КОД БЕЗОПАСНОСТИ

Программный комплекс

Континент-СОВ
Версия 4

Руководство администратора

Система обнаружения вторжений

RU.АМБС.58.29.12.002 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

DNS	Domain Name System
FTP	File Transfer Protocol
GMT	Greenwich Mean Time
GRUB	GRand Unified Bootloader
IETF	Internet Engineering Task Force
HTTPS	HyperText Transfer Protocol Secure
IP	Internet Protocol
MTU	Maximum Transmission Unit
NTP	Network Time Protocol
RPC	Remote Procedure Call
SNMP	Simple Network Management Protocol
SPAN	Switched Port Analyzer
SWAP	Swapping
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USB	Universal Serial Bus
UTC	Coordinated Universal Time
VPN	Virtual Private Network
БД	База данных
БРП	База решающих правил
ДА	Детектор (компьютерных) атак
ДСЧ	Датчик случайных чисел
ОЗУ	Оперативное запоминающее устройство
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
РМ	Рабочее место
СОВ	Система обнаружения вторжений (компьютерных атак)
СУ	Сетевое устройство
УБ	Узел безопасности
УК	Узел коммутации
УМ	Узел маршрутизации
ЦП	Центральный процессор
ЦУС	Центр управления сетью

Введение

Документ предназначен для администраторов изделия "Программный комплекс "Континент-СОВ". Версия 4" RU.АМБС.58.29.12.002 (далее — комплекс). В нем содержатся сведения, необходимые администраторам для управления системой обнаружения вторжений.

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

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

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

Общие сведения

Назначение и основные функции СОВ

Система обнаружения вторжений (компьютерных атак) входит в состав комплекса "Континент" и предназначена для обнаружения и противодействия основным угрозам безопасности информации (носителей информации), возникающим при преднамеренном несанкционированном доступе или специальном воздействии со стороны:

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

Основным компонентом СОВ является детектор компьютерных атак (детектор атак, ДА), который реализует следующие основные 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.

В СОВ реализованы следующие основные функции:

- централизованное управление;
- контроль работы ДА в режиме реального времени;
- регистрация событий управления и работы СОВ;
- возможность обновления БРП по расписанию;
- создание правил СОВ для контроля трафика с последующим применением их на ДА;
- подготовка и отправка отчетов о работе ДА;
- оповещение администратора о наступлении событий.

Функции ЦУС

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

По команде администратора УБ все локальные изменения настроек отправляются на ЦУС, где они встают в очередь на запись в базу данных (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:

- Создание иерархических систем, включающих несколько доменов безопасности, управляемых из единого центра.

- 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 домена Континент с единым центром управления.

Описание работы детектора атак

Детектор атак — это программно-аппаратный компонент комплекса, осуществляющий 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.

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 его локальных журналах 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.

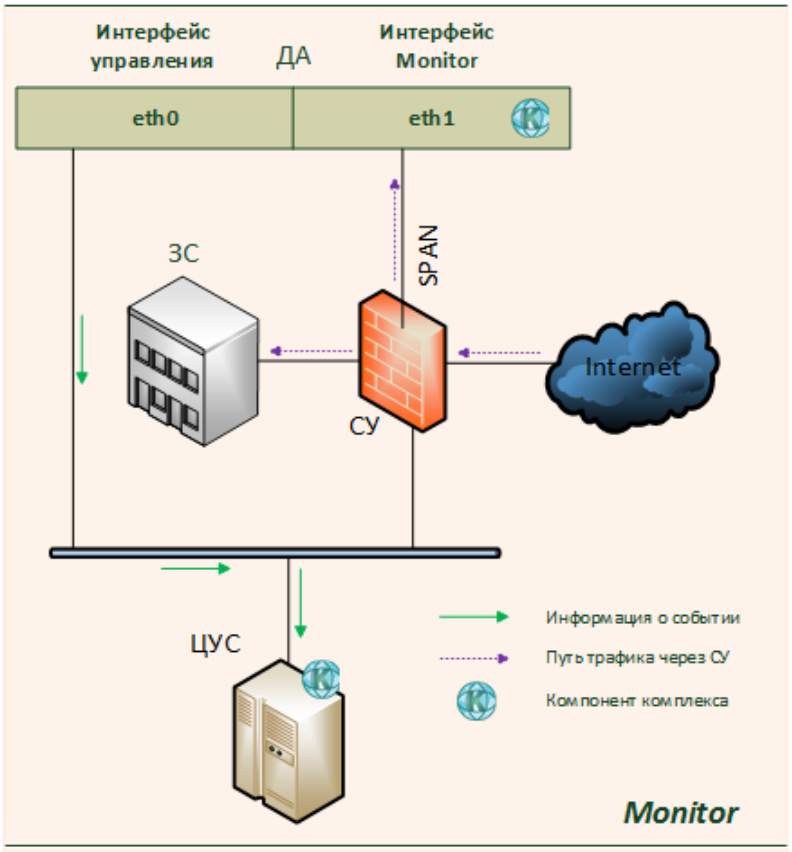
Возможны следующие режимы работы ДА:

- Monitor

  В этом режиме трафик зеркалируется на ДА со SPAN-порта стороннего устройства (СУ), в роли которого обычно выступает коммутатор или маршрутизатор.

  Захват трафика осуществляется с одного или нескольких физических интерфейсов.

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

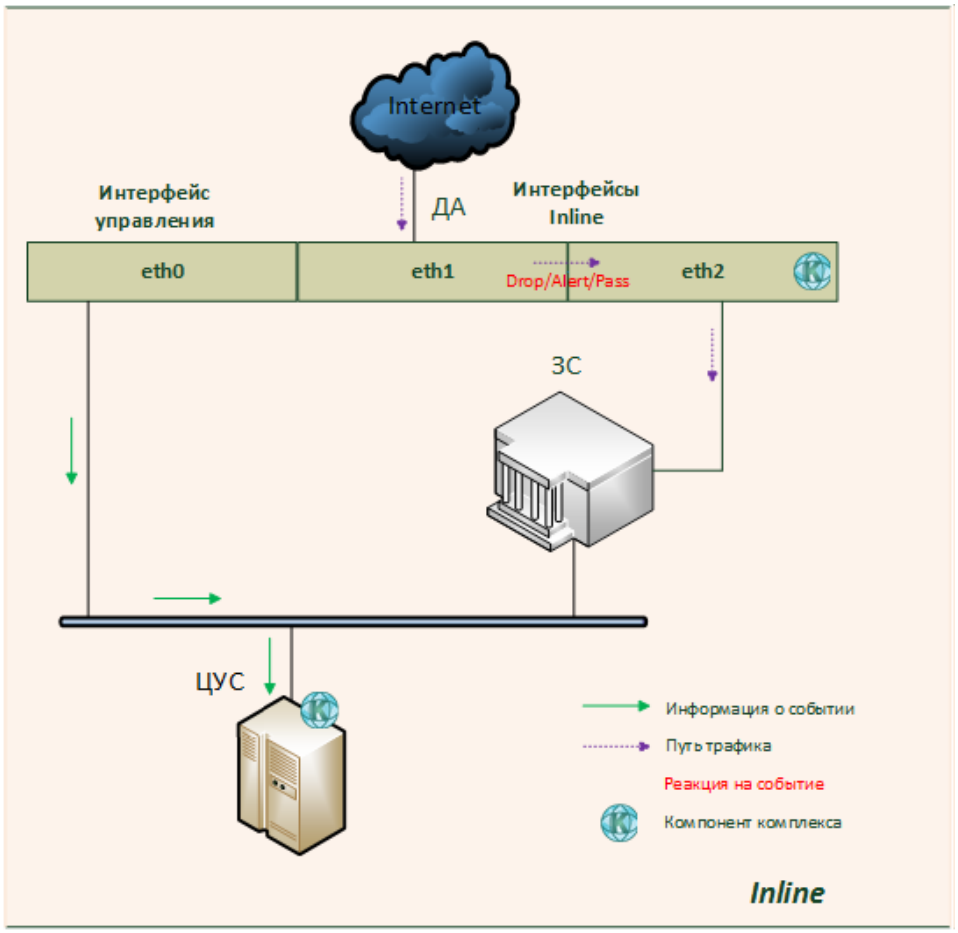


- Inline

  В этом режиме ДА устанавливается "в разрыв" сетевого соединения между сервером Internet 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 на ЦУС.

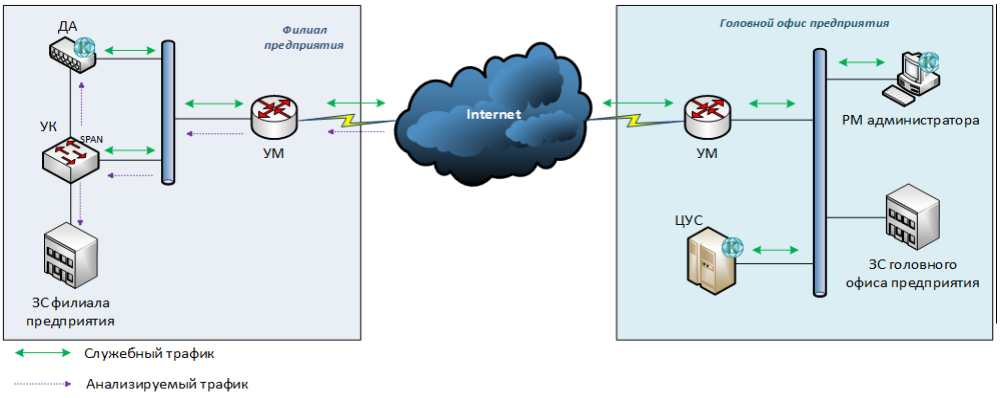


Примеры типовых схем использования

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. 142).

Мониторинг трафика

Ниже представлена схема использования детектора атак для мониторинга трафика.

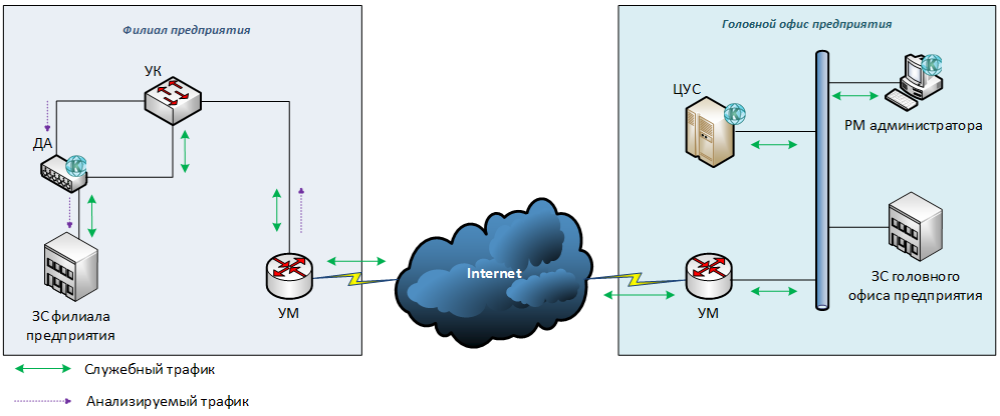


Для развертывания данной схемы требуется инициализация и настройка следующих компонентов:

- 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 с целью обнаружения и предотвращения вторжений осуществляется с использованием сигнатурного метода, основанного на применении набора решающих правил.

База решающих правил (БРП) предварительно загружается на ЦУС, а затем определенный набор этих правил привязывается к профилю СОВ. Для применения этого набора правил на ДА администратор формирует правило СОВ, содержащее нужный профиль СОВ, и назначает его на этот ДА. Каждое правило СОВ определяет действие, которое должно быть выполнено при срабатывании сигнатуры атаки.

При организации иерархической доменной структуры политику и профиль СОВ можно передать на домен нижнего уровня. При этом в домене нижнего уровня названия таких политик и профилей отображаются как global_policy и global_profile, их нельзя редактировать и удалять.

Предоставляемый вендорский набор БРП предварительно разбит по группам. Для администратора предусмотрена возможность клонирования с дальнейшим редактированием вендорского правила или создание нового правила.

Редактирование вендорского правила не предусмотрено.

Каждое правило в наборе содержит сигнатуру атаки, используемую для обнаружения или предотвращения вторжения, тип действия для обнаруженной угрозы (alert — "оповещать", drop — "блокировать", pass — "пропустить"), описание источника и приемника атаки и ссылки на описание угрозы. Администратор СОВ имеет возможность изменить 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 возможно использовать любой тип противодействия. Также администратор может убрать из профиля любое из ранее определенных правил, в этом случае это правило не будет срабатывать.

Примерный синтаксис написания правила приведен в Приложении (см. стр. **142**).

Администрирование СОВ

Управление СОВ 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 домен узлами безопасности.

Примечание. Все учетные записи изначально не обладают правом дистанционного доступа к локальному меню по протоколу SSH (см. стр. **142**).

Предусмотрены четыре встроенные роли:

- главный администратор (ГА);
- администратор безопасности (АБ);
- администратор сети (АС);
- администратор аудита (АУ).

Внимание! При создании или изменении 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. **51**) после их включения.

Управление ролями администраторов

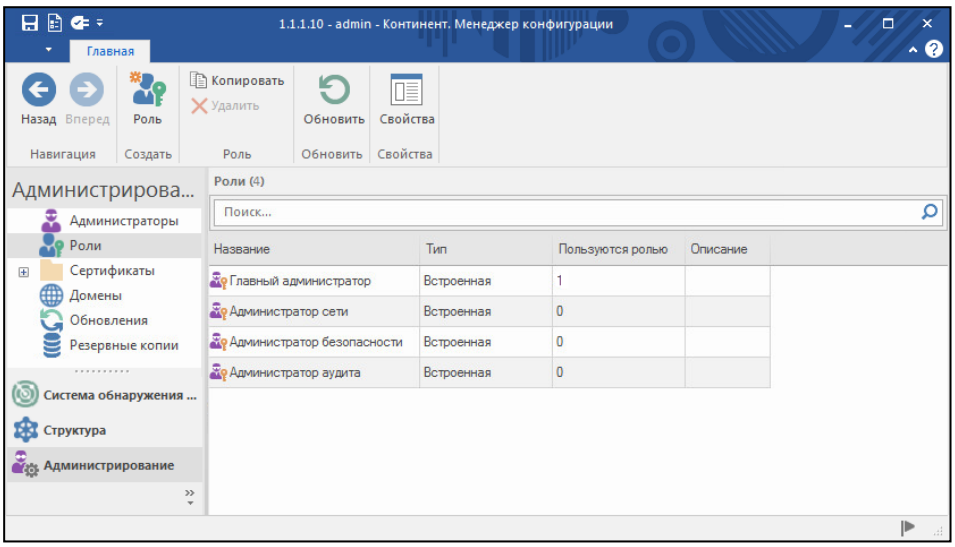
Просмотр роли

Примечание. Интерфейс Менеджера конфигурации рассмотрен в Приложении (см. стр. 125).

Для просмотра роли:

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

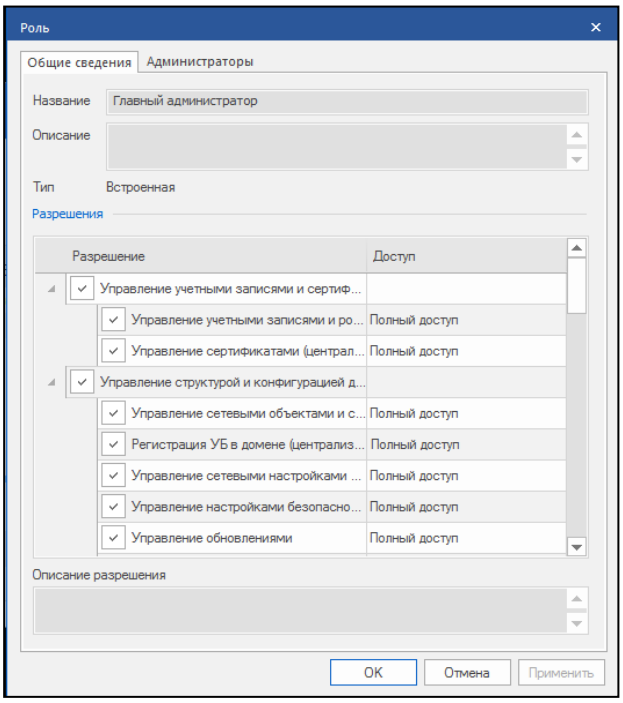
   В правой части окна отобразится список ролей администраторов.



   Для каждой роли указаны тип и количество администраторов, которым назначена данная роль.

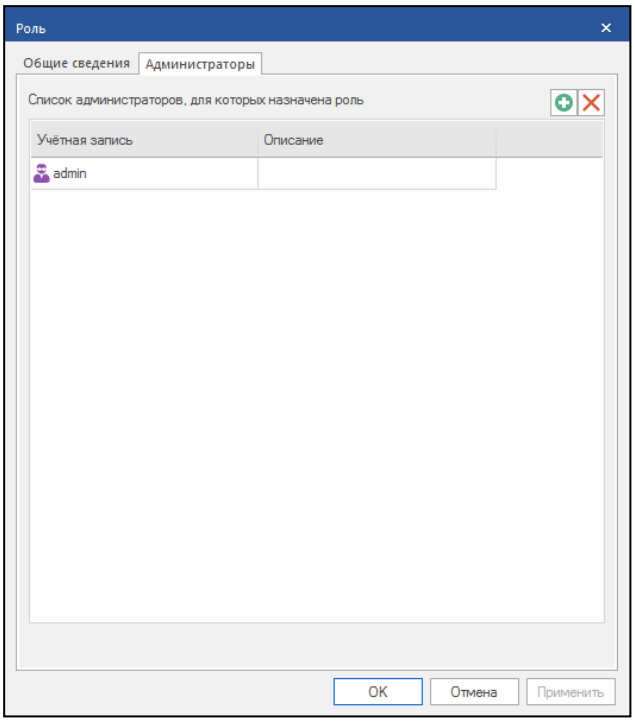
2. Для просмотра привилегий какой-либо из ролей выберите ее в списке и нажмите на панели инструментов кнопку "Свойства".

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



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

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 "ОК" или "Отмена".

Окно "Роль" закроется.

Управление учетными записями

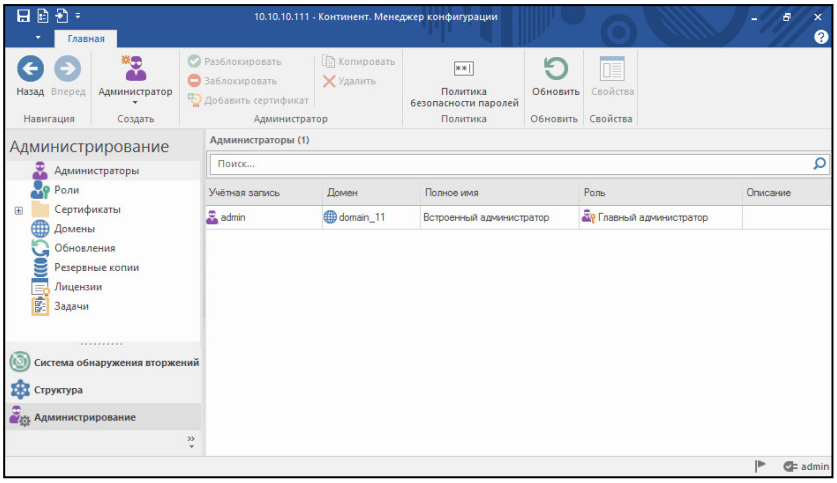
Просмотр учетных записей администраторов

Для просмотра параметров учетной записи:

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

В правой части окна отобразится список администраторов.

Ниже на рисунке в списке отображается только учетная запись администратора admin, созданная при инициализации ЦУС с автоматически присвоенной встроенной ролью главного администратора.



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 (при этом указывается срок действия текущего пароля, действующий у всех записей, кроме встроенного администратора); • 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.

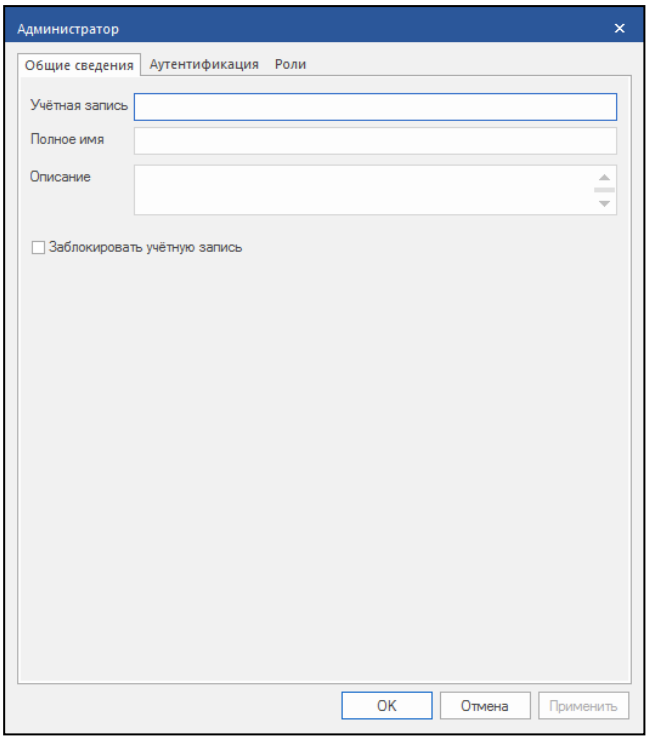
Создание учетной записи администратора

Для создания новой учетной записи администратора:

> **Внимание!** Если для администратора предусматривается тип аутентификации по сертификату, необходимо предварительно выпустить сертификат пользователя (см. стр. 132),а затем установить его в личное хранилище сертификатов пользователя (см. стр. 134).

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".

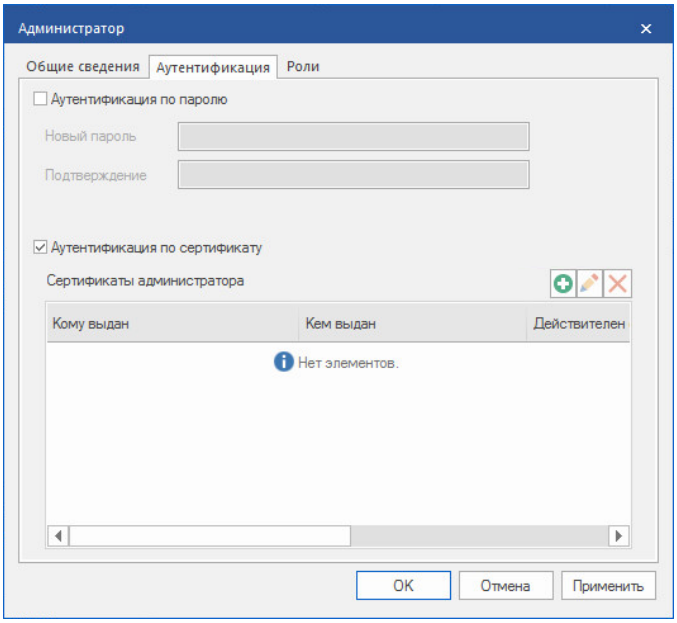


2. Введите имя учетной записи администратора, полное имя и краткое описание и нажмите кнопку "Применить".

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:

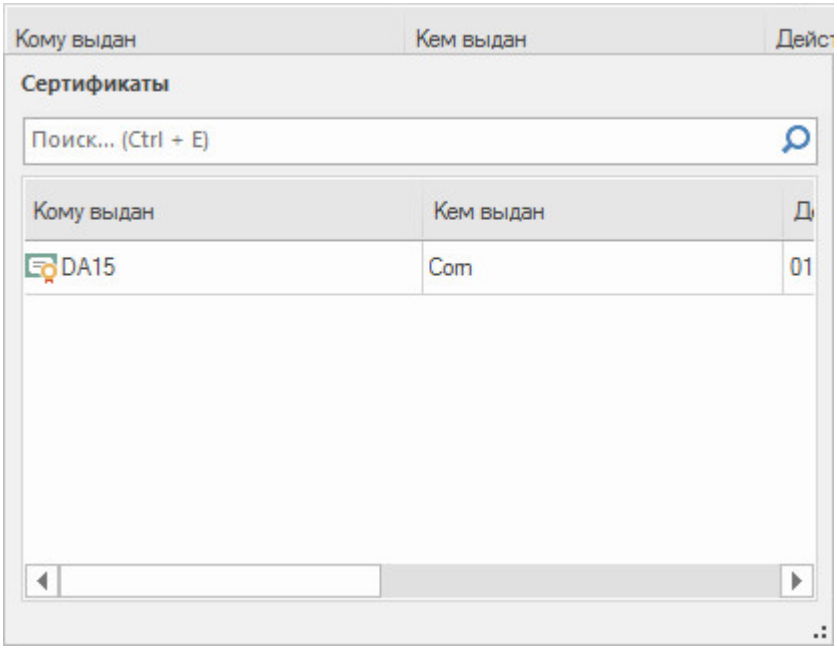
!	@	#	$	%	^	&	*	(	)	_	-	+	;	:	.	,

- не содержать символы кириллицы;
- 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**.

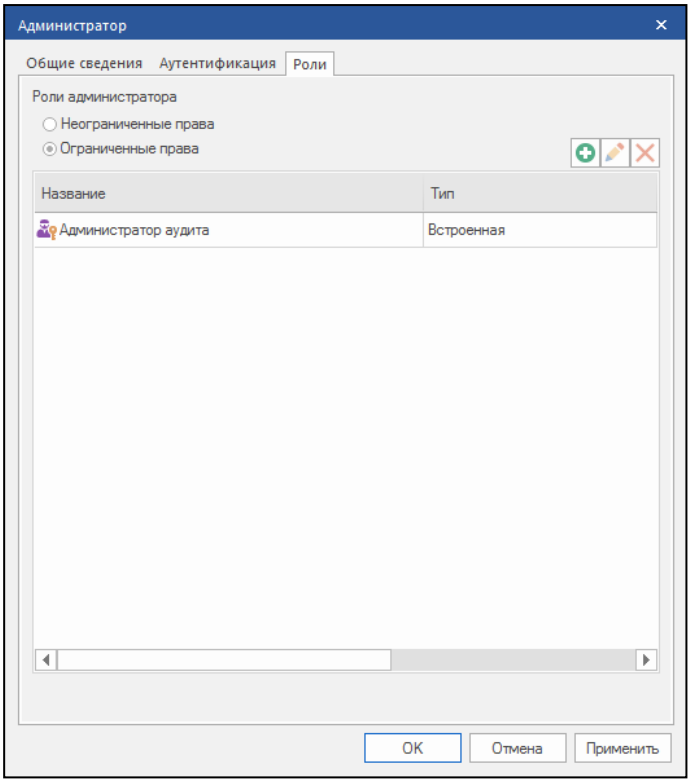
5. Установите флажок "Аутентификация по сертификату" и нажмите кнопку  .

На экране появится окно выбора сертификата.



6. Выберите нужный 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 "OK", 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.

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. **22**).

Для запуска процедуры аутентификации при локальном управлении:

1. Включите питание сетевого устройства.

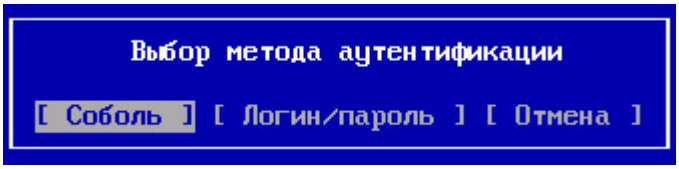
   На экране появится меню администратора, подобное изображенному ниже (для ПАК "Соболь" вер. 3.0).

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>.

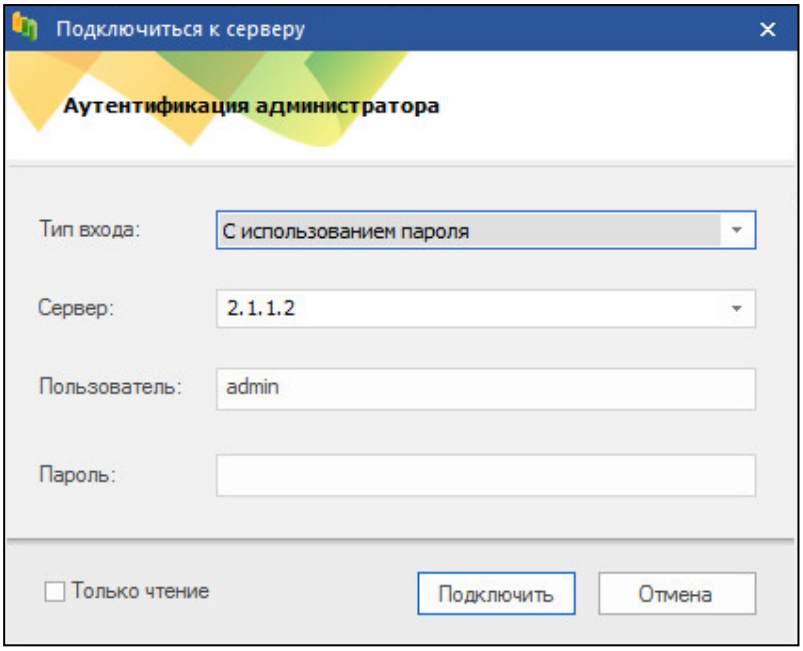
   На экране появится окно "Выбор метода аутентификации ".



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 главного локального 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

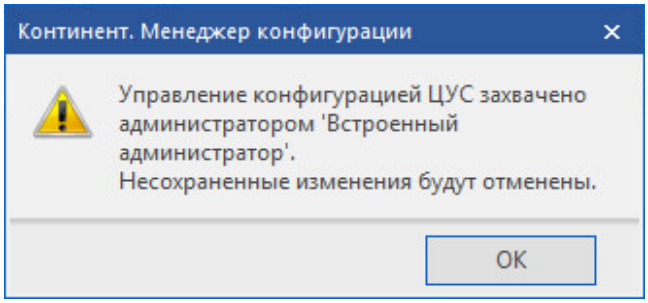
После успешной аутентификации возможна ситуация конфликта управления БД ЦУС локальным администратором и удаленными администраторами через Менеджер конфигурации. В этом случае администратор — инициатор конфликта получит возможность выбора режима работы.

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 и отправлять локальные изменения на ЦУС и 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:

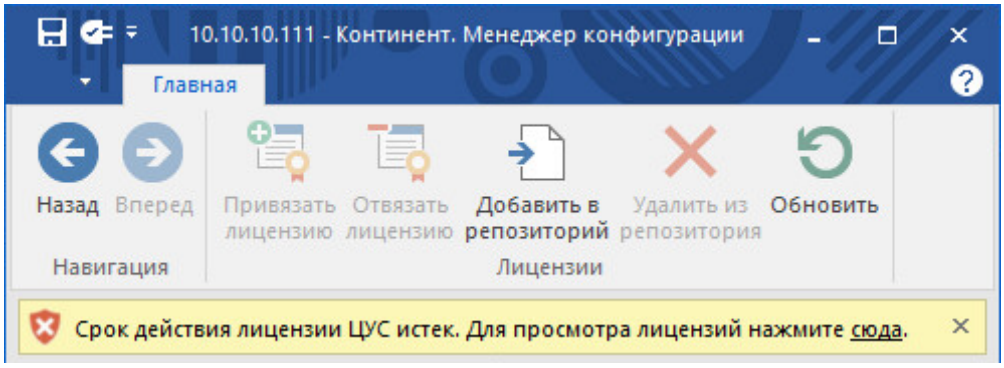
- режим чтения (любое изменение конфигурации запрещено);
- редактирование (идентичен режиму принудительного захвата блокировки, дополнительно отображается информация, какой именно администратор сейчас редактирует конфигурацию ЦУС);
- восстановление (в случае перехвата управления тем же самым администратором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

Управление лицензиями

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 ID клиента, которая позволяет оценить все 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 будет показано соответствующее сообщение:



Примечание. После истечения срока действия лицензии она выделяется красным цветом.

Лицензия опционально привязывается к ID УБ. Лицензия с указанным ID узла может автоматически привязываться к УБ при ее первой загрузке в репозиторий. Отвязанная от УБ лицензия остается в репозитории, для нее возможна только ручная привязка с участием администратора (см. ниже).

При первой привязке лицензии в БД ЦУС прописывается код клиента, содержащийся в лицензии. Далее при добавлении лицензий в репозиторий будут загружаться только лицензии с соответствующим кодом клиента.

Просмотр лицензий

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

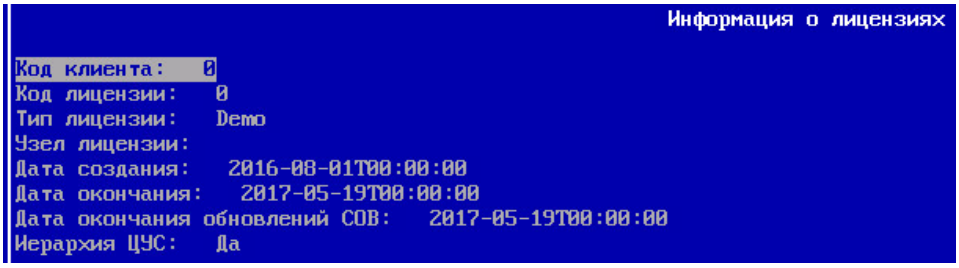
Для просмотра сведений о лицензиях средствами локального управления:

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.



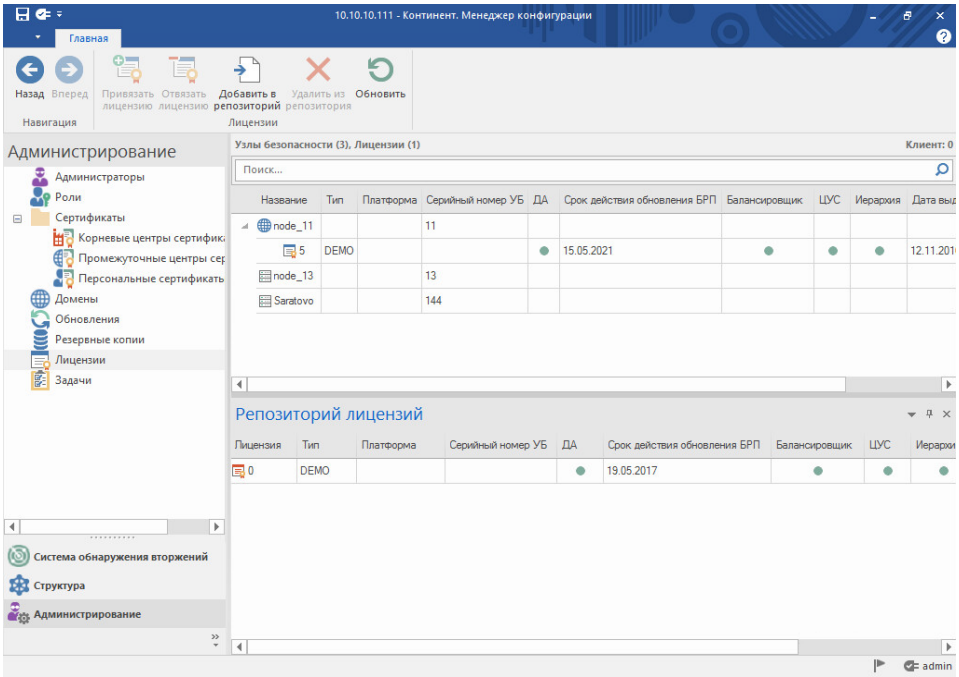
Примечание. До момента привязки лицензии поля кода клиента и кода лицензии содержат нулевые значения.

3. Для выхода необходимо нажать клавишу <Esc>.

Для просмотра сведений о лицензиях в Менеджере конфигурации:

- Откройте Менеджер конфигурации, перейдите на вкладку "Администрирование" и войдите в раздел "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 верхнем правом углу отображается код 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 Менеджере конфигурации.

Для управления лицензиями:

1. В Менеджере конфигурации перейдите на вкладку "Администрирование" и войдите в раздел "Лицензии".
2. Для добавления лицензий нажмите на панели инструментов кнопку "Добавить в репозиторий", в появившемся стандартном диалоге открытия файла укажите лицензионный файл и нажмите кнопку "Открыть".

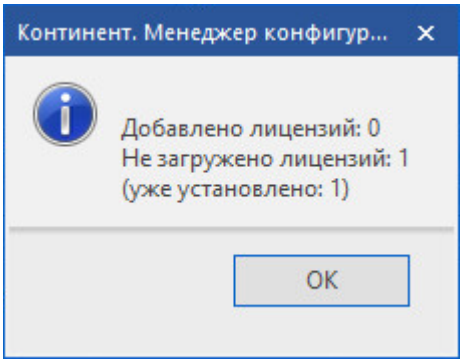
   Лицензии будут загружены из файла, если при этом соблюдены следующие условия:

   - ID клиента в лицензии совпадает с ID клиента на ЦУС или в базе ЦУС присутствуют только лицензии с нулевым значением ID 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.

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

   Примечание. Загруженные лицензии автоматически привязываются к узлам комплекса при соответствии серийного номера УБ в лицензии.

3. Для привязки лицензии к определенному узлу выберите этот узел в таблице на экране, нажмите кнопку "Привязать лицензию" на панели инструментов и в появившемся окне с доступными для назначения и подходящими по типу и сроку действия лицензиями выберите нужную лицензию.

   Лицензия станет 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.
4. Для отзыва лицензии выберите ее в таблице на экране, нажмите кнопку "Отвязать лицензию" на панели инструментов и подтвердите отзыв в появившемся окне подтверждения, нажав кнопку "Да".

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

5. Для удаления лицензии выберите ее в репозитории, нажмите кнопку "Удалить лицензию" на панели инструментов и подтвердите удаление в появившемся окне подтверждения, нажав кнопку "Да".

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

Примечание. Удаленную лицензию можно повторно загрузить из файла в базу ЦУС.

Управление компонентами комплекса

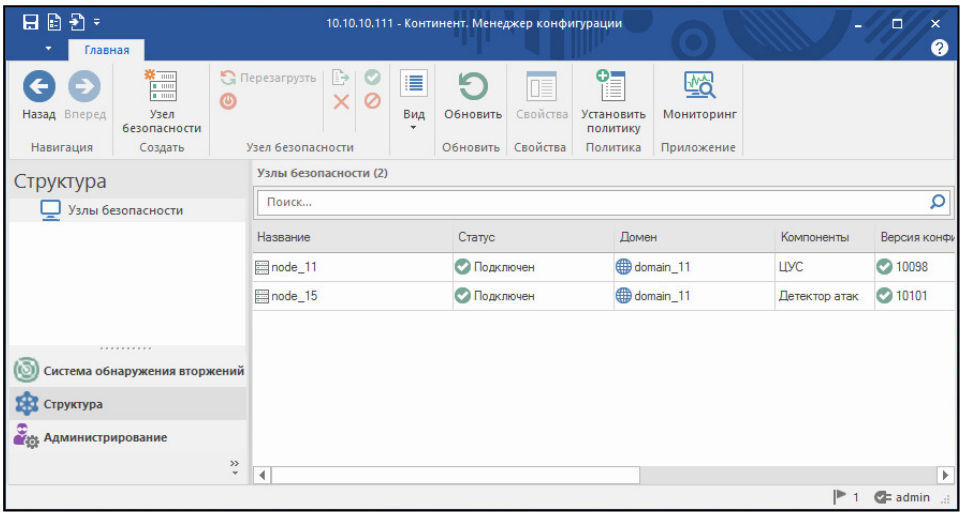
Развертывание компонента комплекса

Инициализация, подключение и регистрация компонента комплекса выполняются средствами локального и удаленного управления (см. [2], разделы "Развертывание Центра управления сетью и регистрация главного администратора" и "Развертывание узла безопасности").

Просмотр свойств

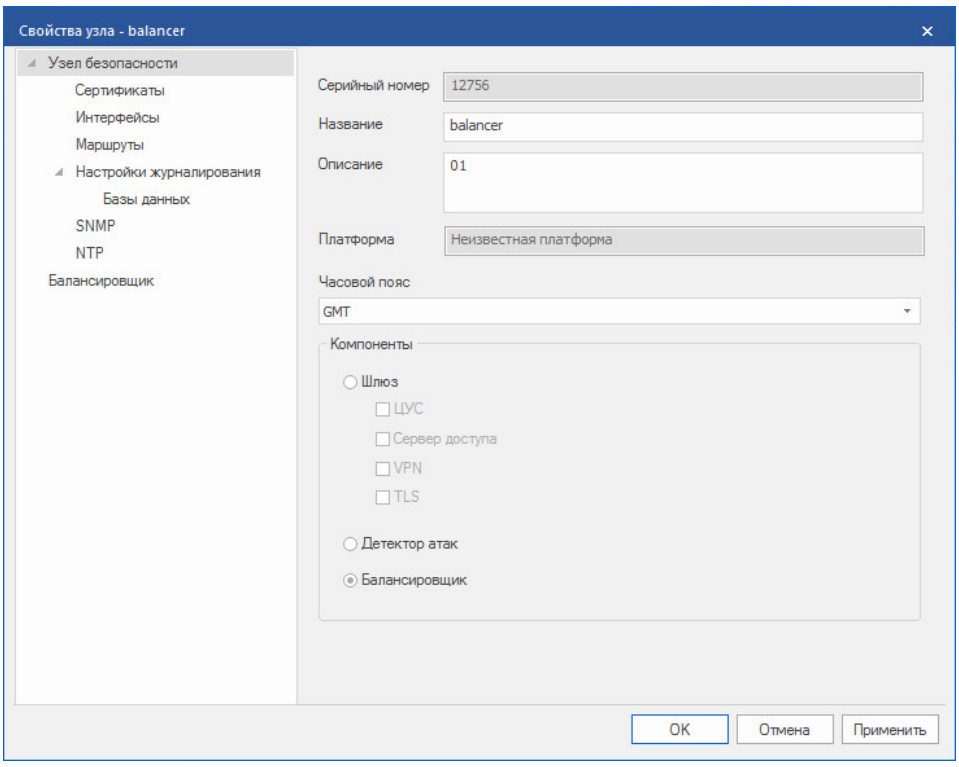
Для просмотра сведений об устройстве в Менеджере конфигурации:

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



2. В списке узлов безопасности выберите нужный компонент и нажмите кнопку "Свойства" на панели инструментов.

   На экране появится окно "Свойства узла".



В левой части окна расположено иерархическое меню параметров узла. Сведения по каждому пункту этого меню отображаются в правой части окна.

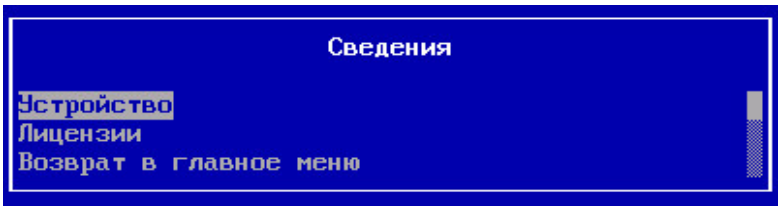
3. После просмотра нажмите кнопку "ОК" для возврата в раздел "Структура".

Для просмотра сведений об устройстве средствами локального управления:

Примечание. Интерфейс локального управления рассмотрен в Приложении (см. стр. 125).

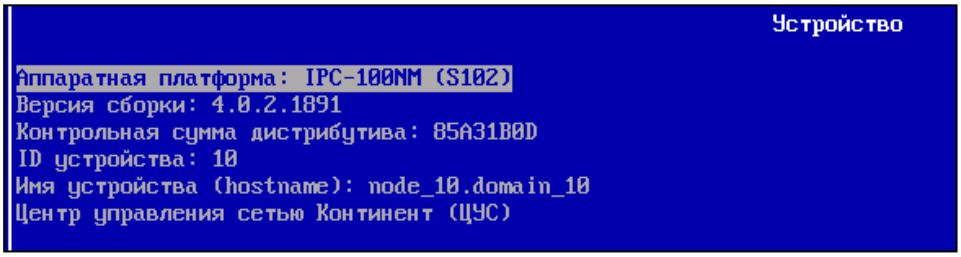
1. В главном меню выберите пункт "Сведения" и нажмите клавишу <Enter>.

   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 окно "Меню инструменты".

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

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

Пункт меню	Назначение
Статистика	Просмотр статистической информации по HTTPS-серверу
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
Возврат в предыдущее меню	Переход в окно "Меню инструменты"

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

Проверка целостности ПО и проверка конфигурации

Для проведения процедуры проверки:

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

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

   На экране появится окно "Диагностика".
3. Выберите пункт "Командная строка" и нажмите клавишу <Enter>.

   На экране появится консольное приложение командной строки.
4. Введите команду **k4_self_check** и нажмите клавишу <Enter>.

   Будет запущен тест целостности ПО и конфигурации.

По окончании процедуры будет выведено сообщение о результатах проверки.

Сетевые настройки

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

Настройка IP-адреса

Для настройки IP-адреса в Менеджере конфигурации:

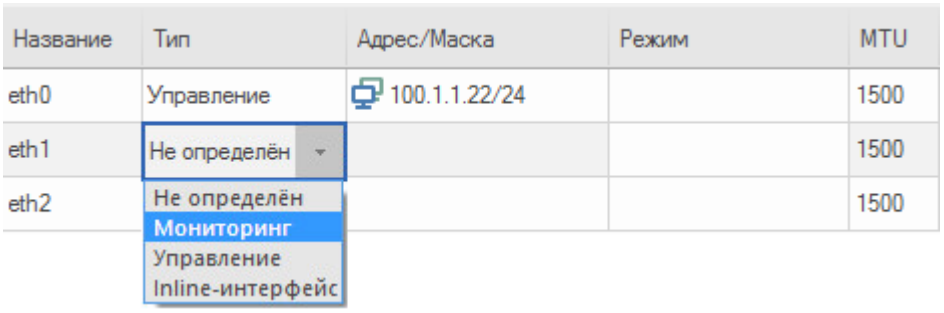
1. В разделе "Структура" Менеджера конфигурации выберите нужный компонент комплекса и вызовите окно настройки свойств.
2. Выберите в левой части окна в разделе "Узел сети" пункт "Интерфейсы".

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

   Примечание. Типы Мониторинг и Inline актуальны для соответствующих схем включения ДА, интерфейс управления предназначен для передачи служебного трафика между элементами комплекса, во всех остальных случаях тип выбирать не нужно.

   - 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. **46**).

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 на вышестоящий ЦУС и подтвердите их локально или через Менеджер конфигурации (см. стр. **48**).

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

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

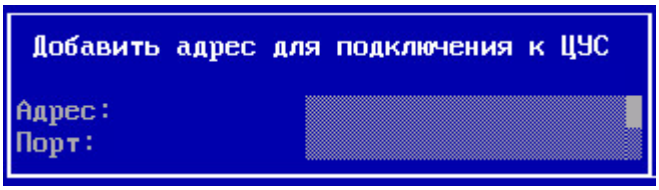
   На экране появится окно "Меню настроек".

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 на ЦУС локально или через Менеджер конфигурации (см. стр. **48**).

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 на 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>.

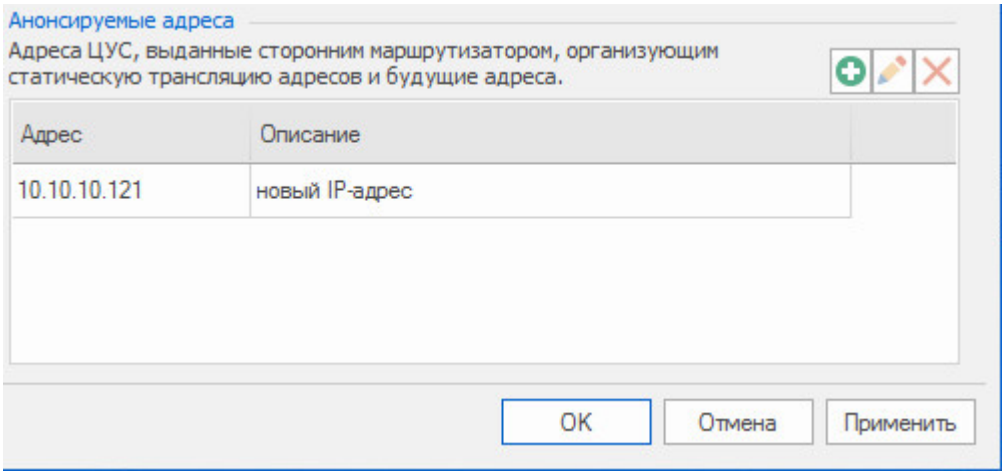
11. Подтвердите изменения конфигурации на вышестоящем ЦУС (см. стр. **50**).

Для смены IP-адреса интерфейса управления ЦУС:

1. В разделе "Структура" Менеджера конфигурации выберите нужный ЦУС и вызовите окно настройки свойств.

2. Выберите в левой части окна в разделе "Узел сети" 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 сети" пункт "Маршруты" и сделайте необходимые изменения.
8. Нажмите кнопку "ОК" и установите политику на ЦУС.

Для изменения IP- адреса вышестоящего ЦУС (только для подчиненного ЦУС):

Примечание. Изменение IP-адреса подчиненного ЦУС не влияет на работу вышестоящего ЦУС и комплекса в целом, поэтому дополнительных настроек в этом случае проводить не нужно.

1. На вышестоящем ЦУС осуществляем необходимое изменение сетевых настроек (см. выше).
2. В главном меню локального управления подчиненного ЦУС выберите пункт "Настройки" и нажмите клавишу <Enter>.

   На экране появится окно "Меню настроек".
3. Выберите пункт "Управление многоуровневой структурой" и нажмите клавишу <Enter>.

   На экране появится окно "Многоуровневая структура".
4. Выберите пункт "Изменение адреса вышестоящего ЦУС" и нажмите клавишу <Enter>.

   На экране появится окно "Изменение адреса вышестоящего ЦУС" с указанным IP-адресом по информации локальной БД.
5. Введите новый IP-адрес вышестоящего ЦУС и нажмите клавишу <Enter>.

   Будет выполнено соответствующее обновление БД. Дождитесь сообщения об успешном завершении операции.

Внимание! Для подключения подчиненного ЦУС к вышестоящему по измененному IP-адресу необходимо перезагрузить подчиненный ЦУС.

6. В главном меню подчиненного ЦУС перейдите к пункту "Завершение работы устройства" и нажмите клавишу <Enter>.

   На экране появится окно "Выключить Континент?".
7. Выберите пункт "Перезагрузка" и нажмите клавишу <Enter>.

   Будет выполнена перезагрузка ЦУС для завершения настройки.

Настройка DNS

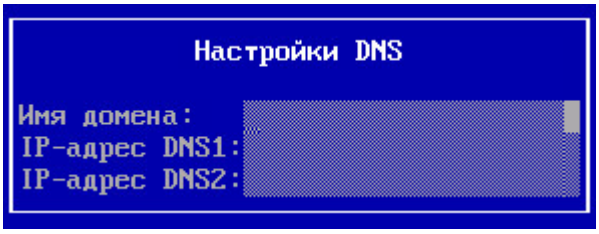
Настройка DNS осуществляется только средствами локального управления.

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>.

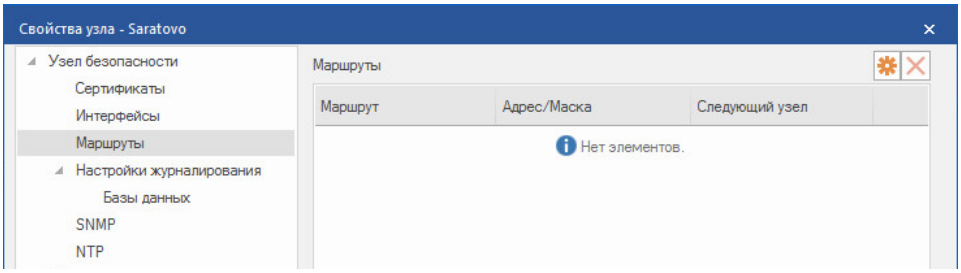
Примечание. При изменении локальной конфигурации достаточно одного применения локальной политики после выполнения всех настроек.

5. Подтвердите изменения конфигурации на вышестоящем ЦУС (см. стр. **50**).

Настройка статической маршрутизации

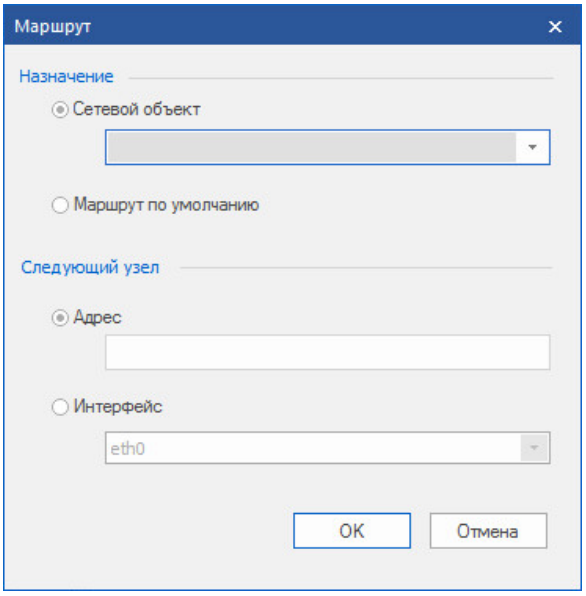
Для настройки таблицы маршрутизации в Менеджере конфигурации:

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



3. Для добавления нового маршрута нажмите кнопку  .

   На экране появится окно "Маршрут".



4. Укажите объект назначения и шлюз, 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. **46**).

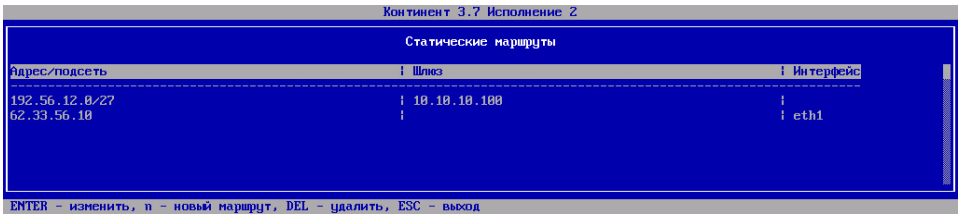
Для настройки статических маршрутов при локальном управлении:

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>.

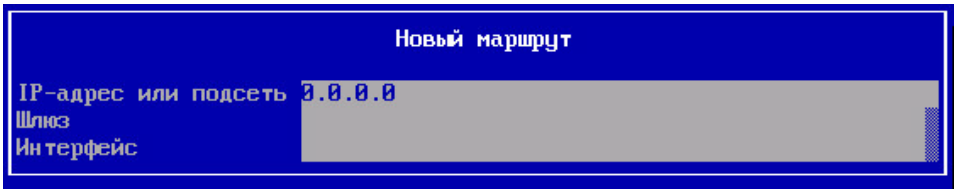
   На экране появится окно "Статические маршруты".



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 на вышестоящем ЦУС (см. стр. **50**).

Настройка дистанционного доступа по протоколу SSH

Для настройки дистанционного доступа к локальному меню УБ или ЦУС:

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

1. В Менеджере конфигурации создайте новую роль (см. стр. **1**) и в ней установите отметку напротив привилегии "Дистанционный доступ к локальному меню" группы "Локальное управление".
2. Сохраните изменения в активной конфигурации ЦУС (см. стр. **51**).
3. Для добавления созданной роли выберите нужного администратора или создайте нового (см. стр. **16**).

   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 "ОК".

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:

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 сетевого устройства с момента включения;
- количество полученных/переданных пакетов;
- состояние интерфейсов (Up/Down) и пр.

Подробное описание параметров, контролируемых по протоколу SNMP, см. на стр. **158**.

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

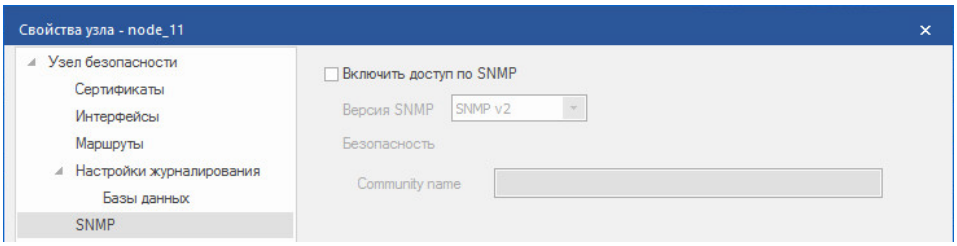
Примечание. При использовании протокола SNMP v3 для настройки SNMP-клиента необходимо в качестве алгоритма аутентификации (Auth Algorithm) использовать MD5, в качестве алгоритма шифрования (Privacy Algorithm) — DES.

Для настройки сервиса SNMP:

5. Откройте Менеджер конфигурации и перейдите в раздел "Структура".
6. В списке узлов выберите нужный компонент комплекса и нажмите кнопку "Свойства".

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

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



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

Настройка системного времени

Настройку системного времени проводят средствами локального управления, выбор зоны журналирования и подключение к NTP-серверу можно осуществлять

как при локальном управлении, так и при удаленном управлении.

По умолчанию синхронизация по протоколу NTP между компонентами комплекса включена (узлы автоматически синхронизируют время с ЦУС своего домена).

Для настройки системного времени и зоны журналирования при локальном управлении:

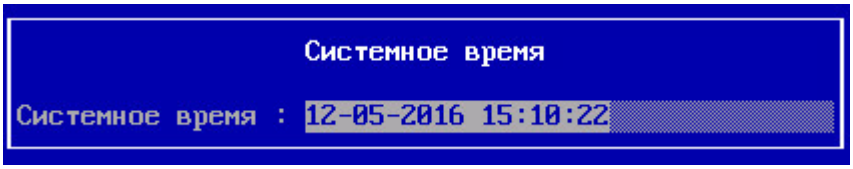
1. В главном меню компонента комплекса выберите пункт "Настройки" и нажмите клавишу <Enter>.

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

   На экране появится окно "Настройка времени".
3. Выберите пункт "Изменить временную зону для дат событий журнала" и нажмите клавишу <Enter>.

   На экране появится окно "Выбор временной зоны".
4. Выберите нужную временную зону.
5. Выберите пункт "Ручная установка времени" и нажмите клавишу <Enter>.

   На экране появится окно "Системное время".



6. Введите текущее время по предлагаемому шаблону по стандарту UTC +0 и нажмите клавишу <Enter>.

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

   Будет выполнено изменение времени на узле с соответствующим оповещением на экране.
7. Выберите пункт "Сохранить конфигурацию" и нажмите клавишу <Enter>.

   Все изменения в настройках системного времени будут переданы в автозагружаемую конфигурацию узла с соответствующим оповещением на экране.
8. Для применения новой конфигурации вернитесь в меню настроек, выберите пункт "Применить локальную политику" и нажмите клавишу <Enter>.

   Дождитесь завершения операции.
9. Подтвердите изменения в конфигурации узла на ЦУС текущего домена (см. стр. **48**).

Для выбора зоны журналирования в Менеджере конфигурации:

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

   На экране появится окно "Свойства узла".
3. В правой части окна в области "Часовой пояс" выберите нужную временную зону для журналирования 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".

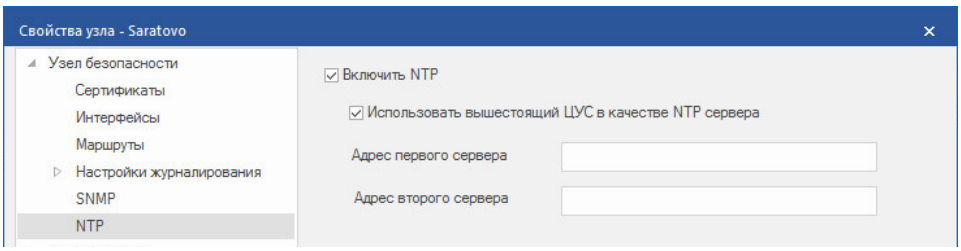
Для настройки синхронизации узла безопасности и NTP-сервера в Менеджере конфигурации:

1. Откройте Менеджер конфигурации 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 "NTP".

   В правой части окна появятся текущие настройки синхронизации узлов по протоколу NTP.



4. Включите синхронизацию по NTP и пропишите IP-адреса основного и резервного NTP-серверов (необязательно).

   Примечание. При необходимости отключения использования вышестоящего ЦУС в качестве первоначального NTP-сервера снимите соответствующий флажок.

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

Для настройки системного времени по протоколу NTP при локальном управлении:

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

   На экране появится окно "Меню настроек".

2. Выберите пункт "Системное время" и нажмите клавишу <Enter>.

   На экране появится окно "Настройка времени".

3. При отключенной синхронизации по протоколу NTP выберите пункт "Включить NTP" и нажмите клавишу <Enter>.

4. Выберите пункт "Настройка NTP" и нажмите клавишу <Enter>.

   На экране появится окно "Настройки NTP".

5. В случае отключения использования ЦУС в качестве сервера NTP выберите соответствующий пункт и нажмите клавишу <Enter>.

6. Для использования иных серверов для синхронизации по протоколу NTP, а также для указания резервных NTP-серверов выберите пункт "Установить адрес NTP-сервера" и нажмите клавишу <Enter>.

   На экране появится окно "Настройки NTP серверов".

7. Введите IP-адреса NTP-серверов, используя курсоры для перемещения между строками, нажмите клавишу <Enter> и выполните возврат в предыдущее меню.

8. Выберите пункт "Сохранить конфигурацию" и нажмите клавишу <Enter>.

   Все изменения в настройках системного времени будут переданы в автозагружаемую конфигурацию УБ с соответствующим оповещением на экране.

9. Для применения новой конфигурации вернитесь в меню настроек, выберите пункт "Применить локальную политику" и нажмите клавишу <Enter>.

   Дождитесь завершения операции.

10. Подтвердите изменения в конфигурации узла на ЦУС текущего домена (см. стр. **48**).

Параметры журналирования

Системой предусмотрены следующие настройки журналирования:

- уровень детализации системного журнала:
- отправка журналов в формате IETF (RFC 5424) на внешний syslog-сервер;

- параметры автоматической очистки журналов;
- хранение журналов во внешней базе данных.

Настройку этих параметров выполняют как в Менеджере конфигурации (см. ниже), так и средствами локального управления.

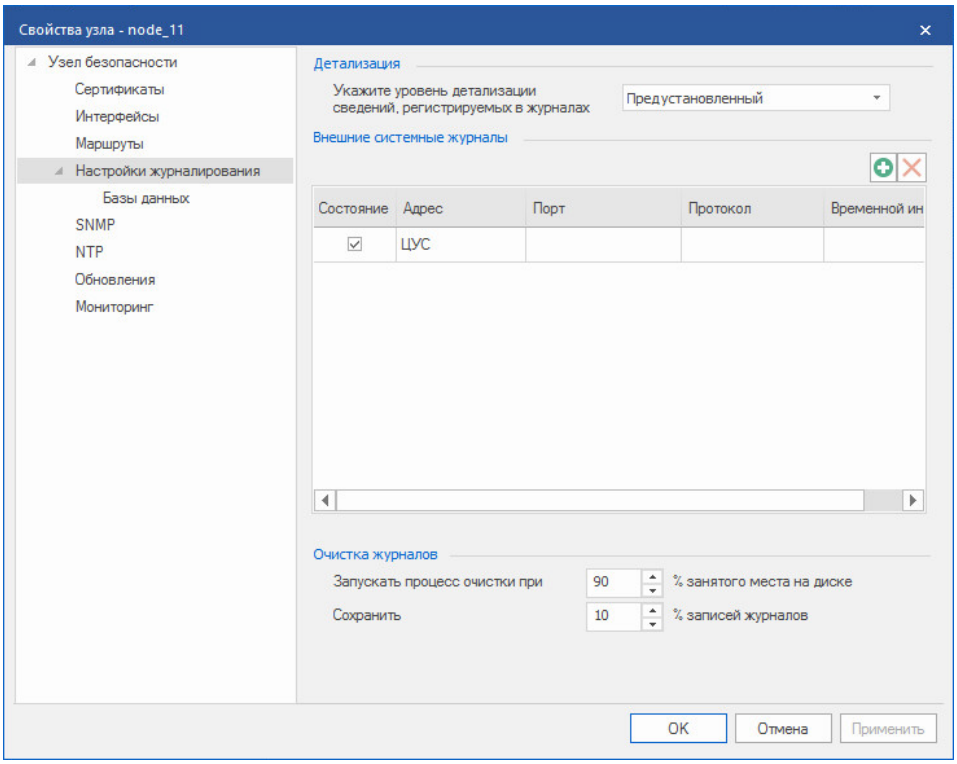
Дополнительно средствами локального управления предусмотрены следующие настройки:

- автоматическая очистка журналов по сроку давности записей (см. стр. **45**);
- хранение журналов компонента комплекса (см. стр. **39**).

Для настройки параметров журналирования в Менеджере конфигурации:

1. Откройте Менеджер конфигурации 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 "Настройки журналирования".

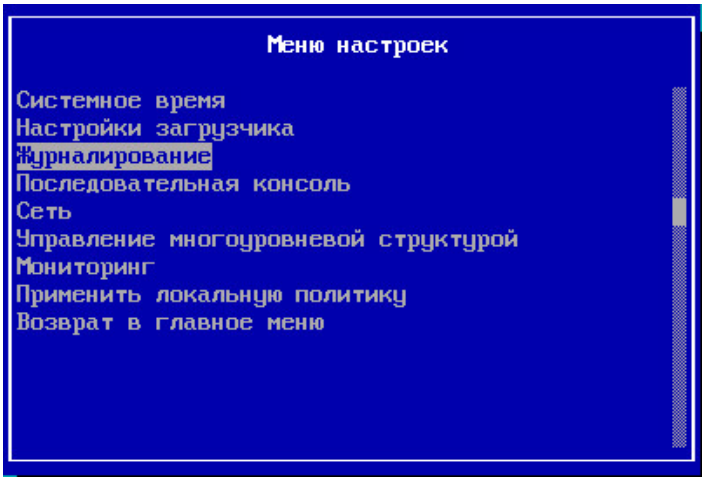


   В правой части окна появятся текущие настройки журналов узла. Сверху расположена область настройки уровня детализации событий, регистрируемых в журналах. Далее перечислены используемые внешние системные журналы. Внизу находится область настройки параметров автоматической очистки журналов при превышении заданного уровня занятого места на жестком диске компонента комплекса.

Для настройки параметров журналирования средствами локального управления:

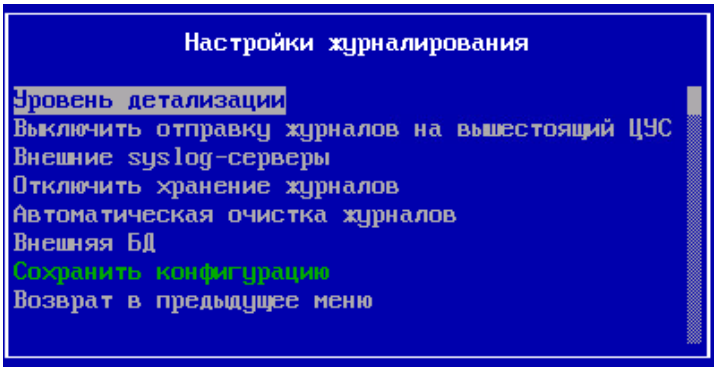
1. В главном меню выберите пункт "Настройки" и нажмите клавишу <Enter>.

   На экране появится меню настроек.



2. Выберите в меню пункт "Журналирование" и нажмите клавишу <Enter>.

   На экране появится меню настройки параметров сбора и хранения журналов.



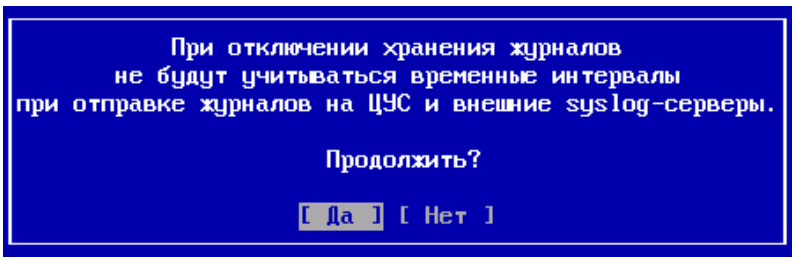
Управление хранением журналов

Включение или отключение функции хранения журналов компонента комплекса производится только при локальном управлении.

Для настройки хранения журналов компонента комплекса:

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

   В случае отключения хранения журналов на экране появится предупреждение.



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

   Будет выполнен возврат в меню "Настройки журналирования".

3. Выберите пункт "Сохранить конфигурацию" и нажмите клавишу <Enter>.
4. После проведения всех необходимых настроек выберите в "Меню настройки" пункт "Применить локальную политику" и нажмите клавишу <Enter>, а затем подтвердите изменения в конфигурации узла на вышестоящем ЦУС (см. стр. **48**).

Уровень детализации журнала

Для выбора уровня детализации в Менеджере конфигурации:

1. В настройках журналирования окна свойств компонента комплекса выберите требуемый уровень детализации журнала из раскрывающегося списка и нажмите кнопку "ОК".

Уровень детализации журнала	Уровень важности события
Отладочный	Отладка (DEBUG)
Минимальный	Информация (INFO)
Низкий	Ошибка (ERR)
Средний	Критическая ошибка (CRIT)
Высокий	Тревога (ALERT)
Предустановленный	Предупреждение (Warning)

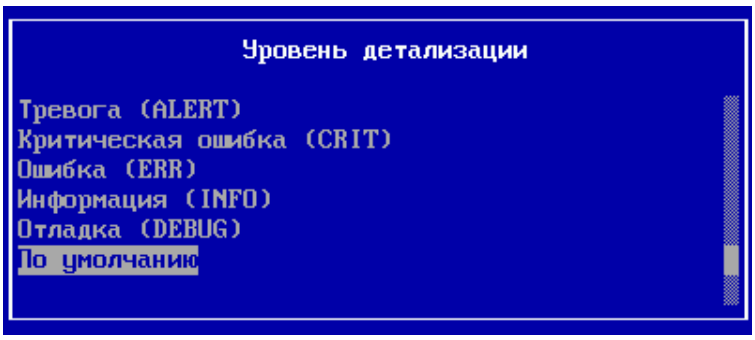
Внимание! При выборе какого-либо уровня в журнал будут попадать также события, имеющие более высокий уровень важности (см. стр. 111).

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

Для выбора уровня детализации при локальном управлении:

1. В меню настроек журналирования выберите пункт "Уровень детализации" и нажмите клавишу <Enter>.

   На экране появится список уровней важности событий.



2. Выберите требуемый уровень и нажмите клавишу <Enter>.

   Внимание! При выборе какого-либо уровня в журнал будут попадать также события, имеющие более высокий уровень важности. Уровню "По умолчанию" соответствуют события с уровнем важности "Предупреждение" (WARNING).

   Будет выполнен возврат в меню "Настройки журналирования".

3. В меню "Настройки журналирования" выберите пункт "Сохранить конфигурацию" и нажмите клавишу <Enter>.

   Дождитесь завершения операции.

4. После проведения всех необходимых настроек выберите в "Меню настройки" пункт "Применить локальную политику" и нажмите клавишу <Enter>, а затем подтвердите изменения в конфигурации узла на вышестоящем ЦУС (см. стр. 48).

Настройка хранения журналов на внешнем syslog-сервере

Внимание! Syslog-сервер должен поддерживать формат событий, описанный в RFC 5424.

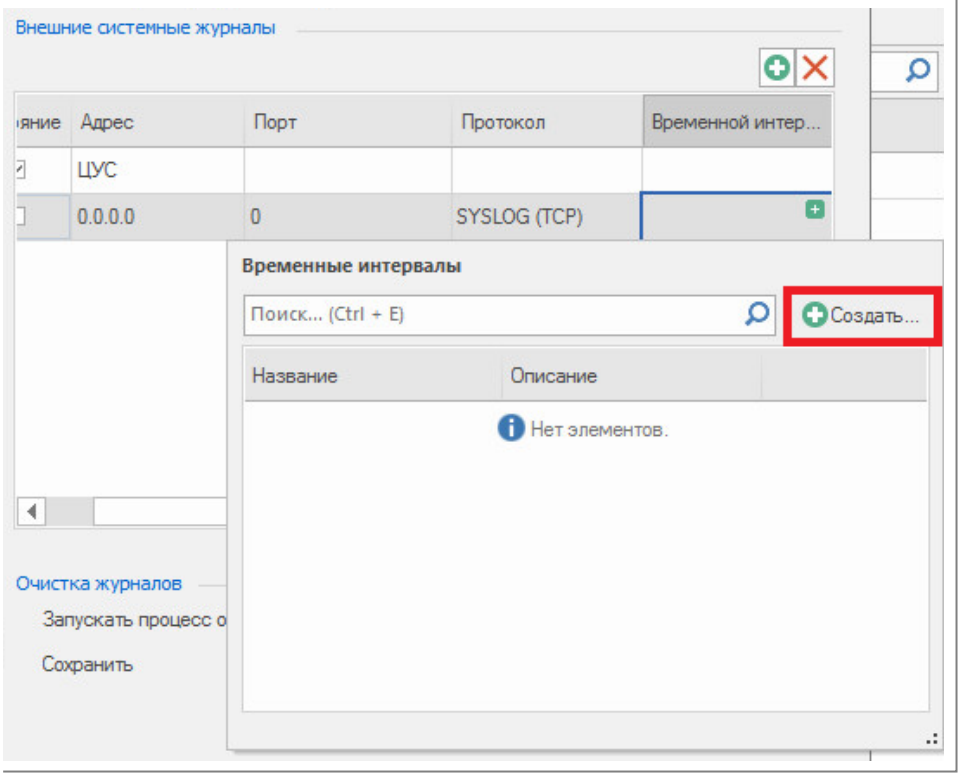
Для добавления нового syslog-сервера в Менеджере конфигурации:

1. В настройках журналирования окна свойств компонента комплекса (см. стр. 37) в области внешних системных журналов нажмите кнопку  .

   На экране появится строка для ввода параметров syslog-сервера.

2. Введите параметры syslog-сервера, переведите флажок состояния в активированное положение и нажмите кнопку "ОК".

Примечание. В случае если доступ к syslog-серверу предоставляется только в определенное время, укажите временной интервал подключения в последней графе строки параметров.



3. При необходимости добавить другой syslog-сервер повторите выполнение пп. **1–2**.
4. Для применения настроек нажмите кнопку "Установить политику" на панели инструментов, отметьте компоненты комплекса с измененными параметрами и нажмите кнопку "ОК".

Для изменения параметров syslog-сервера в Менеджере конфигурации:

1. В настройках журналирования окна свойств компонента комплекса (см. стр. 37) в области внешних системных журналов выберите нужную строку.
2. Измените параметры syslog-сервера нужным образом.
3. Для отключения хранения журналов на этом сервере переведите флажок состояния в отключенное положение.
4. После внесения всех корректировок нажмите кнопку "ОК".
5. Для применения настроек нажмите кнопку "Установить политику" на панели инструментов, отметьте компоненты комплекса с измененными параметрами и нажмите кнопку "ОК".

Для добавления нового syslog-сервера при локальном управлении:

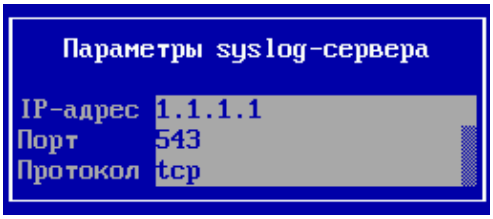
1. В меню "Настройки журналирования" выберите пункт "Внешние syslog-серверы" и нажмите клавишу <Enter>.

   На экране появится меню со списком syslog-серверов.

Примечание. Если syslog-серверы в список не добавлялись, список будет пустым.

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

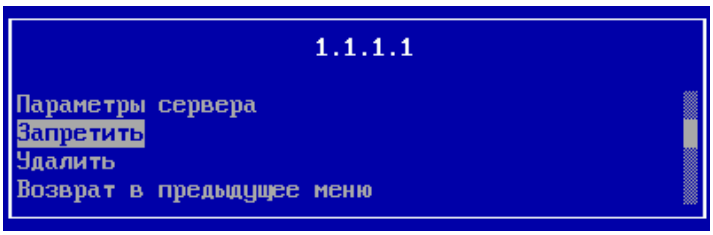
   На экране появится окно для ввода параметров syslog-сервера.



3. Введите параметры и нажмите клавишу <Enter>.

   На экране появится меню управления отправкой журналов на выбранный syslog-сервер.

Примечание. При добавлении нового syslog-сервера на него по умолчанию устанавливается разрешение на отправку журналов.



4. Выберите пункт "Возврат в предыдущее меню" или нажмите клавишу <Esc>.

   Будет выполнен возврат в предыдущее меню. В списке появится добавленный syslog-сервер.

5. При необходимости добавить другой syslog-сервер повторите выполнение пп. **2–4**.

6. Вернитесь в меню "Настройки журналирования", выберите пункт "Сохранить конфигурацию" и нажмите клавишу <Enter>.

7. После проведения всех необходимых настроек выберите в "Меню настройки" пункт "Применить локальную политику" и нажмите клавишу <Enter>, а затем подтвердите изменения в конфигурации узла на вышестоящем ЦУС (см. стр. **48**).

Для изменения параметров syslog-сервера при локальном управлении:

1. В меню "Настройки журналирования" выберите пункт "Внешние syslog-серверы" и нажмите клавишу <Enter>.

   На экране появится меню со списком syslog-серверов.

2. Выберите в списке сервер и нажмите клавишу <Enter>.

   На экране появится меню управления отправкой журналов на выбранный syslog-сервер.

3. Выберите нужный пункт меню и выполните соответствующую настройку.

Пункт меню	Описание
Параметры сервера	Изменение параметров сервера: • IP-адрес; • порт; • протокол
Запретить/Разрешить	Запрет или разрешение на отправку журналов на данный сервер
Удалить	Удаление сервера из списка

4. Вернитесь в меню "Настройки журналирования", выберите пункт "Сохранить конфигурацию" и нажмите клавишу <Enter>.

5. После проведения всех необходимых настроек выберите в "Меню настройки" пункт "Применить локальную политику" и нажмите клавишу <Enter>, а затем подтвердите изменения в конфигурации узла на вышестоящем ЦУС (см. стр. **48**).

Хранение журналов во внешней базе данных

Внимание! Если система мониторинга настроена на работу с внешней базой данных, то при потере соединения с этой базой данных сайт мониторинга будет недоступен.

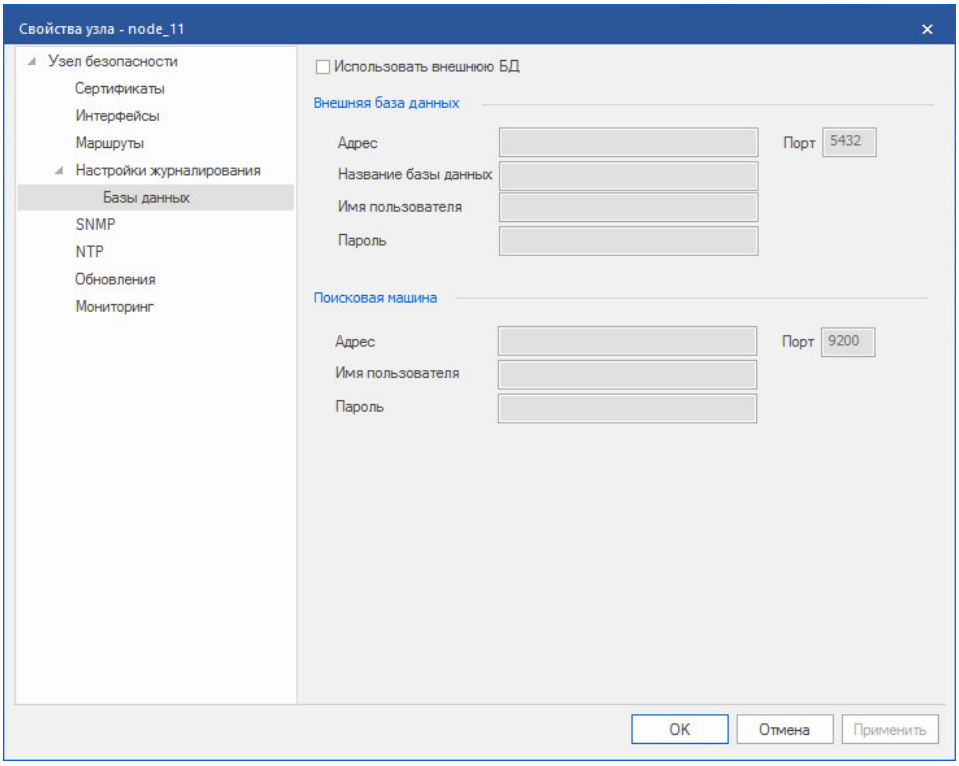
По умолчанию хранение журналов аудита и событий СОВ во внешней базе данных запрещено.

Внимание! В качестве внешней базы данных может выступать только СУБД PostgreSQL версии 9.5.4.

Для настройки хранения журналов во внешней базе данных в Менеджере конфигурации:

1. В окне свойств компонента комплекса в разделе "Узел безопасности" выберите пункт "Настройки журналирования" и подпункт "Базы данных".

   В правой части окна появятся текущие настройки хранения журналов во внешней базе данных.



2. Установите флажок "Использовать внешнюю БД".

   На экране станут активными разделы для ввода параметров внешней базы данных и поисковой машины.

3. Введите требуемые параметры и нажмите кнопку "ОК".

   Внимание! Сервер внешней базы данных должен поддерживать формат событий, описанный в RFC 5424.

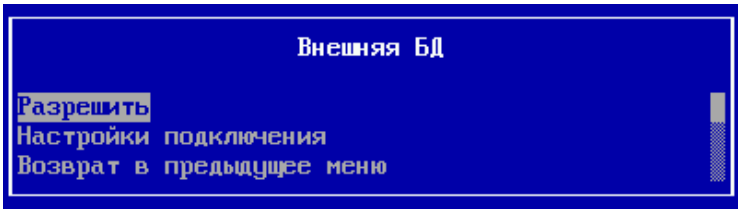
4. Для ведения журналов мониторинга ЦУС во внешней базе данных выберите в левой части окна свойств узла в разделе "Узел безопасности" пункт "Мониторинг" и повторите пп. **2–3**.

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

Для включения хранения журналов во внешней БД при локальном управлении:

6. В меню "Настройки журналирования" выберите пункт "Внешняя БД" и нажмите клавишу <Enter>.

   На экране появится меню управления хранением журналов во внешней БД.



7. Выберите пункт "Разрешить" и нажмите клавишу <Enter>.

   Пункт меню изменится на "Запретить".

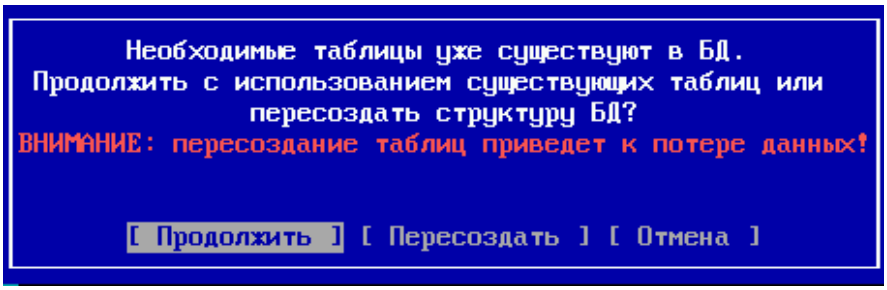
8. Для настройки параметров подключения к БД выберите пункт "Настройки подключения" и нажмите клавишу <Enter>.

   На экране появится окно настройки подключения к БД.

9. Введите параметры подключения к БД и нажмите клавишу <Enter>.

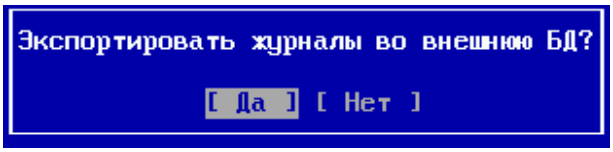
   Начнется подключение к БД и проверка готовности к экспорту журналов.

   - Если во внешней БД отсутствуют необходимые таблицы и у пользователя есть права на их создание, таблицы будут созданы.
   - Если у пользователя отсутствуют права на создание таблиц, на экране появится соответствующее сообщение.
   - Если таблицы уже созданы, на экране появится запрос на использование существующих или на пересоздание новых.



Внимание! При подключении к БД с уже существующими таблицами и данными (СОВ, Аудит или Мониторинг) будет производиться переиндексация этих данных, что может занять длительное время (при 300 млн записей переиндексация может длиться больше суток).

После создания таблиц на экране появится запрос на экспорт всех локальных журналов.



10. Выберите "Да" и нажмите клавишу <Enter>.
11. Вернитесь в предыдущее меню и далее последовательно выполните сохранение конфигурации и применение локальной политики.

> **Внимание!** После применения локальной политики просмотр журналов, выгрузка и очистка будут производиться из внешней базы данных.

12. Подтвердите изменения в конфигурации узла на вышестоящем ЦУС (см. стр. **48**).

Автоматическая очистка журналов

По умолчанию автоматическая очистка по сроку давности записей журналов отключена.

Для ограничения журналирования по использованию диска в Менеджере конфигурации:

1. В настройках журналирования окна свойств компонента комплекса укажите параметры автоматической очистки журналов по достижении заданного уровня заполненности жесткого диска узла и нажмите кнопку "ОК".

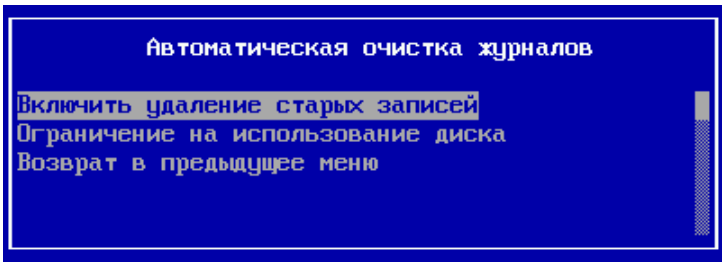
> **Внимание!** Процесс очистки не может оставить менее 10% записей журналов и запускаться при заполненности диска более чем на 90%.

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

Для ограничения журналирования по использованию диска при локальном управлении:

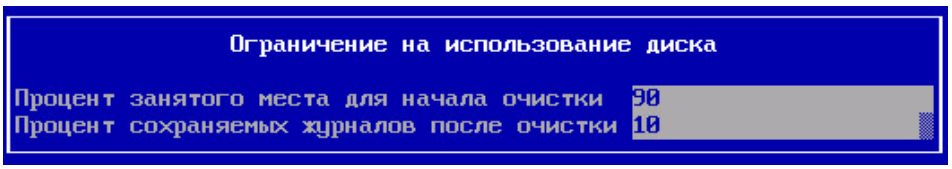
1. В меню "Настройки журналирования" выберите пункт "Автоматическая очистка журналов" и нажмите клавишу <Enter>.

   На экране появится меню управления автоматической очисткой журналов.



1. Выберите пункт "Ограничение на использование диска" и нажмите клавишу <Enter>.

   На экране появится окно настройки параметров.



> **Внимание!** Процесс очистки не может оставить менее 10% записей журналов и запускаться при заполненности диска более чем на 90%.

2. Введите значения параметров и нажмите клавишу <Enter>.
3. Вернитесь в предыдущее меню и далее последовательно выполните сохранение конфигурации и применение политики.

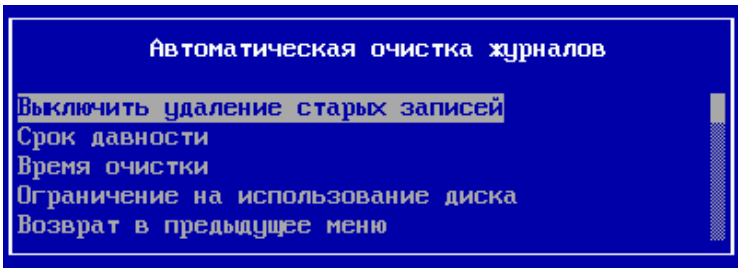
Для включения автоматической очистки журналов при локальном управлении:

4. В меню "Настройки журналирования" выберите пункт "Автоматическая очистка журналов" и нажмите клавишу <Enter>.

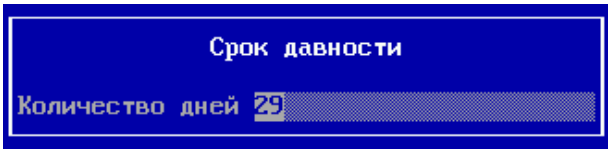
На экране появится меню управления автоматической очисткой журналов.

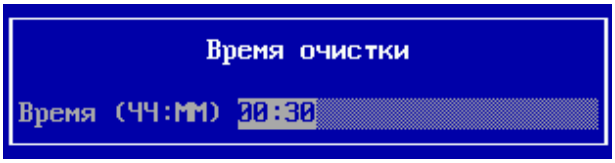
5. Выберите пункт "Включить удаление старых записей" и нажмите клавишу <Enter>.

   Содержание меню изменится: пункт "Включить удаление старых записей" изменится на "Выключить удаление старых записей" и будут добавлены новые пункты.



6. Если нет необходимости изменять параметры автоматической очистки, заданные по умолчанию (см. ниже), вернитесь в предыдущее меню и далее последовательно выполните сохранение конфигурации и применение политики.
7. Если необходимо изменить параметры автоматической очистки, заданные по умолчанию, выберите пункт "Срок давности" или "Время очистки" и введите нужное значение параметра.





8. Вернитесь в предыдущее меню и далее последовательно выполните сохранение конфигурации и применение политики.
9. Подтвердите изменения в конфигурации узла на вышестоящем ЦУС (см. стр. **48**).

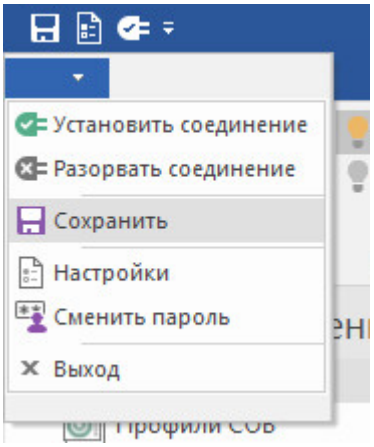
Передача сведений об изменениях в настройках

После внесения изменений в настройки компонента комплекса, например, в его сетевые параметры, необходимо:

- если работы по изменению настроек проводились через Менеджер конфигурации, нужно сохранить настройки и установить политику на узлы с измененной конфигурацией;
- при локальном управлении — администратору компонента комплекса требуется сохранить конфигурацию в локальной базе данных и передать сведения об изменениях на вышестоящий ЦУС, после чего администратор ЦУС должен подтвердить пришедшие изменения.

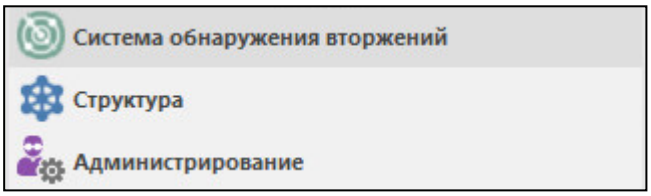
Для сохранения настроек в Менеджере конфигурации:

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

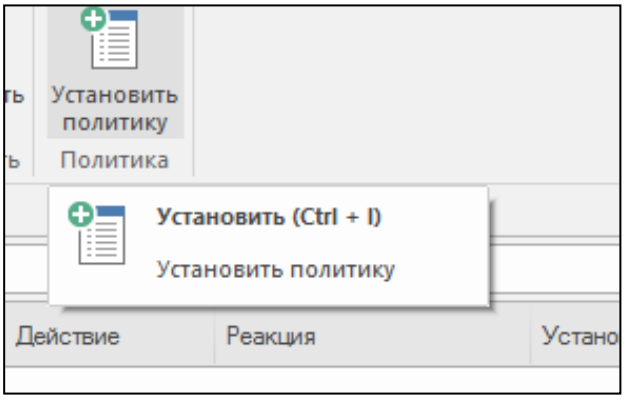


Для установки политики в Менеджере конфигурации:

1. Перейдите в раздел "Система обнаружения вторжений".



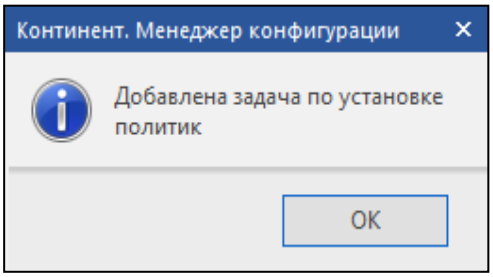
2. Нажмите на панели инструментов кнопку "Установить политику".



На экране появится окно "Установить политики".

3. Выберите в списке компонент комплекса, на который нужно установить политику, и нажмите кнопку "ОК".

На ЦУС будет сформирована задача по установке политики на указанные узлы, и на экране появится сообщение о добавлении новой задачи.



4. Нажмите кнопку "ОК" в окне сообщения.

Окно сообщения закроется.

Если в данный момент на ЦУС никакие другие задачи не выполняются, начнется выполнение добавленной задачи. При этом в нижнем правом углу главного окна Менеджера конфигурации рядом со значком появится

цифра, соответствующая общему количеству поставленных в очередь и выполняющихся задач.

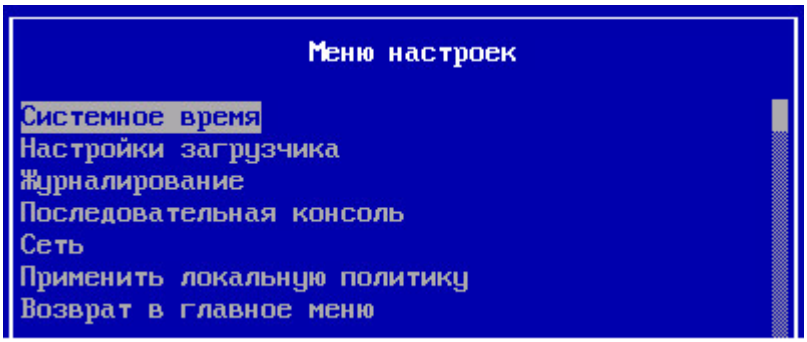
5. Для просмотра сведений о поставленных задачах нажмите на значок .

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

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>.

   Начнется применение локальных изменений и отправка их на ЦУС. При этом будет создан служебный пакет данных по изменениям в локальной политике компонента комплекса, а затем он будет помещен в очередь на запись в вышестоящую базу данных ЦУС с присвоением очередного порядкового номера.

   Дождитесь завершения процесса и появления сообщения "Успешно".

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

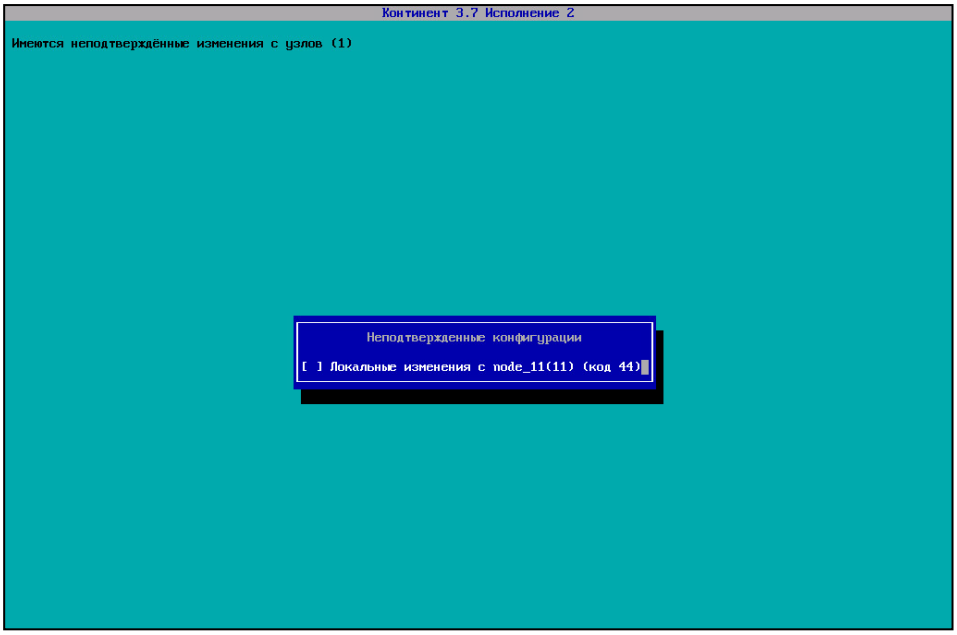
3. Нажмите клавишу <Enter>.

   Будет выполнен возврат в меню "Инструменты".

Для подтверждения изменения конфигурации УБ на ЦУС посредством локального управления:

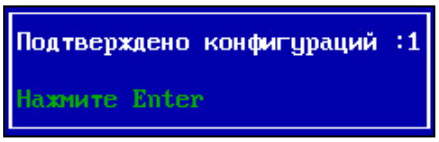
1. В меню "Инструменты" главного меню локального управления ЦУС текущего домена выберите пункт "Подтверждение изменений настроек УБ" и нажмите клавишу <Enter>.

   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>.

   БД ЦУС будет изменена в соответствии с переданной конфигурацией, затем будет выполнен возврат в меню "Инструменты".

4. Для возврата в главное меню нажмите клавишу <Esc>.

Передача сведений при отсутствии связи

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

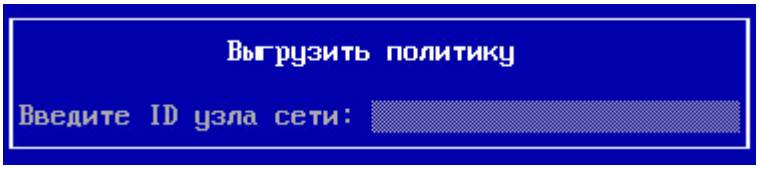
Для выгрузки конфигурации УБ на носитель (только на ЦУС):

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

   На экране появится окно "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 окно "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>.

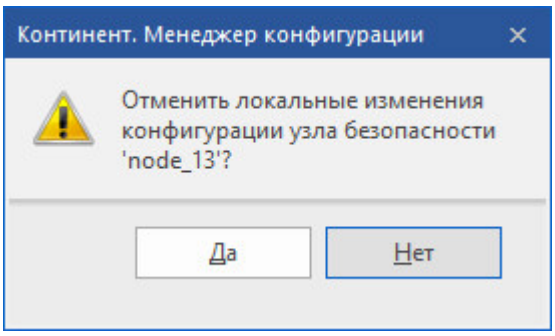
   Будет запущен процесс установки политики, после чего появится сообщение об успешном завершении процесса.

Учет конфигураций узлов

После изменений в настройках подчиненных узлов и отправки локальных изменений на вышестоящий ЦУС в Менеджере конфигурации в поле "Версия конфигурации" для этих узлов числовое значение конфигурации меняется на оповещающий значок "Локальная". Это означает, что на узле безопасности находится неподтвержденная и в то же время неотмененная конфигурация.
Изменения в настройках подчиненных узлов администратор в Менеджере конфигурации может подтвердить или отменить.

Для отмены пришедшей конфигурации:

1. Откройте Менеджер конфигурации и перейдите в раздел "Структура".
2. В списке узлов безопасности выберите узел с измененной 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 "Локальная". Это означает, что на узле безопасности находится отмененная на ЦУС локальная конфигурация.

3. Для применения настроек установите политику на этот узел безопасности (см. выше).

   Оповещающий значок изменится на новое числовое значение конфигурации. На узле безопасности будет действовать конфигурация, пришедшая с ЦУС. Ее параметры совпадают с изначальными (до локальных изменений конфигурации).

Для подтверждения пришедшей конфигурации:

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

Внимание! В случае если конфигурация этого узла безопасности изменялась в Менеджере конфигурации после получения пакета локальных изменений, причем был изменен один из тех же параметров,которые менялись посредством локального управления, то подтвердить локальные изменения не получится, так как впоследствии произойдет конфликт слияния (merge conflict). В этом случае нужно отменить локальные изменения и установить политику на этот узел безопасности из Менеджера конфигурации (см. выше).

Оповещающий значок изменится на новое числовое значение конфигурации. Ее параметры соответствуют заданным пользователем при настройке в локальном меню узла.

Внимание! В случае если конфигурация не установилась автоматически, необходимо установить политику на этот узел безопасности.

Таким образом, в Менеджере конфигурации существуют следующие графические обозначения типа конфигурации:

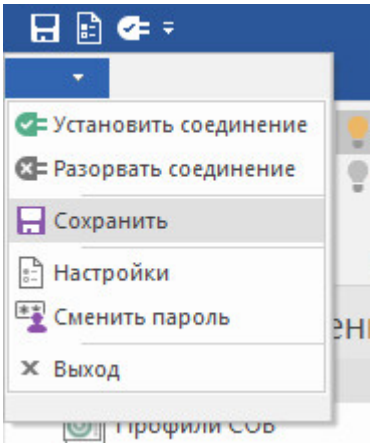
Иконка	Статус конфигурации
	На узле безопасности находится неподтвержденная и в то же время неотмененная локальная конфигурация
	На узле безопасности находится отмененная на ЦУС локальная конфигурация
	На узле безопасности находится утвержденная на ЦУС конфигурация

Сохранение настроек

После выполнения настроек компонента и профиля эти настройки необходимо сохранить.

Для сохранения настроек:

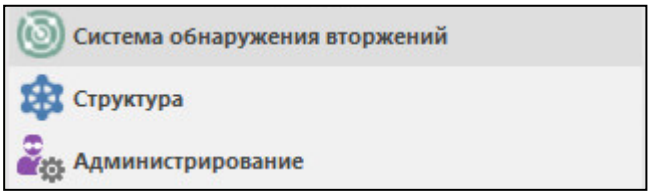
- В левом верхнем углу окна Менеджера конфигурации нажмите кнопку вызова меню и выберите пункт "Сохранить".



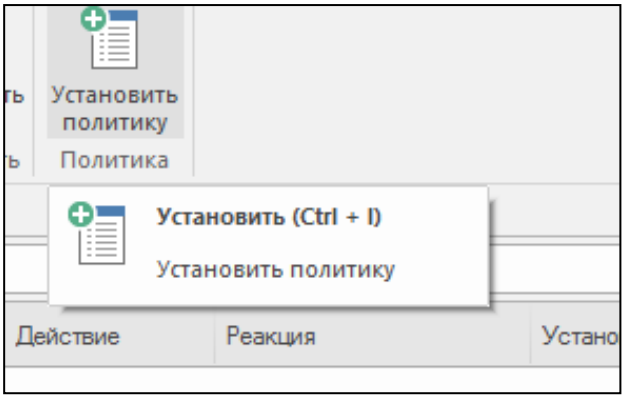
Установка политик

Для установки политики:

1. Перейдите в раздел "Система обнаружения вторжений".



2. Нажмите на панели инструментов кнопку "Установить политику".

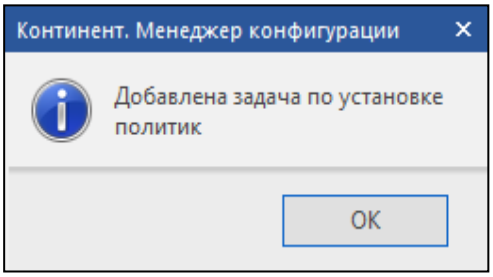


На экране появится окно "Установить политики".

3. Выберите в списке детектор атак, на который будет установлена политика, и нажмите кнопку "ОК".

Примечание. На ДА допускается совместное использование политики активного профиля (но только одного) текущего и вышестоящих доменов. В этом случае эти политики дополняют друг друга в сторону усиления безопасности.

На ЦУС будет сформирована задача по установке политики на указанный детектор атак, и на экране появится сообщение о добавлении новой задачи.



4. Нажмите кнопку "ОК" в окне сообщения.

   Окно сообщения закроется.

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

5. Для просмотра сведений о поставленных задачах нажмите на значок .

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

Список задач

При установке политик на узел безопасности или на домен ЦУС формирует соответствующую задачу. 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 на ЦУС в виде списка, в котором отображается следующая информация:

- название задачи;
- логин администратора — инициатора этой задачи;
- статус ("выполнена", "выполняется", "зарегистрирована", "ошибка");
- прогресс (процент выполнения);

- время добавления задачи в список;
- время начала выполнения;
- время, затраченное на выполнение.

После занесения в список сведения о задаче хранятся в течение 14 дней, после чего автоматически удаляются.

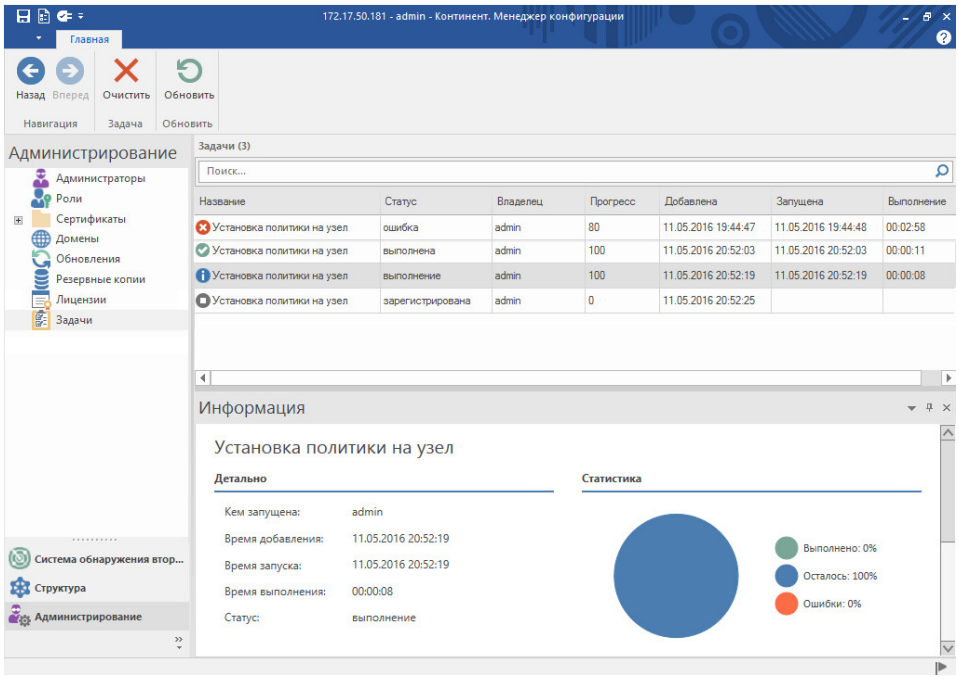
Предусмотрена принудительная очистка списка. Очистка заключается в удалении из списка задач, имеющих статус "выполнена" и "ошибка".

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 Менеджера конфигурации можно выполнить, нажав на значок , расположенный в нижнем правом углу главного окна, а затем ссылку "Переход к списку задач" в появившемся окне центра уведомлений.



   Для отображения в списке статуса задачи используются следующие пиктограммы:

	Зарегистрирована
	Выполняется
	Выполнена
	Ошибка

2. Если задача связана с применением политик к нескольким узлам безопасности или к домену, 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".

   Будут удалены выполненные задачи, а также завершенные с ошибкой. Задачи со статусом "выполняется" или "зарегистрирована" останутся в списке.

Перезагрузка и выключение

Перезагрузку и выключение компонента комплекса выполняет авторизованный пользователь с правами главного администратора.

Для перезагрузки/выключения компонента комплекса в Менеджере конфигурации:

1. В разделе "Структура" Менеджера конфигурации выделите нужный компонент комплекса и нажмите кнопку перезагрузки или завершения работы на панели инструментов.

   На экране появится запрос на подтверждение операции.

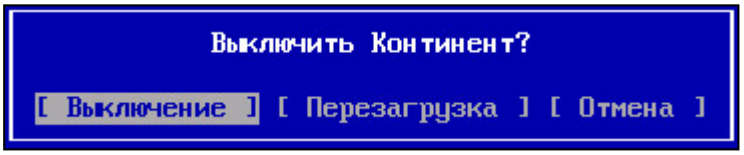
2. Нажмите кнопку "Да".

   В зависимости от выбранного варианта произойдет выключение или перезагрузка компонента комплекса.

Для перезагрузки/выключения компонента комплекса 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 компонента комплекса или начнется его перезагрузка.

Удаление

Для удаления компонента комплекса:

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

   В окне отобразится список всех узлов домена.

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

   На экране появится запрос на подтверждение удаления узла сети.

3. Нажмите кнопку "Да" в окне запроса, после чего сохраните изменения в конфигурации домена.

4. Для применения конфигурации установите политику на ЦУС домена, в котором был удаленный узел (см. стр. **51**).

   Узел безопасности будет удален.

Примечание. Вся накопленная статистическая информация по удаленному узлу будет сохранена по его ID. Если впоследствии узел восстановить (создать новый с тем же ID), то ведение статистического учета для него будет продолжено.

Управление СОВ

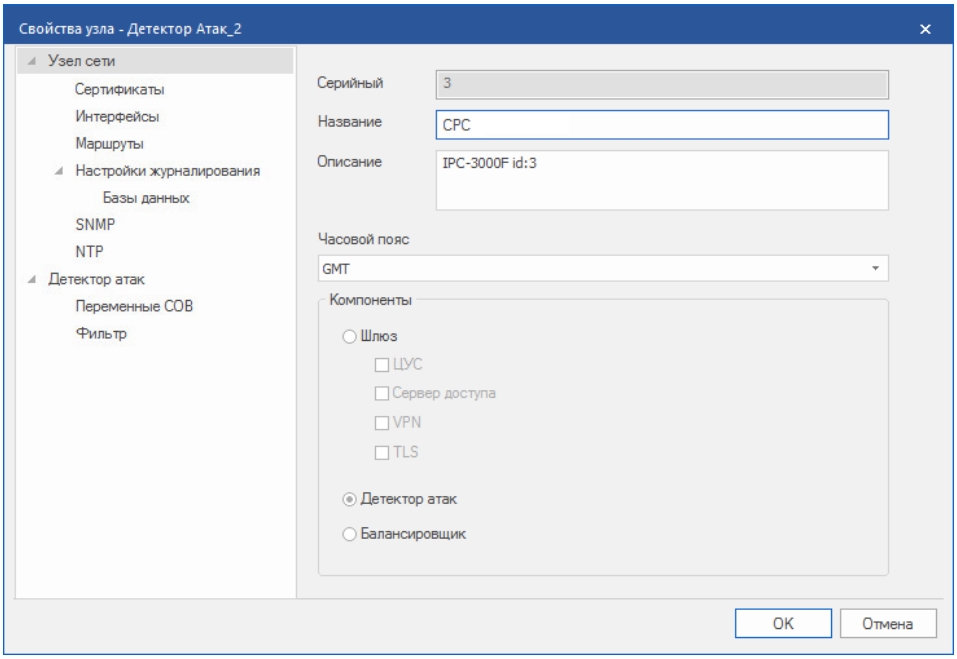
Основным компонентом СОВ является детектор компьютерных атак. Для настройки работы ДА необходимо выполнить следующее:

1. Настроить параметры работы ДА по соответствующей схеме включения (см. ниже).
2. Создать и настроить профиль (см. стр. **58**).
3. Создать правила профиля СОВ (см. стр. **61**).
4. Сохранить выполненные настройки (см. стр. **51**).
5. Установить политику профилей (см. стр. **51**).

Настройка параметров ДА

Для настройки параметров:

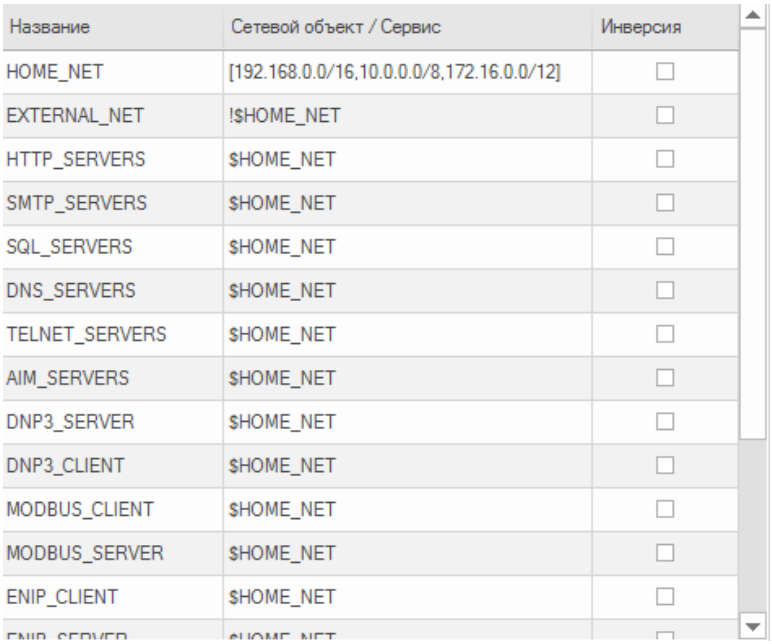
1. Перейдите в раздел "Структура" Менеджера конфигурации, выберите узел безопасности, выполняющий функции детектора атак, и вызовите окно настройки свойств.



2. При необходимости измените содержание полей "Название" и "Описание" и выберите часовой пояс.
3. 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	☐

4. 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.

   Примечание. Для указания сетевых объектов или сервисов допустимо 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).

   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.

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

Для настройки конфигурации прокси-сервера:

1. Перейдите в раздел "Структура" Менеджера конфигурации, выберите детектор атак и вызовите окно настройки свойств.
2. В разделе "Детектор атак" выставите отметку в поле "Пользователи располагаются за http-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 в режиме Inline (интерфейсы, режим bypass, хранение трафика атаки)

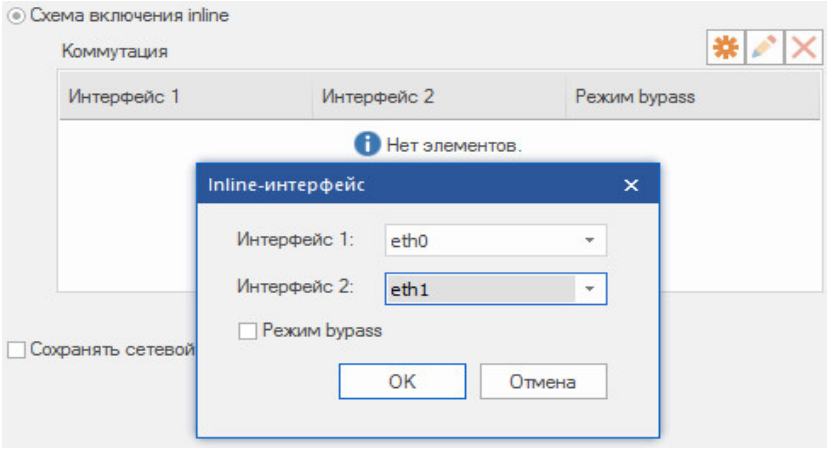
Для настройки параметров:

1. Вызовите окно настройки свойств нужного 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.

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

   Созданные настройки будут сохранены и окно "Свойства узла" автоматически закроется.
7. Для применения настроек нажмите кнопку "Установить политику" на панели инструментов, отметьте ДА с измененными параметрами и нажмите кнопку "ОК".

Настройка ДА в режиме Monitor (интерфейсы и хранение трафика атаки)

Для настройки режима:

1. Вызовите окно настройки свойств нужного 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 и при необходимости установите отметку в поле "Сохранять сетевой трафик атаки".
3. В случае если не указан интерфейс мониторинга, нажмите кнопку и выберите в раскрывающемся списке нужный физический интерфейс.

   Примечание. Для указания сетевых объектов или сервисов допустимо пользоваться их перечислением через запятую (при этом содержание переменной нужно заключить в скобки), а также другими переменными (в формате $Имя_переменной) и флагом инверсии.
4. Нажмите кнопку "ОК".

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

Создание и настройка профиля СОВ

Совет. В процессе эксплуатации комплекса целесообразно перед созданием нового профиля СОВ провести обновление БРП (см. стр. 62). Для этой процедуры необходима соответствующая лицензия.

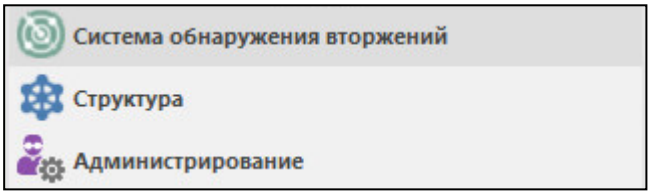
Примечание. В системе доступны предустановленные профили:

- Оптимальный набор, содержащий оптимальную выборку из правил, детектирующих угрозы для служб передачи данных, веб-клиентов и веб-серверов.
- Полный набор, содержащий полную выборку правил.

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

Для создания и настройки профиля СОВ:

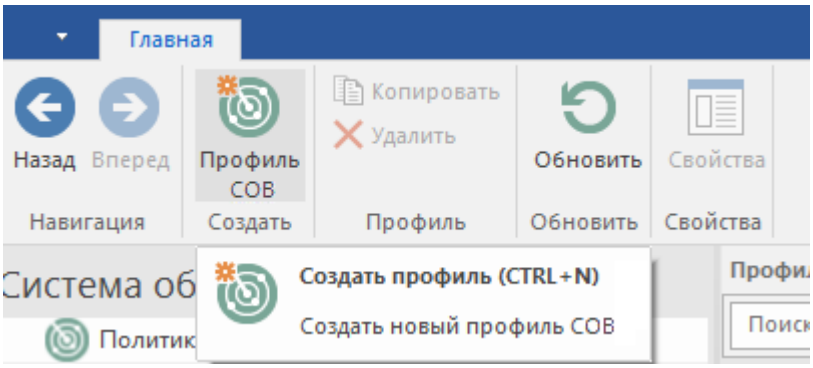
1. В главном окне Менеджера конфигурации откройте раздел "Система обнаружения вторжений".



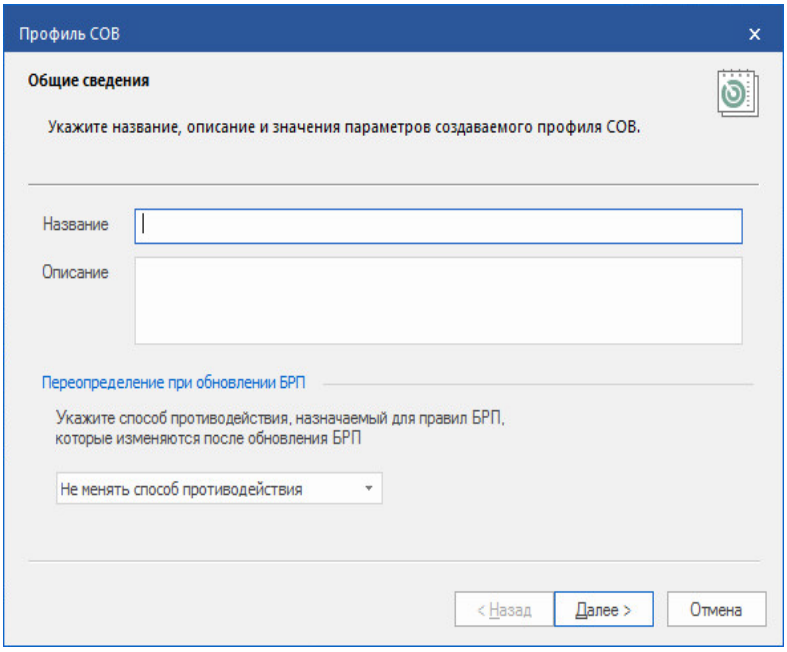
2. Перейдите в подраздел "Профили СОВ".

   Справа появится список созданных профилей.

3. Нажмите на панели инструментов кнопку "Создать новый профиль".



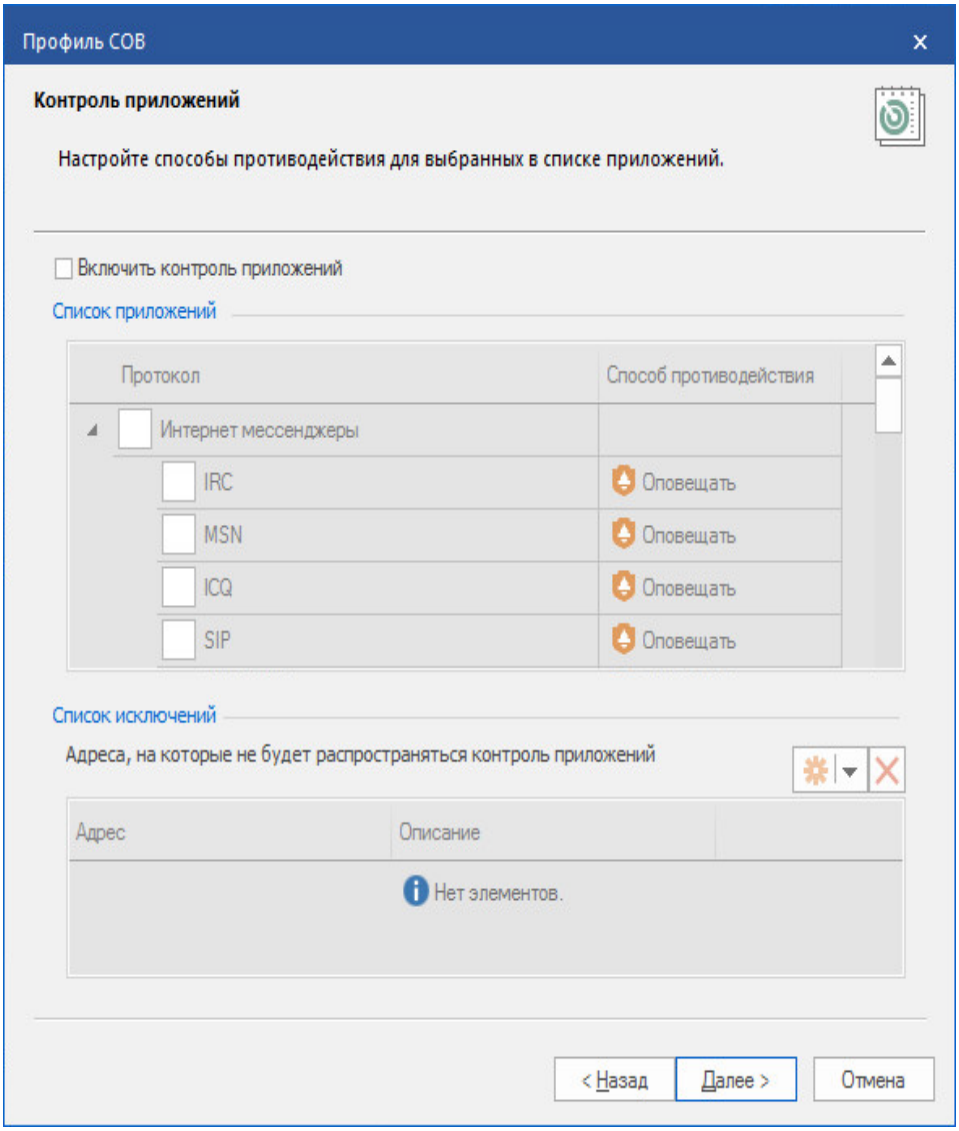
   На экране появится диалоговое окно мастера создания профиля СОВ.



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 контроля приложений.



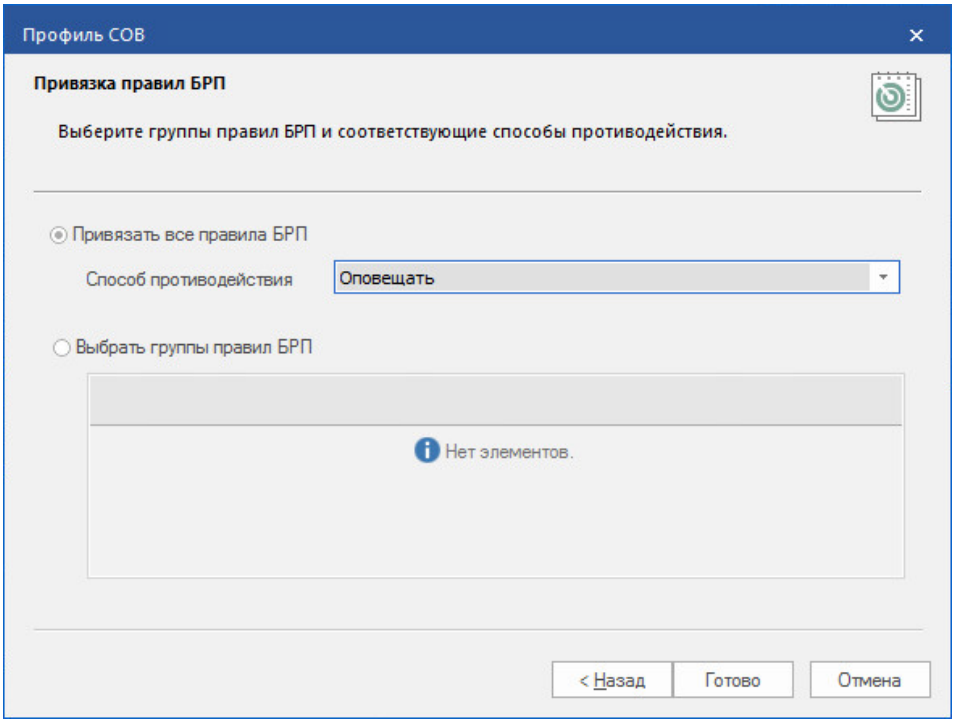
5. При необходимости включить контроль приложений установите отметку в поле "Включить контроль приложений" и назначьте способ противодействия для каждого приложения.

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

6. При необходимости настроить список 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".

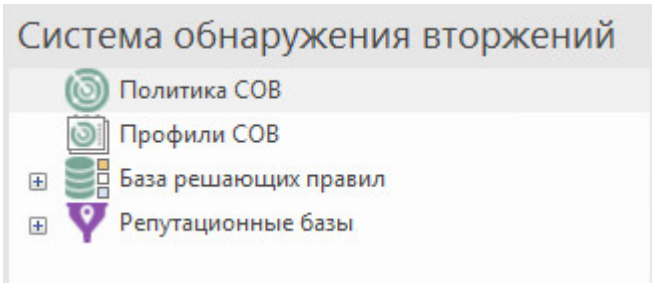
В результате будет создан новый профиль, параметры которого отобразятся в списке на экране, а в подразделе "База решающих правил" в таблице со списком решающих правил появится колонка с названием созданного профиля.

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

Создание и настройка правил политики СОВ

Для создания и настройки правил:

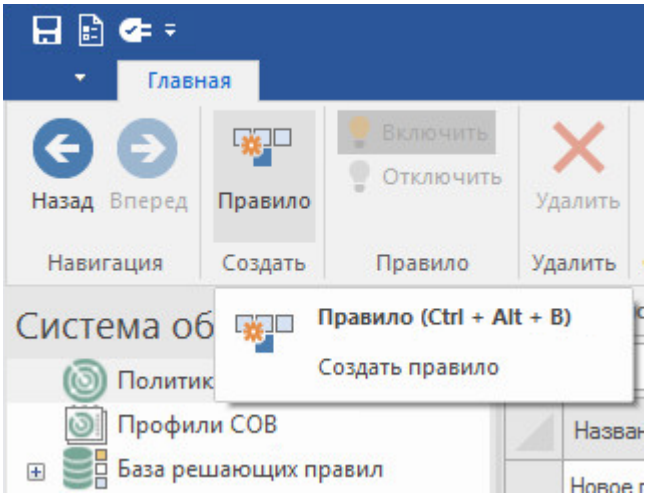
1. В разделе "Система обнаружения вторжений" перейдите на подраздел "Политика СОВ".



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

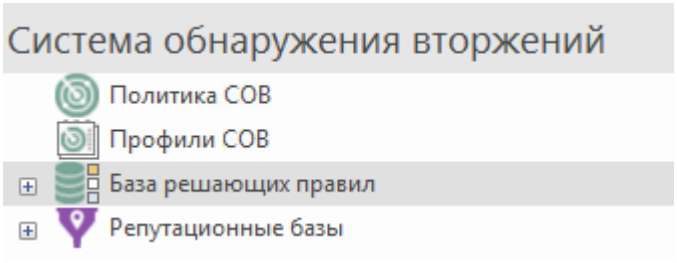
Управление БРП

Обновление БРП

Внимание! 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. ниже).

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
		Степень опасности	Описание	Класс	Ревизия	monitor
		Высокая	EXPLOIT GNOME Project libxslt Librar...	Попытка получения приви...	2	Оповещать
		Высокая	WEB_CLIENT IE Memory Corruption V...	Попытка получения приви...	3	Оповещать
		Высокая	WEB_CLIENT Possible Internet Explor...	Попытка получения приви...	2	Оповещать
		Высокая	WEB_CLIENT Possible Internet Explor...	Попытка получения приви...	3	Оповещать
		Высокая	CURRENT_EVENTS Nuclear EK CVE...	Обнаружена активность т...	4	Оповещать
		Высокая	WEB_SERVER Microsoft SharePoint ...	Атака на веб-приложение	4	Оповещать
		Высокая	WEB_CLIENT Microsoft Internet Explo...	Попытка получения приви...	4	Оповещать
		Высокая	VOIP Asterisk Invalid RTP Payload Ty...	Попытка получения приви...	2	Оповещать

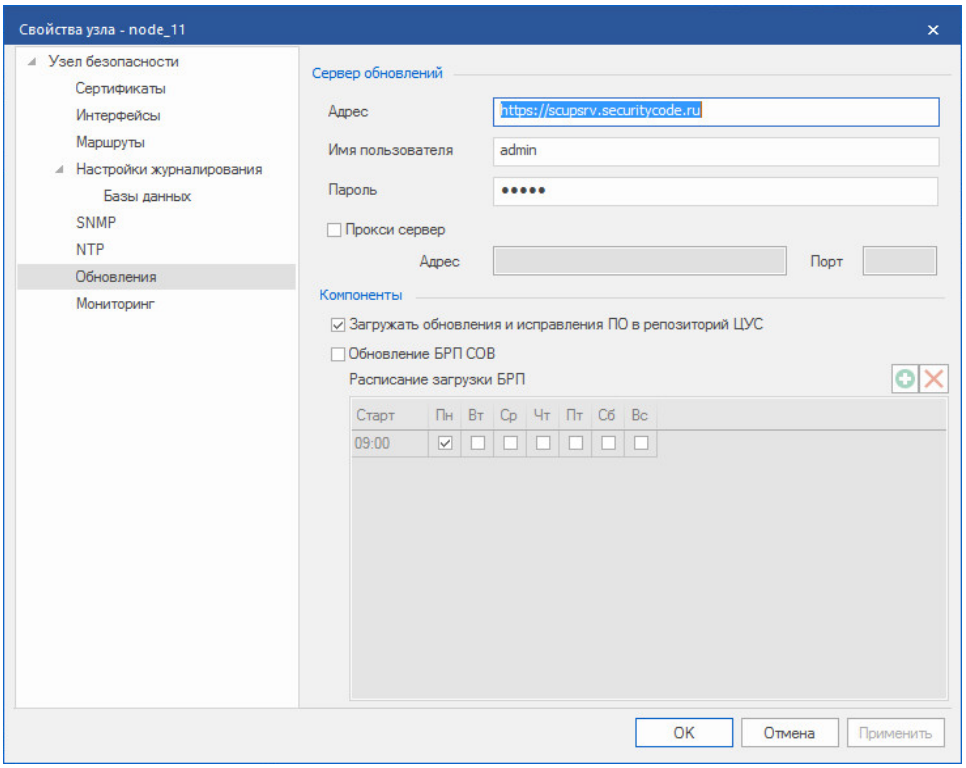
6. Сохраните изменения в конфигурации домена, нажав кнопку в верхнем левом углу Менеджера конфигурации, а затем распространите обновленную БРП на подчиненные узлы безопасности и поддомены (см. стр. **64**).

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.
   - 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 "Обновление БРП СОВ".
- 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 верхнем левом углу Менеджера конфигурации.
6. Для применения настроек нажмите кнопку "Установить политику" на панели инструментов, отметьте ЦУС и его подчиненные УБ и нажмите кнопку "ОК".

Для распространения обновленной БРП на узлы безопасности при иерархической структуре доменов:

1. На корневом домене создайте профиль обновления и политику СОВ для всех узлов сети.

   Примечание. Если требуется только обновить актуальный список решающих правил СОВ по всей иерархии доменов, то данный пункт можно пропустить.

2. Сохраните изменения в конфигурации домена, нажав кнопку  в верхнем левом углу Менеджера конфигурации.
3. Для применения настроек нажмите кнопку "Установить политику" на панели инструментов, отметьте ЦУС, его подчиненные УБ и поддомены и нажмите кнопку "ОК".

   Примечание. Если политику СОВ применить только к корневому домену, то профиль СОВ будет применен только к узлам безопасности корневого домена.

   В случае если на нижестоящих доменах нет пользовательских локальных политик и профилей СОВ, на узлы безопасности нижестоящих доменов будет применен глобальный профиль СОВ с обновленным списком решающих правил.

   В случае если на нижестоящих доменах уже есть пользовательские профили или политики СОВ, на узлы безопасности нижестоящих доменов будут применены глобальный профиль СОВ и глобальная политика СОВ. Пользовательские профили СОВ нижестоящих доменов наследуют способ противодействия решающих правил от глобального профиля СОВ в сторону ужесточения. На узлы безопасности будут сформированы обновленные профили СОВ с унаследованными способами противодействия и обновленным списком решающих правил.

Офлайн-обновление БРП

Перед началом обновления БРП необходимо загрузить и установить ПО «Континент TLS VPN Клиент». Зарегистрируйтесь на сайте компании и загрузите дистрибутив из раздела "Демо-версии".
При первом запуске TLS-клиента будет предложено зарегистрировать программу на сервере регистрации компании "Код Безопасности". Подробнее см. в руководстве администратора СКЗИ "Континент TLS-клиент".

Для офлайн-обновления БРП:

1. Скопируйте с дистрибутивного диска с БРП файлы сертификатов для подключения к серверу обновлений.
2. Импортируйте сертификат:
   - Дважды щелкните по выбранному файлу сертификата.

     Откроется окно управления сертификатом.

- Нажмите кнопку "Установить сертификат".
- Установите сертификат, следуя инструкции.

Внимание! Для параметра "Тип хранилища" установите значение "Доверенные корневые центры сертификации".

- При появлении предупреждения системы безопасности, подтвердите установку сертификата.

3. Запустите "Континент TLS-клиент".
4. В главном окне нажмите кнопку "Добавить", чтобы создать новое соединение.
5. В раскрывающемся списке "Тип соединения" выберите значение "Ресурс".
6. В группе параметров "Редактирование ресурса" укажите параметры соединения:
   - адрес ресурса;
   - имя ресурса;
   - удаленный порт;
   - тип ресурса;
   - описание (необязательно);
7. Нажмите кнопку "Сохранить".
8. В меню настроек на вкладке "Основные" удалите отметку в поле "Проверять сертификаты по CRL".
9. В браузере откройте URL для загрузки архива с БРП https://scupsrv.securitycode.ru/rules/ids_update.json.gz.

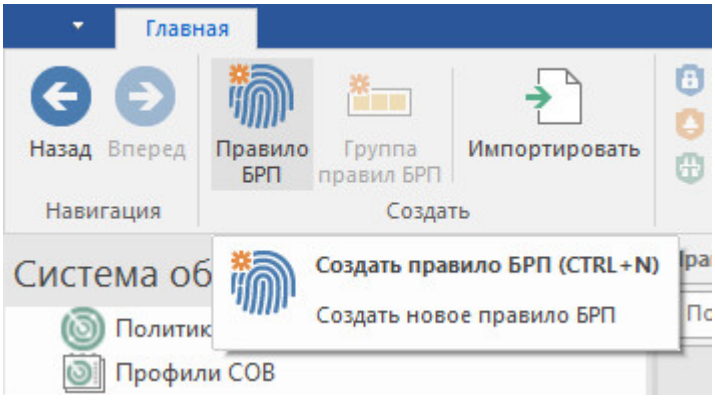
   Примечание. Рекомендуется использовать браузер Internet Explorer.

   На экране отобразится окно авторизации.
10. В окно авторизации введите имя пользователя и пароль, полученные от технической поддержки.
11. Загрузите БРП в Менеджер конфигурации, выполнив процедуру локального обновления (см. стр. **62**)

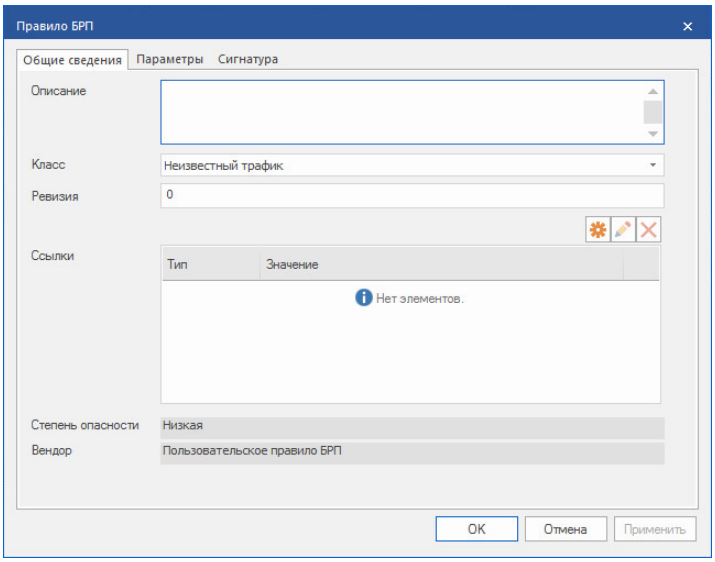
Создание пользовательского решающего правила

Для создания правила:

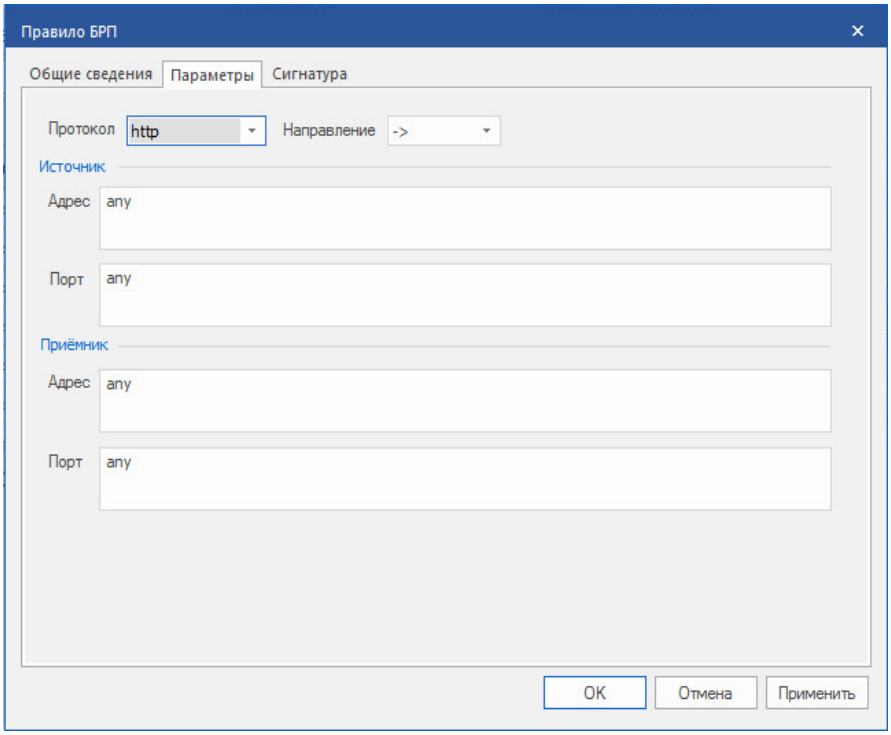
1. На вкладке "Система обнаружения вторжений" перейдите в подраздел "База решающих правил/Пользовательские правила" и нажмите на панели инструментов кнопку "Создать новое правило БРП".



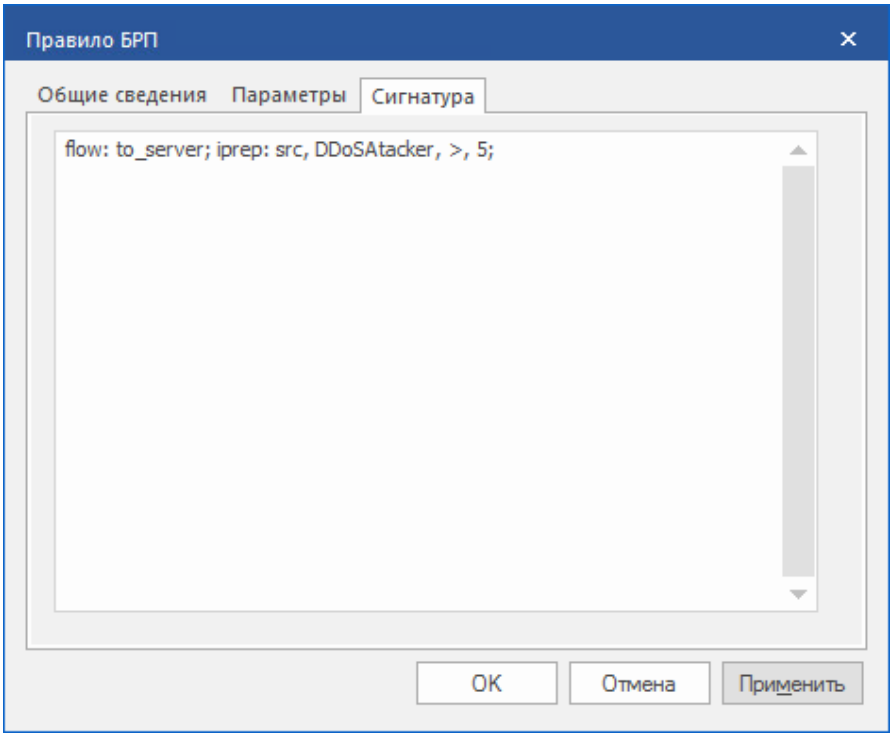
На экране появится окно "Правило БРП".



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



3. Заполните поля параметров источника и приемника (см. стр. **143**) и перейдите на вкладку "Сигнатура".



4. Введите сигнатуру правила (см. стр. **144**) и нажмите кнопку "ОК".

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

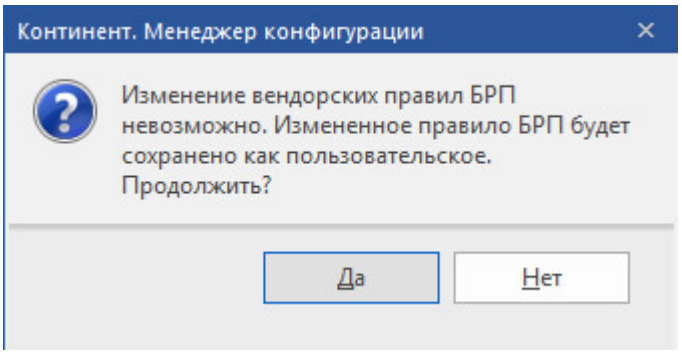
Создание пользовательского решающего правила-исключения

При эксплуатации комплекса может возникнуть ситуация, когда для определенных IP-адресов не требуется срабатывание некоторой сигнатуры, входящей в состав вендорского правила. Для этого необходимо создать пользовательское правило-исключение и включить его в состав соответствующего профиля СОВ.

Для создания пользовательского правила-исключения на базе вендорского:

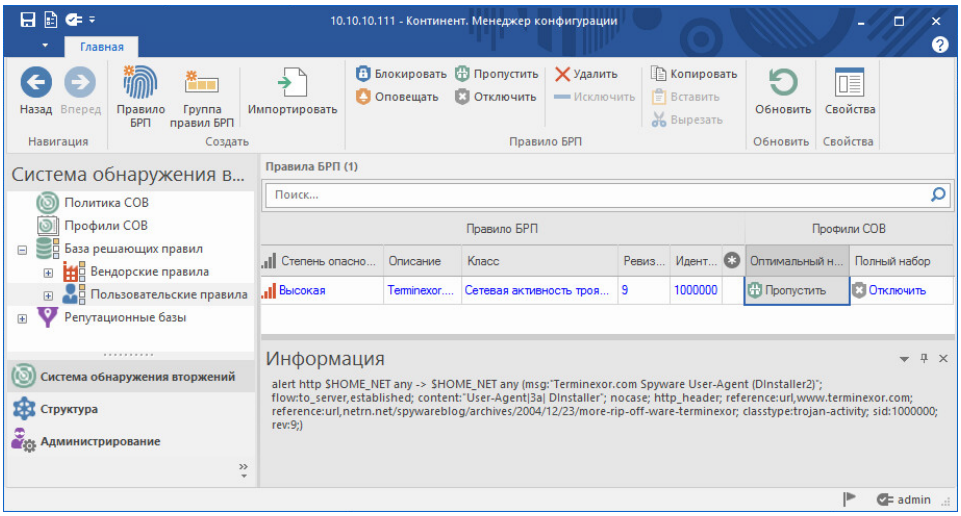
1. На вкладке "Система обнаружения вторжений" перейдите в раздел "База решающих правил", выберите в списке справа нужное правило и нажмите на панели инструментов кнопку "Свойства".
2. Перейдите во вкладку "Параметры" редактируемого правила и внесите изменения в адреса источника и/или приемника.

   К примеру, если необходимо, чтобы вендорское правило, оповещающее об атаке со всего пула адресов источника (HOME_NET), не срабатывало для трафика с IP-адреса 192.168.56.30, то этот IP-адрес следует прописать в поле "Адрес источника".
3. Нажмите кнопку "Применить" и в появившемся окне о сохранении изменений в форме нового пользовательского правила выберите "Да".



Произойдет создание нового пользовательского правила, сохранение его текущих настроек, и на экране окно параметров вендорского правила сменится окном параметров редактируемого пользовательского правила.

4. Нажмите кнопку "ОК".
5. Перейдите в список пользовательских правил и выберите только что созданное новое правило, основанное на вендорском правиле-прототипе.
6. Установите режим "Пропустить" для нужного профиля.



7. Сохраните изменения в конфигурации узла, нажав кнопку в верхнем левом углу Менеджера конфигурации, и установите политику на все подчиненные узлы безопасности (см. стр. **51**).

   В итоге рассматриваемого примера сформированы 2 правила для одной сигнатуры: вендорское правило, оповещающее об атаке, которое работает со всем пулом адресов источника (HOME_NET), и пользовательское правило, игнорирующее (пропускающее) атаку от IP-адреса источника 192.168.56.30.

Управление репутационным IP-фильтром

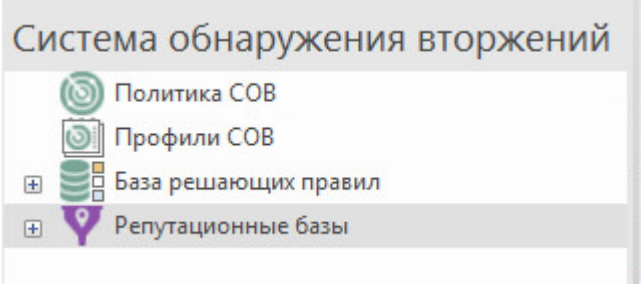
Для создания и применения репутационного IP-фильтра (Reputation IP Filter) необходимо выполнить следующее:

1. Создать новую категорию угроз (см. ниже).
2. Привязать адреса к созданной категории (см. стр. **69**).
3. Создать правило работы фильтра (см. стр. **65**).

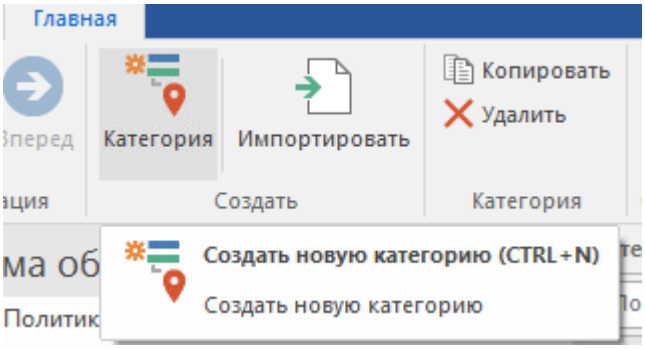
Создание новой категории угроз

Для создания категории:

1. На вкладке "Система обнаружения вторжений" выберите раздел "Репутационные базы".



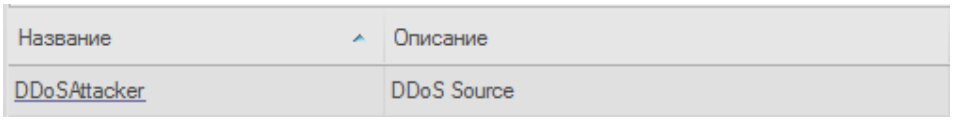
Нажмите на панели инструментов кнопку "Создать новую категорию".



На экране появится окно ввода параметров создаваемой категории.

2. Заполните поля "Название" и "Описание" и нажмите кнопку "ОК".

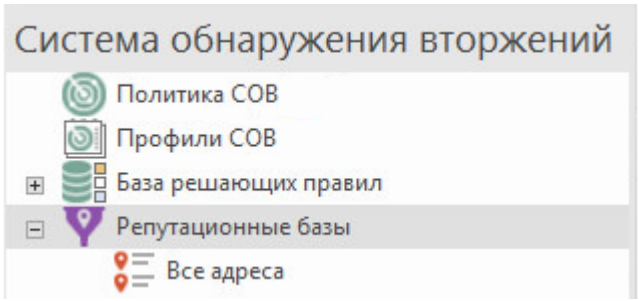
Новая категория отобразится в списке.



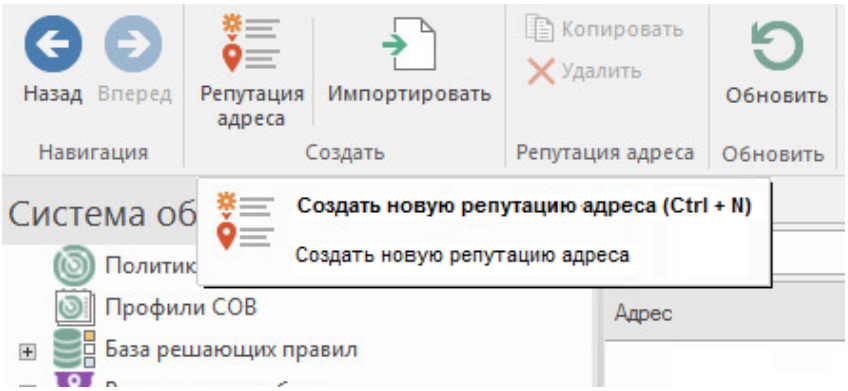
Привязка адреса к категории

Для привязки адреса:

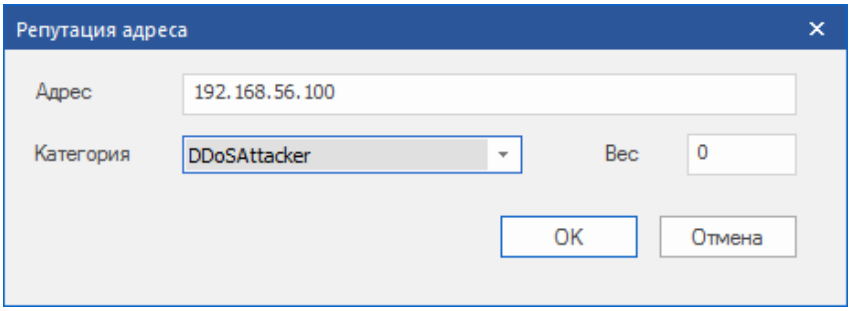
1. На вкладке "Система обнаружения вторжений" раскройте раздел "Репутационные базы" и выберите пункт "Все адреса".



2. Нажмите на панели инструментов кнопку "Создать новую репутацию адреса".

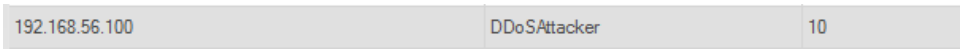


На экране появится окно ввода параметров репутации адреса.



3. Введите IP-адрес, укажите категорию и вес адреса и нажмите кнопку "OK".

   В списке адресов появится введенный адрес с указанием привязки к категории и назначенного веса.



   Если необходимо привязать к данной категории другой адрес, повторите описанную выше процедуру.

Управление иерархической структурой комплекса

Поддержка иерархической структуры доменов комплекса позволяет централизованно распространять сформированные в домене вышестоящего уровня политики СОВ на нижестоящие домены. При этом вместе с политиками передаются также профили с набором решающих правил. Переданные на подчиненные домены политики и профили приобретают статус глобальных.

При распространении политик в нижестоящие домены передаются сведения об учетных записях администраторов. Это дает возможность подключения и управления СОВ нижестоящих доменов. Подключение осуществляется стандартными средствами Менеджера конфигурации. Одновременно с централизованным управлением подчиненными доменами обеспечивается передача данных мониторинга и аудита вверх по иерархии.

Внимание! Вносить изменения в конфигурацию подчиненного домена напрямую нельзя. Для этого необходимо присвоить администратору вышестоящего домена права на управление подчиненным доменом (см. ниже), а затем с помощью Менеджера конфигурации подключиться к ЦУС подчиненного домена и выполнить необходимую настройку.

Иерархическая трехуровневая подчиненная структура строится с помощью связей между доменами вышестоящего и нижестоящего уровней. Такие связи реализуются в виде защищенных каналов, устанавливаемых между ЦУС. При этом связи между доменами одного и того же уровня не предусмотрены.

Построение иерархии доменов

Внимание! Не рекомендуется использовать символы кириллицы для обозначения названия домена.

Формирование иерархической доменной структуры осуществляют средствами Менеджера конфигурации или посредством локального управления ЦУС. При этом установление связей между доменами производится снизу вверх.

Внимание! Для построения иерархической структуры необходимо, чтобы на каждом ЦУС была соответствующая лицензия.

В СОВ реализована поддержка иерархической трехуровневой структуры доменов. Рассмотрим пример реализации иерархии, состоящей из следующих 3 доменов:

- domain_1 — корневой;
- domain_2 — средний;
- domain_3 — нижний.

Для построения трехуровневой структуры доменов:

1. Установите связь между нижним доменом domain_3 и средним доменом domain_2 (см. ниже).

   После того как пройдет процедура согласования: в Менеджере конфигурации подчиненного домена domain_3 статус вышестоящего домена domain_2 станет "Активен"; в Менеджере конфигурации вышестоящего домена domain_2 статус подчиненного домена domain_3 станет "Активен".

2. Установите связь между средним доменом domain_2 и корневым доменом domain_1 (см. ниже).

   После того как пройдет процедура согласования: в Менеджере конфигурации подчиненного домена domain_2 статус корневого домена domain_1 станет "Активен"; в Менеджере конфигурации корневого домена domain_1 статус среднего домена domain_2 станет "Активен", а также появится нижний домен domain_3 со статусом "Активен".

Установление связей между доменами

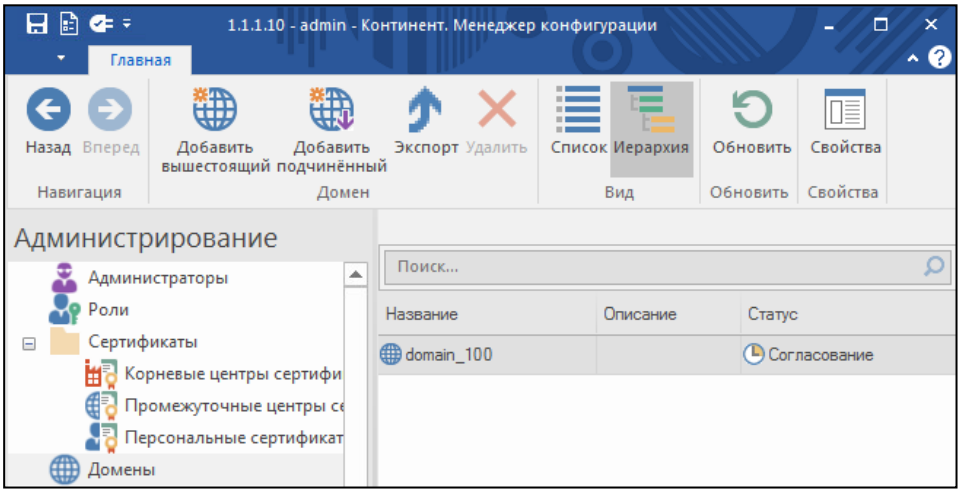
В данном подразделе приведено описание создания связи между двумя доменами с именами **domain_10** и **domain_100**. Предполагается, что связи между доменами не устанавливались и что **domain_100** должен быть подчиненным по отношению к **domain_10**.

Примечание. По умолчанию название домена имеет вид "domain_ID" , где "ID" — это серийный номер ЦУС этого домена.

Для построения иерархии доменов в Менеджере конфигурации:

1. Подключитесь к ЦУС домена, для которого будет устанавливаться связь с вышестоящим доменом. Для этого запустите Менеджер конфигурации, указав IP-адрес ЦУС.
2. В Менеджере конфигурации перейдите в раздел "Администрирование" и выберите папку "Домены".

   В правой части окна отобразится список, содержащий один-единственный домен — **domain_100**.

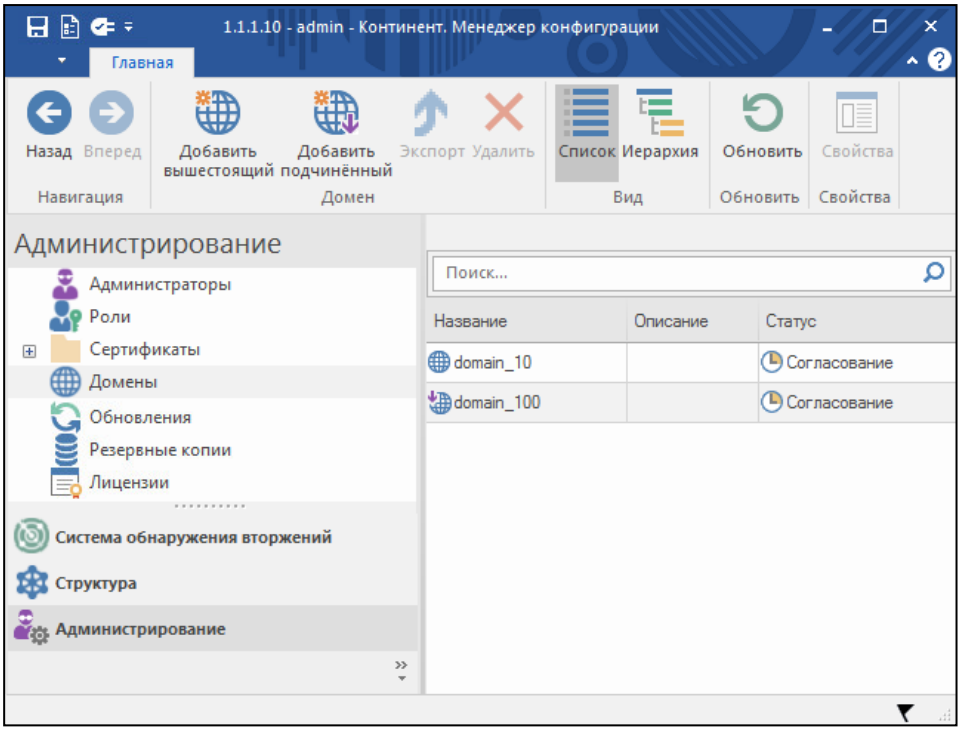


3. Выполните экспорт файла конфигурации домена **domain_100**. Для этого выделите домен в списке и на панели инструментов нажмите кнопку "Экспорт".

   На экране появится стандартное окно сохранения файла.
4. Сохраните файл конфигурации.
5. В Менеджере конфигурации домена **domain_10** выполните импорт конфигурационного файла домена **domain_100**. Для этого в разделе "Администрирование" выберите папку "Домены" и на панели инструментов нажмите кнопку "Добавить подчиненный".

   На экране появится стандартное окно открытия файла.
6. Укажите файл конфигурации домена **domain_100** и нажмите кнопку "Открыть".

   Будет выполнен импорт конфигурационного файла, и в списке доменов появится **domain_100**, отображаемый как подчиненный по отношению к **domain_10**.



7. Сохраните файл конфигурации домена **domain_10** (см. пп. **2-4**).
8. Подключитесь к ЦУС домена **domain_ 100** и выполните импорт конфигурационного файла домена **domain_10**. Для этого в разделе "Администрирование" выберите папку "Домены" и на панели инструментов нажмите кнопку "Добавить вышестоящий".

   На экране появится стандартное окно открытия файла.
9. Укажите файл конфигурации домена **domain_10** и нажмите кнопку "Открыть".

   Будет выполнен импорт конфигурационного файла, и в списке доменов появится вышестоящий домен (**domain_10**). На этом установление связи между доменами будет завершено.

Для построения иерархии доменов из локального меню ЦУС:

1. В главном меню ЦУС, для которого будет устанавливаться связь с вышестоящим доменом, выберите пункт "Настройки" и нажмите клавишу <Enter>.

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

   На экране появится окно "Многоуровневая структура".
3. Вставьте внешний носитель в USB- разъем, выберите пункт "Экспорт конфигурации для вышестоящего ЦУС" и нажмите клавишу <Enter>.

   Начнется запись файла конфигурации домена на внешний носитель. Дождитесь сообщения об успешном завершении операции.
4. Извлеките внешний носитель и нажмите клавишу <Enter>.

   Будет выполнен возврат в окно "Многоуровневая структура".
5. В локальном меню ЦУС, для которого будет устанавливаться связь с подчиненным доменом, перейдите к пункту "Управление многоуровневой структурой" и нажмите клавишу <Enter>.

   На экране появится окно "Многоуровневая структура".
6. Вставьте внешний носитель с файлом конфигурации подчиненного домена (subdomain_idXX.json, где XX — серийный номер подчиненного ЦУС) в USB-

разъем, выберите пункт "Импорт конфигурации с подчиненного ЦУС" и нажмите клавишу <Enter>.

Будет выполнен импорт файла конфигурации нижестоящего домена и экспорт файла конфигурации текущего ЦУС. Дождитесь сообщения об успешном завершении операции.

7. Извлеките внешний носитель и нажмите клавишу <Enter>.

   Будет выполнен возврат в окно "Многоуровневая структура".

8. В локальном меню ЦУС, для которого будет устанавливаться связь с вышестоящим доменом, перейдите к пункту "Управление многоуровневой структурой" и нажмите клавишу <Enter>.

   На экране появится окно "Многоуровневая структура".

9. Вставьте внешний носитель с файлом конфигурации вышестоящего домена (domain_idXX.json, где XX — серийный номер вышестоящего ЦУС) в USB-разъем, выберите пункт "Подключиться к вышестоящему ЦУС" и нажмите клавишу <Enter>.

   Будет выполнен импорт файла конфигурации вышестоящего домена. Дождитесь сообщения об успешном завершении операции.

10. Извлеките внешний носитель и нажмите клавишу <Enter>.

    На этом установление связи между доменами будет завершено.

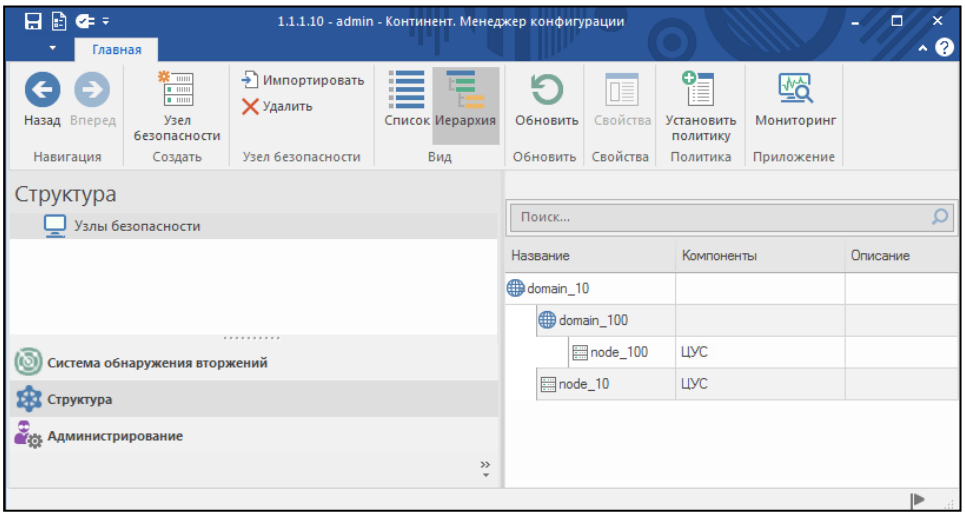
Просмотр структуры доменов

Просмотреть структуру доменов после установления связей можно в разделе "Структура".

Для просмотра структуры доменов:

1. Подключитесь к ЦУС домена **domain_10** и перейдите в раздел "Структура".
2. Нажмите на панели инструментов кнопку "Иерархия".

   В списке отобразится иерархия доменов.



Удаление связей между доменами

При удалении связи между двумя доменами выполняются следующие операции:

- в вышестоящем домене удаляются сведения о нижестоящем домене и поддоменах, а также сведения об их структуре;
- в нижестоящем домене удаляются сведения о вышестоящем домене и глобальные правила, а также сведения об учетной записи администратора вышестоящего домена.

Примечание. В случае выхода из состава комплекса домена среднего уровня сначала необходимо удалить связь между ним и корневым доменом, а затем между ним и подчиненными доменами.

Для удаления связи:

1. В Менеджере конфигурации подключитесь к ЦУС вышестоящего домена, перейдите в раздел "Администрирование" и выберите папку "Домены".

   В правой части окна отобразится домен текущего уровня иерархии и список подчиненных доменов.

2. Выделите в списке подчиненный домен, связь с которым должна быть удалена, и на панели инструментов нажмите кнопку "Удалить".

   На экране появится запрос на подтверждение удаления.

3. Нажмите кнопку "Да" в окне запроса.

   Связь между текущим и подчиненным доменами будет удалена.

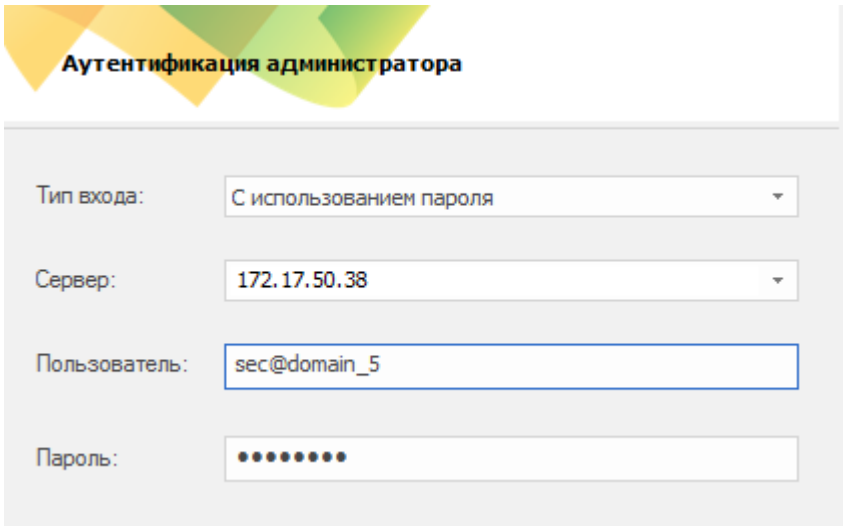
Назначение администраторов для управления нижестоящими доменами

По умолчанию в иерархической структуре доменов права администраторов верхнего уровня не делегируются вниз.

При назначении администратора следует учитывать его способы аутентификации. В случае если для него планируется аутентификация по сертификату, необходимо выполнить следующее:

1. Экспортируйте корневые сертификаты всех вышестоящих доменов (см. стр. **136**).
2. Аналогичным образом экспортируйте персональный сертификат администратора.
3. Установите полученные сертификаты в хранилище Windows, расположенное на локальном компьютере (см. стр. **134**).

Для входа администратора верхнего уровня на нижестоящий домен в Менеджере конфигурации с аутентификацией по логину/паролю в качестве имени пользователя следует указать логин@<домен в котором создан пользователь>.



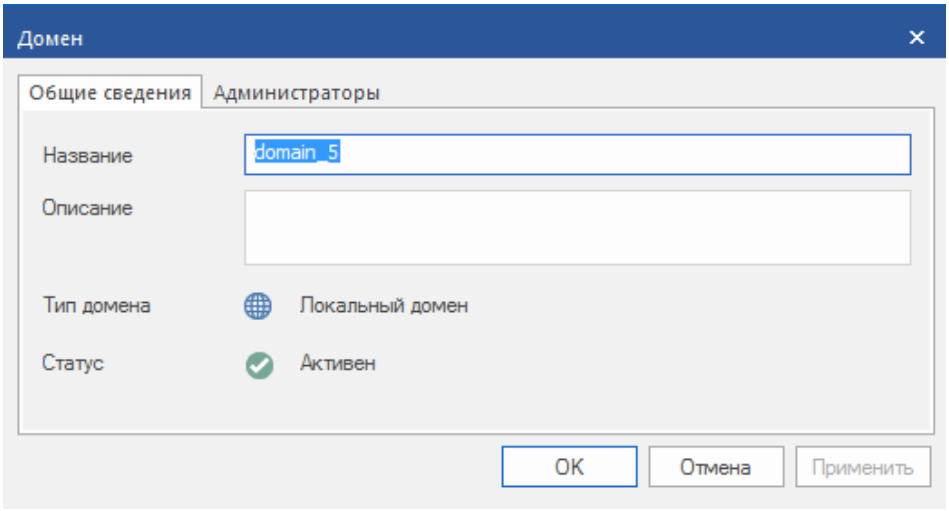
Для назначения администратора верхнего уровня на нижестоящий домен:

1. В Менеджере конфигурации вышестоящего домена перейдите в раздел "Администрирование" и выберите папку "Домены".

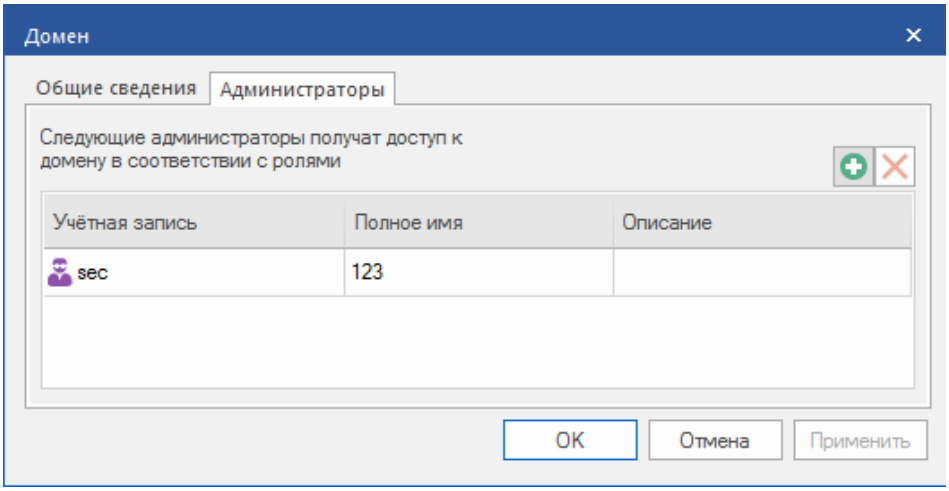
   В центральной части окна отобразится список доменов текущего и нижних уровней иерархии.

2. Выберите нужный нижестоящий домен и на панели инструментов нажмите кнопку "Свойства".

   На экране появится окно "Домен" с описанием его характеристик.



3. Перейдите на вкладку "Администраторы" и добавьте (нажмите кнопку) локального администратора для этого домена.



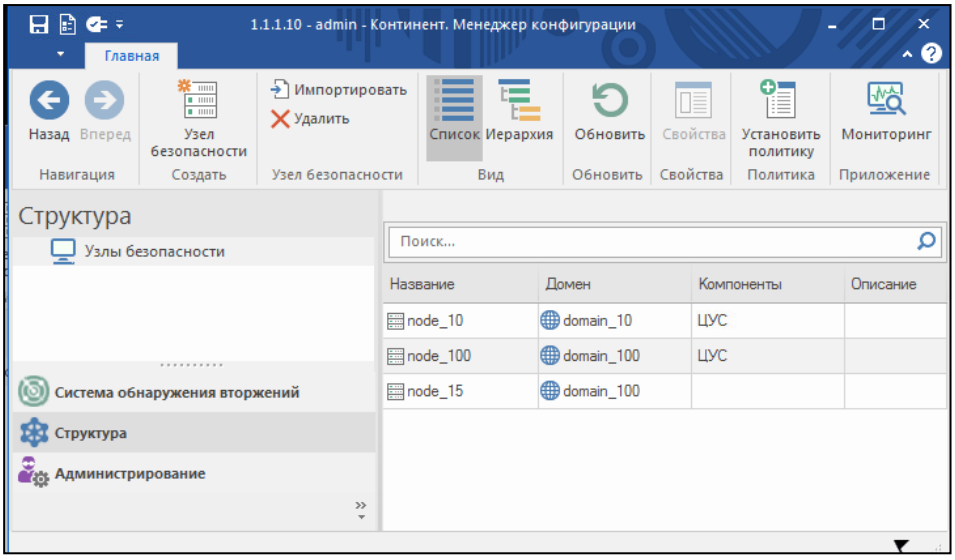
Примечание. При выборе администратора на экране отображается список доступных администраторов, в котором будут присутствовать все пользовательские учетные записи текущего и вышестоящих доменов. Встроенные учетные записи главных администраторов с именем admin будут отсутствовать. В случае отсутствия доступных учетных записей создайте новую (см. стр. 16).

Установка политики в подчиненном домене

Для установки политики в подчиненном домене:

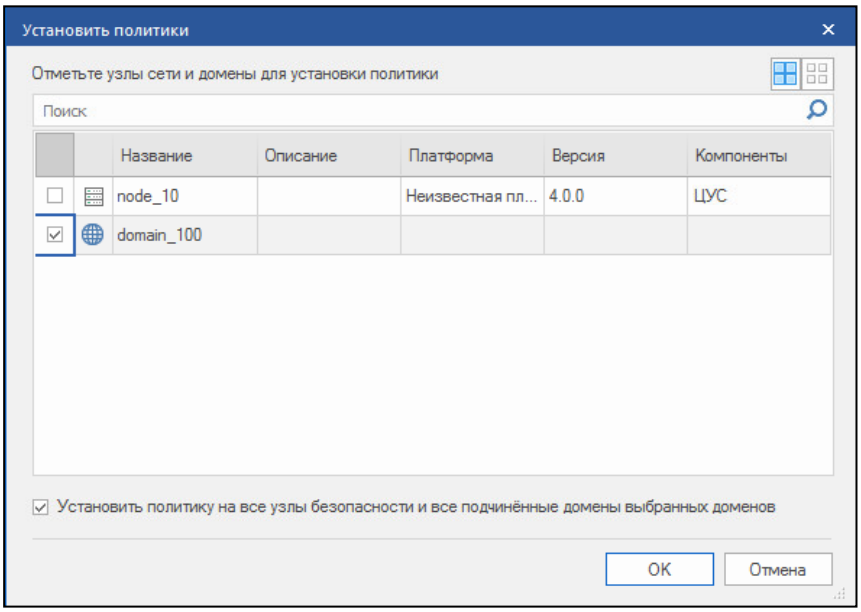
1. В Менеджере конфигурации перейдите в раздел "Структура".

   В центральной части окна отобразится список доменов текущего и нижних уровней иерархии.



2. На панели инструментов нажмите кнопку "Установить политику".

   На экране появится окно "Установить политики".

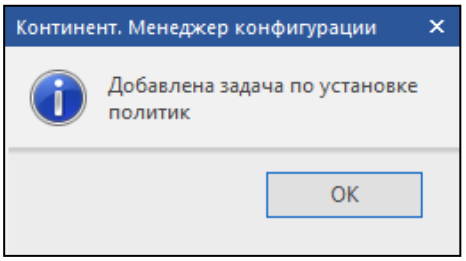


   В окне отображается список узлов текущего домена (**node_10**) и подчиненных доменов (**domain_100**).

3. Установите отметку перед именем домена, в который должна быть передана политика, и нажмите кнопку "ОК".

   Примечание. Для установления политики на все нижестоящие домены и их узлы необходимо перевести флажок "Установить политику на все узлы безопасности и все подчиненные домены выбранных доменов" в активированное положение.

   Начнется передача политик в подчиненный домен (домены), после чего на экране появится сообщение.



4. Закройте окно сообщения.

   Для проверки результатов передачи политик подключитесь с помощью Менеджера конфигурации к ЦУС подчиненного домена и убедитесь, что переданные политики отображаются в разделе "Система обнаружения вторжений".

Мониторинг

Общие сведения

Система мониторинга и аудита Континент (далее — система) — это программное обеспечение, позволяющее проводить мониторинг различных параметров узлов безопасности, входящих в состав комплекса "Континент".

Настройка и подключение системы к Менеджеру конфигурации описано в подразделе "Настройка мониторинга и аудита", [2].

В системе реализован гибкий механизм конфигурирования и оповещения, что позволяет сконфигурировать оповещение для множества настраиваемых событий.

В систему встроены функции отчетности и визуализации данных как в режиме реального времени, так и за выбранный период.

Внимание! Минимально допустимое разрешение экрана для работы с системой — 1024x768.

Объекты мониторинга

Объектами мониторинга домена Континент являются:

- узлы безопасности;
- группы узлов безопасности;
- домены нижнего уровня.

Группы объектов мониторинга

В систему мониторинга сведения о зарегистрированных в домене Континент узлах безопасности и доменах нижнего уровня (поддоменах) поступают от ЦУС.

Изначально в системе мониторинга все узлы и поддомены отображаются как члены группы "Несортированное", входящей в группу корневого домена.

Примечание. Корневая группа домена содержит в себе все узлы и группы. Для нее доступно создание шаблонов, которые действуют на все узлы и группы в структуре. Содержит набор правил по умолчанию. При желании этот набор можно изменить (см. стр. 85).

Пользователь, имеющий права на доступ к странице "Управление группами" системы, может по собственному усмотрению создавать новые группы и помещать в них узлы и поддомены из группы "Несортированное", а также перемещать узлы и поддомены между группами.

Типы и источники отображаемой информации

В системе мониторинга используются следующие типы информации:

- события;
- данные;
- состояние.

Источники для каждого из типов информации приведены ниже в таблице.

Тип информации	Источник
События	Система мониторинга. Система обнаружения вторжений (СОВ). Система аудита
Данные	Сетевые интерфейсы. Система мониторинга. Срабатывание сигнатур
Состояние	Система мониторинга

Тип и источник информации — это параметры, с помощью которых в мониторинге можно настраивать отображение тех или иных сведений о состоянии объектов мониторинга.

Правила и шаблоны

Для того чтобы в системе мониторинга отображались сведения о состоянии того или иного объекта, а также относящиеся к нему события и их описание, необходимо для такого объекта сформировать правило мониторинга.

В мониторинге используются три типа правил:

- общее — распространяется на все узлы и группы узлов;
- групповое — распространяется на все узлы, входящие в группу, и ее подгруппы любого уровня вложенности;
- правило узла — распространяется на соответствующий узел.

Шаблон — правило или несколько правил, описывающих срабатывание сенсоров в системе мониторинга и применяемых к группам узлов и узлам.

Определен приоритет срабатывания по типу правил. Наивысшим приоритетом обладает правило узла, затем следует групповое правило. Общее правило имеет наименьший приоритет.

Статусы объектов

При отображении в мониторинге объекта указывается его статус. Статус может иметь одно из перечисленных ниже в таблице значений.

Статус	Описание
Критический (Critical)	Статус присваивается при наступлении события критического уровня. Объект остается в этом статусе до тех пор, пока состояние параметра, сгенерировавшего событие, не изменится в сторону улучшения, т.е. до тех пор, пока событию не будет присвоено состояние "закрыто"
Предупреждение (Warning)	Статус присваивается при наступлении события, имеющего соответствующий уровень опасности. Объект остается в этом статусе до тех пор, пока состояние параметра, сгенерировавшего событие, не изменится в сторону улучшения или ухудшения, т.е. до тех пор, пока событию не будет присвоено состояние "закрыто" либо статус объекта не изменится на "критический"
Информация (Info)	Статус присваивается при наступлении события информационного уровня. Данный статус сохраняется до изменения состояния параметра

Примечание. Уровень критичности события определяется правилом мониторинга, создавшего это событие (см. стр. **85**).

Для визуализации статуса объекта используются следующие цвета:

- красный — критический;
- оранжевый — предупреждение;
- синий — информация;
- зеленый — отсутствие событий, имеющих перечисленные выше статусы.

Мониторинг в режиме реального времени

В системе мониторинга предусмотрено отображение информации о состоянии узлов и событиях в режиме реального времени. В этом режиме значения параметров обновляются с интервалом 5 секунд.

Режим реального времени доступен при переходе на страницу просмотра состояния узла, а также в панели мониторинга при наличии соответственно настроенного виджета (см. стр. **90**).

Мониторинг иерархической структуры объектов

Система мониторинга поддерживает иерархическую структуру доменов до трех уровней. Информация о состоянии объектов доменов нижнего уровня передается в домен верхнего уровня. Это означает, что при проведении мониторинга домена верхнего уровня администратору доступны сведения о состоянии объектов нижних уровней иерархии. Например, при просмотре структуры домена домен нижнего уровня (поддомен) отображается со статусом "критический". В этом случае администратору достаточно по указанной ссылке перейти на уровень поддомена и в рамках мониторинга получить детальную информацию о состоянии объектов нижнего уровня. Более подробная информация по работе с поддоменами представлена на стр. **106**.

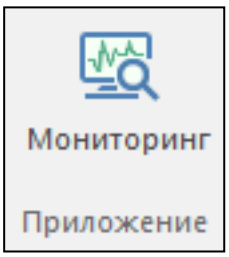
Вход в систему мониторинга

Вход в систему мониторинга выполняют в Менеджере конфигурации или напрямую из интернет-браузера по ссылке https://адрессервера.

Внимание! Система мониторинга корректно работает только при обращении по протоколу https.

Для входа в систему:

1. Откройте Менеджер конфигурации, перейдите в раздел "Структура" и в панели инструментов нажмите кнопку "Мониторинг".



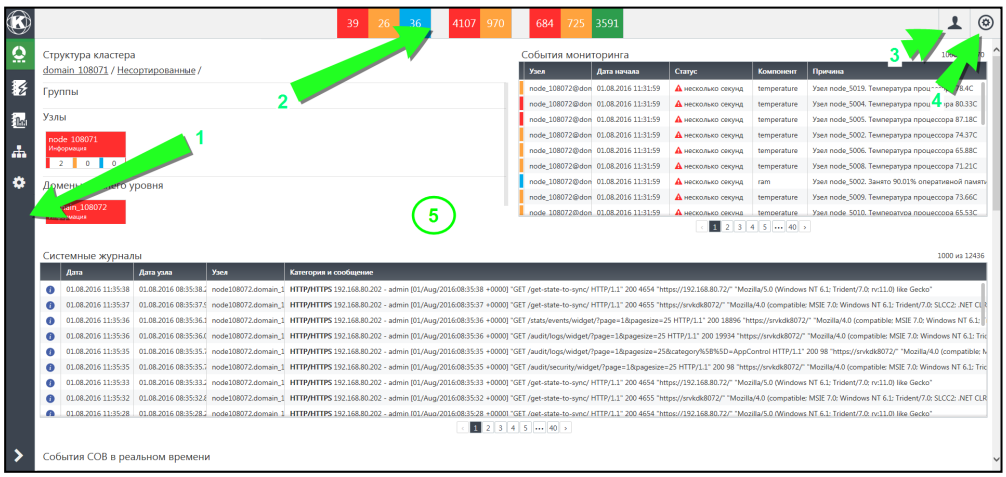
   На экране появится запрос на ввод имени и пароля администратора.

2. Введите имя и пароль администратора и нажмите кнопку "ОК".

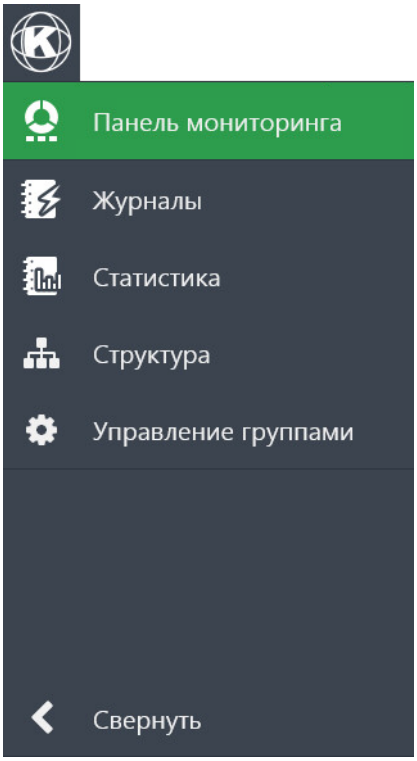
   На экране появится главное окно системы мониторинга.

Главное окно системы мониторинга

Основные элементы главного окна системы мониторинга:



1. Боковая панель навигации, расположенная слева, — служит для перехода между разделами системы.



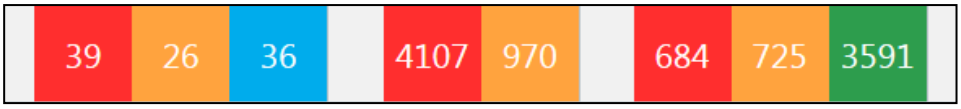
Краткое описание разделов приведено в таблице ниже.

Раздел	Описание
Панель мониторинга	Набор настраиваемых виджетов для отображения информации о состоянии объектов мониторинга. Предусмотрено отображение значений параметров в режиме реального времени
Журналы	Просмотр сообщений журналов системы, аккумулированных со всех узлов контролируемого домена и его поддоменов
Статистика	Формирование и просмотр настраиваемых отчетов, предоставляющих в визуальной форме статистическую информацию за определенный период времени
Структура	Настройка шаблонов групп и узлов. Управление доступом администраторов системы к мониторингу узлов комплекса. Просмотр активных событий на узлах и доменах нижнего уровня. Просмотр сведений о состоянии программных и аппаратных компонентов и сетевых интерфейсов узлов. Просмотр сведений о лицах, ответственных за эксплуатацию групп и узлов
Управление группами	Создание групп и включение в них узлов и поддоменов, зарегистрированных на ЦУС. Перемещение узлов и поддоменов между группами
Свернуть/ Развернуть	Переключение между кратким/полным форматом боковой панели навигации

2. Верхняя панель главного окна системы мониторинга — отображает количество наблюдаемых событий, зарегистрированных на данный момент времени за последние 24 часа.

Примечание 1. Если в течение этих 24 часов были произведены сбросы счетчиков, то будут отображены только события, произошедшие после последнего сброса.

Примечание 2. Отображаются данные счетчиков только тех узлов, к которым есть доступ у текущего пользователя системы.



- Левая часть — события мониторинга. При нажатии на одну из плиток откроется журнал событий мониторинга с установленным фильтром на события соответствующей важности.

  Примечание. Плитка красного цвета отображает количество событий критической важности; оранжевого — события-предупреждения; синего — информационные события.

- Средняя часть — события аудита. При нажатии на одну из плиток откроется журнал аудита с установленным фильтром на события соответствующей важности.

  Примечание. Плитка красного цвета отображает совокупность событий следующей важности: Авария, Тревога, Критическая ошибка, Ошибка; оранжевого цвета — события-предупреждения.

- Правая часть — сообщения СОВ. При нажатии на одну из плиток откроется журнал сообщений СОВ с установленным фильтром на сообщения соответствующей важности.

  Примечание. Плитка красного цвета отображает количество событий высокой важности; оранжевого — средней важности; зеленого — низкой важности.

3. Кнопка вызова настроек пользователя, расположенная в правой части верхней панели.

4. Кнопка вызова меню настроек, расположенная в правой части верхней панели.

   Состав команд меню настроек зависит от выбранного в данный момент раздела системы.

5. Центральная часть — предназначена для отображения информации выбранного раздела и выполнения предусмотренных настроек.

Настройки пользователя

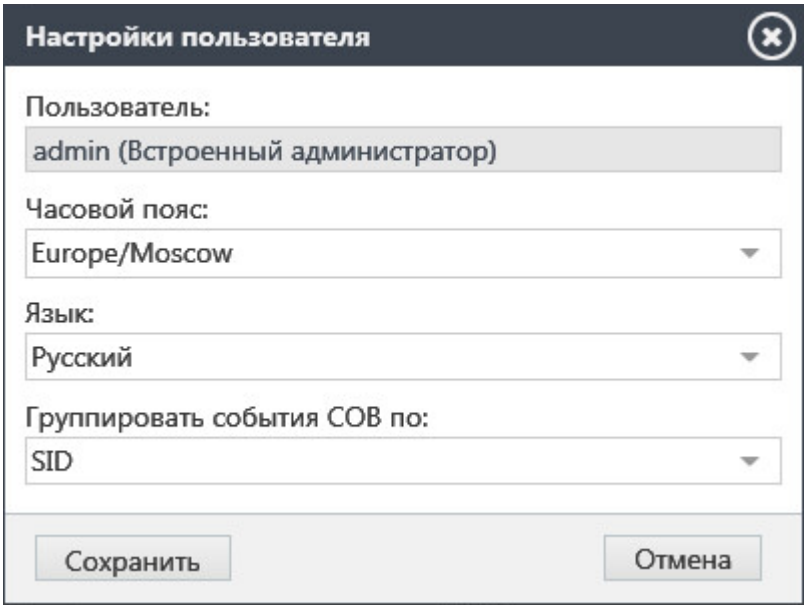
Каждый пользователь системы располагает следующими персональными настройками:

- часовой пояс;
- язык;
- группировка событий СОВ для счетчиков верхней панели.

Для изменения пользовательских настроек:

1. Перейдите в раздел пользовательских настроек, нажав кнопку на верхней панели главного окна системы мониторинга.

   На экране появится окно настроек пользователя.



2. Выберите нужный часовой пояс и язык, после чего нажмите кнопку "Сохранить".

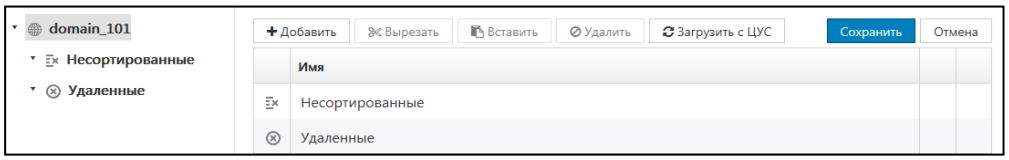
Примечание. В предлагаемом списке часовых поясов города России находятся в подкаталогах Asia и Europe. Также можно воспользоваться подкаталогом Etc с выбором нужного отклонения от GMT.

3. Выберите, по какому критерию будет происходить группировка событий СОВ для счетчиков верхней панели главного окна системы мониторинга.

Примечание. По первоначальным настройкам группировка событий СОВ происходит по идентификатору сигнатуры.

Управление группами

В разделе "Управление группами" можно настроить структуру групп и узлов, отличающуюся от сконфигурированной средствами Менеджера конфигурации на ЦУС.



В центральной части главного окна расположены две панели (левая и правая), в которых отображается структура объектов мониторинга.

Примечание. Изначально, если структура в системе мониторинга не изменялась, в ней представлены две группы: "Несортированное", включающая в себя все зарегистрированные узлы и поддомены, и "Удаленные", в которые будут перемещены все удаленные в Менеджере конфигурации узлы и поддомены.

В верхней части окна расположены кнопки, с помощью которых можно выполнять следующие операции:

- создавать новые группы;
- переименовывать группы;
- удалять группы;
- перемещать группы и их содержимое;
- восстановить структуру, настроенную в ЦУС средствами Менеджера конфигурации.

В верхнем правом углу окна расположены кнопки сохранения и отмены внесенных изменений.

Для создания новой группы:

1. В левой панели выберите родительскую группу (корневой домен или любую группу, кроме "Несортированные" и "Удаленные") и нажмите кнопку "Добавить".

   Группа появится на обеих панелях, получив название "Группа_X", где X — ее порядковый номер.
2. Для сохранения изменений нажмите кнопку "Сохранить", расположенную в верхнем правом углу панели.

Для переименования группы:

1. Для изменения названия группы нажмите на правой панели соответствующую кнопку .

   Появится поле для ввода названия группы.
2. Замените название группы и нажмите кнопку "Сохранить".

Для перемещения группы:

1. Выберите родительскую группу на левой панели.
2. На правой панели перетащите нужную группу на левую панель в новую родительскую группу.
3. Для сохранения изменений нажмите кнопку "Сохранить".

Для удаления группы:

1. Для удаления группы нажмите на правой панели соответствующую кнопку .
2. Нажмите кнопку "Сохранить".

Для включения узла или поддомена в группу:

1. Выделите объект и перетащите его на соседнюю панель в нужную группу.
2. Для сохранения изменений нажмите кнопку "Сохранить".

Для восстановления изначальной структуры корневого каталога:

1. Для восстановления структуры, настроенной в ЦУС средствами Менеджера конфигурации, нажмите на правой панели кнопку "Загрузить с ЦУС" .

   Появится окно подтверждения перезагрузки.
2. Нажмите кнопку "Да", а затем "Сохранить".

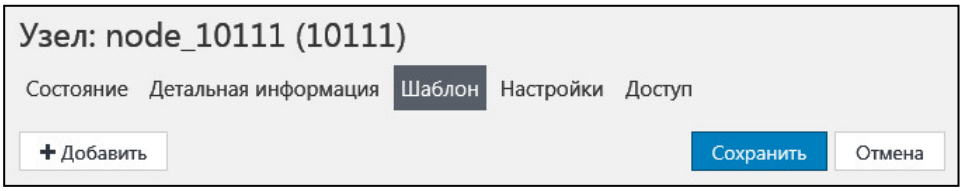
Настройка шаблонов мониторинга

Формирование общих правил и настройка шаблонов мониторинга для групп и узлов осуществляются в разделе "Структура".

Для настройки шаблона:

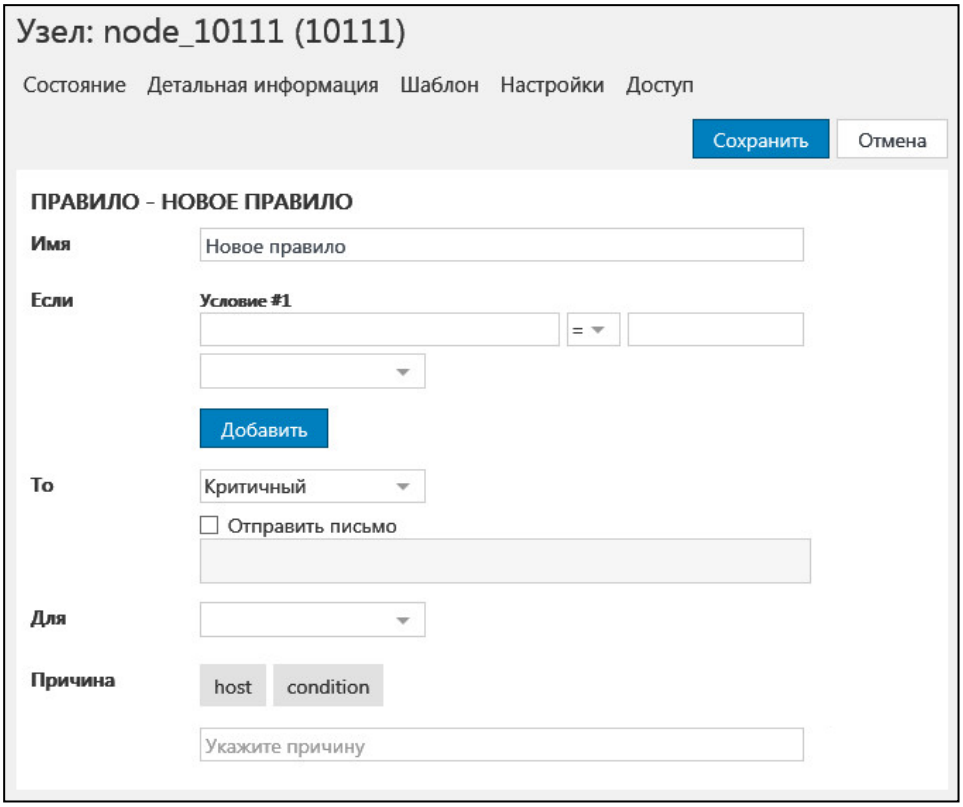
1. Перейдите в раздел "Структура" и выберите в дереве объектов нужную группу или узел.

   В окне отобразится страница с параметрами выбранного объекта.
2. Перейдите на вкладку "Шаблон".



3. Каждое правило в шаблоне можно отредактировать или удалить. Для этого нажмите на соответствующую иконку, расположенную слева от правила. Для добавления правила в шаблон нажмите кнопку "Добавить".

   При добавлении или редактировании правила на экране появится окно его настройки.



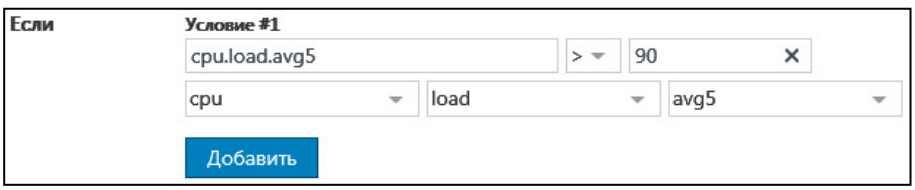
4. Укажите имя правила и условие его срабатывания. Для этого:
   - В поле "Имя" введите имя правила. Допускается использование следующих символов:
     - прописные и строчные буквы латинского алфавита A— Z, a — z;
     - прописные и строчные буквы кириллицы А — Я, а — я;
     - цифры 0 — 9;
     - следующие символы:

(	)	[	]	_	-	*	?	!	%

   - В группе полей "Если" укажите параметр системы мониторинга, логическое условие и порог срабатывания.

     Примечание. Для ввода параметра системы мониторинга можно использовать нижние поля этой группы для выбора нужных составляющих из списка возможных.

     Например, для условия "Когда средняя загрузка ЦП за 5 минут больше 90%" настройка будет выглядеть так:



   Условий срабатывания правила может быть несколько. Для добавления дополнительного условия нажмите кнопку "Добавить".

Примечание. При добавлении нескольких условий можно выбрать вариант срабатывания — при выполнении всех условий или при выполнении одного из условий. Соответствующее поле появится над списком условий при добавлении второго условия.

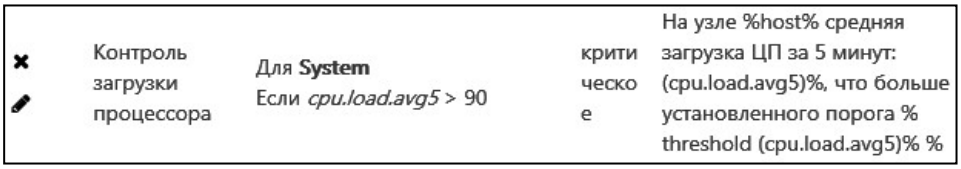
5. Укажите значения параметров.

Параметр	Описание
То	Действие, выполняемое при срабатывании правила. Настраивается критичность события, генерируемого срабатыванием правила, а также рассылка оповещений
Для	Категория сенсора, отвечающего за срабатывание правила
Причина	Сообщение, описывающее событие. В теле сообщения допускается использование макросов, позволяющих более точно формировать сообщение. Поддерживаются следующие макросы для каждого из условий: • %host% — узел, где произошло событие; • %value% — текущее значение параметра; • %condition% — текстовое значение условия (например, "›" — больше); • %threshold% — порог срабатывания. В тексте сообщения допускается использование символов, приведенных в п. **4**

Пример сообщения: "На узле %host% средняя загрузка ЦП за 5 минут: %value (cpu/load/avg5)%, что больше установленного порога в %threshold (cpu/load/avg5)% %".

6. После настройки правила нажмите кнопку "Сохранить".

Сохраненное правило появится в списке правил соответствующей группы или узла.



Для формирования общих правил:

1. Перейдите в раздел "Структура" и выделите в дереве объектов верхний уровень иерархии (текущий домен).

   На экране появится список общих правил. По умолчанию в системе есть набор предустановленных общих правил.

2. Для добавления в список нового правила нажмите кнопку "Добавить".

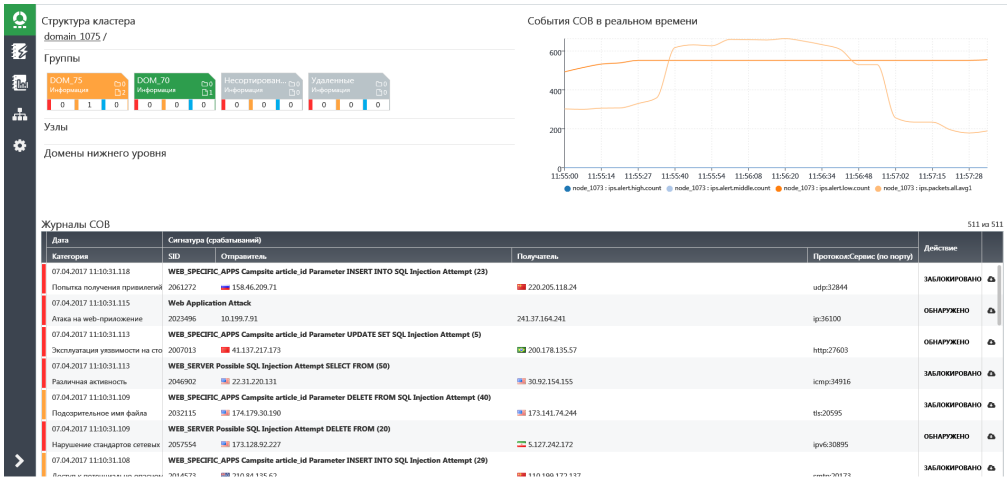
   На экране появится окно настройки правила.

3. Выполните настройку правила (см. выше процедуру настройки шаблона) и сохраните его.

   При необходимости добавьте в список следующее правило.

Панель мониторинга

Панель мониторинга представляет собой набор виджетов. Виджет — конструктивный элемент панели, отвечающий за визуальный вывод части информации, собранной системой.



Максимально допустимое количество виджетов, используемых для отображения в панели мониторинга, — 12.

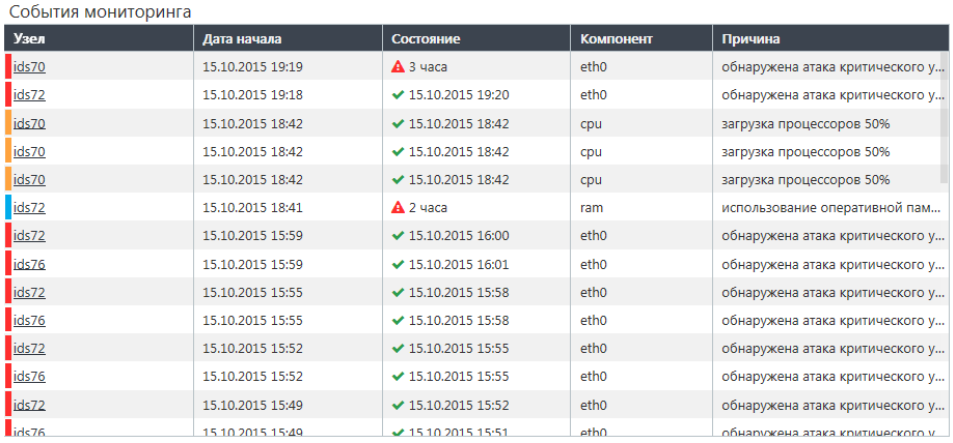
В системе используются виджеты следующих типов:

- табличный;
- графический;
- структура.

Внимание! При сбое виджетов графического типа (некорректное отображение, деформация и пр.) необходимо перезагрузить страницу в браузере (нажать клавишу <F5>).

Табличный виджет

Табличный виджет представляет собой таблицу с данными.

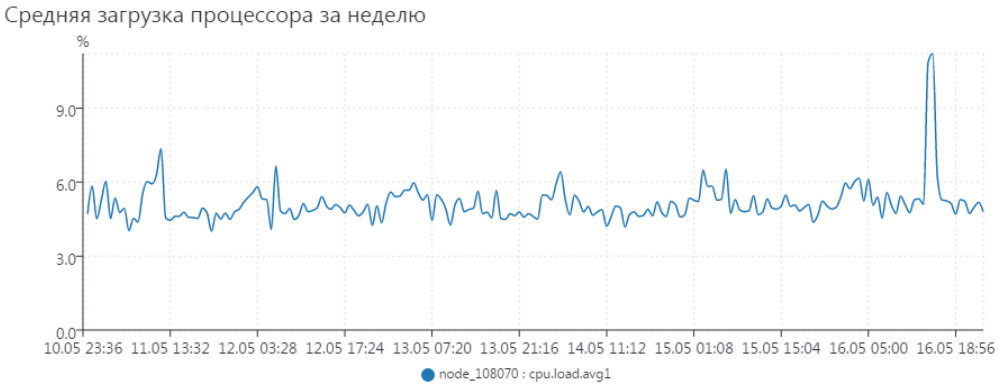


Тип информации виджета выбирается при его настройке и может быть событиями или данными. Источником информации может служить:

- система мониторинга;
- система обнаружения вторжений;
- система журналирования (аудита);
- сетевые интерфейсы.

Графический виджет

Графический виджет представляет собой график или круговую диаграмму.



Источником информации для виджета являются данные системы мониторинга.

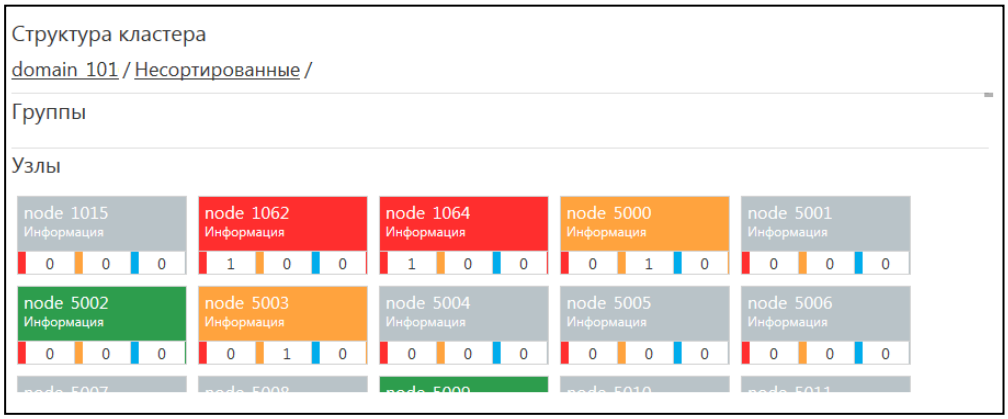
Структура

Виджет типа "Структура" отображает структуру объектов мониторинга домена в виде следующих разделов:

- группы — перечень всех сформированных групп в домене;
- узлы — перечень узлов выбранной группы;
- домены нижнего уровня — перечень подчиненных доменов.

Отображение того или иного раздела задается при настройке виджета.

В каждом разделе входящие в него объекты представлены в виде плитки с указанием имени объекта и количества зарегистрированных событий того или иного уровня критичности. Цвет плитки указывает на максимальный уровень критичности события, произошедшего на данном объекте или на одном из объектов группы.



Нажатие на плитку группы позволяет просмотреть структуру соответствующей группы: вложенные группы и узлы. Для возврата на более высокие уровни в структуре следует воспользоваться строкой навигации вверху виджета.

Нажатие на плитку узла осуществляет переход на страницу узла в раздел "Структура".

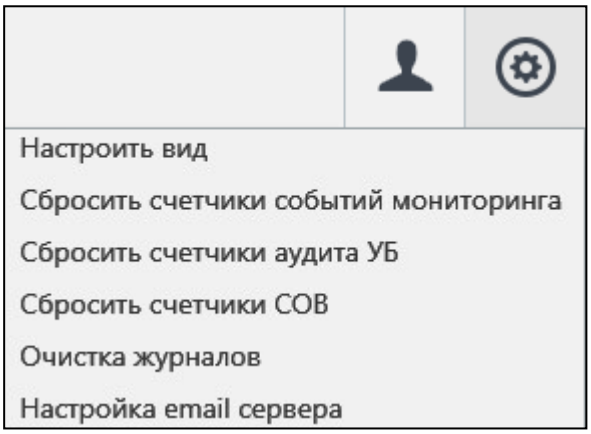
Настройка панели мониторинга

Настройка панели включает в себя:

- добавление новых виджетов на панель;
- удаление виджетов с панели;
- редактирование виджетов;
- перемещение виджета в пределах панели и изменение его размера.

Для настройки панели мониторинга:

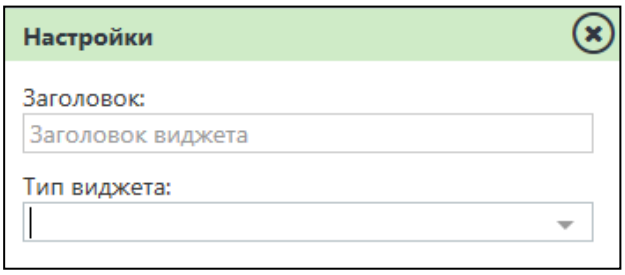
1. Откройте панель мониторинга.
2. Нажмите кнопку вызова меню настроек, расположенную в правом верхнем углу, и в раскрывшемся списке выберите пункт "Настроить вид".



   Панель мониторинга перейдет в режим редактирования.
3. Для добавления на панель нового виджета нажмите на плитку "Добавить виджет".

   На панели появится "пустой" виджет.
4. Для настройки виджета нажмите кнопку  , расположенную в правом верхнем углу виджета.

   В правой части главного окна появится панель настроек виджета.



5. Введите заголовок виджета и выберите тип: таблица, график или структура.

   В панели настроек появится поле для задания следующего параметра. Последующие этапы настройки параметров зависят от выбранных типов виджета и текущего параметра.

   В настройках параметров могут использоваться фильтры по группам и узлам.

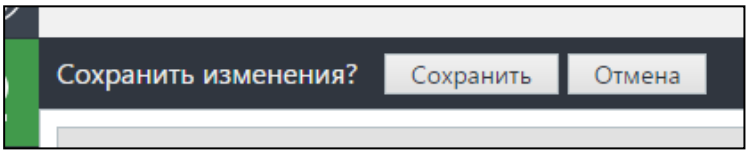
Примечание. Задействованные для виджетов "Таблица. Данные. Мониторинг", "Таблица. Данные. Срабатывание сигнатур СОВ/СОА", "Таблица. Данные. Сетевые интерфейсы", "График. Данные. Мониторинг" узлы системы переводятся в режим реального времени. Если в фильтре для виджета указана группа, то все узлы в этой группе и ее подгруппах переводятся в режим реального времени.

Совет. Не рекомендуется переводить в режим реального времени более 20 узлов в системе, поскольку этот режим является достаточно ресурсоемким и желательно ограничить его использование.

6. Настройте параметры виджета и нажмите кнопку "Применить", расположенную в нижней части панели настройки.

   Виджет отобразит значения заданных параметров.

7. Для изменения размера виджета используйте указатель, расположенный в его нижнем правом углу.
8. Для добавления следующего виджета повторите пп. **3–6**.
9. Для удаления виджета нажмите кнопку  , расположенную в правом верхнем углу виджета.
10. Для перемещения виджета выделите его заголовок и перетащите на свободное место панели.
11. Для изменения параметров виджета нажмите кнопку редактирования, расположенную в его верхнем правом углу, и в открывающейся панели настроек укажите нужные значения параметров (см. пп. **5**,**6**).
12. Для завершения настройки нажмите кнопку "Сохранить", расположенную в верхней части панели мониторинга.



Журналы

В журналах регистрируются события, связанные с работой всех узлов домена, а также с его поддоменов и входящих в них узлов, и передаются на ЦУС.

В системе используются журналы следующих типов:

- Аудит.
- События мониторинга.
- События СОВ.

Каждый журнал обладает возможностью поиска или фильтрации сообщений.

Для осуществления фильтрации:

1. Выберите нужный тип журнала в качестве источника в центральной части главного окна раздела "Журналы".
2. При необходимости выберите классификатор. Для журналов аудита в роли классификатора выступает категория сообщения, для журналов событий СОВ — класс атаки, для журнала мониторинга — состояние события мониторинга.
3. Введите условие запроса фильтрации, используя специализированные теги, расположенные под полем запроса. Завершить ввод условия необходимо клавишей <Enter>.

   Примечание. Нажатие на заголовок столбца в таблице результатов фильтрации в случае совпадения его содержания с одним из тегов также приводит к формированию нового условия фильтрации по этому тегу.

   Совет. Некоторые теги сопровождаются подтегом "точно". Для более общей фильтрации допустимо убрать подтег и часть содержания тега.

4. Для добавления в фильтр дополнительного условия выберите нужную логическую операцию в тегах запроса и повторите п. **4**.

   Примечание. Условия запроса без логических связок между собой будут интерпретироваться обработчиком как теги с союзом ИЛИ.

5. При необходимости уточните временной диапазон запроса.
6. Нажмите кнопку "Применить".

Пример фильтрации:

порт_отправителя: [1000 по 60000]	выборка по диапазону портов отправителя сообщения от 1000 до 60000
страна_получателя: "RU" категория.точно: "Потенциально опасный трафик"	выборка по стране получателя - Россия или категории потенциально опасного трафика
категория: "трафик"	выборка по категориям событий, содержащим слово "трафик"

Для навигации по результатам фильтрации используются кнопки перехода по страницам в центральной части окна журнала. Количество показываемых в окне записей определяется параметром "Результатов на странице" в правой части окна.

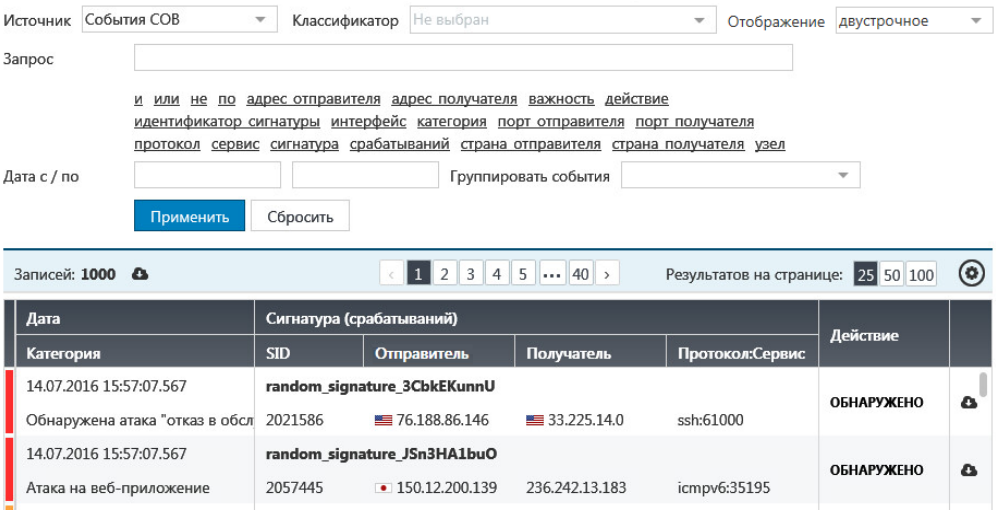
Для выбора отображаемых параметров событий в выбранном журнале требуется нажать кнопку и отметить нужные опции.

При необходимости работы сразу с несколькими вариантами фильтрации или разными журналами необходимо нажать кнопку формирования нового запроса в верхней части экрана +. Параметры запроса сохраняются после каждого нажатия кнопки "Применить". При авторизации оператора системы и переходе в раздел "Журналы" ему будут показаны его последние запросы с сохраненными параметрами фильтрации. Для удаления запроса требуется нажать соответствующую кнопку ✖.

Совет. Для удобства использования целесообразно присвоить созданным запросам идентификационные имена . Для этого выполните двойной щелчок левой кнопкой мыши по имени запроса с автоматически присвоенным порядковым номером, введите нужное имя и нажмите клавишу <Enter>.

События СОВ

Журнал содержит события СОВ, аккумулированные со всех узлов домена, контролируемого текущим ЦУС, а также с его поддоменов и входящих в них узлов.



Данный журнал имеет две формы отображения: двустрочную и однострочную.

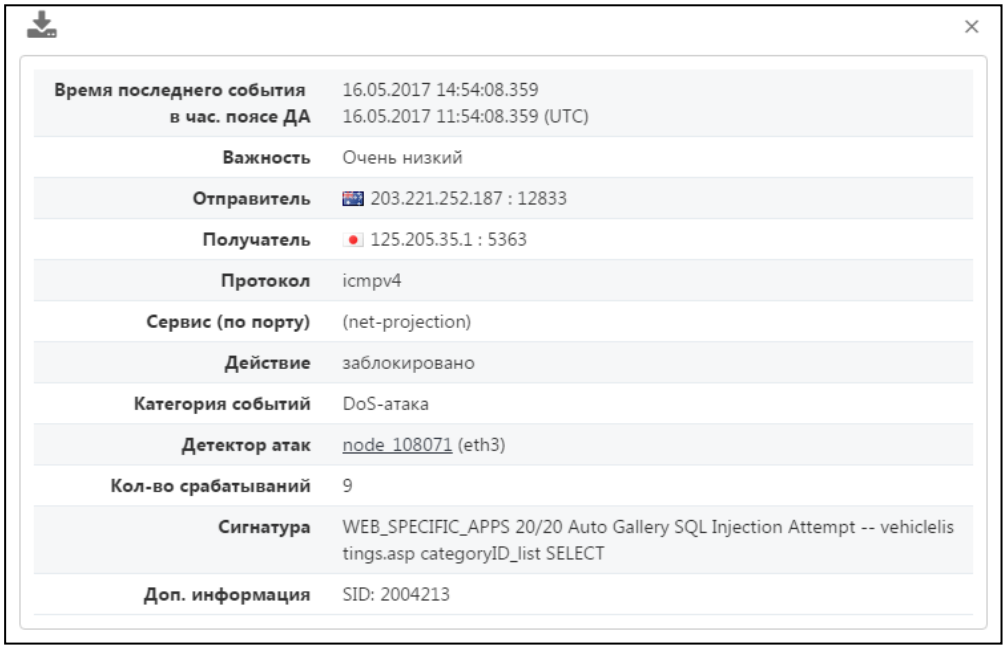
Для смены формы отображения:

1. Выберите нужную форму из раскрывающегося списка в верхнем правом углу экрана.
2. Нажмите кнопку "Применить" в центральной части экрана.

В отображаемых в соответствии с параметрами запроса фильтрации записях журнала содержится следующая информация:

- Важность сообщения — информация об уровне важности события, показываемая соответствующим цветом.
- Дата — дата и время сообщения, представленные во временной зоне ЦУС.
- Категория — категория произошедшего события.
- Сигнатура — сигнатура сообщения, полученного с узла безопасности.
- SID — идентификатор безопасности.
- Отправитель — IP-адрес источника атаки, дополненный флагом страны, к которой относится этот IP-адрес.
- Получатель — IP-адрес цели атаки, дополненный флагом страны, к которой относится этот IP-адрес.
- Протокол — протокол, по которому получено сообщение.
- Сервис — тип протокольной службы.
- Действие — реакция на событие относительно передаваемого трафика: Обнаружено/Заблокировано.

При нажатии на каком-либо событии СОВ открывается окно с полной информацией о событии, содержащей дополнительные данные:



- Детектор атак— узел безопасности, на котором сгенерировано сообщение.
- Отправитель — IP-адрес и порт источника атаки.
- Получатель — порт и IP-адрес, на который производилась атака.

Для просмотра полного текста сообщения о событии в формате *pcap* необходимо нажать кнопку в главном окне журнала либо кнопку в окне с полной информацией о событии.

Для удобства просмотра сообщений в Журнале СОВ есть возможность их группировки по одному из параметров. При этом в главном окне будет показано только последнее сообщение из каждой группы, причем после описания сигнатуры в скобках отобразится количество сообщений в группе. При просмотре полной информации о сообщении эти данные можно увидеть в параметре "Количество срабатываний". Полная информация также содержит время первого и последнего события группы, представленное во временной зоне ДА, на котором сгенерировано сообщение.

Сортировка записей сгруппированных событий в главном окне журнала происходит по количеству срабатываний в сторону их убывания. В результате группировки событий выводится максимум 1000 записей.

Для фильтрации записей используют следующие теги:

- адрес отправителя:[IP-адрес] — выборка событий, сгенерированных атакой с определенного адреса;
- адрес получателя:[IP-адрес] — выборка событий, сгенерированных атакой на определенный адрес;
- важность:[уровень] — выборка событий определенного уровня важности;
- действие:[Обнаружено/Заблокировано] — выборка событий с определенным типом реакции на передаваемый трафик;
- идентификатор сигнатуры:[SID] — выборка событий, сгенерированных срабатыванием сигнатуры с определенным идентификатором;
- интерфейс:[текст] — выборка событий, сгенерированных атакой на определенный интерфейс;
- категория:[текст] — выборка записей, содержащих в поле "Категория" определенный текст;
- порт отправителя:[номер порта] — выборка событий, сгенерированных атакой с определенного порта;
- порт получателя:[номер порта] — выборка событий, сгенерированных атакой на определенный порт;
- протокол:[TCP/UDP] — выборка событий, сгенерированных атакой по определенному протоколу;
- сервис:[текст] — выборка записей, содержащих в поле "Сервис" определенный текст;
- сигнатура:[текст] — выборка записей, содержащих в поле "Сигнатура" определенный текст;
- срабатываний:[число] — выборка групп с определенным числом событий;
- страна отправителя:[код страны] — выборка событий, сгенерированных атаками от IP-адресов определенной страны;
- страна получателя:[код страны] — выборка событий, сгенерированных атаками на IP-адреса определенной страны;
- узел:[имя узла] — выборка записей с определенного узла;

Например, необходимо найти атаки, которые происходили с узла 1.1.1.1 на узел 2.2.2.2 и интерфейс Ethernet0. Для этого следует ввести в строке запроса:

адрес отправителя:1.1.1.1 и адрес получателя:2.2.2.2 и интерфейс:eth0

и нажать кнопку "Применить".

Журнал аудита

Журнал аудита ЦУС представляет собой сообщения о зарегистрированных событиях, аккумулированные со всех узлов домена, контролируемого текущим ЦУС, а также с его поддоменов и входящих в них узлов.

В журнале аудита содержится следующая информация:

- Важность сообщения — информация об уровне важности сообщения, показываемая соответствующей графической иконкой.

Важность сообщения		**Важность сообщения**	
Иконка	**Уровень**	**Иконка**	**Уровень**
	Авария		Тревога
	Критическая ошибка		Ошибка
	Предупреждение		Оповещение
	Информация		Отладка

- Дата — дата и время сообщения, представленные во временной зоне, выбранной оператором системы мониторинга (см. стр. **83**).

- Дата узла — дата и время сообщения, представленные во временной зоне узла безопасности, на котором сгенерировано сообщение.
- Узел — узел безопасности, на котором сгенерировано сообщение.
- Категория событий и сообщение(срабатываний) — категория события, текст сообщения и количество срабатываний.

Для фильтрации записей используют следующие теги:

- важность:[уровень] — выборка сообщений определенного уровня важности;
- категория:[текст] — выборка записей, содержащих в поле "Категория" определенный текст;
- сообщение:[текст] — выборка записей, содержащих в поле "Сообщение" определенный текст;
- срабатываний:[число] — выборка групп с определенным числом событий;
- узел:[имя узла] — выборка сообщений с определенного узла;
- хост:[имя хоста] — выборка сообщений с определенного хоста.

Примечание. Имя хоста образуется из сложения имен узла и домена через разделитель ".".

События мониторинга

Журнал содержит сообщения событий системы мониторинга, аккумулированные со всех узлов домена, контролируемого текущим ЦУС, а также со всех его поддоменов и входящих в них узлов.

В журнале содержится следующая информация:

- Важность сообщения — информация об уровне важности события.
- Узел — узел безопасности, на котором сгенерировано событие.
- Дата начала — дата и время начала события, представленные во временной зоне, выбранной оператором системы мониторинга (см. стр. **83**).
- Состояние — параметр может принимать два значения:
  -  : показывает, что событие еще актуально, при этом дополнительно показывается продолжительность события;
  -  : показывает, что событие уже неактуально, при этом дополнительно показываются дата и время завершения события.
- Компонент — параметр узла безопасности, по которому сгенерировано событие.
- Причина — текст сообщения, соответствующего событию.

Для поиска нужных событий можно использовать фильтр, который настраивается по следующим параметрам:

- важность:[уровень] — выборка событий определенного уровня важности;
- компонент:[тип] — события, относящиеся к указанному параметру узла безопасности;
- причина:[текст] — события, имеющие указанный фрагмент текста в своем описании;
- продолжительность:[число] — события, имеющие указанную длительность в секундах;
- состояние:[Активно/Завершено] — события, соответствующие указанному состоянию;
- узел:[текст] — события, относящиеся только к указанному узлу.

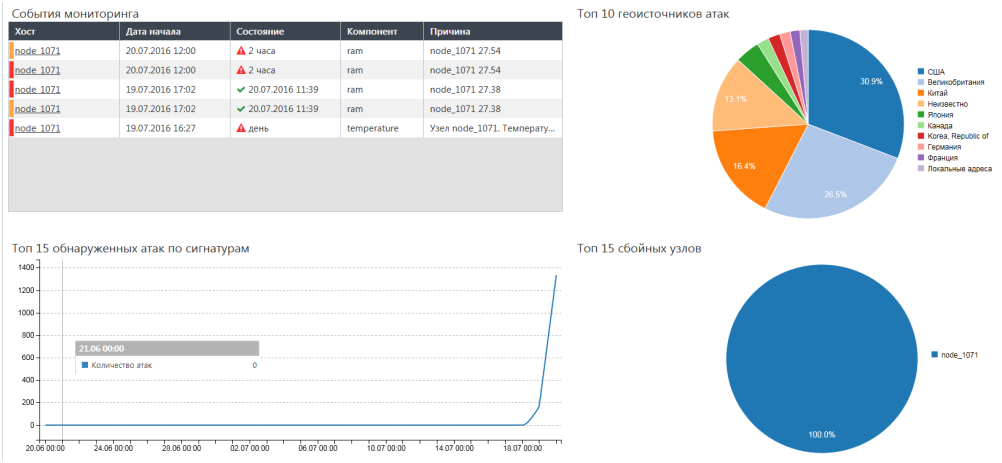
Статистика

Раздел "Статистика" предназначен для формирования и просмотра настраиваемых отчетов, предоставляющих в визуальной форме статистическую информацию за определенный период времени.

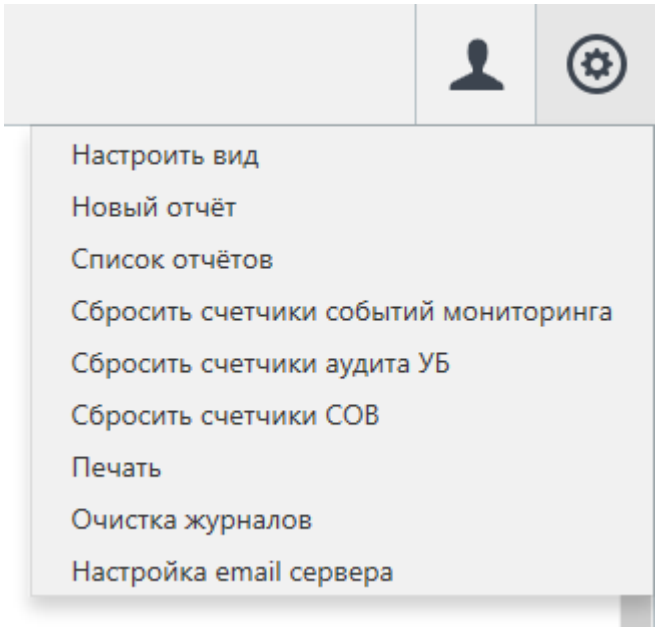
Каждый отчет представляет собой набор виджетов табличного и/или графического типа.

При переходе в раздел "Статистика" в центральной части главного окна отобразится последний из сформированных отчетов. Если отчеты не формировались, в главном окне отобразится отчет, настроенный по умолчанию.

Внимание! На экране виджеты, входящие в состав отчета, отображаются в режиме предварительного просмотра. В связи с этим табличные виджеты событий в таком режиме содержат 1000 последних записей (распределенных на 40 страниц по 25 строк) с указанием их общего количества.



В правом верхнем углу экрана расположена кнопка вызова меню настроек.



Настройка	Описание
Настроить вид	Настройка включает в себя: • добавление новых виджетов в отчет; • удаление виджетов из отчета; • редактирование виджетов; • перемещение виджета в пределах отчета
Новый отчет	Создание нового отчета
Список отчетов	Вывод на экран списка созданных отчетов
Сбросить счетчики событий мониторинга	Сброс счетчиков событий мониторинга
Сбросить счетчики аудита УБ	Сброс счетчиков аудита УБ
Сбросить счетчики СОВ	Сброс счетчиков СОВ
Печать	Вывод на печать текущего отчета
Очистка журналов	Полная или частичная очистка журналов системы
Настройка email сервера	Настройка email сервера

Внимание! Список отчетов не может быть пустым. Если в списке только 1 отчет, его удалить нельзя.

Для виджетов Таблица.Данные.Мониторинг и График.Данные.Мониторинг, с помощью которых можно просмотреть информацию по параметрам узла или группы узлов (загрузка ЦП, ОЗУ и т.д.) за определенный период времени, внедрена функция автоматического прореживания накопленной статистики со следующими параметрами:

Время появления информации	Процент сохраненной информации, %
Последние сутки	100
1–3 дня назад	80
3–7 дней назад	65
7–14 дней назад	50
14 дней–1 месяц назад	35
1–6 месяцев назад	15
6–12 месяцев назад	5
Больше года назад	0

При этом в журнале аудита появляются сообщения следующего характера:

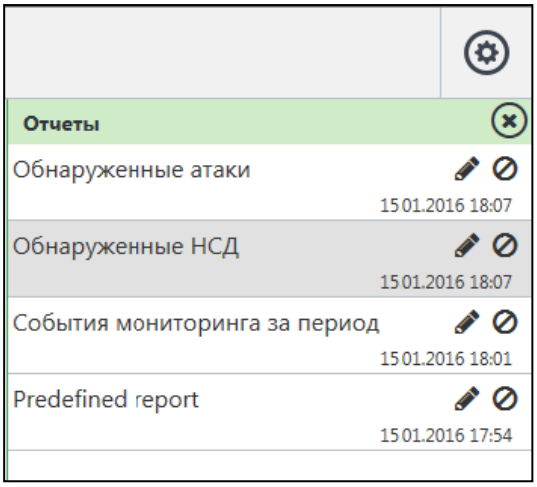
- Аудит: Итоги прореживания статистики мониторинга: удалено 26 из 5249 записей.
- Аудит: Прореживание статистики мониторинга успешно выполнено.

Просмотр отчетов

Для просмотра отчета:

1. Нажмите кнопку вызова меню настроек и в открывшемся меню выберите пункт "Список отчетов".

   В правой части главного окна появится список сформированных отчетов, упорядоченный по времени создания.



Примечание. Если отчеты не создавались, в списке будет один отчет, настроенный по умолчанию.

2. Выберите в списке нужный отчет.

   Отчет отобразится в центральной части главного окна.
3. Для просмотра другого отчета выберите его в списке.
4. При необходимости закройте список отчетов.

Создание и настройка нового отчета

Для создания нового отчета:

1. Нажмите кнопку вызова меню настроек и в открывшемся меню выберите пункт "Новый отчет".

   Содержание центральной части главного окна будет очищено, и в списке отчетов появится название нового отчета, сгенерированное автоматически.
2. Введите в списке осмысленное название нового отчета. Для этого используйте значок редактирования , расположенный справа от названия.

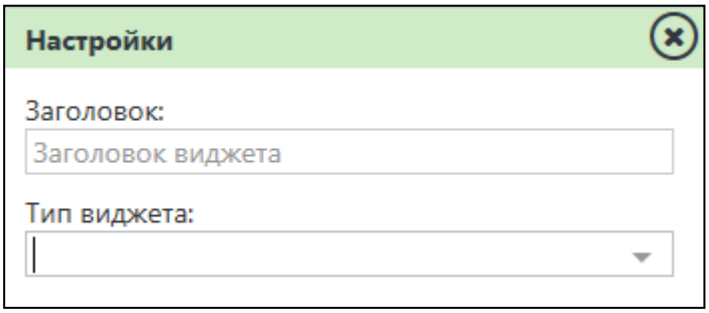
Примечание. Если список отчетов закрыт, откройте его (см. стр. 97).

3. Нажмите кнопку вызова меню настроек и в открывшемся меню выберите пункт "Настроить вид".

   Панель мониторинга перейдет в режим редактирования.
4. Для добавления на панель нового виджета нажмите на плитку "Добавить виджет".

   На панели появится "пустой" виджет.
5. Для настройки виджета нажмите на значок настройки , расположенный в его правом верхнем углу.

   В правой части главного окна появится панель настроек виджета.



6. Введите заголовок виджета и выберите тип: таблица или график.

В панели настроек появится поле для задания следующего параметра. Последующие этапы настройки параметров зависят от выбранных типов виджета и текущего параметра.

7. Настройте параметры виджета и нажмите кнопку "Применить", расположенную в нижней части панели настройки.

   Виджет отобразит значения заданных параметров.

8. Для изменения размера виджета используйте указатель, расположенный в его нижнем правом углу. Для перемещения виджета выделите его заголовок и перетащите на свободное место панели.

9. Для добавления следующего виджета нажмите на плитку "Добавить виджет" и повторите выполнение пп. **5** – **7**.

10. После добавления в отчет всех необходимых виджетов нажмите кнопку "Сохранить", расположенную в левом верхнем углу центральной части окна.

Редактирование отчета

Редактирование отчета включает в себя:

- изменение названия;
- удаление и добавление в состав отчета новых виджетов;
- изменение параметров виджетов, входящих в состав отчета.

Для редактирования отчета:

1. Нажмите кнопку вызова меню настроек и в открывшемся меню выберите пункт "Список отчетов".

   В правой части главного окна появится список сформированных отчетов.

2. Выберите отчет в списке.

Для изменения названия отчета:

- Выберите отчет в списке, нажмите кнопку  , расположенную справа от его названия, и введите новое название.

Для удаления или добавления виджета в отчет:

1. Откройте отчет, нажмите кнопку вызова меню настроек и в открывшемся меню выберите пункт "Настроить вид".

   Отчет перейдет в режим редактирования.

2. Для удаления выберите виджет и нажмите на значок  , расположенный в его правом верхнем углу.

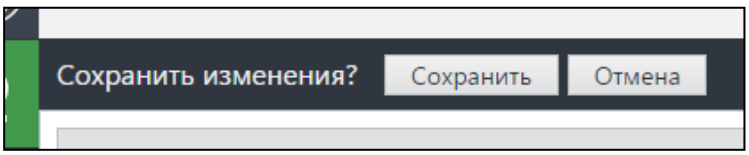
   Виджет будет удален.

3. Для добавления нового виджета нажмите на плитку "Добавить виджет".

   Плитка примет вид виджета в режиме редактирования.

4. Нажмите на значок настройки  , расположенный в его правом верхнем углу, и в открывшейся справа панели выполните настройку параметров виджета.

5. Для сохранения изменений нажмите кнопку "Сохранить", расположенную в верхней части панели мониторинга.



Для изменения параметров виджета:

1. Откройте отчет, нажмите кнопку вызова меню настроек и в открывшемся меню выберите пункт "Настроить вид".

   Отчет перейдет в режим редактирования.

2. Выберите виджет и нажмите на значок настройки в его правом верхнем углу.

   В правой части главного окна появится панель настроек виджета.

3. Укажите нужные значения параметров и нажмите кнопку "Применить", расположенную в нижней части панели настроек.

   Содержание виджета отобразится в соответствии с измененными параметрами.

4. Закройте панель настроек.

   При необходимости измените параметры другого виджета (см. пп. **2–3**).

5. Для сохранения изменений нажмите кнопку "Сохранить", расположенную в верхней части панели мониторинга.

Печать отчета

Сформированный отчет можно сохранить в виде файла в формате PDF и вывести на печать. При этом предусмотрены настройки оформления внешнего вида отчета и фильтра виджетов.

Настройка оформления внешнего вида включает в себя добавление в отчет следующих элементов:

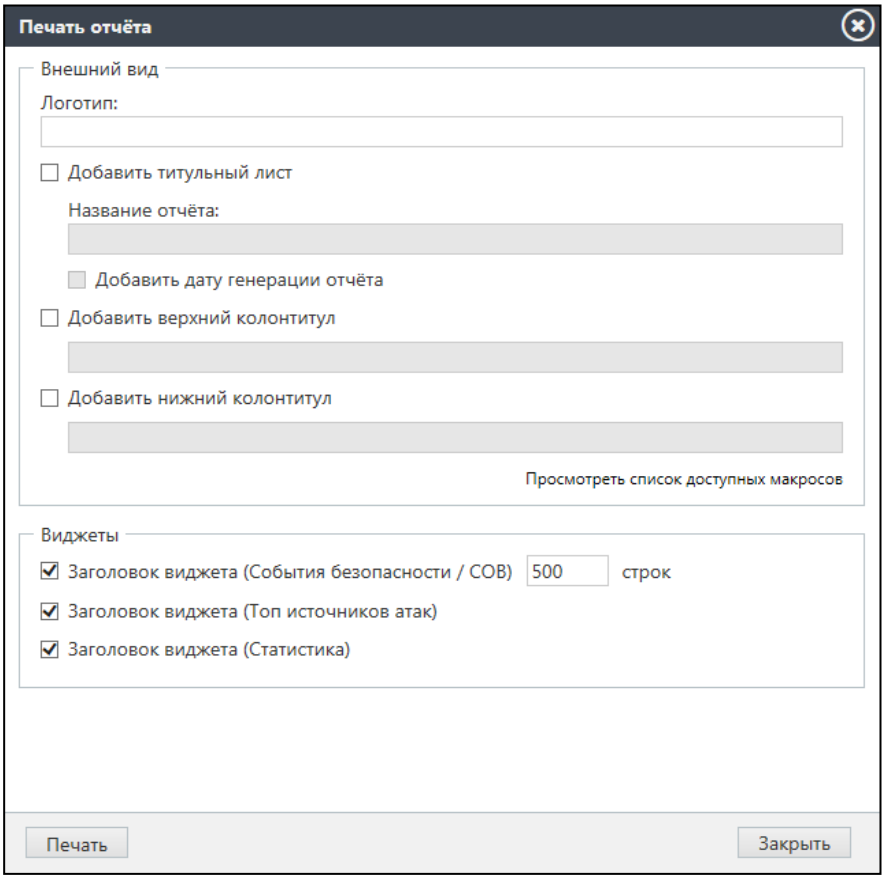
- логотип;
- титульный лист с названием отчета и датой генерации;
- верхний и/или нижний колонтитул.

В настройке фильтра нужно указать виджеты, которые должны войти в состав печатного отчета. Предварительно все виджеты отчета включены в этот состав.

Для сохранения и печати отчета:

1. Откройте отчет, нажмите кнопку вызова меню настроек и в открывшемся меню выберите пункт "Печать".

   На экране появится окно настроек внешнего вида отчета и фильтра.



2. Для добавления в отчет логотипа выделите поле "Логотип" и в открывающемся окне укажите нужный файл.

   В поле появится имя файла логотипа. Для просмотра изображения наведите курсор на ссылку "Показать логотип".

   Для выбора другого файла или удаления выбранного логотипа из отчета удалите имя файла.

3. Укажите остальные параметры оформления внешнего вида отчета.

   Внимание! При добавлении колонтитулов их можно ввести вручную или использовать макросы. Для просмотра доступных макросов нажмите на соответствующую ссылку.

4. При необходимости выборочной печати отчета снимите отметки у тех виджетов, которые не должны войти в отчет. У табличных виджетов также доступно ограничение числа печатаемых строк.

5. После настройки внешнего вида отчета и фильтра виджетов нажмите кнопку "Печать", расположенную в нижней части окна.

   Внизу рабочего окна появится надпись о том, что происходит создание отчета. Данное окно можно закрыть и продолжить работать с системой (переходить на другие страницы и прочее). Когда отчет будет готов, на активной странице появится сообщение о скачивании файла в формате PDF.

   Внимание! Максимальное время выполнения операции по созданию отчета — 30 минут. Если в течение 30 минут не будет предложено скачивание отчета, то, скорее всего, он получается слишком большой и система не может его обработать. Внизу страницы печати будет показано уведомление о произошедшей ошибке. В таком случае рекомендуется выбрать меньше данных для печати.

6. Сохраните документ и при необходимости распечатайте его.

Удаление отчета

Внимание! Если в списке отчетов содержится только один отчет, его удалить нельзя.

Для удаления отчета:

1. Нажмите кнопку вызова меню настроек и в открывшемся меню выберите пункт "Список отчетов".

   В правой части главного окна появится список сформированных отчетов.

2. Выберите в списке нужный отчет и нажмите кнопку "Удалить", расположенную справа от его названия.

   На экране появится запрос на подтверждение операции удаления.

3. Нажмите кнопку "Да".

   Отчет будет удален из списка.

Структура

Раздел "Структура" предназначен для просмотра сведений о состоянии объектов мониторинга и настройки шаблонов.

Для навигации используется дерево объектов, расположенное слева. В дереве представлены три типа элементов:

- группы узлов (выделены жирным шрифтом);
- узлы;
- домены нижнего уровня (выделены жирным шрифтом).

Для перехода на страницу настройки нужного элемента выберите его в дереве объектов, в котором все узлы и поддомены отображаются как члены группы "Несортированное", входящей в корневую группу главного домена.

Примечание. Корневая группа главного домена содержит в себе все узлы и группы. Для нее доступно создание шаблонов, которые действуют на все узлы и группы в структуре. Содержит набор правил по умолчанию. При желании этот набор можно изменить (см. стр. 85).

Узел

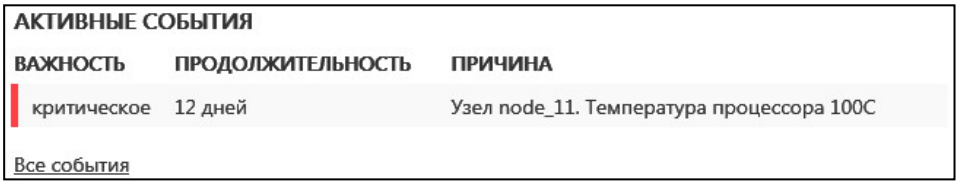
Страница содержит следующие вкладки:

- Состояние.
- Детальная информация.
- Шаблон.
- Настройки.
- Доступ.

Состояние

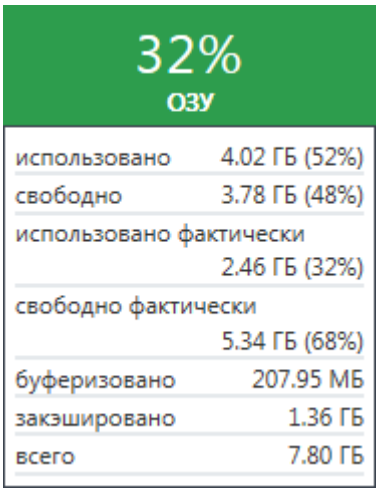
На этой вкладке отображается в режиме реального времени информация, разделенная на следующие группы:

- Активные события — таблица со списком активных событий на узле с указанием их важности, продолжительности и причины; внизу таблицы находится ссылка, позволяющая перейти на страницу "События мониторинга" для просмотра всех событий, произошедших на узле.



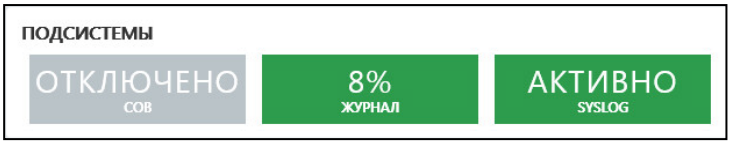
- ЦП и память — сведения о состоянии центрального процессора и оперативной памяти, представленные в виде подгрупп параметров:
  - загрузка ОЗУ;
  - использование SWAP;
  - загрузка ЦП;
  - температура ЦП и дисковой подсистемы.

Каждую подгруппу (здесь и далее) можно раскрыть и просмотреть значения параметров.

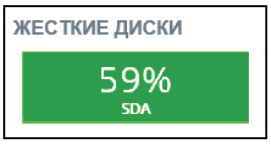


Состав группы можно настраивать — удалять или добавлять подгруппы. Настройку выполняют на вкладке "Настройки" (см. ниже).

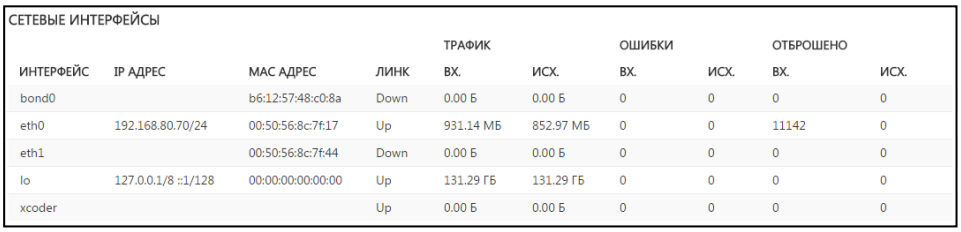
- Подсистемы — сведения о состоянии системы обнаружения вторжений, дисковой подсистемы и системы журналирования.



- Жесткие диски — сведения об имеющихся жестких дисках и состоянии их разделов.



- Сетевые интерфейсы — информация о статусе и статистике сетевых интерфейсов.



В верхней части страницы приводится время непрерывной работы узла и ссылка для генерации отчета о работе узла для передачи в службу технической поддержки в случае некорректной работы узла.

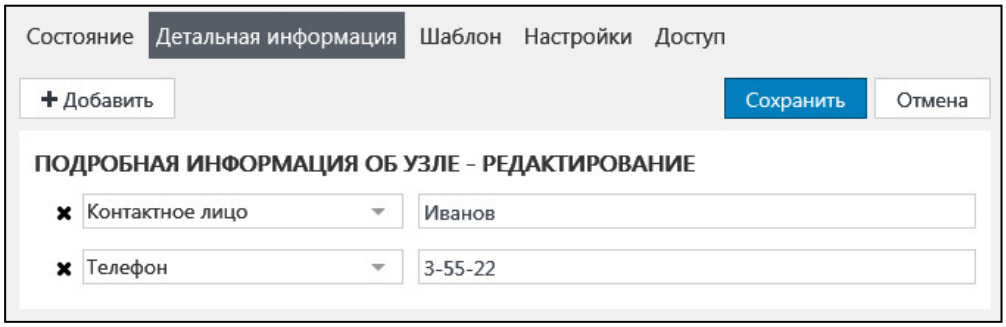
Примечание. Генерация отчета занимает длительное время, по истечении которого будет предложено сохранить файл отчета на диск стандартными средствами веб-браузера.

Детальная информация

Вкладка предназначена для настройки и последующего отображения сведений о лицах, ответственных за эксплуатацию узла:

- ФИО контактного лица;
- номер рабочего телефона;
- номер мобильного телефона;
- учетная запись Skype;
- произвольная дополнительная информация.

Примечание. Содержимое этого поля будет выводиться на плитке виджета типа "Структура" на Панели мониторинга.



Для изменения данных:

1. Для добавления нового параметра нажмите кнопку "Добавить".

Внизу списка появится дополнительное поле для нового параметра.

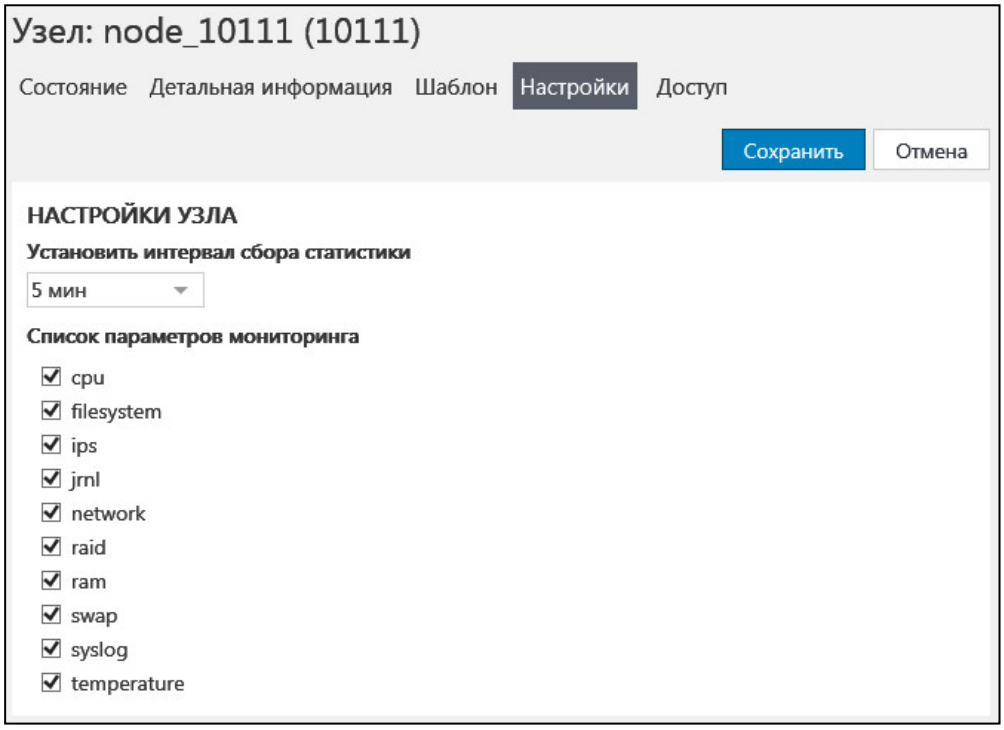
2. Для изменения типа параметра нажмите кнопку и выберите из раскрывшегося списка нужный параметр.
3. Ввести/изменить значение параметра можно в поле справа от его названия.
4. Для удаления параметра нажмите кнопку, расположенную слева от его названия.
5. После внесения необходимых изменений нажмите кнопку "Сохранить".

Шаблон

На данной вкладке настраиваются правила мониторинга для узла. Подробнее см. в разделе "Настройка шаблонов мониторинга" (см. стр. **85**).

Настройки

Вкладка предназначена для задания интервала сбора статистики и настройки параметров мониторинга.



Для выполнения настроек:

1. Выберите из списка интервал сбора статистических показателей от настраиваемого узла.

Примечание. Сбор данных узла можно отключить. Для этого выберите в списке значение "Выключить". Эта настройка равнозначна отключению всех параметров мониторинга этого узла.

Внимание! При отключении параметра мониторинга будет прекращен соответствующий сбор статистических данных и в дальнейшем информация по этому параметру за период отключения будет недоступна. Также не будут работать виджеты и правила, связанные с отключенным параметром.

2. Укажите параметры узла, данные которых должны собираться и отображаться на вкладке "Состояние" и в соответствующих виджетах системы. Для этого установите необходимые отметки и нажмите кнопку "Сохранить".

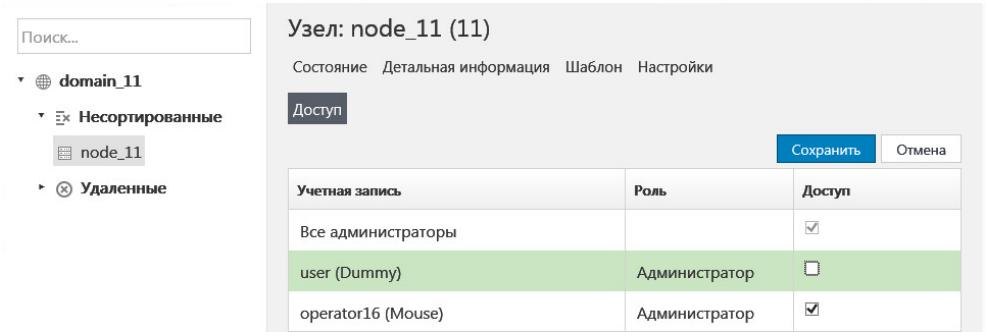
Параметр	Соответствующая подгруппа	Группа
cpu	ЦП	ЦП И ПАМЯТЬ
filesystem	SDA BOOT; DATA; SYSTEM; TEMPORARY	ЖЕСТКИЕ ДИСКИ РАЗДЕЛЫ ЖЕСТКИХ ДИСКОВ

ips	СОВ	ПОДСИСТЕМЫ
jml	ЖУРНАЛ	ПОДСИСТЕМЫ
network	вся таблица	СЕТЕВЫЕ ИНТЕРФЕЙСЫ
raid	RAID	ЖЕСТКИЕ ДИСКИ
ram	ОЗУ	ЦП И ПАМЯТЬ
swap	SWAP	ЦП И ПАМЯТЬ
syslog	SYSLOG	ПОДСИСТЕМЫ
temperature	ТЕМПЕРАТУРА	ЦП И ПАМЯТЬ

Примечание. При переходе на вкладку "Состояние" может быть небольшая задержка при обновлении данных в соответствии с выполненными настройками.

Доступ

На этой вкладке настраивается доступ администраторов системы к мониторингу узла.

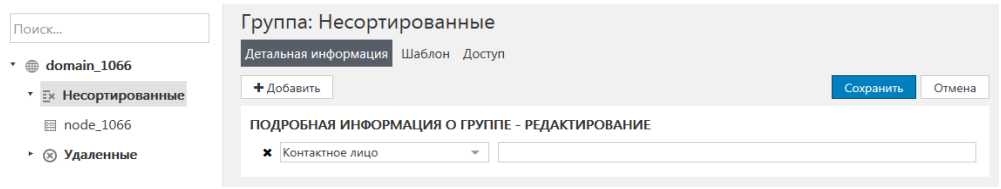


Для ограничения доступа администратора уберите соответствующий флажок в таблице и нажмите кнопку "Сохранить".

Внимание! Нельзя ограничить доступ администратора, имеющего неограниченные права.

Группа узлов

Страница содержит три вкладки: "Детальная информация", "Шаблон" и "Доступ".



Вкладка "Детальная информация" предназначена для настройки данных о лицах, ответственных за эксплуатацию группы узлов:

- контактное лицо;
- мобильный телефон;
- телефон;
- учетная запись Skype;
- произвольная дополнительная информация.

Примечание. Содержимое этого поля будет выводиться на плитке виджета типа "Структура" на Панели мониторинга.

О настройке см. выше в описании страницы "Узел".

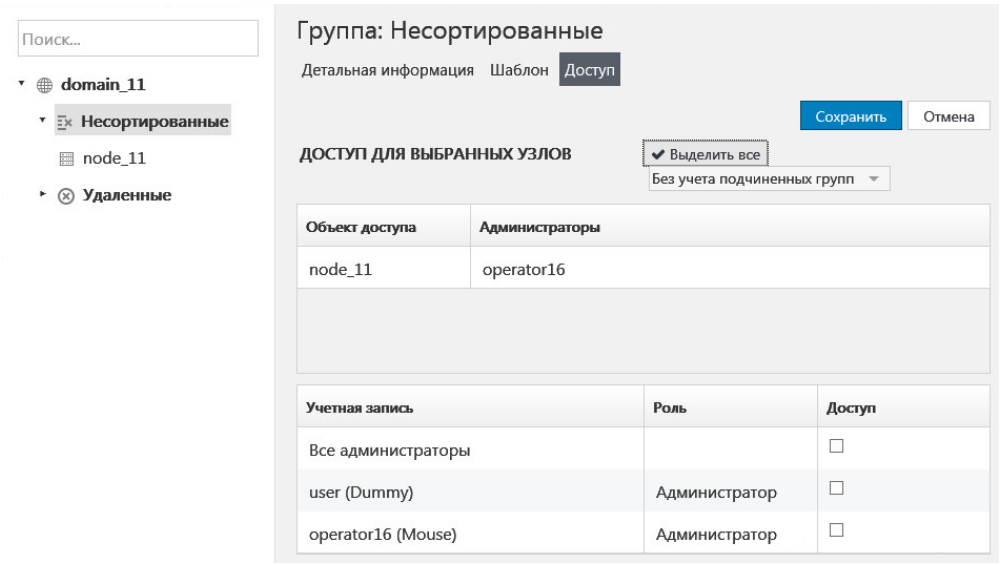
Шаблон

На вкладке "Шаблон" настраиваются правила мониторинга для узлов, входящих в соответствующую группу узлов и ее подгрупп. Подробнее см. в разделе "Настройка шаблонов мониторинга" (см. стр. **85**).

Доступ

Подраздел предназначен для настройки доступа администраторов системы к мониторингу группы узлов и состоит из двух частей:

- верхняя часть отображает узлы и поддомены, входящие в эту группу, с перечнем администраторов, которым разрешен доступ к ним;
- нижняя часть содержит полный список администраторов системы, имеющих ограниченные права.



При выборе в верхней части страницы одного из узлов группы в нижней отобразится текущая ситуация с доступом администраторов к этому узлу. Можно выделить сразу несколько узлов, используя правую кнопку манипулятора типа мышь, а также клавиши "Ctrl" или "Shift". Для выделения всех узлов достаточно нажать кнопку "Выделить все".

Внимание! По умолчанию в список узлов верхней части страницы включены узлы, относящиеся к подгруппам выбранной группы. Для их отключения выберите в раскрывающемся меню над таблицей объектов доступа пункт "Без учета подчиненных групп".

Для настройки доступа определенного администратора к выделенным узлам переведите соответствующий флажок в нужное состояние и нажмите кнопку "Сохранить".

Примечание. Для управления доступом сразу всех администраторов системы, имеющих ограниченные права, можно воспользоваться флажком, соответствующим учетной записи "Все администраторы".

Внимание! Если у пользователя не будет доступа ко всем узлам в группе, то эта группа будет ему недоступна.

Поддомен

Страница поддомена или его узлов содержит следующие вкладки:

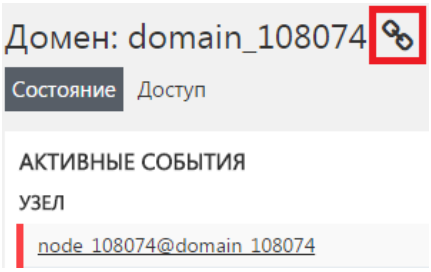
- Состояние.
- Доступ.

Состояние

На странице в виде таблицы отображаются активные события, зарегистрированные на узлах поддомена, с указанием их важности, продолжительности и причины.

Примечание. Внизу таблицы активных событий узла поддомена находится ссылка "Все события", позволяющая перейти на страницу "События мониторинга" для просмотра всех событий, произошедших на этом узле (см. стр. **95**). При переходе на страницу "События мониторинга" будет автоматически включен соответствующий фильтр.

Для перехода к мониторингу домена нижестоящего уровня используйте ссылку, расположенную справа от имени поддомена или его узла в заголовке страницы:



Доступ

Страница предназначена для настройки доступа администраторов системы к мониторингу узла (см. стр. **105**) или поддомена (как группы узлов, см. стр. **106**).

Примечание. Для настройки доступа к узлам поддомена администратор должен быть назначен через Менеджер конфигурации на управление нижестоящим доменом (см. стр. **75**). Тольков этом случае он сможет видеть в мониторинге информацию об узлах поддомена.

Внимание! Встроенного администратора нельзя назначить на управление нижестоящим доменом.

Аудит

Под аудитом подразумевается контроль состояния защищенности и работоспособности комплекса. Оценка функционирования комплекса осуществляется посредством анализа произошедших событий, зарегистрированных в журналах сетевых устройств.

В задачи аудита входят:

- регулярный просмотр содержимого журналов регистрации;
- оптимальная настройка параметров сбора и хранения журналов.

Администратор может проводить аудит, используя на своем рабочем месте консоль веб-управления, а также локально — с помощью команд управления сетевым устройством.

Журналы аудита

В рамках аудита используются два журнала, хранящиеся локально на каждом из сетевых устройств и на ЦУС:

- системный журнал;
- журнал ДА.

В системном журнале хранятся события, связанные с загрузкой операционной системы, события служб и приложений "Континент", а также любые другие системные события, удовлетворяющие требованиям к хранению их в журналах (уровень детализации). В системном журнале ЦУС помимо этого хранятся и события от подчиненных узлов сети.

В журнале ДА хранятся события срабатывания сигнатур на данном устройстве, а на ЦУС — от всех подчиненных узлов сети.

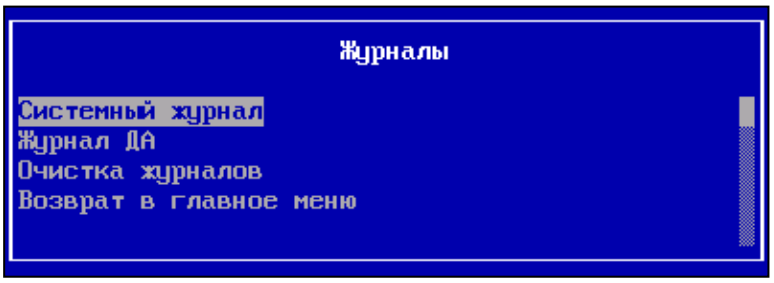
Локальный просмотр журналов

Меню работы с журналами

Для работы с журналами:

- Вызовите главное меню локального управления, выберите пункт "Журналы" и нажмите клавишу <Enter>.

  На экране появится меню работы с журналами.

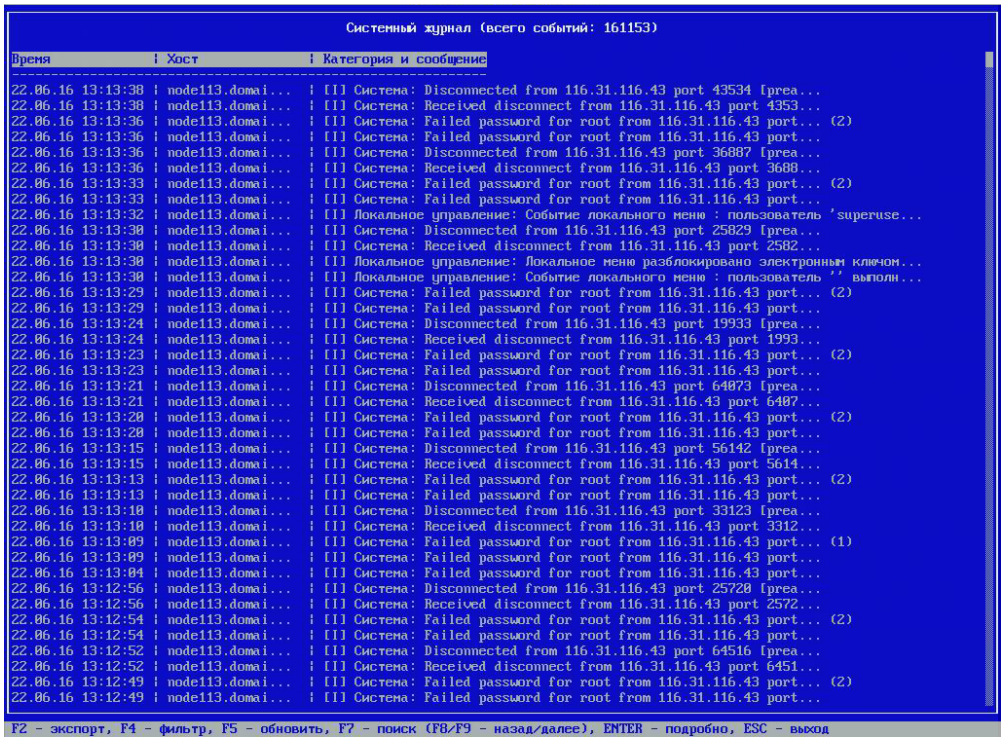


Системный журнал

Для просмотра журнала:

- Выберите в меню работы с журналами пункт "Системный журнал" и нажмите клавишу <Enter>.

  На экране появится окно просмотра системного журнала.



В окне просмотра отображается список всех хранящихся в журнале событий.

Для каждого события приводится следующая информация:

- дата и время;
- хост;
- уровень важности (сокращенно, в квадратных скобках);
- категория;
- текст сообщения (частично).

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

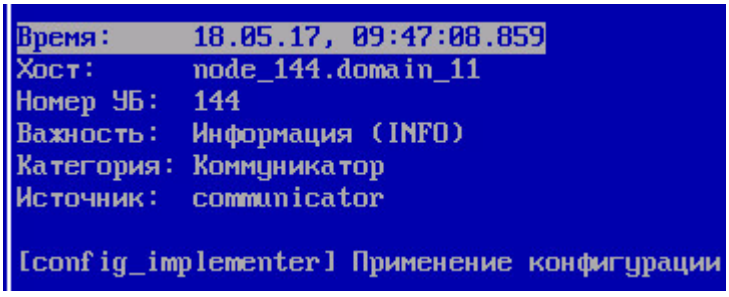
Для обновления журнала используйте клавишу <F5>.

Для возврата в меню работы с журналами нажмите клавишу <Esc>.

Для просмотра подробной информации о событии:

1. Выделите событие в списке и нажмите клавишу <Enter>.

   На экране появится окно с подробными сведениями о выбранном событии.



   Дополнительно приводятся следующие сведения:

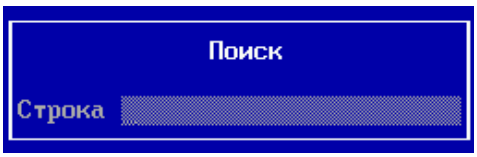
   - номер УБ, на котором зафиксировано событие;
   - уровень важности (полностью);
   - источник;
   - текст сообщения полностью.

2. Для возврата в окно просмотра журнала нажмите клавишу <Esc>.

Для поиска события по фрагменту текста сообщения:

1. Нажмите клавишу <F7>.

   На экране появится окно для ввода фрагмента текста.



   Введите фрагмент текста для поиска и нажмите клавишу <Enter>.

   Начнется поиск события, содержащего в тексте сообщения введенный фрагмент. Поиск осуществляется вниз по списку от текущей выделенной записи.

   Первое найденное событие будет выделено в списке.

2. Для продолжения поиска события с таким же фрагментом текста нажмите клавишу <F9>. При необходимости вернуться к предыдущему найденному событию нажмите клавишу <F8>.
3. Для изменения критерия поиска нажмите клавишу <F7>, введите новый фрагмент текста и нажмите клавишу <Enter>.

   Начнется поиск вниз по списку от выделенной строки.

   Для изменения направления поиска используйте клавишу <F8>.

Фильтр системного журнала

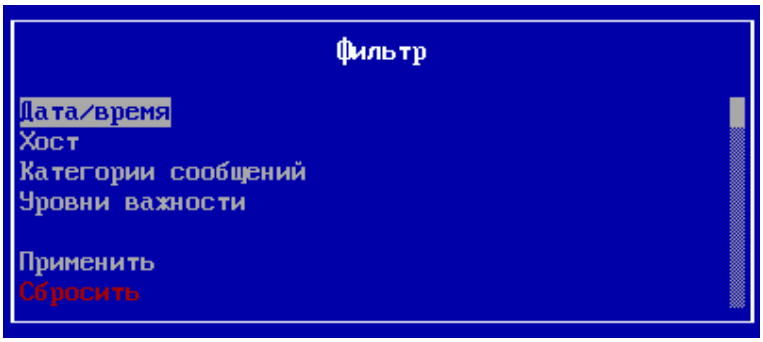
Для отображения определенных событий в окне просмотра системного журнала можно использовать фильтр, настраиваемый по следующим параметрам:

- дата и время;
- хост — источник события;
- категория сообщения;
- уровень важности.

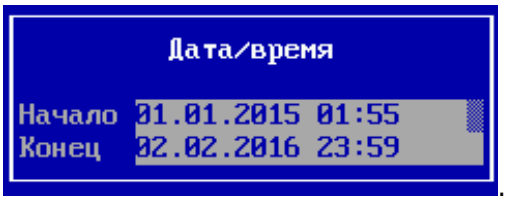
Для настройки фильтра:

1. В окне просмотра системного журнала нажмите клавишу <F4>.

   На экране появится меню настройки фильтра.

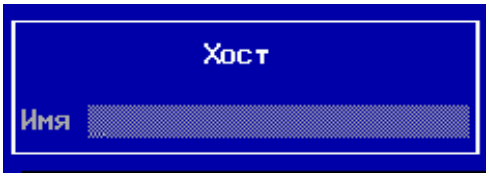


2. Выберите в меню нужный параметр, нажмите клавишу <Enter> и задайте нужное значение.
   - При настройке по дате и времени введите начало и конец периода в соответствии с приведенным ниже форматом.

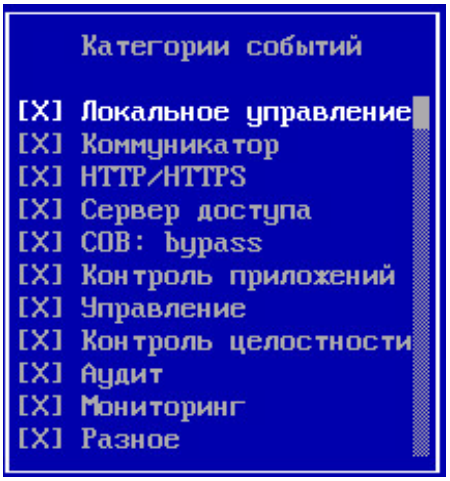


Примечание. Для перемещения между вводимыми параметрами используйте клавиши курсоров: <↑>, <↓>.

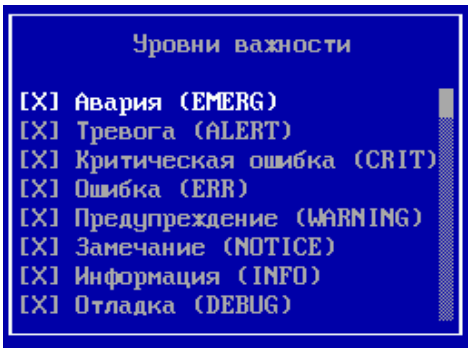
- При настройке по имени хоста введите имя или часть имени хоста. Данный фильтр удобно использовать для просмотра журналов на ЦУС, в котором отображаются события с различных узлов сети.



- Фильтр по категориям событий позволяет отфильтровать события по группам источников. Удалите клавишей <Пробел> категории, события которых не должны отображаться в окне просмотра журнала.



- При настройке по уровню важности удалите клавишей <Пробел> ненужные уровни.



3. После настройки параметра нажмите клавишу <Enter>.

   Будет выполнен возврат в меню настройки фильтра.

   Примечание. После настройки по какому-либо параметру можно выполнить настройку по другому параметру (или параметрам). Для этого повторите выполнение пп. **2–3**. В результате после выполнения п. **4** будет действовать составной фильтр.

4. Выберите пункт "Применить" и нажмите клавишу <Enter>.

   В окне просмотра журнала отобразятся только те события, которые удовлетворяют настройкам фильтра.

5. Для обновления сведений нажмите клавишу <F5>.

   Внимание! Действие фильтра при просмотре журнала будет длиться до тех пор, пока не будет выполнен его сброс.

Для сброса фильтра:

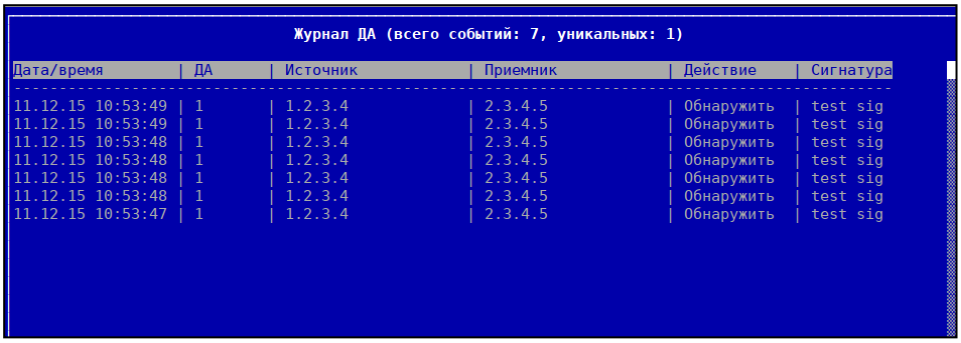
1. В меню настройки фильтра выберите пункт "Сбросить".
2. Нажмите клавишу <Enter>.

Журнал детектора атак

Для просмотра журнала:

- Выберите в меню работы с журналами пункт "Просмотр журнала детектора атак" и нажмите клавишу <Enter>.

  На экране появится окно просмотра журнала детектора атак.



  В окне просмотра отображается список всех хранящихся в журнале событий.

  В заголовке журнала приводится количество событий, зарегистрированных за определенный интервал времени (по умолчанию — 10 секунд). Повторы одного и того же события за этот интервал времени представлены в журнале одной записью.

  Для каждого события приводится следующая информация:

  - дата и время;
  - серийный номер ДА;
  - IP-адрес источника атаки;
  - IP-адрес приемника атаки;
  - тип выполненного действия СОВ;
  - описание сигнатуры.

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

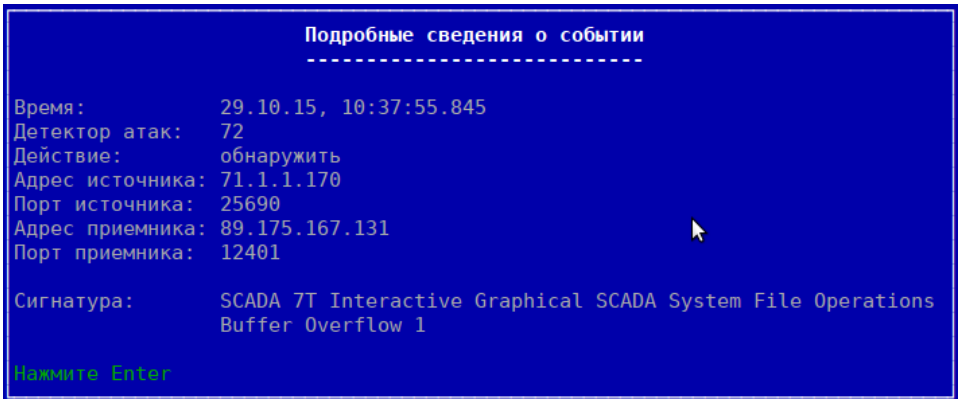
Для обновления журнала используйте клавишу <F5>.

Для возврата в меню работы с журналами нажмите клавишу <Esc>.

Для просмотра подробной информации о событии:

1. Выделите событие в списке и нажмите клавишу <Enter>.

   На экране появится окно с подробными сведениями о выбранном событии.



Дополнительно приводятся следующие сведения:

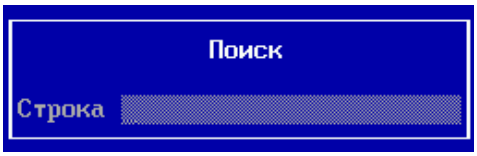
- порт источника;
- порт приемника;
- полное описание сигнатуры.

2. Для возврата в окно просмотра журнала нажмите клавишу <Enter> или <Esc>.

Для поиска события по фрагменту описания сигнатуры:

1. Нажмите клавишу <F7>.

   На экране появится окно для ввода фрагмента описания сигнатуры.



   Введите фрагмент описания сигнатуры для поиска и нажмите клавишу <Enter>.

   Начнется поиск события, содержащего в описании сигнатуры введенный фрагмент. Поиск осуществляется вниз по списку от текущей выделенной записи.

   Первое найденное событие будет выделено в списке.

2. Для продолжения поиска события с таким же фрагментом описания сигнатуры нажмите клавишу <F9>. При необходимости вернуться к предыдущему найденному событию нажмите клавишу <F8>.
3. Для изменения критерия поиска нажмите клавишу <F7>, введите новый фрагмент текста и нажмите клавишу <Enter>.

   Начнется поиск вниз по списку от выделенной строки.

   Для изменения направления поиска используйте клавишу <F8>.

Фильтр журнала детектора атак

Для отображения определенных событий в окне просмотра журнала ДА можно использовать фильтр, настраиваемый по следующим параметрам:

- дата и время;
- серийный номер узла безопасности.

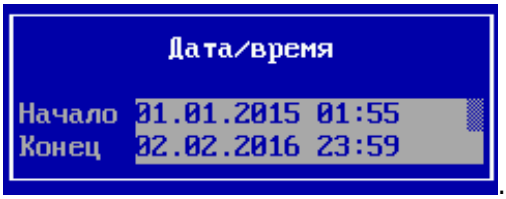
Примечание. Фильтр по серийному номеру узла безопасности рекомендуется использовать при просмотре журнала на ЦУС.

Для настройки фильтра:

1. В окне просмотра журнала ДА нажмите клавишу <F4>.

   На экране появится меню настройки фильтра.

2. Выберите в меню нужный параметр, нажмите клавишу <Enter> и задайте нужное значение.
   - При настройке по дате и времени введите начало и конец периода в соответствии с приведенным ниже форматом.



Примечание. Для перемещения между вводимыми параметрами используйте стандартные клавиши: <↑>, <↓>

- При настройке по серийному номеру узла безопасности введите номера или несколько номеров, используя запятую.

3. После настройки параметра нажмите клавишу <Enter>.

   Будет выполнен возврат в меню настройки фильтра.

   Примечание. После настройки по какому-либо параметру можно выполнить настройку по другому параметру. Для этого повторите выполнение пп. **2–3**. В результате после выполнения п. **4** будет действовать составной фильтр.

4. Выберите пункт "Применить" и нажмите клавишу <Enter>.

   В окне просмотра журнала отобразятся только те события, которые удовлетворяют настройкам фильтра.

5. Для обновления сведений нажмите клавишу <F5>.

   Внимание! Действие фильтра при просмотре журнала будет длиться до тех пор, пока не будет выполнен его сброс.

Для сброса фильтра:

1. В меню настройки фильтра выберите пункт "Сбросить".
2. Нажмите клавишу <Enter>.

Экспорт журналов

Средствами локального управления предусмотрен экспорт журналов на внешний носитель для передачи сведений во внешний аудит или просмотра внешними программами.

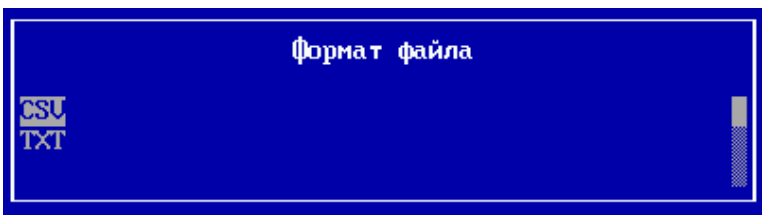
В качестве внешнего носителя используют USB-флеш-накопитель.

На внешнем носителе журналы могут быть сохранены в файлах формата TXT или CSV.

Для экспорта журнала:

1. Откройте окно просмотра журнала.
2. При необходимости настройте и примените фильтр.
3. Нажмите клавишу <F2>.

   На экране появится окно выбора формата файла.



4. Выберите формат и нажмите клавишу <Enter>.

   На экране появится сообщение о необходимости вставить внешний носитель.

5. Вставьте USB-флеш-накопитель в разъем сетевого устройства и нажмите клавишу <Enter>.

   Начнется запись файла на внешний носитель. Дождитесь сообщения об успешном завершении операции.

6. Извлеките внешний носитель и нажмите клавишу <Enter>.

   Будет выполнен возврат в окно просмотра журнала.

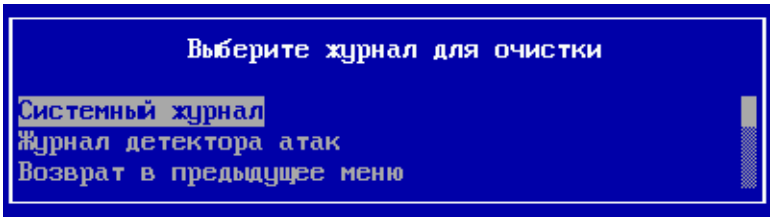
Очистка журналов

При необходимости записи журналов можно удалить. При этом можно удалить как все записи определенного журнала, так и записи за определенный период.

Для удаления записей журнала:

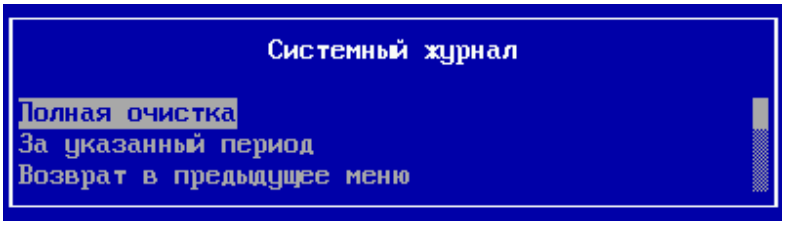
1. Откройте меню работы с журналами, выберите пункт "Очистка журналов" и нажмите клавишу <Enter>.

   На экране появится меню выбора журнала для очистки.



2. Выберите журнал и нажмите клавишу <Enter>.

   На экране появится меню выбора варианта очистки.

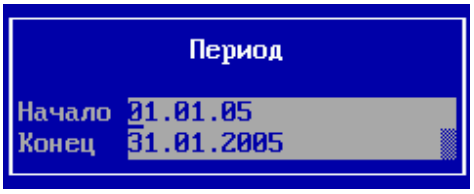


3. Выберите вариант и нажмите клавишу <Enter>.

   - Если было выбрано "Полная очистка", начнется очистка журнала. Дождитесь сообщения "Журнал очищен".

     Перейдите к **п.6**.

   - Если было выбрано "За указанный период", на экране появится окно для ввода начала и конца периода.



   Примечание. Для перемещения между вводимыми параметрами используйте стандартные клавиши: <↑>, <↓>.

   Перейдите к **п.4**.

4. Укажите начало и конец периода и нажмите клавишу <Enter>.

   На экране появится запрос на подтверждение удаления записей за указанный период.

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

   Начнется удаление записей. Дождитесь сообщения "Журнал очищен".

6. Нажмите клавишу <Enter>.

   Будет выполнен возврат в меню выбора варианта очистки журнала.

Резервное копирование и восстановление

Компоненты комплекса при локальном управлении позволяют создавать резервные копии своих БД, а также проводить их восстановление.

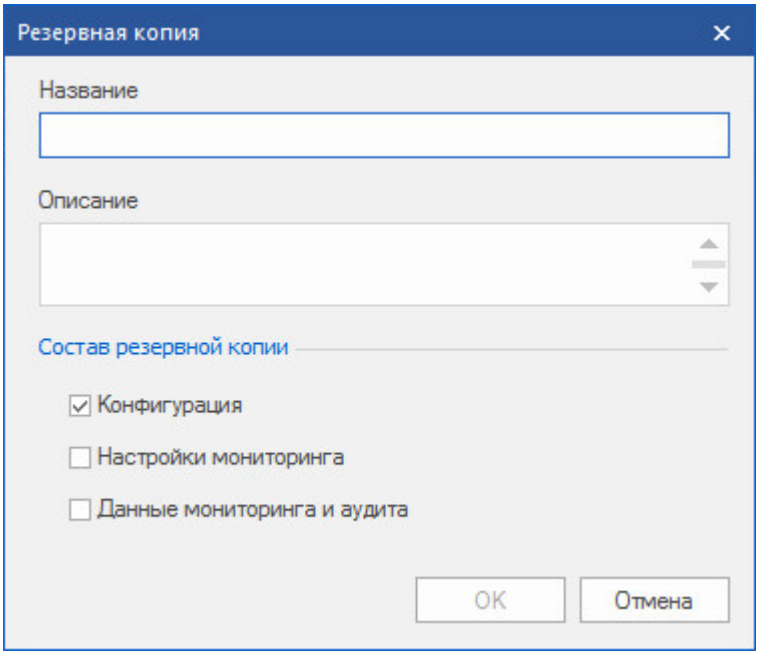
Для ЦУС управление резервными копиями возможно также с помощью Менеджера конфигурации.

Создание резервной копии

Для создания резервной копии БД ЦУС в Менеджере конфигурации:

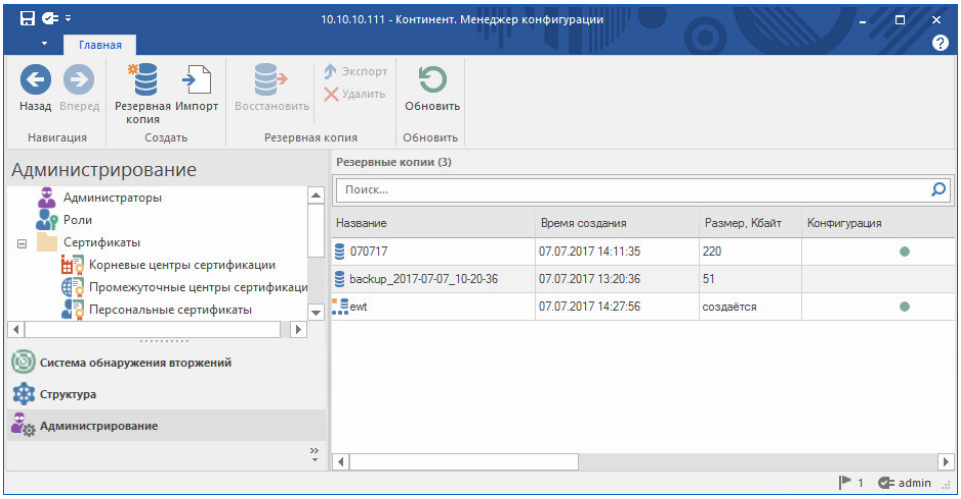
1. В Менеджере конфигурации перейдите в раздел "Администрирование" и выберите подраздел "Резервные копии".
2. Нажмите кнопку "Резервная копия" на панели инструментов.

   На экране появится окно "Резервная копия".



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 иконкой создаваемой БД.



Для создания резервной копии при локальном управлении:

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

   На экране появится окно "Меню инструменты".

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

   Появится окно запроса USB-флеш-накопителя.

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

   Появится окно "Базы для резервного копирования".

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

   Будет выполнена запись резервной копии выбранных компонентов на внешний носитель в файл config.c4b, после чего появится сообщение об успешном завершении операции.

Восстановление из резервной копии

Для восстановления из резервной копии БД ЦУС в Менеджере конфигурации:

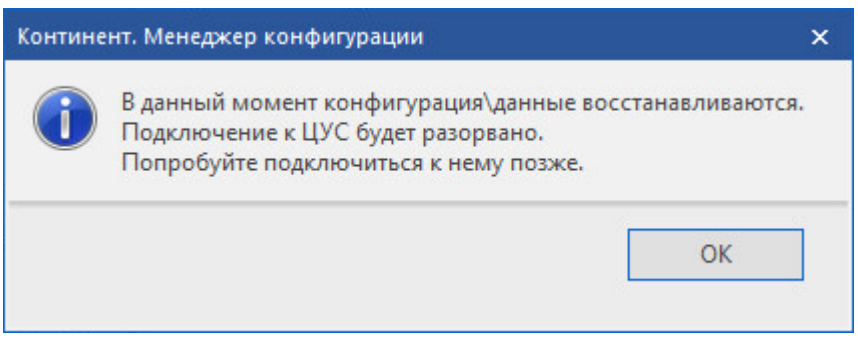
1. В Менеджере конфигурации перейдите в раздел "Администрирование" и выберите подраздел "Резервные копии".

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 резервной копии при локальном управлении:

> **Внимание!** Если Вы не уверены, что резервная копия создана при текущих сетевых настройках интерфейса управления, уточните его текущий IP-адрес перед восстановлением и после него (см. стр. 29).

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

   На экране появится окно "Меню инструменты".

2. Перейдите к пункту "Резервное копирование и восстановление данных | Восстановление из резервной копии".

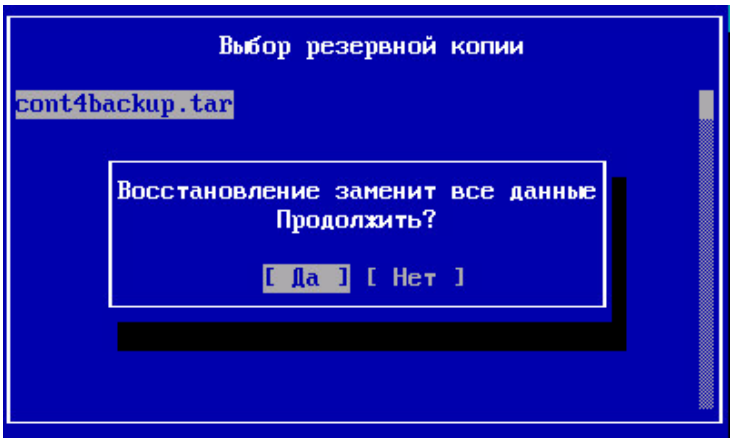
   Появится окно запроса USB-флеш-накопителя.

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>.

   На экране появится запрос на продолжение процедуры.



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

   Появится окно "Базы для резервного копирования".

6. Выберите клавишей <Пробел> восстанавливаемые БД и нажмите клавишу <Enter>.

> **Внимание!** При восстановлении конфигурации УБ более старой, чем в БД ЦУС его домена, отправка локальных изменений на ЦУС будет невозможна!

   Будет выполнена процедура восстановления из резервной копии с внешнего носителя, после чего появится сообщение об успешном завершении процедуры восстановления.

7. Перезагрузите ПО компонента комплекса (Главное меню/Завершение работы устройства/Перезагрузка).

8. Если при восстановлении конфигурации на компоненте комплекса не изменился IP-адрес интерфейса управления, перейдите к **п. 12**.

9. На вышестоящем ЦУС откройте Менеджер конфигурации и перейдите в подраздел "Структура | Узлы безопасности", выберите узел, на котором была восстановлена конфигурация, и нажмите кнопку "Свойства" на панели инструментов.

10. Выберите в свойствах узла безопасности пункт "Интерфейсы" и настройте соответствующем образом IP-адрес интерфейса управления.

11. Нажмите кнопку "OK", после чего сохраните изменения в конфигурации узла, нажав кнопку в верхнем левом углу Менеджера конфигурации.

12. Далее необходимо в Менеджере конфигурации установить политику (см. стр. 51) на узел с восстановленной конфигурацией.

Управление резервными копиями

Для управления резервными копиями БД ЦУС в Менеджере конфигурации:

1. В Менеджере конфигурации 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.

Обновление ПО

Внимание! В Менеджере конфигурации задача обновления ПО имеет стандартный тайм-аут 15 минут и при большом объеме передаваемых данных и медленной пропускной способности канала связи может завершиться со статусом "ошибка", хотя при этом обновление ПО может пройти успешно за более длительный период времени.

Перед обновлением ПО компонентов комплекса необходимо загрузить файлы обновления в репозиторий.

Управление репозиторием обновлений

Загрузить файлы обновления в репозиторий можно двумя способами — с сервера обновлений или из локального источника.

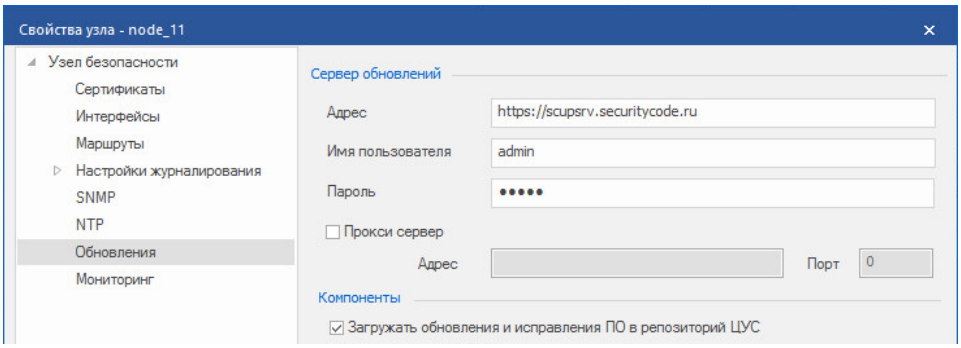
Настройка доступа к серверу обновлений осуществляется в Менеджере конфигурации для каждого ЦУС в отдельности.

Для настройки параметров сервера обновлений:

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" подраздел "Обновления".

   В правой части окна появятся параметры обновлений.



4. Для настройки параметров подключения к серверу обновлений выполните следующие действия:
   - 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.

5. Для включения автоматической загрузки обновлений ПО с сервера в репозиторий ЦУС поставьте 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:

1. Откройте Менеджер конфигурации, перейдите в раздел "Администрирование" и выберите подраздел "Обновления".
2. В списке узлов безопасности выберите нужный узел и нажмите кнопку "Загрузка" на панели инструментов.

   На экране появится окно "Загрузка обновлений".
3. Выберите новую версию ПО из доступных файлов на сервере обновлений и нажмите кнопку "Загрузить".

   После загрузки обновления с сервера в репозиторий в списке обновлений отобразится новый элемент.

Для импорта файла обновления ПО из локального источника:

1. Откройте Менеджер конфигурации, 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 Менеджер конфигурации, перейдите в подраздел "Администри-рование/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 ОС компонента комплекса

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

Для установки обновления ПО:

1. Откройте Менеджер конфигурации и перейдите в подраздел "Администри-рование/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.

4. Нажмите кнопку "ОК" в окне сообщения, после чего сохраните изменения в конфигурации узла, нажав кнопку в верхнем левом углу Менеджера конфигурации.

> **Внимание!** В случае обновления ПО ЦУС система автоматически перезагрузится после обновления ПО, при этом соединение с Менеджером конфигурации будет разорвано. После окончания перезагрузки необходимо заново установить соединение между Менеджером конфигурации и ПО ЦУС, а затем установить политику на все подчиненные узлы и поддомены (см. стр. 76).

Для отмены последнего обновления ПО:

1. Откройте Менеджер конфигурации 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 (в случае появления новой версии Менеджера конфигурации):

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".

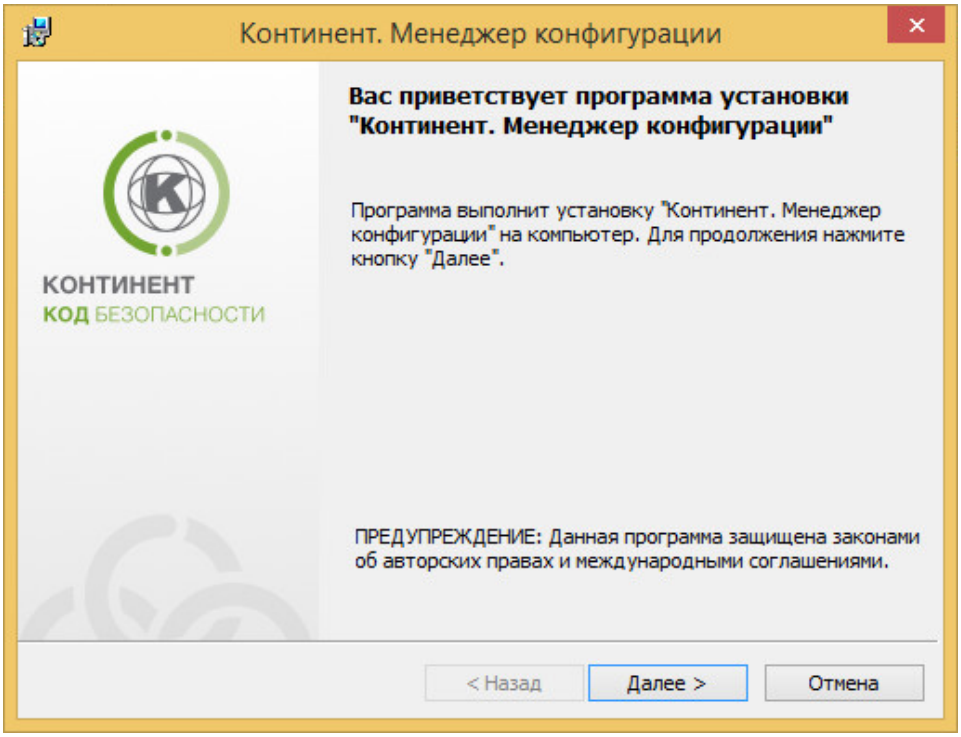
   Начнется процесс деинсталляции ПО.
4. После завершения процесса деинсталляции в появившемся запросе на перезагрузку ПК выберите "Да".

   Будет выполнена перезагрузка РМ администратора для завершения процесса деинсталляции.
5. Поместите установочный диск с дистрибутивом Менеджера конфигурации 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 Менеджера конфигурации получен при критическом обновлении ПО по сети интернет, перейдите к директории, содержащей файл дистрибутива.

6. Запустите файл Setup.exe.
7. На экране появится диалог со списком дополнительных компонентов, которые должны быть установлены до начала установки подсистемы управления.
8. Нажмите кнопку "Install" или "Установить".

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



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

   Появится диалог с текстом лицензионного соглашения.

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

11. Если вы согласны с условиями лицензионного соглашения, подтвердите свое согласие, нажав кнопку "Далее >".

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

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

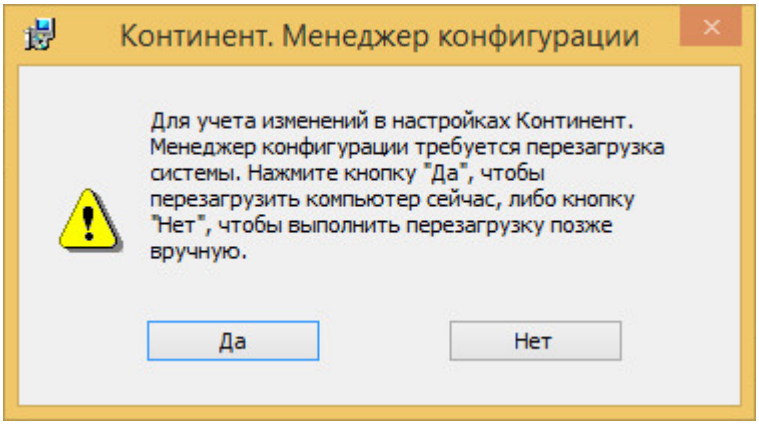
    Для выбора папки используйте кнопку "Изменить". По умолчанию программа установки копирует файлы на системный диск в папку ..\Program Files\Security Code\Continent.

    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".

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

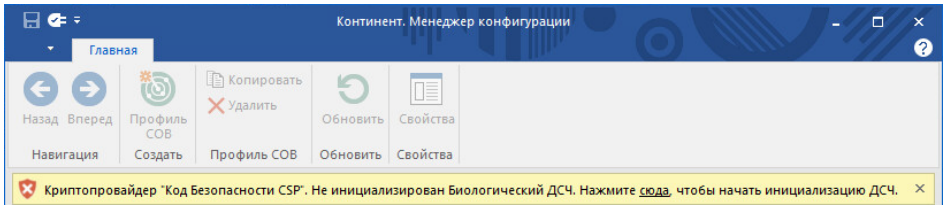
    Программа установки приступит к копированию файлов на жесткий диск компьютера. Ход выполнения процесса копирования отображается на экране в специальном окне. После установки Менеджера конфигурации на экране появится информационное окно об успешной установке приложения.

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

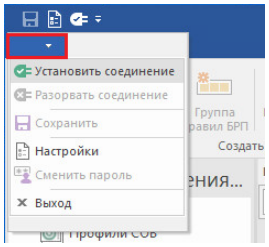


Перезагрузите компьютер.

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



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



Обновление ПО компонентов домена

Процедура обновления ПО компонентов домена состоит из следующих этапов:

1. Создание резервных копий (бэкапов) ЦУС и подчиненных УБ (см. стр. **116**).
2. Обновление ПО ЦУС (см. стр. **120**).
3. Обновление Менеджера конфигурации на РМ администратора (при необходимости, см. стр. **121**).
4. Установка политик на ЦУС и узлы домена (см. стр. **51**).
5. Обновление ПО УБ (см. стр. **120**).
6. Сохранение конфигурации ЦУС, установка политик на узлы домена (см. стр. **51**).

Обновление ПО компонентов комплекса

Процедура обновления ПО в иерархической структуре доменов состоит из следующих этапов:

1. Создание резервных копий (бэкапов) всех компонентов комплекса.
2. Обновление доменов нижнего уровня (проводится аналогично процедуре обновления ПО внутри одного домена, при завершении устанавливаются политики на ЦУС и узлы доменов нижнего уровня).
3. Обновление доменов среднего уровня (проводится аналогично процедуре обновления ПО внутри одного домена, при завершении устанавливаются

политики на ЦУС и узлы доменов среднего уровня, а также на поддомены и узлы доменов нижнего уровня).

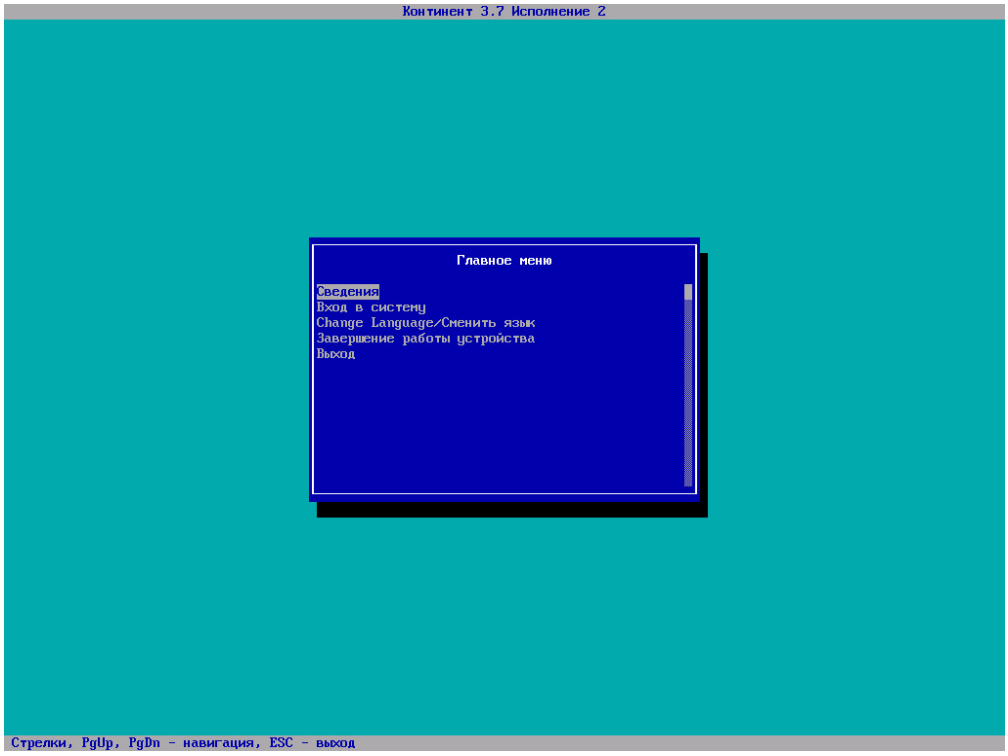
4. Обновление домена верхнего уровня (проводится аналогично процедуре обновления ПО внутри одного домена, при завершении устанавливаются политики на ЦУС и узлы верхнего домена, а также на все поддомены и узлы комплекса).

Приложение

Интерфейс локального управления

Средством локального управления компонентом комплекса является программное обеспечение, входящее в состав комплекса, со специализированным тестовым пользовательским интерфейсом.

После загрузки ОС на экране появится основной экран локального управления, отображающий главное меню.



Вверху экрана отображается название продукта, в центре — текущее меню, внизу экрана расположена строка возможных действий, уникальная для каждого меню.

Для перемещения между пунктами меню используйте клавиши клавиатуры:

- <Enter> — для выбора текущего пункта меню;
- < ↑> — для перемещения на одну строку вверх;
- < ↓> — для перемещения на одну строку вниз;
- <Page Up> — для перемещения в верх списка;
- <Page Down> — для перемещения в низ списка;
- <Esc> — для выхода в предыдущее меню.

Помимо основного экрана для пользователя доступны экраны служебных логов:

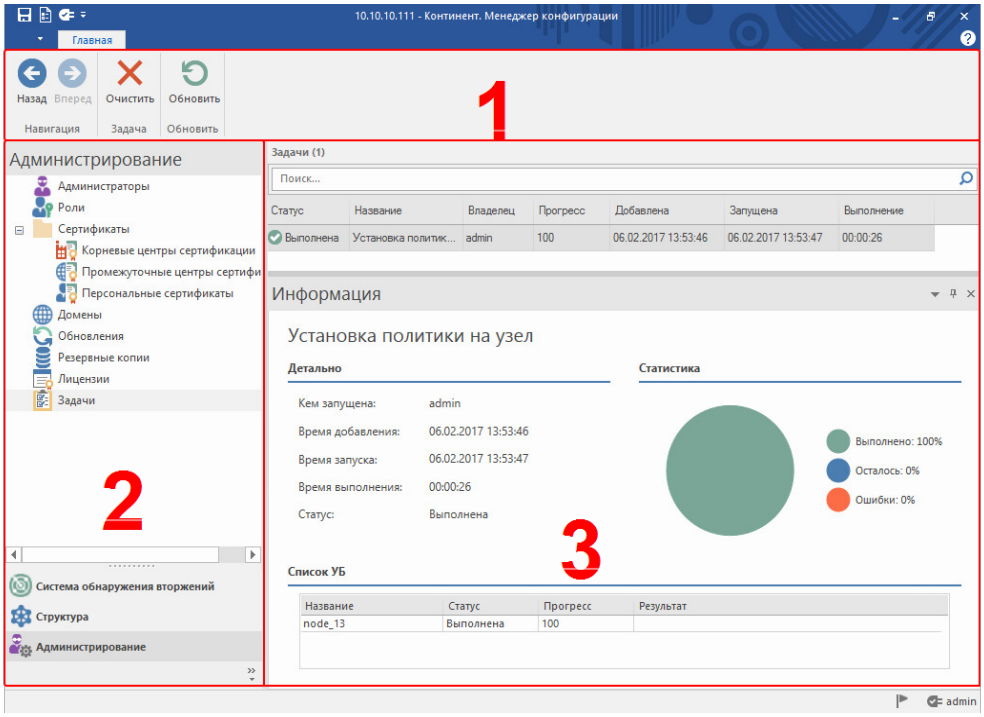
- <Alt> + <F6> — процесс установки локальных изменений, а также процесс установки связи с ЦУС;
- <Alt> + <F8> (только на ЦУС) — процесс подключений УБ к ЦУС.

Примечание. Для возврата к основному экрану нажмите комбинацию клавиш <Alt> + <F1>.

Интерфейс Менеджера конфигурации

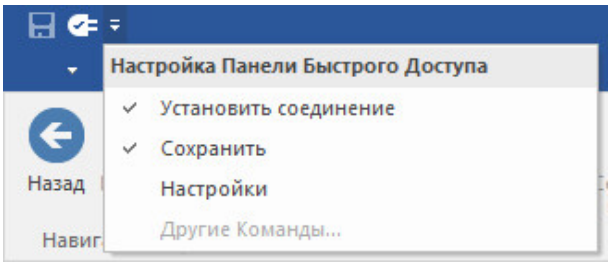
Средством удаленного управления ЦУС, а также другими узлами комплекса является программное обеспечение, входящее в состав комплекса, со специализированным графическим пользовательским интерфейсом.

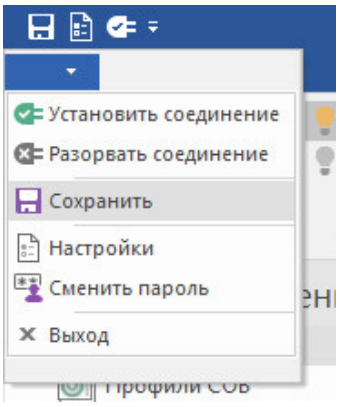
При запуске Менеджера конфигурации и успешной аутентификации на экране монитора будет отражено главное окно приложения.



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

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





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

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

Справа расположена область отображения информации активного подраздела (на рисунке — 3-я область). Данная область может содержать как совокупность структурированных данных, представляемых в виде списков, таблиц и графиков, так и различные функциональные элементы (дополнительные кнопки, активные поля и т. п.). Табличные данные часто имеют свое контекстное меню, вызываемое щелчком правой кнопки мыши, часть команд которого дублирует команды панели инструментов. Двойной щелчок левой кнопки мыши обычно приводит к вызову свойств элемента, аналогично нажатию кнопки "Свойства" на панели инструментов.

Область отображения информации может иметь в своем составе дополнительную зону, по умолчанию отображаемую снизу. В ее верхнем правом углу находятся кнопки управления, с помощью которых можно настроить ее отображение:

Кнопка/ команда меню	**Описание действия**
	Вызов меню управления
Плавающий	Зона отображается при выборе соответствующего подраздела в виде дополнительного окна Windows, которое можно переместить или изменить размеры стандартными средствами. При этом не будут показываться кнопки управления, переход в припаркованный режим осуществляется двойным щелчком мыши по заголовку окна, либо перемещением окна на отображаемые на экране дополнительные кнопки автоматической пристыковки окна к нижней или правой стороне области отображения информации
Припаркованный	Зона отображается при выборе соответствующего подраздела в определенной для нее области. Этот вариант используется по умолчанию
или Скрыть автоматически	Зона перестает отображаться, при этом появляется/дополняется дополнительная панель закрепленных зон. Ее расположение зависит от варианта пристыковки зоны в припаркованном режиме (справа или внизу). Эта панель отображается при любом выбранном разделе. Раскрытие зоны осуществляется при наведении мыши на соответствующий заголовок панели закрепленных зон
или Скрыть	Зона перестает отображаться до смены активного подраздела

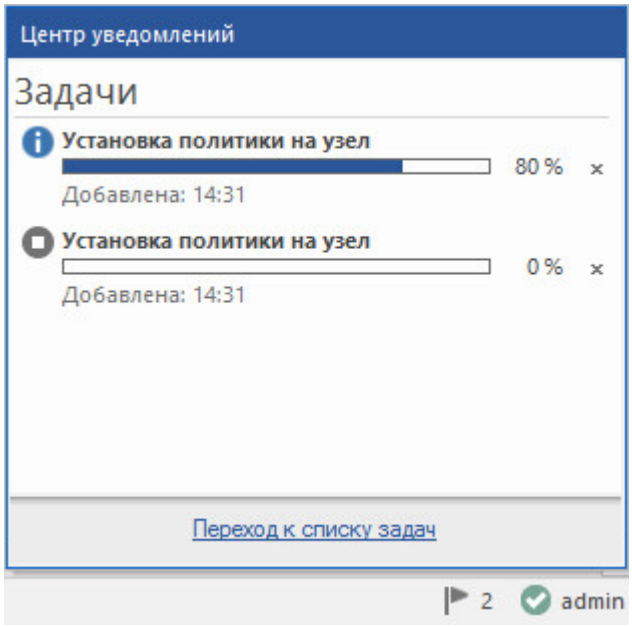
Границы областей списка разделов и отображения информации можно изменять с помощью мыши.

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

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

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

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



Сертификаты безопасности

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

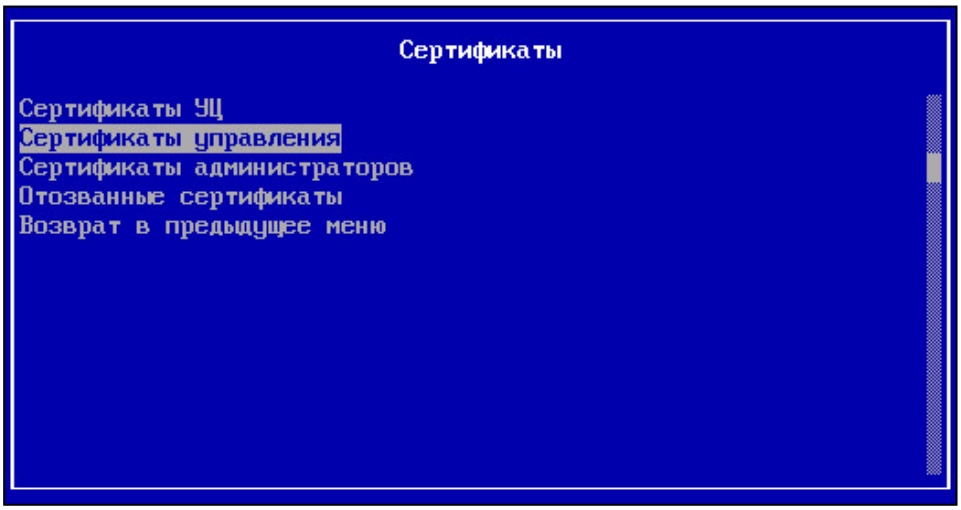
ЦУС, помимо этого, позволяет осуществлять выпуск и экспорт сертификатов.

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".



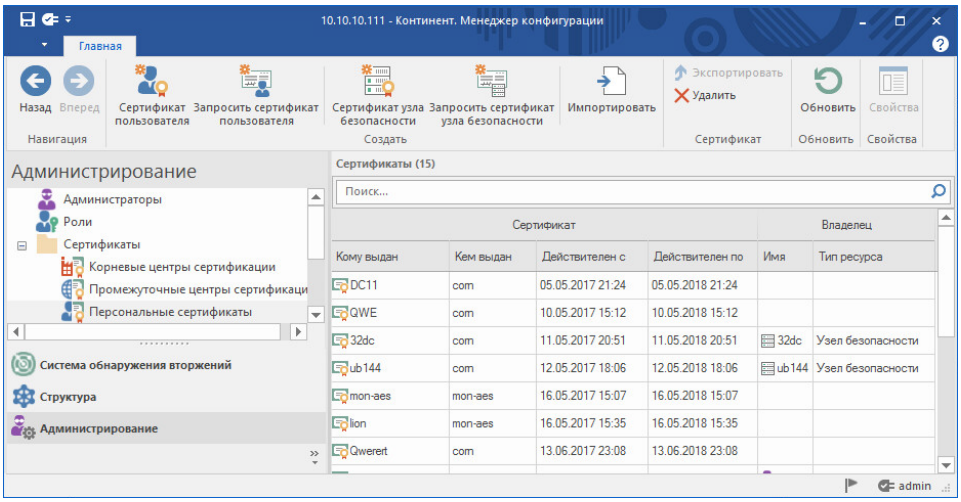
2. Выберите нужный тип сертификатов и нажмите клавишу <Enter>.

   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 Менеджер конфигурации и перейдите в раздел "Администрирование".
2. Для просмотра списка корневых сертификатов выберите в меню слева подраздел "Корневые центры сертификации", для просмотра сертификатов пользователя или УБ — "Персональные сертификаты".



В правой части экрана появится список установленных сертификатов.

Создание сертификатов управления

Создание сертификата управления ЦУС осуществляется на этом ЦУС как локально (см. ниже), так и в Менеджере конфигурации (см. стр. **131**). В случае УБ необходимо сначала создать запрос на сертификат управления посредством его локального управления (см. стр. **128**), а потом выпустить сертификат на ЦУС (см. стр. **130**).

Создание запроса на сертификат управления УБ

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

Для создания запроса на сертификат управления УБ средствами локального управления:

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" — это 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 Менеджер конфигурации и перейдите в раздел "Администрирование".

2. В списке сертификатов выберите "Персональные сертификаты".

   В правой части экрана появится список установленных персональных сертификатов.

3. Нажмите кнопку "Сертификат узла безопасности" на панели инструментов.

   На экране появится окно "Сертификат узла безопасности".

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

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

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

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

Выпуск сертификатов управления ЦУС

Для создания сертификата управления ЦУС средствами локального управления:

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

   На экране появится окно "Сертификаты управления".
2. Нажмите клавишу <F2>.

   На экране появится меню "Выпуск сертификата".
3. Выберите пункт "Выпуск сертификата управления для ЦУС" и нажмите клавишу <Enter>.

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

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

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

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

   Будет выполнен возврат в окно "Сертификаты управления". В окне отобразится созданный сертификат управления ЦУС.
8. Нажмите клавишу <Esc>.

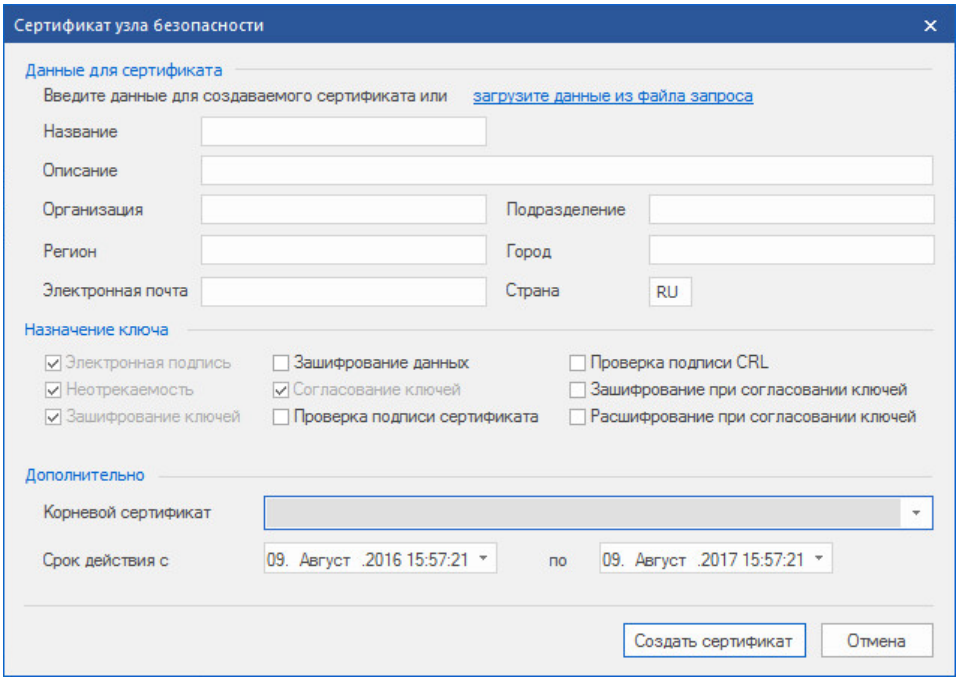
   Будет выполнен возврат в меню "Сертификаты".
9. Для возврата в главное меню локального управления нажмите клавишу <Esc>.

Для создания сертификата управления ЦУС в Менеджере конфигурации:

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

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

   На экране появится окно "Сертификат узла безопасности".



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

   На экране появится информационное сообщение о необходимости выполнить переинициализацию биологического ДСЧ.
7. Следуйте указаниям на экране и дождитесь завершения процесса накопления энтропии.

   На экране появится окно установки пароля на доступ к ключевому контейнеру.
8. 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.
9. 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.

Создание сертификатов пользователя

На ЦУС возможно создание сертификата администратора.

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

После инициализации и настройки ЦУС сертификат можно создавать и в Менеджере конфигурации.

Для создания сертификата администратора средствами локального управления:

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

   На экране появится окно "Сертификаты".

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

   На экране появится окно "Сертификаты администраторов".

3. Нажмите клавишу <F2>.

   На экране появится меню "Выпуск сертификата".

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

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

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

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

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

   На экране появится окно "Атрибуты идентификации".

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

   На экране появится запрос на ввод пароля к ключевому контейнеру.

8. Введите пароль и нажмите клавишу <Enter>.

   На экране появится окно для ввода названия ключевого контейнера.

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

   Появится сообщение об успешной записи запроса на носитель.

10. Нажмите клавишу <Enter>.

    Появится список созданных корневых сертификатов.

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

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

12. Нажмите клавишу <Enter>.

    Будет выполнен возврат в окно "Выпуск сертификата".

13. Нажмите клавишу <Esc>.

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

14. Нажмите клавишу <Esc>.

    Будет выполнен возврат в меню "Сертификаты".

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

Для создания сертификата администратора в Менеджере конфигурации:

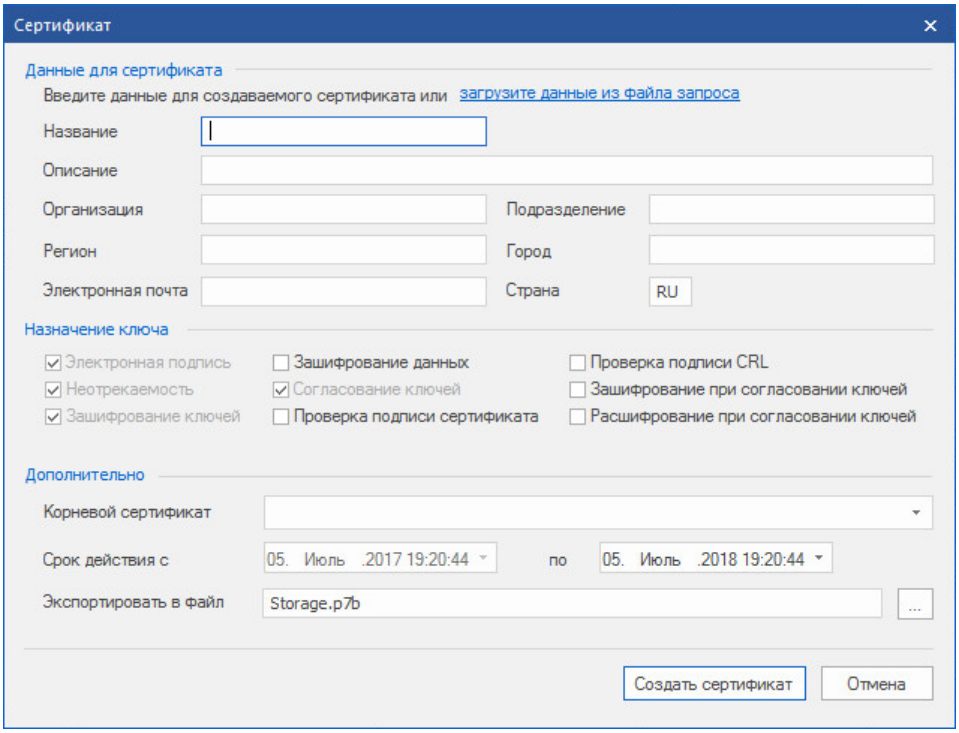
1. Откройте Менеджер конфигурации и перейдите в раздел "Администрирование".

2. В списке сертификатов выберите "Персональные сертификаты".

   В правой части экрана появится список установленных персональных сертификатов.

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

   На экране появится окно "Сертификат".



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

   На экране появится информационное сообщение о необходимости выполнить переинициализацию биологического ДСЧ.
7. Следуйте указаниям на экране и дождитесь завершения процесса накопления энтропии.

   На экране появится окно установки пароля на доступ к ключевому контейнеру.
8. 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.
9. 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 пользователя

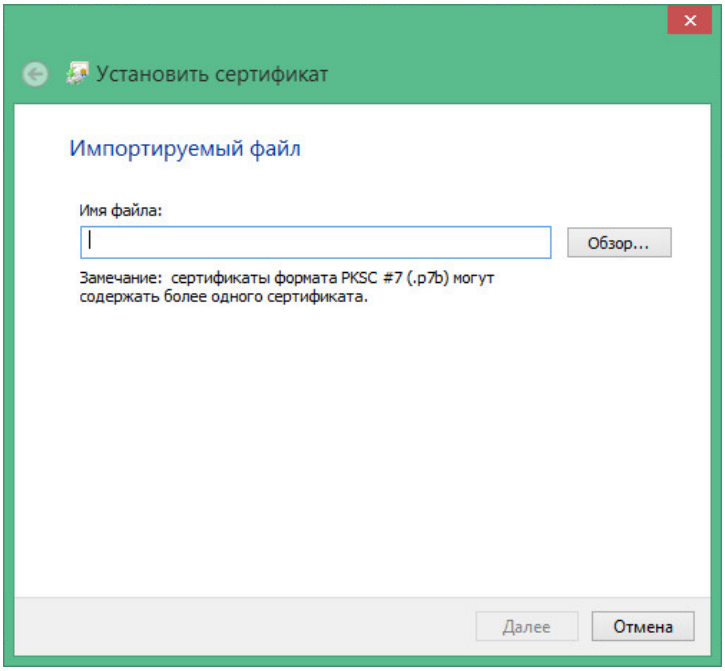
Для выполнения процедуры аутентификации администратора в Менеджере конфигурации с использованием сертификата необходимо установить сертификат в хранилище учетной записи пользователя. Для этого можно использовать ПО "Код Безопасности CSP", входящее в состав комплекса.

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.



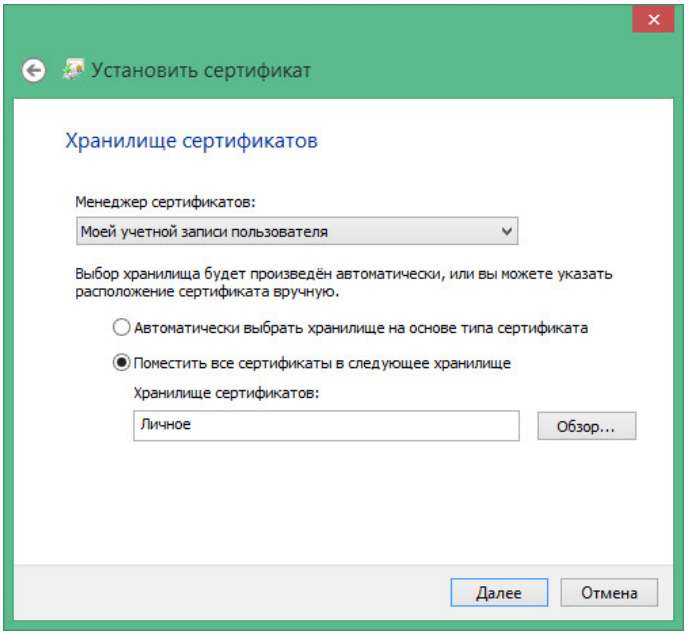
3. Вставьте носитель с файлом сертификата и нажмите кнопку "Обзор".

   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".

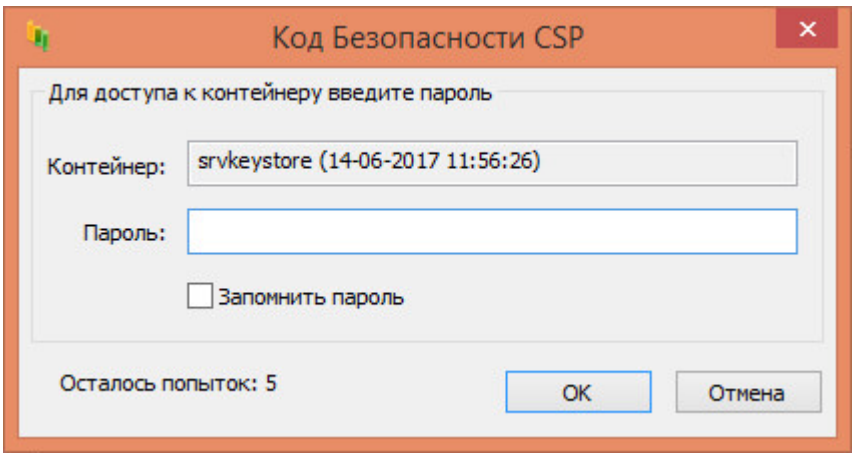
   На экране появится завершающее окно мастера установки сертификата.

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".

Экспорт сертификатов

Для экспорта сертификата в Менеджере конфигурации:

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

   В правой части экрана появится список установленных сертификатов.

3. Выберите нужный сертификат и нажмите кнопку "Свойства" на панели инструментов.

   На экране появится окно "Сертификат".

4. Перейдите на закладку "Состав" и нажмите кнопку "Копировать в файл..." внизу окна.

   На экране появится окно мастера экспорта сертификатов.

5. Нажмите кнопку "Далее" ("Next") внизу окна.

   На экране появится окно выбора формата экспортируемого файла.

6. Выберите любой формат и нажмите кнопку "Далее" ("Next").

   На экране появится окно ввода имени экспортируемого файла.

7. Нажмите кнопку "Обзор" ("Browse").

   На экране появится окно "Сохранение" ("Save").

8. Выберите место для сохранения файла, укажите имя файла и нажмите кнопку "Сохранить" ("Save").

   На экране появится окно с прописанным местом и именем экспортируемого файла.

9. Нажмите кнопки "Далее" ("Next") и "Готово" ("Finish").

   После успешного экспорта сертификата появится соответствующее сообщение.

10. Нажмите кнопку "ОК" в окне сообщения.

Импорт сертификатов и ключей безопасности

Для импорта сертификатов 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>.

Для импорта сертификатов в Менеджере конфигурации:

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

   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" ("Open").

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

   Список установленных сертификатов будет обновлен.

Для импорта ключей безопасности:

1. В меню "Сертификаты" локального управления выберите нужный тип сертификатов и нажмите клавишу <Enter>.
2. Вставьте внешний носитель в USB-разъем для импорта с него файлов, нажмите клавишу <F3>, выберите файл запроса (continent-ID.req, где "ID" — это серийный номер компонента комплекса) и нажмите клавишу <Enter>.

   На экране появится окно для выбора ключевого контейнера.
3. Выберите нужный контейнер и нажмите клавишу <Enter>.

   На экране появится окно для ввода пароля ключевого контейнера.
4. Введите пароль от контейнера и нажмите клавишу <Enter>.

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

Смена сертификата управления

Для смены сертификата управления компонента комплекса:

1. Создайте новый сертификат управления с помощью локального управления или Менеджера конфигурации (см. стр. **128**).
2. Откройте Менеджер конфигурации 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 верхнем левом углу Менеджера конфигурации, и установите политику на этот компонент комплекса (см. стр. **51**).

9. Если смена сертификата управления происходит на ЦУС, то по завершению выполнения задачи по установке политики на ЦУС установите политики на подчиненные ему узлы комплекса.

Настройки локального управления

При локальном управлении компонентом комплекса доступны следующие рубрики в "Меню настроек":

1. Системное время (см. стр. **35**).
2. Настройки загрузчика (позволяет сменить код загрузчика – пароль в GRUB (по умолчанию пароль — "Cont-4.X"(без кавычек)).
3. Журналирование (см. стр. **38**).
4. Последовательная консоль (см. ниже).
5. Сеть (см. стр. **29**).
6. Управление многоуровневой структурой (см. стр. **73**).
7. Мониторинг (см. стр. **139**).

Для подключения ноутбука через консольный порт УБ или ЦУС:

> **Примечание.** Для подключения через консольный порт необходимо в BIOS УБ или ЦУС включить соответствующие параметры в соответствии с Инструкцией по настройке параметров безопасности платформ.

1. Подключите консольный порт УБ или ЦУС кабелем 8P8C (RJ-45)– DB-9 к 9-контактному последовательному порту на ноутбуке.
2. В главном меню УБ или ЦУС выберите пункт "Настройки" и нажмите клавишу <Enter>.

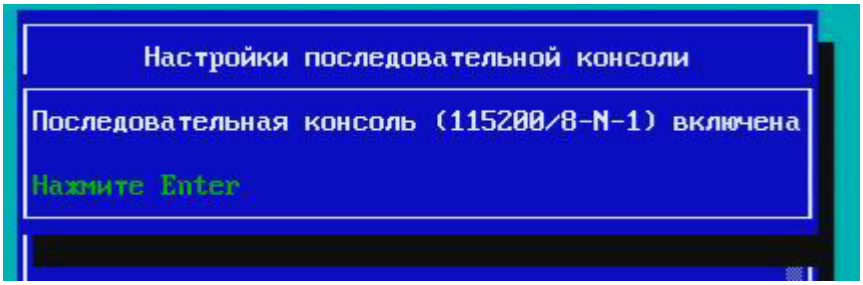
   На экране появится окно "Меню настроек".

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

   На экране появится окно "Настройки последовательной консоли".

4. Выберите пункт "Включить последовательную консоль" и нажмите клавишу <Enter>.

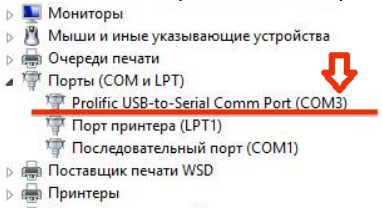
   На экране появится сообщение о включении последовательной консоли, содержащее информацию о рекомендуемой скорости передачи и количестве бит в информационном пакете.



5. Нажмите клавишу <Enter>.

6. На ноутбуке узнайте номер используемого COM-порта. Для этого в зависимости от используемой ОС:

Windows	Linux
Вызовите Диспетчер устройств, к примеру, нажав комбинацию клавиш "Win"+"R" и введя "mmc devmgmt.msc"	В консоли введите "dmesg | grep ttyS attached"

Выберите пункт "Порты(COM и LPT)" и определите № используемого COM-порта 	Определите № используемого COM-порта
	`dmesg | grep ttyS attached`
	`[32364.879561] usb 1-1.2:`
	`p12303 converter now attached to ttyS0`
	`[34517.734338] usb 1-1.4:`
	`ch341-uart converter now attached to ttyS1`

7. На ноутбуке запустите программный эмулятор терминала (к примеру, открытое ПО Putty, лицензия MIT) и настройте параметры подключения:

Параметр	Показатель
№ COM-порта	См. п.6
Тип подключения	Serial
Скорость передачи информации	115200 бит/с
Количество бит в информационном пакете	8
Проверка бита на четность	Отсутствует
Количество стоп-битов	1

8. Нажмите в эмуляторе кнопку "OPEN" или "Соединиться".

   Будет осуществлена попытка подключения. Если она пройдет успешно, то в терминале эмулятора на ноутбуке будет отображено локальное меню УБ или ЦУС.

Для хранения настроек мониторинга на внешнем сервере:

Примечание. В данной процедуре настраивается доступ к серверу с СУБД PostgreSQL для хранения конфигурации системы мониторинга (настройки узлов, статистическая информация по мониторингу).

Внимание! Версия PostgreSQL на внешнем сервере должна совпадать (вплоть до минорного значения) с версией СУБД на ЦУС (на момент поставки комплекса была установлена PostgreSQL версии 9.5.4).

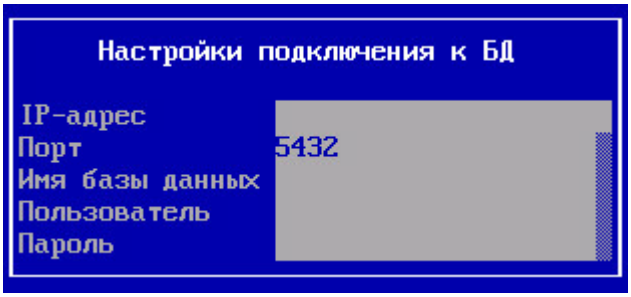
1. В главном меню выберите пункт "Настройки" и нажмите клавишу <Enter>.

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

   На экране появится окно "Настройки мониторинга".
3. Выберите пункт "Внешняя БД" и нажмите клавишу <Enter>.

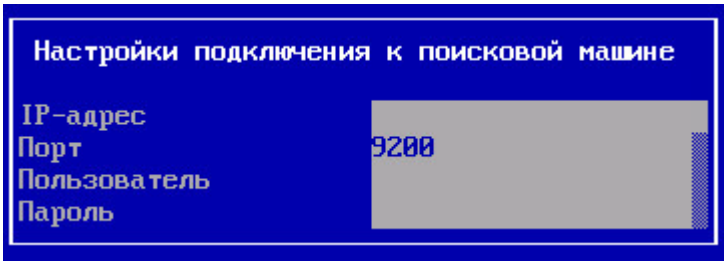
   На экране появится окно "Внешняя БД".
4. Выберите пункт "Настройки подключения" и нажмите клавишу <Enter>.

   На экране появится окно "Настройки подключения к БД".



5. Введите требуемые IP-адрес БД и аутентификационные данные для подключения к внешней базе данных, а затем нажмите клавишу <Enter>.

   На экране появится окно "Настройки подключения к поисковой машине".



6. Введите требуемые IP-адрес БД и аутентификационные данные для подключения к поисковой машине, а затем нажмите клавишу <Enter>.

   Будет осуществлен запрос к поисковой машине. Дождитесь сообщения об успешном завершении операции.

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

   Дождитесь завершения операции.

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
Регистрация УБ в домене (централизованная и локальная)	+	+	-	-
Управление сетевыми настройками УБ (централизованное и локальное)	+	+	0	0
Управление настройками безопасности УБ	+	0	+	0
Управление обновлениями	+	+	0	0
Создание резервной копии конфигурации домена (централизованное)	+	+	+	+

Функция/настройка	ГА	АС	АБ	АА
Управление конфигурацией домена (централизованное и локальное)	+	-	-	-
Управление политиками				
Установка политик (централизованная и локальная)	+	-	+	-
Управление политиками СОВ	+	0	+	0
Управление иерархической структурой				
Построение иерархической структуры доменов (централизованно и локально)	+	0	+	0
Локальное управление				
Работа с аварийным меню	+	-	+	-
Дистанционный доступ к локальному меню (ssh)	-	-	-	-
Управление журналами	+	-	+	-
Просмотр журналов	+	+	+	+
Диагностика УБ	+	+	-	-
Управление локальными политиками	+	+	+	-
Изменение пароля встроенного администратора	+	-	-	-
Повторная инициализация	+	-	-	-
Завершение работы УБ	+	+	+	-
Страницы системы мониторинга				
Панель мониторинга	+	+	+	+
Журнал аудита	+	+	+	+
События СОВ	+	-	+	-
События мониторинга	+	+	+	-
Статистика	+	+	+	+
Структура	+	+	+	-
Управление группами	+	+	+	-
Источники информации для настройки виджетов мониторинга				
Мониторинг	+	+	+	-
Система безопасности/СОВ	+	-	+	-
Система аудита	+	+	+	+
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-сертификата	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 всех указанных условий.

alert	Генерировать сигнал с использованием выбранного метода и записать информацию о пакете в журнальный файл
pass	Пропустить пакет
drop	Отбросить (уничтожить) пакет

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 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|";)

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 портов также поддерживается оператор отрицания. Пример правила, которому будут соответствовать все пакеты TCP, адресованные в любые порты, за исключением портов X Window (6000 – 6010), IP-адресов сети класса C 192.168.1.0:

drop tcp any any -> 192.168.1.0/24 !6000:6010

Оператор направления

Оператор направления -> показывает 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

Опции MetaData

msg

Опция **msg** указывает на необходимость включения текстового сообщения в запись журнального файла или дампа пакета. Представляет собой текстовую строку с использованием символа обратной косой черты (\) в качестве escape-символа для задания символов, имеющих специальное значение в правилах (например символ ;).

Формат:

msg: "<текст сообщения>";

sid

Опция **sid** предназначена для идентификации правила. **Sid** следует использовать вместе с опцией **rev** (см. ниже). В правилах глобального значения используются значения **sid** в диапазоне от 100 до 1 000 000. Значения менее 100 зарезервированы, а значения, превышающие 1 000 000, предназначены для локального использования (идентификации ваших собственных правил).

Файл sid-msg.map содержит список сигналов для различных значений **sid**, используемых правилами. Эта информация может быть полезна при последующей обработке сигналов, поскольку позволяет получить текст сообщения по его идентификатору.

Формат:

sid: <идентификатор правила>;

rev

В опции **rev** указывается значение версии правила, идентифицированного по опции **sid** (см. выше). Эти опции следует использовать совместно.

Формат:

rev: <номер версии>;

Пример правила с идентификатором 1000983 ревизии 1:

alert tcp any any -> any 80 (content:"BOB"; sid:1000983; rev:1;)

classtype

Опция **classtype** используется для классификации атаки.

Стандартная классификация правил:

Имя класса	Описание	Приоритет
attempted-admin	Попытка получения привилегий администратора	Высокий
attempted-user	Попытка получения привилегий пользователя	Высокий
shellcode-detect	Обнаружен исполняемый код	Высокий
successful-admin	Получены права администратора	Высокий
successful-user	Получены права пользователя	Высокий
trojan-activity	Обнаружена сетевая троянская программа	Высокий
unsuccessful-user	Неудачная попытка получения привилегий пользователя	Высокий
web-application-attack	Атака на веб-приложение	Высокий
attempted-dos	Предпринята атака на службы (DoS)	Средний
attempted-recon	Попытка несанкционированной передачи информации (утечка)	Средний
bad-unknown	Непонятный трафик, который может оказаться опасным	Средний
denial-of-service	Обнаружена атака на службы (DoS)	Средний
misc-attack	Прочие атаки	Средний
non-standard-protocol	Зафиксировано использование нестандартного протокола	Средний
rpc-portmap-decode	Обнаружен запрос RPC1	Средний
successful-dos	Успешная атака на службы (DoS)	Средний
successful-recon-largescale	Крупномасштабная утечка информации	Средний
successful-recon-limited	Утечка информации	Средний
suspicious-filename-detect	Обнаружено подозрительное имя файла	Средний
suspicious-login	Попытка входа в систему с использованием подозрительного имени	Средний
system-call-detect	Обнаружен вызов системной функции	Средний
unusual-client-port-connection	Клиент использует необычный порт	Средний
web-application-activity	Доступ к потенциально опасному веб-приложению	Средний
icmp-event	Обычный пакет ICMP	Низкий

Имя класса	Описание	Приоритет
misc-activity	Прочие действия	Низкий
network-scan	Обнаружено сканирование сети	Низкий
not-suspicious	Трафик не является подозрительным	Низкий
protocol-command-decode	Обнаружена обычная команда протокола	Низкий
string-detect	Обнаружена подозрительная строка	Низкий
unknown	Непонятный трафик	Низкий

Формат:

classtype: <имя класса>;

`priority`

Опция **priority** используется для присвоения правилу уровня приоритета. Опция **classtype** присваивает правилу принятый по умолчанию уровень приоритета, который можно изменить с помощью **priority**.

Формат:

priority: <номер приоритета>;

Таблица приоритетов:

Номер	Описание
1	Высокий
2	Средний
3	Низкий
4	Информация

Опции проверки содержимого пакетов

`content`

Опция **content** позволяет пользователю создавать правила для поиска в пакетах определенной информации и выполнения тех или иных действий при ее обнаружении. Для проверки содержимого пакетов используется функция поиска по шаблону Boyer-Moore. Если заданная последовательность данных обнаружена в поле содержимого пакета, проверка считается успешной и выполняется остальная часть правила. Следует помнить, что при поиске учитывается регистр символов.

В одном правиле может присутствовать несколько опций **content**, что позволяет снижать уровень ложных срабатываний за счет более точного задания искомых последовательностей.

Формат:

content: [!] "<строка поиска>";

Если перед опцией помещен знак отрицания (!), правилу будут соответствовать пакеты, не содержащие указанных данных. Такая возможность полезна для генерации сигналов в случае обнаружения пакетов, не содержащих заданной последовательности.

Пример поиска текстовой строки:

alert tcp any any -> any 80 (content:!"GET";)

Аргумент опции может содержать как текст, так и двоичные данные (обычно они указываются между парой символов | и задаются последовательностью шестнадцатеричных представлений байтов).

Пример задания строки поиска, содержащей текст и бинарные данные:

alert tcp any any -> any 139 (content:"|5c 00|P00E|00 5c|";)

Опция **content** может быть дополнена опциями-модификаторами, которые изменяют поведение системы поиска:

- **depth** (размер области поиска);
- **offset** (смещение начала поиска от начала поля данных);
- **distance** (количество пропускаемых байтов после первого найденного соответствия);
- **within** (размер области поиска после первого найденного соответствия);
- **nocase** (без учета регистра символов);
- **rawbytes** (поиск в необработанных данных).

Пример поиска без учета регистра символов:

alert tcp any any -> any 21 (msg:"ROOT"; content:"USER root"; nocase;)

nocase

Опция **nocase** позволяет осуществлять поиск, заданный предыдущей опцией **content** без учета регистра символов.

Формат:

nocase;

rawbytes

Опция **rawbytes** позволяет искать в пакете необработанные (raw) данные, игнорируя декодирование, выполняемое препроцессорами. Опция изменяет поиск данных, указанных предыдущей опцией **content**.

Формат:

rawbytes;

depth

Опция **depth** показывает размер блока данных из пакета, в котором осуществляется поиск, заданный предыдущей опцией content. Например, при **depth 5** будут просматриваться в поисках заданной последовательности только первые 5 байт поля данных в пакете.

Формат:

depth: <количество_байтов>;

offset

Опция **offset** позволяет задать смещение в поле данных пакета, с которого начинается поиск последовательности, заданной предыдущей опцией content. Например, **offset 5** будет начинать поиск, пропустив первые 5 байт поля данных.

Формат:

offset: <количество_байтов>;

distance

Опция **distance** показывает – сколько байтов нужно пропустить после найденной предыдущей опцией **content** строки для начала поиска последовательности, заданной другой опцией **content**.

Формат:

distance: <количество_байтов>;

Пример поиска в поле данных пакета строки вида AB?DEF (знак вопроса означает любой символ):

alert tcp any any -> any any (content: "AB"; content: "DEF"; distance: 1;)

within

Опция **within** показывает размер области поиска для опции **content** от конца предыдущего значения **content**.

Формат:

within: <количество_байтов>;

Пример поиска подстроки FGH в последующих 10 байт после найденной в поле данных подстроки AB:

alert tcp any any -> any any (content: "AB"; content: "FGH"; within:10;)

uricontent

Опция **uricontent** служит для поиска шаблона в нормализованных полях запросов URI. При создании правил, включающих нормализуемые данные (например, %2f или обход каталогов – directory traversal), эти правила не следует использовать.

Эта опция использует тот же набор модификаторов, который применяется для описанной выше опции **content**, и работает совместно с препроцессором HTTP Inspect.

Формат:

uricontent:[!]<строка_шаблона>;

isdataat

С помощью этой опции можно находить и сравнивать данные пакета в указанном диапазоне байтов. Анализ может начинаться с начала пакета либо от последнего найденного фрагмента текста в нем (при использовании тега-модификатора **relative**).
Формат:

isdataat:<диапазон байт>[,relative];

pcre

Опция **pcre** позволяет создавать правила, содержащие регулярные выражения (РВ), совместимые с языком perl. Детальную информацию о РВ см. на сайте http://www.pcre.org.

Формат:

pcre:[!]"(/<строка поиска или РВ>/<РВ>...|m<РВ>)/[ismxAEGRUB]";

Модификаторы в конце правила устанавливают флаги для регулярного выражения.

Модификаторы, совместимые с Perl:

i	Не учитывается регистр символов
s	Метасимволы включают символ перевода строки
m	По умолчанию строка считается одной большой последовательностью символов. При наличии модификатора m специальные символы ^ и $ задают поиск соответствия с начала или с конца каждой новой подстроки (относительно символа перевода строки), а также с начала и с конца пакета
x	Символы пробелов в шаблоне поиска игнорируются, за исключением случаев использования перед таким символом escape-символа или включения пробела в символьный класс (character class)

Модификаторы, совместимые с PCRE:

A	Наличие заданной подстроки проверяется только в начале пакета (аналогично ^)
E	Задает для $ поиск соответствия только в самом конце строки. В том случае, если отсутствует модификатор E, поиск осуществится до символа новой строки
G	Инвертирует трактовку параметров количества повторов (quantifier) так, что если по умолчанию они не являются "жадными" (greedy – число повторов может быть любым, вплоть до максимального), установка знака вопроса (?) вслед за параметром меняет "состояние жадности"

Собственные модификаторы:

R	Задает поиск соответствия относительно конца предыдущего найденного соответствия (аналогично опции **distance:0;**)
U	Задает поиск в декодированном буфере URI (аналогично **uricontent**)
B	Отключает использование декодированного буфера (аналогично **rawbytes**)

Модификаторы R и B не следует использовать совместно.

Пример нечувствительного к регистру символов поиска подстроки BLAX:

alert ip any any -> any any (pcre:"/BLAH/i";)

byte_test

Эта опция позволяет сравнить байт с заданным значением. **Byte_test** может использоваться применительно к двоичным значениям (HEX)или их символьному представлению (ASCII).

Формат:

byte_test: <число_байтов>, [!]<оператор>, <значение>,

<смещение> [,relative] [,<порядок>] [,<тип>, string];

Параметры опции **byte_test**:

Параметр	Описание
число_байтов	Количество байтов, считываемых из пакета
оператор	Операция, выполняемая для сравнения байта с заданным значением: < (меньше), > (больше), = (равно), ! (не равно), & (логическое И), - (логическое ИЛИ). Любой из операторов можно использовать со знаком инверсии (!)
значение	Значение, с которым выполняется сравнение
смещение	Номер байта в поле данных пакета, с которого начинается операция сравнения
relative	Отсчет смещения от конца предыдущего найденного соответствия
порядок	Порядок следования: • big – big endian (старший разряд слева, используется по умолчанию); • little – little endian (старший разряд справа)
тип	Тип считываемых значений: • hex – шестнадцатеричное число; • dec – десятичное число; • oct – восьмеричное число
string	Данные в пакете представлены в символьном формате

Пример сравнения первых 4 байт пакетов со значением 1234, при этом данные в пакете представлены в символьном формате в десятичной системе счисления:

**alert udp any any -> any 1234 (byte_test: 4, =, 1234, 0, dec, string; **

msg: "got 1234!";)

byte_jump

Опция byte_jump сначала определяет размер пропускаемой области данных, преобразуя считанную из пакета информацию в целое число, и затем пропускает соответствующее число байтов, устанавливая указатель, который будет использоваться для следующего считывания информации из пакета. Этот указатель называется detect offset end pointer или doe_ptr.

Формат:

**byte_jump: <число_байтов>, <смещение >, **

**[,relative] [,multiplier <значение>] [,big] [,little][,string] **

[,hex] [,dec] [,oct] [,align] [,from_beginning];

Параметры опции byte_jump:

Параметр	Описание
число_байтов	Количество байтов, считываемых из пакета
смещение	Номер байта в поле данных пакета, с которого начинается обработка
relative	Отсчет смещения от конца предыдущего найденного соответствия
multiplier	Множитель на <значение> для пропуска этого количества байтов
big	Обработка данных со старшего разряда (big endian – используется по умолчанию)
little	Обработка данных с младшего разряда (little endian)
string	Данные в пакете представлены в виде символьной строки (ASCII)
hex	Преобразование строки данных в шестнадцатеричное число
dec	Преобразование строки данных в десятичное число
oct	Преобразование строки данных в восьмеричное число
align	Округление числа конвертируемых байтов по следующей 32-битовой границе
from_beginning	Отсчет байтов от начала поля данных пакета (не от текущей позиции в пакете)

Опции проверки служебных полей пакетов

ack

Опция **ack** используется для проверки номеров подтверждений TCP.

Формат:

ack: <номер_подтверждения>;

dsize

Опция **dsize** используется для проверки размера поля данных пакета. Данная опция позволяет детектировать пакеты аномальных размеров, которые достаточно часто применяются для переполнения буферов.

Формат:

dsize: [<>]<число_байт>[<><число_байт>];

Условие **dsize** не будет выполняться для пакетов перестроения потока (stream rebuilt packet), независимо от их размера.

Примечание. Опция **dsize** не контролирует пакеты перестроения потока (stream rebuilt packet), независимо от их размера.

Приведенный ниже пример позволяет детектировать пакеты размером от 300 до 400 байт:

dsize:300<>400;

flags

Опция **flags** используется для проверки наличия заданных флагов TCP. Список проверяемых флагов:

F — FIN (младший бит поля флагов TCP);

S — SYN;

R — RST;

P — PSH;

A — ACK;

U — URG;

1 — резервный бит 1 (старший бит байта TCP Flags);

2 — резервный бит 2;

0 — отсутствие флагов TCP.

Перечисленные ниже модификаторы позволяют менять поведение опции:

+ — соответствует, если установлены указанные биты;

* — соответствует, если установлен любой из указанных битов;

! — соответствует, если не установлен ни один из указанных битов.

Для создания правил обработки пакетов инициирования сессий (например, пакеты ECN, где установлены флаг SYN и резервные биты 1 и 2) можно задавать маски опций. Маска отделяется от проверяемых флагов запятой. Например, для детектирования SYN-пакетов независимо от значений резервных битов можно задать маску S,12.

Формат:

flags:[!|*|+]<FSRPAU120>[,<FSRPAU120>];

Примечание. Порядок следования флагов значения не имеет.

Для детектирования пакетов с флагами SYN и FIN независимо от значений резервных битов 1 и 2 может использоваться правило:

alert tcp any any -> any any (flags:SF,12;)

flow

Опция **flow** используется вместе со сборкой потоков TCP и позволяет применять правило лишь к некоторым направлениям потока трафика. В результате можно создавать правила, которые будут относиться только к клиентам или только к серверам, что дает возможность легко дифференцировать пакеты, относящиеся к клиентам из $HOME_NET, просматривающим веб-страницы, от пакетов, относящихся к серверам, расположенным в $HOME_NET.

Формат:

**flow: [(established|stateless)] **

**[,(to_client|to_server|from_client|from_server)] **

[,(no_stream|only_stream)]

Параметры опции flow:

Параметр	Описание
to_client	Контроль трафика к клиенту
to_server	Контроль трафика к серверу
from_client	Контроль трафика от клиента
from_server	Контроль трафика от сервера
established	Контроль организованных соединений TCP
stateless	Контроль независимо от состояния обработчика потока (stream processor), что может быть полезно для детектирования пакетов, направленных на аварийное завершение работы системы
no_stream	Игнорирование пакетов перестроения потока (полезно для опций dsize и stream4)
only_stream	Контроль только пакетов перестроения потока

Примечание 1. Параметр **established** заменяет опцию **flags: A+**, часто используемую применительно к уже организованным соединениям TCP.

Примечание 2. Параметр **stateless** может быть полезен для детектирования пакетов, направленных на аварийное завершение работы системы.

flowbits

Опция **flowbits** используется совместно со средствами отслеживания соединений препроцессора **Flow**. Это позволяет создавать правила для сеансов транспортного уровня. Опция **flowbits** наиболее полезна для сеансов TCP.

Для опции **flowbits** поддерживаются 7 параметров, большинство из которых требует указания определенного пользователем имени специфического состояния, которое будет проверяться. При создании таких имен следует ограничиваться буквами латиницы, цифрами, а также символами точки, дефиса и подчеркивания.

Формат:

**flowbits: [set|unset|toggle|isset,reset,noalert] **

[,<название_состояния>];

Параметры опции flowbits:

Параметр	Описание
set	Устанавливает (определяет) указанное состояние для текущего потока данных
unset	Отменяет указанное состояние для текущего потока данных
toggle	Устанавливает указанное состояние, если оно еще не установлено, и отменяет установленное ранее
isset	Проверяет, установлено ли указанное состояние
isnotset	Проверяет, что указанное состояние не установлено
noalert	Отключает для правила генерацию сигнала тревоги независимо от остальных опций детектирования

fragbits

Опция **fragbits** используется для проверки наличия в заголовке IP битов фрагментации и резервного бита. Опция поддерживает следующие параметры:

M — More Fragments (проверять бит MF);

D — Don't Fragment (проверять бит запрета фрагментации);

R — Reserved Bit (проверять резервный бит).

Для изменения характера проверки могут использоваться перечисленные ниже модификаторы:

+ — соответствует, если установлены указанные биты;

* — соответствует, если установлен любой из указанных битов;

! — соответствует, если не установлен ни один из указанных битов.

Формат:

fragbits:[+*!]<[MDR]>

fragoffset

Опция **fragoffset** позволяет сравнивать смещение фрагмента дейтаграммы IP с заданным десятичным значением.

Формат:

fragoffset:[<|>]<целое число>

К примеру, для отсечения всех первых фрагментов можно использовать опцию **fragbits** и просмотр бита More fragments при установке **fragoffset: 0**:

**alert ip any any -> any any (msg: "First Fragment"; **

fragbits: M; fragoffset: 0;)

icode

Опция **icode** используется для проверки значения кода ICMP.

Формат:

icode: [<|>]<значение>[<><значение>];

В приведенном ниже примере детектируются сообщения ICMP со значением кода более 30:

icode:>30;

icmp_id

Опция **icmp_id** служит для проверки значений идентификаторов ICMP. Такая проверка может оказаться полезной для обнаружения некоторых программ организации скрытых каналов, которые используют для передачи информации статические поля ICMP. Подключаемый модуль был создан, в частности, для детектирования DdoS-агентов stacheldraht.

Формат:

icmp_id:<значение>;

Пример проверки наличия нулевого значения в поле ICMP ID:

icmp_id:0;

icmp_seq

Опция **icmp_seq** используется для проверки порядковых номеров ICMP. Такая проверка может оказаться полезной для обнаружения некоторых программ организации скрытых каналов, которые используют для передачи информации статические поля ICMP. Подключаемый модуль был создан, в частности, для детектирования DdoS-агентов stacheldraht.

Формат:

icmp_seq: <значение>;

Пример детектирования сообщения ICMP с порядковым номером 0:

icmp_seq:0;

id

Опция **id** используется для проверки наличия в поле IP ID заданного значения. Некоторые программы (эксплойты, сканеры, старые программы) устанавливают в этом поле определенное значение (например, число 31337 весьма популярно среди хакеров).

Формат:

id:<значение>;

ipopts

Опция **ipopts** позволяет проверять наличие в заголовке IP указанных опций. Поддерживается проверка следующих опций IP:

rr - Record route (запись маршрута);

eol - End of list (завершение списка опций);

nop - No op (нет опции);

ts - Time Stamp (временная метка);

sec - IP security option (опция безопасности);

lsrr - Loose source routing (нежестко заданный отправителем маршрут);

ssrr - Strict source routing (жестко заданный отправителем маршрут);

satid - Stream identifier (идентификатор потока) (устаревшая опция);

any - any IP options are set (любые опции).

Примечание. Опция **satid** устарела и не должна использоваться.

Чаще всего проверяются опции **ssrr** и **lsrr**, которые не используются в распространенных приложениях интернета.

Формат:

ipopts:<rr|eol|nop|ts|sec|lsrr|ssrr|satid|any>;

Внимание! В правиле недопустимо наличие нескольких опций **ipopts**.

iprep

Опция **iprep** позволяет проверять наличие IP-адреса в различных репутационных списках (инфицирован, бот, спам и т. д.).

Формат:

iprep:<направление>,<список>,<оператор>,<значение>;

Параметры опции iprep:

Параметр	Описание
направление: any src dst both	 проверка IP-адреса отправителя или получателя проверка IP-адреса отправителя проверка IP-адреса получателя проверка IP-адреса отправителя и получателя
список	короткое имя репутационного списка
оператор	<, >, =
значение	показатель репутации: 1–127

Пример использования:

alert ip $HOME_NET any -> any any (msg:"IPREP internal host talking to CnC server"; flow:to_server; iprep:dst,CnC,>,30; sid:1; rev:1;)

ip_proto

Опция **ip_proto** позволяет проверять идентификатор протокола в заголовке IP. Список протоколов можно найти в файле /etc/protocols.

Формат:

ip_proto:[!><] <имя или номер протокола>;

Пример детектирования трафика IGMP:

alert ip any any -> any any (ip_proto:igmp;)

itype

Опция **itype** используется для проверки типа сообщения ICMP.

Формат:

itype:[<|>]<идентификатор_типа>[<><идентификатор_типа>];

В приведенном ниже примере детектируются сообщения ICMP со значением идентификатора от 12 до 30:

itype:12<>30;

rpc

Опция **rpc** используется для проверки приложений RPC, номеров версий и процедур в запросах SUNRPC CALL.

Для номера версии и процедуры допускается использование шаблона 0, которому соответствуют любые значения номеров.

Формат:

**rpc: <номер приложения>, **

[<номер версии>|*], [<номер процедуры>|*]>;

Внимание! В силу особенностей машины поиска соответствий детектирование по опции **rpc** работает несколько медленнее, чем поиск значений RPC с использованием опции **content**.

Пример детектирования запросов an RPC portmap GETPORT:

alert tcp any any -> any 111 (rpc: 100000,*,3;);

sameip

Опция **sameip** позволяет детектировать пакеты с совпадающими IP-адресами для получателя и отправителя.

Формат:

sameip;

Пример генерации сигнала при совпадении IP-адресов получателя и отправителя.

alert ip any any -> any any (sampeip;)

`seq`

Опция **seq** служит для проверки значения порядковых номеров TCP.

Формат:

seq:<номер_сегмента>;

Приведенный ниже пример проверяет равенство порядкового номера TCP нулю.

seq:0;

`tos`

Эта опция позволяет проверять в пакетах поле IP TOS (тип обслуживания).

Формат:

tos:[!]<значение>;

В приведенном ниже примере проверяется отличие значения поля TOS от 4:

tos:!4;

`ttl`

Опция **ttl** используется для проверки времени жизни дейтаграмм IP. Эта опция может быть полезна при детектировании попыток трассировки с помощью команды **traceroute**.

Формат:

ttl:[[<число_секунд>-]><=]<число_секунд>;

Пример ограничения времени жизни дейтаграмм IP до 2 секунд:

ttl:<3;

Пример детектирования пакетов со значением TTL от 3 до 5:

ttl:3-5;

`window`

Опция **window** используется для проверки размера окна TCP.

Формат:

window:[!]<число_байт>;

Опции после детектирования

`logto`

Опция **logto** используется для записи всех соответствующих правилу пакетов в специальный файл. Опция не будет работать, если программа обнаружения находится в режиме ведения бинарного журнала (binary logging mode).

Формат:

logto:"filename";

`session`

Опция **session** позволяет получить пользовательскую информацию из сеансов TCP. Это очень удобно, к примеру, для обработки сохраненных файлов (формат pcap).

Опция может использоваться с двумя параметрами — **printable** (выводить только печатаемые символы) и **all** (выводить все). Во втором случае непечатаемые символы выводятся в виде шестнадцатеричных кодов.

Формат:

session: [printable | all];

Внимание! Использование опции **session** может существенно замедлять работу программы поиска.

Пример правила для FTP-сессии:

log tcp any any <> any 21 (session:printable;)

resp

Ключевое слово **resp** используется для попытки закрыть сессию при генерации сигнала.

Параметры опции **resp**:

Параметр	Описание
rst_snd	Отправлять пакеты TCP-RST передающему сокету
rst_rcv	Отправлять пакеты TCP-RST принимающему сокету
rst_all	Отправлять пакеты TCP-RST в обоих направлениях
icmp_net	Передавать пакеты ICMP_NET_UNREACH отправителю
icmp_host	Передавать пакеты ICMP_HOST_UNREACH отправителю
icmp_port	Передавать пакеты ICMP_PORT_UNREACH отправителю
icmp_all	Передавать все перечисленные выше пакеты ICMP отправителю

Перечисленные в таблице опции можно комбинировать для передачи множества откликов одному IP-адресу.

Формат:

resp: <параметр>[,<параметр>[,<параметр>]];

Приведенное ниже правило будет пытаться сбрасывать попытки соединений TCP с портом 1524 в обоих направлениях:

alert tcp any any -> any 1524 (flags:S; resp:rst_all;)

Внимание! Пользоваться опцией **resp** следует с осторожностью, так как можно достаточно легко создать бесконечный цикл типа приведенного ниже:
alert tcp any any -> any any (resp:rst_all;)

react

Основным назначением этой опции является блокирование нежелательных сайтов. Доступна возможность активного закрытия соединений и/или передача в пользовательскую программу соответствующего сообщения. Для опции поддерживаются два основных модификатора:

- **block** — закрыть соединение и передать пользователю видимое уведомление;
- **warn** — передать пользователю видимое предупреждение.

Кроме основных модификаторов опция может использоваться с дополнительными параметрами:

- **msg** — включить заданный текст в передаваемое пользователю сообщение;
- **proxy:<номер порта>** — использовать порт proxy для передачи пользователю видимого предупреждения.

Дополнительные аргументы разделяются запятыми.

Внимание! Опция **react** должна использоваться последней в списке опций правила.

Формат:

react: <react_basic_modifier [, react_additional_modifier]>;

Пример блокирования нежелательных сайтов с генерацией для пользователя соответствующего сообщения:

**alert tcp any any <> 192.168.1.0/24 80 (content: "bad.htm"; **

msg: "Not for children!"; react: block, msg;)

Внимание! При использовании опции **react** следует избегать возникновения петель.

tag

Опция **tag** позволяет записывать в журнальные файлы не только пакет, который вызвал срабатывание правила. После срабатывания правила весь последующий трафик для данной пары "отправитель — получатель" будет помечаться, а отмеченный трафик можно проконтролировать для последующего анализа.

Формат:

tag: <способ>, <количество>, <счетчик>, [direction]

Опция **tag** функционирует двумя способами:

- **session** — запись пакетов сессии, для которых сработало правило;
- **host** — запись пакетов с IP-адреса, который вызвал срабатывание правила (с учетом направления).

Длительность работы опции **tag** ограничивается по одному из видов счетчика:

- **packets** — пометить **<количество>** пакетов;
- **seconds** — помечать пакеты в течение **<количество>** секунд.

В параметре **<количество>** содержится количество единиц, указанных в параметре **<счетчик>**, которые нужно передать процедуре журналирования.

Внимание! Пакеты, для которых сработало правило с опцией **tag**, помечаться не будут.

Пример записи пакетов в течение первых 10 секунд любого сеанса telnet:

alert tcp any any -> any 23 (flags:s,12; tag:session,10,seconds;)

Примеры фильтров сигнатурного анализатора

Рассмотрим примеры строки настройки фильтра сигнатурного анализатора.

Пример 1.

```
Фильтр: src port 80
```

Анализируются все пакеты, поступающие с порта 80.

Пример 2.

```
Фильтр: src host <IP-адрес>
```

Анализируются все пакеты, отправителем которых является источник с указанным в фильтре IP-адресом.

Пример 3.

```
Фильтр: dst host <IP-адрес>
```

Анализируются все пакеты, получателю которых соответствует указанный в фильтре IP-адрес.

Пример 4.

```
Фильтр: dst net <адрес подсети>
```

Анализируются все пакеты, поступающие в указанную подсеть.

Пример 5.

```
Фильтр: not host <IP-адрес>
```

Из анализа исключаются пакеты, содержащие указанный IP-адрес.

Пример 6.

```
Фильтр: net <network> and tcp port 21
```

Анализируется трафик, принадлежащий сети <network> и передаваемый по протоколу TCP с использованием порта 21.

Полный перечень доступных по SNMP данных

Вендорские OID "Континент":

Код параметра	Параметр	Описание
1.3.6.1.4.1.34849.1.1.1.1	**ips**	**Счетчики СОВ**
1.3.6.1.4.1.34849.1.1.1.1.2	ipsComponentState	Состояние системы СОВ: 1 - работает, 0 – не работает
1.3.6.1.4.1.34849.1.1.1.1.3	ipsPcktsCount	Количество пакетов, прошедших через СОВ с момента ее запуска
1.3.6.1.4.1.34849.1.1.1.1.4	ipsPcktsCount1Min	Количество пакетов, прошедших через СОВ за последнюю минуту
1.3.6.1.4.1.34849.1.1.1.1.5	ipsPcktsCount5Min	Количество пакетов, прошедших через СОВ за последние 5 минут
1.3.6.1.4.1.34849.1.1.1.1.6	ipsPcktsCount15Min	Количество пакетов, прошедших через СОВ за последние 15 минут
1.3.6.1.4.1.34849.1.1.1.1.7	ipsDropsCount	Количество пакетов, отброшенных СОВ с момента ее запуска
1.3.6.1.4.1.34849.1.1.1.1.8	ipsDropsCount1Min	Количество пакетов, отброшенных СОВ за последнюю минуту
1.3.6.1.4.1.34849.1.1.1.1.9	ipsDropsCount5Min	Количество пакетов, отброшенных СОВ за последние 5 минут
1.3.6.1.4.1.34849.1.1.1.1.10	ipsDropsCount15Min	Количество пакетов, отброшенных СОВ за последние 15 минут
1.3.6.1.4.1.34849.1.1.1.1.11	ipsEventLvl0Alerts	Число предупреждений уровня "0"с момента запуска СОВ
1.3.6.1.4.1.34849.1.1.1.1.12	ipsEventLvl0Alerts1Min	Число предупреждений уровня "0" за последнюю минуту
1.3.6.1.4.1.34849.1.1.1.1.13	ipsEventLvl0Alerts5Min	Число предупреждений уровня "0" за последние 5 минут
1.3.6.1.4.1.34849.1.1.1.1.14	ipsEventLvl0Alerts15Min	Число предупреждений уровня "0" за последние 15 минут
1.3.6.1.4.1.34849.1.1.1.1.15	ipsEventLvl1Alerts	Число предупреждений уровня "1"с момента запуска СОВ
1.3.6.1.4.1.34849.1.1.1.1.16	ipsEventLvl1Alerts1Min	Число предупреждений уровня "1" за последнюю минуту
1.3.6.1.4.1.34849.1.1.1.1.17	ipsEventLvl1Alerts5Min	Число предупреждений уровня "1" за последние 5 минут
1.3.6.1.4.1.34849.1.1.1.1.18	ipsEventLvl1Alerts15Min	Число предупреждений уровня "1" за последние 15 минут

Код параметра	Параметр	Описание
1.3.6.1.4.1.34849.1.1.1.1.19	ipsEventLvl2Alerts	Число предупреждений уровня "2"с момента запуска СОВ
1.3.6.1.4.1.34849.1.1.1.1.20	ipsEventLvl2Alerts1Min	Число предупреждений уровня "2" за последнюю минуту
1.3.6.1.4.1.34849.1.1.1.1.21	ipsEventLvl2Alerts5Min	Число предупреждений уровня "2" за последние 5 минут
1.3.6.1.4.1.34849.1.1.1.1.22	ipsEventLvl2Alerts15Min	Число предупреждений уровня "2" за последние 15 минут
1.3.6.1.4.1.34849.1.1.1.1.23	ipsEventLvl3Alerts	Число предупреждений уровня "3"с момента запуска СОВ
1.3.6.1.4.1.34849.1.1.1.1.24	ipsEventLvl3Alerts1Min	Число предупреждений уровня "3" за последнюю минуту
1.3.6.1.4.1.34849.1.1.1.1.25	ipsEventLvl3Alerts5Min	Число предупреждений уровня "3" за последние 5 минут
1.3.6.1.4.1.34849.1.1.1.1.26	ipsEventLvl3Alerts15Min	Число предупреждений уровня "3" за последние 15 минут
1.3.6.1.4.1.34849.1.1.1.1.27	ipsEventLvl4Alerts	Число предупреждений уровня "4"с момента запуска СОВ
1.3.6.1.4.1.34849.1.1.1.1.28	ipsEventLvl4Alerts1Min	Число предупреждений уровня "4" за последнюю минуту
1.3.6.1.4.1.34849.1.1.1.1.29	ipsEventLvl4Alerts5Min	Число предупреждений уровня "4" за последние 5 минут
1.3.6.1.4.1.34849.1.1.1.1.30	ipsEventLvl4Alerts15Min	Число предупреждений уровня "4" за последние 15 минут
1.3.6.1.4.1.34849.1.1.1.1.31	ipsEventLvl5Alerts	Число предупреждений уровня "5"с момента запуска СОВ
1.3.6.1.4.1.34849.1.1.1.1.32	ipsEventLvl5Alerts1Min	Число предупреждений уровня "5" за последнюю минуту
1.3.6.1.4.1.34849.1.1.1.1.33	ipsEventLvl5Alerts5Min	Число предупреждений уровня "5" за последние 5 минут
1.3.6.1.4.1.34849.1.1.1.1.34	ipsEventLvl5Alerts15Min	Число предупреждений уровня "5" за последние 15 минут
1.3.6.1.4.1.34849.1.1.1.1.35	ipsEventLvl6Alerts	Число предупреждений уровня "6"с момента запуска СОВ
1.3.6.1.4.1.34849.1.1.1.1.36	ipsEventLvl6Alerts1Min	Число предупреждений уровня "6" за последнюю минуту

Код параметра	Параметр	Описание
1.3.6.1.4.1.34849.1.1.1.1.37	ipsEventLvl6Alerts5Min	Число предупреждений уровня "6" за последние 5 минут
1.3.6.1.4.1.34849.1.1.1.1.38	ipsEventLvl6Alerts15Min	Число предупреждений уровня "6" за последние 15 минут
1.3.6.1.4.1.34849.1.1.1.1.39	ipsSingatureCount	Количество загружаемых сигнатур IPS
1.3.6.1.4.1.34849.1.1.2.1	**cpu**	**Загрузка процессора**
1.3.6.1.4.1.34849.1.1.2.1.1.1	cpuLoadAvg1Min	Средняя загрузка процессора за последнюю минуту
1.3.6.1.4.1.34849.1.1.2.1.1.2	cpuLoadAvg5Min	Средняя загрузка процессора за последние 5 минут
1.3.6.1.4.1.34849.1.1.2.1.1.3	cpuLoadAvg15Min	Средняя загрузка процессора за последние 15 минут
1.3.6.1.4.1.34849.1.1.2.1.2.1	cpuUtilIdleAvg1Min	Загрузка процессора на работу процессов ядра за последнюю минуту
1.3.6.1.4.1.34849.1.1.2.1.2.2	cpuUtilIdleAvg5Min	Загрузка процессора (в режиме ожидания) за последние 5 минут
1.3.6.1.4.1.34849.1.1.2.1.2.3	cpuUtilIdleAvg15Min	Загрузка процессора (в режиме ожидания) за последние 15 минут
1.3.6.1.4.1.34849.1.1.2.1.2.4	cpuUtilNiceAvg1Min	Загрузка процессора на работу программ с измененным приоритетом за последнюю минуту
1.3.6.1.4.1.34849.1.1.2.1.2.5	cpuUtilNiceAvg5Min	Загрузка процессора на работу программ с измененным приоритетом за последние 5 минут
1.3.6.1.4.1.34849.1.1.2.1.2.6	cpuUtilNiceAvg15Min	Загрузка процессора на работу программ с измененным приоритетом за последние 15 минут
1.3.6.1.4.1.34849.1.1.2.1.2.7	cpuUtilUserAvg1Min	Загрузка процессора на работу программ пользователей за последнюю минуту
1.3.6.1.4.1.34849.1.1.2.1.2.8	cpuUtilUserAvg5Min	Загрузка процессора на работу программ пользователей за последние 5 минут
1.3.6.1.4.1.34849.1.1.2.1.2.9	cpuUtilUserAvg15Min	Загрузка процессора на работу программ пользователей за последние 15 минут
1.3.6.1.4.1.34849.1.1.2.1.2.10	cpuUtilSystemAvg1Min	Загрузка процессора на работу процессов ядра за последнюю минуту

Код параметра	Параметр	Описание
1.3.6.1.4.1.34849.1.1.2.1.2.11	cpuUtilSystemAvg5Min	Загрузка процессора на работу процессов ядра за последние 5 минут
1.3.6.1.4.1.34849.1.1.2.1.2.12	cpuUtilSystemAvg15Min	Загрузка процессора на работу процессов ядра за последние 15 минут
1.3.6.1.4.1.34849.1.1.2.1.2.13	cpuUtilIowaitAvg1Min	Загрузка процессора на завершение операций ввода/вывода за последнюю минуту
1.3.6.1.4.1.34849.1.1.2.1.2.14	cpuUtilIowaitAvg5Min	Загрузка процессора на завершение операций ввода/вывода за последние 5 минут
1.3.6.1.4.1.34849.1.1.2.1.2.15	cpuUtilIowaitAvg15Min	Загрузка процессора на завершение операций ввода/вывода за последние 15 минут
1.3.6.1.4.1.34849.1.1.2.1.2.16	cpuUtilInterruptAvg1Min	Загрузка процессора на обработку прерываний за последнюю минуту
1.3.6.1.4.1.34849.1.1.2.1.2.17	cpuUtilInterruptAvg5Min	Загрузка процессора на обработку прерываний за последние 5 минут
1.3.6.1.4.1.34849.1.1.2.1.2.18	cpuUtilInterruptAvg15Min	Загрузка процессора на обработку прерываний за последние 15 минут
1.3.6.1.4.1.34849.1.1.2.1.2.19	cpuUtilSoftirqAvg1Min	Загрузка процессора на обработку отложенных прерываний за последнюю минуту
1.3.6.1.4.1.34849.1.1.2.1.2.20	cpuUtilSoftirqAvg5Min	Загрузка процессора на обработку отложенных прерываний за последние 5 минут
1.3.6.1.4.1.34849.1.1.2.1.2.21	cpuUtilSoftirqAvg15Min	Загрузка процессора на обработку отложенных прерываний за последние 15 минут
1.3.6.1.4.1.34849.1.1.2.2	**ram**	**ОЗУ**
1.3.6.1.4.1.34849.1.1.2.2.1	ramTotalBytes	Общий объем системной оперативной памяти в байтах
1.3.6.1.4.1.34849.1.1.2.2.2	ramUsedBytes	Объем используемой оперативной памяти в байтах
1.3.6.1.4.1.34849.1.1.2.2.3	ramUsedPercents	Объем используемой оперативной памяти в процентах
1.3.6.1.4.1.34849.1.1.2.2.4	ramFreeBytes	Объем свободной оперативной памяти в байтах
1.3.6.1.4.1.34849.1.1.2.2.5	ramFreePercents	Объем свободной оперативной памяти в процентах
1.3.6.1.4.1.34849.1.1.2.3	**swap**	**Файл подкачки**
1.3.6.1.4.1.34849.1.1.2.3.1	swapTotalBytes	Размер файла подкачки в байтах

Код параметра	Параметр	Описание
1.3.6.1.4.1.34849.1.1.2.3.2	swapUsedBytes	Объем используемого пространства файла подкачки в байтах
1.3.6.1.4.1.34849.1.1.2.3.3	swapUsedPercents	Объем используемого пространства файла подкачки в процентах
1.3.6.1.4.1.34849.1.1.2.3.4	swapFreeBytes	Объем свободного пространства файла подкачки в байтах
1.3.6.1.4.1.34849.1.1.2.3.5	swapFreePercents	Объем свободного пространства файла подкачки в процентах

Установка базы решающих правил

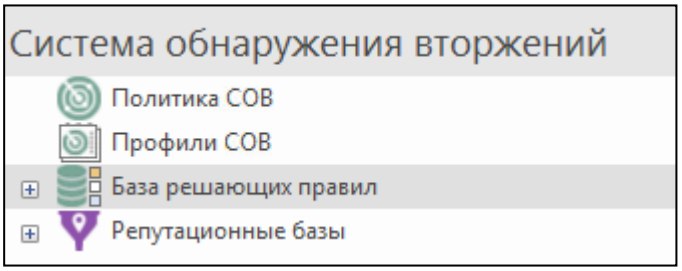
При обновлении ПО комплекса с версии 4.0.1 на 4.0.2 рекомендуется предварительно удалить старый набор БРП из БД ЦУС и со всех ДА.

Очистку и установку БРП выполняют в Менеджере конфигурации (МК). Для установки используется архивный файл, полученный от поставщика БРП.

Примечание. Типовое имя файла БРП – ids_update.json.gz.

Для удаления набора БРП в версии 4.0.1:

1. Откройте МК, перейдите в раздел "Система обнаружения вторжений" и войдите в подраздел "База решающих правил".

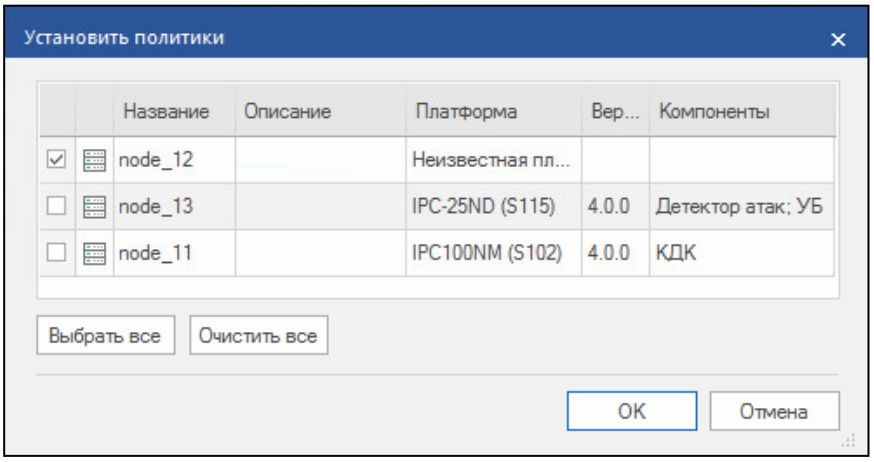


2. Выберите любое решающее правило в области отображения информации и нажмите "Ctrl" + "A". В панели инструментов нажмите кнопку "Удалить".

   Появится окно с сообщением о подтверждении удаления правил.

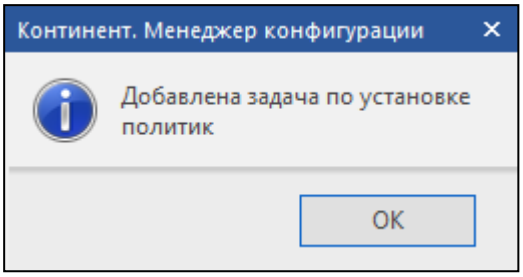
3. Нажмите кнопку "Да" в окне сообщения.
4. В главном окне МК перейдите в раздел "Структура" и нажмите кнопку "Установить политику".

   Откроется окно для установки политик на узлы сети.



5. В окне установки политик отметьте все узлы безопасности (в левой колонке) с обновляемым ПО. Далее нажмите кнопку "ОК".

   Задача по установке политик на выбранные узлы будет добавлена на ЦУС, после чего на экране появится соответствующее сообщение.

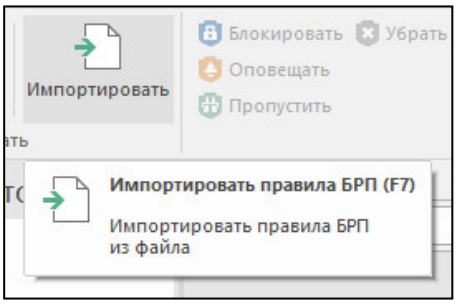


6. Нажмите кнопку "ОК" в окне сообщения.

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

Для установки БРП:

1. Подготовьте файл архива с БРП. Если он находится на сменном носителе — подключите носитель к рабочему месту с установленным МК.
2. Откройте МК, перейдите в раздел "Система обнаружения вторжений" и войдите в подраздел "База решающих правил".
3. В панели инструментов нажмите кнопку "Импортировать".

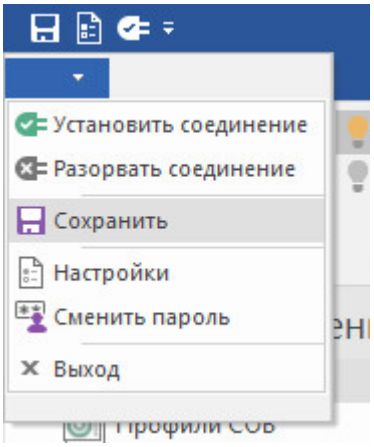


   На экране появится стандартное окно выбора файла.

4. Выберите файл архива с БРП и выполните загрузку.

   Будет выполнена загрузка БРП и на экране появится сообщение: "Файл загружен."

5. Нажмите кнопку "ОК" в окне сообщения.
6. Если на ЦУС установлено ПО версии 4.0.2.1731 или новее, нажмите кнопку вызова меню в левом верхнем углу окна МК и выберите пункт "Сохранить".



Изменения в конфигурации ЦУС будут применены.

7. В главном окне МК перейдите в раздел "Структура" и нажмите кнопку "Установить политику".

   Откроется окно для установки политик узлам сети.

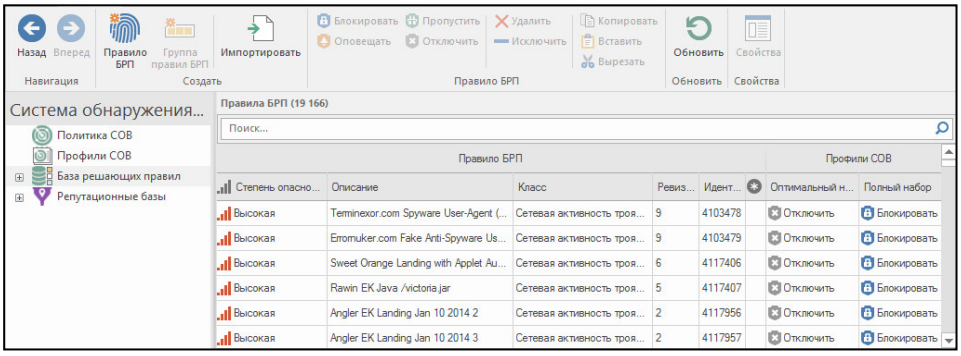
8. Установите отметки у тех узлов (ЦУС и ДА), на которые должна быть загружена новый набор БРП, и нажмите кнопку "ОК" в окне запроса.

   Если в данный момент на ЦУС никакие другие задачи не выполняются, начнется выполнение добавленной задачи.

9. Для просмотра сведений о поставленных задачах нажмите на значок в нижнем правом углу главного окна МК. В правой части экрана отобразится список задач, отсортированный по времени их добавления. Статус "выполнена" будет свидетельствовать о завершении процедуры установки политик.

   После установки политик загруженные правила отобразятся в окне МК.

Примечание. Если загруженные правила не отобразились — нажмите кнопку "Обновить" на панели инструментов.



Документация

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