КОД безопасности

Аппаратно-программный комплекс шифрования

Континент
Версия 3.9

Руководство администратора

Обнаружение вторжений

RU.88338853.501430.022 90 9

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

АПКШ	Аппаратно-программный комплекс шифрования
БД	База данных
БРП	База решающих правил
ДА	Детектор (компьютерных) атак
КШ	Криптографический шлюз
НСД	Несанкционированный доступ
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
ПУ	Программа управления
СОВ	Система обнаружения вторжений (компьютерных атак)
ЦУС	Центр управления сетью криптографических шлюзов
ICMP	Internet Control Message Protocol
IP	Internet Protocol
NAT	Network Address Translation
SID	Security Identifier
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USB	Universal Serial Bus

Введение

Документ предназначен для администраторов изделия "Аппаратно-программный комплекс шифрования "Континент" Версия 3.9" (далее — АПКШ "Континент", комплекс). В нем содержатся сведения, необходимые администраторам для управления системой обнаружения вторжений (компьютерных атак).

Дополнительные сведения, необходимые администратору комплекса, содержатся в [**1**]–[**4**].

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

Служба технической поддержки. Связаться со службой технической поддержки можно по телефону 8 800 505-30-20 или по электронной почте support@securitycode.ru.

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

Общий порядок ввода в эксплуатацию СОВ

Система обнаружения вторжений входит в состав АПКШ "Континент" и предназначена для обнаружения основных угроз безопасности информации, относящихся к вторжениям (компьютерным атакам).

Основным компонентом СОВ является детектор компьютерных атак, обеспечивающий обнаружение основных угроз безопасности информации. Подробные сведения об описании работы ДА и примеры его использования приведены в [**1**].

Ввод СОВ в эксплуатацию состоит из следующих последовательных этапов:

1. Регистрация и инициализация детекторов атак. Выполняется в полном соответствии с процедурой ввода в эксплуатацию сетевых устройств комплекса (см. [**2**], "Развертывание сетевого устройства").
2. Установка лицензии на обновление БРП. Выполняется средствами ПУ ЦУС (см. [**3**]).
3. Загрузка в БД ЦУС сертификатов для получения и обновления БРП (см. стр. **10**).
4. Загрузка БРП в БД ЦУС (см. стр. **11**).

   Внимание! Для соответствия АПКШ «Континент» сертификату ФСТЭК России после инициализации ДА администратор обязан загрузить все решающие правила, поставляемые на диске с БРП, и назначить ДА весь набор решающих правил. Модификация набора решающих правил может выполняться только с учетом актуальных угроз сети эксплуатирующей организации. Производитель не несет ответственности за последствия модификации назначаемого набора решающих правил.
5. Настройка режима работы ДА. Выполняется отдельно для каждого ДА (см. стр. **16**).
6. Назначение правил. Выполняется для каждого зарегистрированного ДА (см. стр. **21**).
7. Настройка автоматического обновления БРП (см. стр. **28**).

Глава 1
Управление системой обнаружения вторжений

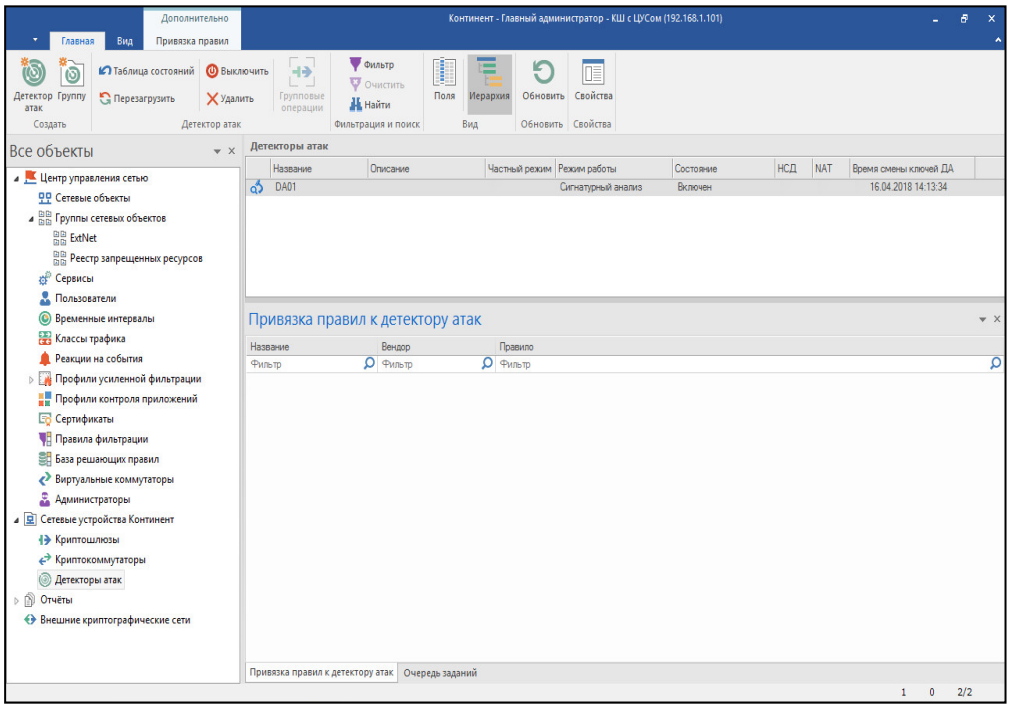
Управление СОВ включает в себя настройку детекторов атак и периодического обновления базы решающих правил. Настройка выполняется администратором в ПУ ЦУС. Для работы с детекторами атак и решающими правилами в ПУ ЦУС в области объектов управления выбирают соответственно пункт "Детекторы атак" или "База решающих правил".

Список детекторов атак

Для перехода к списку детекторов атак:

- Выберите в области объектов управления главного окна ПУ ЦУС пункт "Детекторы атак".

  В области отображения информации появится список зарегистрированных детекторов атак.



Примечание. Если в сети не было зарегистрировано ни одного детектора атак, список будет пустым.

Для каждого детектора в списке приводится следующая информация:

- название — имя, под которым детектор зарегистрирован в базе данных ЦУС;
- описание — дополнительные сведения, введенные при регистрации;
- режим работы — режим работы сигнатурного анализатора:
  - сигнатурный анализ;
  - выключен;
- состояние — состояние работы детектора атак:
  - отключен;
  - отключен (не введен в эксплуатацию);
  - включен;

  - включен (не введен в эксплуатацию);
- НСД — наличие НСД, обнаруженного данным детектором атак;
- NAT — контроль подключения к ЦУС через NAT;
- время смены ключей ДА — дата и время последней смены ключа связи с ЦУС и главного ключа детектора;
- идентификатор — идентификатор изделия, указанный в его паспорте;
- версия ПО — версия ПО, установленного на ДА.

Примечание. По умолчанию параметры "Идентификатор" и "Версия ПО" в главном окне не отображаются. Для редактирования состава информации о ДА используйте кнопку "Поля" на панели инструментов.

При выборе в списке какого-либо из детекторов в дополнительном окне, расположенном ниже, отобразится общий список правил. При этом правила, назначенные для выбранного детектора, имеют отметку перед названием.

С помощью кнопок панели инструментов выполняются следующие операции:

	Создание ДА
	Создание группы ДА
	Очистка таблицы состояния соединений ДА
	Перезагрузка ДА
	Выключение ДА
	Удаление ДА
	Включение фильтра
	Выключение фильтра
	Поиск в списке ДА
	Настройка параметров представления списка ДА
	Отображение ДА дочерних групп
	Обновление списка ДА
	Просмотр и редактирование свойств ДА

Список правил

Для перехода к списку правил:

- Выберите в области объектов управления главного окна ПУ ЦУС пункт "База решающих правил".

  В области отображения информации появится список групп загруженных в БД ЦУС решающих правил.

Примечание. Если правила в БД ЦУС не загружались, список будет пустым. Процедура загрузки правил приведена на стр. 11.

Правила сгруппированы по типам атак. Каждая группа имеет свое название, присвоенное поставщиком правил.

Отметка  , стоящая перед названием группы, означает, что данная группа правил доступна для использования в СОВ. Если отметка отсутствует, данная группа правил в системе не используется.

Для просмотра списка правил, входящих в группу:

- Раскройте группу.

  При раскрытии группы в полях "Вендор" и "Правило" будут отображены соответственно поставщик правила и содержание правила.

  Отметка, установленная перед названием правила, означает, что оно доступно для использования. Если отметка отсутствует, данное правило в системе не используется.

  Для поиска нужного правила могут быть использованы фильтры по названию, вендору и содержимому правила.

С помощью кнопок панели инструментов выполняются следующие операции:

	Добавление нового правила
	Удаление правила
	Просмотр и редактирование параметров правила
	Принудительная загрузка правил (обновление)
	Сохранение внесенных изменений
	Обновление отображаемого списка

Глава 2
Работа с правилами

Для работы с правилами используются средства ПУ ЦУС.

Загрузка сертификата пользователя

Для первоначальной загрузки базы решающих правил и последующего ее обновления необходимо получить у поставщика правил сертификат, который используется для проверки цифровой подписи при загрузке или обновлении правил.

Загрузка сертификатов выполняется средствами ПУ ЦУС. Поэтому рекомендуется предварительно сохранить файл сертификата в любой доступной в ПУ ЦУС папке жесткого диска или на внешнем носителе.

Для загрузки сертификата:

1. В области объектов управления главного окна ПУ ЦУС выберите раздел "Центр управления сетью" и в нем — пункт "Сертификаты".

   В правой части окна отобразится список зарегистрированных в БД ЦУС сертификатов.

   Если сертификаты в БД ЦУС не загружались, список будет пустым.

2. Для загрузки сертификата нажмите на панели инструментов кнопку "Импортировать".

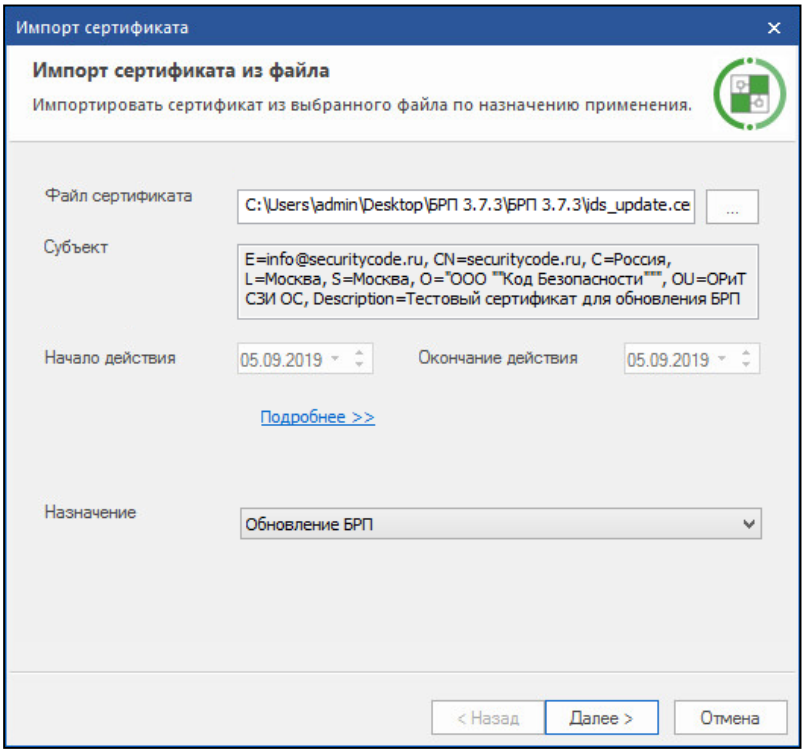
   На экране появится окно "Импорт сертификата".

3. Нажмите кнопку [...] справа от поля "Файл сертификата".

   На экране появится стандартное окно Windows для открытия файла.

4. Укажите папку и затем файл сертификата.

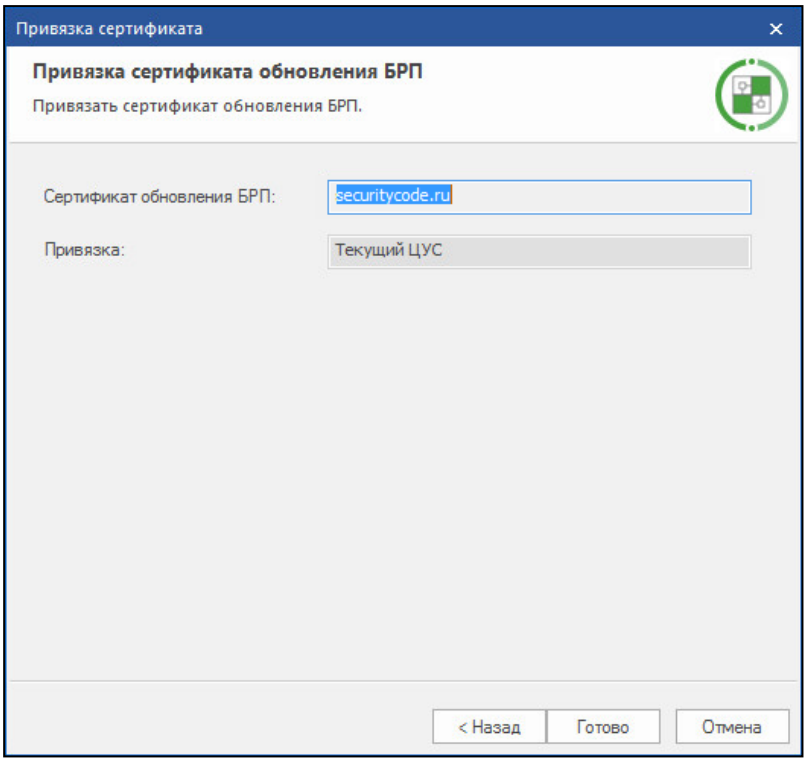
   На основании сведений, содержащихся в указанном сертификате, заполнятся поля "Субъект", "Начало действия" и "Окончание действия".



При необходимости просмотреть содержание сертификата используйте ссылку "Подробнее>>".

5. В поле "Назначение" выберите значение "Обновление БРП" и нажмите кнопку "Далее".

   На экране появится окно "Привязка сертификата".



   Поля в окне будут заполнены автоматически.

6. Нажмите кнопку "Готово".

   Окно закроется, и сертификат обновления БРП появится в списке сертификатов.

Загрузка правил

Для работы ДА в режиме сигнатурного анализа в БД ЦУС должны быть загружены правила, на основании которых детектором атак принимаются решения об атаках. Источником правил является БРП, размещенная на сервере обновлений.

Рекомендуется выполнить загрузку правил до регистрации ДА в ПУ ЦУС.

Внимание! Для загрузки правил и их обновления необходимо иметь установленную в ПУ ЦУС лицензию на обновление базы решающих правил (см.[3]).

Предусмотрено два варианта загрузки правил:

- принудительная загрузка (с внешнего накопителя, см. ниже).
- автоматическая загрузка (по расписанию, с использованием агента обновлений и абонентского пункта, см. стр. **28**).

Независимо от варианта при загрузке выполняется проверка цифровой подписи поставщика правил. Для проверки используется сертификат, выпущенный поставщиком правил и загруженный в БД ЦУС (см. стр. **10**).

Принудительная загрузка правил

Загрузка правил в БД ЦУС осуществляется администратором с USB-флеш-накопителя.

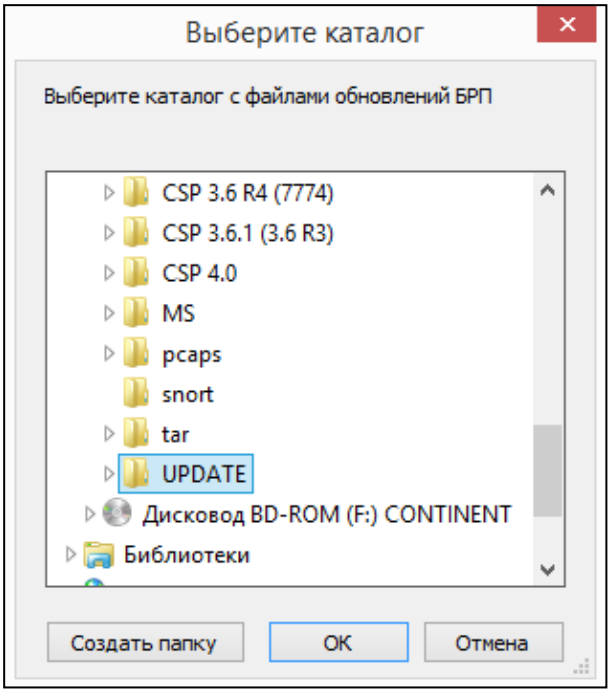
Для загрузки правил:

1. Выберите в области объектов управления главного окна ПУ ЦУС пункт "База решающих правил".

В области отображения информации появится список групп загруженных в БД ЦУС правил.

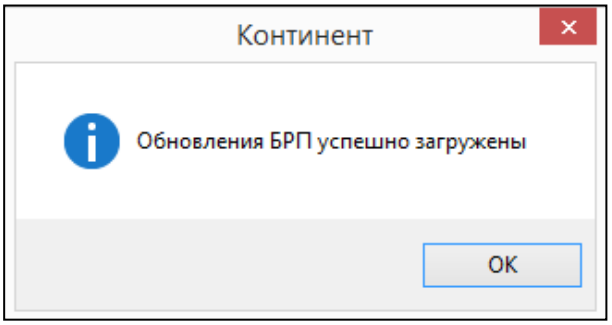
2. Вставьте USB-флеш-накопитель с записанными на нем решающими правилами (обновлениями).
3. В панели инструментов нажмите кнопку "Загрузить".

   На экране появится стандартное окно выбора каталога.



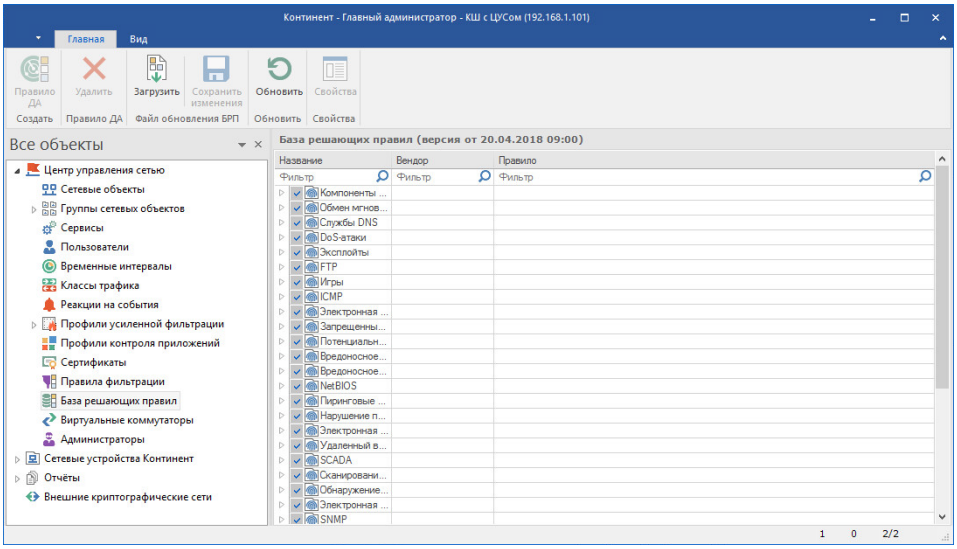
4. Укажите каталог, содержащий файлы с решающими правилами, и нажмите кнопку "OK".

   Начнется загрузка правил в БД ЦУС и после ее завершения на экране появится сообщение об успешной загрузке.



5. Нажмите кнопку "OK" в окне сообщения.

   Окно сообщения закроется и в области отображения информации появятся группы загруженных правил.



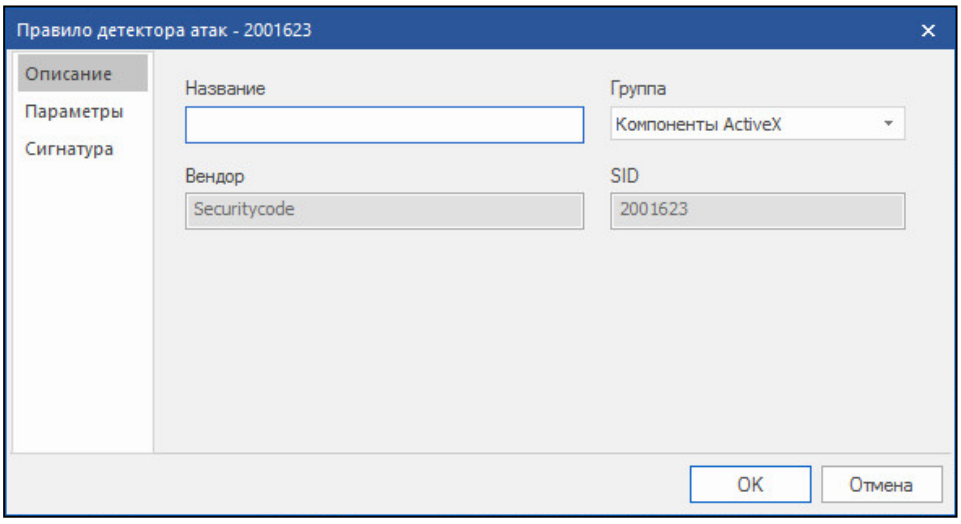
Просмотр и редактирование правил

Просмотр параметров правил без возможности их редактирования доступен при работе со списком детекторов атак (см. стр. **19**).

Для редактирования параметров правила:

1. Откройте список правил (см. стр. **8**).
2. Раскройте нужную группу, выберите правило и нажмите в панели инструментов кнопку "Свойства".

   На экране появится окно "Правило детектора атак", открытое на вкладке "Описание". В заголовке окна отображается SID выбранного правила.



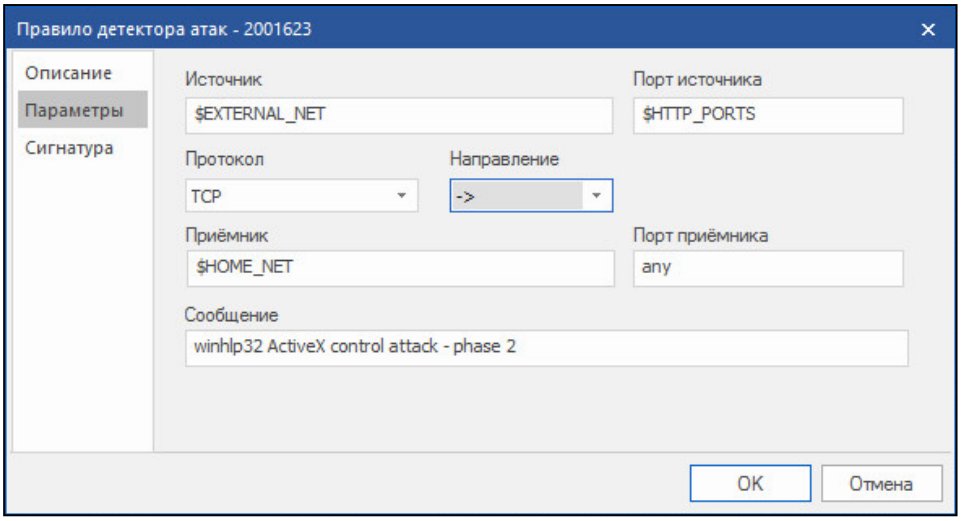
3. При необходимости изменить название правила вручную отредактируйте содержимое поля "Название".

   Внимание! Не рекомендуется изменять группу, в которую входит данное правило.

   Поля "Вендор" и "SID" для редактирования недоступны.

   Если дальнейшее редактирование правила не требуется, нажмите кнопку "ОК".

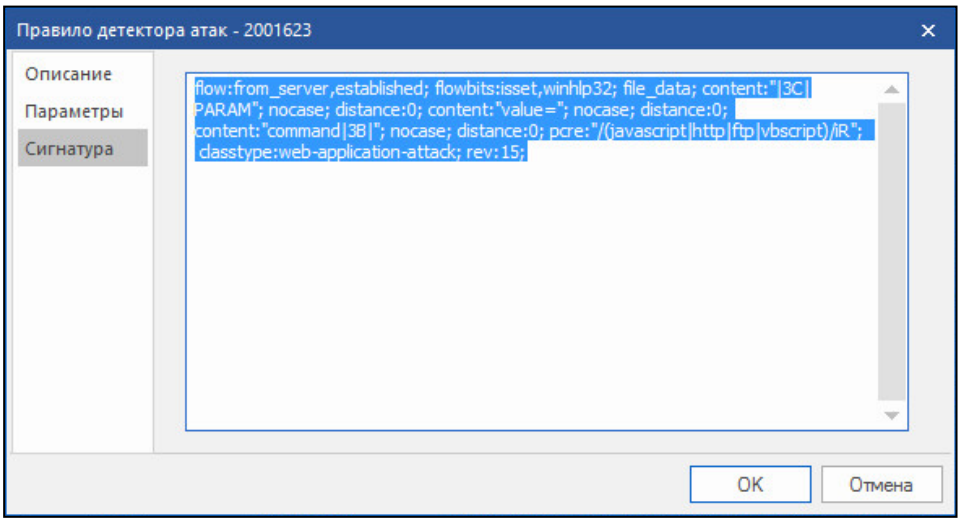
4. Для редактирования параметров правила перейдите на вкладку "Параметры".



5. При необходимости измените значения параметров.

Источник	IP-адрес (для IP4V и IP6V) или параметр ДА
Порт источника	Порт источника, параметр ДА или "any" для обозначения любого порта
Протокол	Протокол, выбираемый из списка: • TCP; • UDP; • ICMP; • IP
Направление	Направление трафика: • –> (к приемнику); • < > (в обоих направлениях)
Приемник	IP-адрес (для IP4V и IP6V) или параметр ДА
Порт приемника	Порт источника, параметр ДА или "any" для обозначения любого порта
Сообщение	Текст сообщения для журналирования (разрешены только символы латинского алфавита)

6. Перейдите на вкладку "Сигнатура".



7. При необходимости внесите изменения в содержимое сигнатуры, в соответствии с синтаксисом решающих правил (см. стр. **35**).
8. Для завершения процедуры редактирования нажмите кнопку "ОК".

   Окно "Правило детектора атак" закроется.

9. Проверьте наличие отметки в поле правила для использования его в СОВ и нажмите кнопку "Сохранить изменения" на панели инструментов для соответствующего изменения БД ЦУС.

Добавление нового правила

При создании нового правила оно автоматически включается в группу, выделенную в данный момент в списке правил. При этом параметр "Вендор" принимает значение "Пользовательские правила".

Для добавления нового правила:

1. Откройте список решающих правил (см. стр. **8**).
2. Нажмите кнопку "Правило ДА" на панели инструментов.

   На экране появится окно "Правило детектора атак", открытое на вкладке "Описание".
3. Введите название создаваемого правила, выберите требуемую группу, в которой оно будет размещено, и перейдите на вкладку "Параметры".

   Примечание. В поле "Вендор" по умолчанию установлено значение "Пользовательские правила". Поле редактированию не подлежит.
4. Заполните поля и перейдите на вкладку "Сигнатура".
5. Введите сигнатуру правила в соответствии с синтаксисом решающих правил СОВ (см. стр. **35**) и нажмите кнопку "ОК".

   Будет выполнена синтаксическая проверка сформированного правила и в случае обнаружения каких-либо ошибок на экране появится одно из двух сообщений:

   - сообщение об ошибке — отсутствует какой-либо важный параметр или задано его недопустимое значение (сохранение правила невозможно);
   - предупреждение — значение какого-либо из параметров не соответствует оптимальному режиму работы детектора атак (правило может быть сохранено).

   Если ошибки не обнаружены, окно "Правило детектора атак" закроется и новое правило будет добавлено в список.
6. Для сохранения правила в БД ЦУС нажмите кнопку "Сохранить изменения" на панели инструментов.

   После сохранения в свойствах правила появится поле "SID" с автоматически сгенерированным значением.

Удаление правила

Для удаления правила:

1. Откройте список решающих правил (см. стр. **8**).
2. Выберите в списке нужное правило и нажмите кнопку "Удалить" на панели инструментов.

   На экране появится запрос на подтверждение удаления.
3. Выберите "Да".

   Правило будет удалено из списка.
4. Для сохранения изменений нажмите соответствующую кнопку на панели инструментов.

Глава 3
Централизованное управление детекторами атак

Настройка детектора атак

Для настройки ДА:

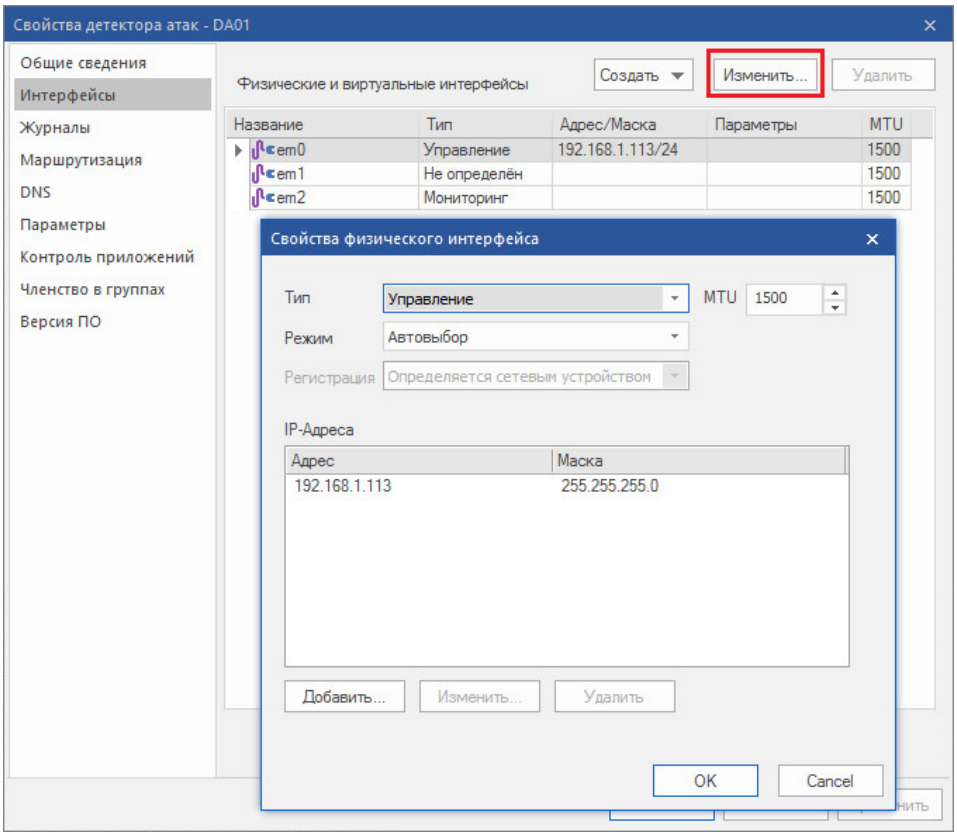
1. Выберите в области объектов управления главного окна ПУ ЦУС пункт "Сетевые устройства Континент | Детекторы атак", затем требуемый ДА в списке и нажмите кнопку "Свойства" на панели инструментов.

   На экране появится окно свойств ДА.

2. Для активации работы сигнатурного анализатора перейдите на вкладку "Общие сведения" и установите отметку в поле "Сигнатурный анализатор включен".

   Если для экономии производительности режим сигнатурного анализатора должен быть отключен, удалите эту отметку. В этом случае ДА будет функционировать только в режиме контроля приложений.

3. Перейдите на вкладку "Интерфейсы", настройте параметры интерфейсов управления и мониторинга, выбрав их в списке и нажав кнопку "Изменить...".

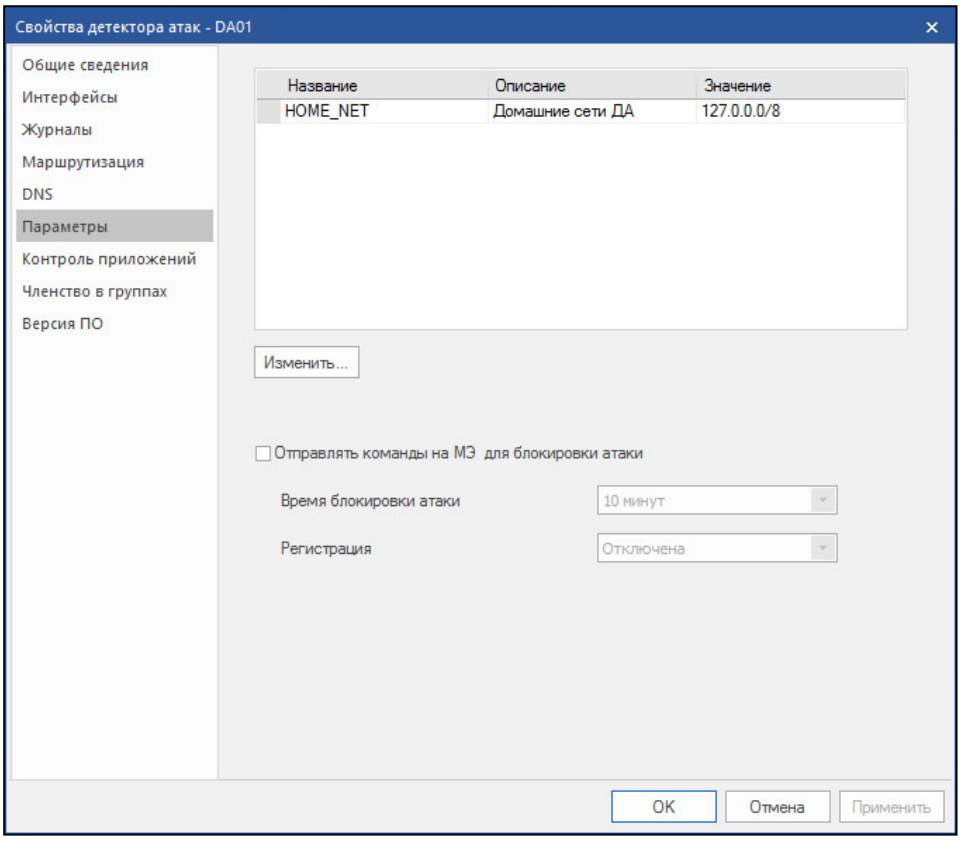


Тип	Выберите из списка одно из трех значений: • мониторинг – интерфейс используется для приема анализируемого трафика; • управление – интерфейс используется для управления со стороны ЦУС; • не определено – интерфейс не используется

MTU	Выберите из списка максимальную единицу передачи данных (в байтах). Только для типа интерфейса "Управление". По умолчанию установлено значение 1500
Режим	Выберите скорость передачи данных. По умолчанию установлено рекомендуемое значение "Автовыбор"
IP-адреса	Только для интерфейса типа "Управление". Для формирования списка IP-адресов используйте кнопки "Добавить...", "Изменить..." и "Удалить". При вводе IP-адреса допустимо указать префикс маски. При этом поле "Маска" заполняется автоматически

Примечание. Описание настройки иных физических и виртуальных интерфейсов приведено в [3].

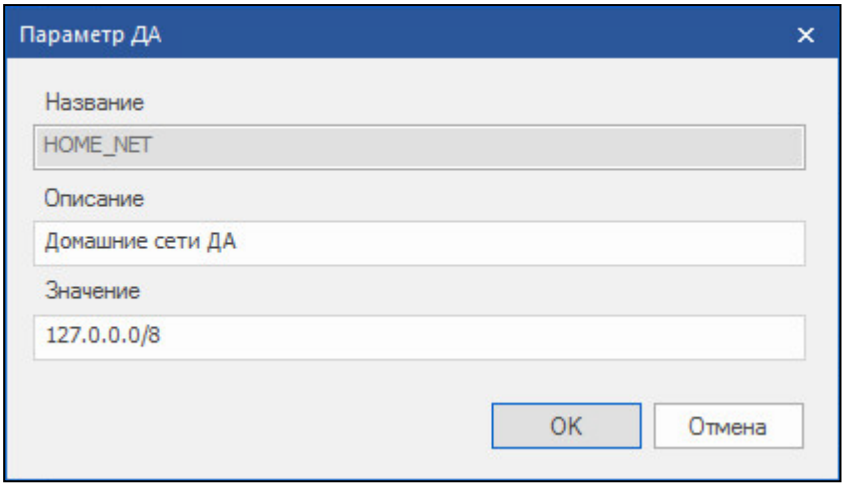
4. Перейдите на вкладку "Параметры".



На вкладке отображается параметр HOME_NET, описывающий защищаемые сети, контролируемые данным детектором атак. Для параметра приводятся его описание и значение — список контролируемых подсетей. При регистрации нового ДА по умолчанию параметру HOME_NET соответствует подсеть внутренних коммуникаций.

5. Выберите HOME_NET и нажмите кнопку "Изменить...".

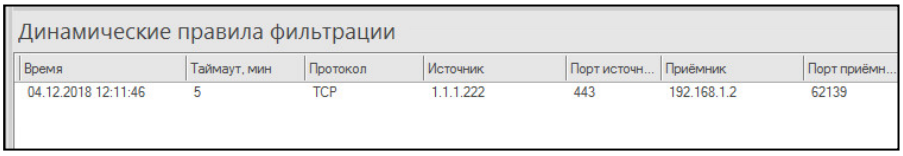
   На экране появится окно "Параметр ДА".



6. При необходимости внесите изменения в поле "Описание".
7. В поле "Значение" удалите отображаемую по умолчанию подсеть, укажите через запятую подсети, которые должны контролироваться данным детектором атак, и нажмите кнопку "ОК".

   Окно "Параметр ДА" закроется и на вкладке "Параметры" отобразятся введенные изменения.
8. Для совместной работы компонентов комплекса СОВ и МЭ установите отметку в поле "Отправлять команды на МЭ для блокировки атаки" и укажите требуемые параметры:
   - время блокировки атаки (время действия динамического правила МЭ по блокировке вредоносного трафика, обнаруженного ДА);
   - тип регистрации события в журналах сетевого трафика тех КШ, на которых произойдет блокировка вредоносного трафика.

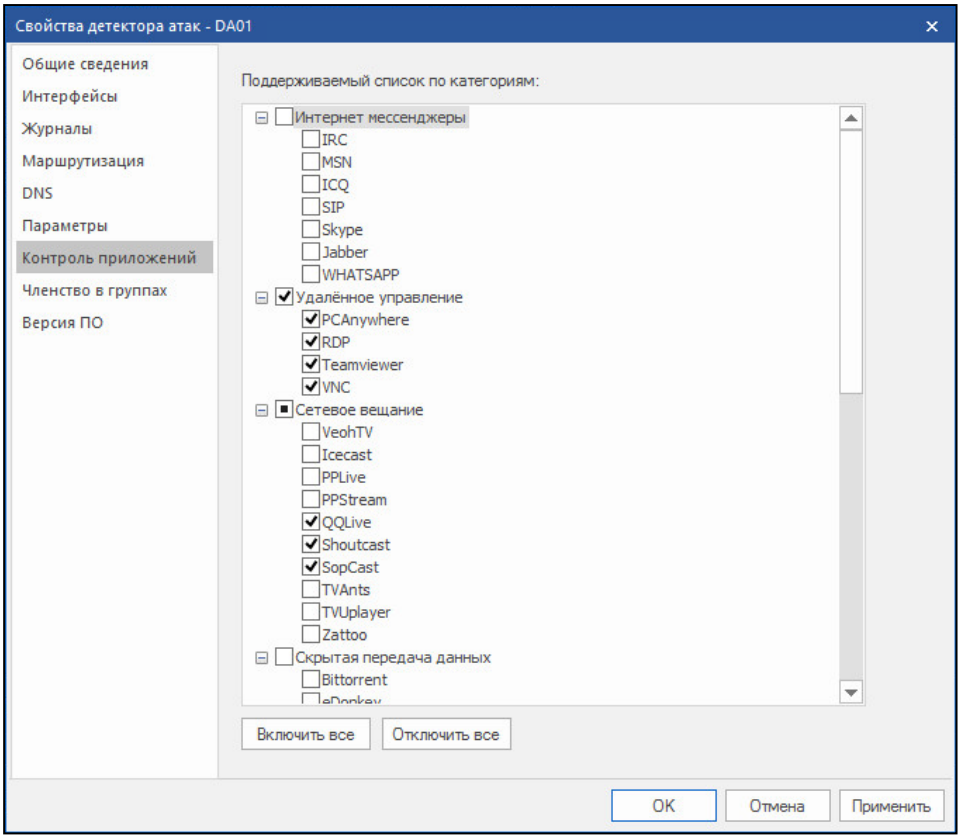
   Примечание. Просмотр созданных динамических правил можно выполнить в ПУ ЦУС на вкладке "Динамические правила фильтрации" соответствующих КШ.

   Внимание! Для блокирования атаки ее адресат должен быть в составе защищаемой сети, определяемой параметром HOME_NET.
9. Для сохранения внесенных изменений нажмите кнопку "Применить".
10. Для постановки приложений на контроль перейдите на вкладку "Контроль приложений".

    На вкладке представлен сгруппированный по категориям список приложений, которые могут быть поставлены на контроль.

    Примечание. По умолчанию после установки ПО детектора атак ни одно из приложений не контролируется.
11. Установите отметки у тех приложений, которые должны быть поставлены на контроль.



12. Для завершения настройки режима работы детектора атак нажмите кнопку "Применить" или "ОК".

Удаление детектора атак из списка

Для удаления ДА:

1. Выберите в списке ДА, подлежащий удалению, и нажмите кнопку ☒ на панели инструментов.

   На экране появится запрос на подтверждение удаления.
2. Для удаления нажмите кнопку "Да".

   Детектор атак будет удален из списка.

Просмотр решающих правил

В данном режиме редактирование параметров правил недоступно.

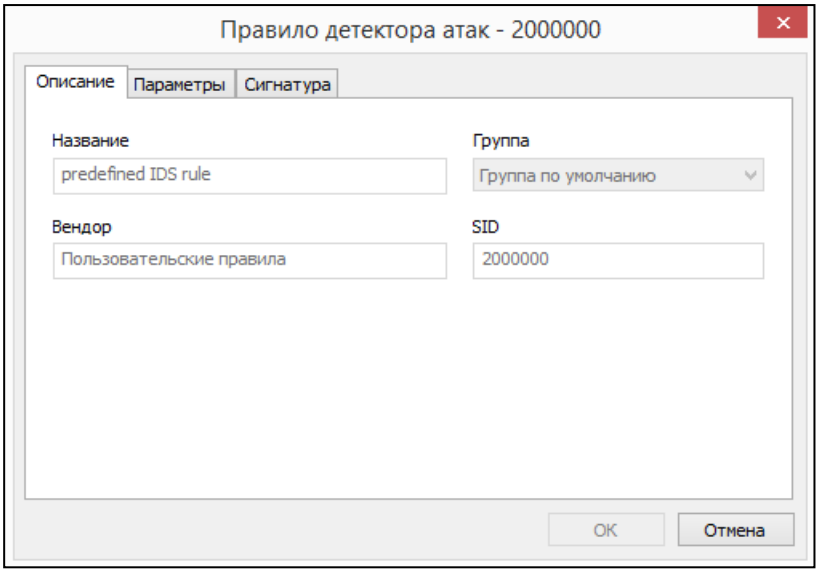
Для просмотра правил:

1. Выберите в списке ДА требуемое устройство.

   В дополнительном окне отобразится полный список групп решающих правил. Группы, назначенные выбранному ДА, имеют отметку.
2. Раскройте группу правил, назначенную детектору атак.

   Появится список правил, входящих в группу. Правила, назначенные детектору атак, имеют отметку.
3. Установите курсор на строку правила и дважды нажмите левую кнопку мыши.

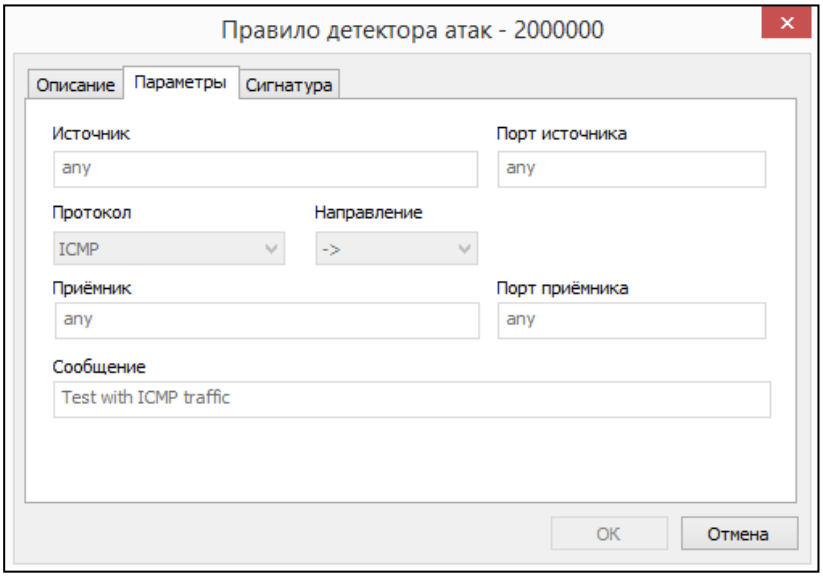
   На экране появится окно "Правило детектора атак", открытое на вкладке "Описание".



На вкладке представлены значения общих параметров правила:

- название;
- группа, в которую входит данное правило;
- вендор (поставщик правила);
- SID – уникальный номер правила, присвоенный вендором.

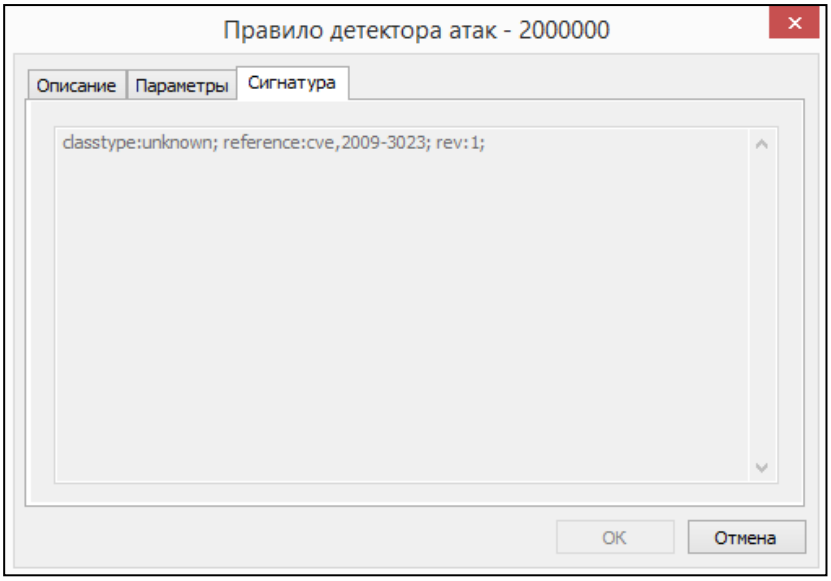
4. Перейдите на вкладку "Параметры".



На вкладке приведены значения следующих параметров:

- источник;
- порт источника;
- протокол;
- направление;
- приемник;
- порт приемника;
- сообщение, фиксируемое в журнале в случае обнаружения атаки.

5. После просмотра параметров перейдите на вкладку "Сигнатура".



На вкладке приведено содержание сигнатуры.

6. Для завершения просмотра правила нажмите кнопку "Отмена".

   Окно "Правило детектора атак" закроется.

Назначение правил

Для назначения детектору атак правила необходимо установить соответствующую отметку в списке решающих правил.

Можно назначить ДА как всю группу целиком (или несколько групп), так и отдельные правила, входящие в данную группу (или в разные группы).

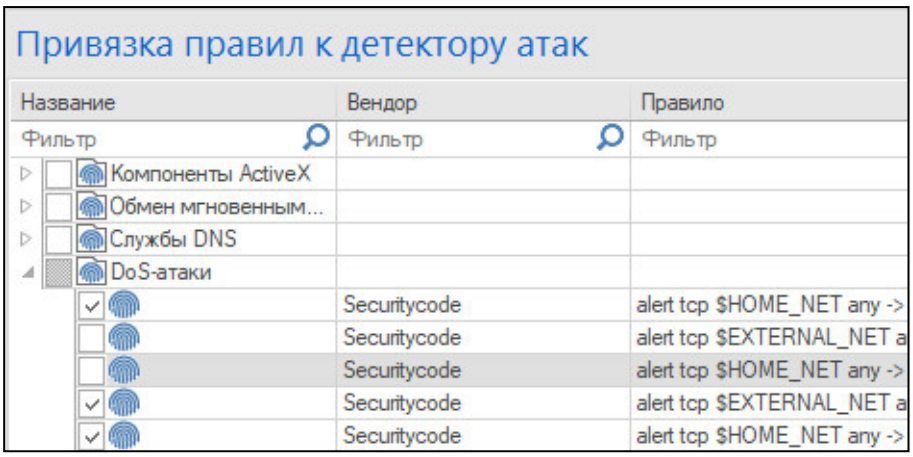
Для улучшения производительности СОВ рекомендуется назначение только актуальных для защищаемой сети решающих правил. Например, если VoIP-сервисы не используются, следует отключить правила для VoIP-траффика.

Для назначения правил:

1. Выберите в списке ДА, для которого необходимо назначить правила.

   В дополнительном окне отобразится полный список групп решающих правил.

2. Установите или удалите отметки у назначаемых правил в соответствии со следующим порядком:
   - Если отметка устанавливается/удаляется у группы, автоматически отметки будут установлены/удалены у каждого правила, входящего в данную группу.
   - Если необходимо назначить отдельное правило (или правила), раскройте группу и поставьте отметку у нужного правила (правил). При этом отметка у группы примет вид: ▩. Пример такой группы приведен на рисунке ниже.



3. Для просмотра правила установите курсор на строку правила и дважды нажмите левую кнопку мыши.

   На экране появится окно "Правило детектора атак", открытое на вкладке "Описание" (см. стр. **13**).

   Примечание. В данном режиме редактирование параметров правила недоступно.

4. Для сохранения внесенных изменений перейдите на вкладку "Привязка правил" панели инструментов и нажмите кнопку "Сохранить".

Глава 4
Локальное управление детектором атак

Включение/выключение и перезагрузка ДА, а также администрирование ПАК "Соболь" выполняются в полном соответствии с описанием данных процедур для сетевых устройств (см. [**3**], раздел "Общие операции").

Локальное управление осуществляется с помощью команд главного локального меню. Главное локальное меню доступно только после загрузки ОС с предъявлением персонального идентификатора администратора ПАК "Соболь".

Таким образом, доступ к локальному управлению ДА имеет только пользователь, обладающий правами администратора ПАК "Соболь".

Внимание! После трех неудачных попыток предъявления персонального идентификатора администратора ПАК "Соболь" детектор атак блокируется. При этом на экран выводится соответствующее сообщение.

Для локального взаимодействия с ДА также доступно дополнительное меню (см. стр. **26**), доступ к которому имеет только локальный администратор ДА. Учетная запись локального администратора создается на этапе регистрации ДА (см. [**2**], раздел "Развертывание сетевого устройства").

Переход к режиму настройки детектора атак

Для локального управления ДА необходимо подключить к нему клавиатуру и монитор.

Для перехода к режиму настройки:

1. Перезагрузите ДА, нажав комбинацию клавиш <Ctrl> + <Alt> + <Del>.

   На экране появится основное окно ПАК "Соболь", в центре которого будет отображаться запрос персонального идентификатора.

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

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

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

2. Введите пароль администратора и нажмите клавишу <Enter>.

   На экране появится меню администратора ПАК "Соболь".

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

   По окончании загрузки операционной системы на экране появится сообщение:

   ```
   Нажмите Enter для настройки параметров
   ```

4. Нажмите клавишу <Enter>.

   Если в течение 5 секунд клавиша <Enter> нажата не будет, ДА автоматически продолжит загрузку имеющейся конфигурации.

После нажатия клавиши <Enter> на экране появится главное меню:

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

5. Введите в строке ввода номер команды "Настройка ДА" и нажмите клавишу <Enter>.

   На экране появится меню настройки ДА:

```
1: Включить/Выключить сигнатурный анализатор
2: Включить/Выключить контроль приложений
3: Фильтры трафика
0: Выход
Выберите пункт меню (0-3):
```

Примечание. Содержание команд меню зависит от текущего режима работы ДА.

6. Для выбора нужной команды введите ее номер и нажмите клавишу <Enter>.

Управление режимами работы детектора атак

Управление сигнатурным анализатором

Для включения/выключения сигнатурного анализатора:

1. Войдите в меню настройки ДА (см. стр. **23**).
2. Введите номер команды "Включить/Выключить сигнатурный анализатор" и нажмите клавишу <Enter>.

   Команда будет выполнена и содержание команды, отображаемое в меню, будет изменено на противоположное.
3. Для возврата в главное меню введите номер команды "Выход" и нажмите клавишу <Enter>.

Управление контролем приложений

Для включения или отключения режима:

1. Войдите в меню настройки ДА (см. стр. **23**).
2. Введите номер команды "Включить/выключить контроль приложений" и нажмите клавишу <Enter>.

   Команда будет выполнена и содержание команды, отображаемое в меню, будет изменено на противоположное.
3. Для возврата в главное меню введите в меню настройки ДА номер команды "Выход" и нажмите клавишу <Enter>.

Настройки фильтров трафика

Данные настройки позволяют устанавливать и настраивать на интерфейсах мониторинга фильтры с целью снижения нагрузки на систему. В результате будет производиться анализ только тех пакетов, которые соответствуют параметрам фильтра. Такими параметрами могут быть, например, тип протокола, IP-адрес, источник/получатель и пр.

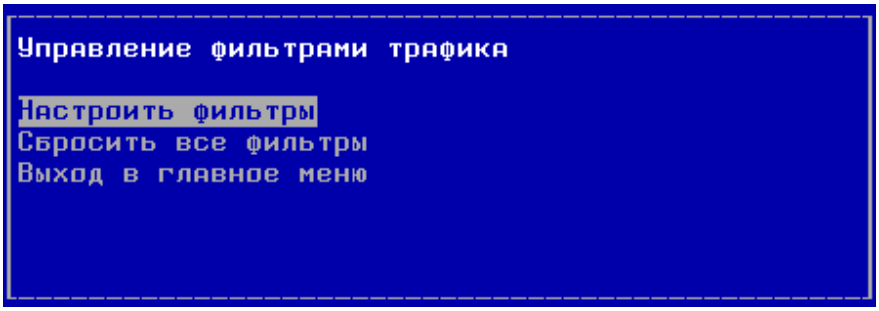
Работа с фильтрами выполняется в меню "Управление фильтрами трафика".

Для работы с фильтрами:

1. Войдите в меню настройки ДА (см. стр. **23**).

2. Введите номер команды "Фильтры трафика" и нажмите клавишу <Enter>.

   На экране появится меню "Управление фильтрами трафика".



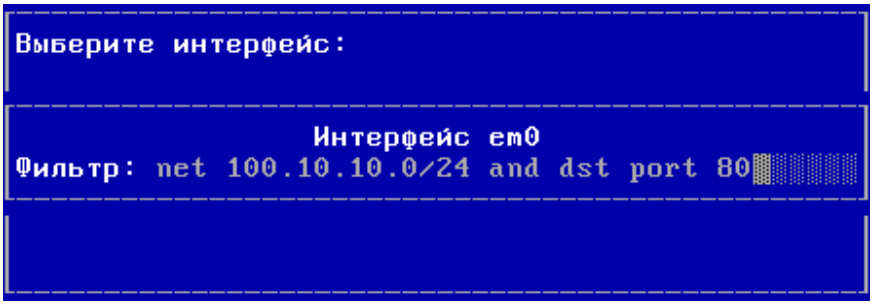
Для настройки фильтров:

1. В меню "Управление фильтрами трафика" выберите команду "Настроить фильтры" и нажмите клавишу <Enter>.

   На экране появится список интерфейсов детектора атак.

2. Для настройки фильтра выберите интерфейс и нажмите клавишу <Enter>.

   На экране появится строка настройки фильтра для выбранного интерфейса. В строке отображаются параметры настройки фильтра.



Примечание. Если фильтр для данного интерфейса не настраивался или был сброшен, строка будет пустой.

3. Введите параметры фильтрации в формате tcpdump (BPF-фильтр) и нажмите клавишу <Enter>.

Примечание. Примеры настройки фильтров приведены в приложении (см. стр. 37).

   На экране появится сообщение об установленном фильтре.

4. Нажмите клавишу <Enter>.

   Будет выполнен возврат в список интерфейсов данного ДА.

5. Для настройки фильтра на другом интерфейсе выполните пп. **2**–**4**.

6. Для применения настроек фильтров:

   - нажмите клавишу <Esc>;
   - вернитесь в главное меню;
   - введите номер команды "Выход" и нажмите клавишу <Enter>.

   Дождитесь сообщения об успешном запуске устройства.

Для отключения фильтра:

1. В меню "Управление фильтрами трафика" выберите команду "Настроить фильтры" и нажмите клавишу <Enter>.

   На экране появится список интерфейсов детектора атак.

2. Для отключения фильтра выберите интерфейс и нажмите клавишу <Enter>.

   На экране появится строка настройки выбранного интерфейса.

3. Удалите содержимое строки настройки и нажмите клавишу <Enter>.

   На экране появится сообщение о сброшенном фильтре интерфейса.

4. Нажмите клавишу <Enter>.

Будет выполнен возврат в список интерфейсов.

5. Для применения изменений нажмите клавишу <Esc>, вернитесь в главное меню, введите номер команды "Выход" и нажмите клавишу <Enter>.

   Дождитесь сообщения об успешном запуске устройства.

Для отключения всех фильтров:

1. В меню "Управление фильтрами трафика" выберите команду "Сбросить все фильтры" и нажмите клавишу <Enter>.

   На экране появится предупреждение о сбросе фильтров.

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

   На экране появится сообщение о сбросе всех фильтров.

3. Нажмите клавишу <Enter>.

   Будет выполнен возврат в меню "Управление фильтрами трафика".

4. Для применения изменений вернитесь в главное меню, введите номер команды "Выход" и нажмите клавишу <Enter>.

   Дождитесь сообщения об успешном запуске устройства.

Дополнительные возможности

Команды дополнительного меню

Для использования дополнительного меню к системному блоку ДА заранее должны быть подключены клавиатура и монитор.

Для перехода к дополнительному меню:

1. У работающего ДА нажмите комбинацию клавиш <ALT+F2>.

   На экране появится запрос на предъявление персонального идентификатора администратора.

2. Предъявите персональный идентификатор и при необходимости введите пароль.

   Количество неудачных попыток предъявления персонального идентификатора и время блокировки задаются политикой аутентификации администраторов (см. [**3**]).

   На экране появится дополнительное меню (см. Табл.1).

3. Введите номер команды и нажмите клавишу <Enter>.

   Выполняйте указания, отображаемые на экране.

4. Для выхода из дополнительного меню нажмите комбинацию клавиш <ALT+F1>.

Табл.1 Команды дополнительного меню

Команда	Описание
Сведения об устройстве	Отображает на экране сведения о версии и конфигурации ПО
Информация о загруженных ключах	Отображает на экране сведения о загруженных ключах (основном и резервном): • наименование и серийный номер носителя, с которого ключ был загружен; • номер комплекта; • номер ключа; • дата истечения срока хранения ключа
Вывести полный список интерфейсов	Отображает на экране полный список интерфейсов ДА
Диагностика	Выводит на экран меню команд диагностики
Перезагрузка	Запускает перезагрузку ДА

Команда	Описание
Завершение работы	Выключает электропитание ДА

Табл.2 Команды меню "Диагностика"

Команда	Описание
Загруженность ЦП	Отображает на экране информацию о загруженности каждого процессора
Использование памяти	Отображает на экране сведения о загруженности оперативной памяти
Использование жесткого диска	Отображает на экране общий объем жесткого диска, а также объем используемого и свободного пространства
Выполнить ping	Функция недоступна
Выполнить traceroute	Функция недоступна
Выполнить arp/ndp	Отображает на экране содержимое ARP- и NDP-кеша
Сведения о сетевых соединениях	Отображает на экране сведения об открытых сетевых соединениях
Количество пропущенных пакетов	Количество потерянных пакетов на интерфейсах мониторинга в СОВ (в процентах)
Сведения о работе шифратора	Функция недоступна
Просмотр дампа сетевого трафика	Отображает на экране информацию о сетевом трафике выбранного интерфейса с возможностью применения фильтра в формате tcpdump
Сведения о состоянии журналов	Отображает на экране максимальные и текущие объемы журналов
Сохранить конфигурацию и журналы событий динамической маршрутизации	Функция недоступна
Сохранить технологическую информацию	Выгружает на отчуждаемый носитель технологический отчет для отправки в службу поддержки
Сохранить отладочные журналы	Выгружает на отчуждаемый носитель записи системного журнала
Выход	Закрывает меню "Диагностика"

Глава 5
Настройка автоматического обновления БРП

Автоматическое обновление БРП в БД ЦУС осуществляется агентом обновлений БРП, входящим в состав компонентов ПУ ЦУС, устанавливаемых по умолчанию. Источником обновлений БРП является сервер поставщика правил (сервер обновлений). Для связи агента обновлений с сервером обновлений используется защищенное соединение, устанавливаемое СКЗИ "Континент-АП" (абонентским пунктом) по команде агента.

Примечание. ПО абонентского пункта используется в фоновом режиме исключительно для установления защищенного соединения с сервером обновлений.

Для установления защищенного соединения на абонентском пункте должны быть зарегистрированы сертификаты (пользовательский и корневой), а также должны быть предъявлены ключи шифрования.

Примечание. Решающие правила и обновления могут быть загружены в принудительном режиме без использования агента обновлений и абонентского пункта (см. стр. 11).

До начала настройки автоматической загрузки правил необходимо получить от поставщика правил сертификаты:

- сертификат сервера обновлений;
- корневой сертификат.

Для получения сертификатов необходимо обратиться в службу технической поддержки поставщика базы решающих правил (ООО "Код Безопасности") и сообщить номер лицензии на обновление БРП.

Для настройки автоматической загрузки правил необходимо выполнить следующее:

1. Установить ПО агента обновлений и абонентского пункта (см. ниже).
2. Установить на компьютер с агентом обновлений сертификат сервера обновлений и корневой сертификат (см. стр. **29**).
3. Средствами ПУ ЦУС настроить расписание автоматического обновления БРП (см. стр. **31**).
4. Настроить агент обновлений (см. стр. **33**).

Установка агента

Примечание. Агент устанавливают на компьютер, на котором установлен абонентский пункт версии не ниже 3.7.

Установку агента обновлений выполняют с установочного диска компонентов подсистемы управления АПКШ "Континент". Процедура установки подсистемы управления описана в [**2**]. Вид установки – "Выборочная". Устанавливаемый компонент – "Агент обновлений БРП".

После завершения процедуры на компьютере будут установлены агент обновлений и программа управления агентом, а в меню "Пуск | Все программы" в программной группе "Код Безопасности" появится команда "Программа управления агентом обновлений БРП".

Программа управления агентом обновлений

Программа используется для настройки и локального управления агентом обновлений.

После завершения процедуры установки агента и перезагрузки компьютера программа запускается автоматически, при этом агент обновлений по умолчанию находится в остановленном состоянии.

Для контроля состояния работы агента в правой части панели задач Windows располагается пиктограмма программы управления агентом обновлений. Цвет пиктограммы указывает на состояние агента обновлений:

	Зеленый	Агент запущен
	Красный	Агент остановлен

Управление агентом осуществляется через контекстное меню пиктограммы.

Команда контекстного меню	**Описание**
Запустить агент	Запуск агента
Остановить агент	Остановка агента
Импорт сертификата сервера обновлений	Запуск процедуры установки сертификата пользователя и корневого сертификата на компьютер
Параметры агента...	Открытие окна параметров агента для просмотра и редактирования
Журнал приложений системы	Вызов на экран журнала приложений Windows
О программе...	Открытие окна, содержащего сведения о номере версии программы управления агентом, а также сведения об авторских правах на программный продукт
Выход	Выход из программы управления агентом и удаление пиктограммы с панели задач. Агент продолжает функционировать в соответствии с установленным состоянием

Все команды, приведенные в таблице, доступны при запуске программы от имени локального администратора компьютера. В противном случае будут доступны только следующие команды:

- Журнал приложений системы.
- О программе...
- Выход.

Внимание! Программа управления агентом обновлений запускается автоматически в пользовательском режиме при загрузке ОС компьютера. Для внесения изменений в настройку программы требуется выйти из нее и осуществить принудительный запуск от имени администратора.

Установка сертификата сервера обновлений и корневого сертификата

Сертификат сервера обновлений и корневой сертификат, полученные от поставщика в виде двух файлов и ключевого контейнера, хранятся на внешнем носителе.

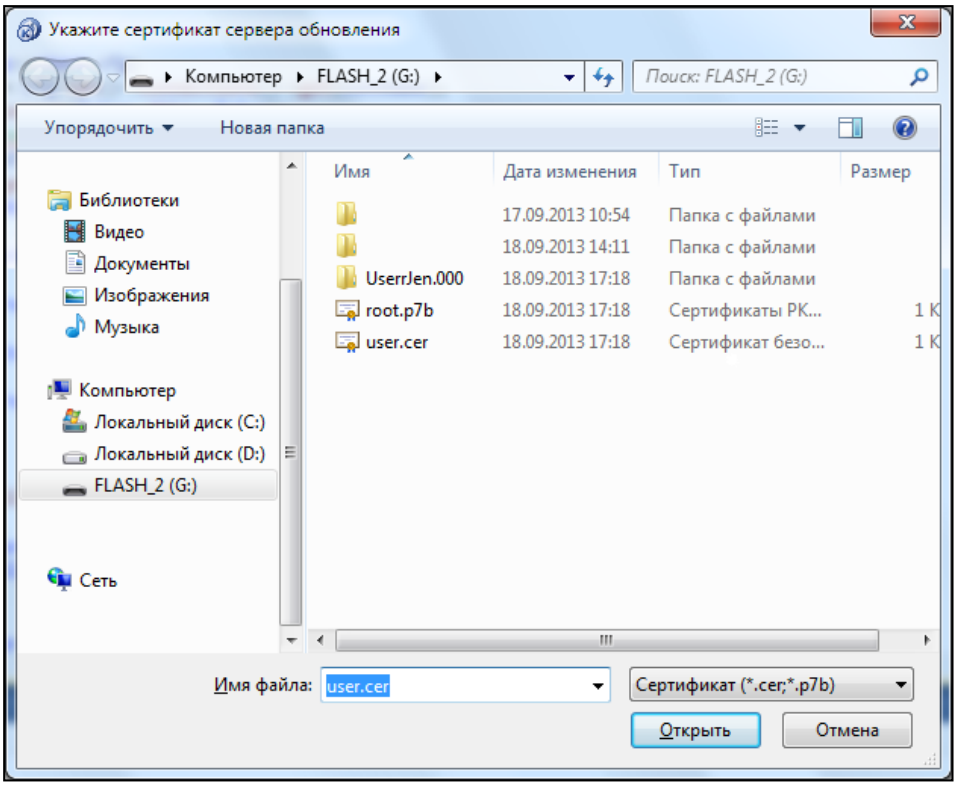
Установка сертификатов выполняется в программе управления агентом обновлений.

Для установки сертификатов:

1. Вставьте внешний носитель с сертификатами и ключевым контейнером.

2. Вызовите контекстное меню пиктограммы агента обновлений (см. стр. **29**) в панели задач и выберите команду "Импорт сертификата сервера обновлений".

   На экране появится стандартное окно выбора файла.



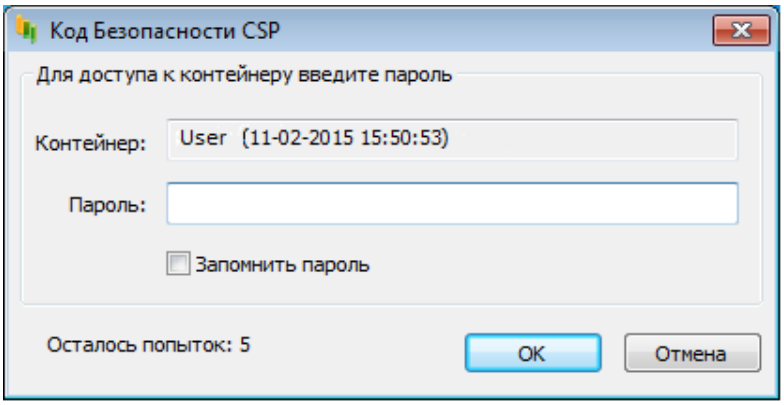
3. Выберите на внешнем носителе требуемый сертификат и нажмите кнопку "Открыть".

   Начнется настройка и установление защищенного соединения абонентского пункта с сервером обновлений. При этом на панели задач появится всплывающее сообщение о выполнении проверки соединения.

   Дождитесь завершения проверки соединения.

   Примечание. Если внешний носитель защищен PIN-кодом, на экране появится запрос на ввод защитного кода. Введите PIN-код и установите отметку в поле "Запомнить PIN".

   На экране появится окно ввода пароля доступа к ключевому контейнеру.



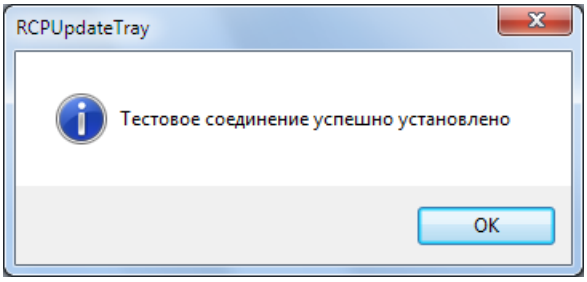
4. Введите пароль доступа к ключевому контейнеру, полученный от поставщика, установите отметку в поле "Запомнить пароль" и нажмите кнопку "OK".

   На экране появится запрос на занесение сервера обновлений и корневого сертификата в списки разрешенных.

5. Нажмите в окне запроса кнопку "Да".

Начнется тестовое соединение абонентского пункта с сервером обновлений. Пиктограмма абонентского пункта в панели задач изменится и будет отображать установление соединения.

Дождитесь окончания процесса. На экране появится сообщение об установленном тестовом соединении.



Пиктограмма абонентского пункта в панели задач будет отображать установленное соединение.

- Если соединение установить не удалось, на экране появится соответствующее сообщение.

  Закройте окно сообщения нажатием кнопки "OK" и установите причину ошибки соединения, используя журнал приложений.

6. Нажмите кнопку "OK" в окне сообщения.

   Окно сообщения закроется и соединение будет разорвано. Пиктограмма абонентского пункта в панели задач изменится и будет отображать отсутствие соединения.

   Сертификат сервера обновлений и корневой сертификат установлены.

Настройка агента обновлений

Для настройки агента необходимо выполнить следующее:

1. Настроить расписание загрузки обновлений в БД ЦУС.
2. Задать и настроить режим работы агента.

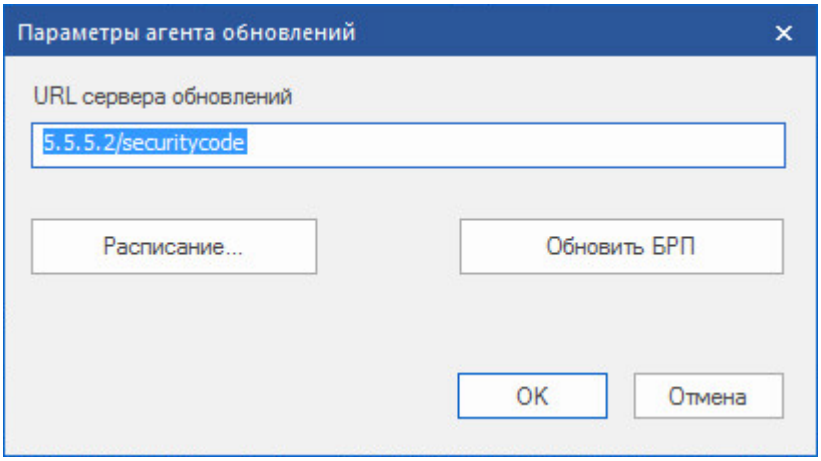
Настройка расписания

Перед началом настройки расписания убедитесь, что пользовательский сертификат обновлений БРП загружен (см. стр. **10**).

Для настройки расписания:

1. В области объектов управления главного окна ПУ ЦУС вызовите контекстное меню раздела "Центр управления сетью" и выберите команду "Настройка агента обновлений БРП".

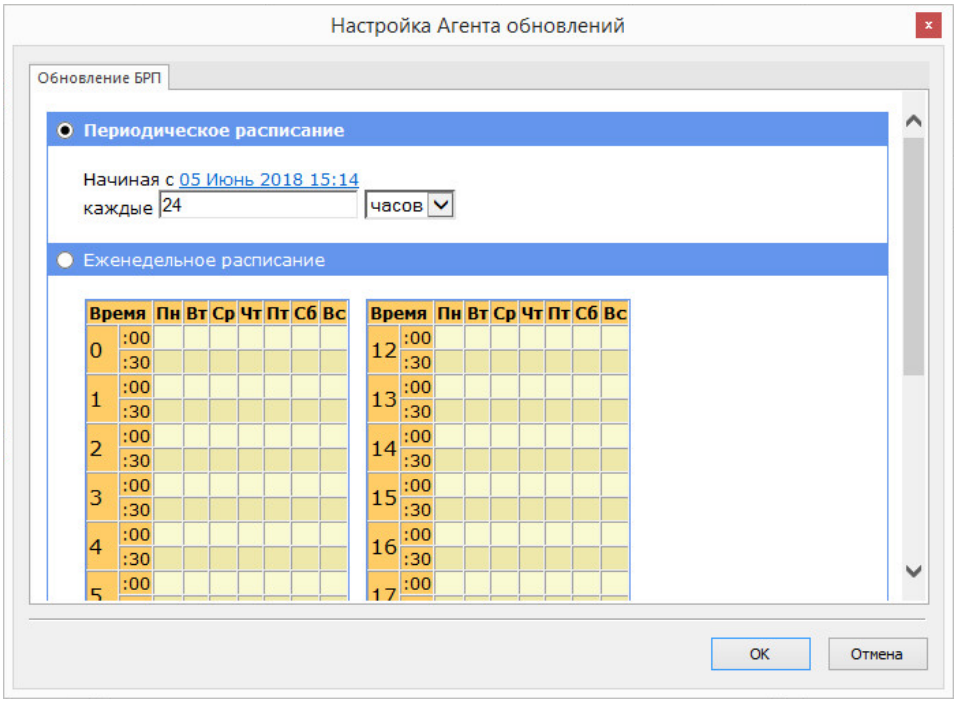
   На экране появится окно "Параметры агента обновлений".



URL сервера обновлений (5.5.5.2/securitycode) задан по умолчанию.

2. Нажмите кнопку "Расписание" в окне "Параметры агента обновлений".

   На экране появится окно "Настройка агента обновлений".



   В окне представлены два варианта настройки расписания.

3. Выберите нужный вариант расписания и настройте его.

Периодическое расписание	Включает режим загрузки обновлений, при котором запуск процесса осуществляется через равные промежутки времени. Продолжительность промежутка задается количеством минут или часов. Режим начинает действовать с момента наступления определенной даты и времени. Чтобы указать другой момент начала действия режима, активируйте ссылку с текущим значением даты и времени и в появившемся на экране окне введите нужные значения. Способы выбора и редактирования значений в этом окне аналогичны стандартным способам, принятым в ОС Windows
Еженедельное расписание	Включает режим загрузки обновлений, при котором запуск процесса осуществляется в моменты времени, заданные специальным расписанием. Расписание представлено в виде таблицы, разделенной, для оптимального отображения, на две части. В столбцах таблицы перечислены дни недели, а в строках — часы и минуты с шагом 30 минут. Выбор времени запуска процесса осуществляется посредством установки отметки в соответствующей ячейке таблицы. Для установки отметки поместите указатель в ячейку и нажмите левую кнопку мыши. Повторное нажатие кнопки приводит к удалению отметки. Действие расписания повторяется еженедельно

4. После настройки расписания нажмите кнопку "OK".

   Окно "Настройка агента обновлений" закроется.

5. Для сохранения выполненных настроек нажмите кнопку "OK" в окне "Параметры агента обновлений".

   Окно "Параметры агента обновлений" закроется.

Примечание. Для загрузки правил и обновлений по настроенному расписанию агент обновлений должен быть запущен (см. стр. 33).

Задание и настройка параметров агента

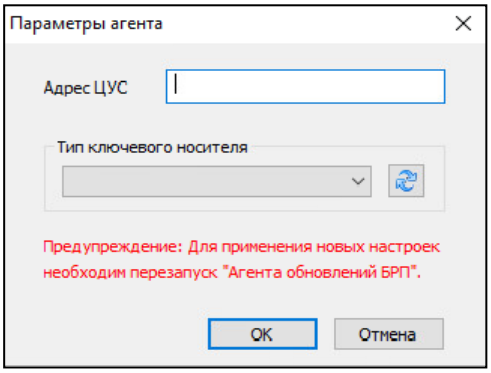
Работа агента обновлений осуществляется с использованием подключения к ЦУС. Загрузка обновлений осуществляется через установленное защищенное соединение с ЦУС.

Данная настройка выполняется локально на компьютере с установленным агентом обновлений и заключается указании типа ключевого носителя, на котором хранятся ключи для связи с ЦУС, и адреса ЦУС.

Для настройки агента:

1. Вставьте в USB-разъем внешний носитель с ключами связи с ЦУС.
2. Вызовите контекстное меню пиктограммы "Программа управления агентом" (см. стр. 29) и активируйте команду "Параметры агента".

   На экране появится окно "Параметры агента".



3. Заполните поля параметров и нажмите кнопку "OK".

Поле	Описание
Адрес ЦУС	Введите или измените IP-адрес КШ с ЦУС
Тип ключевого носителя	Выберите из списка нужный ключевой носитель

   Окно "Параметры агента" закроется. Для активации внесенных изменений требуется перезапуск агента.

Запуск агента

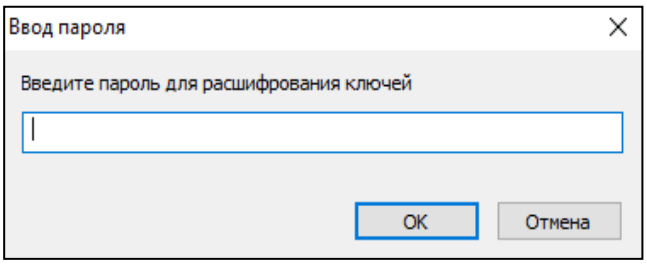
Запуск агента осуществляется по команде программы управления.

При запуске агента потребуется ввести пароль доступа к ключевому контейнеру.

Для запуска агента:

1. Вызовите контекстное меню пиктограммы программы управления и выберите команду "Запустить агент".

   На экране появится запрос на ввод пароля для расшифрования ключей:



2. Введите пароль доступа к ключевому контейнеру.

3. Нажмите кнопку "ОК".

   Агент будет запущен и цвет пиктограммы в панели задач изменится с красного на зеленый.

Принудительная загрузка обновлений

Предусмотрена принудительная загрузка обновлений агентом по команде из ПУ ЦУС. Загрузка выполняется с сервера обновлений. Для загрузки необходима предварительная настройка и запуск агента обновлений (см. выше).

В тех случаях, когда по каким-либо причинам отсутствует связь агента обновлений с ЦУС, необходимо получить обновления с сервера поставщика решающих правил и сохранить их на жестком диске или внешнем носителе. Далее обновления вручную загружаются в БД ЦУС средствами ПУ ЦУС (см. стр. **11**).

Для принудительной загрузки обновлений из ПУ ЦУС:

1. В области объектов управления главного окна ПУ ЦУС вызовите контекстное меню раздела "Центр управления сетью" и выберите команду "Настройка агента обновлений БРП".

   На экране появится окно "Параметры агента обновлений".

2. Нажмите кнопку "Обновить БРП".

   Агенту будет направлена команда на загрузку обновлений и на экране появится соответствующее сообщение.

3. Закройте окно сообщения, нажав кнопку "ОК".
4. Закройте окно "Параметры агента обновлений", нажав кнопку "ОК".

Для загрузки и экспорта обновлений с сервера поставщика:

1. Если планируется сохранение обновлений на внешнем носителе, вставьте его в USB-разъем.
2. В контекстном меню пиктограммы абонентского пункта, расположенной на панели задач Windows, установите соединение "Обновление БРП".
3. С помощью браузера зайдите на станицу по адресу http://5.5.5.2/securitycode.

   Загрузится страница с файлами обновлений.

4. Скачайте файлы, нажав на название каждого файла. При необходимости сохраните файлы обновлений на внешний носитель.

Приложение

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

Для всех режимов	
alert	Генерировать сигнал с использованием выбранного метода и записать информацию о пакете в журнальный файл
log	Записать информацию о пакете в журнальный файл
pass	Пропустить (игнорировать) пакет
activate	Генерировать сигнал и активировать другое динамическое правило
dynamic	Правило не выполняет никаких действий до его активации с помощью действия activate в другом правиле, а при активации действует как log
Только для режима Inline	
drop	Отброс пакета (пакет не пропускается). Генерация сигнала (alert) и запись информации о пакете в файл журнала. Применяется только при работе СОВ в режиме Inline. **Внимание!** Отбрасывание пакета приводит к тайм-ауту ожидания в случае использования протокола TCP
sdrop	Отброс пакета (пакет не пропускается). **Внимание!** Отбрасывание пакета приводит к тайм-ауту ожидания в случае использования протокола TCP
reject	Отброс пакета с уведомлением. И отправитель, и получатель получают специальный reject пакет одного из двух типов. Если пакет, на котором сработало правило, был TCP, то будет послан TCP RST пакет, в остальных случаях — ICMP пакет с ошибкой. Генерация сигнала (alert) и запись информации о пакете в файл журнала.

Протокол

Используются протоколы tcp, udp, icmp или ip.

Отправитель и получатель

В качестве отправителя и получателя пакетов в правиле указываются IP-адрес (допустимо применение как IPv4, так и IPv6) и маска подсети либо ключевое

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

Пример правила, которому будут соответствовать пакеты, отправленные с любого (any) 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

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

Также для указания адреса можно использовать параметры ДА:

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

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

Порт

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

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

drop udp any any -> 192.168.1.0/24 :1024

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

Для портов также поддерживается оператор отрицания (!).

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

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

Направление

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

получатель. Такие правила удобны для анализа пакетов в сеансовых соединениях (например, по протоколу POP3).

Пример двунаправленного правила:

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

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

Использование в правилах оператора <- недопустимо.

Правила Activate/Dynamic

С помощью одного правила (activate) можно активировать при наступлении определенных условий другое правило, действие которого будет выполнено для заданного числа пакетов. Это очень полезно в тех случаях, когда необходимо сохранить некоторое количество пакетов при возникновении того или иного события. Правила активации подобны правилам alert, но включают добавочное поле activates, служащее для добавления (активации) другого правила при выполнении заданных условий.

Динамические правила похожи на правила log, но включают два добавочных поля – activated_by и count. Правила dynamic включаются только при выполнении правила activate с заданным идентификатором. Все добавочные поля правил activate/dynamic являются обязательными.

Опции правил

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

Существуют 4 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

За подробными сведениями об опциях правил обращайтесь в службу технической поддержки.

Примеры фильтров сигнатурного анализатора

Ниже приведены 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.

Контроль целостности

В СОВ предусмотрен контроль целостности установленного программного обеспечения ДА и агента обновлений (см. [**1**]). Перечень контролируемых файлов устанавливается производителем и изменению не подлежит.

Контроль целостности программного обеспечения ДА выполняется автоматически при каждой загрузке его ОС.

Контроль целостности файлов агента обновлений осуществляется при необходимости с помощью специальной программы ngc.exe, хранящейся в папке "...\Континент\Update Agent", указываемой при установке ПО РМ администратора АПКШ "Континент".

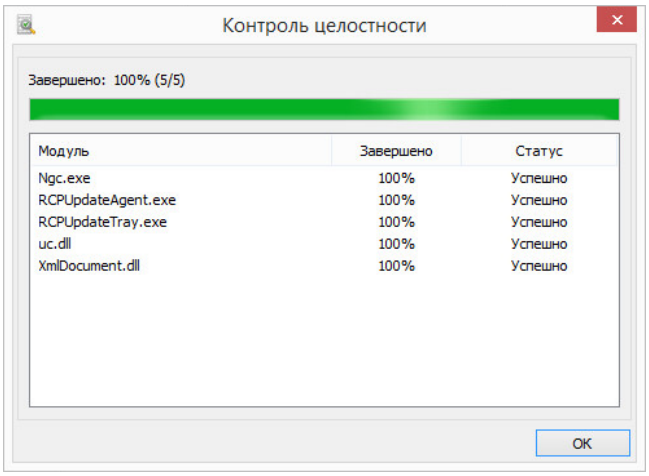
Примечание. По умолчанию при установке ПО РМ администратора АПКШ "Континент" файлы копируются на системный диск в папку \Program Files (x86)\Код Безопасности\Континент.

Принудительный запуск процедуры контроля целостности может выполнить только пользователь, входящий в локальную группу администраторов компьютера.

Для запуска процедуры контроля целостности:

1. Откройте папку ...\Континент\Update Agent и запустите на исполнение находящийся в ней файл ngc.exe.

   На экране появится окно программы "Контроль целостности" и начнется проверка целостности контролируемых файлов с отображением результатов для каждого из них.



2. После завершения проверки нажмите в окне "Контроль целостности" кнопку "OK".

   Окно программы закроется.

Документация

1. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9. Руководство администратора. Принципы функционирования комплекса.
2. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9. Руководство администратора. Ввод в эксплуатацию.
3. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9. Руководство администратора. Управление комплексом.
4. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9. Руководство администратора. Настройка VPN.