Код безопасности
ГК «Информзащита»

Средство криптографической защиты информации

Континент-АП
Версия 3.5

Руководство администратора
Межсетевой экран

УВАЛ. 00300-99 91



© Компания "Код Безопасности", 2010. 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:	**127018, г. Москва, ул. Сущевский вал, дом 47, стр. 2, помещение №1**
Телефон:	**(495) 980-23-45**
Факс:	**(495) 980-23-45**
e-mail:	**info@securitycode.ru**
Web:	**http://www.securitycode.ru**

Версия: 3.5 Последнее обновление: 14-05-10

Оглавление

Введение **4**

Назначение и основные функции МСЭ **4**

Принципы функционирования **5**

Списки правил фильтрации 5

Порядок обработки IP-пакетов 5

Контроль целостности установленного ПО 6

Установка, переустановка и удаление **6**

Требования к аппаратному и программному обеспечению 7

Установка МСЭ 7

Изменение, исправление и удаление ПО 9

Вызов мастера обслуживания 9

Доустановка МСЭ 9

Исправление установленного ПО 10

Удаление МСЭ 10

Запуск МСЭ **11**

Администрирование МСЭ **11**

Ввод пароля администратора 11

Изменение пароля администратора 12

Завершение сеанса работы администратора 12

Скрытие и отображение пиктограммы МСЭ 12

Обеспечение отказоустойчивости 13

Проверка контрольных сумм 13

Управление параметрами фильтрации **13**

Управление списками правил фильтрации 13

Настройка расписания 14

Настройка оповещений о срабатывании правил фильтрации 14

Настройка МСЭ для защищенной работы в составе АПКШ "Континент" 15

Журналы **15**

Журнал событий 15

Журнал прикладной фильтрации 16

Журнал пакетов 16

Приложение **18**

Язык правил фильтрации 18

Синтаксис правил фильтрации 18

Синтаксис правил прикладной фильтрации 18

Флаги правил фильтрации 19

Текст правил фильтрации 19

Примитивы фильтров 20

Логические выражения 23

Метасимволы в регулярных выражениях 24

Примеры правил фильтрации 24

Структура файла с расписаниями 27

Перечень файлов для контроля целостности 28

Документация **29**

Введение

Данное руководство предназначено для администраторов изделия "Средство криптографической защиты информации "Континент-АП" (далее — Абонентский пункт). В нем содержатся сведения, необходимые администратору для управления межсетевым экраном, входящим в состав Абонентского пункта, и контроля целостности установленного программного обеспечения.

Условные обозначения

В руководстве для выделения некоторых элементов текста (примечаний и ссылок) используется ряд условных обозначений.

Внутренние ссылки обычно содержат указание на номер страницы с нужными сведениями. Ссылки на другие документы или источники информации размещаются в тексте документа.

Важная и дополнительная информация оформлена в виде примечаний. Степень важности содержащихся в них сведений отображают пиктограммы на полях.



- Так обозначается дополнительная информация, которая может содержать примеры, ссылки на другие документы или другие части этого руководства.
- Такой пиктограммой выделяется важная информация, которую необходимо принять во внимание.
- Эта пиктограмма сопровождает информацию предостерегающего характера.

Исключения. Некоторые примечания могут и не сопровождаться пиктограммами. А на полях, помимо пиктограмм, могут быть приведены и другие графические элементы, например, изображения кнопок, действия с которыми упомянуты в тексте расположенного рядом абзаца.

Другие источники информации

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 и hotline@infosec.ru).

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно на курсах Учебного центра "Информзащита". Перечень курсов и условия обучения представлены на сайте http://www.itsecurity.ru/. Связаться с представителем учебного центра можно по электронной почте (edu@infosec.ru).

Назначение и основные функции МСЭ

В состав программного обеспечения Абонентского пункта входит межсетевой экран (далее — МСЭ), предназначенный для фильтрации IP-пакетов сетевого трафика компьютера, на котором установлен Абонентский пункт.

МСЭ обеспечивает фильтрацию входящих и исходящих IP-пакетов по следующим признакам:

- IP-адреса отправителя и получателя;
- тип прикладного протокола (POP3, HTTP, SMTP и т. д.);
- сетевой интерфейс, через который пакет был получен или будет отправлен;
- по полям заголовков и содержимому IP-пакетов.

Кроме того, IP-пакеты фильтруются:

- по типу транспортного протокола (TCP/UDP/ICMP/…);
- по портам TCP/UDP;
- по типам и кодам протокола ICMP.

Проверка входящих и исходящих IP-пакетов осуществляется по правилам фильтрации и в соответствии с заданным расписанием.

События, происходящие при фильтрации сетевого трафика, регистрируются в журнале событий и в журнале пакетов.

Принципы функционирования

Списки правил фильтрации

Межсетевой экран обрабатывает все входящие и исходящие IP-пакеты сетевого трафика. Порядок действий над IP-пакетами с заданными характеристиками определяется правилами фильтрации.

В МСЭ используются несколько списков правил фильтрации:

- правила фильтрации, которые действуют до авторизации пользователя в системе;
- правила фильтрации, которые действуют после авторизации пользователя в системе.

До авторизации пользователя действуют правила фильтрации, поставляемые с программным обеспечением МСЭ. Изменить эти правила нельзя.

Для фильтрации сетевого трафика после авторизации пользователя используются следующие списки:

- правила фильтрации (пакетный фильтр) — используются для фильтрации IP-пакетов по полям заголовков протокола TCP/IP;
- правила прикладной фильтрации — используются для фильтрации IP-пакетов по полям заголовков и по содержимому пакетов.

В правилах прикладной фильтрации используется механизм регулярных выражений.

Регулярные выражения — система синтаксического разбора текстовых фрагментов по формализованному шаблону, основанная на системе записи образцов для поиска.

С помощью этого механизма в правилах прикладной фильтрации задается дополнительный признак, на основании которого определяется необходимость применения данных правил к IP-пакетам. Таким признаком является наличие в поле данных IP-пакета определенной последовательности символов.

Например, для протокола TFTP атрибутами могут быть коды выполняемых операций (запрос на запись или на чтение). Чтобы предотвратить несанкционированную передачу данных по протоколу TFTP, необходимо составить правило фильтрации, запрещающее передачу пакетов (на порт #69), и задать дополнительный признак — наличие в передаваемых пакетах запросов на запись или на чтение.

Другим примером атрибута или информационного объекта является наличие команд сервера в поле данных IP-пакета для протоколов HTTP (GET, POST и т. д.). В этом случае для запрета передачи или отправки данных к правилу фильтрации необходимо добавить регулярное выражение, содержащее в явном виде наименование команды. Также в качестве информационного объекта может быть указан фрагмент текста, на основании которого можно сделать вывод о передаче той или иной информации.

Файлы с правилами фильтрации и правилами прикладной фильтрации состоят из последовательных записей правил, по одному правилу на каждой строке. Описание языка правил фильтрации см. в Приложении на стр. 18. Примеры правил фильтрации представлены в Приложении на стр. 24.

Каждый входящий и исходящий IP-пакет проверяется на соответствие правилам фильтрации, начиная с первого правила в списке. Проверка производится до тех пор, пока не будет найдено правило, удовлетворяющее данному пакету. В этом случае будут выполнены соответствующие действия, и проверка пакета будет прекращена.

Период работы правил фильтрации определяется расписанием. Для управления параметрами фильтрации необходимо ввести пароль администратора.

Порядок обработки IP-пакетов

Входящие IP-пакеты сетевого трафика первоначально проверяются на соответствие правилам фильтрации, а затем, если пакет пропущен, — на соответствие правилам прикладной фильтрации.

Исходящие IP-пакеты первоначально проверяются на соответствие правилам прикладной фильтрации, а затем, если пакет пропущен, — на соответствие правилам фильтрации.

При совпадении характеристик входящего IP-пакета с их описанием в правиле фильтрации осуществляется предусмотренное правилом действие и дальнейшая проверка этого пакета на соответствие оставшимся правилам не выполняется.

Все IP-пакеты сетевого трафика, не попавшие под действие ни одного из правил фильтрации, отбрасываются фильтром. Все IP-пакеты сетевого трафика, не попавшие под действие ни одного из правил прикладной фильтрации, пропускаются фильтром.

При пустом списке правил фильтрации все IP-пакеты отбрасываются фильтром. При пустом списке прикладных правил фильтрации все IP-пакеты пропускаются.

После установки программного обеспечения МСЭ на компьютер в правилах фильтрации и правилах прикладной фильтрации по умолчанию содержится единственное правило, разрешающее прохождение через МСЭ любых IP-пакетов.

Контроль целостности установленного ПО

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

Для расчета и проверки контрольных сумм используется модуль cpverify.exe из программного продукта КриптоПро CSP.

Эталонные значения рассчитываются при установке или обновлении программного обеспечения Абонентского пункта. Контролю подлежат все служебные файлы Абонентского пункта (см. стр. 28), размещенные в каталоге установки и системных папках ОС Windows.

Рассчитанные при установке программного обеспечения контрольные суммы содержатся в файле check.xml, перечень контролируемых файлов и полные пути к ним — в файле cpverify.xml из каталога установки.

Проверка контрольных сумм выполняется в следующих случаях:

- автоматически при запуске операционной системы;
- автоматически при попытке соединения с сервером доступа;
- вручную по команде оператора.

Результаты проверки заносятся в журнал приложений ОС Windows. При отрицательном результате автоматической проверки на экран выводится сообщение "Нарушена целостность файлов Абонентского Пункта. Обратитесь к системному администратору".

При отрицательном результате проверки соединение абонентского пункта с сервером доступа установлено не будет.

При проверке контрольных сумм выполняется также проверка на наличие программного продукта КриптоПро CSP версии не ниже 3.0. В случае отрицательного результата проверки (например, при деинсталляции КриптоПро CSP) файл check.xml будет автоматически удален из каталога установки. Для восстановления этого файла необходимо либо переустановить Абонентский пункт (см. [9]), либо последовательно выполнить процедуры исправления МСЭ (см. стр. 10) и перерасчета контрольных сумм.

Установка, переустановка и удаление

Программное обеспечение МСЭ поставляется на компакт-дисках и входит в комплект поставки Абонентского пункта. В комплект также входит программный продукт компании "Крипто-Про" КриптоПро CSP.

Перед установкой МСЭ убедитесь, что компьютер удовлетворяет всем требованиям, предъявляемым к аппаратному и программному обеспечению.

Требования к аппаратному и программному обеспечению

МСЭ предназначен для использования на компьютерах, оснащенных процессорами семейства Intel X86 или совместимыми с ними. Требования к конфигурации компьютеров приведены в таблице ниже.

Элемент	Минимально	Рекомендуется
Процессор	Celeron 300 МГц	Pentium IV 1,8 ГГц
Оперативная память	128 Мб	512 Мб
Жесткий диск (свободное пространство)	512 Мб	512 Мб
Операционная система	Windows 2000 32 bit SP4, Update RollUp 1 for Windows 2000 SP4 (KB891861), MS04-011 (KB835732); или Windows XP 32 bit SP3; или Windows Vista 32 bit SP2	
Установленное ПО	КриптоПро CSP версии 3.0.3293 и выше для Windows 2000 Professional и Windows XP Professional, КриптоПро CSP версии 3.6 для Windows Vista, MS Internet Explorer версии 6.0 или выше, СЗИ Secret Net 5.0	

На компьютере должны быть установлены компоненты операционной системы, обеспечивающие работу с сетевыми протоколами TCP/IP.

Внимание! Все службы, реализующие штатные механизмы удаленного управления операционной системой должны быть отключены.

Процедуры установки и настройки программных продуктов КриптоПро CSP и СЗИ Secret Net 5.0 подробно рассматриваются в эксплуатационной документации на данные программные продукты.

Установка МСЭ

Установка МСЭ может производиться либо одновременно с установкой Абонентского пункта (см. ниже), либо позже, после установки программного обеспечения Абонентского пункта на компьютер (см. стр. 9). Установка МСЭ без Абонентского пункта невозможна.

После установки Абонентского пункта все работающие сетевые подключения будут автоматически разорваны. Для их восстановления необходима перезагрузка компьютера.

Для установки МСЭ совместно с Абонентским пунктом:

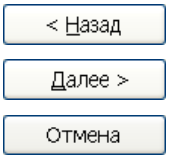
1. Войдите в систему с правами администратора компьютера.

   Правами администратора компьютера обладает пользователь, входящий в локальную группу администраторов.

2. Завершите работу всех приложений, выполняющихся на компьютере.
3. Поместите установочный диск в устройство чтения компакт-дисков и запустите на исполнение файл Setup.exe, находящийся в каталоге с дистрибутивом Абонентского пункта, путь к которому указан в документе Release Notes.

   Для установки с жесткого диска скопируйте файлы с установочного диска в любой рабочий каталог (локальный или сетевой) и запустите на исполнение файл Setup.exe.

   Программа установки начнет выполнение подготовительных действий, и на экране появится сообщение об этом. После завершения подготовительных действий на экран будет выведен стартовый диалог мастера установки.



Совет. Для управления процессом установки используйте кнопки:

- "Назад" — для возврата к предыдущему диалогу;
- "Далее" — для перехода к следующему диалогу;
- "Отмена" — для прекращения процесса установки. После нажатия этой кнопки подтвердите свое решение в появившемся окне запроса.

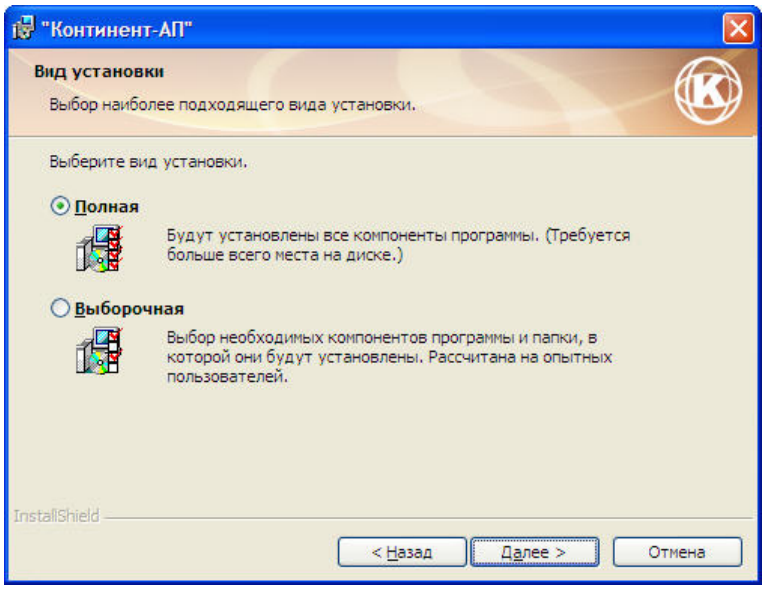
4. Нажмите кнопку "Далее >" для продолжения установки. На экране появится диалог, содержащий лицензионное соглашение на использование программного продукта.
5. Прочтите лицензионное соглашение и, если вы принимаете его условия, поставьте отметку в поле "Я принимаю условия лицензионного соглашения" и нажмите кнопку "Далее >".

Внимание! Если вы не согласны с условиями лицензионного соглашения, поставьте отметку в поле "Я не принимаю условия лицензионного соглашения" и нажмите кнопку "Отмена". Установка Абонентского пункта будет прекращена.

На экране появится диалог выбора папки для размещения компонентов программы. По умолчанию программа установки копирует файлы в каталог \ Program Files \ SecurityCode \ ClientContinent.

Для установки программы в другую папку нажмите кнопку "Изменить..." и укажите нужную папку в диалоге, появившемся на экране.

6. Нажмите кнопку "Далее >". На экране появится диалог для выбора вида установки.



По умолчанию выбрана полная установка, т. е. установка Абонентского пункта совместно с МСЭ.

7. Нажмите кнопку "Далее >". На экране появится диалог для ввода IP-адреса сервера доступа.

IP-адрес сервера доступа необходим для работы Абонентского пункта. Если предполагается использование Абонентского пункта, то введите нужное значение IP-адреса.

8. Нажмите кнопку "Далее >". На экране появится диалог с информацией о том, что программа готова приступить к установке.
9. Проверьте правильность значений, введенных в предыдущих диалогах, и нажмите кнопку "Установить" для начала установки. Программа установки приступит к копированию файлов в указанную папку.

В процессе установки на экране будут появляться сообщения о том, что устанавливаемое программное обеспечение не тестировалось на совместимость с операционной системой. В окне таких сообщений следует нажимать кнопку "Все равно продолжить".

Сообщения, появляющиеся на экране, отображают этапы процесса установки.

Если по какой-то причине отсутствует какой-либо из файлов, входящих в комплект поставки, на экране появится предупреждающее сообщение с указанием имени отсутствующего файла. В этом случае проверьте компьютер на наличие вирусов и повторите установку. Если в дальнейшем данная ошибка будет повторяться, обратитесь к поставщику комплекса.

По окончании процесса копирования на экране появится заключительное окно мастера установки.

10. Нажмите кнопку "Готово".

На экране появится запрос на перезагрузку компьютера. Выберите вариант завершения установки:

- для немедленной перезагрузки компьютера и начала работы МСЭ нажмите кнопку "Да";
- для продолжения работы без перезагрузки компьютера нажмите кнопку "Нет". В этом случае работа с МСЭ будет возможна только после окончания сеанса работы и перезагрузки компьютера.

Если до установки МСЭ были установлены какие-либо сетевые подключения, они будут разорваны, а на экране появится соответствующее сообщение. Восстановление сетевых подключений будет возможно только после перезагрузки компьютера.

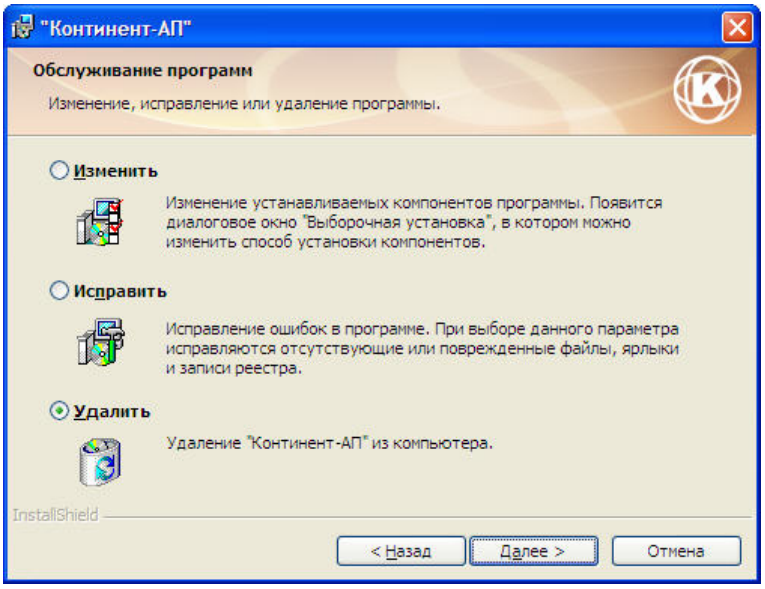
Изменение, исправление и удаление ПО

Вызов мастера обслуживания

Управление программным обеспечением МСЭ выполняют с помощью мастера обслуживания программы.

Для вызова диалога обслуживания программы:

1. Нажмите кнопку "Пуск" и в главном меню Windows найдите и активируйте команду "Панель управления".
2. В окне "Панель управления" активируйте элемент "Установка и удаление программ".
3. Выберите в списке установленных программ элемент "Континент-АП" и нажмите кнопку "Изменить". После выполнения подготовительных действий на экране появится стартовое окно мастера удаления.
4. Нажмите кнопку "Далее >". На экране появится диалог обслуживания программы:



Доустановка МСЭ

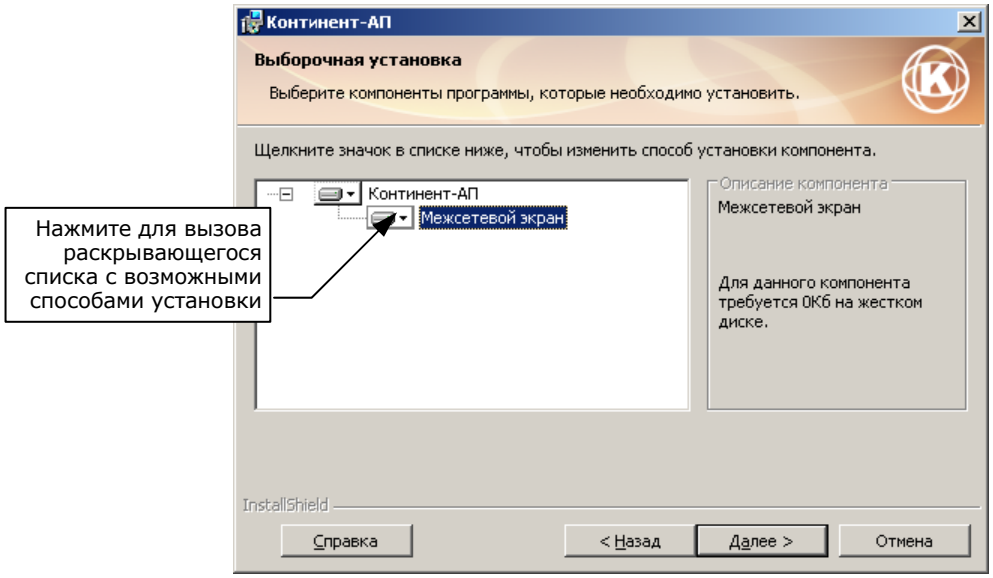
Доустановка МСЭ выполняется в том случае, если при первоначальной установке было установлено ПО Абонентского пункта без МСЭ. В этом случае программное обеспечение МСЭ можно доустановить.

Внимание! Перед тем как приступить к доустановке МСЭ, вставьте установочный диск в устройство чтения компакт-дисков.

Для доустановки МСЭ:

1. Вызовите на экран диалог обслуживания программы (см. выше).

2. Выберите действие "Изменить" и нажмите кнопку "Далее >". На экране появится диалог выборочной установки:



3. Перейдите к выполнению п. **7** процедуры установки МСЭ (см. стр. 8).

Исправление установленного ПО

Исправление МСЭ выявляет и исправляет поврежденные файлы, ошибки в реестре и т. д.

Для исправления МСЭ:

1. Вызовите на экран диалог обслуживания программы (см. стр. 9).
2. Выберите действие "Исправить" и нажмите кнопку "Далее >".
3. Перейдите к выполнению п. **7** процедуры установки МСЭ (см. стр. 8).

Удаление МСЭ

Удаление МСЭ может быть выполнено:

- отдельно от Абонентского пункта (МСЭ будет удален, Абонентский пункт не будет удален);
- вместе с Абонентским пунктом.

Для удаления МСЭ:

1. Вызовите на экран диалог обслуживания программы (см. стр. 9).
2. Выберите действие "Изменить" и нажмите кнопку "Далее >". На экране появится диалог выборочной установки (см. рис. выше).

   Вызовите раскрывающийся список с возможными способами установки для компонента "Межсетевой экран". Выберите в нем вариант "Данный компонент будет недоступен".



Пиктограмма возле компонента "Межсетевой экран" будет отмечена красным крестом.

3. Нажмите кнопку "Далее >".
4. Перейдите к выполнению п. **7** процедуры установки МСЭ (см. стр. 8).

Для удаления МСЭ и Абонентского пункта:

1. Вызовите на экран диалог обслуживания программы (см. стр. 9).
2. Выберите действие "Удалить" и нажмите кнопку "Далее >".

   На экране появится диалог для подтверждения удаления. По умолчанию в поле "Удалить также все соединения, использующие виртуальный адаптер Континент" установлена отметка. Это означает, что одновременно с удалением программы будут удалены все соединения, использующие виртуальный адаптер Continent 3 PPP Adapter. Для того чтобы после удаления

Абонентского пункта такие соединения сохранились, удалите отметку в этом поле.

3. Нажмите кнопку "Удалить".

   Программа удаления приступит к удалению файлов. По завершении процесса удаления на экране появится сообщение о необходимости перезагрузки компьютера.

4. Выберите вариант завершения удаления:
   - нажмите кнопку "Да" для немедленной перезагрузки компьютера;
   - нажмите кнопку "Нет", чтобы продолжить работу без перезагрузки компьютера.

Запуск МСЭ

МСЭ начинает свою работу автоматически, сразу же после перезагрузки компьютера, а в дальнейшем — при каждом входе в систему.

Администрирование МСЭ



Пиктограммы МСЭ

После запуска МСЭ в системной области панели задач Windows появится пиктограмма МСЭ.

Примечание. В случае ошибок запуска сервиса пиктограмма МСЭ изменит свой вид.

Контекстное меню пиктограммы содержит команды для настройки параметров:

Пункт меню	Назначение
Изменить расписание	Формирование расписания работы правил фильтрации
Изменить правила фильтрации	Формирование правил фильтрации, действующих после идентификации пользователя на компьютере
Изменить правила прикладной фильтрации	Формирование правил прикладной фильтрации IP-пакетов
Просмотреть правила фильтрации до авторизации	Просмотр правил фильтрации, действующих до входа пользователя в систему
Включить оповещение	Включение сигнализации на срабатывание правил фильтрации
Изменить пароль администратора	Изменение пароля администратора
Ввести пароль администратора/ Завершить сеанс работы администратора	Вход в программу с правами администратора, чтобы иметь возможность менять настройки. После выхода из режима администратора такая возможность пропадает
Журналы	Вызов на экран выбранного в подменю регистрационного журнала
Справка	Вызов справки МСЭ
О программе	Просмотр информации об установленной на компьютере версии программного обеспечения МСЭ
Выход	Завершение работы пользовательского интерфейса МСЭ

Так как настройку параметров МСЭ может выполнить лишь пользователь, наделенный правами администратора, часть команд контекстного меню доступна для активации только после ввода пароля администратора (см. ниже).

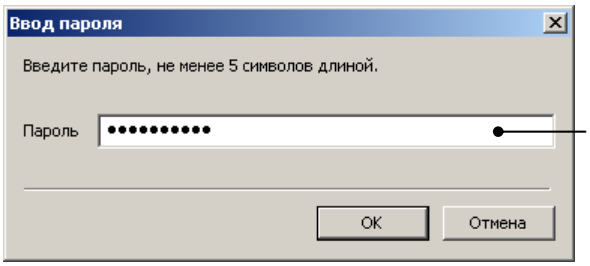
Ввод пароля администратора

Для администрирования МСЭ необходимо ввести пароль, подтверждающий полномочия пользователя на выполнение операций.

Для ввода пароля администратора:

1. Активируйте в контекстном меню пиктограммы МСЭ команду "Ввести пароль администратора".

На экране появится диалог для ввода пароля.



По умолчанию пароль администратора МСЭ имеет значение "111111"

2. Введите пароль и нажмите кнопку "ОК".

   Если пароль введен правильно, станут доступными все команды контекстного меню, иначе на экране появится сообщение об ошибке. Нажмите кнопку "ОК" и повторно введите пароль, указав его правильно.

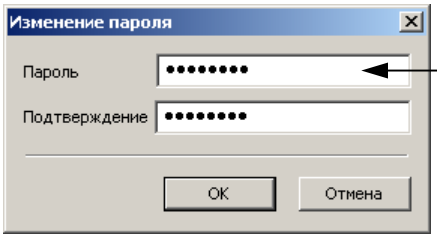
Изменение пароля администратора

После установки программного обеспечения пароль пользователя — администратора МСЭ имеет значение "111111". В дальнейшем этот пароль необходимо изменить.

Для изменения пароля администратора:

1. Введите пароль администратора МСЭ (см. стр. 11).
2. Активируйте в контекстном меню пиктограммы МСЭ команду "Изменить пароль администратора".

   На экране появится диалог для ввода пароля.



Длина пароля должна быть не менее 5 символов

3. Заполните поля диалога и нажмите кнопку "ОК":
   - в поле "Пароль" введите новый пароль;
   - в поле "Подтверждение" укажите тот же пароль еще раз.

   Для администратора МСЭ будет установлен новый пароль.

Завершение сеанса работы администратора

Для завершения сеанса:

- Активируйте в контекстном меню пиктограммы МСЭ команду "Завершить сеанс работы администратора".

  Сеанс работы администратора будет завершен и часть команд контекстного меню пиктограммы МСЭ станет недоступной для активации.

Скрытие и отображение пиктограммы МСЭ

Пользовательский интерфейс МСЭ может быть выгружен из памяти компьютера. При этом все сервисы МСЭ будут работать в штатном режиме, за исключением сервиса оповещения.

Внимание! При выгруженном пользовательском интерфейсе оповещения о срабатывании правил фильтрации на экран не выводятся.

Для скрытия пиктограммы МСЭ:

- Активируйте в контекстном меню пиктограммы МСЭ команду "Выход".

  Пиктограмма МСЭ будет удалена из системной области панели задач Windows.

Для отображения пиктограммы МСЭ:

- Для отображения пиктограммы МСЭ выполните одно из действий:
  - перезагрузите компьютер;
  - активируйте в меню Windows команду "Пуск > Программы > Код Безопасности > Абонентский Пункт Континент > Программа управления";
  - запустите на исполнение файл mseGui.exe из каталога установки программного обеспечения МСЭ. Каталог установки по умолчанию: "C:\Program Files\SecurityCode\ClientContinent".

Обеспечение отказоустойчивости

Правила фильтрации сетевого трафика содержатся в файле USRRules.txt, список правил прикладной фильтрации — в файле APPFilterRules.txt, расписание — в файле Schedules.txt. Для обеспечения отказоустойчивости МСЭ рекомендуется каждый раз после редактирования правил фильтрации, правил прикладной фильтрации и расписания копировать эти файлы на сетевой или отчуждаемый носитель.

Файлы USRRules.txt, APPFilterRules.txt и Schedules.txt находятся в каталоге установки программного обеспечения Абонентского пункта.

В дальнейшем это позволит быстро восстановить работу МСЭ с актуальными правилами фильтрации и расписанием.

Проверка контрольных сумм

Проверка контрольных сумм выполняется в следующих случаях:

- автоматически при запуске операционной системы;
- автоматически при попытке соединения с сервером доступа;
- вручную по команде оператора.

Для проверки контрольных сумм вручную:

- Активируйте в меню Windows команду "Пуск > Программы > Код Безопасности > Абонентский Пункт Континент > Проверка контрольных сумм".

По окончании выполнения процедуры проверки на экране появится информационное окно, в котором будет представлен отчет о результатах проверки.

В отчете содержится информация о количестве проверенных файлов и сведения о каждом из них:

- наименование и полный путь к файлу;
- результат проверки:
  - ok — результат проверки положительный;
  - Not found — файл не найден;
  - Has incorrect hash — содержимое файла изменено.

Управление параметрами фильтрации

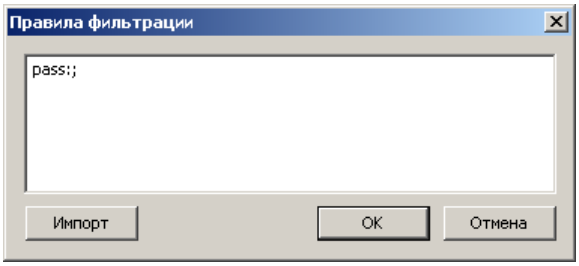
Управление списками правил фильтрации

Для управления списком:

1. Активируйте в контекстном меню пиктограммы МСЭ нужную команду:

Просмотреть правила фильтрации до авторизации	для просмотра списка правил фильтрации, действующих до авторизации
Изменить правила фильтрации	для редактирования списка правил фильтрации, действующих после авторизации
Изменить правила прикладной фильтрации	для редактирования списка правил прикладной фильтрации

   На экране появится указанный список правил.



2. Отредактируйте список правил, удалив ненужные правила или создав новые. Описание языка правил фильтрации представлено в Приложении на стр. 18.
3. Если требуется загрузить созданный ранее набор правил, нажмите кнопку "Импорт".

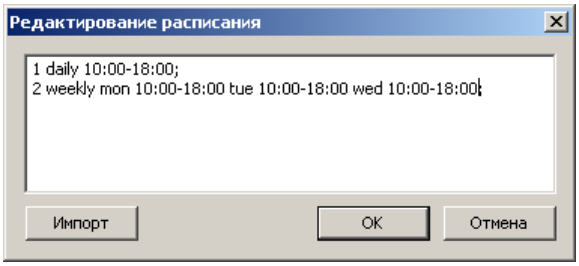
   На экране появится типовой диалог для открытия файлов. Выберите нужный файл. Содержимое файла отобразится в диалоге для редактирования правил фильтрации.
4. Для применения новых правил нажмите кнопку "ОК".

Настройка расписания

Для настройки расписания:

1. Активируйте в контекстном меню пиктограммы МСЭ команду "Изменить расписание".

   На экране появится диалоговое окно с расписанием.



2. Отредактируйте расписание, удалив ненужные строки или добавив новые. Структура файла с расписаниями представлена в Приложении на стр. 27.
3. Если требуется загрузить созданное ранее расписание, нажмите кнопку "Импорт".

   На экране появится типовой диалог для открытия файлов. Выберите нужный файл. Содержимое файла отобразится в диалоговом окне.
4. Для применения расписания нажмите кнопку "ОК".

Настройка оповещений о срабатывании правил фильтрации

Средства МСЭ позволяют оповещать пользователя о срабатывании правил фильтрации.

Для настройки оповещений необходимо:

- в списке правил фильтрации установить флаг alert для тех правил фильтрации, о срабатывании которых требуется оповещать пользователя (см. стр. 18);
- включить режим оповещения.

Для включения режима оповещения:

- Отметьте в контекстном меню пиктограммы МСЭ команду "Включить оповещение".

Для отмены оповещений — снимите отметку.

Настройка МСЭ для защищенной работы в составе АПКШ "Континент"

Для защищенной работы в составе АПКШ "Континент" в МСЭ необходимо установить список правил фильтрации, пропускающий протокол ARP, а также весь трафик на адрес сервера доступа, к которому он будет подключаться. В случае использования на АП DHCP, следует также разрешить протокол DHCP. Для доступа к ресурсам в незащищенной сети можно разрешить установку исходящих соединений на эти ресурсы. Рекомендуется запретить входящие соединения с незащищенных ресурсов.

Например, для АП, работающего с сервером доступа с IP-адресом 10.2.0.77 и использующего DHCP, список правил может выглядеть следующим образом:

pass:arp;

pass:host 10.2.0.77;

pass:src port 67 or src port 68 or dst port 67 or dst port 68;

in:tcp[13] == 2;

pass:tcp;

МСЭ автоматически пропускает весь трафик, проходящий через адаптер Континент-АП, поэтому будет разрешен доступ с этого АП на ресурсы защищенной и незащищенной сетей, разрешен доступ к этому АП из защищенной сети, но запрещен доступ к этому АП из незащищенных сетей.

Журналы

Для записи событий, имеющих отношение к фильтрации сетевого трафика, используются журналы:

- журнал событий Windows — для хранения записей о событиях, относящихся к фильтрации IP-пакетов, а также записей о срабатывании правил фильтрации. Журнал доступен для просмотра в Windows-приложении "Просмотр событий";
- журнал прикладной фильтрации — для хранения записей о соединениях;
- журнал пакетов — для хранения записей о событиях, происходящих с IP-пакетами.

Сведения о событиях сохраняются в виде записей, содержащих подробную информацию о событии.

Журнал событий

Об управлении журналом событий смотрите соответствующий раздел документации для используемой операционной системы.

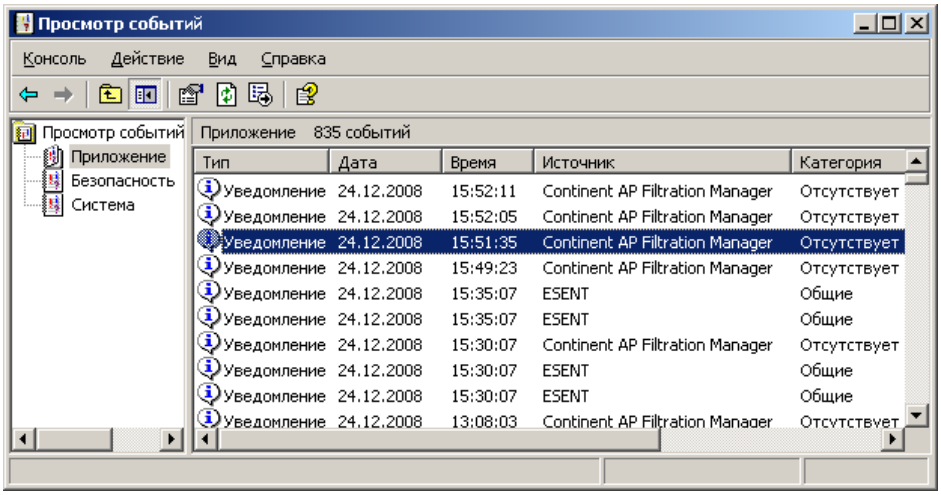
Для просмотра информации о событии:

1. Выполните одно из действий:
   - активируйте в контекстном меню пиктограммы МСЭ команду "Журналы | Журнал событий"
   - вызовите контекстное меню пиктограммы Абонентского пункта, расположенной на панели задач Windows, и активируйте команду "Журнал").

   Пиктограмма Абонентского пункта

   На экране появится окно журнала событий.
2. Перейдите к папке "Приложение".

   Справа отобразится содержимое выбранной папки:



У событий, относящихся к фильтрации трафика МСЭ, в столбце "Источник" содержится значение "Continent AP Filtration Manager".

3. Выберите нужную запись.
4. В контекстном меню выбранной записи активируйте команду "Свойства".

   На экране появится окно, в котором содержится информация о событии.

События запуска процессов регистрируются в журнале событий и имеют номер события равный 85.

Журнал прикладной фильтрации

Журнал прикладной фильтрации хранится в файле App_log.txt из каталога установки.

По результатам фильтрации сетевого трафика в журнале пакетов регистрируется следующая информация о соединении:

- совершенное действие (пропущено/блокировано и т. п.);
- дата и время регистрации события;
- IP-адреса локального и удаленного компьютеров;
- наименование сетевого протокола;
- номера портов локального и удаленного компьютеров.

Для просмотра журнала:

- Выполните одно из действий:
  - активируйте в контекстном меню пиктограммы МСЭ команду "Журналы | Журнал прикладной фильтрации";
  - откройте файл App_log.txt с помощью приложения, работающего с файлами CSV-формата (например, MS Office Excel).

  На экране появится окно журнала прикладной фильтрации.

Журнал пакетов

Журнал пакетов хранится в файле ip_log.txt из каталога установки. При достижении файлом размера 800 кб он переименовывается в IP_log.tx1, а на его месте создается новый, пустой.

В журнале фиксируются только те пакеты, в правилах для которых имеется флаг log. Регистрируется следующая информация:

- совершенное действие над IP-пакетом (пропущен/блокирован и т. п.);
- дата и время регистрации события;
- размер IP-пакета;
- номер Ethernet-протокола;
- IP-адреса отправителя и получателя IP-пакета;

- наименование сетевого протокола;
- номера портов отправителя и получателя IP-пакета;
- направление пакета (входящий, исходящий).

Для просмотра журнала:

- Выполните одно из действий:
  - активируйте в контекстном меню пиктограммы МСЭ команду "Журналы | Журнал пакетов";
  - откройте файл ip_log.txt с помощью приложения, работающего с файлами CSV-формата (например, MS Office Excel).

  На экране появится окно журнала пакетов.

Приложение

Язык правил фильтрации

Синтаксис правил фильтрации

Правила фильтрации IP-пакетов имеют следующую структуру:

[pass] [in] [out] [log] [iface=<наименование соединения>]:[<текст правила>];

где:

- перед символом ":" указывают флаги, описывающие применение правила (см. стр. 19).

  Если указаны два флага — in и out или не указан ни один из них, правило применяется как к входящим, так и к исходящим IP-пакетам.

- между символами ":" и ";" содержится собственно текст правила (см. стр. 19).

Флаги, символы ":" и ";" могут разделяться любым количеством символов табуляции, пробелов и переносов строки.

Синтаксис правил прикладной фильтрации

Правила прикладной фильтрации имеют формат:

[pass] [in] [out] [log]:[<текст правила>]:[<регулярное выражение>];

где:

- в заголовке допустимы следующие флаги: **pass**, **in**, **out**, **log** (см. стр. 19);
- в тексте правила допустимы следующие примитивы: **tcp**, **udp**, **src port <port>**, **dst port <port>**, **src host <host>**, **dst host <host>**, **outbuf <size>**, **inbuf <size>** (см. стр. 20).

  Если указано не пустое регулярное выражение, в правиле должен быть указан параметр outbuf, inbuf или оба.

- регулярное выражение, если оно указано, должно соответствовать правилам синтаксиса regex (источник FreeBSD Man Pages). Дополнительно в регулярном выражении можно указывать числовые коды в шестнадцатеричном формате в виде "\xFF". Перечень метасимволов, используемых в регулярных выражениях см. ниже на стр. 24).

  Для правил, принадлежащих одному диапазону IP-адресов, допустимо только одно регулярное выражение.

Флаги и параметры должны быть разделены пробелами, каждое правило должно заканчиваться символом ";" (точка с запятой).

Пример правила прикладной фильтрации:

pass:tcp dst port 80 dst host 192.168.1.40 outbuf 100:google.com\x00;

Флаги правил фильтрации

Флаг	Описание
pass	пакет, удовлетворяющий данному правилу, пропускается. Если данный флаг не указан — IP-пакет отбрасывается
in	правило применяется только к входящим IP-пакетам
out	правило применяется только к исходящим IP-пакетам
log	IP-пакет, удовлетворяющий данному правилу, записывается в файл IP_log.txt из каталога установки
iface	правило применяется только к IP-пакетам, проходящим через указанное соединение. Наименование соединения должно быть идентичным наименованию, под которым оно указано в меню "Пуск > Настройка > Сетевые подключения". Если наименование соединения содержит пробелы, оно должно указываться в кавычках (например: "Local Area Connection 2")
alert	уведомление пользователя об обработке IP-пакета правилом с таким флагом **Примечания.** В правила фильтрации, в которых используется флаг alert, автоматически добавляется флаг log. При постоянном применении флага alert ко всем IP-пакетам происходит быстрое заполнение журнала событий. В связи с этим рекомендуется выборочное применение данного флага к правилам фильтрации.
sched	правило действует по расписанию. После знака равно указывается идентификатор расписания. Например, sched = 1 означает, что правило будет работать только в период времени, указанный в расписании с идентификатором 1

Текст правил фильтрации

Каждое выражение, задающее фильтр, включает один или несколько примитивов, состоящих обычно из одного или нескольких идентификаторов объекта и предшествующих ему классификаторов. Идентификатором объекта может служить его имя или номер. Классификаторы объектов могут относиться к одному из трех видов:

type
указывает тип объекта, заданного идентификатором. В качестве типа объектов могут указываться значения host (хост), net (сеть) и port (порт). Если тип объекта не указан, предполагается значение host.

dir
задает направление по отношению к объекту. Для этого классификатора поддерживаются значения src (объект является отправителем), dst (объект является получателем), src or dst (отправитель или получатель) и src and dst (отправитель и получатель). Например, src foo указывает на пакеты, отправленные с хоста foo, dst net 128.3 - пакеты, адресованные в сеть 128.3.0.0/16, а src or dst port ftp-data – пакеты данных протокола FTP (порт ftp-data), передаваемые в обоих направлениях. Если классификатор dir не задан, предполагается значение src or dst. Для некоторых типов соединений (например, SLIP) и режимов захвата (например, захват с фиктивного интерфейса any в Linux-системах) могут использоваться классификаторы inbound и outbound.

proto
задает протокол, к которому должны относиться пакеты. Этот классификатор может принимать значения ether, tr, wlan, ip, arp, rarp, decnet, tcp и udp. Если примитив не содержит классификатора протокола, предполагается, что данному фильтру удовлетворяют все протоколы, совместимые с типом объекта.

Кроме объектов и классификаторов примитивы могут содержать ключевые слова gateway (шлюз), broadcast (широковещательный), less (меньше), greater (больше) и арифметические выражения.

Сложные фильтры могут содержать множество примитивов, связанных между собой с использованием логических операторов and, or и not (например, host foo and not port ftp and not port ftp-data). Для сокращения задающих фильтры выражений можно опускать идентичные списки классификаторов. Например, выражение tcp dst port ftp or ftp-data or domain будет краткой формой выражения

tcp dst port ftp or tcp dst port ftp-data or tcp dst port domain

Примитивы фильтров

Примитив	Описание
dst host <хост>	будет отбирать пакеты, в которых поле адреса получателя IPv4 содержит адрес хоста, заданного в примитиве
src host <хост>	будет выбирать все пакеты, в которых поле отправителя содержит адрес указанного хоста
host <хост>	будет отбирать все пакеты, для которых адрес хоста указан в поле получателя или отправителя. Все три приведенных выше выражения могут содержать идентификаторы протоколов ip, arp или rarp, как в выражении ip host <хост> эквивалентном фильтру: ether proto ip and host <хост> Если именем задан хост, с которым связано несколько адресов IP, фильтру будут соответствовать пакеты с любым из этих адресов в заголовках пакетов
ether src<ehost>	будет выбирать все кадры, в которых поле MAC-адреса отправителя содержит значение ehost
ether host<ehost>	будет отбирать все пакеты с адресом, указанным значением ehost в поле отправителя или получателя
gateway <шлюз>	будет отбирать все пакеты, использующие указанный именем хост в качестве шлюза. Указанное параметром имя хоста должно преобразовываться в IP-адрес механизмами преобразования имен, доступными локальному компьютеру (файл /etc/hosts, DNS, NIS и т. п.), а также механизмами определения MAC-адреса по имени хоста (/etc/ethers и т. п.). Эквивалентное выражение ether host ehost and not host <хост> позволяет указывать хост по имени или адресу, указанному в файле host/ehost
dst net <сеть>	отбирает все пакеты IPv4, направленные в указанную сеть. Для указания сети можно использовать имя из файла /etc/networks или номер сети
src net <сеть>	выбирает все пакеты IPv4, отправленные из указанной сети
net <сеть>	выбирает все пакеты IPv4, содержащие адреса из указанной сети в поле отправителя или получателя
net <сеть> mask <маска сети>	будет отбирать все пакеты IP, содержащие в поле отправителя или получателя адреса из сети, указанной с использованием маски
net <сеть/размер маски>	будет отбирать все пакеты IPv4, содержащие в поле отправителя или получателя адреса из сети, указанной с использованием маски
dst port <порт>	отберет все пакеты ip/tcp и ip/udp, направленные в указанный порт. Номера портов могут задаваться номерами или именами из файла /etc/services. При указании имени (протокол/порт) проверяется как порт, так и протокол. Если примитив содержит номер или неоднозначное обозначение порта (только порт, без протокола) фильтру будут соответствовать пакеты обоих протоколов (tcp и udp). Например, фильтру dst port 513 будут соответствовать пакеты tcp/login и udp/who, а фильтру port domain – трафик tcp/domain и udp/domain
src port <порт>	отбирает все пакеты, отправленные из указанного порта
port <порт>	отбирает все пакеты, содержащие указанный номер порта в поле отправителя или получателя. Любое из трех перечисленных правил для портов может включать в качестве префикса идентификатор протокола tcp или udp (например, tcp src port <порт>, будет отбирать пакеты tcp, отправленные из указанного порта)
less <размер>	будет собирать пакеты, размер которых не превышает указанного значения
greater <размер>	будет собирать пакеты, размер которых не меньше указанного значения
ip proto <протокол>	отбирает все пакеты IP, содержащие заданный идентификатор типа в поле типа протокола. Типы протоколов IP можно указывать по именам или (icmp, icmp6, igmp, igrp, pim, ah, esp, vrrp, udp, tcp) или номерам. Поскольку tcp, udp и icmp используются также в качестве ключевых слов, перед этими идентификаторами следует помешать символ (слэш). Отметим, что этот примитив не проверяет цепочки протокольных заголовков

Примитив	Описание
ip protochain <протокол>	отберет все пакеты IPv4, содержащие в цепочке протокольных заголовков идентификатор указанного типа протокола. Например, фильтру ip protochain 4 будут соответствовать все пакеты IPv4 с заголовками TCP в цепочке заголовков. Такой пакет может содержать, например, заголовок аутентификации (AH), маршрутный заголовок (routing header), или заголовок опции hop-by-hop между заголовками IPv4 и TCP. Отметим, что порождаемый этим примитивом код BPF достаточно сложен и не может быть оптимизирован средствами tcpdump, поэтому использование данного фильтра может замедлять работу программы
ether broadcast	обеспечивает отбор всех широковещательных кадров Ethernet. Ключевое слово ether может быть опущено
ip broadcast	отбирает все широковещательные пакеты IPv4. Этому правилу будут соответствовать широковещательные адреса, содержащие только нули (all-zeroes) и только единицы (all-ones) с учетом маски подсети для интерфейса, который используется для захвата пакетов. Если маска подсети для интерфейса недоступна, фильтр может работать некорректно
ether multicast	собирает все кадры с групповыми адресами Ethernet. Ключевое слово ether использовать необязательно. Логически это правило эквивалентно выражению ether[0] & 1 != 0
ip multicast	отбирает пакеты с групповыми адресами IP
ether proto <протокол>	отбирает кадры Ethernet с заданным типом протокола. Протокол может быть указан по номеру или имени (ip, arp, rarp, atalk, aarp, decnet, sca, lat, mopdl, moprc, iso, stp, ipx, netbeui). В случаях использования правила для протоколов Token Ring (например, tr protocol arp) и IEEE 802.11 (например, wlan protocol arp) в большинстве случаев идентификация протокола производится на основании заголовка 802.2 Logical Link Control (LLC), который обычно помещается после заголовка Token Ring или 802.11. При фильтрации для большинства протоколов Token Ring и 802.11 программа фильтр проверяет только поле идентификатора протокола (protocol ID) в заголовке LLC так называемого SNAP-формата с идентификатором OUI = 0x000000 (Organizational Unit Identifier), указывающим на инкапсуляцию Ethernet. Проверка для пакетов использования формата SNAP с OUI = 0x000000 не выполняется за исключением перечисленных ниже случаев: iso фильтр проверяет поля DSAP11 и SSAP12 в заголовках LLC; stp netbeui фильтр проверяет поле DSAP в заголовке LLC; atalk фильтр проверяет использование в кадре формата SNAP с OUI = 0x080007 и тип (etype) AppleTalk. Для случая Ethernet проверяются поля типа Ethernet для большинства протоколов. Исключениями являются протоколы iso sap netbeui фильтр проверяет для кадра принадлежность к 802.3 и заголовок LLC (как это описано выше для Token Ring и 802.11); atalk проверяется типа AppleTalk в кадре Ethernet и формат заголовка SNAP (как для Token Ring и 802.11); aarp проверяется тип AppleTalk ARP в кадре Ethernet или использование формата 802.2 SNAP с OUI = 0x000000; ipx фильтр проверяет тип IPX в кадре Ethernet, поле IPX DSAP в заголовке LLC, инкапсуляцию IPX и тип IPX в кадре SNAP
ifname <интерфейс>	отбирает все пакеты, полученные от указанного интерфейса
on <интерфейс>	синоним ifname

Примитив	Описание
ip, arp, rarp, atalk, aarp, decnet, iso, stp, ipx, netbeui	используются в качестве сокращения для: ether proto p где p – один из перечисленных протоколов
tcp, udp, icmp	используется в качестве сокращения для ip proto p где p – один из перечисленных протоколов
iso proto <протокол>	собирает пакеты с указанным типом протокола OSI. Протокол может быть указан по номеру или имени (clnp, esis, isis)
clnp, esis, isis	сокращения для выражений: iso proto p где p – один из перечисленных протоколов
l1, l2, iih, lsp, snp, csnp, psnp	сокращения для типов IS-IS PDU
vpi n	собирает пакеты ATM с указанным идентификатором виртуального пути для SunATM (Solaris)
vci n	собирает пакеты ATM с указанным идентификатором виртуального канала для SunATM (Solaris)
lane	собирает пакеты эмуляции ЛВС (ATM LANE) для SunATM (Solaris). Первое ключевое слово lane в выражении изменяет проверки для остальной части фильтра в предположении что пакет относится к пакетам эмуляции Ethernet или LANE LE Control. Если ключевое слово lane не указано, проверки выполняются в предположении LLC-инкапсуляции
llc	собирает пакеты ATM с инкапсуляцией LLC для SunATM (Solaris)
oamf4s	собирает пакеты ATM для SunATM (Solaris), являющиеся сегментами потока ячеек OAM F4 (VPI=0, VCI=3)
oamf4e	собирает пакеты ATM для SunATM (Solaris), относящиеся к сквозным потокам OAM F4 (VPI=0, VCI=4)
oamf4	собирает пакеты ATM для SunATM (Solaris), являющиеся сегментами сквозного потока ячеек OAM F4 (VPI=0, (VCI=3 или VCI=4))
oam	собирает пакеты ATM для SunATM (Solaris), являющиеся сегментами сквозного потока ячеек OAM F4 (VPI=0, (VCI=3 или VCI=4))
metac	собирает пакеты ATM для SunATM (Solaris), относящиеся к сигнальным мета-устройствам (VPI=0, VCI=1)
bcc	собирает пакеты ATM для SunATM (Solaris), относящиеся к широковещательным сигнальным устройствам (VPI=0, VCI=2)
sc	собирает пакеты ATM для SunATM (Solaris), относящиеся к сигнальным устройствам (VPI=0, VCI=5)
ilmic	собирает пакеты ATM для SunATM (Solaris), относящиеся к клиентским устройствам ILMI (VPI=0, VCI=16)
connectmsg	собирает пакеты ATM для SunATM (Solaris), относящиеся к сигнальным устройствам и содержащие сообщения Q.2931 Setup, Call Proceeding, Connect, Connect Ack, Release, Release Done
metaconnect	собирает пакеты ATM для SunATM (Solaris), относящиеся к сигнальным мета-устройствам и содержащие сообщения Q.2931 Setup, Call Proceeding, Connect, Connect Ack, Release, Release Done
outbuf <size>	соединение пропускается, если в первых исходящих <size> байтах, переданных в рамках соединения, не обнаружено данных, соответствующих регулярному выражению
inbuf <size>	соединение пропускается, если в первых входящих <size> байтах, переданных в рамках соединения, не обнаружено данных, соответствующих регулярному выражению

Логические выражения

Выражения типа

expr <операция> expr

возвращают логическое значение, соответствующее отношениям между левой и правой часть. В качестве операции могут использоваться >, <, >=, <=, =, !=, а операнды expr могут быть арифметическими выражениями, включающими целые константы (запись в стандарте C), бинарные операторы +, -, *, /, &, |, <<, >>, оператор длины (offset) и данные из пакетов. Для получения значений полей из пакетов применяется синтаксис:

proto [offset : size]

Параметр proto может содержать идентификатор одного из протоколов (ether, tr, wlan, ppp, slip, link, ip, arp, rarp, tcp, udp, icmp) и задает уровень протокола15, для которого извлекаются данные. Отметим, что tcp, udp и другие протоколы верхних уровней относятся только к пакетам IPv4, а не IPv616. Параметр offset задает смещение в байтах относительно начала заголовка указанного уровня. Необязательный параметр size определяет размер интересующего поля в байтах. Допустимы значения размера 1, 2 и 4, по умолчанию просматривается 1 байт.

Оператор длины, указываемый ключевым словом len, определяет размер пакета в байтах. Например, выражению

ether[0] & 1 != 0

будет соответствовать весь multicast-трафик, выражение

ip[0] & 0xf != 5

позволяет собрать все пакеты IP, в которых присутствует поле опций, а фильтр

ip[6:2] & 0x1fff = 0

соберет только нефрагментированные дейтаграммы и первые фрагменты.

При выборе полей из заголовков учитывается структура пакетов соответствующего уровня. Например, tcp[0] всегда будет возвращать первый байт заголовка TCP, игнорируя фрагменты.

Некоторые поля и значения смещений могут задаваться не только числами, но и именами. В частности, для протокола поддерживается параметр icmptype (поле типа ICMP), который может принимать значения icmp-echoreply, icmp-unreach, icmp-sourcequench, icmp-redirect, icmp-echo, icmp-routeradvert, icmp-routersolicit, icmp-timxceed, icmp-paramprob, icmp-tstamp, icmp-tstampreply, icmp-ireq, icmp-ireqreply, icmp-maskreq, icmp-maskreply. Для флагов TCP можно использовать идентификаторы tcp-fin, tcp-syn, tcp-rst, tcp-push, tcp-ack и tcp-urg.

Примитивы в выражениях можно группировать с использованием

- скобок;
- отрицания (! или not);
- логического пересечения (&& или and);
- логического объединения (|| или or).

Оператор отрицания имеет высший уровень приоритета, операции объединения и пересечения имеют одинаковый приоритет и выполняются слева направо в порядке следования. Отметим, что для операции логического пересечения недостаточно просто указать операнды рядом, а требуется явно задать операцию (&& или and).

Если идентификатор указан без ключевого слова, предполагается ключевое слово, которое до этого использовалось последним. Например, выражение

not host vs and ace

является простым сокращением от

not host vs and host ace

Отметим, что эти выражения не эквивалентны фильтру not (host vs or ace).

Аргументы выражений могут передаваться программе фильтр как один или множество аргументов (используйте более удобную для вас форму). В общем случае выражения, содержащие мета-символы командного интерпретатора, должны передаваться как один аргумент, заключенный в кавычки.

Метасимволы в регулярных выражениях

Регулярное выражение представляет собой поисковый шаблон в виде строки, состоящей из обычных символов и метасимволов. Например, для поиска имен пользователей **Ivanov** или **Ivanof** можно использовать следующее регулярное выражение: **Ivano(v|f)**, где **|** является метасимволом логического ИЛИ.

Наиболее применяемые метасимволы представлены в таблице ниже.

Метасимвол	Назначение	Пример
. **(точка)**	Любой символ	По шаблону **a.c** могут быть найдены последовательности символов **abc**, **anc**, **a4c** и т. п.
+	Совпадение 1 или более раз	По шаблону **a+** могут быть найдены последовательности **a**, **aa**, **aaa**, **aaaa** и т. д.
?	Совпадение 1 или 0 раз	По шаблону **ab?c** могут быть найдены две последовательности **abc** и **ac**
*****	Совпадение 0 или более раз	По шаблону **ab*c** могут быть найдены последовательности **ac**, **abc**, **abbc**, **abbbc**, **abbbbc** и т. п.
{n}	Совпадение ровно n раз	По шаблону **a{5}** может быть найдена последовательность **aaaaa**
{n,}	Совпадение не менее n раз	По шаблону **a{3,}** могут быть найдены последовательности **aaa**, **aaaa**, **aaaaa** и т. д.
{n,m}	Совпадение от n до m раз	По шаблону **a{3,5}** могут быть найдены последовательности **aaa**, **aaaa**, **aaaaa**
|	Логическое ИЛИ	По шаблону **a|b** будут найдены символы **a** или **b**

Примеры правил фильтрации

Правило	Описание
pass :tcp port 25;	Разрешается прохождение любых TCP-пакетов по протоколу TCP через порт 25 (например, для получения почты)
pass :tcp port 110;	Разрешается прохождение любых TCP-пакетов по протоколу TCP через порт 110 (например, для отправки почты)
pass :tcp port 21;	Разрешается прохождение TCP-пакетов по протоколу TCP через порт 21 (например, для доступа на FTP-порты)
:tcp port 80; :tcp port 8080;	Запрещается прохождение TCP-пакетов по протоколу TCP через порты 80 и 8080 (например, для запрета выхода в сеть Интернет)
:net <адрес сети>;	Запрещается прохождение IP-пакетов в определенную сеть
Pass iface="Local Area Connection 2":tcp port 80;	Разрешается прохождение TCP-пакетов через соединение "Local Area Connection 2" по протоколу TCP через порт 80
pass:;	Прохождение всех пакетов разрешается
alert : ip proto 1;	Запрещается прохождение всех IP-пакетов по протоколу ICMP. При срабатывании правила выдается оповещение
pass sched = 1 : ip proto 1;	Разрешается прохождение IP-пакетов по протоколу ICMP в период времени, определенный в расписании идентификатором 1
pass log:;	Пропускаются все (ICMP, UDP, ARP, TCP) пакеты. Журнал пакетов регистрирует детальную информацию о пакетах
pass:arp: pass in log:;	Пропускаются все входящие пакеты, все исходящие блокируются. Журнал пакетов регистрирует детальную информацию о пропущенных, входящих пакетах
pass:arp; pass out log:;	Пропускаются все исходящие пакеты, все входящие блокируются. Журнал пакетов регистрирует детальную информацию о пропущенных, исходящих пакетах
pass log alert :icmp[icmptype]=icmp-echo; pass:;	Пропускаются icmp-запросы, появляется окно с информацией о пакетах (при включенном оповещении). Журнал пакетов регистрирует детальную информацию о icmp-запросах
pass log alert: icmp[icmptype]=icmp-echoreply; pass:;	Пропускаются icmp-ответы, появляется окно с информацией о пакетах (при включенном оповещении). Журнал пакетов регистрирует детальную информацию о icmp-ответах. Остальные пакеты пропускаются без регистрации

Правило	Описание
pass log iface=«имя интерфейса»:;	Пропускаются все пакеты через указанный интерфейс. Журнал пакетов регистрирует информацию обо всех пропущенных пакетах
pass log alert iface=«имя интерфейса»: icmp[icmptype]=icmp-echo; pass:;	Пропускаются icmp-запросы через указанный сетевой интерфейс, появляется окно с информацией о пакетах (при включенном оповещении). Журнал пакетов регистрирует детальную информацию о icmp-запросах. Остальные пакеты пропускаются без регистрации
pass log alert iface=«имя интерфейса»: icmp[icmptype]=icmp-echoreply; pass:;	Пропускаются icmp-ответы через указанный сетевой интерфейс, появляется окно с информацией о пакетах (при включенном оповещении). Журнал пакетов регистрирует детальную информацию о icmp-ответах. Остальные пакеты пропускаются без регистрации
log:;	Блокируются все входящие и исходящие (ICMP, UDP, ARP, TCP) пакеты. Журнал пакетов, регистрирует детальную информацию о заблокированных пакетах
pass:arp; in log:; pass out:;	Блокируются все входящие пакеты, все исходящие пропускаются. Журнал пакетов регистрирует детальную информацию, о заблокированных входящих пакетах
pass:arp; out log:; pass in:;	Блокируются все исходящие пакеты, все входящие пропускаются. Журнал пакетов регистрирует детальную информацию, о заблокированных исходящих пакетах
pass:arp; log alert: icmp[icmptype]=icmp-echo; pass:;	Блокируются icmp-запросы. Появляется окно с информацией о заблокированных пакетах (при включенном оповещении). Журнал пакетов регистрирует детальную информацию, о заблокированных icmp-запросах
pass:arp; log alert: icmp[icmptype]=icmp-echoreply; pass:;	Блокируются icmp-ответы. Появляется окно с информацией о заблокированных пакетах (при включенном оповещении). Журнал пакетов регистрирует детальную информацию, о заблокированных icmp-ответах
log iface=«имя интерфейса»:;	Блокируются все пакеты через указанный интерфейс. Журнал пакетов регистрирует детальную информацию, обо всех заблокированных пакетах
pass:arp; log iface=«имя интерфейса»: icmp[icmptype]=icmp-echo; pass:;	Блокируются icmp-запросы через указанный интерфейс. Журнал пакетов регистрирует детальную информацию, о заблокированных icmp-запросах
pass:arp; log iface=«имя интерфейса»: icmp[icmptype]=icmp-echoreply; pass:;	Блокируются icmp-ответы через указанный интерфейс. Журнал пакетов регистрирует детальную информацию, о заблокированных icmp-ответах
pass:arp; log iface=«имя интерфейса»: tcp;» pass:;	Блокируется только tcp-соединения через указанный интерфейс. Журнал пакетов регистрирует детальную информацию о заблокированных tcp-пакетах
pass:arp; log iface=«имя нтерфейса»:icmp; pass:;	Блокируется только icmp-соединения. Журнал пакетов регистрирует детальную информацию, о заблокированных icmp-пакетах
pass:arp; log iface=«имя интерфейса»: tcp port 21; pass:;	Блокируется только tcp-соединение на 21-й порт (подключения к ftp). Журнал пакетов регистрирует детальную информацию о заблокированных соединениях, через 21-й порт
pass:arp; log iface=«имя интерфейса»: tcp port 80; pass:;	Блокируется только tcp-соединения, проходящие через 80-й порт (http). Журнал пакетов регистрирует детальную информацию, о заблокированных соединениях, через 80-й порт

Правило	Описание
pass:arp; out log iface=«имя интерфейса»: udp port 68; pass:;	Блокируется только исходящие соединения на 68-й udp порт. Журнал пакетов регистрирует детальную информацию, о заблокированных исходящих соединениях, через 68-й порт
log iface="имя интерфейса":greater 100; pass:;	Блокируются через указанный интерфейс, пакеты размером более 100 байт. Меньше 100, проходят. Журнал пакетов, регистрирует детальную информацию о заблокированных пакетах
log iface="имя интерфейса":greater 100 and less 200; pass:;	Блокируются через указанный интерфейс пакеты размером от 100 до 200 байт. Остальные проходят. Журнал пакетов регистрирует детальную информацию, о заблокированных пакетах
log iface="имя интерфейса":udp and greater 100; pass:;	Блокируются через указанный интерфейс, UDP-пакеты размером более 100 байт. Меньше 100, проходят. Журнал пакетов, регистрирует детальную информацию о заблокированных udp-пакетах
log iface=”имя интерфейса”:udp and (greater 100 and less 250); pass:;	Блокируются через указанный интерфейс UDP-пакеты от 100 до 250 байт. Остальные проходят. Журнал пакетов, регистрирует детальную информацию о заблокированных udp-пакетах
log iface="имя интерфейса":src port 21; pass:;	Через указанный интерфейс, блокируется отправка пакетов, с указанного порта источника. Журнал пакетов регистрирует детальную информацию, о заблокированных пакетах
log iface="имя интерфейса": tcp and (dst port 1025); pass:;	Блокируется через указанный интерфейс, только tcp-соединения на порт 1025. Остальные пакеты разрешены. Журнал пакетов регистрирует детальную информацию, о заблокированных tcp-соединениях
log iface="имя интерфейса":udp and (portrange 2000-3000); pass:;	Блокируются через указанный интерфейс, пакеты с и/или на заданный диапазон портов. Журнал пакетов регистрирует детальную информацию, о заблокированных пакетах
log iface="имя интерфейса":udp and (dst portrange 2000-3000); pass:;	Блокируются через указанный интерфейс, пакеты с и/или на заданный диапазон портов. Журнал пакетов регистрирует детальную информацию, о заблокированных пакетах
out log iface="имя интерфейса":icmp and dst host 192.x.x.x; pass:;	Блокируются через указанный интерфейс, исходящие пакеты на указанный хост (указывается свой адрес хоста). Журнал пакетов регистрирует детальную информацию, о заблокированных исходящих пакетах
log iface="имя интерфейса":net 10.2; pass:;	Блокируются через указанный интерфейс, трафик из/в сеть 10.2.0.0/16. Журнал пакетов регистрирует детальную информацию, о заблокированных пакетах
log iface="имя интерфейса":src net 10.2; log iface="имя интерфейса":dst net 10.2.2;	Блокируются через указанный интерфейс трафик из/в сеть 10.2.2.0/24. Журнал пакетов регистрирует детальную информацию, о заблокированных пакетах

Структура файла с расписаниями

Файл с расписаниями состоит из строк вида:

id [daily|weekly] [mon|tue|wed|thu|fri|sat|sun] [HH:MM-HH:MM];

где:

- **Id** — уникальный идентификатор расписания, число;
- **daily|weekly** — тип расписания, ежедневное или недельное;
- далее:
  - для ежедневных расписаний — временные интервалы в формате ЧасНачала:МинутаНачала- ЧасОкончания:МинутаОкончания;
  - для недельных расписаний — дни недели в виде строк (mon|tue|wed|thu|fri|sat|sun), после каждой из которых идут временные интервалы в формате ЧасНачала:МинутаНачала- ЧасОкончания:МинутаОкончания.

Каждая строка задает отдельное расписание и завершается точкой с запятой.

Пример	Пояснение
1 daily 10:00-18:00;	Правила фильтрации с идентификатором расписания "1" работают ежедневно с 10 до 18 часов
2 weekly mon 10:00-18:00 tue 10:00-18:00 wed 10:00-18:00 thu 10:00-18:00 fri 10:00-17:00;	Правила фильтрации с идентификатором расписания "2" работают с понедельника по четверг с 10 до 18 часов и в пятницу с 10 до 17

Перечень файлов для контроля целостности

Контроль целостности выполняется для следующих служебных файлов Абонентского пункта и МСЭ:

Файлы, общие для всех типов ОС Windows	**Файлы ОС Windows 2000/XP**	**Файлы ОС Windows Vista**
AP_Mgr.exe	cont3flt.sys	c3mse_vi.sys
EAPExt161.dll	cont3ppp.sys	c3ppp_vi.sys
EAPSigner161.exe	c3mse4.sys	c3flt_vi.sys
InfsCerImport.dll	mseApp.sys	
PacketFilterMgr.dll		
RouteMgr.exe		
RouteMgrPS.dll		
SStart.exe		
SobolChecker.dll		
cont3flt.dll		
c3mse4_svc.exe		
c3mse4mgr.dll		
mseGui.exe		

Документация

1	Аппаратно-программный комплекс шифрования "Континент". Централизованное управление комплексом. Руководство администратора
2	Аппаратно-программный комплекс шифрования "Континент". Локальное управление криптографическим шлюзом. Руководство администратора
3	Аппаратно-программный комплекс шифрования "Континент". Аудит. Руководство администратора
4	Аппаратно-программный комплекс шифрования "Континент". Сервер доступа. Руководство администратора
5	Аппаратно-программный комплекс шифрования "Континент". Программа мониторинга КШ. Руководство пользователя
6	Аппаратно-программный комплекс шифрования "Континент". Тестирование каналов связи. Руководство администратора
7	Аппаратно-программный комплекс шифрования "Континент". Обновление программного обеспечения. Руководство администратора
8	Средство криптографической защиты информации "Континент-АП". Межсетевой экран. Руководство администратора
9	Средство криптографической защиты информации "Континент-АП". Абонентский пункт. Руководство пользователя
10	Аппаратно-программный комплекс шифрования "Континент". Аутентификация хоста. Руководство администратора

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