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 — комплекс, АПКШ "Континент"). В нем содержатся сведения, необходимые администраторам для управления системой обнаружения вторжений (компьютерных атак).

Дополнительные сведения, необходимые администратору комплекса, содержатся в [**1**]–[**6**].

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.

Версия — 3.9.3 от 20.06.2024.

Общие сведения

Назначение и основные функции

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

Основным компонентом СОВ является детектор компьютерных атак (детектор атак, ДА), обеспечивающий обнаружение следующих основных угроз безопасности информации:

- преднамеренный несанкционированный доступ или специальные воздействия на информацию (носители информации) со стороны внешних нарушителей, действующих из информационно-телекоммуникационных сетей, в том числе сетей международного информационного обмена;
- преднамеренный несанкционированный доступ или специальные воздействия на информацию (носители информации) со стороны внутренних нарушителей, обладающих правами и полномочиями на доступ к информации в информационной системе.

Детектор атак реализует следующие основные функции:

- сбор информации о пакетах данных;
- анализ собранной информации;
- оперативное реагирование на выявленные вторжения;
- оповещение ЦУС КШ о своей активности и о событиях, требующих оперативного вмешательства в режиме реального времени;
- регистрация событий, связанных с работой ДА;
- идентификация и аутентификация администратора при запуске ДА;
- контроль целостности программного обеспечения ДА.

Описание работы детектора атак

Детектор атак представляет собой программное средство, предварительно установленное на специализированной аппаратной платформе и предназначенное для работы в сетях с пропускной способностью 100 Мбит/с при средней длине сетевых пакетов 150 байт.

Детектор атак подключается по Т-образной схеме к SPAN-порту КШ либо к зеркалируемому порту маршрутизатора защищаемой подсети. Выявление компьютерных атак осуществляется на основе анализа полученного таким образом сетевого трафика. Сетевой интерфейс, захватывающий сетевой трафик для анализа, имеет тип "мониторинг".

Детектором атак поддерживаются следующие протоколы:

- сетевой уровень – ICMPv4, ICMPv6, IPv4, IPv6;
- транспортный уровень – TCP, UDP, SCTP;
- канальный уровень – PPPoE, PPP;
- прикладной уровень – FTP, HTTP, SMB, SSH, SMTP;
- сеансовый уровень – SSL, DCE/RPC.

Детектор атак контролирует следующие данные о сетевом трафике:

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

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

Метод сигнатурного анализа основан на применении набора решающих правил, предварительно загруженных в базу данных ЦУС и постоянно обновляемых с требуемой периодичностью. При этом обновление решающих правил может выполняться как автоматически по настраиваемому расписанию, так и вручную.

Автоматическое обновление решающих правил осуществляется специальным агентом – агентом обновлений, в функции которого входят проверка наличия новых обновлений, получение обновлений от поставщика и загрузка их в соответствии с расписанием в базу данных ЦУС.

Эвристический анализ позволяет выявить нежелательную активность контролируемых приложений и протоколов и может применяться в дополнение к сигнатурному анализу. В режиме эвристического анализа поддерживается работа с протоколами прикладного уровня, что позволяет контролировать следующие приложения:

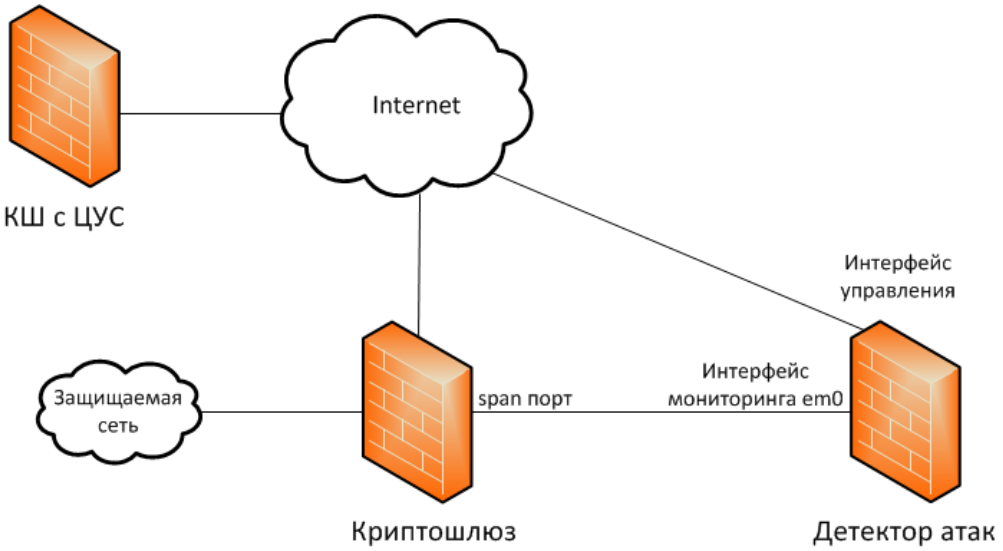
- P2P-сети (Bittorrent, Direct Connect, Bittorrent Link, FastTrack, OpenFT, eDonkey);
- аутентификация (Diameter, Kerberos,Radius);
- бизнес-приложения (Bloomberg, Google, Google Maps, Zoom);
- виртуализация (VMWare, VRRP);
- голосовая связь (Skinny, H.323, IAX, MGCP, H.248, SIP, Skype, TeamSpeak,WhatsApp Call);
- облачное хранилище (DropBox, Google Drive, Microsoft OneDrive);
- обмен сообщениями (IRC, ICQ, Signal, Telegram, Jabber, Viber, WhatsApp);
- передача файлов (AFP, FTP, LDAP, Rsync, TFTP);
- потоковое вещание (RTP, RTSP, TvAnts, Twitch, YouTube);
- сетевые функции (AMQP, Ayiya, BGP, Capwap, Collectd, DHCP, DNP3, DNS, Git, HTTP, IGMP, LLMNR, MQTT, Mining, Modbus, NFS, NetBIOS, NetFlow, QUIC, SMPP, SNMP, SSDP, STUN, Syslog, Teredo, UPnP, Windows update, Zabbix, ZeroMQ, ntop, sFlow);
- скрытая передача данных (Tor, Kazaa/Fasttrack, Gnutella, eDonkey, Bittorrent, HTTP Application Activesync, RemoteScan);
- социальные сети (Facebook, Instagram, LinkedIn, Twitter);
- удаленный доступ (Citrix, RDP, SMBv1,SMBv23, SSH, TeamViever, Telnet, VNC);
- электронная почта (Gmail, IMAP, POP3, SMTP);

События, связанные с работой ДА и обнаружением вторжений, регистрируются в его локальных журналах и средствами агента ЦУС передаются в базу данных. Просмотр событий осуществляется в программе просмотра журналов. Кроме того, в случае обнаружения вторжения или нарушения безопасности администратору отсылается сообщение по электронной почте, а в программе управления ЦУС появляется визуальное отображение зафиксированного НСД.

Примеры типовых вариантов использования детектора атак

Подключение детектора атак с одним интерфейсом мониторинга

На рисунке, представленном ниже, защищаемая корпоративная сеть предприятия находится за криптошлюзом АПКШ "Континент". Трафик между защищаемой сетью и сетями общего доступа (например, Интернет) зеркалируется на span- порт криптошлюза. Span- порт криптошлюза подключен к интерфейсу мониторинга детектора атак.

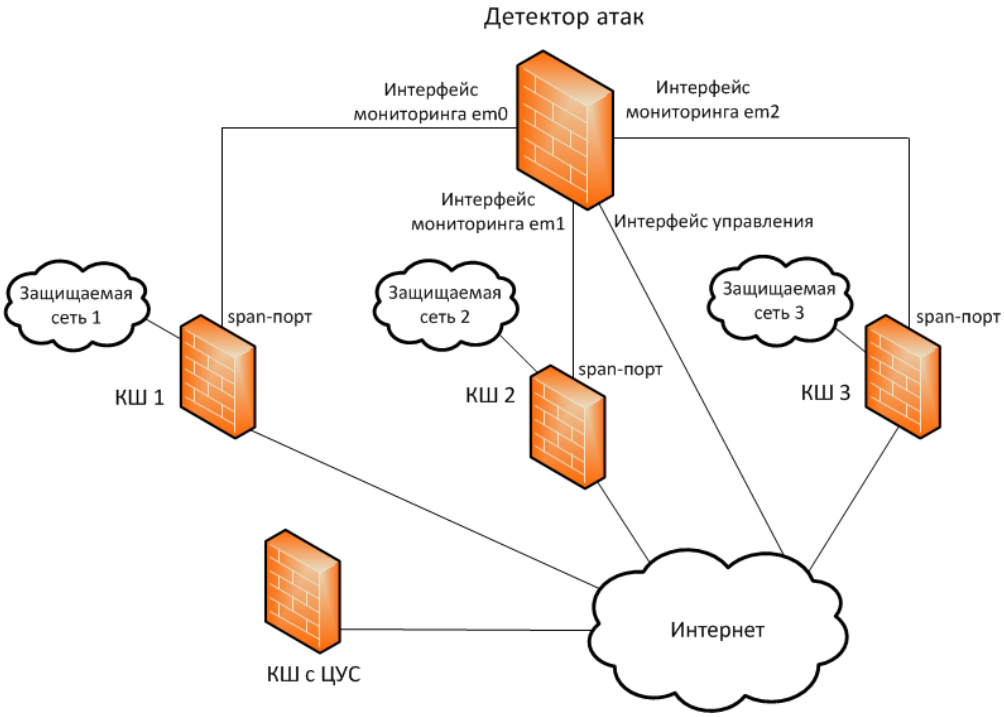


Команды управления от ЦУС поступают на интерфейс управления детектора атак по защищенному каналу.

Подключение детектора атак с несколькими интерфейсами мониторинга

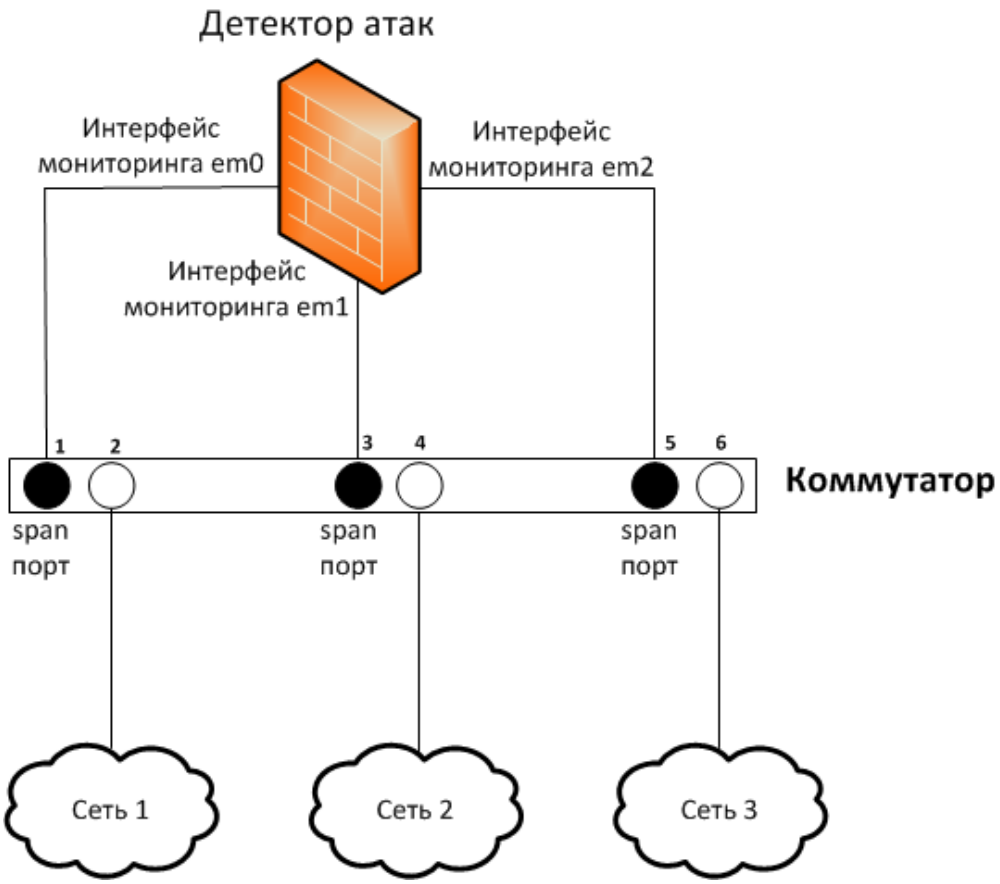
В зависимости от используемой аппаратной платформы в детекторе атак может быть настроено от одного до трех интерфейсов мониторинга. Это дает возможность одновременно контролировать и анализировать трафики, приходящие на каждый из таких интерфейсов.

На рисунке ниже показано подключение к детектору атак трех криптошлюзов АПКШ "Континент" (КШ1, КШ2, КШ3), каждый из которых зеркалирует трафик на свой span-порт.



Подключение детектора атак к коммутационному оборудованию сторонних производителей

Детектор атак может быть подключен к коммутационному оборудованию (маршрутизатору, коммутатору и пр.), имеющему в своем составе span-порт. На рисунке ниже показано подключение детектора атак к коммутатору с тремя span-портами (порты 1.3.5), на которые зеркалируются трафики с портов 2,4,6.



Управление системой обнаружения вторжений

Управление СОВ включает в себя следующие функции:

- подключение и начальная настройка параметров работы ДА;
- установка лицензии на обновление базы решающих правил;
- загрузка в БД ЦУС и обновление решающих правил;
- настройка параметров автоматической загрузки решающих правил;
- назначение решающих правил детекторам атак;
- включение/выключение ДА;
- управление режимами работы сигнатурного и эвристического анализаторов;
- добавление в БД ЦУС собственных правил (при необходимости).

Управление СОВ входит в функции администратора безопасности и выполняется как централизованно, так и локально. При этом некоторые функции в локальном управлении недоступны.

Централизованное управление осуществляется средствами ПУ ЦУС. При этом все действия, связанные с входом и выходом администратора из подсистемы управления, использующей ПУ ЦУС, регистрируются в системном журнале.

Локальное управление каждым из детекторов атак выполняется в его командном интерфейсе.

В соответствии с принципом разграничения прав доступа функции управления доступны только администратору безопасности.

Система обнаружения вторжений поддерживает следующие роли:

- главный администратор;
- администратор сети;
- аудитор;
- администратор ключей.

СОВ ассоциирует пользователей с ролями с помощью уникального идентификатора, предъявляемого пользователем при входе в систему. Этот идентификатор создается при добавлении новой учетной записи.

Набор прав пользователя на управление СОВ средствами централизованного управления зависит от присвоенной ему роли.

Организация работы администраторов комплекса средствами централизованного управления представлена в [**3**].

Доступ к командному интерфейсу локального управления ДА предоставляется только пользователю, имеющему права на администрирование ПАК "Соболь". Права на локальное управление определяются при идентификации пользователя средствами ПАК "Соболь" (см. документацию на это изделие).

Контроль целостности

Функция контроля целостности (КЦ) предназначена для слежения за неизменностью содержимого установленного программного обеспечения ДА. Действие функции основано на сравнении текущих значений содержимого контролируемых файлов и значений, принятых за эталон.

Перечни контролируемых файлов ПО детектора атак и агента обновлений устанавливаются производителем и изменению не подлежат (см. стр. **45**). Эталонные значения рассчитываются при установке или обновлении программного обеспечения. Прочие возможности модификации контрольных сумм исключены.

Контроль целостности ПО детектора атак

Контроль целостности файлов ПО детектора атак осуществляется средствами ПАК "Соболь".

Списки контролируемых объектов и значения их контрольных сумм хранятся в виде файлов-шаблонов на жестком диске компьютера. Контрольные суммы самих файлов-шаблонов хранятся в защищенной памяти платы ПАК "Соболь". Для расчета контрольных сумм используется алгоритм ГОСТ 28147–89 в режиме выработки имитовставки.

Проверка контрольных сумм контролируемых объектов осуществляется при входе администратора и пользователей в систему. Сначала рассчитываются контрольные суммы файлов-шаблонов и сравниваются со значениями, сохраненными в защищенной памяти платы ПАК. После этого рассчитываются и проверяются контрольные суммы всех контролируемых объектов. При обнаружении нарушения целостности файлов-шаблонов или контролируемых объектов в журнале событий регистрируется событие "Ошибка при контроле целостности", а работа ДА блокируется. Использование модифицированного ПО становится невозможным.

Контроль целостности ПО агента обновлений

Эталонные значения рассчитываются при установке или обновлении программного обеспечения агента обновлений.

Перечень контролируемых файлов и рассчитанные для них при установке программного обеспечения контрольные суммы содержатся в файле integrity.xml. Файл хранится в папке ...\Континент\Update Agent. Контрольные суммы рассчитываются по алгоритму, определенному ГОСТ Р 34.11-2012.

Проверка контрольных сумм выполняется автоматически при запуске программы управления агентом обновлений. Также проверка может быть выполнена вручную пользователем, входящим в группу локальных администраторов компьютера.

Результаты проверки заносятся в журнал приложений ОС Windows. При отрицательном результате проверки на экран выводится сообщение "Нарушена целостность файлов агента обновлений БРП. Обратитесь к системному администратору", и запуск программы управления агентом будет заблокирован.

Глава 1
Ввод в СОВ эксплуатацию

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. **16**).
4. Загрузка БРП в БД ЦУС (см. стр. **17**).

   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. Регистрация ДА в БД ЦУС. Выполняется отдельно для каждого ДА (см. стр. **26**).
6. Запись конфигурации ДА и ключей на отчуждаемый носитель. Выполняется отдельно для каждого ДА (см. стр. **29**, стр. **29**).
7. Инициализация и подключение ДА. Выполняется локально для каждого ДА (см. стр. **29**).
8. Настройка режима работы ДА. Выполняется отдельно для каждого ДА (см. стр. **26**).
9. Назначение правил. Выполняется для каждого зарегистрированного ДА (см. стр. **32**).
10. Настройка автоматического обновления БРП (см. стр. **39**).

Глава 2
Управление системой обнаружения вторжений

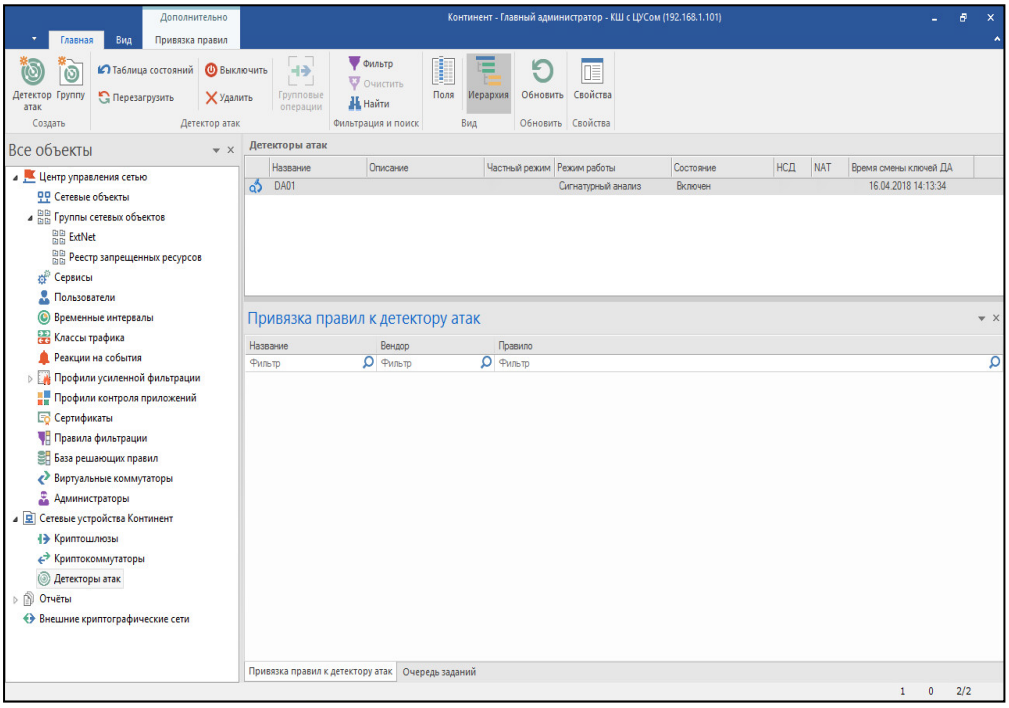
Управление СОВ включает в себя настройку детекторов атак и периодического обновления базы решающих правил. Настройка выполняется администратором в ПУ ЦУС. Для работы с детекторами атак и решающими правилами в ПУ ЦУС в области объектов управления выбирают соответственно пункт "Детекторы атак" или "База 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. 17.

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 3
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.

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

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

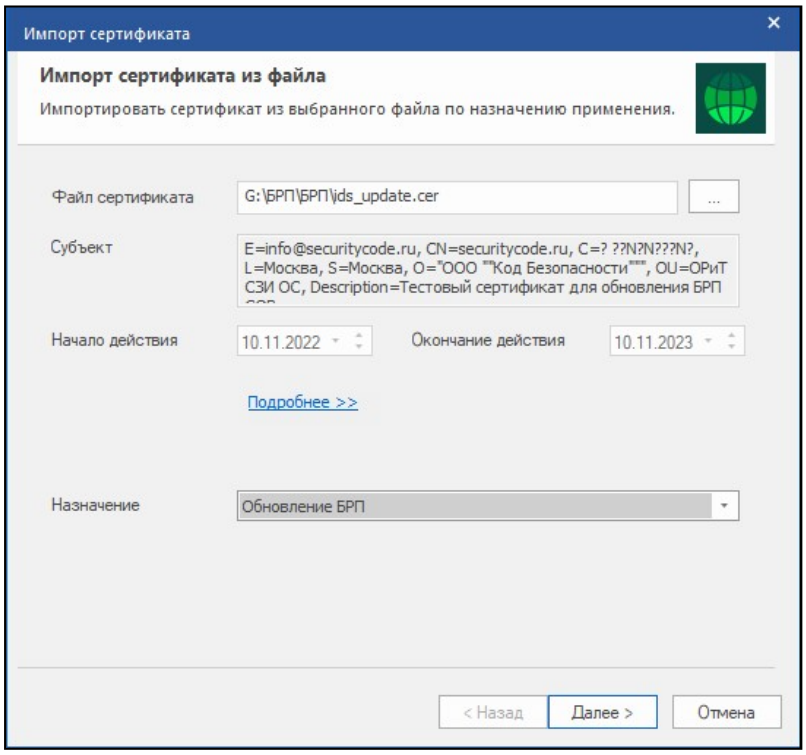
   На экране появится окно "Импорт сертификата".

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

   На экране появится стандартное окно Windows для открытия файла.

4. Укажите папку и затем файл сертификата.

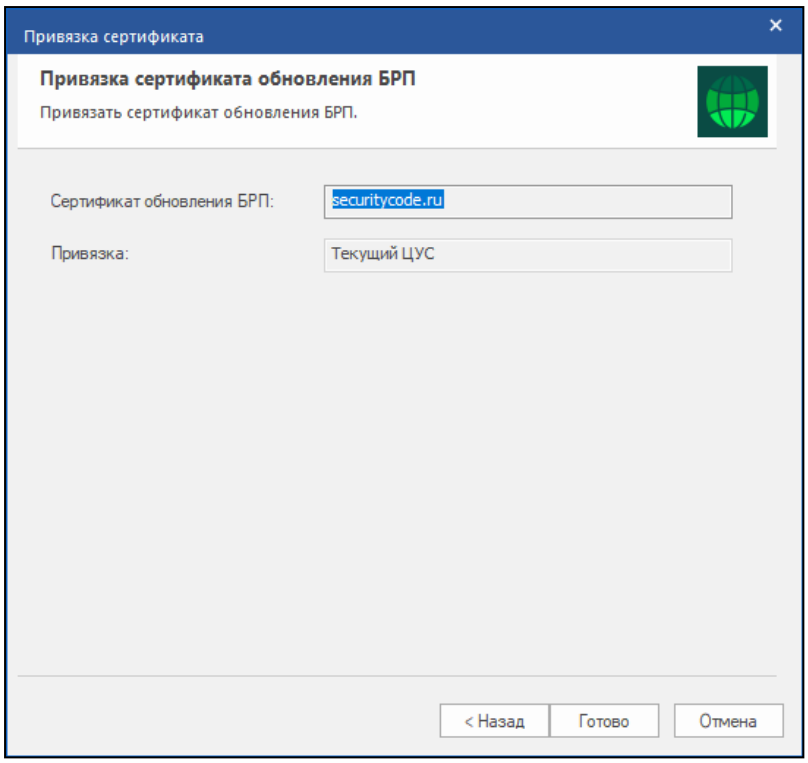
   На основании сведений, содержащихся в указанном сертификате, заполнятся поля "Субъект", "Начало действия" и "Окончание действия".



   Примечание. 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. **39**).

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. **16**).

Автоматическая загрузка правил

Загрузка правил в БД ЦУС осуществляется агентом обновлений в соответствии с настроенным расписанием.

Для связи агента обновлений с сервером обновлений используется защищенное соединение, устанавливаемое абонентским пунктом по команде агента. Для установления защищенного соединения на абонентском пункте должны быть зарегистрированы сертификаты (пользовательский и корневой), а также должны быть предъявлены ключи шифрования.

После получения от сервера сведений об имеющихся обновлениях агент обращается к ЦУС и получает от него данные о последних обновлениях в БД ЦУС. При обнаружении на сервере новых обновлений, отсутствующих в БД ЦУС, агент скачивает их, сохраняет в определенной папке на жестком диске и затем загружает в ЦУС.

При загрузке правил (обновлений) ЦУС выполняет проверку цифровой подписи поставщика правил, используя предварительно загруженный в БД ЦУС сертификат. Если сертификат поставщика в БД ЦУС отсутствует или является недействительным, загрузка правил (обновлений) в БД ЦУС отменяется.

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

- сертификат обновлений;
- сертификат пользователя;
- 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. Средствами ПУ ЦУС настроить расписание автоматического обновления БРП (см. стр. **42**).
2. Подготовить внешний носитель с ключами ЦУС.
3. Настроить агент обновлений для связи с ЦУС (см. стр. **43**).

Загрузка правил вручную

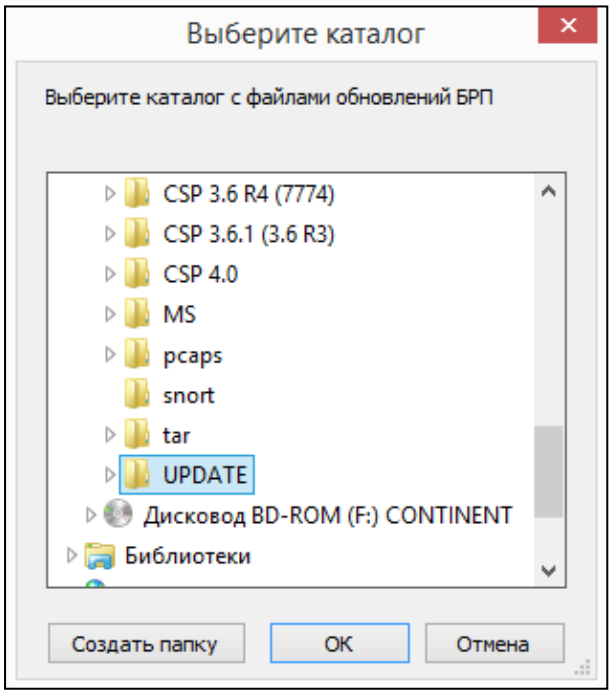
Загрузка правил в БД ЦУС осуществляется администратором с USB-флеш-накопителя.

Для загрузки правил:

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

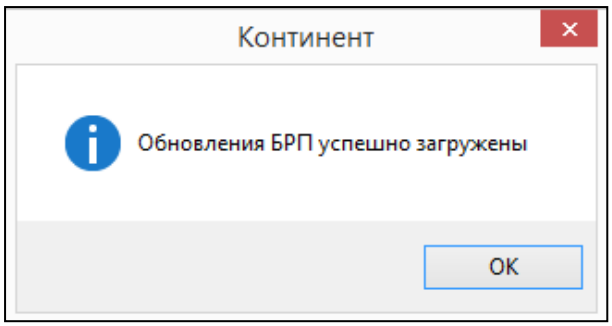
   В области отображения информации появится список групп загруженных в БД ЦУС правил.
2. Вставьте USB-флеш-накопитель с записанными на нем решающими правилами (обновлениями).
3. В панели инструментов нажмите кнопку "Загрузить".

   На экране появится стандартное окно выбора каталога.



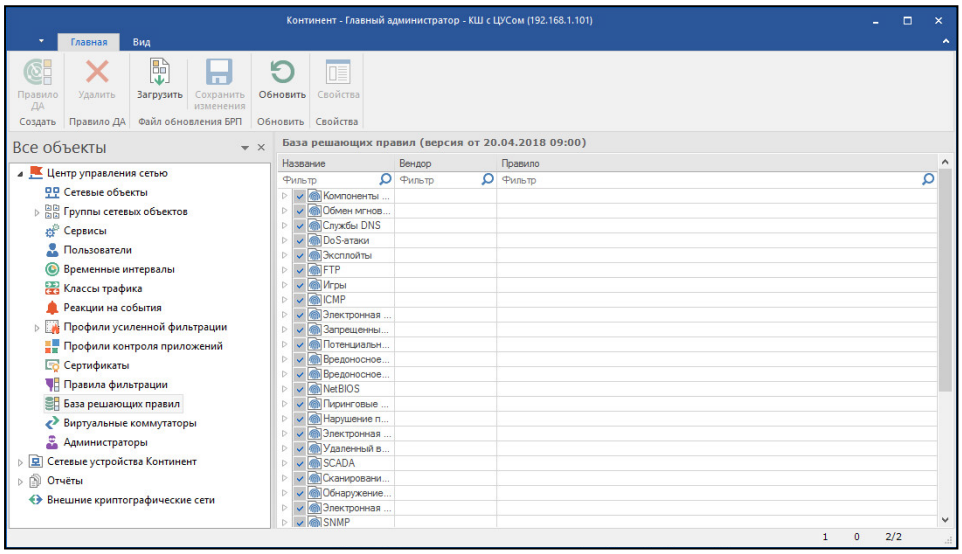
4. Укажите каталог, содержащий файлы с решающими правилами, и нажмите кнопку "OK".

   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.



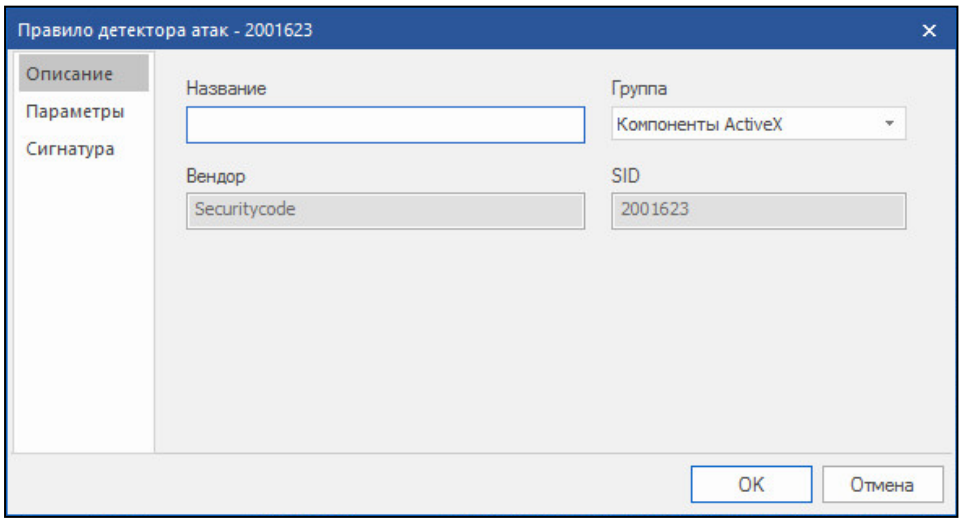
Просмотр и редактирование правил

Просмотр параметров правил без возможности их редактирования доступен при работе со списком детекторов атак (см. стр. **30**).

Для редактирования параметров правила:

1. Откройте список правил (см. стр. **14**).
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.



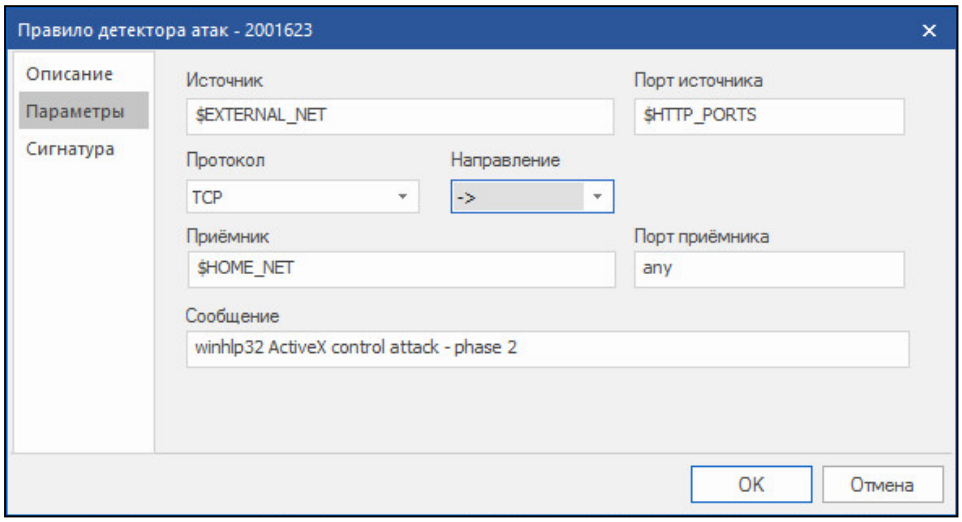
3. При необходимости изменить название правила вручную отредактируйте содержимое поля "Название".

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

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

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

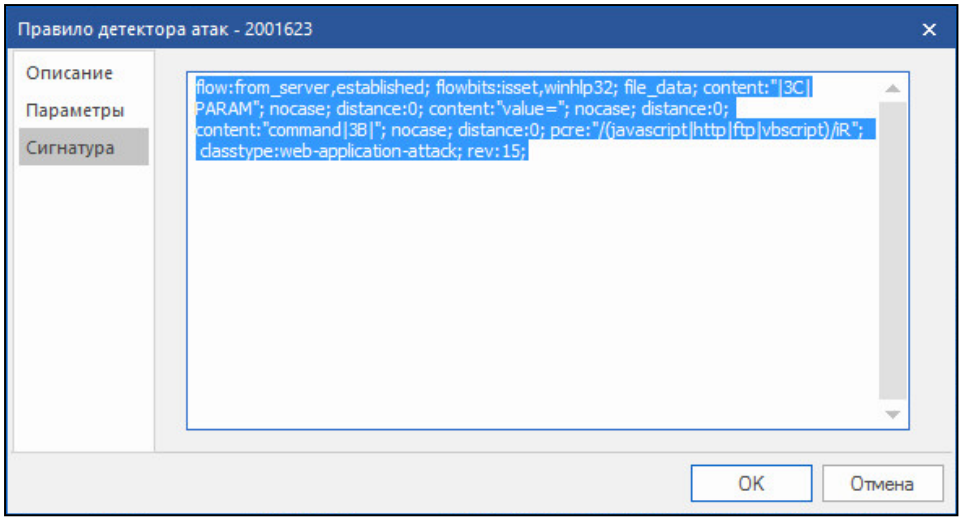
4. Для редактирования параметров правила перейдите на вкладку "Параметры".



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. **48**).
8. Для завершения процедуры редактирования нажмите кнопку "OK".

   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. **14**).
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. **48**) и нажмите кнопку "OK".

   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. **14**).

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.

Агент обновлений

Агент обновлений предназначен для получения решающих правил и их обновлений от сервера поставщика правил (сервера обновлений). Полученные правила и обновления записываются средствами агента обновлений на внешний носитель и далее вручную загружаются в БД ЦУС.

Агент устанавливают на компьютер, на котором установлен абонентский пункт версии не ниже 4.1. При этом абонентский пункт используется исключительно для установления защищенного соединения с сервером обновлений.

Установка программного обеспечения абонентского пункта описана в документации на этот продукт. При установке ПО абонентского пункта необходимо выполнить следующее:

- в окне "Конфигурация АП" выбрать вариант "Использовать настройки по умолчанию" и не изменять значение параметра "Адрес сервера доступа".
- в разделе "Параметры | Основные" окна АП снять отметку для параметра "Проверять сертификаты по CRL".

После установки ПО настройка параметров абонентского пункта не требуется.

Установка агента

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 | Континент 4.1" появится команда "Программа управления агентом обновлений БРП".

Далее в рамках подготовки агента обновлений к работе необходимо выполнить следующее:

1. Запустить программу управления агентом (см. стр. **23**).
2. Запустить агента (см. стр. **24**).

Программа управления агентом обновлений

Программа используется для локального управления агентом обновлений.

После завершения процедуры установки агента программа изначально находится в выключенном состоянии. Для управления агентом программу необходимо запустить.

Для запуска программы управления:

- Активируйте в главном меню Windows команду "Пуск | Все программы | Код Безопасности | Континент 4.1 | Программа управления агентом обновлений БРП".

  В правой части панели задач Windows появится пиктограмма программы управления агентом обновлений.

  Цвет пиктограммы указывает на состояние агента обновлений:

	Зеленый	Агент запущен
	Красный	Агент остановлен

Примечание.
Программа управления агентом обновлений запускается автоматически при перезагрузке компьютера. При этом агент остается в состоянии "остановлен".

После запуска программы управления становятся доступными команды контекстного меню пиктограммы в панели задач.

При выключении программы управления пиктограмма из панели задач удаляется и вызов контекстного меню становится невозможным. При этом агент, если он был запущен, продолжает свою работу.

Команды управления агентом обновлений

Ниже в таблице приведены все команды программы управления агентом обновлений.

Название команды	Описание
Запустить агент	Осуществляет запуск агента
Остановить агент	Осуществляет остановку агента
Импорт сертификата сервера обновлений	Запускает процедуру установки сертификата пользователя и корневого сертификата на компьютер
Обновление БРП...	Открывает диалог, предназначенный для получения обновлений решающих правил от сервера обновлений
Отключить уведомления об ошибках	Отключает/включает вывод всплывающих сообщений об ошибках в работе агента
Журнал приложений системы	Вызывает на экран журнал приложений Windows
О программе…	Открывает окно, содержащее сведения о номере версии программы управления агентом, а также сведения об авторских правах на программный продукт
Выход	Осуществляет выход из программы управления агентом и удаляет пиктограмму с панели задач. Внимание! При удалении пиктограммы агент не выключается!

Все команды, приведенные в таблице, доступны только пользователю, входящему в локальную группу администраторов компьютера.

Пользователям, не входящим в локальную группу администраторов, при открытии контекстного меню доступны только следующие команды:

- Журнал приложений системы;
- О программе;
- Выход;
- Отключить уведомления об ошибках (только для просмотра установленного режима).

Запуск агента

Для запуска агента:

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

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

Для остановки агента:

- Вызовите контекстное меню пиктограммы программы управления и выберите команду "Остановить агент".

  Агент будет остановлен и цвет пиктограммы в панели задач изменится с зеленого на красный.

Внимание! При перезагрузке системы происходит автоматический запуск агента.

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".

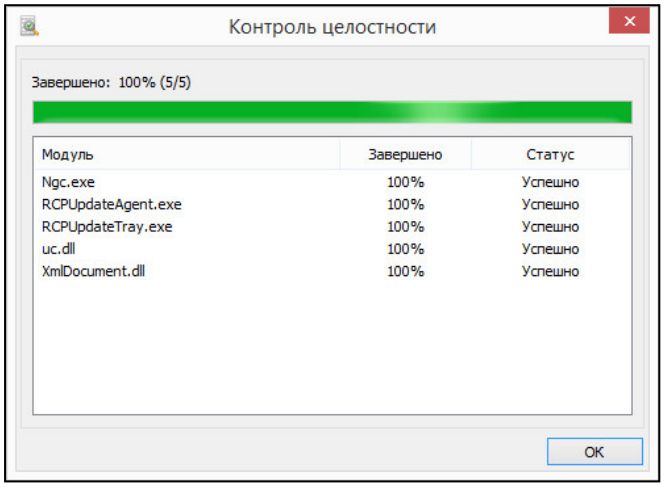
Примечание.
По умолчанию при установке ПО РМ администратора АПКШ "Континент" файлы копируются на системный диск в папку \Program Files (x86)\Код Безопасности\Континент.

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.

Глава 4
Централизованное управление детекторами атак

Настройка детектора атак

Для настройки ДА:

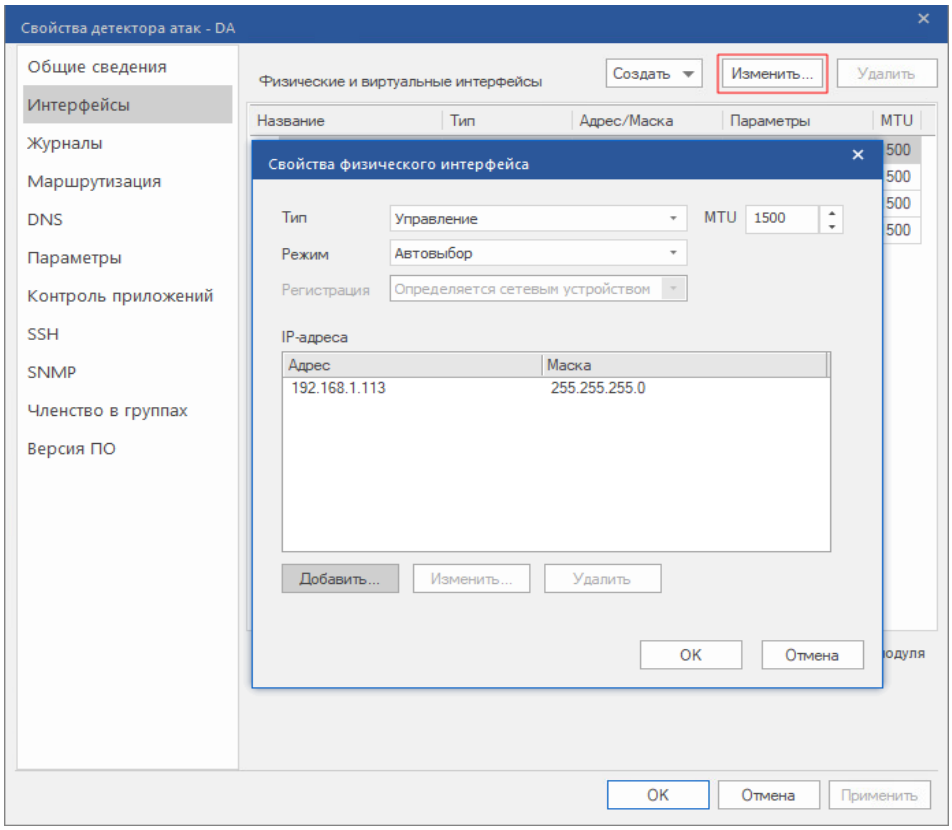
1. Выберите в области объектов управления главного окна ПУ ЦУС пункт "Сетевые устройства Континент | Детекторы атак", затем требуемый ДА в списке и нажмите кнопку "Свойства" на панели инструментов.

   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.

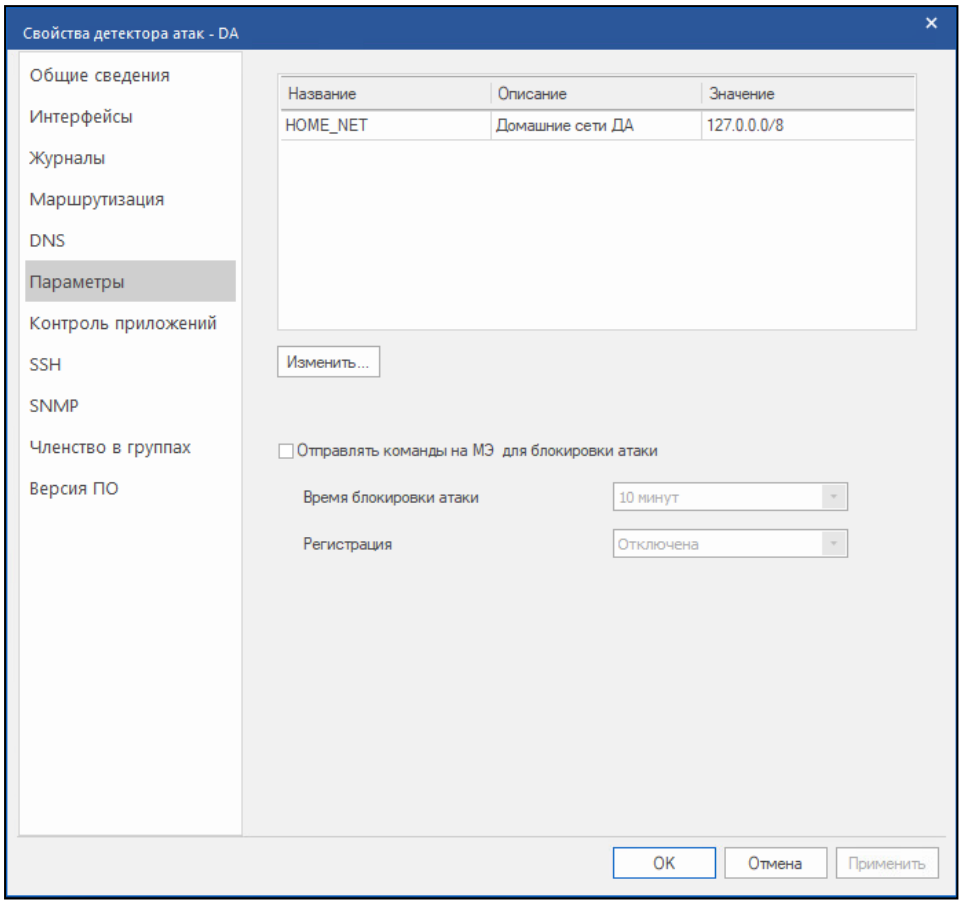
3. Перейдите на вкладку "Интерфейсы", настройте параметры интерфейсов управления и мониторинга, выбрав их в списке и нажав кнопку "Изменить...".



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 интерфейсовприведено в [3].

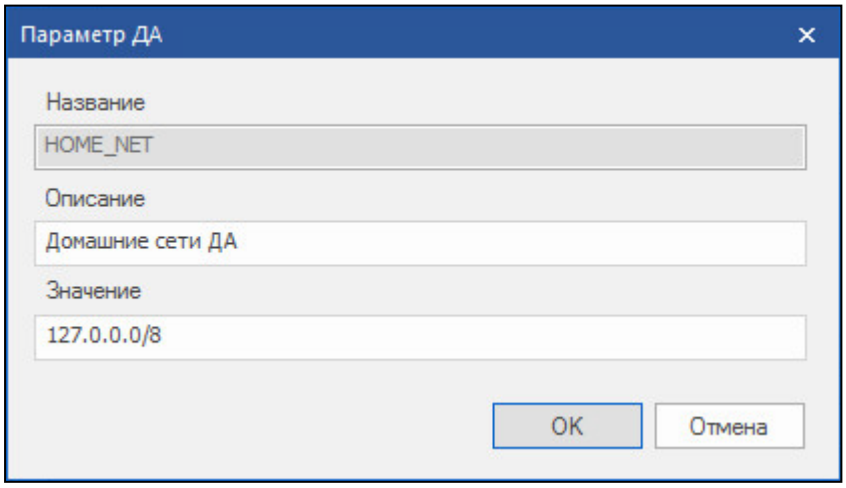
4. Перейдите на вкладку "Параметры".



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".

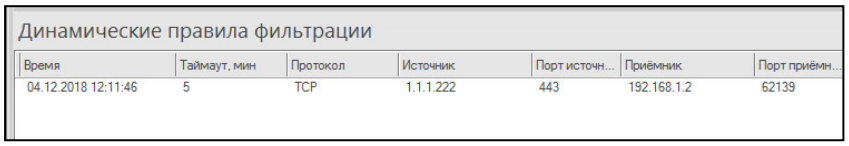


6. При необходимости внесите изменения в поле "Описание".
7. В поле "Значение" удалите отображаемую по умолчанию подсеть, укажите через запятую подсети, которые должны контролироваться данным детектором атак, и нажмите кнопку "OK".

   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.



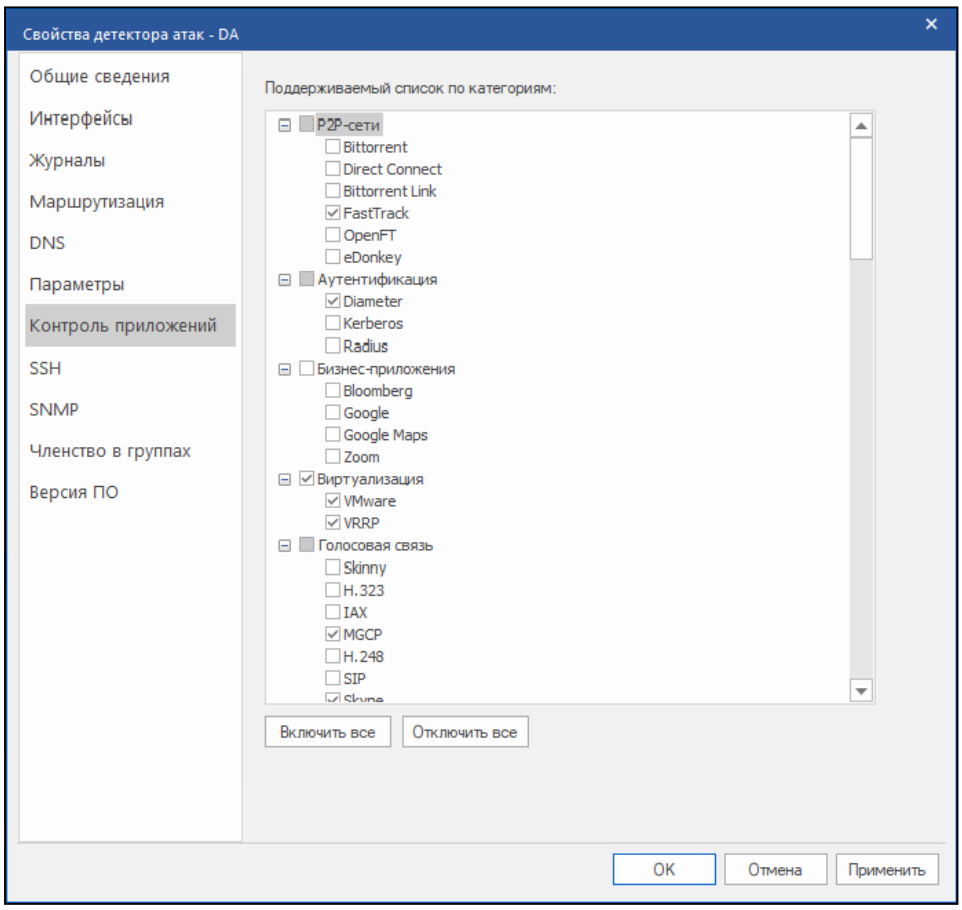
Внимание!
Для блокирования атаки ее адресат должен быть в составе защищаемой сети, определяемой параметром HOME_NET.

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".

Запись конфигурации на носитель

Для инициализации зарегистрированного ДА необходимо средствами ПУ ЦУС записать его конфигурацию на отчуждаемый носитель (USB-флеш-накопитель) для последующей локальной загрузки в ДА.

Конфигурацию ДА записывают на носителе в файл ids-<id>.cfg, где id — идентификатор ДА.

Для записи конфигурации:

1. Предъявите носитель для записи конфигурации.
2. В списке детекторов атак в контекстном меню зарегистрированного ДА активируйте команду "Сохранить конфигурацию ДА".

   На экране появится диалог "Сохранение конфигурации ДА".
3. Заполните поля диалога и нажмите кнопку "ОК".

Пароль	Пароль, с помощью которого будет ограничен доступ к сохраняемой конфигурации ДА. Длина пароля должна составлять не менее 5 символов. Этот пароль запрашивается при считывании конфигурации детектором атак
Подтверждение	Подтверждение пароля
Режим	Доступно только значение "Основной"
Имя файла	Полное имя файла ids-<id>.cfg. Для вызова стандартного диалога сохранения файла используйте кнопку "…"

   После успешного завершения записи конфигурации ДА на экране появится сообщение об этом. Закройте окно этого сообщения.

Запись ключей на носитель

Для функционирования ДА требуются главный ключ и ключ связи с ЦУС. Эти ключи предъявляют при инициализации ДА в виде файла с именем ids-<ID>.keyset, где ID — идентификатор узла, хранящегося на отдельном USB-флеш-накопителе.

Для записи ключей:

1. Предъявите носитель для записи ключей.
2. В списке детекторов атак в контекстном меню зарегистрированного ДА активируйте команду "Сохранить текущие ключи на носитель".

   На экране появится диалог назначения пароля.
3. Введите и подтвердите пароль.

   На экране появится стандартный диалог выбора каталога для хранения ключей.
4. Укажите в качестве каталога предъявленный носитель.

   В результате успешной записи ключей на носитель появится сообщение "Текущие ключи детектора атак сохранены".

Инициализация и подключение детектора атак

Для инициализации и подключения зарегистрированного в БД ЦУС детектора атак необходимо иметь предварительно записанные на USB-флеш-накопителе файл конфигурации и ключи (см. стр. **29**, стр. **29**).

Процедура инициализации и подключения ДА выполняется локально и полностью совпадает с аналогичной процедурой для КШ (см. [**3**]).

После завершения инициализации перейдите к настройке режима работы ДА.

Просмотр и изменение свойств детектора атак

Для просмотра и изменения свойств ДА:

1. Выберите в списке нужный ДА и вызовите диалог "Свойства детектора атак" одним из следующих способов:
   - нажмите кнопку  в панели инструментов;
   - наведите курсор на строку ДА в списке и дважды нажмите левую кнопку мыши;

- вызовите контекстное меню для строки детектора атак и выберите команду "Свойства".

На экране появится диалог "Свойства детектора атак", открытый на вкладке "Общие сведения".

2. При необходимости внесите изменения в значения параметров, нажмите кнопку "Применить" и перейдите на следующую вкладку.

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.

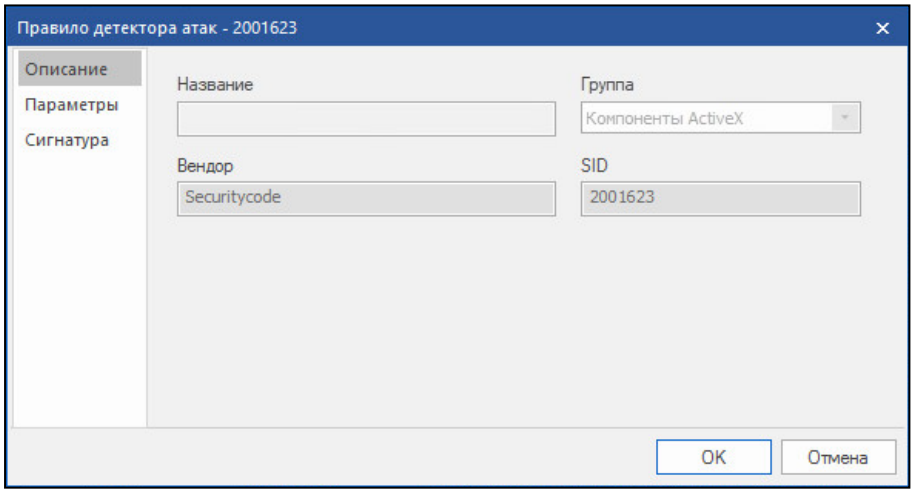
Для просмотра правил:

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.

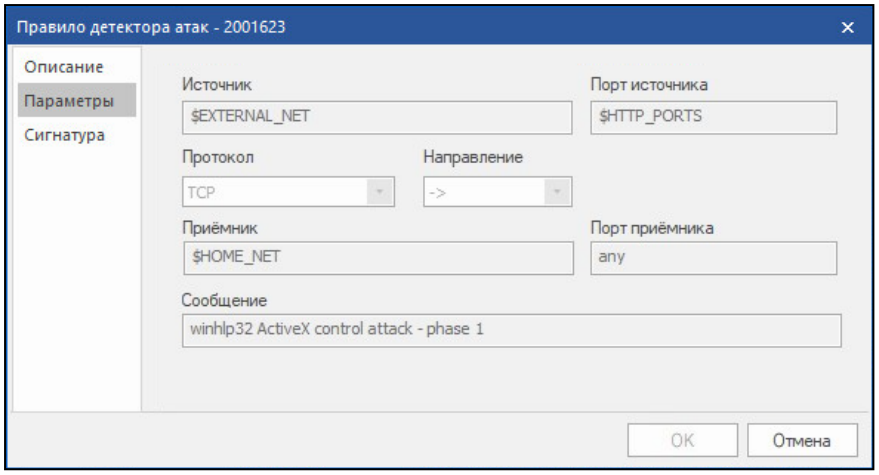
   На экране появится окно "Правило детектора атак", открытое на вкладке "Описание".



На вкладке представлены значения общих параметров правила:

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

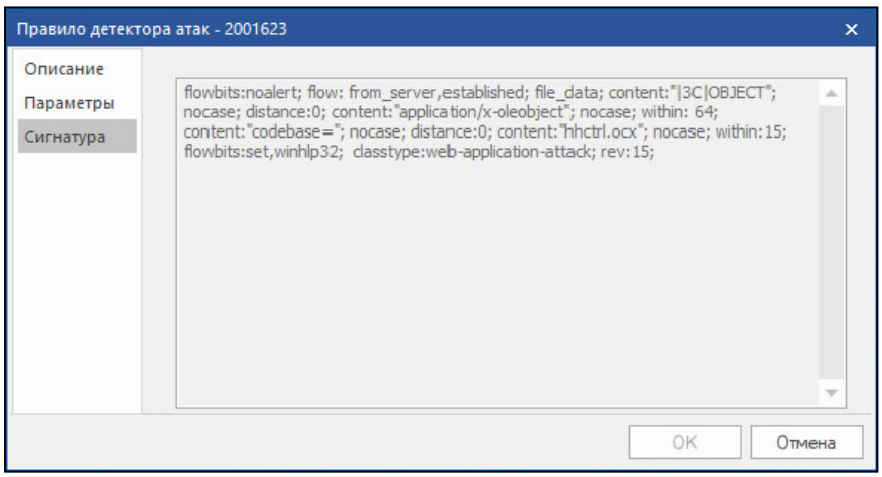
4. Перейдите на вкладку "Параметры".



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.

Просмотр параметров правил

В данном режиме просмотра редактирование параметров правил недоступно.

Для просмотра параметров правил:

1. В дополнительном окне установите курсор на строку правила и дважды нажмите левую кнопку мыши.

   На экране появится диалог "Правило детектора атак", открытый на вкладке "Описание". Подробнее описание вкладок см. стр. **30**.

2. Для завершения просмотра параметров правила нажмите кнопку "Отмена".

   Диалог "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).

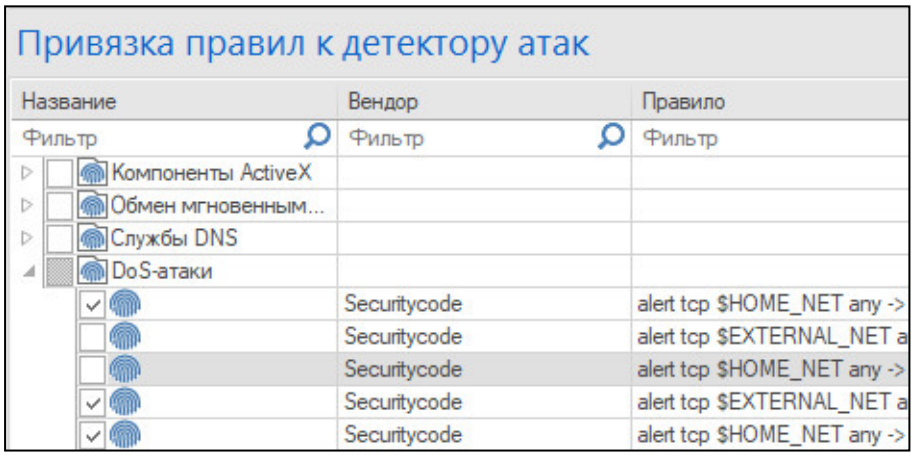
Для улучшения производительности СОВ рекомендуется назначение только актуальных для защищаемой сети решающих правил. Например, если VoIP-сервисы не используются, следует отключить правила для VoIP-трафика.

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. **19**).

   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 5
Локальное управление детектором атак

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. **36**), 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. **33**).
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. **33**).
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

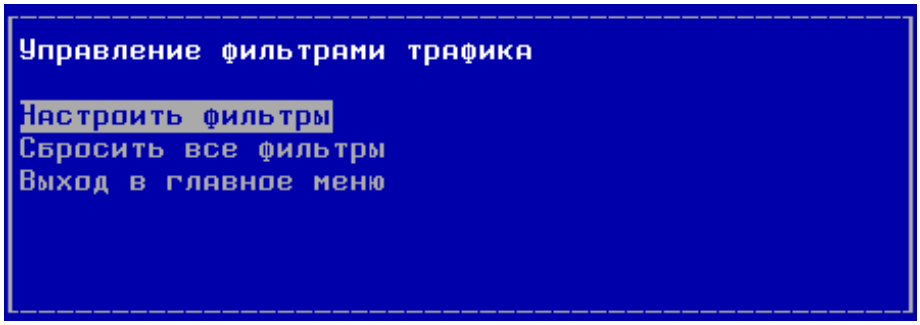
Данные настройки позволяют устанавливать и настраивать на интерфейсах мониторинга фильтры с целью снижения нагрузки на систему. В результате будет производиться анализ только тех пакетов, которые соответствуют параметрам фильтра. Такими параметрами могут быть, например, тип протокола, IP-адрес, источник/получатель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

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

Для работы с фильтрами:

1. Войдите в меню настройки ДА (см. стр. **33**).
2. Введите номер команды "Фильтры трафика" и нажмите клавишу <Enter>.

   На экране появится меню "Управление фильтрами трафика".



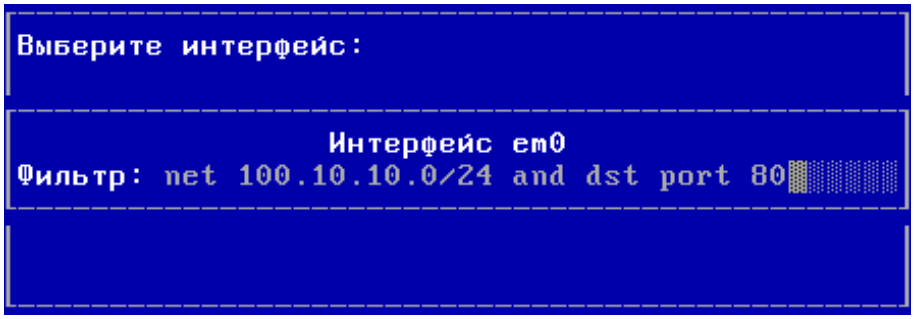
Для настройки фильтров:

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. 68).

   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 следующие сведения: • тип аппаратной платформы; • версия, контрольная сумма и конфигурация ПО; • идентификатор СУ; • статус мягкого режима (вкл/выкл); • ввод в эксплуатацию (да/нет). Если устройство входит в состав кластера, отображается статус – основной/резервный. Дополнительные сведения для ЦУС: • режим работы ЦУС в кластере (активный/пассивный); • дата и время последнего изменения БД ЦУС
Ключи и носители	Отображает на экране следующий список команд: подготовить ключ, присланный с ЦУС; информация о загруженных ключах; выход
Вывести полный список интерфейсов	Отображает на экране список всех интерфейсов с возможностью сохранения информации в файл и экспорта его на внешний носитель информации
Вывести таблицы маршрутизации	Отображает на экране таблицы маршрутизации для протоколов IPv4 и IPv6 с возможностью сохранения информации в файл и экспорта его на внешний носитель информации
Диагностика	Выводит на экран меню команд диагностики (см. Табл.2)

Команда	Описание
Перезагрузка	Запускает перезагрузку сетевого устройства
Завершение работы	Выключает электропитание сетевого устройства
Выход	Закрывает дополнительное меню

Табл.2 Команды меню "Диагностика"

Команда	Описание
Загруженность ЦП	Отображает на экране информацию о загруженности каждого процессора
Использование памяти	Отображает на экране общий, используемый и свободный объем оперативной памяти
Использование жесткого диска	Отображает на экране общий объем жесткого диска, а также объем используемого и свободного пространства
Выполнить ping*	Запускает на компьютере команду ping и отображает на экране результаты выполнения этой команды. Укажите IP-адрес, соединение с которым необходимо проверить
Выполнить traceroute*	Запускает на компьютере команду traceroute и отображает на экране результаты выполнения этой команды. Укажите IP-адрес, маршрут к которому требуется определить
Выполнить arp/ndp	Отображает на экране содержимое ARP- и NDP-кеша с возможностью сохранения результатов в файл и экспорта его на внешний носитель информации
Сведения о сетевых соединениях	Отображает на экране сведения об открытых сетевых соединениях с возможностью сохранения информации в файл и экспорта его на внешний носитель информации
Количество пропущенных пакетов	Отображает на экране количество пакетов, пропущенных при диагностике прохождения пакетов
Просмотр дампа сетевого трафика	Отображает на экране информацию о сетевом трафике. Для запуска команды задайте имя тестируемого интерфейса, фильтр в формате команды tcpdump и количество пакетов для просмотра. Есть возможность сохранения результатов в файл и экспорта его на внешний носитель информации. Для сетевого устройства, выведенного из эксплуатации, предусмотрено сохранение информации в двоичном коде для последующего просмотра в специализированном приложении
Сведения о состоянии журналов	Отображает на экране максимальные и текущие объемы журналов
Сохранить конфигурацию и журналы событий динамической маршрутизации**	Записывает конфигурационные файлы на отчуждаемый носитель
Сохранить технологическую информацию	Выгружает на отчуждаемый носитель технологический отчет для отправки в службу поддержки. Файл отчета получит имя debug_report_DDMMYYYY_HHMMSS.dump, где DDMMYYYY_HHMMSS - дата и время его создания
Сохранить отладочные журналы	Выгрузка информации системных журналов на USB-флеш-накопитель в файл syslog
Командная строка	Переход в режим командной строки (Continent Shell). Выход по команде exit
Идентифицировать интерфейсы***	Запускает идентификацию выбранного порта на корпусе сетевого устройста
Выход	Закрывает меню "Диагностика"

- *Для выполнения команд ping и traceroute на КШ автоматически создаются временные правила фильтрации, разрешающие прохождение соответствующих пакетов.

- **Для сохранения журналов событий в конфигурационном файле для используемых протоколов маршрутизации должна быть включена функция логирования (Log stdout) и указан путь к файлу журнала. Например, для протокола BGP: log file /var/bgpd.log.
- ***Работоспособность зависит от типа порта.

Глава 6
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. 18).

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. Средствами ПУ ЦУС настроить расписание автоматического обновления БРП (см. стр. 42).
3. Настроить агент обновлений (см. стр. 43).

Глава 6

Порядок настройки 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. 18).

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. Средствами ПУ ЦУС настроить расписание автоматического обновления БРП (см. стр. 42).
3. Настроить агент обновлений (см. стр. 43).

Установка агента

Примечание.
Агент устанавливают на компьютер, на котором установлен абонентский пункт версии 4.1.

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".

В рамках подготовки агента обновлений к работе необходимо выполнить настройку абонентского пункта:

1. В меню "Пуск" выберите пункт "Все приложения | Код Безопасности | Континент-АП" или дважды нажмите левой кнопкой мыши на значок "Континент-АП".
2. Выберите пункт "Сертификаты" на панели навигации, а затем перейдите на вкладку "Корневые сертификаты".
3. На панели инструментов нажмите кнопку "Импортировать".

   На экране появится стандартное окно открытия файла.
4. Укажите файл корневого сертификата, полученного от поставщика, и нажмите кнопку "Открыть".

   Начнутся загрузка и установка сертификата. После успешного завершения операции на экране появится соответствующее информационное сообщение.
5. Нажмите кнопку "ОК".
6. Перейдите на вкладку "Пользовательские сертификаты" и на панели инструментов нажмите кнопку "Импортировать".

На экране появится диалог настройки параметров импорта.

7. В поле "Имя файла" укажите полный путь и имя файла, содержащего полученный от поставщица сертификат пользователя. Нажмите кнопку "Далее".
8. В раскрывающемся списке "Хранилище сертификатов" выберите тип хранилища "Локальный компьютер".
9. Для выбора расположения хранилища сертификатов выберите опцию "Поместить все сертификаты в следующую папку" и укажите папку "Личное". Нажмите кнопку "Далее".

   Появится окно запроса контейнера закрытого ключа сертификата.
10. Выберите требуемый контейнер и нажмите кнопку "Далее".

    На экране появится завершающий диалог мастера установки сертификата.
11. Нажмите кнопку "Готово".

    При импорте пользовательского сертификата появится окно запроса пароля к контейнеру закрытого ключа сертификата.
12. Введите требуемый пароль и нажмите кнопку "ОК".

    Начнутся загрузка и установка сертификата в указанное хранилище. После успешного завершения операции на экране появится соответствующее информационное сообщение.
13. Нажмите кнопку "ОК".
14. На панели навигации выберите пункт "Профили" и нажмите кнопку "Добавить" на панели инструментов.

    В правой части области отображения информации основного окна появится список настроек профиля.

Примечание.
При использовании абонентского пункта с агентом обновлений БРП должен использоваться только один профиль для подключения к централизованному серверу обновлений.

15. Выполните следующие настройки профиля:
    - Установите отметки в полях "Глобальный профиль" и "Использовать по умолчани".
    - Введите имя профиля в соответствующем поле.
    - В поле "Сертификат" выберите пользовательский сертификат.
    - Добавьте в список адресов СД адрес ids-update.securitycode.ru.
16. Нажмите кнопку "Сохранить".
17. Выполните подключение к СД. При первом подключении установите актуальную цепочку сертификатов сервера.
18. После успешного подключения отключитесь от СД, дальнейшее управление будет осуществляться с помощью агента обновлений БРП и ПУ ЦУС.

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
	Серый	Агент остановлен

Команда контекстного меню	Описание
Запустить агент	Запуск агента
Остановить агент	Остановка агента
Параметры агента…	Открытие окна параметров агента для просмотра и редактирования

Команда контекстного меню	Описание
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.

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. **16**).

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) задан по умолчанию.

   В окне представлены два варианта настройки расписания.
2. 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, в поле "Начиная с" нажмите пиктограмму и выберите дату в выпадающем календаре, затем установите время, используя стрелки в правой части поля
Еженедельное расписание	Включает режим загрузки обновлений, при котором запуск процесса осуществляется в моменты времени, заданные специальным расписанием. Расписание представлено в виде таблицы. В столбцах таблицы перечислены дни недели, а в строках — время запуска процесса. Для добавления строки нажмите пиктограмму , для удаления — . Чтобы изменить время запуска процесса, щелкните два раза левой кнопкой мыши в соответствующей ячейке таблицы и введите нужные значения. Выбор дня недели осуществляется посредством установки отметки в соответствующей ячейке. Для установки отметки поместите указатель в ячейку и нажмите левую кнопку мыши. Повторное нажатие кнопки приводит к удалению отметки. Действие расписания повторяется еженедельно

3. После настройки расписания нажмите кнопку "ОК".

   Настройки расписания сохранятся и на экране появится соответствующее сообщение.

4. Нажмите кнопку "OK".

   Окно "Параметры агента обновлений" закроется.

Примечание.
Для загрузки правил и обновлений по настроенному расписанию агент обновлений должен быть запущен (см. стр. 43).

Задание и настройка параметров агента

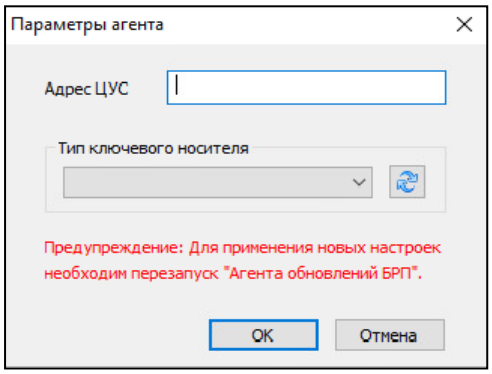
Работа агента обновлений осуществляется с использованием подключения к ЦУС. Загрузка обновлений осуществляется через установленное защищенное соединение с ЦУС.

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. 41) 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

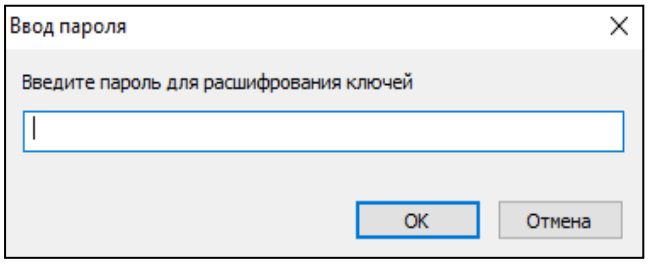
Запуск агента осуществляется по команде программы управления.

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 "OK".

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. **18**).

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 страницу 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

Программные модули, требующие контроля целостности

Ниже в таблицах приведены списки всех используемых модулей ПО ДА, требующих контроля целостности.

Табл.3 Программные модули детектора атак

Имя	Описание
/bin/arp	Программа для просмотра и изменения ARP-таблиц
/bin/atntserver	Сервер аутентификации
/bin/bgpd	Сервер динамической маршрутизации
/bin/chat	Вспомогательный модуль для PPP
/bin/csum	Программа для расчета и проверки контрольных сумм
/bin/df	Программа для определения занятого/свободного дискового пространства
/bin/dhcpd	DHCP-сервер
/bin/dhcrelay	DHCP-ретранслятор
/bin/echo	Программа для вывода сообщений на экран
/bin/fsck_ffs	Программа проверки целостности файловой системы FFS
/bin/fsck	Программа проверки целостности файловых систем (вызывает fsck_ffs)
/bin/ftpmon	Мониторинг ftp-соединений
/bin/grep	Программа поиска текста в файлах
/bin/ids_bpf_filter	Программа управления фильтрами
/bin/ifconfig	Программа настройки сетевых интерфейсов
/bin/kill	Программа для отправки сигналов процессам
/bin/localcmd	Программа, реализующая локальное меню ДА
/bin/ndp	Программа для просмотра и изменения NDP-таблиц
/bin/netstat	Программа для получения информации об открытых сетевых подключениях
/bin/sockstat	Программа для получения информации об открытых сетевых подключениях (вызывается в localcmd)
/bin/ospfd	Сервер динамической маршрутизации
/bin/pfctl	Программа управления ПФ
/bin/ping	Программа для отправки ping-запросов (IPv4)
/bin/ping6	Программа для отправки ping-запросов (IPv6)
/bin/ppp	Подключение через dialup
/bin/ps	Программа для получения информации о запущенных процессах
/bin/pwait	Программа слежения за процессами
/bin/ripd	Сервер динамической маршрутизации
/bin/route	Программа для просмотра и изменения таблицы маршрутизации
/bin/scheck	Программа для постановки файлов на КЦ (используется системной службой установки и обновления). Прямого доступа пользователям не предоставляется
/bin/sh	Обработчик команд (используется системными сервисами при загрузке). Прямого доступа пользователям не предоставляется
/bin/snmptrap	Программа генерации уведомлений SNMP
/bin/sysctl	Программа для просмотра и изменения параметров ядра ОС
/bin/tcpdump	Программа для получения дампа сетевого трафика

Имя	Описание
/bin/timeout	Программа, ограничивающая время запуска переданной команды указанным временем
/bin/tput	Программа, используемая для очистки экрана
/bin/traceroute	Отображение маршрутов
/bin/traceroute6	Отображение маршрутов
/bin/tuicmdwrapper	Программа, визуализирующая вывод, полученный от команд, в псев-дографических окнах
/bin/tuistates	Программа просмотра таблицы состояний ПФ
/bin/vmstat	Программа для получения сведений о загруженности системы
/bin/wc	Программа для подсчета количества строк
/bin/zebra	Сервер динамической маршрутизации
/agent	Агент ДА
/boot/loader	Системный загрузчик
/boot/modules/accelerator /cgw_conf	Меню конфигурации
/cgwlogger	Сборщик журналов ДА, отправляющий их на ЦУС
/kernel	Ядро ОС
/lib/libc.so.7	Динамическая библиотека для программ на языке С
/lib/libcrypto.so.6	Основная криптографическая библиотека для С++
/lib/libgcc_s.so.1	Низкоуровневая библиотека GCC
/lib/libm.so.5	Математическая библиотека языка С
/lib/libopensc.so.3	Библиотека поддержки смарт-карт по стандарту PKCS#15
/lib/libpcsclite.so.1	Связующая библиотека для доступа к PC/SC-совместимым смарт-картам
/lib/librt.so.1	Библиотека для поддержки функций реального времени ОС
/lib/librtpkcs11ecp.so	Библиотека поддержки функций реального времени для использования PKCS#11 со смарт-картами
/lib/libstdc++.so.6	Динамическая библиотека для программ на языке С++
/lib/libthr.so.3	Библиотека поддержки потоков
/lib/libusb.so.2	Библиотека поддержки протокола USB
/lib/pcsc/drivers/ifd-ccid.bundle/Contents/FreeBSD/libccid.so	PC/SC драйвер для ACS USB CCID смарт-карт
/lib/pcsc/drivers/ifd-ccid.bundle/Contents/Info.plist	Список смарт-карт, совместимых с ACS USB CCID драйвером
/libexec/ld-elf.so.1	Линковщик для исполняемых файлов типа ELF формата
/sbin/badblocks	Программа проверки жесткого диска
/sbin/init	Программа инициализации процессов
/sbin/pcscd	Rutoken
/snmpd	Сервер SNMP
/bin/snort	СОВ
/bin/svm_traffic	Эвристический анализатор – поиск туннелированного трафика
/bin/schmm	Эвристический анализатор – поиск SQL-инъекций
/lib/snort_dynamicpreprocessor/libsf_dce2_preproc.so	Обработчик протокола DCE/RPC
/lib/snort_dynamicpreprocessor/libsf_ssh_preproc.so	Обработчик протокола SSH

Имя	Описание
/lib/snort_dynamicpreprocessor/libsf_smtp_preproc.so	Обработчик протокола SMTP
/lib/snort_dynamicpreprocessor/libsf_sip_preproc.so	Обработчик протокола SIP
/lib/snort_dynamicpreprocessor/libsf_sdf_preproc.so	Обработчик протокола SDF
/lib/snort_dynamicpreprocessor/libsf_reputation_preproc.so	Обработчик, реализующий черные/белые списки IP-адресов
/lib/snort_dynamicpreprocessor/libsf_pop_preproc.so	Обработчик протокола POP3
/lib/snort_dynamicpreprocessor/libsf_modbus_preproc.so	Обработчик протокола Modbus
/lib/snort_dynamicpreprocessor/libsf_imap_preproc.so	Обработчик протокола IMAP
/lib/snort_dynamicpreprocessor/libsf_gtp_preproc.so	Обработчик протокола GTP
/lib/snort_dynamicpreprocessor/libsf_ftptelnet_preproc.so	Обработчик протоколов FTP и Telnet
/lib/snort_dynamicpreprocessor/libsf_dns_preproc.so	Обработчик DNS-запросов
/lib/snort_dynamicpreprocessor/libsf_dnp3_preproc.so	Обработчик протокола DNP3
/lib/snort_dynamicpreprocessor/libsf_ssl_preproc.so	Обработчик SSL
/lib/daq/daq_pcap.so	Модуль библиотеки DAQ, осуществляющий захват трафика с помощью системной библиотеки libpcap
/lib/libpcap.so.1.3.0	Системная библиотека для захвата трафика
/lib/libsfbpf.so.0	Модуль библиотеки DAQ, формирующий фильтр для захвата трафика
/lib/libdaq.so.2	Библиотека, используемая для захвата трафика
/lib/libpcre.so.3	Динамическая библиотека для работы с регулярными выражениями

Табл.4 Файлы конфигурации детектора атак

Имя	Описание
/etc/snort/snort.conf.tpl	Шаблон конфигурационного файла
/etc/snort/reference.config	Описывает псевдонимы URL, используемые в правилах СОВ
/etc/snort/classification.config	Файл с описанием классов атак для правил СОВ
/etc/snort/threshold.conf	Файл с указанием предельного количества срабатываний правил СОВ за определенный период
/etc/schmm/schmm.pcap	Образцы трафика с SQL-инъекциями для эвристического анализатора
/etc/master.passwd	Файл с учетными записями пользователей (для запуска СОВ)
/etc/group	Файл с учетными записями групп (для запуска СОВ)
/etc/pwd.db	Индексированная БД пользователей (для запуска СОВ)
/etc/spwd.db	Индексированная БД пользователей (для запуска СОВ)
/etc/svm_traffic.bck/normal_traffic.log	Резервная копия выборок с образцами обычного трафика для эвристического анализатора
/etc/svm_traffic.bck/abnormal_traffic.log	Резервная копия выборок с образцами туннелированного трафика для эвристического анализатора

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.

Опции Meta-Data

`classtype`

Опция **classtype** используется для классификации атаки. Каждому классу устанавливается свой приоритет.

Принято, что **classtype** предшествует **sid** и **rev** в конце сигнатуры правила.

Стандартная классификация правил:

Имя класса	Описание	Приоритет
attempted-admin	Попытка получения привилегий администратора	Высокий
attempted-user	Попытка получения привилегий пользователя	Высокий
inappropriate-content	Обнаружено неприемлемое (несоответствующее) содержание	Высокий
policy-violation	Потенциальное нарушение корпоративной конфиденциальности	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
default-login-attempt	Попытка входа с помощью стандартного логина/пароля	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

Имя класса	Описание	Приоритет
web-application-activity	Доступ к потенциально опасному веб-приложению	Средний
icmp-event	Обычный пакет ICMP	Низкий
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
tcp-connection	Обнаружено TCP-соединение	Очень низкий

Формат:

classtype: <имя класса>;

Формат строки файла classification.config:

config classification: <имя класса>,<описание>,<номер приоритета>;

Пример строки файла classification.config:

config classification: <string-detect>,<String Detect>,<3>;

gid

Данная опция используется для задания правилу номера группы. По умолчанию правило относится к первой группе (можно не указывать gid: 1 в правиле).

Формат:

gid: номер группы;

metadata

Данная опция позволяет задать дополнительную информацию в формате ключ–значение.

Ключ	Значение
engine	Shared Library Rule (”shared”)
soid	Shared Library Rule Generator and SID (gid|sid)
service	Target-Based Service Identifier (”http”)

Примечание. Не описанные выше ключи игнорируются.

Формат:

metadata:<ключ> <значение> [, <ключ> <значение>];

Пример:

metadata:engine shared;

metadata:soid 3|12345;

msg

Опция **msg** содержит текстовое сообщение для записи в файл журнала 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 ;).

Принято, что **msg** является первой опцией в сигнатуре правила.

Формат:

msg: "<текст сообщения>";

priority

Опция **priority** используется для присвоения правилу уровня приоритета в диапазоне от 1 до 255. Чаще всего используют уровни от 1 до 4. Сигнатуры с более высоким приоритетом будут проверяться первыми. Наивысший

приоритет — 1. 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

reference

Позволяет включать в правило ссылки на внешние системы идентификации атак (bugtraq, cve, nessus, arachnids, mcafee, osvdb (snort), msb (snort), url).

Формат:

reference: <идентификатор системы>, <идентификатор атаки>; [reference: <идентификатор системы>, <идентификатор атаки>;]

Примеры:

reference: arachnids, IDS287; reference: bugtraq, 1387;

reference: cve, CAN-2000-1574;

rev

В опции **rev** указывается значение версии правила, идентифицированного по опции **sid** (см. ниже). Эти опции следует использовать совместно.

Если сигнатура правила изменилась, значение **rev** увеличивается на 1.
Формат:

rev: <номер версии>;

Принято, что опции **sid** и **rev** записываются в самом конце правила, причем сначала указывается идентификатор правила.

Пример правила с идентификатором 1000983 ревизии 1:

alert tcp any any -> any 80 (content:"BOB"; sid:1000983; rev:1;)

sid

Опция **sid** предназначена для уникальной идентификации правила. **Sid** следует использовать вместе с опцией **rev** (см. выше).

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>;

Опции проверки содержимого пакетов

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 (от 1 до 10)
смещение	Номер байта в поле данных пакета, с которого начинается обработка (от -65535 до 65535)
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)

Пример:

**alert tcp any any -> any any (content:"Begin"; **
**byte_jump:0, 0, from_end, post_offset -6; **
**content:"end.."; distance:0; within:5; **
msg:"Content match from end of the payload";)

byte_math

Опция byte_math позволяет производить математические операции над извлеченными значениями в заданной переменной и сохранять результат в новую переменную.

Формат:

**byte_math:bytes <число_байт>, offset <смещение>, **
**oper <оператор>, rvalue <значение>, result <имя_переменной> **
**[, relative] [, endian <тип>] [, string <тип>] [, dce] **
[, bitmask <маска>];

Параметры опции byte_math:

Параметр	Описание
bytes	Количество байтов, считываемых из пакета (от 1 до 10)
offset	Номер байта в поле данных пакета, с которого начинается обработка (от -65535 до 65535)
oper	Математический оператор ('+' | '-' | '*' | '/' | '<<' | '>>')
rvalue	<значение> для математической операции (от 0 до 4294967295)
result	Имя переменной, в которой сохранится результат
relative	Отсчет смещения от конца предыдущего найденного соответствия
endian	Обработка данных с: • старшего разряда (big) – используется по умолчанию; • младшего разряда (little)
string	Данные в пакете представлены в виде символьной строки (ASCII)
bitmask	Применяет битовую маску по оператору И к параметру bytes. Результат будет смещен вправо на количество битов, равное количеству завершающих нулей в маске (от 1 до 4 бит в шестнадцатеричном формате)

Пример:

**alert udp any any -> any 1234 **
**(content: "Packets start"; **

**byte_math: bytes 2, offset 0, oper -, rvalue 100, result var, **

**relative, bitmask 0x7FF0; **

**content: "Packets end"; distance: 2; within var; **

msg:"Content match with bitmask applied to the bytes extracted";)

byte_test

Эта опция позволяет провести сравнение с заданным значением. **Byte_test** может использоваться применительно к численным значениям 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!";)

content

Опция **content** позволяет пользователю создавать шаблон для поиска в пакетах определенной информации и выполнения тех или иных действий при ее обнаружении. Шаблон может быть выражен в текстовом или шестнадцатеричном виде, также возможны смешанные варианты. Строка шаблона указывается в кавычках. В шестнадцатеричном виде данные записываются между символами (|). Возможно использовать исключение в поиске определенного шаблона, используя символ (!). Специальные символы (;), (\), (“), если они применяются в текстовом формате, должны обязательно экранироваться либо записываться в шестнадцатеричном виде: (“) как |22|, (;) как |3B|, (:) как |3A|, (|) как |7C|.

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 могут присутствовать несколько опций **content**, что позволяет снижать уровень ложных срабатываний за счет более точного задания искомых последовательностей. При этом поиск будет проводиться слева направо и переход к следующему шаблону произойдет только после нахождения соответствия предыдущему шаблону. Исключением является использование специальной опции **fast_pattern** (см. ниже).

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":)

Пример задания строки поиска, содержащей текст и бинарные данные:

alert tcp any any -> any 139 (content:"|5C 00|P|00|I|00|E|00 5c|";)

Опция **content** может быть дополнена опциями-модификаторами, которые изменяют поведение системы поиска и всегда указываются после **content**:

depth	Опция показывает размер блока данных (от 1 до 65535 байт) из пакета, в котором осуществляется поиск, заданный сопутствующей опцией **content**. Допустима ссылка на переменную, образованную опцией **byte_extract**, если она используется в этом же правиле. Например, при **depth 5** будут просматриваться в поисках заданной последовательности только первые 5 байт поля данных в пакете. Формат: **depth: <количество_байтов>;**
distance	Опция показывает, на сколько байт нужно сместиться после найденного предыдущей опцией **content** шаблона для начала поиска последовательности, заданной другой опцией **content**. Диапазон значений от -65535 до 65535. Допустима ссылка на переменную, образованную опцией **byte_extract**, если она используется в этом же правиле. 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;)**
http_ client_ body	Опция ограничивает поиск шаблона телом HTTP-запроса. Размер (глубина) проверяемого тела настраивается в конфигурационном файле в разделе libhtp, параметр limit-body-limit. Формат: **http_client_body;**
http_ cookie	Опция ограничивает поиск шаблона полем заголовка Cookie (за исключением самого заголовка (Cookie для HTTP-клиента или Set-Cookie для HTTP-сервера) и перевода строки (CRLFF)). Может применяться к запросу HTTP-клиента или ответу HTTP-сервера. Формат: **http_cookie;**
http_ encode	Опция определяет тип кодировки в запросе HTTP-клиента или ответа HTTP-сервера, в зависимости от настройки препроцессора http_inspect. Опция не будет работать с ненормализованными полями. При задании опции возможно использовать логические операторы (!) и (|), а также дополнительные опции: • uri — Проверка указанного типа кодировки в поле URI HTTP-запроса клиента. • header — Проверка указанного типа кодировки в полях HTTP-запроса или HTTP-ответа в зависимости от указанного направления потока захвата пакетов. • cookie — Проверка указанного типа кодировки в полях cookie HTTP-запроса или HTTP-ответа в зависимости от указанного направления потока захвата пакетов. • utf-8 — Проверка наличия кодировки utf-8 в указанном буфере (опции вышеописанной). • double_encode — Проверка наличия двойной кодировки в указанном буфере (опции вышеописанной). • non_ascII — Проверка наличия кодировки не ASCII в указанном буфере (опции вышеописанной). • uencode — Проверка наличия кодировки unicode в указанном буфере (опции вышеописанной). • bare_byte — Проверка наличия закодированного байта в указанном буфере (опции вышеописанной). • ascII — Проверка наличия кодировки ASCII в указанном буфере (опции вышеописанной). • iis_encode — Проверка наличия кодировки IIS Unicode в указанном буфере (опции вышеописанной). Формат: **http_encode:[uri|header|cookie], [!][<utf8|double_encode|non_ascii|uencode|bare_ byte|ascii|iis_encode>];** Пример: **alert tcp any any -> any any (msg:"UTF8/UEncode Encoding present"; http_ encode:uri,utf8|uencode;)**
http_ header	Опция ограничивает поиск шаблона заголовком HTTP-запроса или HTTP-ответа. СОВ помещает в один буфер все заголовки, за исключением имеющих собственный модификатор. Формат: **http_header;**
http_ method	Опция ограничивает поиск шаблона извлеченным полем метода HTTP-запроса. Поддерживаемые методы: GET, POST, PUT, HEAD, DELETE, TRACE, OPTIONS, CONNECT, PATCH. Формат: **http_method;**
http_raw_ header	Опция ограничивает поиск шаблона ненормализованным заголовком HTTP-запроса или HTTP-ответа. СОВ помещает в один буфер все заголовки, за исключением имеющих собственный модификатор. Формат: **http_raw_header;**

http_raw_cookie	Опция ограничивает поиск шаблона полем заголовка Cookie (за исключением самого заголовка (Cookie для HTTP-клиента или Set-Cookie для HTTP-сервера) и перевода строки (CRLFF)). Может применяться к запросу HTTP-клиента или ответа HTTP-сервера. Указывается после параметра content, к которому применяется. Применяется к ненормализованным полям. Также результат извлечения зависит от настройки препроцессора http_inspect. Формат: **http_raw_cookie;** Пример: **content:"%3D|3b 20|cc4="; http_raw_cookie;**
http_raw_uri	Опция ограничивает поиск шаблона ненормализованным полем URI-запроса. Формат: **http_raw_uri;**
http_stat_code	Опция ограничивает поиск шаблона полем состояния HTTP-ответа. Формат: **http_stat_code;**
http_stat_msg	Опция ограничивает поиск шаблона полем Message Status из ответа HTTP-сервера. Формат: **http_stat_msg;** **Пример: content:"OK"; http_stat_msg; content:"Not Found"; http_stat_msg;**
http_uri	Опция ограничивает поиск шаблона нормализованным полем URI-запроса. Формат: **http_uri;**
nocase	Опция позволяет осуществлять поиск, заданный предыдущей опцией **content** без учета регистра символов. Формат: **nocase;** Пример поиска без учета регистра символов: **alert tcp any any -> any 21 (msg:"ROOT"; content:"USER root"; nocase;)**
offset	Опция позволяет задать смещение в поле данных пакета, с которого начинается поиск шаблона, заданного сопутствующей опцией **content**. Например, **offset 5** будет начинать поиск, пропустив первые 5 байт поля данных. Максимальное значение 65535. Допустима ссылка на переменную, образованную опцией **byte_extract**, если она используется в этом же правиле. Формат: **offset: <количество_байтов>;**
rawbytes	Опция позволяет искать в пакете необработанные (raw) данные, игнорируя декодирование, выполняемое препроцессорами. Опция изменяет поиск данных, указанных предыдущей опцией **content**. Формат: **rawbytes;**
within	Опция показывает размер области поиска шаблона, заданного сопутствующей опцией **content**, после нахождения шаблона, заданного предыдущей опцией **content**. Допустима ссылка на переменную, образованную опцией **byte_extract**, если она используется в этом же правиле. 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;)**

cvs

Эта опция обнаруживает уязвимости Bugtraq-10384, CVE-2004-0396. Параметр invalid-entry позволяет искать строку ввода, которая может вызвать переполнение буфера.

Формат:

cvs:invalid-entry;

Пример:

alert tcp any any -> any 2401 (msg:"CVS Invalid-entry"; flow:to_server,established; cvs:invalid-entry;)

fileext

Эта опция позволяет проводить поиск расширения файла.

Формат:

fileext:<текст>;

Пример:

fileext:"jpg";

filemagic

Опция **filemagic** позволяет проводить поиск по информации о файле, возвращаемой от библиотеки libmagic.

Формат:

filemagic:<текст>;

Пример:

filemagic:"executable for MS Windows";

Внимание! Ответы libmagic разных исполнений на один и тот же запрос могут не совпадать.

filemd5

Эта опция позволяет проводить проверку MD5-суммы файла по списку контрольных MD5-сумм.

Файл списка контрольных MD5-сумм состоит из построчных тестовых строк, каждая из которых содержит MD5-сумму в шестнадцатеричном формате. Любая дополнительная информация в строке после MD5-суммы игнорируется обработчиком.

Внимание! При обработке файла каждая MD5-сумма занимает 16 байт памяти. Для работы со списком в 20 млн записей потребуется примерно 310 МБ ОЗУ.

Формат:

filemd5:[!]<имя файла контрольных сумм MD5>;

Примечание. В случае если файл контрольных сумм MD5 находится в директории, отличной от /etc/suricata/rules/filename, требуется при написании имени указать полный путь к файлу.

Пример:

filemd5:md5-blacklist;

filename

Опция **filename** позволяет проводить поиск имени файла.

Формат:

filename:<текст>;

Пример:

filename:"secret";

filesize

Опция **filesize** позволяет проконтролировать размер передаваемого файла.

Формат:

filesize:min<>max;

filesize:[<|>]<значение>;

Пример:

filesize:100; # ровно 100 байт

filesize:100<>200; # от 101 до 199 байт

filesize:>100; # больше 100 байт

ftpbounce

Эта опция позволяет детектировать скрытые атаки (FTP bounce).

Формат:

ftpbounce;

Опции препроцессора GTP

Доступен ряд опций для работы с протоколом передачи данных GTP (GPRS Tunneling Protocol):

gtp_info	Проверка конкретного элемента сообщения GTP. Допустимы значения от 0 до 255 (GTP information elements type), а также его содержание ("rai" ,"tmsi", ...). Формат: **gtp_info:<элемент>;** Пример: **gtp_info:16; gtp_info: tmsi**

gtp_ type	Проверка типа GTP. Допустимы значения от 0 до 255 (GTP message type), а также их содержание ("echo_ request" ,"echo_response", ...). Формат: **gtp_type:<перечень_типов>** Пример: **gtp_type:10, 11, echo_request;**
gtp_ version	Проверка конкретной версии GTP (от 0 до 2). Формат: **gtp_version:<версия>;** Пример: **gtp_version: 1;**

Примечание. Функционирование опций зависит от настройки препроцессора и декодера GTP.

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";)

protected_content

Опция выполняет поиск хэша в пакете заданного алгоритма. Поддерживаются алгоритмы MD5, SHA256, SHA512. В одном правиле может поддерживаться более одного параметра protected_content. Параметр сильно увеличивает нагрузку на ЦП и ОЗУ и может повлиять на производительность СОВ, так как поиск выполняется с помощью хэширования частей входящих пакетов и сравнения результатов с предоставленным хэшем. Несовместим в использовании с параметрами **nocase**, **fast_pattern**, **depth**, **within**.

Модификаторы, совместимые с protected_content:

hash	Параметр, указывающий алгоритм хэширования. Формат: **hash:[md5|sha256|sha512];**
length	Параметр, указывающий длину заданного хэша. Значение должно быть больше 0 и меньше 65536. Формат: **length:[<длина>];**

Формат: **protected_content:[!]"<content hash>", length:orig_len[, hash:md5|sha256|sha512];**

Пример:

alert tcp any any <> any 80 (msg:"MD5 Alert"; protected_ content:"293C9EA246FF9985DC6F62A650F78986"; hash:md5; offset:0; length:4;)

Опции препроцессора SIP

Доступен ряд опций для работы с протоколом передачи данных SIP:

sip_body	Параметр определяет начало поиска на соответствие другим опциям правила с начала тела сообщения SIP. Формат: **sip_body;**
sip_ header	Параметр ограничивает поиск извлеченным полем заголовка SIP-запроса или SIP-ответа. Формат: **sip_header;**
sip_ method	Параметр проверяет конкретные методы запроса SIP ("invite"|"cancel"|"ack" |"bye"|"register"| "options" |"refer"|"subscribe" |"update"|"join"|"info" |"message" |"notify"|"prack"). Для указания метода допустимо использование символа инверсии (!) непосредственно перед его именем. Формат: **sip_method:<перечень_методов>;** Пример: **sip_method:invite, cancel; sip_method:!bye;**
sip_ stat_ code	Параметр проверяет код состояния ответа SIP (от 1 до 9 и от 100 до 999). Коды от 1 до 9 означают проверку кодов 1xx, 2xx, 3xx, ... Формат: **sip_stat_code:<перечень_кодов>;** Пример: **sip_stat_code:2; sip_stat_code:200,180;**

Примечание. Функционирование опций зависит от настройки препроцессора SIP.

stream_reassemble

Опция **stream_reasseble** позволяет включать или выключать повторную сборку (реассемблинг) TCP-потока на трафике. Опция доступна, только если включен Stream-препроцессор.

Формат:

stream_ reassemble:<enable|disable>, <server|client|both> [, noalert] [, fastpath];

Параметр	Описание
enable|disable	Включение/выключение реассемблинга
server|client|both	Трафик от сервера|клиента|в обе стороны
noalert	Отключение генерации сообщений (alert)
fastpath	Игнорирование остатка сессии

Пример:

stream_reassemble:disable, client, noalert;

Опции проверки служебных полей пакетов

ack

Опция **ack** используется для проверки номеров подтверждений TCP (поле заголовка Acknowledgment Number).

Формат:

ack: <номер_подтверждения>;

dns_query

Опция **dns_query** используется для анализа ответа DNS-сервера. Все следующие за данной опцией **content** будут исследовать DNS-ответ.

Формат:

dns_query;

Пример использования:
dns_query; content:"google"; nocase; sid:1;

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 установленных флагов TCP. Список проверяемых флагов:

- **F** — FIN (завершение соединения, начальный флаг)
- **S** — SYN (синхронизация номеров последовательности)
- **R** — RST (обрыв соединения)
- **P** — PSH (проталкивание данных, накопившихся в приемном буфере)
- **A** — ACK (номер подтверждения)
- **U** — URG (указатель важности)
- **C** — CWR (окно насыщения уменьшено)
- **E** — ECE (сигнал о возникновении перегрузки сети, конечный флаг)
- **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, пакетов ECN, где установлены флаги SYN, CWR и ECE) можно задавать маски опций. В маске проверяемые флаги отделяются запятой. Например, для детектирования SYN-пакетов независимо от значений конечных битов можно задать маску S,CE.

Формат:

flags:[!|*|+]<FSRPAUCE0>[,<FSRPAUCE0>];

Примечание. Порядок следования флагов значения не имеет.

Для детектирования пакетов с флагами SYN и FIN независимо от значений конечных (резервных) битов CWR и ECE может использоваться правило:

alert tcp any any -> any any (flags:SF,CE;)

flow

Опция **flow** позволяет применять правило лишь к определенному виду трафика или состоянию соединения. 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|not_established|stateless)] **

**[,(to_client|to_server|from_client|from_server)] **

[,(no_stream|only_stream)] [,(no_frag|only_frag)];

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 пакетов установленных соединений TCP
not_ established	Контроль пакетов, не принадлежащих установленным соединениям TCP
stateless	Контроль любых пакетов, 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
no_frag	Игнорирование фрагментированных пакетов
only_frag	Контроль только фрагментированных пакетов

Примечание. Параметр **established** заменяет опцию **flags: A+**, часто используемую применительно к уже установленным соединениям TCP.

flowbits

Опция **flowbits** контролирует состояние потока и 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|isset|toggle|unset|isnotset|noalert|setx|reset] **

[,<название_состояния>];

Параметры опции flowbits:

Параметр	Описание
set	Установка указанного состояния
isset	Проверка, что установлено указанное состояние
toggle	Установка указанного состояния, если оно еще не было установлено, либо отмена установленного ранее состояния
unset	Отмена указанного состояния
isnotset	Проверка, что указанное состояние не установлено
noalert	Отключение для правила генерации сигнала тревоги независимо от остальных опций детектирования
setx	Установка указанного и отмена остальных состояний
reset	Сброс всех состояний

flowint

Опция **flowint** позволяет производить математические операции над переменными с сохранением результата. Похожа на **flowbits**, но с добавлением математических возможностей и того факта, что целочисленное значение может быть сохранено и изменено, а не только установлен флаг.

Может использоваться для подсчета событий, добавления или вычитания событий, контроля пороговых значений.

Формат:

flowint: <переменная>, [[<операция|сравнение>]|[<переменная>]]

[,[<операция|сравнение>]|[<переменная>]];

Примеры:

```
alert tcp any any -> any any (msg:"Setting a flowint counter"; \
content: "GET"; flowint:myvar, notset; flowint:maxvar,notset; \
flowint: myvar, =, 1; flowint: maxvar, =, 6;)

alert tcp any any -> any any (msg:"Adding to flowint counter"; \
content: "Unauthorized"; flowint: myvar, isset; flowint: myvar, +, 2;)

alert tcp any any -> any any \
(msg:"if the flowint counter is 3 create a new counter"; \
content:"Unauthorized"; flowint: myvar, isset; flowint: myvar, ==, 3; \
flowint: cntpackets, notset; flowint: cntpackets, =, 0;)
```

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 поле смещения 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-пакета (второй байт ICMP-заголовка).

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 2-байтного идентификатора ICMP-пакета. 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 2-байтных 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 идентификатора IP-пакета. 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 (защита данных);
- **esec** — IP extended security (расширенная защита данных);

- **lsrr** — loose source routing (не жестко заданный маршрут);
- **lsrre** — loose source routing (For MS99-038 and CVE-1999-0909);
- **ssrr** — strict source routing (жестко заданный маршрут);
- **satid** — stream identifier (идентификатор потока);
- **any** — any IP options are set (любые опции).

Примечание. Опция **satid** устарела и не рекомендуется к использованию.

Чаще всего проверяются опции **ssrr** и **lsrr**, которые не используются в распространенных приложениях интернета.

Формат:

ipopts:<rr|eol|nop|ts|sec|esec|lsrr|lsrre|ssrr|satid|any>;

Внимание! В правиле недопустимо наличие нескольких опций **ipopts**.

ip_proto

Опция **ip_proto** позволяет проверять 1-байтный идентификатор протокола в заголовке IP-пакета. 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 ICMP-пакета (первый байт ICMP-заголовка).

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 (sameip;)

seq

Опция **seq** служит для проверки значения порядковых номеров TCP (поле заголовка Sequence Number).

Формат:

seq:<номер>;

Приведенный ниже пример проверяет равенство порядкового номера TCP нулю.

seq:0;

`stream_size`

Опция служит для проверки размера пакетов трафика (по TCP Sequence number).

Формат:

stream_size:<направление>, [!=|=|<|>|>=|<=], <число байт>;

Параметр "направление" может принимать следующие значения:

- **server** — от сервера;
- **client** — от клиента;
- **both** — в обе стороны;
- **either** — в любую сторону.

Пример обнаружения пакета от клиента размером меньше 6 байт:

alert tcp any any -> any any (stream_size: client,<,6;)

`tos`

Эта опция позволяет проверять тип обслуживания IP-пакета (Type of Service).

Формат:

tos:[!]<значение>;

В приведенном ниже примере проверяется отличие значения поля TOS от 4:

tos:!4;

`ttl`

Опция **ttl** используется для проверки времени жизни пакета. Эта опция может быть полезна при детектировании попыток трассировки с помощью команды **traceroute**.

Формат:

ttl:[[<число_секунд>-]|[>, <, =, <=, >=]]<число_секунд>;

Пример ограничения времени жизни датаграмм 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 (поле заголовка Window size). Диапазон возможных значений — 2 ... 65 535 байт.

Формат:

window:[!]<число_байт>;

Опции после детектирования

`activates/activated_by`

Динамическое правило выполняется при прохождении определенного числа пакетов, соответствующих активирующему правилу (см. стр. **48**).

Формат:

activates:<id>; — активирующее правило.

activated_by:<id>; count: <количество_пакетов>; — динамическое правило.

Пример создания оповещения (alert) при обнаружении переполнения буфера IMAP и наборе 50 пакетов, направленных в порт 143 любого хоста защищаемой сети с любого внешнего хоста:

activate tcp !$HOME_NET any -> $HOME_NET 143 (flags: PA; content: "|E8C0FFFFFF|\bin|; activates: 1; msg: "IMAP buffer overflow!";)

dynamic tcp !$HOME_NET any -> $HOME_NET 143 (activated_by: 1; count: 50;)

detection_filter

Опция **detection_filter** используется для выдачи сигнала тревоги (alert) после достижения порогового значения контролируемого параметра. В качестве контролируемого параметра выступает количество пакетов с разными IP-адресами отправителя (by_src) или получателя (by_dst) за определенный период времени. После генерации сигнала счетчик параметра обнуляется и начинается новый период контроля.

Опция **detection_filter** проверяется системой последней, даже если эта опция будет не на последней позиции в правиле. В каждом правиле может быть только одна такая опция.

Формат:

detection_filter: track <by_src|by_dst>, count <счетчик пакетов>, seconds <период контроля>;

Пример выдачи сигнала тревоги после каждой фиксации трафика от 15 и более разных отправителей за период в две секунды:

detection_filter: track by_src, count 15, seconds 2;

filestore

Опция сохраняет файлы на диск при соответствии правилу.

Формат:

filestore:[<направление>,<контент>];

В качестве направления трафика указывают:

- **request|to_server** — из запроса (из трафика к серверу);
- **response|to_client** — из ответа (из трафика к клиенту);
- **both** — с обоих направлений.

Сохранению подлежат:

- **file** — совпавшие файлы (для опций **filename**, **fileext**, **filemagic**);
- **tx** — сохранение всех файлов из соответствующей правилу HTTP-транзакции;
- **ssn|flow** — сохранение всех файлов из TCP-сессии или TCP-потока.

По умолчанию используется такое же направление трафика, как обозначено в правиле, а сохранению подлежат совпавшие файлы.

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";

replace

Опция **replace** используется для замены шаблона, найденного по предшествующей опции **content**. При этом количество символов передаваемой информации не должно измениться. Допустимо множество замен в правиле, по одной на каждый найденный шаблон.

Внимание! Опция **replace** может быть использована только в режиме Inline.

Формат:

replace:"текст";

Пример:

content:"abc"; replace:"def";

session

Опция **session** позволяет получить пользовательскую информацию из сессий TCP. Это очень удобно, к примеру, для обработки сохраненных файлов (формат pcap).

Опция может использоваться с тремя параметрами — **printable** (вывод только печатаемых символов), **binary** (вывод данных в бинарном формате) и **all** (выводить все, заменяя непечатаемые символы шестнадцатеричными эквивалентами).

Формат:

session: [printable | binary | all];

Внимание! Использование опции **session** может существенно замедлять работу программы поиска.

Пример правила для FTP-сессии:

log tcp any any <> any 21 (session:printable;)

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.

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.

Формат:

tag:host, <количество>, <метрика>, <направление>;

или

tag:session[, <количество>, <метрика>][, exclusive];

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 метрики:

- **packets** — контроль **<количества>** пакетов;
- **seconds** — контроль пакетов в течение **<количества>** секунд;
- **bytes** — контроль **<количества>** байт.

Направление для **host**:

- **exclusive** — контроль пакетов только первой соответствующей сессии.

Пример записи пакетов в течение первых 10 секунд любого сеанса telnet:

alert tcp any any -> any 23 (flags:s,12; tag:session,10,seconds;)

threshold

Опция **threshold** используется для контроля частоты генерации сигнала тревоги (alert) в правиле. В качестве контролируемого параметра выступает количество пакетов с разными IP-адресами отправителя (by_src) или получателя (by_dst).

Формат:

threshold: type <режим>, track <by_src|by_dst>, count <N>, seconds <T>

Используются три режима:

1) Режим "threshold".

При каждом достижении установленного порога в N событий за указанный промежуток времени генерируется сигнал.

Пример:

threshold: type threshold, track by_src, count 10, seconds 60;

2) Режим "limit".

Сигнал генерируется не более N раз за указанный промежуток времени.

Пример:

threshold: type limit, track by_src, seconds 180, count 1;

3) Режим "both".

При первом достижении установленного порога в N событий за указанный промежуток времени генерируется сигнал, после этого новый отсчет событий начнется только по истечении текущего периода контроля.

Пример:

threshold: type both, track by_src, count 5, seconds 360;

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.

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. Межсетевое экранирование.
5. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9. Руководство администратора. Сетевые функции.
6. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9. Руководство администратора. Настройка VPN.