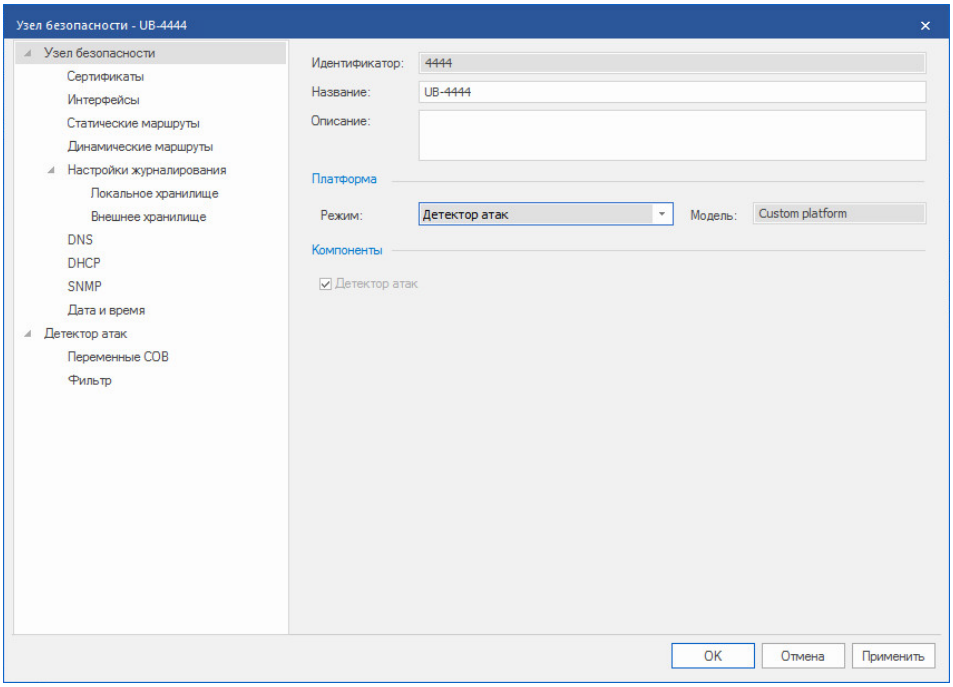
Глава 6
Настройка СОВ

Настройка параметров СОВ

Для настройки параметров:

1. Перейдите в раздел "Структура" Менеджера конфигурации, выберите узел безопасности, выполняющий функции детектора атак, и вызовите окно настройки свойств.
2. При необходимости измените содержание полей "Название" и "Описание".
3. Установите отметку напротив пункта "Детектор атак".

   В левой части окна в меню появится раздел "Детектор атак" с подразделами "Переменные СОВ" и "Фильтр". В правой части окна изменится список подключаемых компонентов.



4. Выберите в левой части окна в разделе "Детектор атак" пункт "Переменные СОВ".

   Примечание. Переменные СОВ используются для определения домашней сети и внешней, в вендорских правилах и при создании пользовательских правил для указания источника и приемника.

   В правой части окна появится список переменных.

Название	Сетевой объект / Сервис	Инверсия
HOME_NET	[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]	☐
EXTERNAL_NET	!$HOME_NET	☐
HTTP_SERVERS	$HOME_NET	☐
SMTP_SERVERS	$HOME_NET	☐
SQL_SERVERS	$HOME_NET	☐
DNS_SERVERS	$HOME_NET	☐
TELNET_SERVERS	$HOME_NET	☐
AIM_SERVERS	$HOME_NET	☐
DNP3_SERVER	$HOME_NET	☐
DNP3_CLIENT	$HOME_NET	☐
MODBUS_CLIENT	$HOME_NET	☐
MODBUS_SERVER	$HOME_NET	☐
ENIP_CLIENT	$HOME_NET	☐
ENIP_SERVER	$HOME_NET	☐

5. Настройте нужные переменные. Для этого в строке переменной активируйте поле ввода в столбце "Сетевой объект / Сервис" и укажите сетевые объекты или сервисы.

   Совет. Для поиска в списке нужной переменной используйте строку поиска, расположенную в верхней части окна.

   Для указания сетевых объектов или сервисов можно пользоваться их перечислением через запятую (при этом содержание переменной нужно заключить в скобки), а также другими переменными (в формате $Имя_переменной) и флагом инверсии (или символом "!" непосредственно перед именем переменной). Пользователь может создать новую переменную СОВ, воспользовавшись кнопкой  .

   Совет. При необходимости исключения из совокупности сетевых объектов какого-либо элемента можно использовать новую переменную, указав в ней необходимый для исключения сетевой объект и установив для нее флажок инверсии.

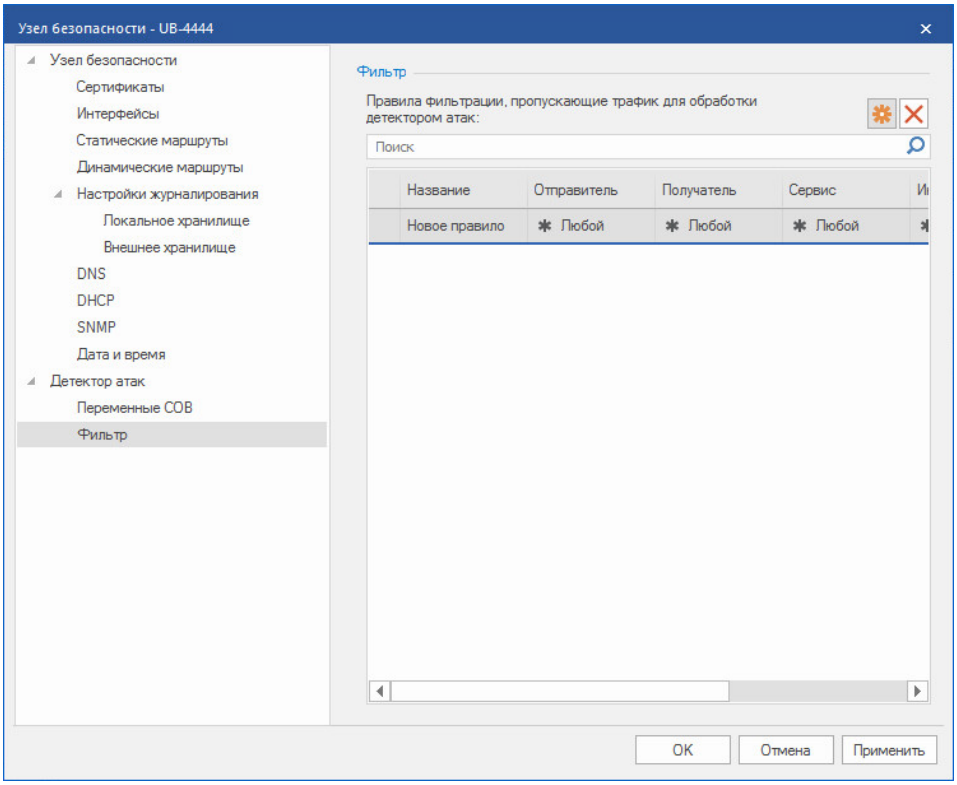
6. Нажмите кнопку "Применить".
7. Выберите в левой части окна в разделе "Детектор атак" пункт "Фильтр". Правила в пункте "Фильтр" пропускают трафик на обработку ДА. Раздел "Фильтр" актуален только для режима Monitor.

   Справа появится список правил фильтрации, созданных для данного детектора атак.

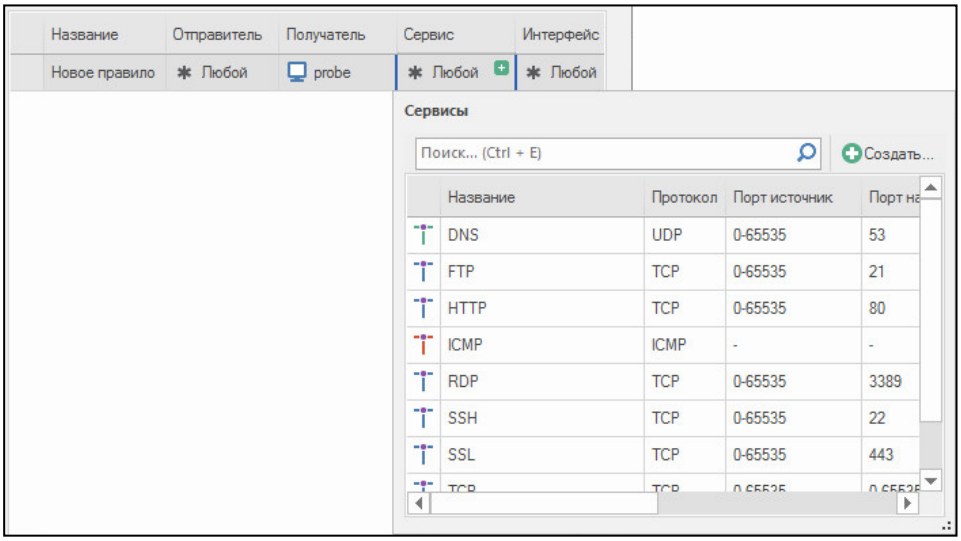
   Примечание. Если правила не создавались, список будет пустым.

8. Добавьте в список новое правило, нажав кнопку  .

   В списке появится строка нового правила.



9. Активируя в строке правила поля ввода и нажимая соответствующие кнопки , выберите из предлагаемых вариантов нужные значения параметров.



10. При необходимости добавьте в список другое правило или правила.

Для настройки конфигурации прокси-сервера:

> **Примечание.** Для совместной работы с прокси-сервером в комплексе предусмотрены инструменты определения отправителя, располагающегося за прокси-сервером или цепочкой прокси-серверов. Методы для прямого и обратного прокси-серверов разные.

1. Перейдите в раздел "Структура" Менеджера конфигурации, выберите детектор атак и вызовите окно настройки свойств.
2. Выберите в левой части окна раздел "Детектор атак" и выставите отметку в поле "Конфигурация прокси".
3. Выберите тип прокси (прямой или обратный) и нажмите кнопку "ОК".
4. Для применения настроек нажмите кнопку "Установить политику" на панели инструментов, отметьте компоненты комплекса с измененными параметрами и нажмите кнопку "ОК".

Настройка ДА по схеме Inline (интерфейсы, режим bypass, хранение трафика атаки)

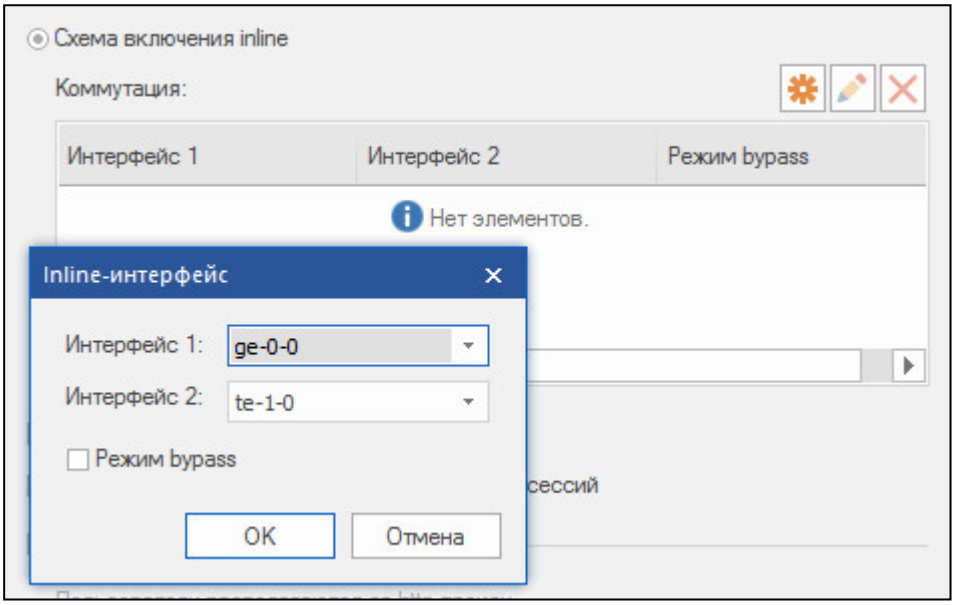
Для настройки параметров:

1. Вызовите окно настройки свойств требуемого ДА в разделе "Структура" Менеджера конфигурации и выберите в левой части окна раздел "Детектор атак".

   В правой части окна отобразятся настройки режима работы ДА.

2. Выберите схему включения Inline и в списке "Коммутация" добавьте Inline-интерфейсы. Для этого нажмите кнопку "Добавить" .

   На экране появится окно настройки Inline-интерфейсов.



3. Установите соответствие логических и физических Inline-интерфейсов.
4. 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.

5. Нажмите кнопку "Да" в окне сообщения.

   Назначенные интерфейсы появятся в списке коммутации интерфейсов ДА по схеме включения Inline.

6. При необходимости установите отметку в поле "Сохранять сетевой трафик атаки".

   В этом случае в журнале безопасности в детальной информации о событии будет доступен для скачивания соответствующий файл в формате CSV.

7. Нажмите кнопку "ОК".

   Созданные настройки будут сохранены и окно "Свойства узла" автоматически закроется.

8. Для применения настроек нажмите кнопку "Установить политику" на панели инструментов, отметьте ДА с измененными параметрами и нажмите кнопку "ОК".

Настройка ДА по схеме Monitor (интерфейсы и хранение трафика атаки)

Для настройки режима:

1. Вызовите окно настройки свойств требуемого ДА в разделе "Структура" Менеджера конфигурации и выберите в левой части окна раздел "Детектор атак".

   Справа отобразится окно настройки режима работы ДА.
2. Выберите схему включения Monitor.
3. Если не указан интерфейс мониторинга, нажмите кнопку  и выберите в появившемся списке нужный физический интерфейс. В окне подтверждения нажмите кнопку "Да".
4. В окне свойств ДА нажмите кнопку "ОК".

   Созданные настройки будут сохранены и окно "Свойства узла" автоматически закроется.

Создание и настройка профиля СОВ

В системе доступны предустановленные профили:

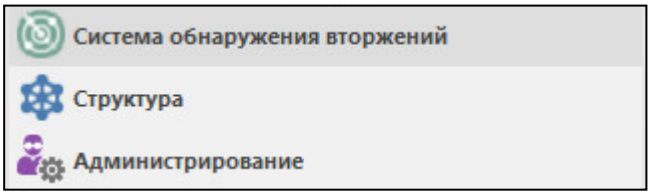
- Оптимальный набор, содержащий базовую выборку из правил, детектирующих угрозы для служб передачи данных, веб-клиентов и веб-серверов.
- Полный набор, содержащий полную выборку правил.
- Рекомендованный набор, содержащий выборку правил на наиболее опасные угрозы.

Данные профили можно использовать для настройки работы детектора атак, но редактировать их нельзя.

Совет. В процессе эксплуатации комплекса целесообразно перед созданием нового профиля СОВ провести обновление БРП (см. стр. 56). Для этой процедуры необходима соответствующая лицензия.

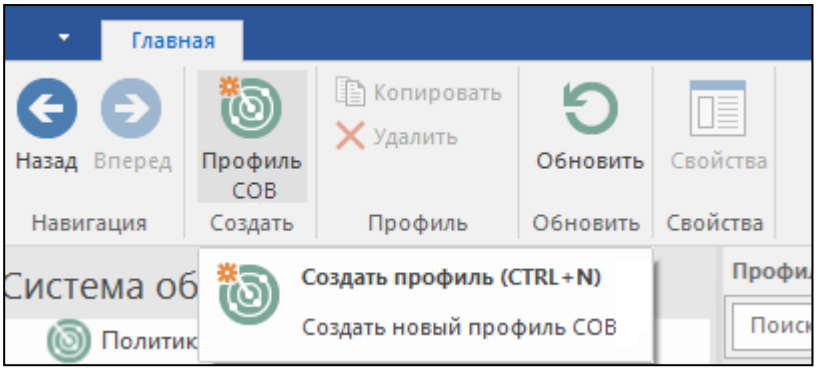
Для создания и настройки профиля СОВ:

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

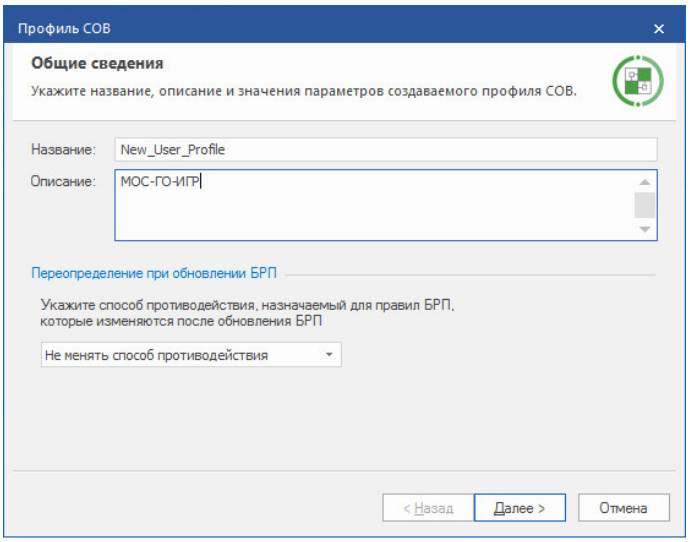


2. Перейдите в подраздел "Профили СОВ".

   Справа появится список созданных профилей.
3. Нажмите на панели инструментов кнопку "Создать новый профиль".



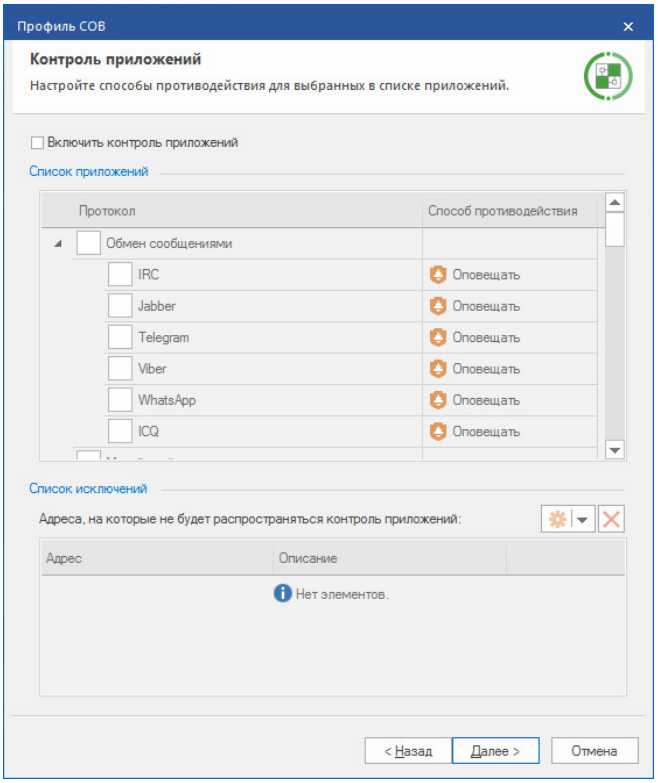
На экране появится диалоговое окно мастера создания профиля СОВ.



4. Заполните поля "Название" и "Описание", укажите способ противодействия для используемых в данном профиле правил БРП в случае их изменения при обновлении БРП и нажмите кнопку "Далее".

Способ противодействия	**Описание изменений в профиле СОВ после обновления набора БРП**
Не менять способ противодействия	Способ противодействия для обновленных вендорских сигнатур не будет изменен
Блокировать	Способ противодействия для обновленных вендорских сигнатур изменится на "Блокировать"
Оповещать	Способ противодействия для обновленных вендорских сигнатур изменится на "Оповещать"
Пропустить	Способ противодействия для обновленных вендорских сигнатур изменится на "Пропустить"

На экране появится диалог "Контроль приложений".

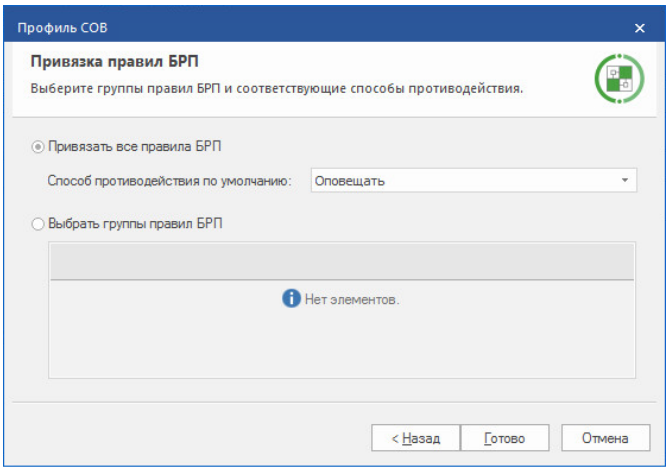


5. При необходимости включения контроля приложений установите отметку в поле "Включить контроль приложений" и назначьте способ противодействия для каждого приложения.

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

6. При необходимости настройки списка исключений для сетевых объектов, на которые не будет распространяться контроль приложений, нажмите кнопку добавления исключения (для указания группы IP-адресов выберите в раскрывающемся списке слева от кнопки добавления пункт "Сетевой объект") и укажите IP-адреса и описания (при необходимости) этих объектов.
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".

Внимание! Для ДА, функционирующих в режиме Monitor, способ противодействия "Блокировать" будет функционировать как "Оповещать".

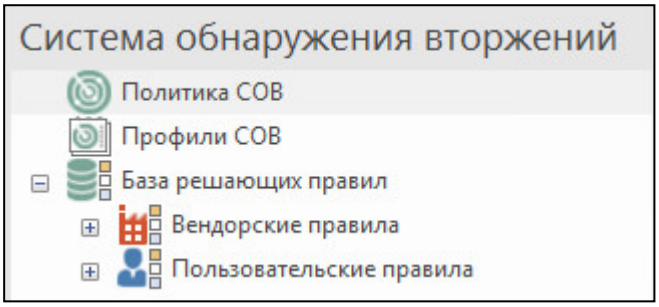
В результате будет создан новый профиль, параметры которого отобразятся в списке на экране, а в подразделе "База решающих правил" в таблице со списком решающих правил появится колонка с названием созданного профиля.

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

Создание и настройка правил политики СОВ

Для создания и настройки правил:

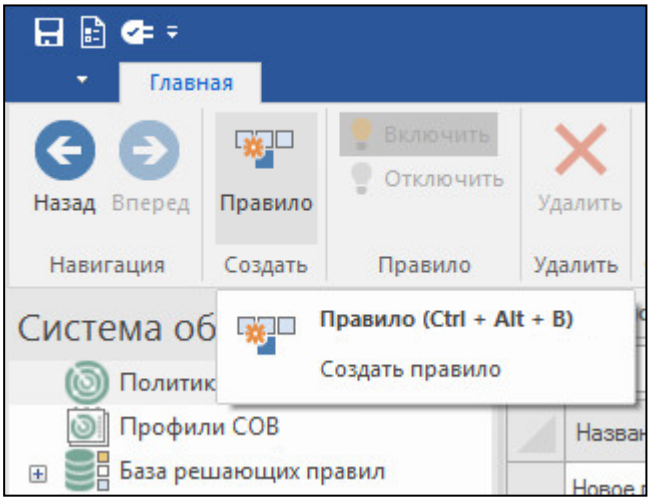
1. В разделе "Система обнаружения вторжений" перейдите на подраздел "Политика СОВ".



Справа отобразится список правил.

Примечание. Если правила не создавались, список будет пустым.

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



В списке правил появится строка нового правила.

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

Название	Введите название правила
Профиль	Выберите из списка профиль СОВ
Установить	Выберите из списка ДА, которому должно быть назначено правило. Для удаления уже выбранного ДА выберите его и нажмите клавишу <Delete>
Описание	Введите описание или пояснение к данному правилу

Управление БРП

Обновление БРП

Загрузка и обновление БРП в ручном или автоматическом режиме происходит на уровне БД ЦУС. Для распространения обновленных правил на узлы безопасности администратору требуется изменить соответствующие профили СОВ (см. стр. **52**).

Если БРП в базе данных ЦУС была обновлена после истечения лицензии на обновление БРП, то при установке политики с обновленной БРП на детектор атак произойдет следующее:

- новые правила на детектор атак установлены не будут;
- правила, которые в обновленной базе были удалены, удалятся с детектора атак;
- правила, которые в обновленной базе были изменены, не обновятся (останутся такими же, какими были до окончания срока действия лицензии).

Примеры:

При обновлении БРП до истечения лицензии:

1. На детектор атак установлен набор правил.
2. Обновление БРП устанавливается в базу данных ЦУС.
3. Истекает лицензия на обновление БРП.
4. Устанавливается политика с обновленным набором правил на детектор атак.

Итог: на детекторе атак удалятся правила, которых нет в обновленной БРП, добавятся новые правила и обновятся измененные.

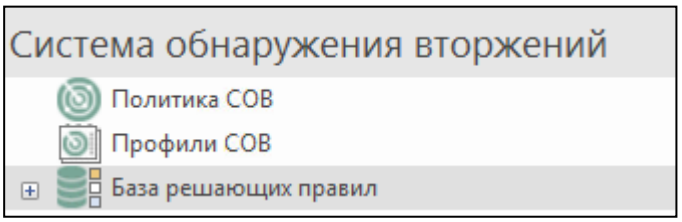
При обновлении БРП после истечения лицензии:

1. На детектор атак установлен набор правил.
2. Истекает лицензия на обновление БРП.
3. Обновление БРП устанавливается в базу данных ЦУС.
4. Устанавливается политика с обновленным набором правил на детектор атак.

Итог: на детекторе атак удалятся правила, которых нет в обновленной БРП, не добавятся новые правила и не обновятся измененные.

Для локальной загрузки обновлений:

1. Подготовьте файл обновлений, полученный от поставщика БРП.
2. Откройте Менеджер конфигурации, перейдите на вкладку "Система обнаружения вторжений" и войдите в раздел "База решающих правил".



3. Нажмите кнопку "Импортировать" на панели инструментов.

   На экране появится стандартное окно выбора файла.
4. Выберите файл с обновлениями БРП и выполните загрузку.

   Будет выполнена загрузка БРП, что займет некоторое время, после чего на экране появится сообщение: "Файл загружен".
5. Нажмите кнопку "ОК" в окне сообщения.

   В окне Менеджера конфигурации отобразится список обновленных правил.

Правило БРП					Профили СОВ		
Важность	Описание	Класс	Ревиз...	Идент...	Оптимальный н...	Полный набор	Рекомендованн...
Высокая	SSL Cert Used In Unknown Exploit Kit	Потенциально опасные s...	1	4115...	Отключить	Блокировать	Отключить
Высокая	Possible Locky AlphaNum Download...	Программа загрузчик вр...	2	4123...	Блокировать	Блокировать	Блокировать
Средняя	Known Tor Relay/Router (Not Exit) N...	Потенциально опасный т...	3281	4213...	Отключить	Оповещать	Отключить
Высокая	W32/Liftoh.Downloader Get Final Pa...	Программа загрузчик вр...	3	4117...	Блокировать	Блокировать	Блокировать
Высокая	Win32/CryPy Ransomware Encryptin...	Криптолокеры	2	4123...	Блокировать	Блокировать	Блокировать

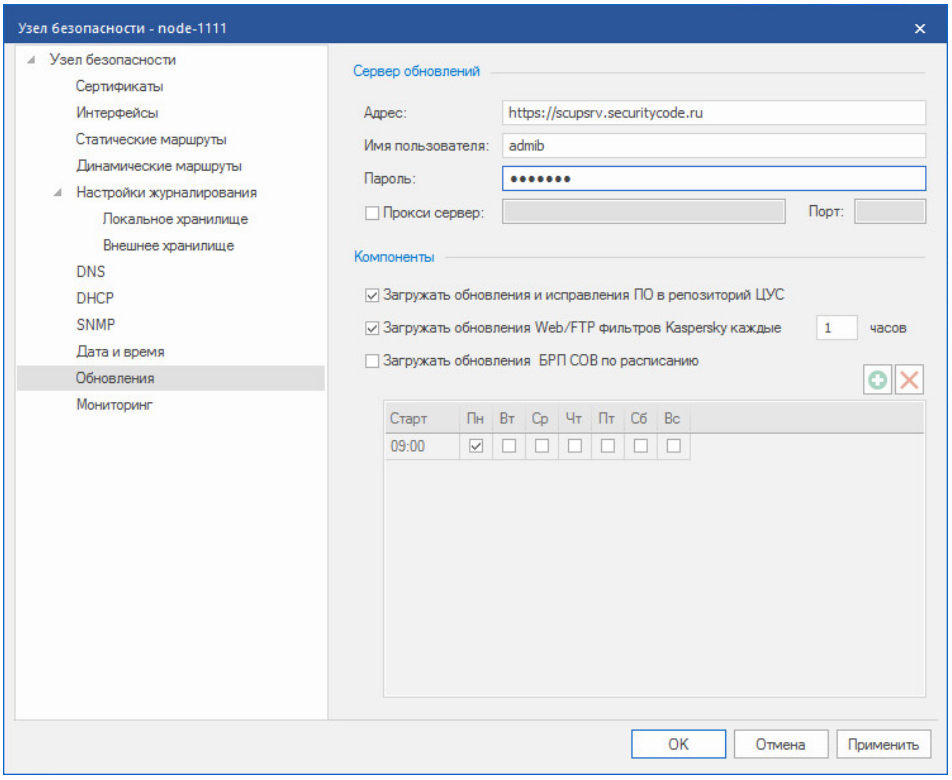
6. Сохраните изменения в конфигурации домена, нажав кнопку в левом верхнем углу Менеджера конфигурации.

Для дистанционной загрузки с сервера обновлений по расписанию:

1. Откройте Менеджер конфигурации и перейдите в раздел "Структура".
2. В списке узлов безопасности выберите необходимый ЦУС и нажмите кнопку "Свойства" на панели инструментов.

   На экране появится окно "Свойства узла".
3. Выберите в левой части окна в разделе "Узел безопасности" пункт "Обновления".

   В правой части окна появятся параметры автоматического обновления ПО.



4. Для настройки параметров выполните следующие действия:
   - Проверьте адрес сервера обновлений.

     Внимание! При написании пути обновления необходимо указать протокол HTTPS.

     Примечание. Источником обновления БРП является сервер обновлений https://scupsrv.securitycode.ru.
   - Укажите учетные данные пользователя с правами администратора.

     Примечание. Для получения учетных данных необходимо обратиться в службу технической поддержки поставщика базы решающих правил (ООО "Код Безопасности") по электронной почте support@securitycode.ru.
   - При необходимости использования прокси-сервера укажите параметры соединения.

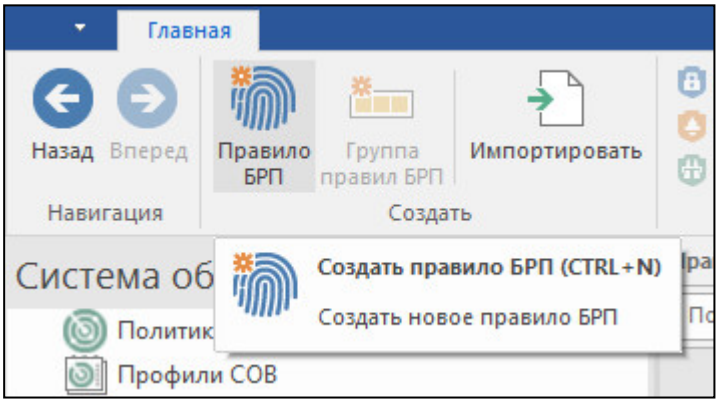
- Установите флажок в пункте "Загружать обновления БРП СОВ по расписанию".
- В области расписания загрузки БРП нажмите кнопку добавления строки расписания .
- В появившейся строке расписания укажите время и отметьте дни, когда нужно производить обновление БРП.
- При необходимости добавьте в расписание дополнительные строки с указанием интервалов обновлений.

5. Нажмите кнопку "ОК" в окне диалога, после чего сохраните изменения в конфигурации домена, нажав кнопку в левом верхнем углу Менеджера конфигурации.
6. Для применения настроек нажмите кнопку "Установить политику" на панели инструментов, отметьте ЦУС и его подчиненные УБ и нажмите кнопку "ОК".

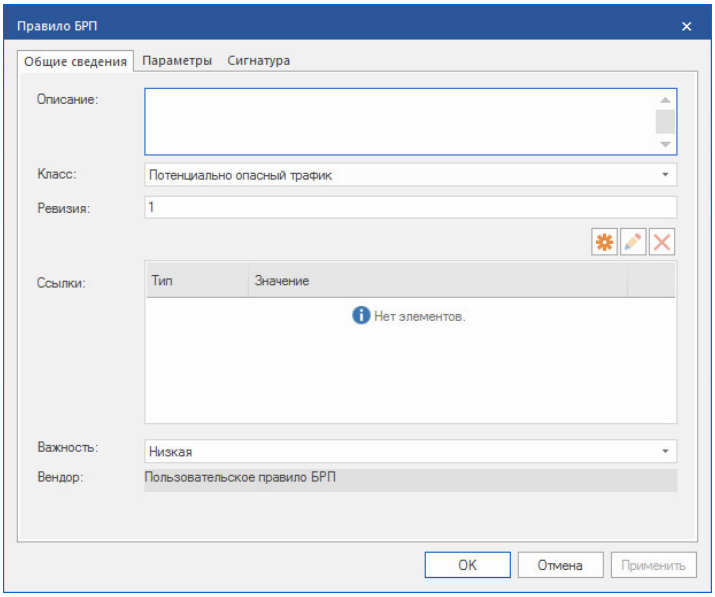
Создание пользовательского решающего правила

Для создания пользовательского правила:

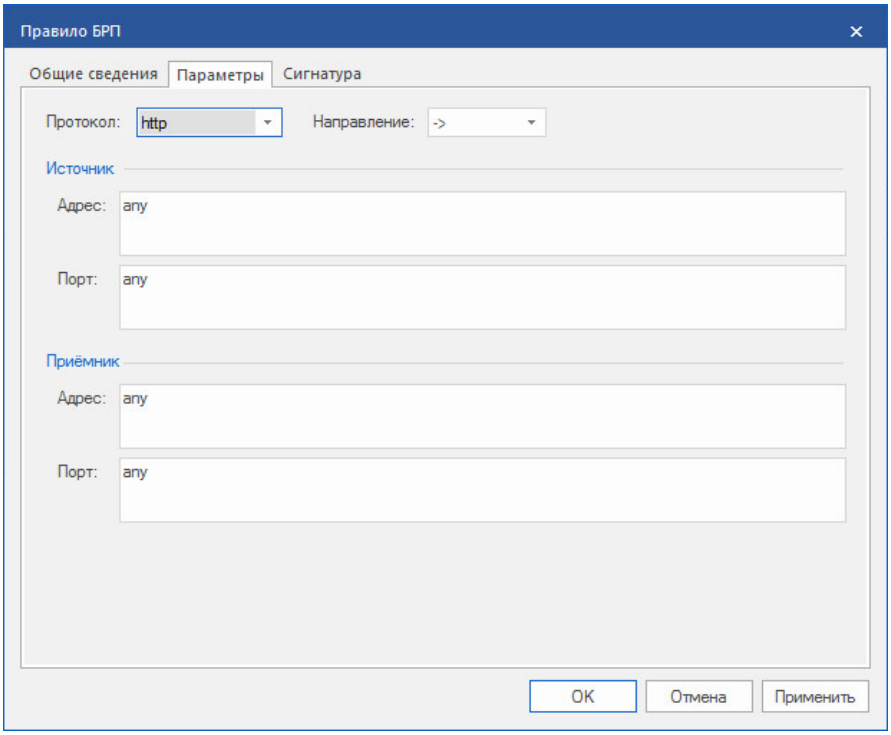
1. На вкладке "Система обнаружения вторжений" МК перейдите в подраздел "База решающих правил/Пользовательские правила" и нажмите на панели инструментов кнопку "Правило БРП".



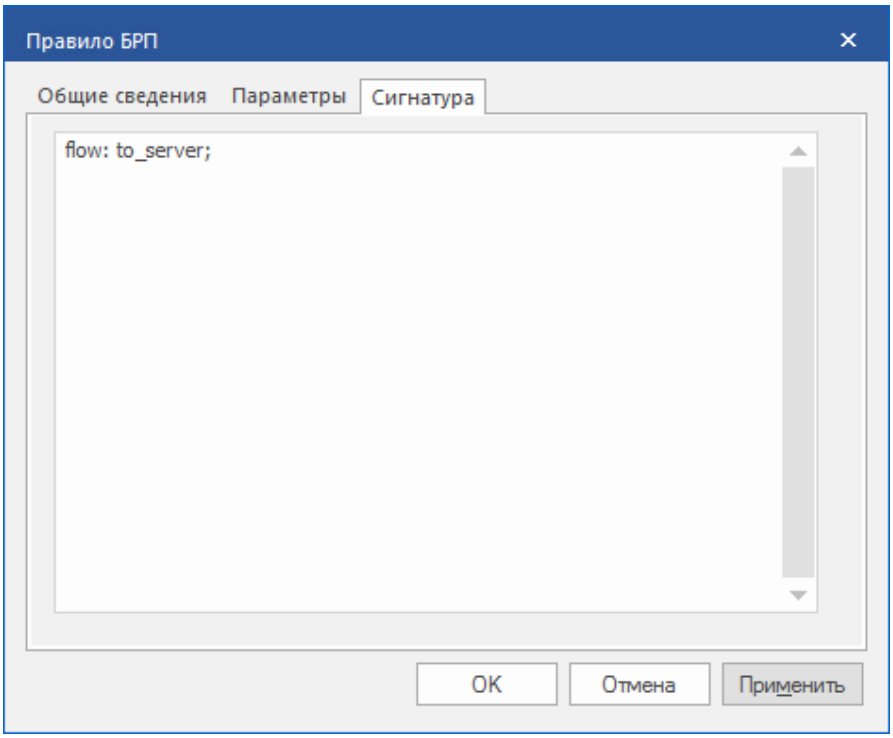
На экране появится окно "Правило БРП".



2. Заполните поля на вкладке "Общие сведения" и перейдите на вкладку "Параметры".



3. Заполните поля заголовка правила (см. стр. **84**) и перейдите на вкладку "Сигнатура".

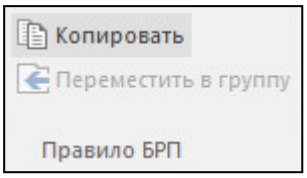


4. Введите опции правила (см. стр. **85**) и нажмите кнопку "ОК".

   Окно "Правило БРП" закроется, и новое правило добавится в список.

Для создания пользовательского правила на основе вендорского:

1. На вкладке "Система обнаружения вторжений" МК перейдите в подраздел "База решающих правил/Вендорские правила", выберите донорское правило и нажмите на панели инструментов кнопку "Копировать".



Глава 7
Обеспечение отказоустойчивости комплекса

Резервное копирование и восстановление

УБ при локальном управлении позволяют создавать резервные копии своих БД, а также осуществлять восстановление БД из резервной копии.

Внимание! В случае переинициализации УБ процедуру восстановления БД из резервной копии необходимо провести сразу после инициализации УБ, не создавая запрос на новый сертификат УБ.

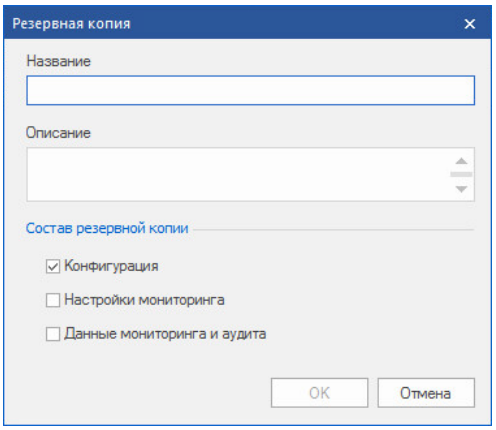
Управление резервными копиями БД ЦУС возможно также с помощью МК.

Создание резервной копии

Для создания резервной копии БД ЦУС в Менеджере конфигурации:

1. В МК перейдите в раздел "Администрирование" и выберите подраздел "Резервные копии".
2. Нажмите кнопку "Резервная копия" на панели инструментов.

   На экране появится окно "Резервная копия".

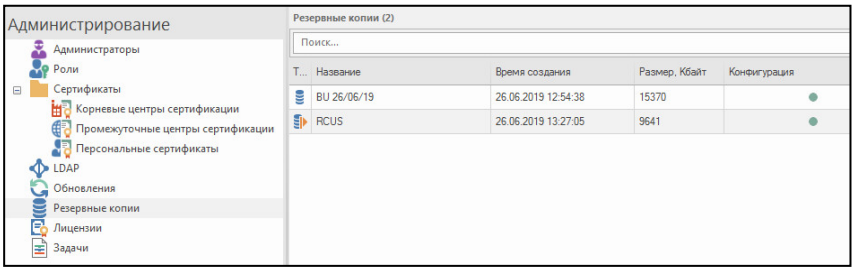


Примечание. При наличии несохраненной конфигурации ЦУС будет предложено применить изменения в конфигурации перед созданием резервной копии.

3. Заполните поля "Название", "Описание", выберите резервируемые компоненты и нажмите кнопку "ОК".

   Начнется создание резервной копии, при этом в списке на экране появится новая строка. До окончания процесса в поле "Размер" будет стоять отметка "создается", а название копии будет сопровождаться значком создаваемой БД.

Примечание. Для резервного ЦУС операция производится аналогично с использованием кнопки "Копия резервного ЦУС". В списке резервная копия такого ЦУС будет отмечаться значком 



Для создания резервной копии при локальном управлении:

1. В главном меню компонента комплекса выберите пункт "Инструменты" и нажмите клавишу <Enter>.

   На экране появится меню "Инструменты".

2. Перейдите к пункту "Резервное копирование и восстановление | Создание резервной копии".

   Появится окно запроса USB-флеш-накопителя.

3. Вставьте внешний носитель в USB-разъем и нажмите клавишу <Enter>.

   Появится окно "Базы для резервного копирования".

4. Выберите клавишей <Пробел> резервируемые компоненты и нажмите клавишу <Enter>.

5. Если был выбран компонент "Данные мониторинга и аудита", на экране появится запрос "Сделать резервную копию данных поисковой машины?". Выберите требуемый вариант ответа и нажмите клавишу <Enter>.

   Будет выполнена запись резервной копии выбранных компонентов на внешний носитель в файл, после чего появится сообщение об успешном завершении операции. Имя файла резервной копии — backup_ID_YYYYMMDD_HHMMSS.c4b, где:

   - ID — идентификатор УБ;
   - YYYYMMDD_HHMMSS — дата и время создания файла.

Восстановление из резервной копии

Для восстановления из резервной копии БД ЦУС в Менеджере конфигурации:

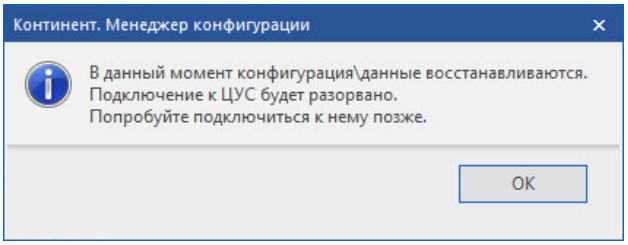
1. В МК перейдите в раздел "Администрирование" и выберите подраздел "Резервные копии".

2. Выберите в списке нужную копию и нажмите кнопку "Восстановить" на панели инструментов.

   На экране появится окно "Восстановление из резервной копии".

3. Выберите восстанавливаемые компоненты из доступных в данной копии и нажмите кнопку "ОК".

   Начнется процесс восстановления, при этом на экране появится соответствующее информационное окно.



Для восстановления конфигурации УБ из резервной копии БД ЦУС:

Примечание. Данная процедура применяется при утере или компрометации ключевой информации УБ.

1. При недоступности УБ в текущей конфигурации ЦУС восстановите рабочую конфигурацию ЦУС из его резервной копии.

2. В МК создайте новый сертификат УБ, укажите его в настройках УБ и осуществите экспорт конфигурации УБ.

3. При локальном управлении проведите повторную инициализацию и настройку подключения к ЦУС. По завершении процедуры проверьте в МК успешное подключение узла.

4. В МК удалите прежний сертификат УБ, подтвердите полученную от УБ конфигурацию (см. стр. **44**).
5. Если в п. **1** было выполнено восстановление конфигурации ЦУС, установите политику на все узлы комплекса (см. стр. **43**).

> **Примечание.** После восстановления кластера рекомендуется создать полную резервную копию ЦУС (см. стр. **61**).

Для восстановления конфигурации УБ из резервной копии при локальном управлении:

> **Внимание!** ЦУС не получает данные о возможных изменениях конфигурации после ее восстановления на УБ из резервной копии. На ЦУС будут поступать только данные о локальных изменениях, выполненных после процедуры восстановления из резервной копии.

1. В главном меню компонента комплекса выберите пункт "Инструменты" и нажмите клавишу <Enter>.

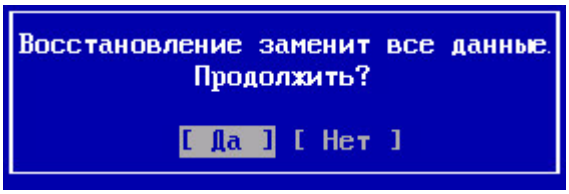
   На экране появится меню "Инструменты".
2. Перейдите к пункту "Резервное копирование и восстановление | Восстановление из резервной копии".

   Появится окно запроса USB-флеш-накопителя.
3. Вставьте внешний USB-флеш-накопитель в USB-разъем и нажмите клавишу <Enter>.

   Появится окно "Выбор резервной копии".
4. Выберите нужный файл и нажмите клавишу <Enter>.

   Появится окно "Базы для восстановления из резервной копии".
5. Выберите клавишей <Пробел> восстанавливаемые БД и нажмите клавишу <Enter>.

   На экране появится запрос на продолжение процедуры.



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

   Будет выполнена процедура восстановления из резервной копии с внешнего носителя, после чего появится сообщение об успешном завершении процедуры восстановления.
7. Если с момента создания резервной копии менялся IP-адрес интерфейса управления ЦУС, требуется добавить его новый IP-адрес в качестве альтернативного и при необходимости дополнить таблицу маршрутизации (см. [**7**], "Смена IP-адреса" и "Настройка параметров маршрутизации").
8. Если восстановленная конфигурация УБ изменяет режим работы его межсетевого экрана, перезагрузите ПО компонента комплекса (см. стр. **46**).
9. Если при восстановлении конфигурации на компоненте комплекса не изменился его IP-адрес интерфейса управления, перейдите к п. **13**.
10. На ЦУС откройте МК и перейдите в подраздел "Структура | Узлы безопасности", выберите узел, на котором была восстановлена конфигурация, и нажмите кнопку "Свойства" на панели инструментов.
11. Выберите в свойствах узла безопасности пункт "Интерфейсы" и настройте соответствующим образом IP-адрес интерфейса управления.
12. Нажмите кнопку "ОК", после чего сохраните изменения в конфигурации узла, нажав кнопку в левом верхнем углу МК.
13. Далее необходимо в МК установить политику (см. стр. **43**) на узел с восстановленной конфигурацией.

Управление резервными копиями

Для управления резервными копиями БД ЦУС:

1. В МК перейдите в раздел "Администрирование" и выберите подраздел "Резервные копии".
2. Для экспорта резервной копии выберите нужную копию, нажмите кнопку "Экспорт" на панели инструментов, укажите место и имя создаваемого файла резервной копии и нажмите кнопку "Сохранить".
3. Для импорта резервной копии нажмите кнопку "Импорт" на панели инструментов, укажите место и имя файла и нажмите кнопку "Открыть".
4. Для удаления резервной копии выберите нужную копию, нажмите кнопку "Удалить" на панели инструментов и нажмите кнопку "Да" в появившемся окне подтверждения.

Глава 8
Обновление программного обеспечения

Обновление ПО комплекса выполняют в следующем порядке:

1. Загрузка файлов обновления в репозиторий (см. ниже).
2. Обновление ПО ЦУС (процедура аналогична процедуре обновления УБ, см. стр. **67**).
3. Обновление МК (см. стр. **67**).
4. Обновление ПО УБ защищаемой сети (см. стр. **67**).

В случае сбоя при обновлении ПО узла безопасности произойдет автоматическое восстановление последней рабочей версии ПО. Повторите процедуру обновления ПО этого узла безопасности еще раз.

Примечание. Информация о версиях ПО на компонентах комплекса отображается в подразделе "Администрирование | Обновления" МК.

Управление репозиторием обновлений

Загрузить файлы обновления в репозиторий можно двумя способами — с сервера обновлений (в том числе без участия администратора) или из локального источника.

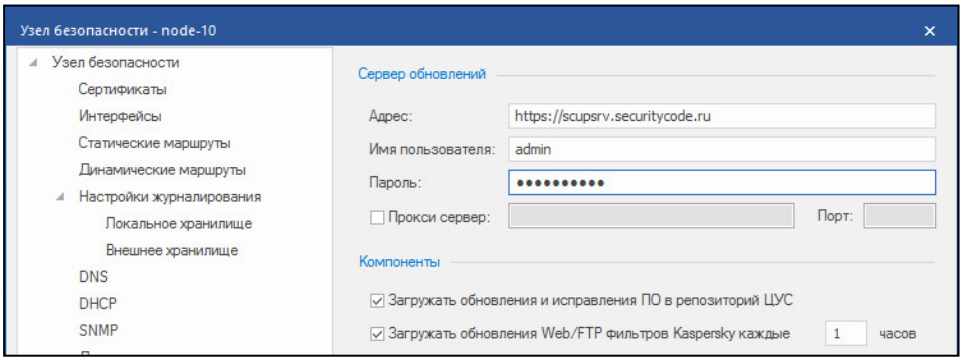
Настройка доступа к серверу обновлений осуществляется в МК только для ЦУС.

Для настройки параметров сервера обновлений:

1. Откройте МК и перейдите в раздел "Структура".
2. В списке узлов безопасности выберите ЦУС и нажмите кнопку "Свойства" на панели инструментов.

   На экране появится окно "Свойства узла".
3. Выберите в левой части окна в разделе "Узел безопасности" подраздел "Обновления".

   В правой части окна появятся параметры обновлений.



4. Для настройки параметров подключения к серверу обновлений выполните следующие действия:
   - Укажите учетные данные пользователя.

     Примечание. Для получения учетных данных пользователя обратитесь в службу технической поддержки (см. стр. **6**).
   - При необходимости использования прокси-сервера укажите его IP-адрес и порт подключения.
5. Для включения автоматической загрузки обновлений и исправлений ПО в репозиторий ЦУС установите отметку в соответствующем поле.
6. Нажмите кнопку "ОК".

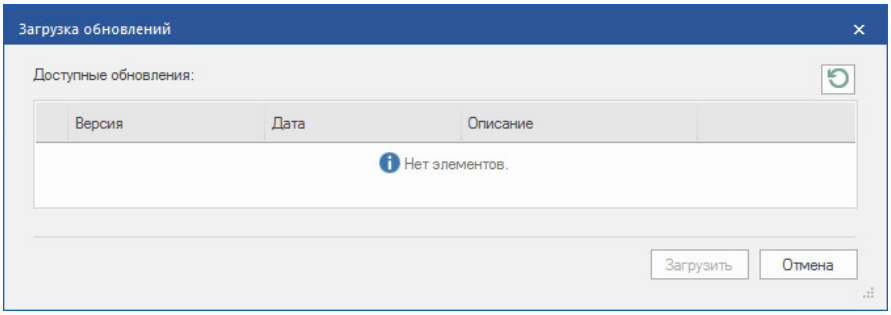
7. Для применения настроек нажмите кнопку "Установить политику" на панели инструментов, отметьте ЦУС и его подчиненные УБ и нажмите кнопку "ОК".

Для принудительной загрузки обновлений в репозиторий:

Примечание. Перед выполнением процедуры необходимо задать все параметры для подключения к серверу обновлений.

1. Откройте МК, перейдите в раздел "Администрирование" и выберите подраздел "Обновления".
2. Нажмите кнопку "Загрузка" на панели инструментов.

   На экране появится окно "Загрузка обновлений".



3. Нажмите кнопку  для получения актуального списка доступных обновлений.

   Будет выполнен запрос к серверу обновлений и, при наличии доступных обновлений, на экране отобразится список ПО.
4. Выберите требуемую версию ПО из списка и нажмите кнопку "Загрузить".

   После загрузки файла с сервера в репозиторий в списке обновлений отобразится новая версия ПО.

Для импорта файла обновления ПО из локального источника:

1. Откройте МК, перейдите в подраздел "Администрирование | Обновления" и нажмите кнопку "Импорт" на панели инструментов.

   На экране появится стандартное окно открытия файла.
2. Укажите файл обновления с расширением *.tgz.signed (при импорте с установочного диска с ПО файлы обновления обычно лежат в корневом каталоге).

   Начнется процесс загрузки файла обновления в базу ЦУС. После успешной загрузки появится соответствующее информационное окно.
3. Нажмите кнопку "ОК".

   В репозитории обновлений появится файл обновления с указанием его типа, версии и размера.

Для удаления файла обновления из репозитория:

1. Откройте МК, перейдите в подраздел "Администрирование | Обновления", выделите ненужный файл обновления и нажмите кнопку "Удалить" на панели инструментов.

   На экране появится окно подтверждения удаления.
2. Нажмите кнопку "Да".

   Файл с обновлением будет удален из репозитория.

Обновление ПО УБ

Внимание! Перед обновлением/откатом ПО рекомендуется создать резервную копию (бэкап) настроек узла, а в случае обновления ПО ЦУС — и его подчиненных узлов.

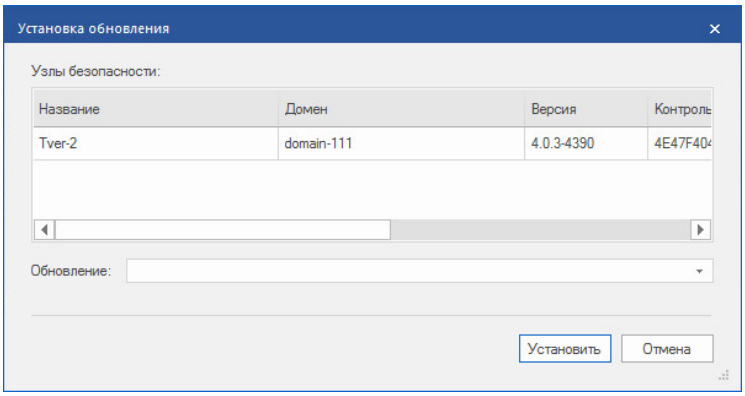
Обновление ПО УБ кластера необходимо проводить в следующем порядке:

1. Выполните обновление ПО компонента кластера со статусом "В ожидании".
2. Назначьте обновленный УБ активным.
3. Выполните обновление ПО компонента кластера со статусом "В ожидании".
4. Установите политику на кластер, затем назначьте требуемый УБ активным.

Для установки обновления ПО:

1. Откройте МК и перейдите в подраздел "Администрирование | Обновления".
2. В списке узлов безопасности выберите нужный узел и нажмите кнопку "Установить обновление" на панели инструментов.

   На экране появится окно "Установка обновления".



3. Выберите нужную версию обновления ПО из раскрывающегося списка поля "Обновление" и нажмите кнопку "Установить" в окне запроса.

   На экране появится сообщение о добавлении новой задачи.

Внимание! После обновления ПО узел безопасности автоматически перезагрузится. В случае обновления ПО ЦУС соединение с МК будет разорвано, после окончания перезагрузки ЦУС необходимо заново установить соединение между МК и ЦУС.

Одновременное обновление активного и резервного ЦУС невозможно. Необходимо дождаться завершения установки обновлений.

Для отмены последнего обновления ПО:

1. Откройте МК и перейдите в подраздел "Администрирование/Обновления".
2. В списке узлов безопасности выберите нужные узлы и нажмите кнопку "Отменить последнее обновление" на панели инструментов.

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

   Будет восстановлена версия ПО до обновления, после чего на экране появится соответствующее информационное окно.
4. Нажмите кнопку "ОК" в окне сообщения.

Обновление Менеджера конфигурации

Для обновления ПО на РМ администратора:

1. В Панели управления ОС Windows на РМ администратора выберите элемент "Программы и компоненты", вызовите контекстное меню программы "Континент. Менеджер конфигурации" и выберите в нем команду "Изменить".
2. В открывшемся окне сервисной программы нажмите кнопку "Далее".

3. В окне обслуживания программ выберите "Удалить" и нажмите кнопку "Далее".

   Начнется процесс деинсталляции ПО.

4. После завершения процесса деинсталляции в появившемся запросе на перезагрузку ПК выберите "Да".

   Будет выполнена перезагрузка РМ администратора для завершения процесса деинсталляции.

5. В Панели управления выберите элемент "Программы и компоненты", вызовите контекстное меню программы "Код Безопасности CSP" и выберите в нем команду "Удалить".

6. В открывшемся окне сервисной программы нажмите кнопку "Да".

   Начнется процесс деинсталляции ПО.

7. После завершения процесса деинсталляции в появившемся запросе на перезагрузку ПК выберите "Да".

   Будет выполнена перезагрузка РМ администратора для завершения процесса деинсталляции.

8. Поместите установочный диск с дистрибутивом МК в устройство чтения компакт-дисков и перейдите в директорию \Setup\Continent\MS\Rus, а затем выберите директорию, соответствующую разрядности ОС РМ администратора.

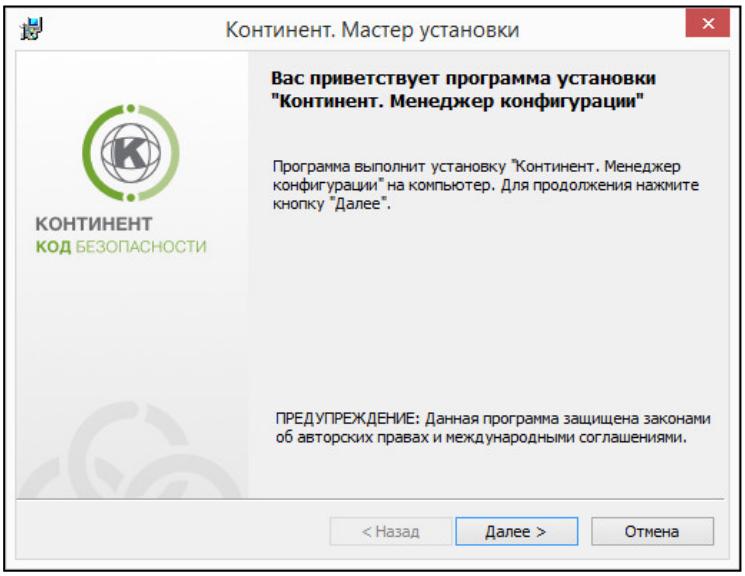
   Примечание. В случае если дистрибутив МК получен при критическом обновлении ПО по сети интернет, перейдите к директории, содержащей файл дистрибутива.

9. Запустите файл Setup.exe.

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

11. Нажмите кнопку "Install" или "Установить".

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



12. Нажмите кнопку "Далее >" для продолжения установки.

    Появится диалог с текстом лицензионного соглашения.

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

    Если вы согласны с условиями лицензионного соглашения, установите отметку в поле "Я принимаю условия лицензионного соглашения", а затем нажмите кнопку "Далее >" и перейдите к следующему шагу установки.

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

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

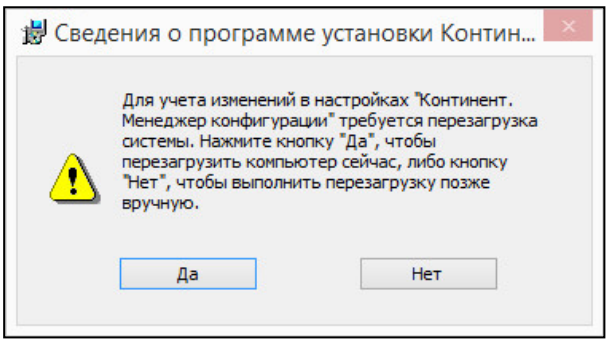
Для выбора папки используйте кнопку "Изменить". По умолчанию программа установки копирует файлы на системный диск в папку ..\Program Files\Security Code\Continent.

На экране появится окно проверки выбранных настроек. На этом шаге перед началом копирования файлов можно проверить и откорректировать выполненные настройки. Для корректировки настроек используйте кнопку "< Назад".

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

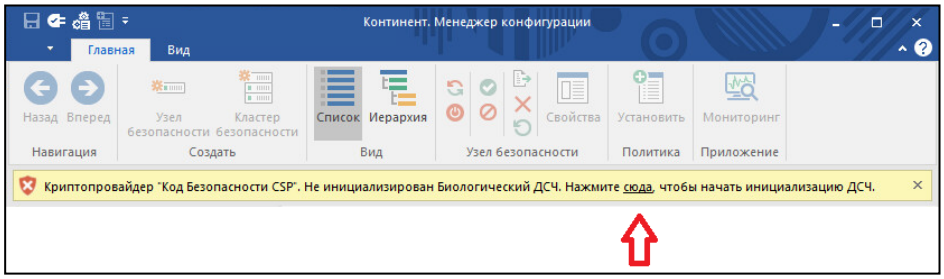
Программа установки приступит к копированию файлов на жесткий диск компьютера. Ход выполнения процесса копирования отображается на экране в специальном окне. После установки МК на экране появится информационное окно об успешной установке приложения.

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

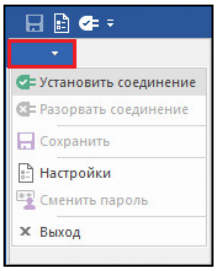


17. Перезагрузите компьютер.

Примечание. При первом запуске МК после его обновления в главном окне может быть отображено информационное сообщение о необходимости выполнить инициализацию биологического 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 МК и в раскрывшемся списке выберите команду "Установить соединение".



Глава 9
Сертификаты безопасности комплекса

Все компоненты комплекса позволяют просматривать имеющиеся на них сертификаты безопасности, делать импорт сертификатов и ключей безопасности, а также создавать запросы на сертификат управления.

ЦУС, помимо этого, позволяет осуществлять создание и экспорт сертификатов:

Тип сертификата	Срок действия	Алгоритм подписи	Примечание
Корневые центры сертификации			
Доверенный издатель КБ	11 лет	ГОСТ 34.10-2012	Предназначен только для связи с сервером обновлений
Корневой сертификат (сертификат УЦ)	5 лет	ГОСТ 34.10-2012	См. стр. **71**
Корневой сертификат RSA (корневой сертификат веб-сервера мониторинга)	5 лет	RSA	См. [**2**], раздел "Настройка подключения к системе"
Персональные сертификаты			
Сертификат администратора	1 год	ГОСТ 34.10-2012	См. стр. **74**
Сертификат узла безопасности (сертификат управления)	1 год	ГОСТ 34.10-2012	См. стр. **72**
Сертификат безопасности веб-сервера мониторинга (сертификат веб-мониторинга)	1 год	RSA	См. [**2**], раздел "Настройка подключения к системе"

Просмотр сертификатов

Для просмотра сертификатов безопасности средствами локального управления:

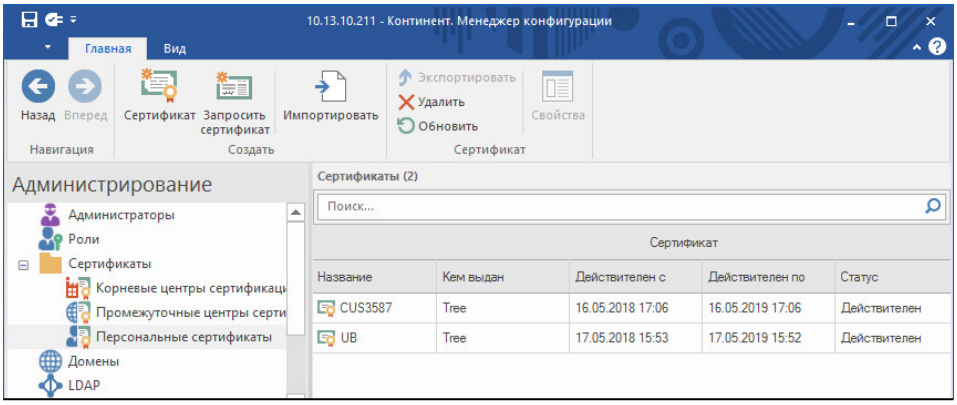
1. В главном меню выберите пункт "Сертификаты" и нажмите клавишу <Enter>.

   На экране появится окно "Сертификаты".
2. Выберите нужный тип сертификатов и нажмите клавишу <Enter>.

   На экране появится окно со списком имеющихся сертификатов данного типа.
3. Для просмотра детальных сведений о сертификате выберите нужный в списке, используя курсоры клавиатуры, и нажмите клавишу <Enter>.
4. Для выхода в предыдущее меню нажмите клавишу <Esc>.

Для просмотра сертификатов безопасности в Менеджере конфигурации:

1. Откройте МК и на панели навигации перейдите в раздел "Администрирование".
2. Для просмотра списка сертификатов раскройте каталог "Сертификаты" и выберите требуемый пункт.



В области отображения информации появится список установленных сертификатов.

Создание сертификатов

Создание корневых сертификатов

Для создания корневого сертификата средствами локального управления ЦУС:

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

   На экране появится окно "Сертификаты".

2. Выберите пункт "Сертификаты УЦ" и нажмите клавишу <Enter>.

   На экране появится окно "Сертификаты УЦ".

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

3. Для создания корневого сертификата нажмите клавишу <F2>.

   На экране появится окно "Выпуск сертификата".

4. Выберите пункт "Выпуск корневого сертификата" и нажмите клавишу <Enter>.

   На экране появится окно "Сертификат".

5. 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".

6. Нажмите клавишу <Enter>.

   Будет выполнен возврат в окно "Выпуск сертификата".

7. Нажмите клавишу <Esc>.

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

8. Нажмите клавишу <Esc>.

   Будет выполнен возврат в меню "Сертификаты".

Для создания корневого сертификата в Менеджере конфигурации:

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

   В правой части экрана появится список установленных персональных сертификатов.
3. Нажмите кнопку "Корневой сертификат" на панели инструментов.

   На экране появится окно "Корневой сертификат".
4. Заполните поля данными о владельце сертификата, установите отметки в требуемых полях назначения ключа, выберите алгоритм подписи, укажите срок действия сертификата и нажмите кнопку "Создать сертификат".

   Будет выполнен возврат к списку корневых сертификатов, в котором отобразится созданный сертификат.

Создание сертификатов управления УБ

Создание сертификата ЦУС осуществляется при локальном управлении ЦУС (см. ниже).

В случае УБ есть два варианта создания сертификата:

- при локальном управлении УБ создать запрос на сертификат (см. стр. **73**), а потом выпустить сертификат на ЦУС (см. стр. **73**) по этому запросу;
- выпустить сертификат на ЦУС без запроса.

> **Примечание.** В этом случае вместе с сертификатом будет выпущен запрос на сертификат, который необходимо импортировать на УБ посредством локального управления УБ (см. стр. **78**). В файле запроса передается контейнер закрытого ключа.

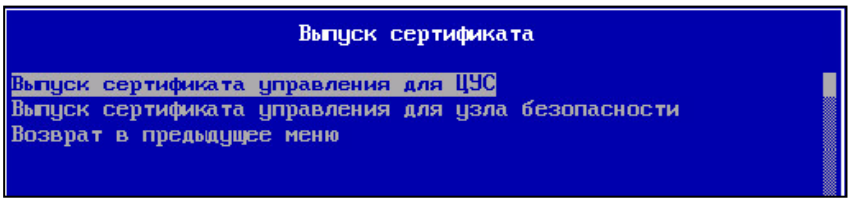
Для создания сертификата управления ЦУС:

1. В главном меню локального управления выберите пункт "Сертификаты" и нажмите клавишу <Enter>.
2. 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.
3. Нажмите клавишу <F2>.

   На экране появится меню "Выпуск сертификата".



4. Выберите пункт "Выпуск сертификата управления для ЦУС" и нажмите клавишу <Enter>.

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

   На экране появится список созданных корневых сертификатов.
6. Выберите корневой сертификат и нажмите клавишу <Enter>.

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

   Будет выполнен возврат в окно "Выпуск сертификата".
8. Нажмите клавишу <Esc>.

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

9. Нажмите клавишу <Esc>.

   Будет выполнен возврат в меню "Сертификаты".

Создание запроса на сертификат управления УБ

Для создания запроса на сертификат УБ средствами локального управления УБ:

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

   На экране появится окно "Сертификаты управления".

2. Вставьте внешний носитель в USB-разъем для экспорта на него файла запроса на сертификат и нажмите клавишу <F4>.

   На экране появится окно "Выпуск запроса на сертификат".

3. Выберите пункт для создания запроса на сертификат управления УБ и нажмите клавишу <Enter>.

   На экране появится меню "Атрибуты идентификации".

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

   На экране появится окно для ввода пароля ключевого контейнера.

5. Введите пароль и нажмите клавишу <Enter>.

   На экране появится окно для ввода названия ключевого контейнера.

6. Введите название и нажмите клавишу <Enter>.

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

7. Нажмите клавишу <F5>, выберите файл запроса (continent-ID.req, где "ID" — серийный номер УБ) и нажмите клавишу <Enter>.

   На экране появится окно для выбора ключевого контейнера.

8. Выберите нужный контейнер и нажмите клавишу <Enter>.

   На экране появится окно для ввода пароля ключевого контейнера.

9. Введите пароль от контейнера и нажмите клавишу <Enter>.

   На экране появится информационное окно об успешном завершении операции.

10. Нажмите клавишу <Enter> для возврата в меню "Выпуск запроса на сертификат", извлеките внешний носитель и перейдите на ЦУС или РМ администратора для выпуска сертификата управления УБ.

Выпуск сертификатов управления УБ

Для выпуска сертификата управления УБ средствами локального управления ЦУС:

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

   На экране появится окно "Сертификаты управления".

2. Вставьте внешний носитель в USB-разъем для импорта с него файла запроса на сертификат (см. выше) и нажмите клавишу <F2>.

   На экране появится меню "Выпуск сертификата".

3. Выберите пункт "Выпуск сертификата управления для УБ" и нажмите клавишу <Enter>.

   На экране появится окно с вопросом о наличии файла запроса на сертификат.

4. Выберите пункт "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.

5. Выберите нужный файл запроса и нажмите клавишу <Enter>.

   На экране появится окно выбора корневого сертификата.

6. Выберите нужный корневой сертификат и нажмите клавишу <Enter>.

   Будет создан файл сертификата управления для УБ, после чего произойдет возврат к окну "Выпуск сертификата".

7. 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 выпуска сертификата управления УБ в Менеджере конфигурации:

1. Откройте МК 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" на панели инструментов.

   На экране появится окно "Сертификат".

4. Выберите в графе "Тип сертификата:" пункт "Узел безопасности".
5. 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.

6. В дополнительных параметрах выберите созданный при развертывании ЦУС корневой сертификат, а также установите требуемый срок действия сертификата управления.
7. Нажмите кнопку "Создать сертификат".

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

Создание сертификатов администратора

Для создания сертификата администратора:

1. Откройте МК 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" на панели инструментов.

   На экране появится окно "Сертификат".

4. Выберите в графе "Тип сертификата:" пункт "Администратор".
5. Введите данные для создаваемого сертификата и отметьте нужные назначения ключа.
6. В дополнительных параметрах выберите созданный при развертывании ЦУС корневой сертификат, а также установите требуемый срок действия сертификата управления.
7. Укажите имя файла ключа и нажмите кнопку "Создать сертификат".

   На экране появится информационное сообщение о необходимости выполнить переинициализацию биологического ДСЧ.

8. Следуйте указаниям на экране и дождитесь завершения процесса накопления энтропии.

   На экране появится окно установки пароля на доступ к ключевому контейнеру.

9. Установите пароль и нажмите кнопку "ОК".

   Внимание! Запомните этот пароль, он понадобится для установки сертификата, а также при аутентификации администратора по сертификату.

   На экране появится окно выбора носителя для хранения ключевого контейнера.

10. Выберите ключевой носитель, при необходимости подключив его и нажав кнопку "Обновить", и нажмите кнопку "ОК".

    В результате будут сформированы файлы сертификата пользователя и его криптографического контейнера, после чего данные сертификата отобразятся в списке на экране.

Установка сертификатов администратора

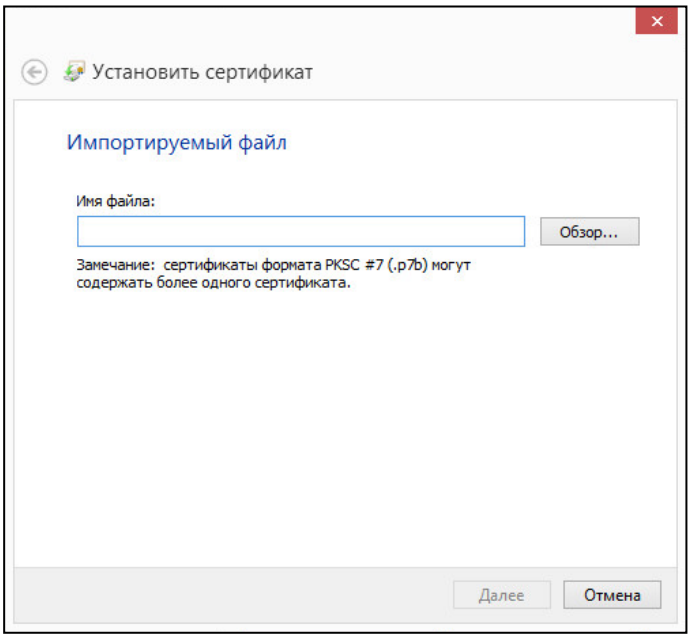
Для выполнения процедуры аутентификации администратора в МК с использованием сертификата необходимо установить сертификат в хранилище учетной записи пользователя. Для этого можно использовать криптопровайдер "Код Безопасности CSP", входящий в состав комплекса.

Внимание! Сторонние криптопровайдеры использовать запрещено.

Для установки сертификата администратора посредством "Код Безопасности CSP":

1. Запустите "Код Безопасности CSP" (Все программы/Код Безопасности/Код Безопасности CSP) и перейдите во вкладку "Сертификаты".
2. Нажмите кнопку "Установить сертификат".

   На экране появится окно мастера установки сертификата.



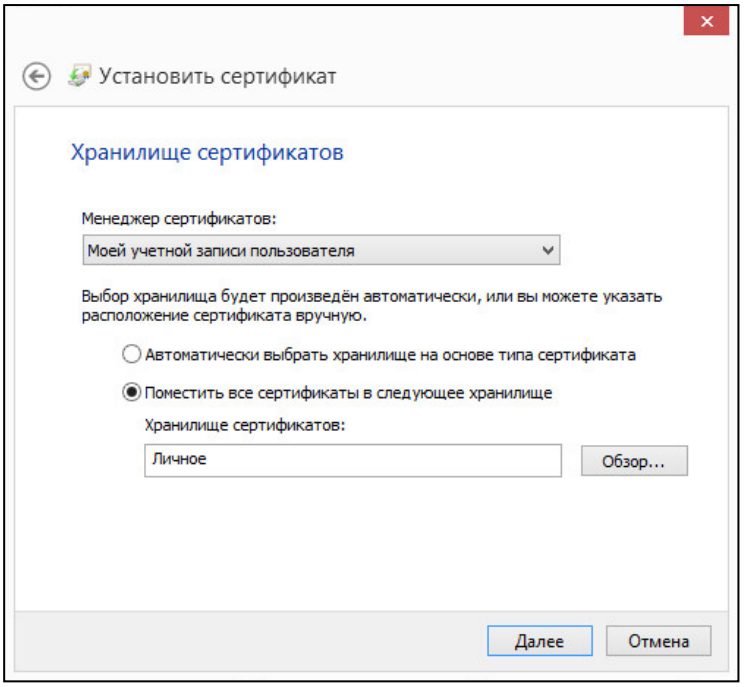
3. Вставьте носитель с файлом сертификата и нажмите кнопку "Обзор".

   На экране появится стандартное окно выбора файла.

4. Укажите файл сертификата и нажмите кнопку "Открыть", а затем "Далее".

   На экране появится окно выбора хранилища сертификатов.

5. Настройте установку сертификата в личное хранилище учетной записи пользователя и нажмите кнопку "Далее".



На экране появится окно выбора контейнера закрытого ключа сертификата.

Примечание. Анализ внешних носителей может занять некоторое время, список доступных контейнеров будет обновляться по мере считывания информации.

6. Укажите контейнер с ключевой информацией, при необходимости подключив ключевой носитель и нажав кнопку "Обновить", и нажмите кнопку "Далее".

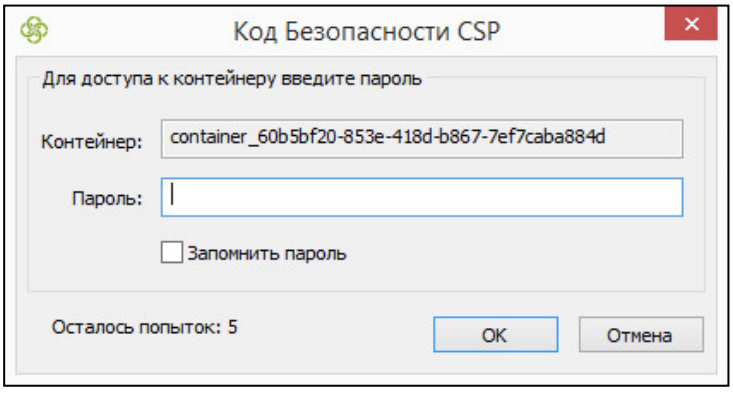
   На экране появится завершающее окно мастера установки сертификата.

7. Проверьте введенные данные и нажмите кнопку "Готово".

   На экране появится информационное сообщение о необходимости выполнить переинициализацию биологического ДСЧ.

8. Следуйте указаниям на экране и дождитесь завершения процесса накопления энтропии.

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



9. Введите пароль и нажмите кнопку "ОК".

   При корректно введенном пароле будет выполнена установка сертификата в личное хранилище сертификатов пользователя, после чего на экране появится соответствующее информационное окно.

10. Нажмите кнопку "ОК".

Смена сертификатов

Для смены сертификата управления ЦУС в МК:

1. Перейдите в раздел "Администрирование".
2. На панели навигации в папке "Сертификаты" выберите подраздел "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. Подключите внешний USB-флеш-накопитель.
6. Нажмите кнопку ..., выберите корневой каталог внешнего USB-флеш-накопителя для записи файлов и нажмите кнопку "Сохранить".
7. Нажмите кнопку "Создать сертификат".

   На экране появится окно для ввода пароля на доступ к контейнеру.
8. Задайте и подтвердите пароль, затем нажмите кнопку "ОК".

   Примечание. Минимальная длина пароля — 6 символов.

   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.
9. Сохраните изменения в конфигурации узла, нажав кнопку  в левом верхнем углу МК.
10. В главном меню локального управления ЦУС выберите меню "Сертификаты" и нажмите клавишу <Enter>.
11. В меню "Сертификаты" выберите пункт "Сертификаты управления" и нажмите клавишу <Enter>.

    На экране появится окно "Сертификаты управления".
12. Вставьте внешний носитель в USB-разъем и нажмите клавишу <F5> для импорта запроса на сертификат.

    На экране появится окно выбора файла запроса.
13. Выберите нужный файл с расширением .req и нажмите клавишу <Enter>.

    На экране появится окно выбора контейнера закрытого ключа.
14. Выберите нужный контейнер и нажмите клавишу <Enter>.

    На экране появится окно ввода пароля.
15. Введите пароль и нажмите клавишу <Enter>.

    Выполнится импорт файла запроса сертификата и ключевой информации, после чего на экране появится сообщение об успешном завершении операции.
16. Нажмите клавишу <Enter>.
17. Откройте МК и перейдите в раздел "Структура".

    В правой части окна отобразится список УБ комплекса.
18. Выберите ЦУС и нажмите кнопку "Свойства" на панели инструментов.

    На экране появится окно свойств УБ.
19. Выберите в левой части окна в разделе "Узел безопасности" пункт "Сертификаты".

20. В области серверных или корневых сертификатов выберите старый сертификат и нажмите кнопку исключения сертификата.

    Сертификат будет удален из списка.

21. В области серверных или корневых сертификатов нажмите кнопку добавления нового сертификата.

    На экране появится окно "Сертификаты".

22. Выберите в списке требуемый сертификат.

    Сертификат отобразится в списке.

23. Нажмите кнопку "ОК".

24. Сохраните изменения в конфигурации узла, нажав кнопку в левом верхнем углу МК, и установите политику на ЦУС (см. стр. **43**).

25. По завершении выполнения задачи по установке политики на ЦУС установите политики на подчиненные ему узлы комплекса.

Для смены сертификатов:

1. Откройте МК и перейдите в раздел "Структура".
2. В области отображения информации выберите требуемый УБ и нажмите кнопку "Свойства" на панели инструментов.

   На экране появится окно свойств УБ.

3. Выберите в левой части окна в разделе "Узел безопасности" пункт "Сертификаты".
4. В области серверных или корневых сертификатов выберите старый сертификат и нажмите кнопку исключения сертификата.

   Сертификат будет удален из списка.

5. В области серверных или корневых сертификатов нажмите кнопку добавления нового сертификата.

   На экране появится окно "Сертификаты".

6. Выберите в списке требуемый сертификат.

   Сертификат отобразится в списке.

7. Нажмите кнопку "ОК".
8. Сохраните изменения в конфигурации узла, нажав кнопку в левом верхнем углу МК, и установите политику на этот УБ (см. стр. **43**).

Экспорт сертификатов

Для экспорта сертификата:

1. Откройте МК и перейдите в раздел "Администрирование".
2. Раскройте список сертификатов и выберите требуемый тип.

   В правой части экрана появится список установленных сертификатов.

3. Вызовите контекстное меню требуемого сертификата и выберите команду "Экспортировать".

   На экране появится стандартное окно сохранения файла сертификата.

4. Выберите место для сохранения файла, укажите имя и тип файла, а затем нажмите кнопку "Сохранить".

   После экспорта файла сертификата произойдет возврат к списку сертификатов.

Импорт сертификатов и ключей безопасности

Внимание! Импортируемый сертификат должен иметь имя владельца (subject), не совпадающее с уже установленными сертификатами.

Для импорта сертификатов в Менеджере конфигурации:

1. Откройте МК и перейдите в раздел "Администрирование".
2. Раскройте список сертификатов и выберите требуемый тип.

   В правой части экрана появится список установленных сертификатов.
3. Нажмите кнопку "Импортировать" на панели инструментов.

   На экране появится стандартное окно открытия файла.
4. Выберите нужный файл и нажмите кнопку "Открыть".

   После успешного импорта сертификата появится соответствующее сообщение.
5. Нажмите кнопку "ОК" в окне сообщения.

   Список установленных сертификатов будет обновлен.

Для импорта сертификатов УЦ или УБ средствами локального управления:

1. В меню "Сертификаты" выберите нужный тип сертификатов и нажмите клавишу <Enter>.
2. Вставьте внешний носитель в USB-разъем для импорта с него файлов и нажмите клавишу <F3>.

   На экране появится окно для выбора файла.
3. Выберите файл сертификата (*.cer) и нажмите <Enter>.

   На экране появится информационное окно об успешном завершении операции.
4. Нажмите клавишу <Enter>.

Смена сертификата управления

Для смены сертификата управления компонента комплекса:

1. Создайте новый сертификат управления с помощью локального управления или МК (см. стр. **72**).
2. Откройте МК и перейдите в раздел "Структура".
3. В списке узлов безопасности выберите необходимый узел и нажмите кнопку "Свойства" на панели инструментов.

   На экране появится окно "Свойства узла".
4. Выберите в левой части окна в разделе "Узел безопасности" пункт "Сертификаты".
5. В области серверных сертификатов выберите старый сертификат и нажмите кнопку исключения сертификата  .
6. В области серверных сертификатов нажмите кнопку добавления нового сертификата  .

   На экране появится окно "Сертификаты".
7. Выберите в списке нужный сертификат и нажмите кнопку "ОК".
8. Сохраните изменения в конфигурации узла, нажав кнопку  в левом верхнем углу МК, и установите политику на этот компонент комплекса (см. стр. **43**).
9. Если смена сертификата управления происходит на ЦУС, то по завершении выполнения задачи по установке политики на ЦУС установите политики на подчиненные ему узлы комплекса.

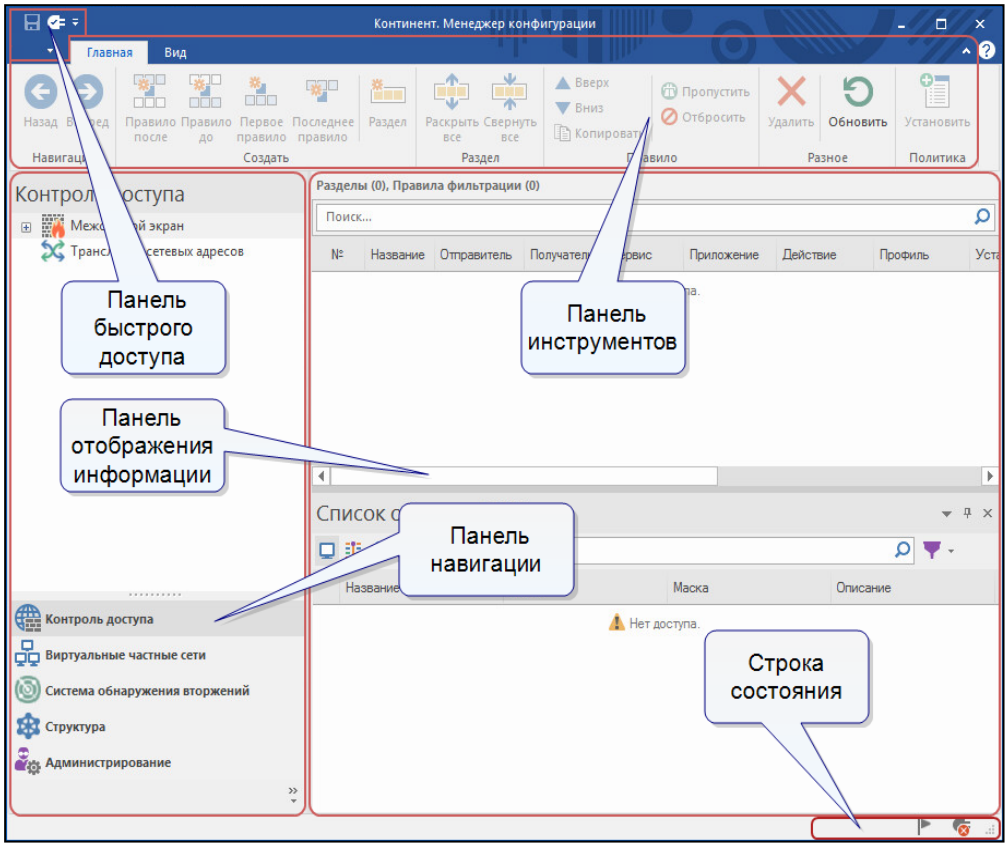
Приложение

Запуск Менеджера конфигурации

Для запуска Менеджера конфигурации:

- Активируйте в главном меню Windows команду "Код Безопасности | Менеджер конфигурации" или на рабочем столе Windows ярлык приложения "Менеджер конфигурации".

  На экране появится окно "Менеджер конфигурации".



Окно "Менеджер конфигурации" содержит следующие основные элементы интерфейса:

Элемент интерфейса	Описание
	Содержит набор инструментов и две вкладки: • "Главная" — отображает панель инструментов; • "Вид" — настройка отображения элементов окна Менеджера конфигурации. Инструменты — это функциональные кнопки, предназначенные для запуска часто используемых команд. Состав кнопок зависит от выбора подраздела на панели навигации, а их доступность определяется рабочей ситуацией. При наведении курсора мыши на кнопку появляется всплывающая подсказка с дополнительной информацией

Элемент интерфейса	Описание
Панель быстрого доступа	Предназначена для быстрого доступа к часто используемым командам. Содержит кнопки: •  — сохранение текущей конфигурации; •  — установка политики безопасности; •  — настройка подключений к ЦУС и вида панели быстрого доступа; •  — установка соединения с ЦУС; •  — настройка панели быстрого доступа; •  — вызов меню команд быстрого доступа
Панель навигации	Содержит следующие разделы: • "Контроль доступа" — предназначен для управления правилами фильтрации и трансляции трафика; • "Виртуальные частные сети" — предназначен для создания и настройки параметров VPN; • "Структура" — предназначен для управления параметрами УБ комплекса; • "Система обнаружения вторжений" — предназначен для настройки параметров системы обнаружения и предупреждения вторжений; • "Администрирование" — предназначен для управления сервисными функциями (работа с сертификатами, резервными копиями, управление лицензиями, обновлением и др.)
Панель отображения информации	Предназначена для отображения информации выбранного раздела панели навигации
Строка состояния	Содержит следующие данные: • число выполняемых задач и кнопка вызова центра уведомлений  , содержащего информацию о выполняемых задачах и ссылку на переход к общему списку задач (см. раздел "Администрирование"); • пиктограмма состояния соединения с ЦУС (при установленном соединении – с именем учетной записи авторизованного администратора, к примеру )

Полномочия встроенных ролей администратора

Встроенные роли администратора:

- ГА — главный администратор;
- АС — администратор сети;
- АБ — администратор безопасности;
- АА — администратор аудита.

Ниже приведены полномочия встроенных ролей администратора.

Функция/настройка	ГА	АС	АБ	АА
Управление учетными записями и сертификатами				
Управление учетными записями и ролями администраторов	+	0	0	0
Управление сертификатами (централизованное и локальное)	+	0	+	0
Управление структурой и конфигурацией домена				
Управление сетевыми объектами и сервисами	+	+	0	0

Функция/настройка	ГА	АС	АБ	АА
Регистрация УБ в домене (централизованная и локальная)	+	+	-	-
Управление сетевыми настройками УБ (централизованное и локальное)	+	0	+	0
Управление настройками безопасности УБ	+	0	+	0
Управление обновлениями	+	+	-	-
Создание резервных копий (централизованное)	+	+	+	+
Управление конфигурациями домена (централизованное и локальное)	+	-	-	-
Управление политиками				
Установка политик (централизованная и локальная)	+	+	+	+
Управление политиками СОВ	+	0	+	0
Управление политиками МСЭ	+	+	+	0
Локальное управление				
Работа с аварийным меню	+	-	+	-
Дистанционный доступ к локальному меню	-	-	-	-
Управление журналами	+	-	-	-
Просмотр журналов	+	+	+	+
Диагностика УБ	+	+	-	-
Управление локальными политиками	+	+	+	-
Изменение пароля встроенного администратора	+	-	-	-
Повторная инициализация	+	-	-	-
Завершение работы УБ	+	+	+	-
Мониторинг и диагностика. Страницы системы				
Панель мониторинга	+	+	+	+
Системный журнал	+	+	+	+
Журнал сетевой безопасности	+	-	+	-
Журнал управления	+	+	+	-
Статистика	+	+	+	+
Структура (мониторинг и настройка параметров)	+	+	+	-
Структура (мониторинг и настройка доступа)	+	-	+	-
Управление группами	+	-	+	-
Мониторинг и диагностика. Доступные виджеты дашборда и статистики				
Управление	+	+	+	-
Мониторинг	+	+	+	-
Журнал сетевой безопасности	+	-	+	-
Системный журнал	+	+	+	+
Сетевые интерфейсы	+	+	-	-
Срабатывание сигнатур СОВ/СОА	+	-	+	-
Топ сбойных узлов	+	+	+	+
Количество атак	+	-	+	+
Топ сигнатур	+	-	+	+
Топ источников атак	+	-	+	+
Топ жертв атак	+	-	+	+

+ — полный доступ;

- — недоступно;

0 — просмотр.

Протоколы и порты

В данном разделе представлены сведения о протоколах и портах, используемых для связи между компонентами комплекса. Компонент комплекса, инициирующий сеанс связи, устанавливает подключение со своего случайного порта из динамического диапазона на определенный порт получателя, который, в свою очередь, отвечает на тот порт, с которого было произведено обращение.

Примечание. Динамический диапазон портов, выделенный для подключения на стороне источника, зависит от версии установленной на нем ОС. На ОС, установленной на аппаратных компонентах комплекса, используется диапазон портов 10000–65000.

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

Протокол / порт	Назначение	Источник / получатель
TCP / 22	Передача данных SSH между РМ администратора и ЦУС или УБ	РМ / УБ РМ / ЦУС
TCP / 80	Передача CRL	УБ/ ЦУС ЦУС / ЦУС
TCP / 443	Передача данных мониторинга и аудита между РМ администратора и ЦУС	РМ / ЦУС
	Загрузка обновлений с сервера обновлений (СО) на ЦУС	ЦУС / СО
	Загрузка обновлений с ЦУС на УБ	УБ / ЦУС
TCP / 444	Передача конфигурационных данных между РМ администратора и ЦУС	РМ / ЦУС
TCP / 6666	Канал управления между ЦУС и УБ, вышестоящим и нижестоящим ЦУС	УБ / ЦУС ЦУС / ЦУС
TCP / 8888	Передача журналов с УБ на ЦУС, с нижестоящего на вышестоящий ЦУС	УБ / ЦУС ЦУС / ЦУС
UDP / 123	Передача данных синхронизации NTP между ЦУС и УБ, нижестоящим и вышестоящим ЦУС	УБ / ЦУС ЦУС / ЦУС
UDP / 161	Передача данных SNMP между РМ администратора и ЦУС или УБ	РМ / УБ РМ / ЦУС

Решающие правила

Синтаксис правила

Решающее правило имеет следующую структуру:

<заголовок правила> (<опции правила>)

Опции правила указываются в круглых скобках. Для разделения опций в правилах используется точка с запятой (;). Ключевые слова опций отмечают двоеточием (:), следующим за опцией.

Допускается запись одного правила в несколько строк, если все строки, за исключением последней, завершаются символом \.

Пример простого правила:

alert tcp any any -> 192.168.1.0/24 111

(content:"|00 01 86 a5|"; msg:"mountd access";)

Заголовок правила

Заголовок правила имеет вид:

<действие> <протокол> <отправитель> <порт> <направление> <получатель> <порт>

Действие

Первым в правиле задается действие, выполняемое при совпадении сигнатуры.

Действие	Описание
alert	Генерация сигнала (alert) и запись информации о пакете в файл журнала
drop	Отброс пакета (пакет не пропускается). Генерация сигнала (alert) и запись информации о пакете в файл журнала. Применяется только при работе СОВ в режиме Inline. **Внимание!** Отбрасывание пакета приводит к тайм-ауту ожидания в случае использования протокола TCP
pass	Прекращение сканирования пакета и перемещение в конец списка правил (только для текущего пакета)

Правила загружаются в порядке их появления в файлах, но обрабатываются в другом порядке. Правила имеют разный приоритет. Наиболее важные будут сканироваться первыми. По умолчанию порядок следующий: pass, drop, alert. Есть возможность изменить порядок приоритета (опции classtype и priority).

Протокол

В следующем поле заголовка указывается используемый протокол: **udp, tcp**, **ip** или **icmp**.

Отправитель и получатель

В качестве отправителя и получателя пакетов в правиле указываются IP-адрес (допустимо применение как IPv4, так и IPv6) и маска подсети либо ключевое слово **any**, которому соответствуют все IP-адреса (0.0.0.0/0). Механизм определения адресов по доменным именам не поддерживается, поэтому в правилах должны указываться IP-адреса или блоки CIDR [RFC1518]. Блок CIDR показывает префикс сети и размер маски, которая будет применяться правилом к адресам во всех пакетах для проверки соответствия указанному префиксу. Блок CIDR /24 указывает сеть класса C, /16 – класса B, а /32 указывает адрес отдельного IP-адреса.

Пример правила, которому будут соответствовать пакеты, отправленные с любого адреса в сеть класса C 192.168.1.0:

alert tcp any any -> 192.168.1.0/24 111

(content:"|00 01 86 a5|"; msg:"mountd access";)

Применительно к адресам и блокам может использоваться оператор отрицания "!". При использовании этого оператора правилу будут соответствовать пакеты, которые не попадают в указанный диапазон адресов. Ниже приведен пример правила, которому будут соответствовать пакеты, отправленные в сети класса C 192.168.1.0 из всех остальных сетей (не 192.168.1.0/24).

alert tcp !192.168.1.0/24 any -> 192.168.1.0/24 111

(content:"|00 01 86 a5|"; msg:"mountd access";)

Адреса можно задавать также в виде списка, заключенного в квадратные скобки и разделенного запятыми:

alert tcp ! [192.168.1.0/24,10.1.1.0/24] any - > [192.168.1.0/24,10.1.1.0/24] 111

(msg:"mountd access"; content:"|00 01 86 a5|";)

Также для указания адреса можно использовать переменные СОВ:

alert ip !$HOME_NET $EXTERNAL_NET-> any any (ip_proto:igmp;)

Примечание. Если в качестве $HOME_NET задана любая подсеть, а $EXTERNAL_NET — как !$HOME_NET, то в правиле переменную внешней подсети использовать нельзя, так как это приведет к ошибке.

Порт

Номера портов у отправителя и получателя можно задавать в виде конкретного значения, диапазона, списка или ключевого слова **any** (любой порт). Для задания диапазона указываются верхний и нижний пределы, разделенные двоеточием (:). Если одна из границ диапазона не задана, вместо нее используется минимальный (0) или максимальный (65535) номер порта. Граничные значения включаются в диапазон.

Пример правила, которому будут соответствовать все пакеты UDP, адресованные в порты с 0 по 1024 IP-адресов сети класса C 192.168.1.0:

drop udp any any -> 192.168.1.0/24 :1024

Для задания списка порты разделяются запятой. В этом случае, а также при использовании нескольких блоков портов необходимо использовать символы выделения ([]).

Для портов также поддерживается оператор отрицания (!).

Пример правила, которому будут соответствовать все пакеты TCP, адресованные в любые порты, за исключением портов X Window (6000 – 6010) и PostgreSQL (5432), IP-адресов сети класса C 192.168.1.0:

drop tcp any any -> 192.168.1.0/24 ![6000:6010, 5432]

Оператор направления

Оператор направления (-> или <>) показывает ориентацию или направление передачи трафика для данного правила. Адреса и порт слева от этого оператора относятся к отправителю, а справа — к получателю пакетов. Можно также создавать "двунаправленные" правила с помощью оператора <>. В этом случае каждая из пар "адрес– порт" будет трактоваться и как отправитель, и как получатель. Такие правила удобны для анализа пакетов в сеансовых соединениях (например, по протоколу POP3).

Пример двунаправленного правила:

pass tcp !192.168.1.0/24 any <> 192.168.1.0/24 23

В соответствии с этим правилом будут пропускаться все пакеты, адресованные в порт telnet каждого IP-адреса сети класса C 192.168.1.0 с любого адреса за пределами этой сети, а также все пакеты, исходящие из порта telnet IP-адресов сети 192.168.1.0/24 и адресованные в другие сети.

Использование в правилах оператора <- недопустимо.

Опции правил

Для разделения опций в правилах используется точка с запятой (;). Ключевые слова опций отличаются от аргументов двоеточием (:).

Существуют четыре основные категории опций правил.

Категория	Описание
meta-data	Информация о правиле, не оказывающая влияния на детектирование пакетов и выполняемые по отношению к ним операции
payload	Опция проверки содержимого пакетов (packet payload)
non-payload	Опция проверки служебных полей пакетов
post-detection	Опция, указывающая, что нужно сделать после выполнения заданных для правила условий

Подробные сведения об опциях правил можно получить в службе технической поддержки.

Управление записью сетевого трафика

В локальном меню УБ предусмотрена функция записи сетевого трафика.

Для начала записи сетевого трафика:

1. Подключите внешний накопитель к УБ.
2. В главном меню локального управления УБ перейдите в меню "Инструменты" | "Управление записью сетевого трафика".

   На экране появится окно "Управление записью сетевого трафика".
3. Выберите пункт "Запуск записи сетевого трафика" и нажмите клавишу <Enter>.

   На экране появится список съемных носителей.
4. Выберите съемный носитель, необходимый для записи дампа сетевого трафика, и нажмите клавишу <Enter>.

   На экране появится список сетевых интерфейсов.
5. Выберите анализирующий сетевой интерфейс ДА (monitoring или один из inline интерфейсов), на который приходит трафик для анализа и нажмите клавишу <Enter>.

   На экране появится окно "Интервал ротации файла".
6. Установите интервал ротации записи файла.

   Примечание. Под интервалом ротации записи файла понимается время записи дампа трафика, по истечении которого начинается запись следующего файла. Значение должно быть между 60 и 3600. По умолчанию — 900.

   Нажмите клавишу <Enter>.

   На экране появится сообщение об успешном запуске записи сетевого трафика.
7. Нажмите клавишу <Enter>.

Для остановки записи сетевого трафика:

1. В главном меню локального управления УБ перейдите в меню "Инструменты" | "Управление записью сетевого трафика".

   На экране появится окно "Управление записью сетевого трафика".
2. Выберите пункт "Остановка записи сетевого трафика" и нажмите клавишу <Enter>.

   На экране появится окно запроса подтверждения.
3. Выберите "Да" и нажмите клавишу <Enter>.

   На экране появится сообщение об успешной остановке записи сетевого трафика.
4. Нажмите клавишу <Enter>.

Для просмотра статуса функции записи сетевого трафика:

1. В главном меню локального управления УБ перейдите в меню "Инструменты" | "Управление записью сетевого трафика".

   На экране появится окно "Управление записью сетевого трафика".
2. Выберите пункт "Статус" и нажмите клавишу <Enter>.

   На экране появится информационное окно, содержащее информацию о статусе функции записи сетевого трафика.
3. Для возврата в предыдущее меню нажмите клавишу <Enter>.

Настройка тайм-аута неактивности

В локальном меню УБ можно настроить тайм-аут неактивности, по истечении которого происходит завершение сеанса текущего пользователя.

Для установки тайм-аута неактивности:

1. В главном меню локального управления УБ перейдите в меню "Настройки" | "Настройка тайм-аута неактивности".

   На экране появится окно "Тайм-аут неактивности".

2. Задайте необходимое значение тайм-аута неактивности в секундах.

   Примечание. Значение должно быть между 10 и 3600. По умолчанию — 300.

   Нажмите клавишу <**Enter**>.

   Для тайм- аута неактивности будет установлено указанное значение и произойдет возврат в предыдущее меню.

Документация

1. Программный комплекс "Континент-СОА". Версия 4. Руководство администратора. Ввод в эксплуатацию.
2. Программный комплекс "Континент-СОА". Версия 4. Руководство администратора. Мониторинг и аудит.