КОД БЕЗОПАСНОСТИ

Аппаратно-программный комплекс шифрования

Континент
Версия 3.7

Руководство администратора

Система обнаружения вторжений

RU.88338853.501430.006 96 5 1

© Компания "Код Безопасности", 2017. Все права защищены.

Все авторские права на эксплуатационную документацию защищены.

Этот документ входит в комплект поставки изделия. На него распространяются все условия лицензионного соглашения. Без специального письменного разрешения компании "Код Безопасности" этот документ или его часть в печатном или электронном виде не могут быть подвергнуты копированию и передаче третьим лицам с коммерческой целью.

Информация, содержащаяся в этом документе, может быть изменена разработчиком без специального уведомления, что не является нарушением обязательств по отношению к пользователю со стороны компании "Код Безопасности".

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

Оглавление

Список сокращений

ICMP	Internet Control Message Protocol
IP	Internet Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USB	Universal Serial Bus
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
ПФ	Правила фильтрации
СОВ	Система обнаружения вторжений (компьютерных атак)
ЦУС	Центр управления сетью криптографических шлюзов

Введение

Данный документ предназначен для администраторов изделия "Аппаратно-программный комплекс шифрования «Континент». Версия 3.7" RU.88338853.501430.006 (далее — комплекс). В нем содержатся сведения, необходимые администраторам для управления системой обнаружения вторжений (компьютерных атак) (далее – СОВ).

Приступая к изучению данного руководства, необходимо предварительно ознакомиться с [**1**].

Сайт в Интернете. Если у вас есть доступ в Интернет, вы можете посетить сайт компании "Код Безопасности" (http://www.securitycode.ru/) или связаться с представителями компании по электронной почте (support@securitycode.ru).

Служба технической поддержки. Связаться со службой технической поддержки можно по телефону 8-495-982-30-20 или по электронной почте support@securitycode.ru . Страница службы технической поддержки на сайте компании "Код Безопасности": http://www.securitycode.ru/products/technical-support/.

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

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:

- интернет-мессенджеры (Skype, ICQ, Jabber, MSN, IRC, SIP, WhatsApp);
- удаленное управление (TeamViewer, RDP, VNC, PCAnywhere);
- сетевое вещание (Icecast, PPLive, PPStream, Zattoo, SHOUTCast, SopCast, TVAnts, TVUplayer, VeohTV, QQLive);
- скрытая передача данных (Tor, Kazaa/Fasttrack, Gnutella, eDonkey, Bittorrent, HTTP Application Activesync, RemoteScan);
- процессы туннелирования (IP in IP, GRE, STUN, SSL (в том числе инкапсулированные в HTTP), SSH (в том числе инкапсулированные в HTTP));
- компьютерные игры (Warcraft3, World of Kung Fu, Steam, Halflife2, World of Warcraft, Battlefield, Quake, Thunder/Webthunder);
- поисковые системы, социальные сети и др. (Google, YouTube, Gmail, Google Maps, FaceBook, Twitter).

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.

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 [**1**].

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. **48**). 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.

Общий порядок ввода в эксплуатацию СОВ

Внимание! Установка ПО каждого из детекторов атак, входящих в СОВ, выполняется в полном соответствии с процедурой установки программного обеспечения КШ (см. [**2**], "Установка ПО и инициализация КШ").

После установки ПО администратор должен выполнить следующее:

1. В настройках общих параметров ПАК "Соболь" проверить значение параметров, установленных по умолчанию (см. стр.**66**).
2. Сменить пароль администратора ПАК "Соболь" (см. документ "Программно-аппаратный комплекс "Соболь". Версия 3.0. Руководство администратора").

Ввод в эксплуатацию состоит из следующих последовательных этапов:

1. Установка лицензии на обновление базы решающих правил. Выполняется средствами ПУ ЦУС. Установка лицензий описана в [**1**].
2. Загрузка в БД ЦУС сертификатов для получения и обновления базы решающих правил (см. стр.**25**).
3. Загрузка в БД ЦУС базы решающих правил (см. стр.**27**).
4. Регистрация ДА в БД ЦУС. Выполняется отдельно для каждого ДА (см. стр.**15**).
5. Запись конфигурации ДА и ключей на отчуждаемый носитель. Выполняется отдельно для каждого ДА (см. стр.**19**, стр.**20**).
6. Инициализация и подключение ДА. Выполняется локально для каждого ДА (см. стр.**20**).
7. Настройка режима работы ДА. Выполняется отдельно для каждого ДА (см. стр.**20**).
8. Назначение правил. Выполняется для каждого зарегистрированного ДА (см. стр.**24**).
9. Установка и настройка агента обновлений БРП (см. стр.**33**).

Средства управления системой обнаружения вторжений

Управление СОВ включает в себя настройку детекторов атак и периодическое обновление базы решающих правил. Операции, связанные с настройкой ДА и обновлением БРП, выполняются администратором в ПУ ЦУС. Подробнее о работе в ПУ ЦУС см. [**1**].

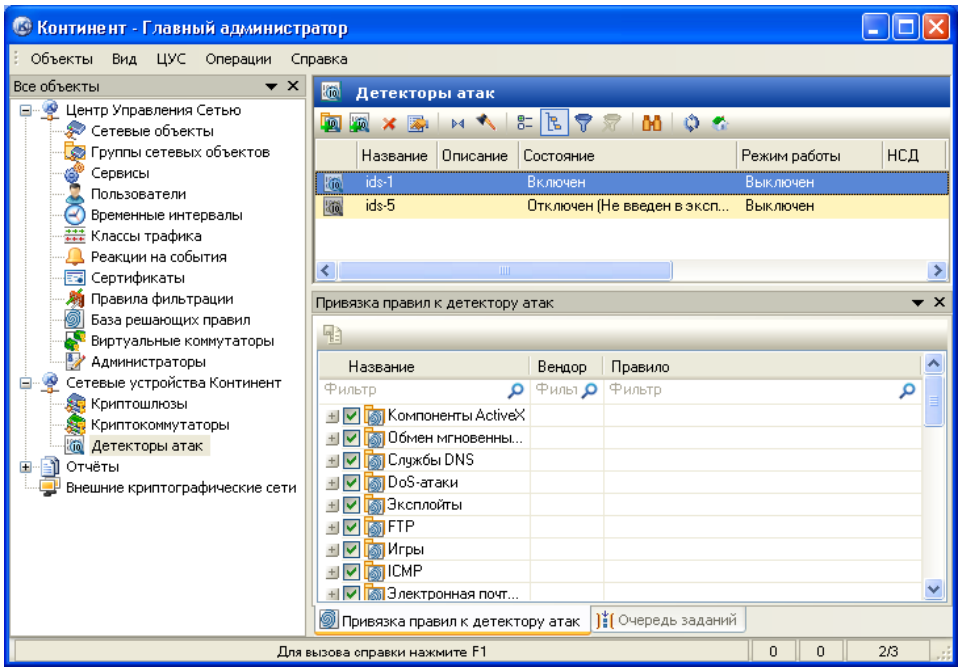
Для работы с детекторами атак и решающими правилами в ПУ ЦУС в окне объектов выбирают соответственно папку "Детекторы атак" или "База решающих правил".

Список детекторов атак

Для перехода к списку детекторов атак:

- Выберите в окне объектов папку "Детекторы атак".

  В главном окне отобразится список зарегистрированных детекторов атак.



Примечание. Если в сети не было зарегистрировано ни одного детектора атак, список будет пустым. Регистрацию и добавление нового детектора в список см. стр.15.

Для каждого детектора в списке приводится следующая информация:

- название – имя, под которым детектор зарегистрирован в базе данных ЦУС;
- описание – дополнительные сведения, введенные при регистрации;
- состояние – возможные значения:
  - отключен;
  - отключен (не введен в эксплуатацию);
  - включен;
  - включен (не введен в эксплуатацию);
- режим работы – возможные значения:
  - сигнатурный анализ;
  - выключен;
- НСД – наличие НСД, обнаруженного данным детектором атак;

- время смены ключей – дата и время последней смены ключа связи с ЦУС и главного ключа детектора;
- идентификатор изделия, указанный в его паспорте;
- версия ПО.

Примечание. В зависимости от настроек интерфейса параметры "Идентификатор" и "Версия ПО" в главном окне могут не отображаться. Для их отображения используйте кнопку  в 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.

При работе со списком могут выполняться следующие операции:

- регистрация нового ДА;
- запись конфигурации и ключей на носитель;
- просмотр и изменение параметров свойств ДА;
- удаление ДА из списка;
- просмотр списка правил, назначенных детекторам атак;
- просмотр параметров решающих правил;
- назначение правил.

С помощью кнопок панели инструментов выполняются следующие операции:

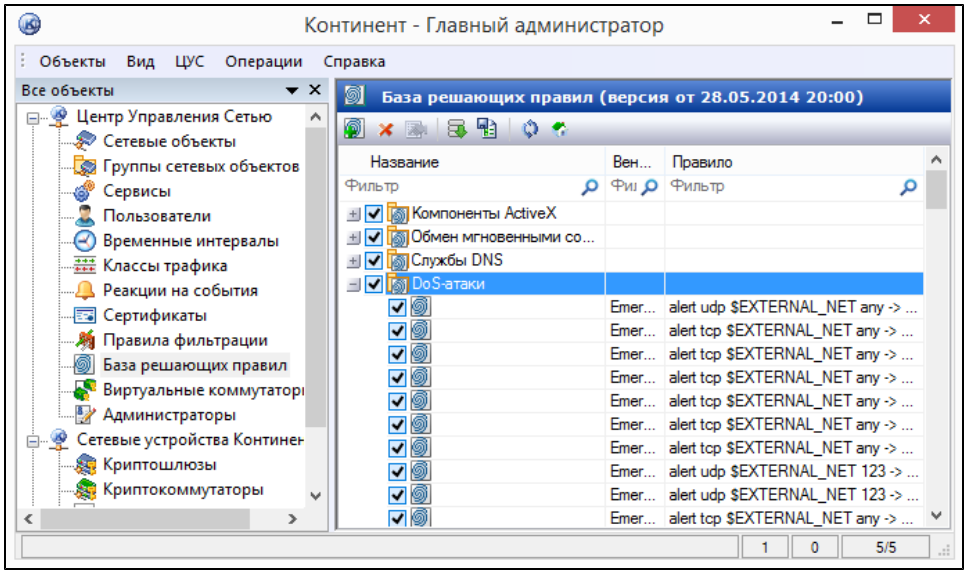
	Создание группы
	Создание детектора атак
	Удаление детектора атак
	Просмотр и редактирование свойств ДА
	Перезагрузка ДА
	Очистка таблицы состояния соединений детектора атак
	Выбор полей отображения
	Отображение в списке ДА дочерних групп
	Включение фильтра
	Выключение фильтра
	Поиск в списке
	Обновление отображаемого списка
	Возврат на домашнюю страницу

Список правил

Для перехода к списку правил:

- Выберите в окне объектов папку "База решающих правил".

  В главном окне отобразится список групп загруженных в БД ЦУС решающих правил.



Примечание. Если правила в БД ЦУС не загружались, список будет пустым. Загрузку правил см. стр.27.

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 самого 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.

При работе со списком правил могут выполняться следующие операции:

- просмотр и изменение параметров выбранного в списке правила;
- добавление в список нового правила;
- удаление правила из списка;
- ручная загрузка (обновление) правил в БД ЦУС.

С помощью кнопок панели инструментов выполняются следующие операции:

	Добавление нового правила
	Удаление правила
	Просмотр и редактирование параметров правила
	Ручная загрузка правил (обновление)
	Сохранение внесенных изменений
	Обновление отображаемого списка
	Возврат на домашнюю страницу

Управление детекторами атак

Регистрация детектора атак

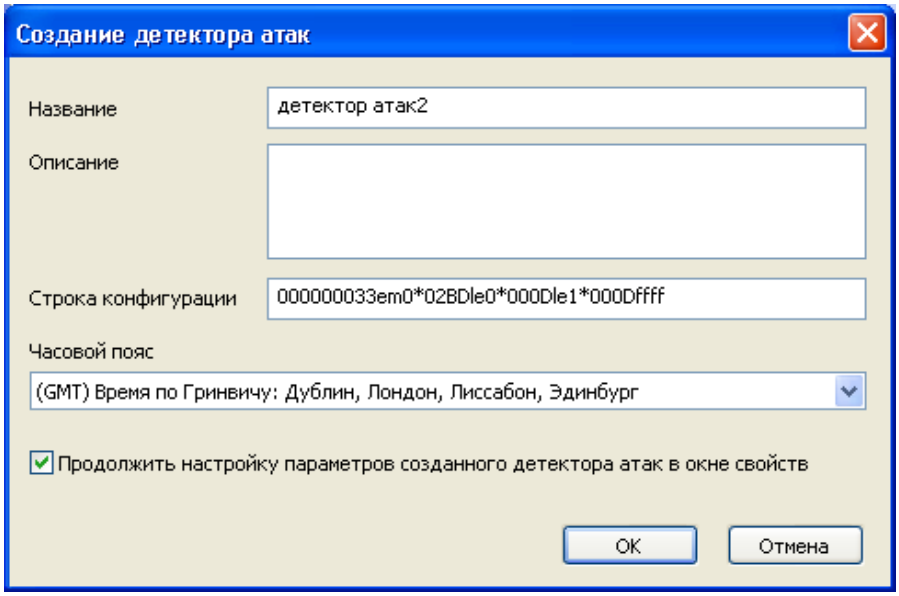
Регистрация нового ДА выполняется в ПУ ЦУС и включает в себя выполнение следующих операций:

- задание общих параметров ДА;
- настройка интерфейсов;
- автоматическая генерация ключей.

Для регистрации нового ДА:

1. Выберите в окне объектов папку "Детекторы атак" и выполните одно из следующих действий:
   - вызовите контекстное меню и выберите команду "Создать детектор атак";
   - в панели инструментов нажмите кнопку "Создать детектор атак";
   - поместите курсор в область главного окна, вызовите контекстное меню и выберите команду "Создать детектор атак".

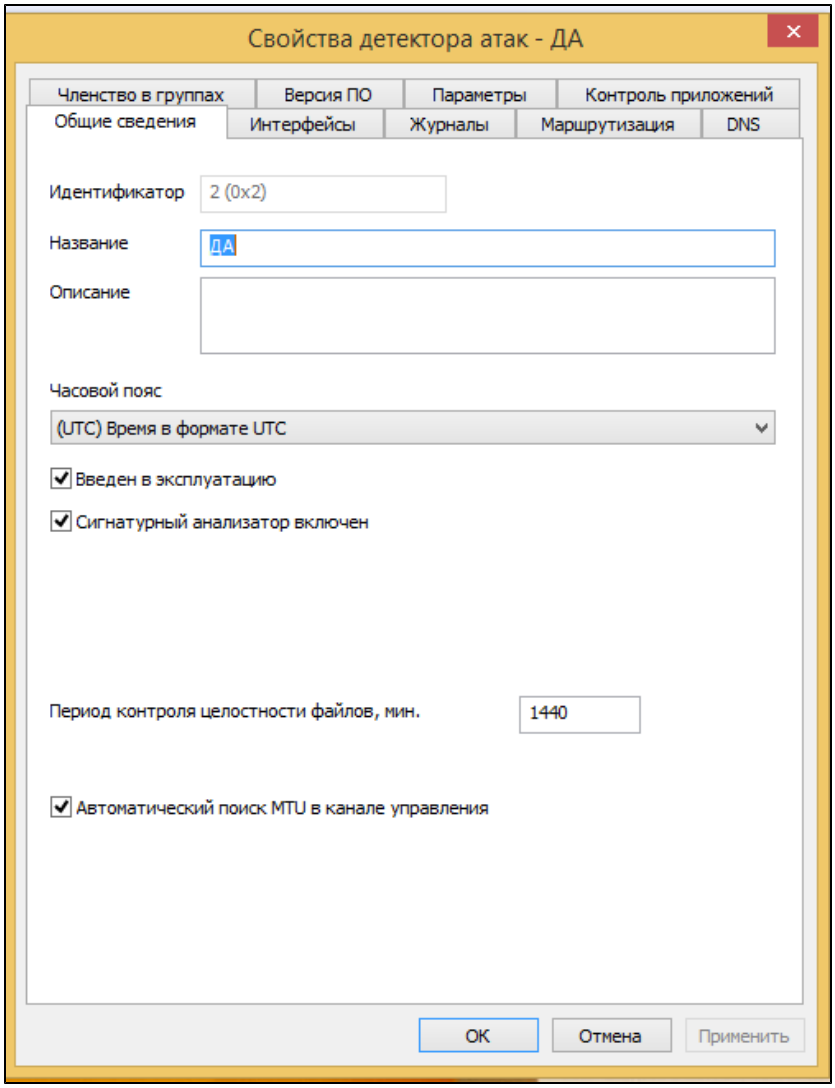
   На экране появится диалог "Создание детектора атак".



2. Введите название нового ДА и его краткое описание.
3. Введите строку аппаратной конфигурации ДА, указанную в его паспорте.
4. Выберите из раскрывающегося списка часовой пояс.
5. Если необходимо завершить регистрацию без настройки параметров и сохранения конфигурации ДА и ключей на носитель, удалите отметку в поле "Продолжить настройку параметров..." и нажмите кнопку "OK".

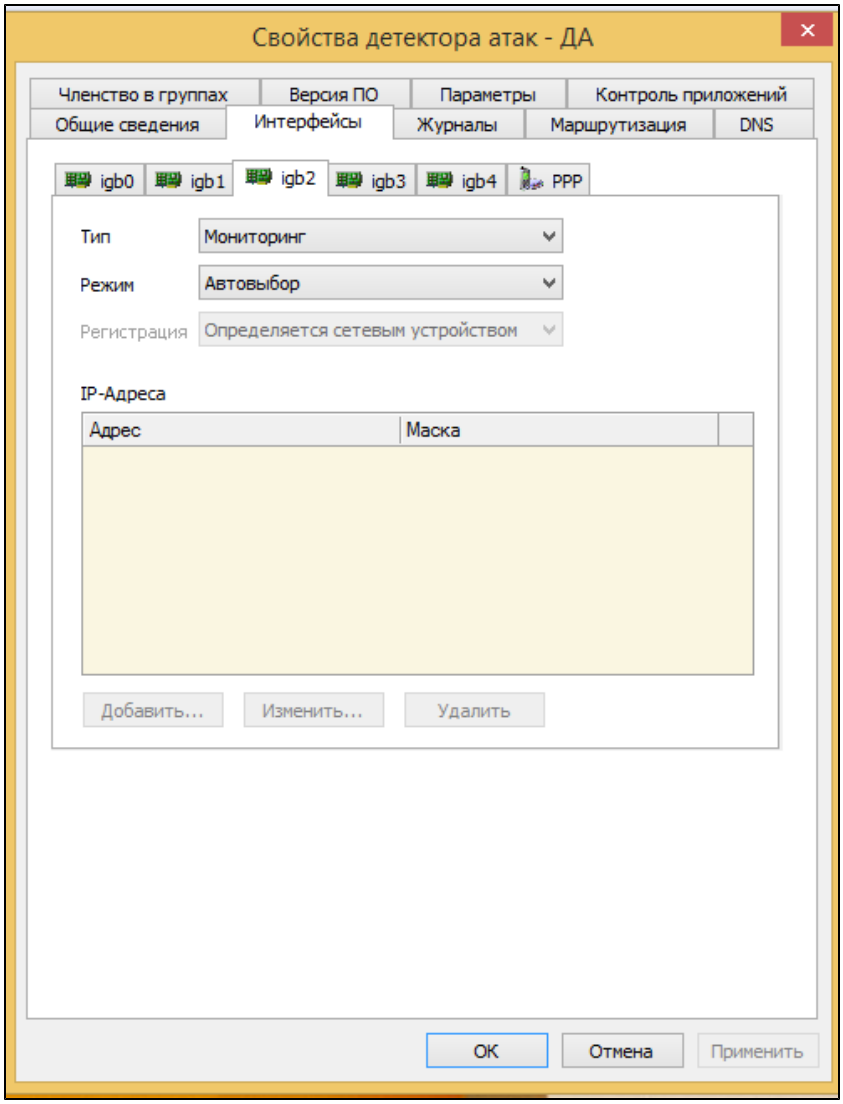
   Диалог "Создание детектора атак" закроется и в главном окне в список добавится строка созданного ДА.
6. Если необходимо продолжить настройку параметров ДА, убедитесь, что в поле "Продолжить настройку параметров..." установлена отметка, и нажмите кнопку "OK".

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



На вкладке отображаются значения параметров, устанавливаемые для данного ДА по умолчанию.

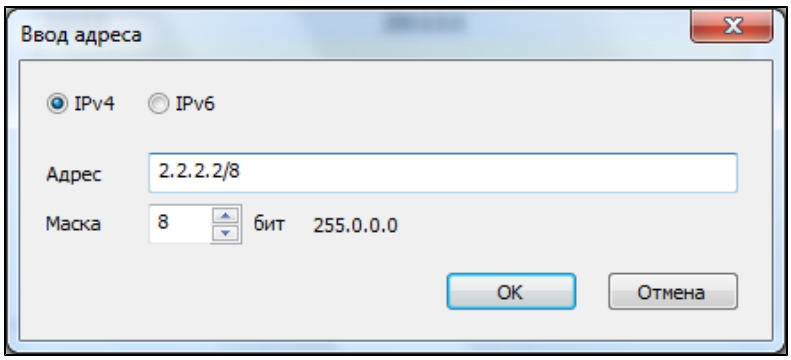
7. Перейдите на вкладку "Интерфейсы" и затем перейдите на вкладку нужного интерфейса для настройки его параметров.



8. Настройте параметры интерфейса и нажмите кнопку "Применить".

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 (рекомендуется) значение "автовыбор"
IP-адреса	Только для интерфейса типа "управление". Введите IP-адрес (список IP-адресов) ДА. Для добавления IP-адреса и формирования списка используйте кнопки "Добавить", "Изменить" и "Удалить"

При вводе IP-адреса предусмотрено два способа задания маски:

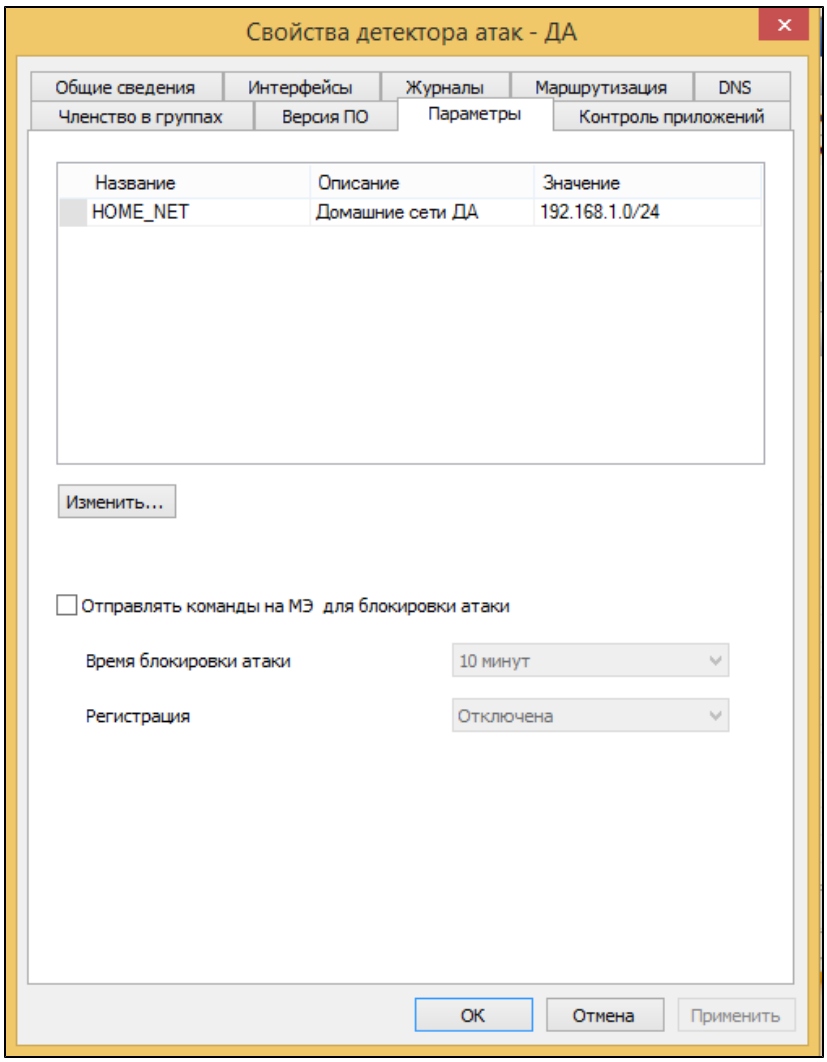


- введите в поле "Адрес" значение с указанием маски, например 2.2.2.2/8, и нажмите кнопку "OK" или клавишу <Enter>; при этом поле "Маска" (см. рисунок выше) не используется;
- введите в поле "Адрес" значение, например 2.2.2.2, перейдите в поле "Маска" (для перехода можно использовать клавишу табуляции), введите значение, например 8, и нажмите кнопку "OK" или клавишу <Enter>.

9. Перейдите к следующему интерфейсу и настройте его параметры в соответствии с описанием п.**8**.

Если необходимо настроить интерфейс PPP, перейдите на соответствующую вкладку и выполните настройку. Описание настройки см. [**1**].

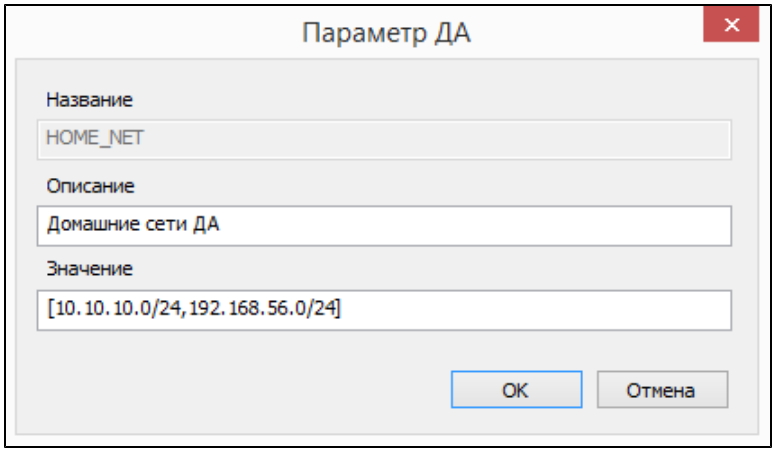
10. Перейдите на вкладку "Параметры".



На вкладке отображается параметр HOME_NET, описывающий домашние сети, контролируемые данным детектором атак. Для параметра приводятся его описание и значение – список контролируемых подсетей. При регистрации нового ДА по умолчанию в списке отображается произвольная подсеть.

11. Нажмите кнопку "Изменить".

    На экране появится диалог "Параметр ДА".



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

    Диалог "Параметр ДА" закроется и на вкладке "Параметры" отобразятся введенные изменения.

Примечание. В некоторых случаях в журналах регистрации могут отображаться атаки на сети, не контролируемые данным детектором атак.

14. Для сохранения внесенных изменений нажмите кнопку "Применить".
15. Для завершения процедуры регистрации нажмите кнопку "ОК".

    Диалог "Свойства детектора атак" закроется и в главном окне в список добавится строка созданного ДА. При этом в дополнительном окне отобразится список групп решающих правил (при условии, что предварительно была выполнена их загрузка в БД ЦУС).

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 "gate.cfg".

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 gate.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 keyset, 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.**19**, стр.**20**).

Процедура инициализации и подключения ДА выполняется локально и полностью совпадает с аналогичной процедурой для КШ (см. [**2**]).

После завершения инициализации перейдите к настройке режима работы ДА.

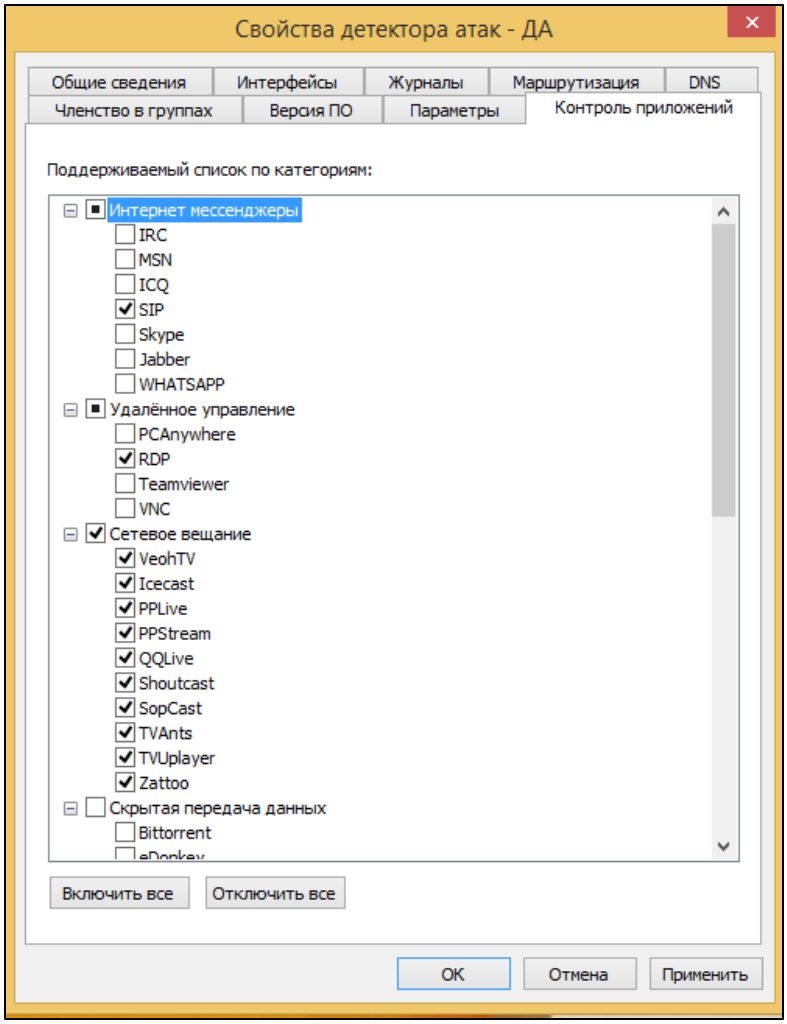
Настройка режима работы детектора атак

Для настройки режима работы ДА:

1. Выберите в списке нужный детектор атак, вызовите контекстное меню и активируйте команду "Свойства".

   На экране появится диалог "Свойства детектора атак", открытый на вкладке "Общие сведения".
2. Для активации работы сигнатурного анализатора установите отметку в поле "Сигнатурный анализатор включен".

   Если режим сигнатурного анализатора должен быть отключен, удалите отметку.
3. 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.

4. Установите отметки у тех приложений, которые должны быть поставлены на контроль.
5. Для завершения настройки режима работы детектора атак нажмите кнопку "Применить" или "ОК".

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  в панели инструментов.

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

   Детектор атак будет удален из списка.

Просмотр правил, назначенных детектору атак

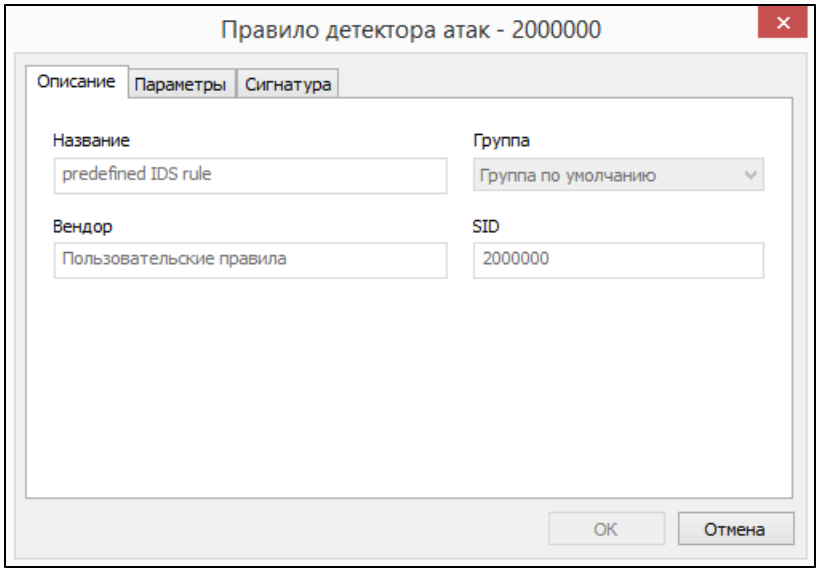
Для просмотра правил:

1. Выберите в списке ДА для просмотра назначенных ему правил.

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

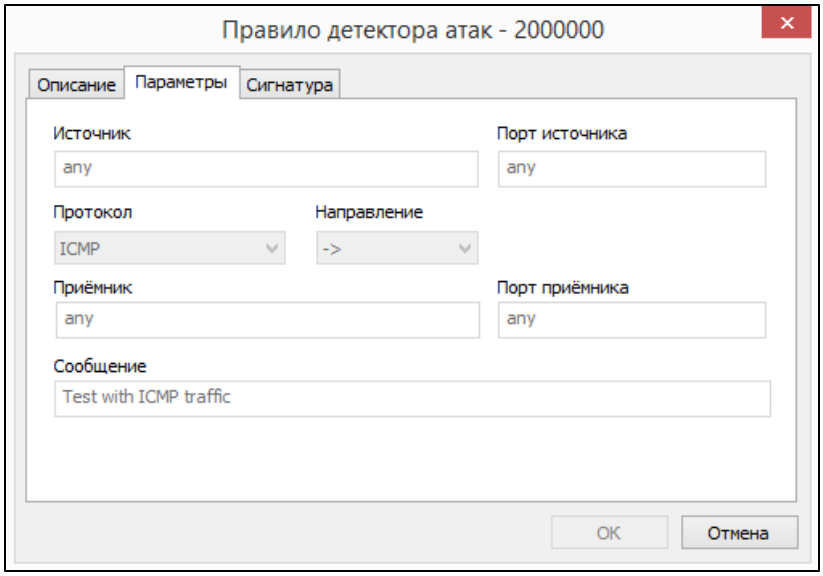
   Появится список правил, входящих в группу. Правила, назначенные детектору атак, имеют отметку.
3. Установите курсор на строку правила и дважды нажмите левую кнопку мыши.

   На экране появится диалог "Правило детектора атак", открытый на вкладке "Описание".



   На вкладке представлены значения общих параметров правила:

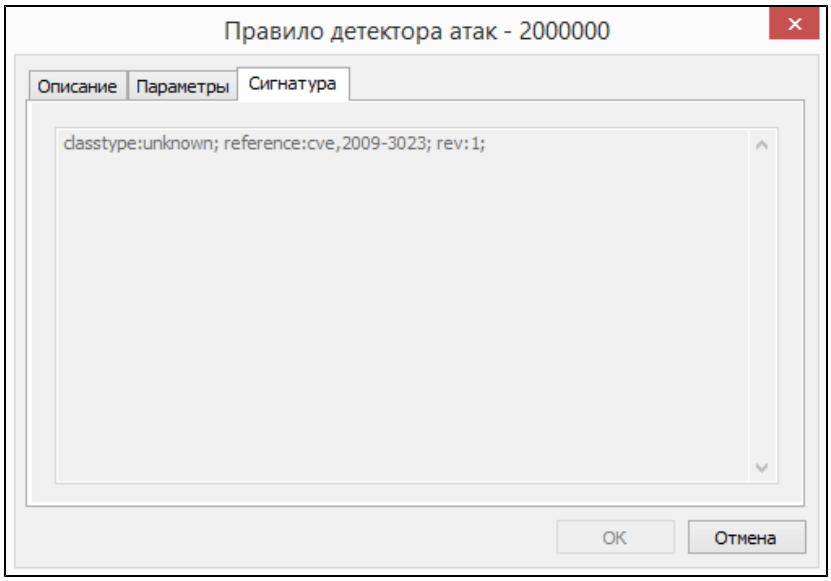
   - название;
   - группа, в которую входит данное правило;
   - вендор (поставщик правила);
   - SID – уникальный номер правила, присвоенный вендором.
4. Перейдите на вкладку "Параметры".



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".

Диалог "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.**22**.

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

   Диалог "Правило детектора атак" закроется.

Назначение правил

Для назначения детектору атак правила необходимо установить отметку у этого правила в дополнительном окне.

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

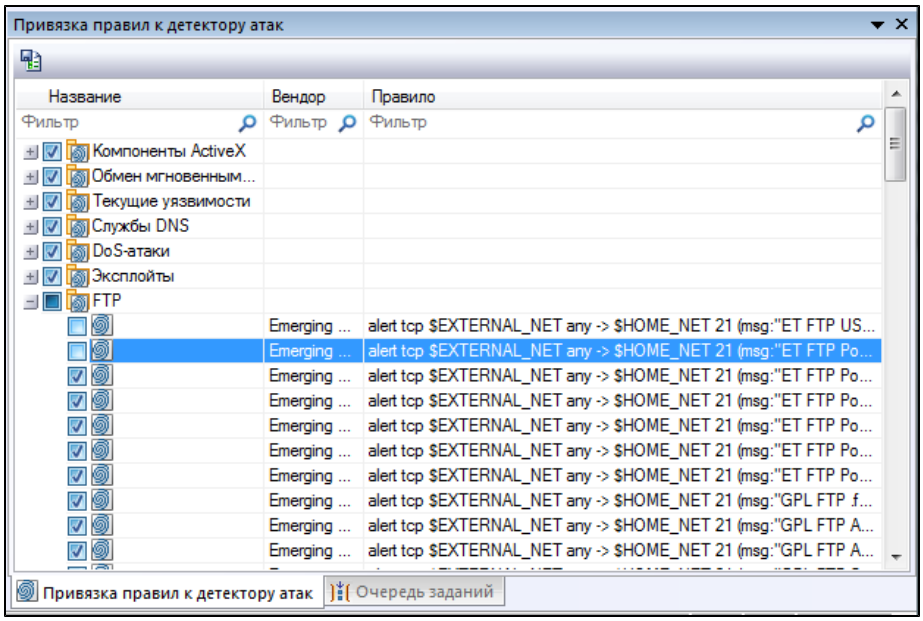
Для назначения правил:

1. Выберите в списке детектор, 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 сохранения внесенных изменений нажмите кнопку  в панели инструментов дополнительного окна.

Работа с правилами

Для работы с правилами используются средства ПУ ЦУС.

Работа с правилами включает в себя выполнение следующих операций:

- просмотр и редактирование параметров правил;
- назначение правил детекторам атак;
- создание новых правил и занесение их в БД ЦУС;
- удаление правил из БД ЦУС;
- загрузка правил в БД ЦУС с сервера обновлений.

Загрузка сертификатов обновлений

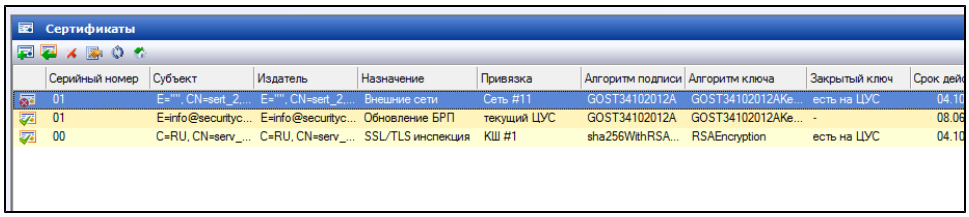
Для первоначальной загрузки базы решающих правил и последующего ее обновления необходимо получить у поставщика правил сертификат, который используется для проверки цифровой подписи при загрузке или обновлении правил.

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 дереве объектов главного окна ПУ ЦУС выберите узел "Центр управления сетью" и в нем — папку "Сертификаты".

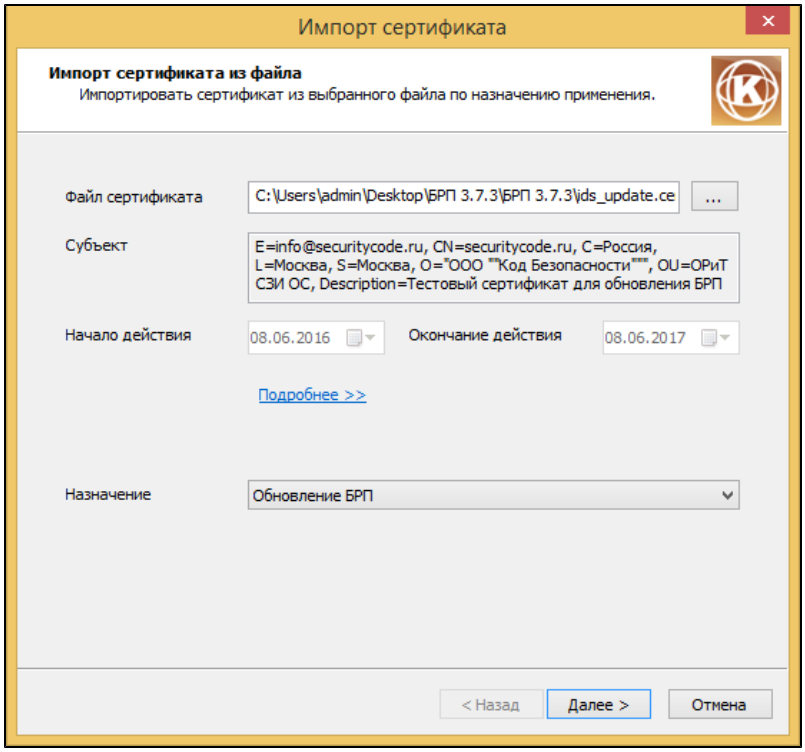
   В правой части окна отобразится список зарегистрированных в БД ЦУС сертификатов.



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

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

   На экране появится диалог "Импорт сертификата".



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

   На экране появится стандартный диалог ОС Windows открытия файла.

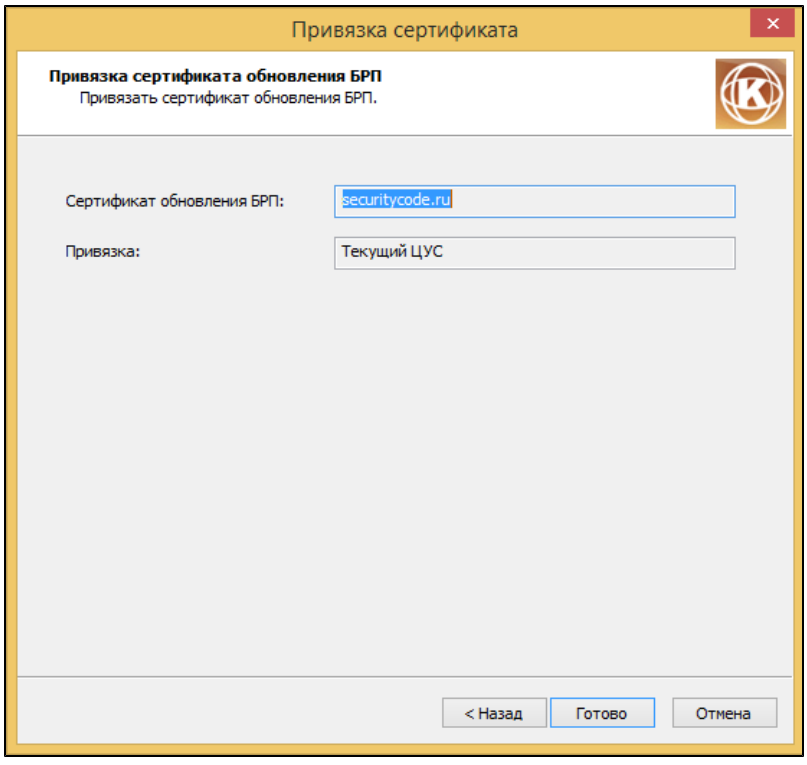
4. Укажите папку и затем файл сертификата.

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

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

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

   Диалог "Импорт сертификата" закроется, и на экране появится диалог "Привязка сертификата".



Поля в диалоге будут заполнены автоматически.

6. Нажмите кнопку "Готово".

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

Загрузка правил

Для работы ДА в режиме сигнатур в БД ЦУС должны быть загружены правила, на основании которых детектором атак принимаются решения об атаках. Источником правил является база решающих правил, 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.

Предусмотрено два варианта загрузки правил:

- автоматическая загрузка (по расписанию, с использованием агента обновлений и абонентского пункта);
- ручная загрузка (с USB-флеш-накопителя).

Независимо от варианта при загрузке выполняется проверка цифровой подписи поставщика правил. Для проверки используется сертификат, выпущенный поставщиком правил и загруженный в БД ЦУС. Загрузку сертификата см. стр.**25**.

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 проверить наличие установленной лицензии на загрузку обновлений базы решающих правил. Работа с лицензиями описана в [**1**].
2. Установить в ПУ ЦУС сертификат поставщика обновлений базы решающих правил, используемый для проверки цифровой подписи (см. стр.**25**).
3. Настроить расписание автоматического обновления базы решающих правил (см. стр.**36**).

4. Установить на компьютер с агентом обновлений сертификат пользователя и корневой сертификат (см. стр.**35**).
5. Подготовить внешний носитель с ключами ЦУС.
6. Настроить агент обновлений для связи с ЦУС (см. стр.**38**).

Ручная загрузка правил

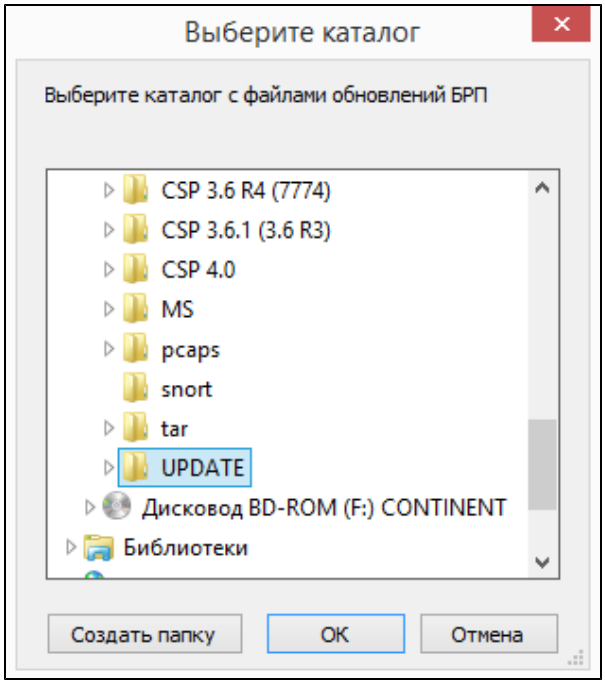
Загрузка правил в БД ЦУС осуществляется администратором с USB-флеш-накопителя.

Для загрузки правил:

1. Выберите в окне объектов папку "База решающих правил".

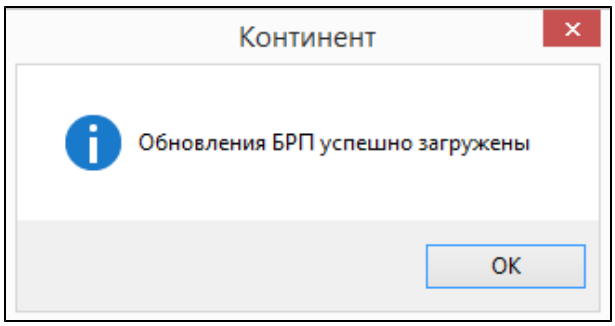
   В главном окне отобразится список групп загруженных в БД ЦУС правил.
2. Вставьте USB- флеш- накопитель с записанными на нем решающими правилами (обновлениями).
3. В панели инструментов нажмите кнопку  .

   На экране появится стандартный диалог 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 главном окне появятся группы загруженных правил.

Просмотр и редактирование правил

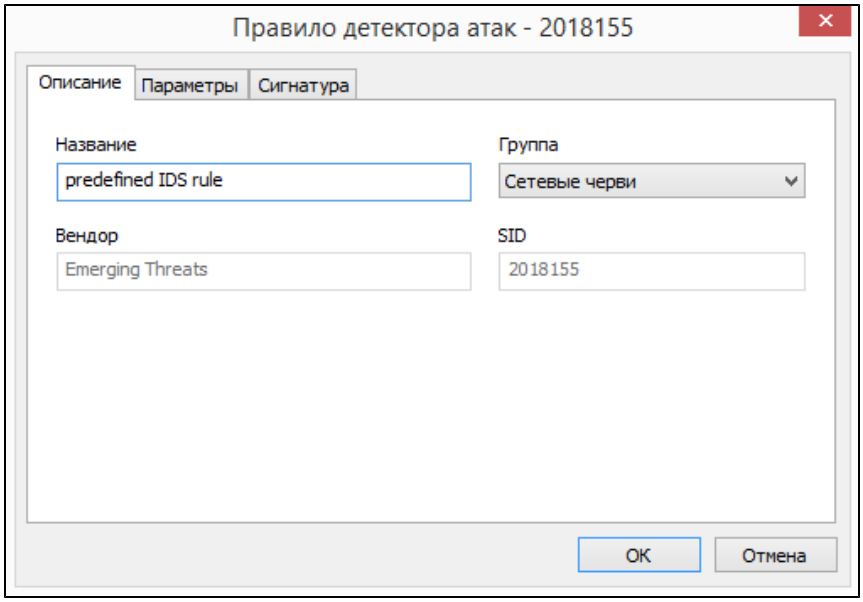
Просмотр параметров правил без возможности их редактирования может выполняться при работе со списком детекторов атак (см. стр.**22**).

Редактирование правил выполняется при работе со списком правил.

Для редактирования параметров правила:

1. Откройте список правил (см. стр.**13**).
2. Раскройте нужную группу, выберите правило и нажмите в панели инструментов кнопку  .

   На экране появится диалог "Правило детектора атак", открытый на вкладке "Описание". В заголовке диалога отображается SID выбранного правила.



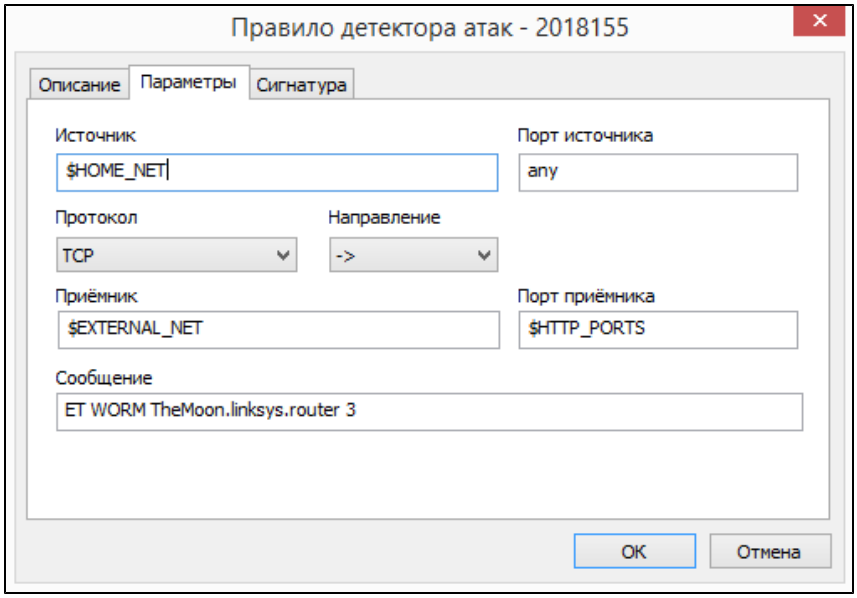
3. При необходимости изменить название правила вручную отредактируйте содержимое поля "Название".

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

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

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

4. Перейдите на вкладку "Параметры".

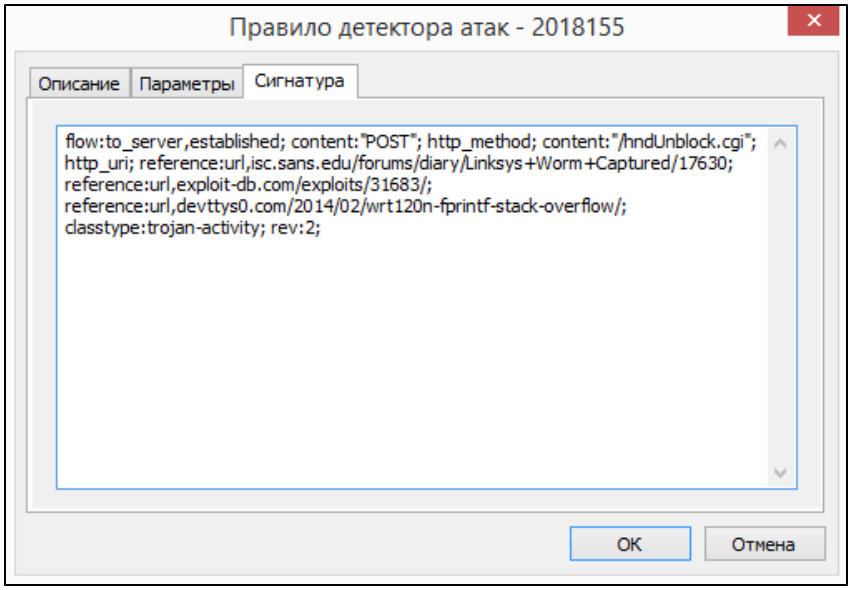


5. При необходимости измените значения параметров.

Источник	Введите IP-адрес (для IP4V и IP6V) или переменную в соответствии с синтаксисом решающих правил СОВ
Порт источника	Введите порт источника в соответствии с синтаксисом решающих правил СОВ
Протокол	Выберите из списка протокол. Доступные значения: • TCP; • UDP; • ICMP; • IP
Направление	Выберите из списка направление. Доступные значения: • ->; • < >
Приемник	Введите IP-адрес (для IP4V и IP6V) или переменную в соответствии с синтаксисом решающих правил СОВ
Порт приемника	Введите порт источника в соответствии с синтаксисом решающих правил СОВ
Сообщение	Введите текст сообщения, используя буквы латинского алфавита

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

6. Перейдите на вкладку "Сигнатура".



7. При необходимости внесите изменения в содержимое сигнатуры, используя синтаксис решающих правил СОВ.
8. Для завершения процедуры редактирования нажмите кнопку "ОК".

   Диалог "Правило детектора атак" закроется.
9. Для сохранения изменений в БД ЦУС нажмите кнопку в панели инструментов.

   Внимание! Если отредактированное правило необходимо привязать к ДА, к которому оно не было привязано (отметка отсутствует), установите отметку и нажмите кнопку в панели инструментов.

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 правил стр.13.
2. Нажмите кнопку в панели инструментов.

   На экране появится диалог "Правило детектора атак", открытый на вкладке "Описание". Описание полей вкладки см. стр.22.
   - В поле "Вендор" по умолчанию установлено значение "Пользовательские правила". Поле редактированию не подлежит.
   - В поле "Группа" по умолчанию установлено значение "Группа по умолчанию". Изменять значение не рекомендуется.
   - Поле "SID" отсутствует. Значение SID будет автоматически сгенерировано в ЦУС после завершения процедуры формирования правила.
3. Введите название создаваемого правила и перейдите на вкладку "Параметры". Описание полей вкладки см. стр.22.
4. Заполните поля и перейдите на вкладку "Сигнатура".
5. Введите правило в соответствии с синтаксисом решающих правил СОВ и нажмите кнопку "ОК".

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

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

Если ошибки не обнаружены, диалог "Правило детектора атак" закроется и новое правило будет добавлено в список.

6. Для сохранения правила в БД ЦУС нажмите кнопку  в панели инструментов.

   После сохранения в поле "Правило" появится автоматически сгенерированное значение SID.

Удаление правила

Для удаления правила:

1. Откройте список правил (см. стр.**13**).
2. Выберите в списке нужное правило и нажмите кнопку  в панели инструментов.

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

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

Агент обновлений

Агент обновлений предназначен для загрузки в БД ЦУС решающих правил и их обновлений. Источником решающих правил и обновлений является сервер поставщика правил (сервер обновлений).

Примечание. Решающие правила и обновления могут быть загружены в ручном режиме без использования агента обновлений (см. стр.28).

Агент устанавливают на компьютер, на котором установлен абонентский пункт версии не ниже 3.7. При этом абонентский пункт используется исключительно для установления защищенного соединения с сервером обновлений.

Программное обеспечение абонентского пункта содержится в составе дистрибутивного диска №2 "Документация и утилиты", входящего в комплект поставки.

При установке ПО абонентского пункта необходимо выполнить следующее:

- исключить из состава устанавливаемого ПО компонент "межсетевой экран";
- в диалоге "Конфигурация АП" оставить без изменения все установленные по умолчанию параметры.

После установки ПО настройка параметров абонентского пункта не требуется.

Предусмотрено два режима работы агента обновлений:

- с использованием подключения к ЦУС; в этом режиме загрузка обновлений осуществляется через установленное защищенное соединение с ЦУС;
- без подключения к ЦУС; в этом режиме агентом выполняется выгрузка обновлений на внешний носитель и далее обновления вручную загружаются в БД ЦУС средствами ПУ ЦУС.

Режим работы задают при настройке агента (см. стр.36).

Установка агента

Установку агента обновлений выполняют с установочного диска компонентов подсистемы управления АПКШ "Континент". Процедура установки подсистемы управления описана в [1]. 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 в программной группе "Код Безопасности | Континент 3.7" 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.33).
2. Установить сертификат пользователя и корневой сертификат (см. стр.35).
3. Настроить и запустить агент (см. стр.36, стр.39).

Программа управления агентом обновлений

Программа используется для настройки и 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 3.7 | 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 в соответствии с заданными настройками.

Команды программы 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
Параметры агента...	Открывает диалог программы управления агентом, предназначенный для просмотра и настройки параметров агента
Обновление БРП...	Открывает диалог, предназначенный для получения обновлений без соединения с ЦУС с последующей ручной загрузкой. При работе агента в режиме с подключением к ЦУС команда заблокирована
Удалить сохраненный пароль к ЦУС	Удаляет сохраненный пароль доступа к ключам ЦУС. При выполнении команды "Запустить агент" потребуется ввести пароль. При работе агента в режиме без подключения к ЦУС команда заблокирована
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).

Установка сертификата пользователя и корневого сертификата

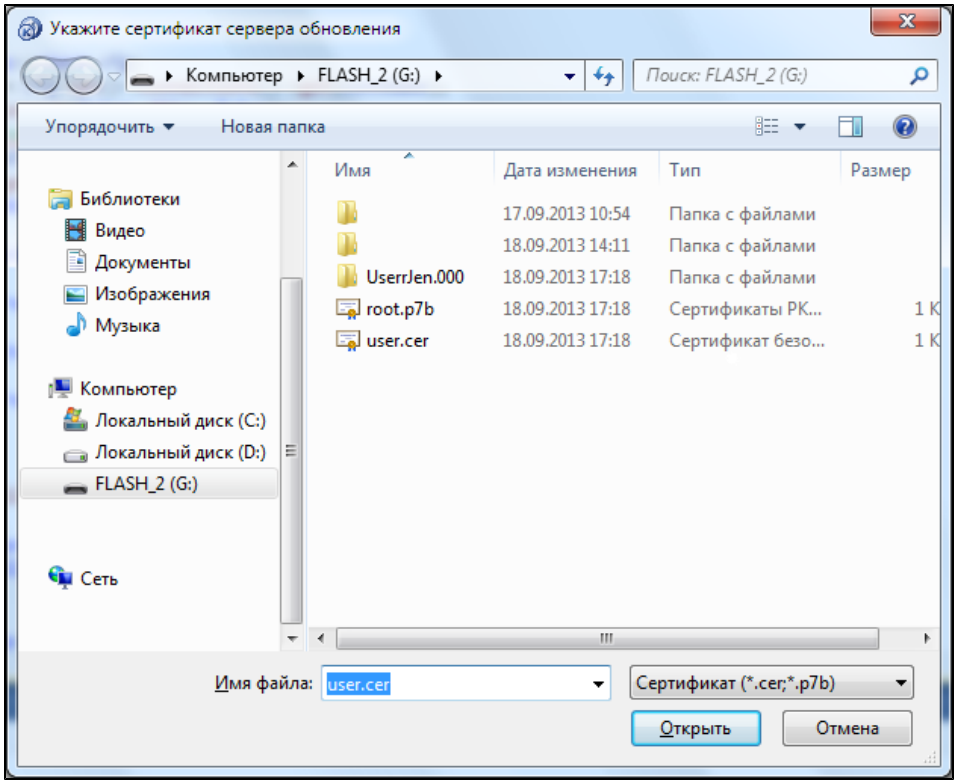
Сертификат пользователя и корневой сертификат, полученные от поставщика в виде двух файлов и ключевого контейнера, хранятся на внешнем носителе.

Установка сертификатов выполняется в программе управления агентом обновлений.

Для установки сертификатов:

1. Вставьте внешний носитель с сертификатами и ключевым контейнером.
2. Вызовите контекстное меню пиктограммы агента обновлений в панели задач и выберите команду "Импорт сертификата сервера обновлений".

   На экране появится стандартный диалог выбора файла.



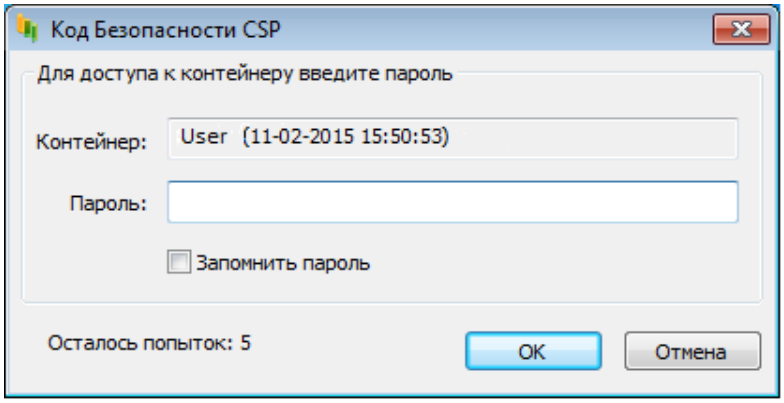
3. Выберите на внешнем носителе пользовательский сертификат и нажмите кнопку "Открыть".

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

   Дождитесь завершения проверки соединения.

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

   На экране появится диалог ввода пароля доступа к ключевому контейнеру.



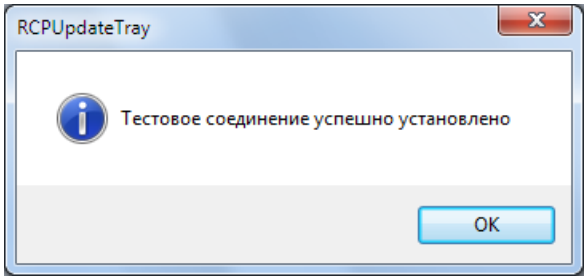
4. Введите пароль доступа к ключевому контейнеру, полученный от поставщика, установите отметку в поле "Запомнить пароль" и нажмите кнопку "OK".

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

5. Нажмите в окне запроса кнопку "Да".

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

   Дождитесь установления соединения. На экране появится сообщение об установленном тестовом соединении.



   Пиктограмма абонентского пункта в панели задач будет отображать установленное соединение.

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

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

6. Нажмите кнопку "OK" в окне сообщения.

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

   Сертификат пользователя и корневой сертификат установлены.

Настройка агента обновлений

Для настройки агента необходимо выполнить следующее:

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

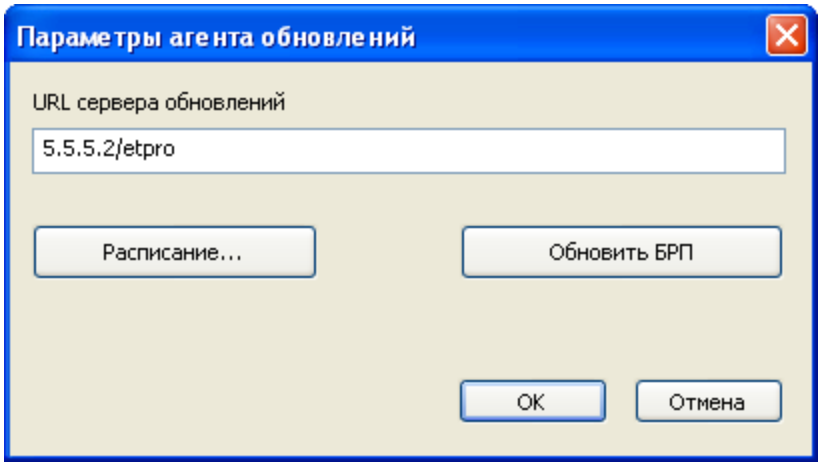
Настройка расписания

Перед началом настройки расписания убедитесь, что сертификат обновлений загружен (см. стр.**25**).

Для настройки расписания:

1. В главном меню ПУ ЦУС выберите команду "ЦУС | Настройка агента обновлений БРП".

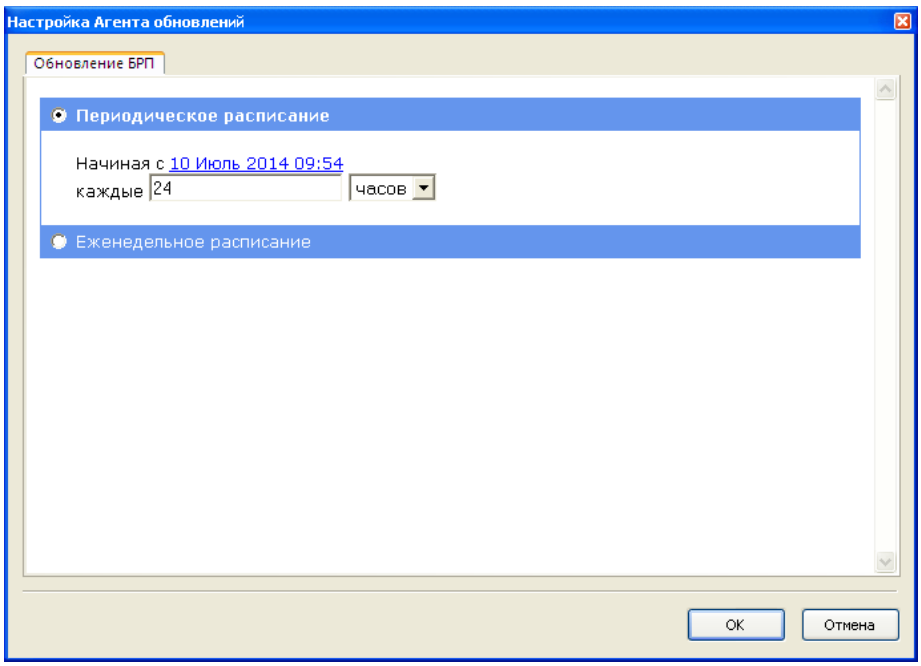
   На экране появится диалог "Параметры агента обновлений".



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

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

   На экране появится диалог "Настройка агента обновлений".



   В диалоге представлены два варианта настройки расписания.

3. Выберите нужный вариант расписания и настройте его.

Периодическое расписание	Включает режим загрузки обновлений, при котором запуск процесса осуществляется через равные промежутки времени. Продолжительность промежутка задается количеством минут или часов. Режим начинает действовать с момента наступления определенной даты и времени. Чтобы указать другой момент начала действия режима, активируйте ссылку с текущим значением даты и времени и в появившемся на экране диалоге введите нужные значения. Способы выбора и редактирования значений в этом диалоге аналогичны стандартным способам, принятым в ОС Windows

Еженедельное расписание	Включает режим загрузки обновлений, при котором запуск процесса осуществляется в моменты времени, заданные специальным расписанием. Расписание представлено в виде таблицы, разделенной, для оптимального отображения, на две части. В столбцах таблицы перечислены дни недели, а в строках — часы и минуты с шагом 30 минут. Выбор времени запуска процесса осуществляется посредством установки отметки в соответствующей ячейке таблицы. Для установки отметки поместите указатель в ячейку и нажмите левую кнопку мыши. Повторное нажатие кнопки приводит к удалению отметки. Действие расписания повторяется еженедельно

4. После настройки расписания нажмите кнопку "ОК".

   Диалог "Настройка агента обновлений" закроется.

5. Для сохранения выполненных настроек нажмите кнопку "ОК" в диалоге "Параметры агента обновлений".

   Диалог "Параметры агента обновлений" закроется.

Примечание. Для загрузки правил и обновлений по настроенному расписанию агент обновлений должен быть запущен (см. стр.39).

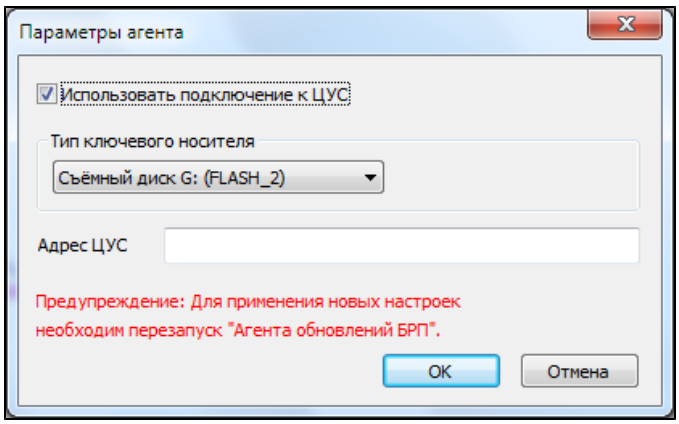
Задание и настройка режима работы агента

Данная настройка выполняется локально на компьютере с установленным агентом обновлений и заключается в задании режима работы агента (с подключением или без подключения к ЦУС) и указании типа ключевого носителя, на котором хранятся ключи для связи с ЦУС.

Для настройки агента:

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

   На экране появится диалог "Параметры агента".



3. Заполните поля диалога и нажмите кнопку "ОК".

Поле	Описание
Использовать подключение к ЦУС	• Установите отметку, если необходимо включить режим работы агента с подключением к ЦУС. • Удалите отметку, если необходимо использовать режим работы агента без подключения к ЦУС
Тип ключевого носителя	Выберите из списка нужный ключевой носитель
Адрес ЦУС	Введите или измените IP-адрес КШ с ЦУС

Диалог "Параметры агента" закроется. Измененные значения параметров будут применены при следующем запуске агента.

Запуск агента

В зависимости от настроек запуск агента осуществляется автоматически или вручную по команде программы управления.

Автоматический запуск агента происходит в следующих случаях:

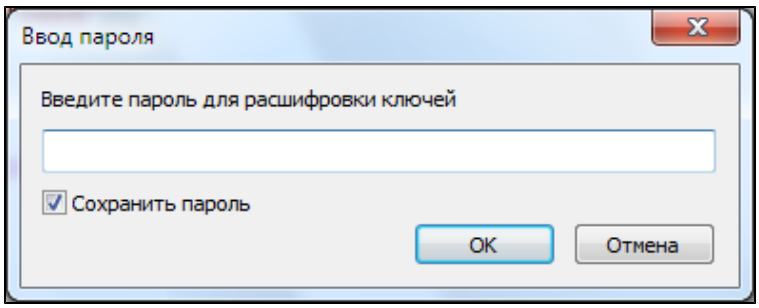
- при перезагрузке системы, если в настройках агента задан режим без использования соединения с ЦУС;
- при перезагрузке системы, если в настройках агента задан режим с использованием соединения с ЦУС и был установлен режим хранения пароля для доступа к ключевому контейнеру.

При запуске агента вручную, если задан режим с использованием соединения с ЦУС и во время предыдущего запуска не был задан режим хранения пароля, потребуется ввести пароль доступа к ключевому контейнеру.

Для запуска агента вручную:

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

   Если используется режим соединения с ЦУС и во время предыдущего запуска не был задан режим хранения пароля, на экране появится запрос на ввод пароля для расшифровки ключей:



2. Введите пароль доступа к ключевому контейнеру.
3. Если запрос пароля при следующем запуске не требуется, установите отметку в поле "Сохранить пароль". В этом случае при следующей перезагрузке системы агент запустится автоматически.

   Внимание! При использовании ключей связи с ЦУС версии 3.6 сохранение пароля недоступно.
4. 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 должны быть соблюдены следующие условия:

- настроена автоматическая загрузка правил (см. стр.**27**);
- агент обновлений запущен (см. стр.**39**).

Для принудительной загрузки обновлений:

1. В главном меню ПУ ЦУС выберите команду "ЦУС | Настройка агента обновлений БРП".

   На экране появится диалог "Параметры агента обновлений".
2. Нажмите кнопку "Обновить БРП".

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

3. Закройте окно сообщения.
4. Закройте диалог "Параметры агента обновлений" нажатием кнопки "ОК".

Ручная загрузка обновлений

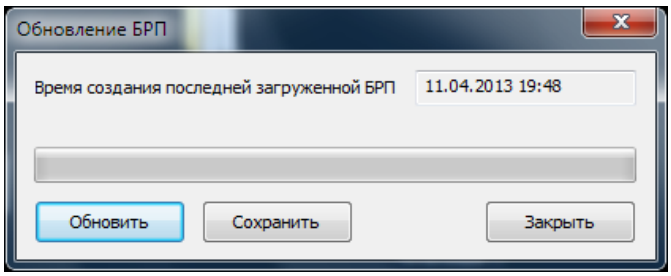
Ручная загрузка обновлений применяется в тех случаях, когда по каким-либо причинам отсутствует связь агента обновлений с ЦУС. Агент получает обновления с сервера поставщика решающих правил и сохраняет их на жестком диске или внешнем носителе. Далее обновления вручную загружаются в БД ЦУС средствами ПУ ЦУС (см. стр.**28**).

Внимание! Перед выполнением данной процедуры необходимо перевести агент обновлений в режим работы без подключения к ЦУС (см. стр.**38**).

Для загрузки обновлений:

1. Если планируется сохранение обновлений на внешнем носителе, вставьте его в USB-разъем.
2. Вызовите контекстное меню пиктограммы "Программа управления агентом" и активируйте команду "Обновление БРП".

   На экране появится диалог "Обновление БРП".



   В верхней части диалога отображаются дата и время загрузки правил или их последнего обновления. Если правила в БД ЦУС не загружались, поле – пустое.
3. Нажмите кнопку "Обновить".

   Начнется установление соединения с сервером поставщика правил и проверка агентом наличия обновлений.

   - Если обновления на сервере поставщика правил отсутствуют, на экране появится сообщение об актуальности БРП.

     Закройте окно сообщения и затем закройте диалог "Обновление БРП" нажатием кнопки "Закрыть".
   - Если обновления на сервере обнаружены, агент начнет их загрузку. При этом в средней части диалога будут появляться сообщения о загружаемых файлах с отображением индикатора загрузки, а кнопка "Обновить" заменится кнопкой "Отмена".

     При необходимости отменить загрузку нажмите кнопку "Отменить" или "Закрыть".

     После успешной загрузки всех файлов обновлений на экране появится соответствующее сообщение.
4. Закройте окно сообщения и нажмите кнопку "Сохранить".

   На экране появится стандартный диалог выбора места сохранения файлов.
5. Укажите в диалоге папку или внешний носитель для сохранения файлов обновлений и нажмите кнопку "ОК".

   Диалог закроется и на экране появится сообщение об успешном сохранении БРП.

Обновления сохраняются в виде папки **update**, содержащей четыре файла. При копировании обновлений вручную с жесткого диска на внешний носитель необходимо скопировать всю папку целиком.

6. Закройте окно сообщения и затем закройте диалог "Обновление БРП" нажатием кнопки "Закрыть".
7. Сохраненные файлы обновлений вручную загрузите в БД ЦУС средствами ПУ ЦУС (см. стр.**28**).

Ручной запуск контроля целостности

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

Контроль целостности осуществляется с помощью специальной программы ngc.exe, хранящейся в папке "...\Континент\Update Agent", указанной при установке подсистемы управления АПКШ "Континент".

Примечание. По умолчанию при установке подсистемы управления файлы копируются на системный диск в папку \Program Files\Код Безопасности\Континент.

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 "ОК".

   Окно программы закроется.

Локальное управление детектором атак

Общие операции

Включение/выключение и перезагрузка ДА, а также администрирование ПАК "Соболь" выполняются в полном соответствии с описанием данных процедур для сетевых устройств (см. [**2**], раздел "Общие операции").

Локальное управление осуществляется с помощью команд главного локального меню. Главное локальное меню доступно только пользователю, обладающему правами администратора ПАК "Соболь".

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

Переход к режиму настройки детектора атак

Для перехода к режиму настройки:

1. Выключите питание ДА. Подключите к системному блоку ДА клавиатуру и монитор.
2. Включите питание ДА. 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.
3. Введите пароль администратора и нажмите клавишу <Enter>.

   На экране появится меню администратора ПАК "Соболь".
4. 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
   ```
5. 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: Выключить
   2: Перезагрузить
   3: Управление
   4: Настройки безопасности
   5: Настройка ДА
   6: Настройка СД (функция недоступна)
   7: Тестирование
   0: Выход
   Выберите пункт меню (0-7):
   ```
6. Введите в строке ввода номер команды "Настройки 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.

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

Управление режимами работы детектора атак

Включение и выключение сигнатурного анализатора

Для включения/выключения сигнатурного анализатора:

1. Войдите в меню настройки ДА (см. стр.**42**).
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>.

Включение и выключение контроля приложений

Внимание! При включении режима средствами локального управления будут восстановлены последние настройки контроля приложений, выполненные в ПУ ЦУС.

Для включения/выключения режима:

1. Войдите в меню настройки ДА (см. стр.**42**).
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

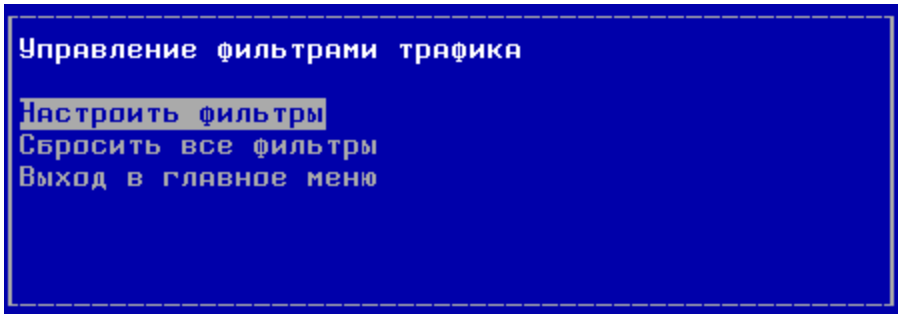
Данные настройки позволяют устанавливать и настраивать на интерфейсах мониторинга фильтры с целью снижения нагрузки на систему. В результате будет производиться анализ только тех пакетов, которые соответствуют параметрам фильтра. Такими параметрами могут быть, например, тип протокола, IP-адрес, источник/получатель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

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

Для работы с фильтрами:

1. Войдите в меню настройки ДА (см. стр.**42**).
2. Введите номер команды "Фильтры трафика" и нажмите клавишу <Enter>.

   На экране появится меню "Управление фильтрами трафика".



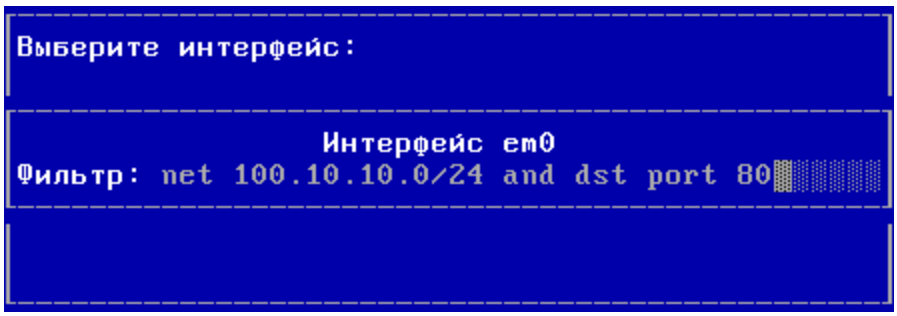
Для настройки фильтров:

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.67).

   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

Внимание! 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. [**1**]).

   На экране появится дополнительное меню (см. Табл.1).
3. Введите номер команды и нажмите клавишу <Enter>.

   Выполняйте указания, отображаемые на экране.
4. Для выхода из дополнительного меню нажмите комбинацию клавиш <ALT+F1>.

Табл.1 Команды дополнительного меню

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

Табл.2 Команды меню "Диагностика"

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

Передача сведений в СОПКА

Описание функции

В АПКШ "Континент" имеется возможность передавать в систему обнаружения и предупреждения компьютерных атак (СОПКА) сведения о компьютерных атаках, зарегистрированных в СОВ.

Сведения представляют собой записи журнала НСД. О каждой компьютерной атаке передается следующая информация:

- время атаки (в формате UTC);
- ID сенсора (ID детектора атак);
- ID модуля (назначается ФСБ России для ПО Континент);
- ID сигнатуры (Код сигнатуры);
- ревизия сигнатуры;
- Src IP;
- Dst IP;
- Src port;
- Dst port;
- протокол;
- ID SigGenerator (из snort);
- приоритет из описания сигнатуры;
- критичность.

Отправка сведений осуществляется по защищенному каналу на основании запроса администратора СОПКА.

Описание работы

Для передачи сведений в СОПКА используется специальное клиент-серверное приложение.

Клиентская часть (далее — клиент) устанавливается вместе с программой просмотра журналов на компьютер, расположенный в локальной сети АПКШ "Континент". Серверная часть (далее — Сервер), реализованная как веб-сервер, устанавливается в локальной сети СОПКА и настраивается на совместную работу с NFS-сервером.

Клиент в соответствии с настройками извлекает из базы данных журналов нужные записи и передает их по защищенному каналу на веб-сервер. Далее в соответствии с настройками сведения помещаются в определенное хранилище NFS-сервера.

Для реализации защищенного канала используются СКЗИ "Континент-АП" и сервер доступа, входящий в состав АПКШ "Континент".

Примечание. Защищенный канал может быть реализован на базе решения TLS-клиент — TLS-сервер.

Процедура передачи сведений в СОПКА и все необходимые для этого настройки приведены в [**3**].

Приложение

Программные модули, требующие контроля целостности

Ниже в таблицах приведены списки всех используемых модулей ПО ДА и агента обновлений, 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

Имя	Описание
/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
/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 псевдографических 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
/bin/memtester	Программа проверки оперативной памяти
/bin/nictest	Программа проверки сетевых интерфейсов
/bin/stress	Программа проверки процессора
/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

Имя	Описание
/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 C++
/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	Рутокен
/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
/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

Имя	Описание
/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

Табл.5 Программные модули агента обновлений

Имя*	Описание
...\Континент\Update Agent\Ngc.exe	Утилита проверки контроля целостности
...\Континент\Update Agent\RCPUpdateAgent.exe	Агент обновлений
...\Континент\Update Agent\RCPUpdateTray.exe	ПУ агента обновлений
...\Континент\Update Agent\uc.dll	Библиотека общих и вспомогательных функций
...\Континент\Update Agent\XmlDocument.dll	Библиотека для работы с XML-документами

* Программные модули находятся в папке, указанной при установке агента обновлений. В таблице указывается папка, предлагаемая мастером установки по умолчанию.

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

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

Протокол

Используются tcp, udp, icmp и ip.

Адреса IP

После протокола в правиле указываются адреса и номера портов для данного правила. Ключевому слову **any** будут соответствовать все адреса IP (0.0.0.0/0). Механизм определения адресов по именам хостов не поддерживается, поэтому в правилах должны указываться адреса IP 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 хоста.

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";)

Номера портов

Номера портов можно задавать в виде конкретного значения, диапазона, списка или ключевого слова **any** (любой порт). Для портов также поддерживается оператор отрицания. Для задания диапазона указываются верхний и нижний пределы, разделенные двоеточием (:). Граничные значения включаются в диапазон.

Пример правила, которому будут соответствовать все пакеты UDP, адресованные в порты с 1 по 1024 хостов сети класса C 192.168.1.0:

log udp any any -> 192.168.1.0/24 1:1024 log udp

Оператор направления

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

Пример двунаправленного правила:

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

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 похожи на правила alert, но включают добавочное поле activates. Динамические правила похожи на правила log, но включают два добавочных поля – activated_ by и count. Все добавочные поля правил activate/dynamic являются обязательными.

Правила activate подобны правилам alert, но кроме генерации сигнала говорят о необходимости добавления (активации) другого правила при выполнении заданных условий. Правила dynamic подобны правилам log, но включаются только при выполнении правила activate с заданным идентификатором.

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

Опции Meta-Data

msg

Указывает на необходимость включения текстового сообщения в запись журнального файла или дампа пакета. Представляет собой текстовую строку с использованием в качестве escape-символа для задания символов, имеющих специальное значение в правилах (например символ ;).

Формат:

msg: "<текст сообщения>";

reference

Позволяет включать в правила ссылки на внешние системы идентификации атак.

Формат:

reference: ,; [reference: ,;]

sid

Ключевое слово sid предназначено для идентификации правил. Значения идентификаторов используются подключаемыми модулями вывода. Опцию следует использовать вместе с ключевым словом rev (см. ниже). В правилах глобального значения используются значения sid в диапазоне от 100 до 1000000. Значения менее 100 зарезервированы, а значения, превышающие 1 000 000, предназначены для локального использования (идентификации ваших собственных правил).

Файл sid-msg.map содержит список сигналов для различных значений sid, используемых правилами. Эта информация может быть полезна при последующей обработке сигналов, поскольку позволяет получить текст сообщения по его идентификатору.

Формат:

sid: <идентификатор правила>;

rev

Ключевое слово sid служит для идентификации правил, а используемое вместе с ним ключевое слово rev позволяет указать номер ревизии (версии) правила с данным идентификатором. Эту опцию следует использовать совместно с ключевым словом sid (см. выше).

Формат:

rev: <номер ревизии>

classtype

Ключевое слово classtype указывает категорию сигнала в соответствии с классом атаки по частоте использования и важности. Пользователь может самостоятельно задать уровень приоритета для каждого типа правил.

Формат:

classtype: <имя класса>;

Стандартная классификация правил:

Имя класса	Описание	Приоритет
attempted-admin	Попытка получения привилегий администратора	Высокий
attempted-user	Попытка получения привилегий пользователя	Высокий
shellcode-detect	Обнаружен исполняемый код	Высокий
successful-admin	Получены права администратора	Высокий

Имя класса	Описание	Приоритет
successful-user	Получены права пользователя	Высокий
trojan-activity	Обнаружена сетевая троянская программа	Высокий
unsuccessful-user	Неудачная попытка получения привилегий пользователя	Высокий
web-application-attack	Атака на веб-приложение	Высокий
attempted-dos	Предпринята атака на службы (DoS)	Средний
attempted-recon	Попытка несанкционированной передачи информации (утечка)	Средний
bad-unknown	Непонятный трафик, который может оказаться опасным	Средний
denial-of-service	Обнаружена атака на службы (DoS)	Средний
misc-attack	Прочие атаки	Средний
non-standard-protocol	Зафиксировано использование нестандартного протокола	Средний
rpc-portmap-decode	Обнаружен запрос RPC1	Средний
successful-dos	Успешная атака на службы (DoS)	Средний
successful-recon-largescale	Крупномасштабная утечка информации	Средний
successful-recon-limited	Утечка информации	Средний
suspicious-filename-detect	Обнаружено подозрительное имя файла	Средний
suspicious-login	Попытка входа в систему с использованием подозрительного имени	Средний
system-call-detect	Обнаружен вызов системной функции	Средний
unusual-client-port-connection	Клиент использует необычный порт	Средний
web-application-activity	Доступ к потенциально опасному веб-приложению	Средний
icmp-event	Обычный пакет ICMP	Низкий
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

priority

Тег priority используется для присвоения правилам уровня приоритета. Опция classtype присваивает правилу принятый по умолчанию уровень приоритета, который можно изменить с помощью priority.

Формат:

priority: <целое число>;

Опции проверки содержимого пакетов (Payload)

content

Эта опция позволяет пользователю создавать правила для поиска в пакетах определенной информации и выполнения тех или иных действий при ее обнаружении. Для проверки содержимого пакетов используется функция поиска по шаблону Boyer- Moore. Если заданная последовательность данных обнаружена в поле содержимого пакета, проверка считается успешной и выполняется остальная часть правила. Следует помнить, что при поиске учитывается регистр символов.

Аргумент опции может содержать как текст, так и двоичные данные (обычно они указываются между парой символов | и задаются последовательностью шестнадцатеричных представлений байтов).

Пример задания строки поиска, содержащей текст и бинарные данные:

alert tcp any any -> any 139 (content:"|5c00|P00|I|00|E|00 5c|";)

В одном правиле может присутствовать более одной опции content, что позволяет снижать уровень ложных срабатываний за счет более точного задания искомых последовательностей.

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.

Формат:

content: [!] "<строка поиска>";

Пример поиска текстовой строки:

alert tcp any any -> any 80 (content:!"GET":)

Изменение параметров поиска

Ключевое слово content поддерживает множество опций-модификаторов, которые изменяют поведение системы поиска.

Список модификаторов:

- depth (размер области поиска);
- offset (смещение начала поиска от начала поля данных);
- distance (количество пропускаемых байтов после первого найденного соответствия);
- within (размер области поиска после первого найденного соответствия);
- nocase (без учета регистра символов);
- rawbytes (поиск в необработанных данных).

nocase

Ключевое слово nocase позволяет осуществлять поиск, заданный предыдущей опцией content, без учета регистра символов.

Формат:

nocase;

rawbytes

Ключевое слово rawbytes позволяет искать в пакете необработанные (raw) данные, игнорируя декодирование, выполняемое препроцессорами. Ключевое слово изменяет поиск данных, указанных предыдущей опцией content.

Формат:

rawbytes;

depth

Ключевое слово **depth** показывает размер блока данных из пакета, в котором осуществляется поиск, заданный предыдущей опцией content. Например, при задании глубины 5 будут просматриваться в поисках заданной последовательности только первые 5 байтов поля данных в пакете.

Ключевое слово **depth** меняет режим поиска для опции **keyword**, указанной перед **depth**.

Формат:

depth: <целое число>;

offset

Ключевое слово **offset** позволяет задать смещение в поле данных пакета, с которого начинается поиск последовательности, заданной предыдущей опцией content. Например, **offset 5** будет начинать поиск, пропустив первые 5 байтов поля данных.

Ключевое слово **offset** меняет режим поиска для опции **keyword**, указанной перед **offset**.

Формат:

offset: <целое число>;

distance

Ключевое слово **distance** показывает – сколько байтов нужно пропустить после найденной предыдущей опцией **content** строки поиска для начало поиска последовательности, заданной другой опцией **content**. Например, правило

alert tcp any any -> any any (contenet: ”ABC”; content: “DEF”; distance: 1;)

позволяет находить в поле данных пакета строки вида ABC?DEF (знак вопроса означает любой символ).

Формат:

distance: <число байтов>;

within

Ключевое слово **within** показывает размер области поиска для опции **content** от конца подстроки, найденной предыдущей опцией **content**. Например, правило

alert tcp any any -> any any (contenet: ”ABC”; content: “DEF”; distance: 1;)

ограничивает поиск подстроки DEF 10 байтами после найденной в поле данных подстроки ABC.

Формат:

within: <число байтов>;

uricontent

Опция **uricontent** служит для поиска в нормализованных полях запросов URI. При создании правил, включающих нормализуемые данные (например, %2f или обход каталогов – directory traversal), эти правила не следует использовать.

При создании правил **uricontent** укажите содержимое, которое необходимо найти в контексте нормализованного URI. Например, если нормализуется обход каталогов (directory traversal), не включайте directory traversal.

Можно создавать правила поиска в ненормализованном содержимом пакетов с помощью опции content (см. выше).

Эта опция использует тот же набор модификаторов, который применяется для описанной выше опции content.

Эта опция работает совместно с препроцессором HTTP Inspect.

Формат:

uricontent:[!];

isdataat

Эта опция позволяет проверить наличие данных в заданном участке пакета (возможно относительно завершения подстроки, найденной с помощью опции content).

Формат:

isdataat:[,relative];

pcre

Ключевое слово pcre позволяет создавать правила, содержащие регулярные выражения, совместимые с языком perl.

Формат:

pcre:[!]"(//|m)[ismxAEGRUB]";

Модификаторы в конце правила устанавливают флаги для регулярного выражения.

Модификаторы, совместимые с Perl:

i	Регистр символов не принимается во внимание
s	Включать символы новой строки в dot metacharacter
m	По умолчанию строка трактуется как одна большая последовательность символов. С помощью специальных символов ^ и $ можно задать проверку соответствия для начала или конца строки. При наличии модификатора m символы ^ и $ задают поиск соответствия в начале или в конце каждой новой строки (относительно символа перевода строки в буфере), а также в начале и в конце буфера
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 буфера (аналогично ^)
E	Задает для $ поиск соответствия только в самом конце строки. Без модификатора E символ $ будет задавать также поиск перед символом новой строки (если таковой имеется) в конце буфера
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.

byte_test

Эта опция позволяет сравнить байт с заданным значением. Опция может использоваться применительно к двоичным значениям или их символьному представлению.

Формат:

byte_test: <bytes to to convert>, [!]<operator>, <value>, <offset> \ [,relative] [,<endian>] [,<number type>, string];

Параметры опции byte_test:

Параметр	Описание
bytes_to_ convert	Число байтов, которые могут извлекаться из пакета
operator	Операция, выполняемая для сравнения байта с заданным значением: • < - меньше; • > - больше; • = - равно; • ! - не совпадает; • & - побитовая операция И (AND); • - побитовая операция ИЛИ (OR)
value	Значение, с которым выполняется сравнение
offset	Смещение в поле данных пакета, с которого начинается операция сравнения
relative	Задает отсчет смещения от конца предыдущего найденного соответствия
endian	Задает порядок следования: • big - big endian (старший разряд слева, используется по умолчанию); • little - little endian (старший разряд справа)
string	Указывает, что данные в пакете представлены в символьном формате
number type	Задает тип считываемых значений: • hex – шестнадцатеричное число; • dec - десятичное число; • oct - восьмеричное число

Любой из операторов можно использовать со знаком инверсии (!). При использовании знака ! без оператора в качестве последнего принимается оператор равенства (=).

byte_jump

Опция byte_jump позволяет создавать простые правила считывания данных из пакетов с пропуском некоторого количества байтов, задаваемого значением поля в пакете. С помощью этой опции считывается размер части пакета, которую следует пропустить, и считываются данные, расположенные после этой части.

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: ,

[,relative] [,multiplier] [,big] [,little][,string]

[,hex] [,dec] [,oct] [,align] [,from_beginning];

Параметры опции byte_jump:

Параметр	Описание
bytes_to_convert	Число байтов, считываемых из пакета
offset	Смещение в поле данных пакета, с которого начинается обработка
relative	Задает использование смещения относительно конца предыдущего найденного соответствия
multiplier	Умножает количество вычисленных байтов на значение параметра <value> и пропускает полученное количество байтов
big	Обрабатывает данные как big endian (старший разряд сначала – используется по умолчанию)

Параметр	Описание
little	Обрабатывает данные как little endian (сначала младший разряд)
string	Данные в пакете представлены в виде текстовой строки
hex	Преобразовать строку данных в шестнадцатеричное значение
dec	Преобразовать строку данных в десятичное значение
oct	Преобразовать строку данных в восьмеричное значение
align	Округляет число конвертируемых байтов по следующей 32-битовой границе
from_beginning	Задает отсчет пропускаемых байтов от начала поля данных пакета, а не от текущей позиции в пакете

Опции проверки служебных полей пакетов (Non-payload)

fragoffset

Опция fragoffset позволяет сравнивать смещение фрагмента дейтаграммы IP с заданным десятичным значением. Для отсечения всех первых фрагментов можно использовать ключевое слово fragbits и просмотр опции More fragments при установке fragoffset: 0.

Формат:

fragoffset:[<|>]<целое число>

ttl

Ключевое слово ttl используется для проверки времени жизни дейтаграмм IP. Эта опция может быть полезна при детектировании попыток трассировки с помощью traceroute.

Формат:

ttl:[[<целое число>-]><=]<целое число>;

tos

Эта опция позволяет проверять в пакетах поле IP TOS (тип обслуживания).

Формат:

tos:[!]<целое число>;

id

Ключевое слово id используется для проверки наличия в поле IP ID заданного значения. Некоторые программы (эксплойты, сканеры, старые программы) устанавливают в этом поле определенное значение (например, число 31337 весьма популярно среди хакеров).

Формат:

id:<целое число>;

ipopts

Ключевое слово ipopts позволяет проверять наличие в заголовке IP указанных опций. Поддерживается проверка следующих опций IP:

rr - Record route (запись маршрута);

eol - End of list (завершение списка опций);

nop - No op (нет опции);

ts - Time Stamp (временная метка);

sec - IP security option (опция безопасности);

lsrr - Loose source routing (нежестко заданный отправителем маршрут);

ssrr - Strict source routing (жестко заданный отправителем маршрут);

satid - Stream identifier (идентификатор потока) (устаревшая опция);

any - any IP options are set (любые опции).

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

Формат:

ipopts:;

В правиле недопустимо наличие нескольких ключевых слов ipopts.

fragbits

Ключевое слово 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;

! - обращение (соответствует, если не установлен ни один из указанных битов).

Формат:

fragbits:[+*!]<[MDR]>

dsize

Ключевое слово dsize используется для проверки размера поля данных пакета. Данная опция позволяет детектировать пакеты аномальных размеров, которые достаточно часто применяются для переполнения буферов.

Формат:

dsize: [<>]<целое число>[<><целое число>];

Условие dsize не будет выполняться для пакетов перестроения потока (stream rebuilt packet), независимо от их размера.

flags

Ключевое слово flags используется для проверки наличия заданных флагов TCP. Список проверяемых флагов:

F - FIN (младший бит поля флагов TCP);

S - SYN;

R - RST;

P - PSH;

A - ACK;

U - URG;

1 - резервный бит 1 (старший бит байта TCP Flags);

2 - резервный бит 2;

0 - отсутствие флагов TCP.

Перечисленные ниже модификаторы позволяют менять поведение опции:

+ - соответствует, если установлены указанные биты;

* - соответствует, если установлен любой из указанных битов;

! - обращение (соответствует, если не установлен ни один из указанных битов).

Для создания правил обработки пакетов инициирования сессий (например, пакеты ECN, где установлены флаг SYN и резервные биты 1 и 2) можно задавать

маски опций. Маска отделяется от проверяемых флагов запятой. Например, для детектирования SYN-пакетов независимо от значений резервных битов можно задать маску S,12.

Формат:

flags:[!|*|+][,];

Для детектирования пакетов с флагами SYN и FIN независимо от значений резервных битов 1 и 2 может использоваться правило

alert tcp any any -> any any (flags:SF,12;)

flow

Опция flow используется вместе со сборкой потоков TCP и позволяет применять правило лишь к некоторым направлениям потока трафика. В результате можно создавать правила, которые будут относиться только к клиентам или только к серверам, что дает возможность легко дифференцировать пакеты, относящиеся к клиентам из $HOME_NET, просматривающим веб-страницы, от пакетов, относящихся к серверам, расположенным в $HOME_NET.

Ключевое слово established будет заменять опцию flags: A+, часто используемую применительно к уже организованным соединениям TCP.

Формат:

flow: [(established|stateless)]

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

[,(no_stream|only_stream)]

Параметры опции flow:

Параметр	Описание
to_client	Переключается на серверные отклики от A к B
to_server	Переключается на клиентские запросы от A к B
from_client	Переключается на клиентские запросы от A к B
from_ server	Переключается на серверные отклики от A к B
established	Переключается только на организованные соединения TCP
stateless	Переключается независимо от состояния обработчика потока (stream processor) и может быть полезно для детектирования пакетов, направленных на аварийное завершение работы системы
no_stream	Не переключается пакетами перестроения потока (полезно для опций dsize и stream4)
only_ stream	Переключается только пакетами перестроения потока

flowbits

Опция flowbits используется совместно со средствами отслеживания соединений препроцессора Flow. Это позволяет создавать правила для сеансов транспортного уровня. Опция flowbits наиболее полезна для сеансов TCP.

Для опции flowbits поддерживаются 7 ключевых слов. Большинство параметров требует указания определенного пользователем имени специфического состояния, которое будет проверяться. При создании таких имен следует ограничиваться буквами латиницы, цифрами, а также символами точки, дефиса и подчеркивания.

Формат:

flowbits: [set|unset|toggle|isset,reset,noalert][,];

Параметры опции flowbits:

Параметр	Описание
set	Устанавливает (определяет) указанное состояние для текущего потока данных
unset	Отменяет указанное состояние для текущего потока данных
toggle	Устанавливает указанное состояние, если оно еще не установлено, и отменяет установленное ранее
isset	Проверяет, установлено ли указанное состояние
isnotset	Проверяет, что указанное состояние не установлено
noalert	Отключает для правила генерацию сигнала независимо от остальных опций детектирования

seq

Опция seq служит для проверки значения порядковых номеров TCP.

Формат:

seq:<целое число>;

ack

Ключевое слово ack используется для проверки номеров подтверждений TCP.

Формат:

ack: <целое число>;

window

Ключевое слово window используется для проверки размера окна TCP.

Формат:

window:[!]<целое число>;

itype

Ключевое слово itype используется для проверки типа сообщения ICMP.

Формат:

itype:[<|>]<целое число>[<><целое число>];

icode

Ключевое слово icode используется для проверки значения кода ICMP.

Формат

icode: [<|>]<целое число>[<><целое число>];

icmp_id

Ключевое слово icmp_id служит для проверки значений идентификаторов ICMP. Такая проверка может оказаться полезной для обнаружения некоторых программ организации скрытых каналов, которые используют для передачи информации статические поля ICMP. Подключаемый модуль был создан, в частности, для детектирования DdoS-агентов stacheldraht.

Формат:

icmp_id:<целое число>;

icmp_seq

Ключевое слово icmp_seq используется для проверки порядковых номеров ICMP. Такая проверка может оказаться полезной для обнаружения некоторых программ организации скрытых каналов, которые используют для передачи инфор-

мации статические поля ICMP. Подключаемый модуль был создан, в частности, для детектирования DdoS-агентов stacheldraht.

Формат:

icmp_seq: <целое число>;

rpc

Ключевое слово 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>|*]>;

В силу особенностей машины поиска соответствий детектирование по ключевому слову rpc работает несколько медленнее, чем поиск значений RPC с использованием ключевого слова content.

ip_proto

Ключевое слово ip_proto позволяет проверять идентификатор протокола в заголовке IP. Список протоколов вы можете найти в файле /etc/protocols.

Формат:

ip_proto:[!><] <имя или номер протокола>;

sameip

Ключевое слово sameip позволяет детектировать пакеты с совпадающими адресами IP для получателя и отправителя.

Формат:

sameip;

Опции после детектирования

logto

Опция logto используется для записи всех пакетов, которые соответствуют правилу в специальный файл. Опция не будет работать, если программа обнаружения находится в режиме ведения бинарного журнала (binary logging mode).

Формат:

logto:"filename";

session

Ключевое слово session позволяет получить пользовательскую информацию из сеансов TCP.

Опция может использоваться с двумя аргументами – printable (выводить только печатаемые символы) и all (выводить все). Во втором случае непечатаемые символы выводятся в виде шестнадцатеричных кодов.

Формат:

session; [printable | all];

Использование опции session может существенно замедлять работу программы поиска. Эта опция очень удобна для обработки сохраненных файлов (формат pcap).

resp

Ключевое слово resp используется для попытки закрыть сессию при генерации сигнала.Такая реакция называется flexible response (гибкий отклик).

Параметры опции resp:

Параметр	Описание
rst_snd	Отправлять пакеты TCP-RST передающему сокету
rst_rcv	Отправлять пакеты TCP-RST принимающему сокету
rst_all	Отправлять пакеты TCP-RST в обоих направлениях
icmp_net	Передавать пакеты ICMP_NET_UNREACH отправителю
icmp_host	Передавать пакеты ICMP_HOST_UNREACH отправителю
icmp_port	Передавать пакеты ICMP_PORT_UNREACH отправителю
icmp_all	Передавать все перечисленные выше пакеты ICMP отправителю

Перечисленные в таблице опции можно комбинировать для передачи множества откликов одному хосту.

Формат:

resp: <resp_mechanism>[,<resp_mechanism>[,<resp_ mechanism>]];

Пользоваться этой опцией следует с осторожностью, так как можно достаточно легко создать бесконечный цикл.

react

Основным назначением этой опции является блокирование нежелательных сайтов. Код Flex Resp позволяет активно закрывать соединения и/или передавать в пользовательскую программу соответствующее сообщение. Для опции поддерживаются два основных модификатора:

- **block** – закрыть соединение и передать пользователю видимое уведомление;
- **warn** – передать пользователю видимое предупреждение.

Кроме основных модификаторов опция может использоваться с дополнительными параметрами:

- **msg** – включить заданный текст в передаваемое пользователю сообщение;
- **proxy:<номер порта>** – использовать порт proxy для передачи пользователю видимого предупреждения.

Дополнительные аргументы разделяются запятыми. Ключевое слово react должно использоваться последним в списке опций правила.

Формат:

react: <react_basic_modifier [, react_additional_modifier]>;

tag

Ключевое слово tag позволяет записывать в журнальные файлы не только пакет, который вызвал срабатывание правила. После срабатывания правила весь последующий трафик для данной пары "отправитель – получатель" будет помечаться, а отмеченный трафик можно проконтролировать для последующего анализа.

Формат:

tag: <type>, <count>, <metric>, [direction]

type

- **session** – записывать пакеты сессии, для которых сработало правило;
- **host** – записывать пакеты с хоста, который вызвал срабатывание правила (с учетом направления).

count – подсчитывать с использованием единиц, заданных параметром **<metric>**.

metric

- **packets** – пометить **<count>** пакетов для хоста/сессии;
- **seconds** – помечать пакеты для хоста/сессии в течение **<count>** секунд.

Параметры настройки ПАК "Соболь"

Для корректной работы СОВ необходимо проверить значения следующих параметров ПАК "Соболь", установленных по умолчанию:

Параметр	Значение	Примечание
Минимальная длина пароля	6	Установлено по умолчанию. Изменение недоступно
Использование случайных паролей	Да	Установлено по умолчанию. Изменение недоступно
Автономный режим работы	Нет	Установлено по умолчанию. Изменение недоступно
Время ожидания автоматического входа в систему	5–40	Доступно изменение в указанных пределах
Запрет загрузки с внешних носителей	Да	Установлено по умолчанию

Проверку значений параметров ПАК "Соболь" можно выполнить при установке ПО ДА (см. [**2**], "Установка ПО и инициализация сетевого устройства" и документ "Программно-аппаратный комплекс "Соболь". Версия 3.0. Руководство администратора", "Настройка общих параметров") или после установки до начала ввода ДА в эксплуатацию. Проверка параметров на работающем ДА выполняется в ходе перезагрузки.

Для проверки параметров ПАК "Соболь" после установки ПО ДА:

1. На работающем ДА нажмите на клавиатуре комбинацию клавиш <Alt>+<F2>.

   На экране появится главное локальное меню ДА.
2. Выберите пункт "Перезагрузка" и нажмите клавишу <Enter>.

   На экране появится запрос на перезагрузку.
3. Выберите "Да" и нажмите клавишу <Enter>.

   Начнется перезагрузка ДА и на экране появится основное окно ПАК "Соболь", в центре которого будет отображаться запрос персонального идентификатора.
4. Не дожидаясь автоматической загрузки сетевого устройства, аккуратно приложите персональный идентификатор администратора к считывателю.

   На экране появится запрос на ввод пароля администратора ПАК "Соболь".
5. Введите пароль и нажмите клавишу <Enter>.

   После успешного считывания пароля из идентификатора на экране появится окно с информацией о предъявленном идентификаторе.
6. Нажмите любую клавишу.

   На экране появится меню администратора.
7. Выберите в меню пункт "Общие параметры системы" и нажмите клавишу <Enter>.

   На экране появится окно настройки параметров ПАК "Соболь".
8. Проверьте значения параметров, приведенные в таблице выше. При необходимости измените значение параметра "Время ожидания автоматического входа в систему".
9. После просмотра параметров нажмите клавишу <Esc> для возврата в меню администратора.

10. Для завершения перезагрузки выберите в меню администратора пункт "Загрузка операционной системы" и нажмите клавишу <Enter>.

    Начнется проверка контроля целостности. Дождитесь сообщения о ее успешном завершении.

11. Нажмите клавишу <Enter>.

    Начнется загрузка операционной системы и после ее завершения на экране появится соответствующее сообщение.

12. Нажмите клавишу <Enter>.

    На экране появится главное локальное меню ДА.

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". Руководство администратора. Централизованное управление комплексом
2.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Локальное управление сетевыми устройствами
3.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Аудит
4.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Аутентификация пользователя
5.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Сервер доступа
6.	Аппаратно-программный комплекс шифрования "Континент". Руководство пользователя. Программа мониторинга КШ
7.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Тестирование каналов связи
8.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Обновление программного обеспечения
9.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Автоматизированное рабочее место генерации ключей
10.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Система обнаружения вторжений

Примечание. Набор документов, входящих в комплект поставки, может отличаться от указанного списка.