Антивирус Касперского 5.5 для Proxy Server

Руководство администратора

ВЕРСИЯ ПРОГРАММЫ: 5.5 ПЛАНОВОЕ ОБНОВЛЕНИЕ 3

Уважаемый пользователь!

Спасибо за то, что выбрали наш продукт. Мы надеемся, что этот документ поможет вам в работе и ответит на большинство возникающих вопросов.

Дата редакции документа: 30.05.2012

http://www.kaspersky.ru
http://support.kaspersky.ru

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Программа Антивирус Касперского 5.5 для Proxy Server предназначена для антивирусной защиты трафика прокси-сервера, поддерживающего протокол ICAP (Internet Content Adaptation Protocol).

Программа позволяет:

- выполнять антивирусную проверку объектов, передаваемых через прокси-сервер;

  Антивирус Касперского не проверяет данные, передаваемые по протоколу HTTPS.

- лечить обнаруженные зараженные объекты и, если лечение невозможно, запрещать доступ к зараженному объекту;

- использовать групповые настройки для определения различных параметров фильтрации, применяемых в зависимости от адреса запрашивающего объект пользователя и адреса (URL) объекта;

- вести статистику работы, включающую в себя помимо прочего информацию о выполнении и результатах антивирусной проверки, ошибках в работе Антивируса Касперского и предупреждениях;

- уведомлять администратора об обнаружении вредоносных программ;

- обновлять антивирусные базы; ресурсом для обновления баз являются сервера обновлений Лаборатории Касперского. Также есть возможность настроить Антивирус Касперского на обновление баз из локальной директории;

  Антивирусные базы используются для обнаружения и лечения зараженных объектов. На основе записей, содержащихся в них, каждый объект во время проверки анализируется на присутствие вирусов: содержание объекта сравнивается с кодом, характерным для того или иного вируса.

  Следует помнить, что каждый день появляются новые вирусы и поэтому необходимо поддерживать антивирусные базы в актуальном состоянии. Обновления для антивирусных баз публикуются на серверах обновлений Лаборатории Касперского каждый час.

В ЭТОМ РАЗДЕЛЕ

Что нового

В текущей версии Антивируса Касперского имеются следующие нововведения:

- Добавлена поддержка Squid версии 3.0 и выше.

- Расширены возможности различной настройки Антивируса Касперского для групп пользователей. В частности, теперь для групп можно задавать значения параметров (см. стр. 32), определяющих набор баз Антивируса Касперского и максимальное время проверки.

- Добавлена поддержка возможности **preview** (см. стр. 41) протокола ICAP. Использование **preview** позволяет уменьшить объем данных, передаваемых по сети, и ускорить процесс фильтрации проверяемых объектов.
- Добавлена возможность просмотра подробной информации о лицензии по трафику (см. стр. 22).
- Улучшена производительность Антивируса Касперского.

Аппаратные и программные требования к системе

Для работы Антивируса Касперского необходимо соответствие системы следующим аппаратным и программным требованиям:

- Минимальные аппаратные требования:
  - процессор Intel Pentium® II 400 МГц или выше;
  - 1 ГБ оперативной памяти;
  - 150 МБ на жестком диске для установки Антивируса Касперского;
  - 200 МБ на жестком диске для хранения временных файлов.
- Программные требования:
  - для 32-битной платформы одна из следующих операционных систем:
    - Red Hat Enterprise Linux Server 6.2;
    - Fedora 16;
    - CentOS 5.7, 6.2;
    - SUSE Linux Enterprise Server 11 SP1;
    - Novell Open Enterprise Server 2 SP3;
    - openSUSE Linux 12.1;
    - Debian GNU/Linux 6.0.4 Squeeze;
    - Mandriva Enterprise Server 5.2;
    - Ubuntu 10.04, 12.04 LTS;
    - FreeBSD 8.2, 9.0;
  - для 64-битной платформы одна из следующих операционных систем:
    - Red Hat Enterprise Linux Server 6.2;
    - Fedora 16;
    - CentOS 5.7, 6.2;
    - SUSE Linux Enterprise Server 11 SP1;

- Novell Open Enterprise Server 2 SP3;
- openSUSE Linux 12.1;
- Debian GNU/Linux 6.0.4 Squeeze;
- Ubuntu 10.04, 12.04 LTS;
- FreeBSD 8.2, 9.0.

- Прокси-сервер Squid 3.0 или выше с поддержкой ICAP-протокола.

  Интеграция Антивируса Касперского с Squid 3.1.6 не поддерживается. Более подробная информация приведена на сайте http://bugs.squid-cache.org/show_bug.cgi?id=3011.

- Библиотека Glibc версии 2.2.x или выше (для дистрибутивов Linux).
- Интерпретатор языка Perl версии 5.0 или выше (более подробная информация приведена на сайте http://www.perl.org).

Получение информации об Антивирусе Касперского

«Лаборатория Касперского» предоставляет различные источники информации об Антивирусе Касперского. Выберите наиболее удобный для себя в зависимости от важности и срочности вопроса.

Вы можете обратиться к источникам для самостоятельного поиска или в Департамент продаж. Если вы уже приобрели Антивирус Касперского, обратитесь в Службу технической поддержки. Если вопрос не требует срочного ответа, его можно обсудить со специалистами «Лаборатории Касперского» и другими пользователями на нашем форуме.

Источники информации для самостоятельного поиска

В вашем распоряжении находятся следующие источники информации об Антивирусе Касперского:

- документация;
- manual pages.

Документация

Руководство администратора содержит следующую информацию:

- о назначении Антивируса Касперского;
- о требованиях к аппаратному и программному обеспечению для установки и работы Антивируса Касперского;
- об установке Антивируса Касперского;
- об управлении Антивирусом Касперского с помощью командной строки.

Этот документ в формате PDF входят в комплект поставки Антивируса Касперского. Также вы можете загрузить его со страницы Антивируса Касперского на сайте «Лаборатории Касперского».

Manual pages

Для получения информации об Антивирусе Касперского вы можете просматривать файлы manual pages, которые после установки Антивируса Касперского находятся в директории */opt/kaspersky/kav4proxy/share/man/*.

ОБРАЩЕНИЕ В СЛУЖБУ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

Если вы уже приобрели Антивирус Касперского, информацию о нем можно получить у специалистов Службы технической поддержки по телефону или через интернет.

Прежде чем обратиться в Службу технической поддержки, пожалуйста, ознакомьтесь с правилами ее оказания (http://support.kaspersky.ru/support/rules).

Электронный запрос в Службу технической поддержки

Вы можете задать вопрос специалистам Службы технической поддержки, заполнив веб-форму системы обработки клиентских запросов (http://support.kaspersky.ru/helpdesk.html).

Запрос можно отправить на русском, английском, немецком, французском или испанском языках.

Чтобы отправить электронный запрос, вам нужно указать в нем **номер клиента**, полученный при регистрации на веб-сайте Службы технической поддержки, и **пароль**.

Если вы еще не являетесь зарегистрированным пользователем программ «Лаборатории Касперского», вы можете заполнить регистрационную форму (https://support.kaspersky.com/ru/personalcabinet/registration/form/). При регистрации укажите имя файла ключа.

Вы получите ответ на свой запрос от специалиста Службы технической поддержки в своем Персональном кабинете (https://support.kaspersky.com/ru/PersonalCabinet) и по электронному адресу, который вы указали в запросе.

В веб-форме запроса как можно подробнее опишите возникшую проблему. В обязательных для заполнения полях укажите:

- **Тип запроса**. Выберите тему, наиболее точно соответствующую характеру возникшей проблемы, например, «Проблема установки / удаления продукта» или «Проблема поиска / удаления вирусов».
- **Название и номер версии Антивируса Касперского**.
- **Текст запроса**. Подробно опишите возникшую проблему.
- **Номер клиента и пароль**. Введите номер клиента и пароль, которые вы получили при регистрации на веб-сайте Службы технической поддержки.
- **Электронный адрес**. По этому адресу специалисты Службы технической поддержки перешлют ответ на ваш запрос.

Техническая поддержка по телефону

Если возникла неотложная проблема, вы всегда можете позвонить в Службу технической поддержки в вашем городе. Обращаясь к сотрудникам русскоязычной (http://support.kaspersky.ru/support/support_local) или интернациональной (http://support.kaspersky.ru/support/international) технической поддержки, пожалуйста, не забудьте предоставить им информацию об Антивирусе Касперского (http://support.kaspersky.ru/support/details), чтобы наши специалисты могли помочь вам как можно быстрее.

Обсуждение программ «Лаборатории Касперского» на веб-форуме

Если ваш вопрос не требует срочного ответа, его можно обсудить со специалистами «Лаборатории Касперского» и другими пользователями на нашем форуме по адресу http://forum.kaspersky.com.

На форуме вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы, пользоваться поиском.

АЛГОРИТМ РАБОТЫ И ТИПИЧНЫЕ СХЕМЫ РАЗВЕРТЫВАНИЯ ПРОГРАММЫ

Информация, содержащаяся в данной главе необходима для корректного понимания работы Антивируса Касперского, его настройки и интеграции в структуру существующей сети.

В ЭТОМ РАЗДЕЛЕ

Алгоритм работы Антивируса Касперского

Антивирус Касперского не проверяет данные, передаваемые по протоколу HTTPS.

Антивирус Касперского выполняет проверку HTTP-трафика в двух режимах работы прокси-сервера: **REQMOD** и **RESPMOD**.

В режиме **RESPMOD** выполняется проверка объектов, запрошенных пользователем через прокси-сервер. В режиме **REQMOD** проверке подвергаются объекты, передаваемые от пользователя через прокси-сервер. В качестве примера использования режима **REQMOD** можно привести отправку почтовых сообщений при помощи веб-интерфейса почтового сервера. Вложенные в почтовое сообщение объекты, передаваемые пользователем на почтовый сервер, проверяются Антивирусом Касперского.

Антивирусная проверка интернет-трафика в режиме **RESPMOD** выполняется программой согласно следующему алгоритму (см. рис. 1):

1. Пользователь запрашивает объект по протоколу HTTP через прокси.
2. Если запрашиваемый объект содержится в кеше прокси, то он возвращается пользователю. Если требуемый объект в кеше не найден, то прокси обращается к удаленному серверу и скачивает запрашиваемый объект.
3. Используя ICAP-протокол, прокси передает полученный объект Антивирусу Касперского для антивирусной проверки.
4. Антивирус Касперского проверяет, соответствуют ли параметры запроса (IP-адрес пользователя, URL запрашиваемого объекта) какой-либо из групп (см. стр. 31), и если такая группа найдена, то выполняет проверку и при необходимости обработку полученного объекта, в соответствии с заданными для группы правилами. Если запрос не соответствует ни одной из групп, то в качестве параметров антивирусной проверки и обработки используются параметры, заданные в группе по умолчанию.
5. По результатам антивирусной проверки объекту присваивается статус, в соответствии с которым разрешается или запрещается доступ пользователей к данному объекту. Запрет или разрешение на доступ к объектам с определенным статусом задается параметрами группы обработки (см. стр. 31).

6. Если доступ к объекту разрешен, то Антивирус Касперского разрешает прокси кеширование данного объекта и передачу его пользователю. Если доступ к объекту запрещен, то Антивирус Касперского запрещает прокси кеширование данного объекта и передачу его пользователю. Вместо запрошенного объекта пользователю отправляется уведомление о запрете доступа к объекту.

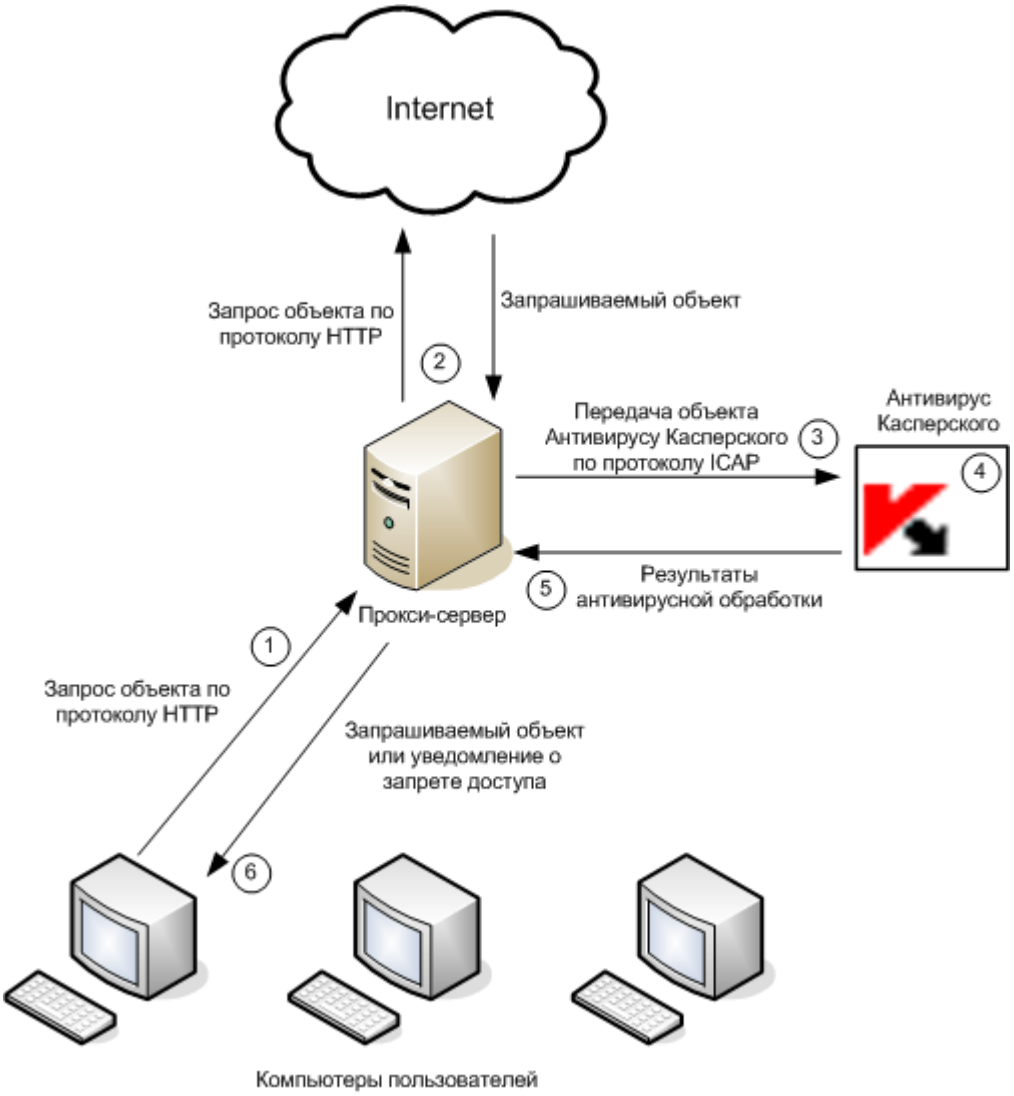

Рисунок 1. Антивирусная проверка трафика в режиме RESPMOD

Антивирусная проверка интернет-трафика в режиме **REQMOD** выполняется программой согласно следующему алгоритму (см. рис. 2):

1. Пользователь отправляет объект по протоколу HTTP через прокси.

2. Используя ICAP-протокол, прокси передает полученный объект Антивирусу Касперского для антивирусной проверки.

3. Антивирус Касперского проверяет, соответствуют ли параметры запроса какой-либо из групп (см. стр. 31), и если такая группа найдена, то выполняет проверку и при необходимости обработку полученного объекта, в соответствии с заданными для группы правилами. Если запрос не соответствует ни одной из групп, то в качестве параметров антивирусной проверки и обработки используются параметры, заданные в группе по умолчанию.

4. По результатам антивирусной проверки объекту присваивается статус, в соответствии с которым разрешается или запрещается передача данного объекта. Запрет или разрешение на передачу объекта с определенным статусом задается параметрами группы обработки (см. стр. 31).

5. Если передача разрешена, то прокси-сервер выполняет передачу объекта, отправленного пользователем. Если передача запрещена, то прокси не выполняет передачу объекта, а пользователю высылается уведомление о запрете передачи.

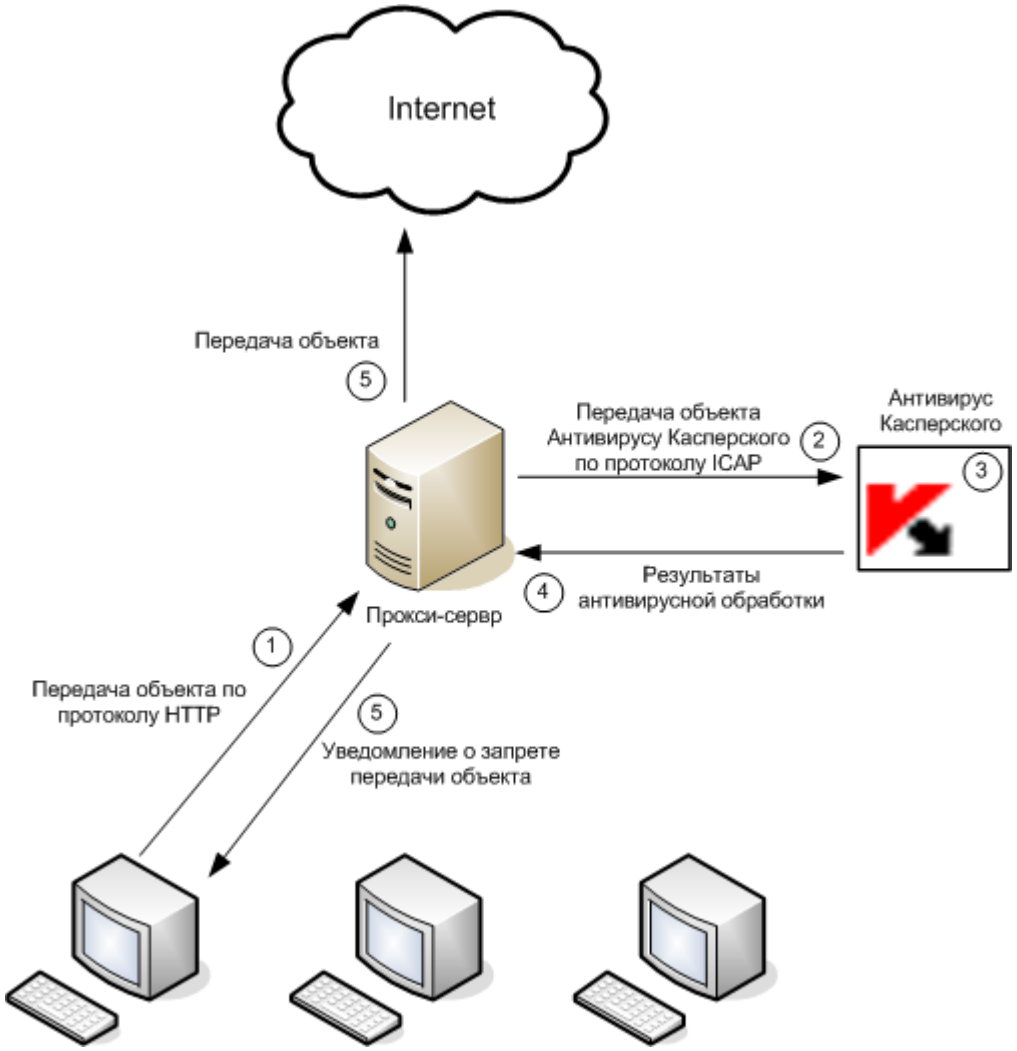

Рисунок 2. Антивирусная проверка трафика в режиме REQMOD

Алгоритм обработки ICAP-запросов

При взаимодействии с прокси-сервером Антивирус Касперского выступает в роли ICAP-сервера. Основной процесс ICAP-сервера управляет дочерними процессами, которые выполняют следующие функции:

- прием и обработка запросов со стороны ICAP-клиента (прокси-сервера);
- взаимодействие с антивирусным ядром: отправка запросов на проверку и получение результатов проверки;
- сбор статистических данных о проверке;
- передача данных от антивирусного ядра ICAP-клиенту.

Для каждого дочернего процесса запускается несколько антивирусных ядер, которые загружаются в отдельных процессах. Максимальное количество антивирусных ядер, которое может использовать один дочерний процесс, задается параметром **MaxEnginesPerChild**.

При запуске программы основной процесс ICAP-сервера запускает один дочерний процесс. После запуска и до перехвата запроса дочерний процесс находится в состоянии ожидания.

При поступлении соединения от ICAP-клиента дочерний процесс перехватывает это соединение и переходит в рабочее состояние. В дальнейшем все запросы, приходящие в рамках этого соединения, будут обрабатываться этим дочерним процессом. Когда дочерний процесс заканчивает обработку всех запросов, он переходит в состояние ожидания.

Если все дочерние процессы находятся в рабочем состоянии и их количество не превышает значение параметра **MaxChildren**, основной процесс ICAP-сервера запускает еще один дочерний процесс.

Дочерний процесс обрабатывает запросы до тех пор, пока число обработанных запросов не достигнет значения параметра **MaxReqsPerChild**. После этого процесс прекращает прием новых соединений от ICAP-клиента, заканчивает обработку всех текущих запросов, и завершается.

Другим вариантом завершения работы процесса является его принудительное завершение основным процессом. Это происходит, если количество дочерних процессов, находящихся в состоянии ожидания, превышает значение параметра **IdleChildren**. При этом в первую очередь завершают работу процессы, обработавшие максимальное количество запросов.

Типичные схемы развертывания программы

Данный раздел содержит описание двух основных схем развертывания Антивируса Касперского:

- установка на один сервер с прокси;
- установка на выделенный сервер.

Общие рекомендации, описанные в данных примерах, позволят вам настроить Антивируса Касперского в соответствии со структурой вашей сети.

Установка на один сервер с прокси

Далее в этом документе, рассматривая работу Антивируса Касперского и его настройку, мы будем описывать именно такой вариант работы – на одном сервере с прокси!

Установка на один сервер с прокси позволяет добиться более высокой скорости обработки объектов, за счет того, что передача данных между прокси и Антивирусом Касперского выполняется локально, а не по сети. Данная схема развертывания эффективна при невысокой загруженности прокси-сервера. Если прокси-сервер используется для обслуживания большого числа запросов пользователей, рекомендуется устанавливать программу на отдельный сервер (см. стр. 14), так как антивирусная проверка и обработка являются ресурсоемкими процедурами и могут тем самым отрицательно повлиять на общую производительность прокси-сервера.

При установке программы автоматически выполняется следующая настройка:

1. Антивирус Касперского настраивается на автоматический запуск при загрузке операционной системы и ожидание запросов со стороны прокси на порт 1344 для всех сетевых интерфейсов сервера.

2. В секцию **ICAP OPTIONS** конфигурационного файла прокси, указанного при инсталляции программы, вносятся следующие строки:

```
icap_enable on

icap_send_client_ip on

icap_service is_kav_resp respmod_precache 0 \

icap://localhost:1344/av/respmod
```

```
icap_service is_kav_req reqmod_precache 0 \

icap://localhost:1344/av/reqmod

icap_class ic_kav is_kav_req is_kav_resp

icap_access ic_kav allow all
```

определяющие, что все запрошенные объекты будут переданы Антивирусу Касперского на порт 1344 локального интерфейса.

Установка на выделенный сервер

Установка программы на выделенный сервер рекомендуется при высокой загруженности прокси-сервера, а также при использовании Антивируса Касперского для обработки трафика нескольких прокси-серверов.

Так как при реализации данной схемы развертывания автоматическая настройка программы и прокси-сервера невозможна, выполните ручную настройку.

Настройка работы со Squid-прокси

Интеграция Антивируса Касперского с выделенным Squid-сервером производится по следующему алгоритму:

1. После установки Антивируса Касперского задайте с помощью параметра **ListenAddress** секции `[icapserver.network]` конфигурационного файла kav4proxy.conf IP-адрес сетевого интерфейса и порт, на котором Антивирус Касперского будет ожидать запросы на антивирусную проверку запрашиваемых объектов от прокси-сервера. По умолчанию Антивирус Касперского ожидает запрос по адресу **localhost:1344**.

   Перед изменением значения параметра **ListenAddress** остановите службу Антивируса Касперского с помощью следующей команды:

   для Linux:

   ```
   # /etc/init.d/kav4proxy stop
   ```

   для FreeBSD:

   ```
   # /usr/local/etc/rc.d/kav4proxy stop
   ```

   Чтобы запустить службу Антивируса Касперского, выполните следующую команду:

   для Linux:

   ```
   # /etc/init.d/kav4proxy start
   ```

   для FreeBSD:

   ```
   # /usr/local/etc/rc.d/kav4proxy start
   ```

2. Внесите следующие изменения в конфигурационный файл прокси:

   - для Squid 3.0:

     a. В секцию `ACCESS CONTROLS` добавьте следующую строку:

        ```
        acl acl_kav_GET method GET
        ```

     b. В секцию `ICAP OPTIONS` добавьте следующие строки:

```
icap_enable on
icap_send_client_ip on
icap_service is_kav_resp respmod_precache 0 \
icap://<ip_address>:<port>/av/respmod
icap_service is_kav_req reqmod_precache 0 \
icap://<ip_address>:<port>/av/reqmod
icap_class ic_kav_resp is_kav_resp
icap_class ic_kav_req is_kav_req
icap_access ic_kav_req allow all !acl_kav_GET
icap_access ic_kav_resp allow all
```

- для Squid 3.1:

```
icap_enable on
icap_send_client_ip on
icap_service is_kav_resp respmod_precache 0 \
icap://<ip_address>:<port>/av/respmod
icap_service is_kav_req reqmod_precache 0 \
icap://<ip_address>:<port>/av/reqmod
adaptation_access is_kav_req allow all
adaptation_access is_kav_resp allow all
```

где `<ip_address>` – IP-адрес сервера, на котором установлен Антивирус Касперского; `<port>` – порт, на котором Антивирус Касперского ожидает запросы на антивирусную проверку от прокси-сервера.

Интеграция Антивируса Касперского с Squid 3.1.6 не поддерживается. Более подробная информация приведена на сайте http://bugs.squid-cache.org/show_bug.cgi?id=3011.

3. Перезапустите прокси.

УСТАНОВКА ПРОГРАММЫ

Прежде чем приступить к установке Антивируса Касперского, мы рекомендуем вам:

1. Убедиться, что система соответствует аппаратным и программным требованиям для установки Антивируса Касперского (см. стр. 6).

2. Войти в систему с правами пользователя **root**.

В ЭТОМ РАЗДЕЛЕ

УСТАНОВКА НА СЕРВЕР ПОД УПРАВЛЕНИЕМ LINUX

Антивирус Касперского для серверов под управлением операционной системы Linux распространяется в двух форматах:

- **.rpm** – для систем, поддерживающих RPM Package Manager;
- **.deb** – для дистрибутивов, поддерживающих систему управления пакетами dpkg.

Чтобы установить Антивирус Касперского из rpm-пакета, выполните следующую команду:

```
# rpm –i kav4proxy-<версия дистрибутива>.i386.rpm
```

Чтобы установить Антивирус Касперского из deb-пакета, выполните следующую команду:

```
# dpkg –i kav4proxy-<версия дистрибутива>.deb
```

Чтобы установить Антивирус Касперского из deb-пакета на 64-битную операционную систему, выполните следующую команду:

```
# dpkg –i --force-architecture kav4proxy-<версия дистрибутива>.deb
```

В процессе инсталляции потребуется указать дополнительные сведения (см. стр. 17), необходимые для подключения к интернету, загрузки баз и настройки взаимодействия с прокси-сервером.

УСТАНОВКА НА СЕРВЕР ПОД УПРАВЛЕНИЕМ FREEBSD

Для серверов, работающих под управлением операционной системы FreeBSD, дистрибутив Антивируса Касперского поставляется в tgz-пакете.

Чтобы установить Антивирус Касперского из tgz-пакета, выполните следующую команду:

```
# pkg_add kav4proxy-<версия дистрибутива>.tgz
```

В процессе инсталляции потребуется указать дополнительные сведения (см. стр. 17), необходимые для подключения к интернету, загрузки баз и настройки взаимодействия с прокси-сервером.

Процесс установки

Алгоритмы, описанные в этом разделе, предполагают, что на сервере уже установлен прокси-сервер Squid 3.0 или выше.

Интеграция Антивируса Касперского с Squid 3.1.6 не поддерживается. Более подробная информация приведена на сайте http://bugs.squid-cache.org/show_bug.cgi?id=3011.

Установка Антивируса Касперского производится в два этапа. Первый этап выполняется в автоматическом режиме после выполнения команд, описанных в разделах Установка на сервер под управлением Linux (на стр. 16) и Установка на сервер под управлением FreeBSD (на стр. 16), и включает в себя следующие шаги:

1. Создание группы **klusers** и пользователя **kluser**, с правами которых будет запускаться и работать Антивирус Касперского.

2. Установка файлов дистрибутива на компьютер.

3. Регистрация сервисов, необходимых для работы Антивируса Касперского.

Постинсталляционная настройка

Вторым этапом установки Антивируса Касперского является постинсталляционная настройка, включающая в себя настройку программы и настройку прокси-сервера. Для запуска настройки используйте скрипт postinstall.pl, расположенный в директории /opt/kaspersky/kav4proxy/lib/bin/setup. После запуска скрипта вам будет предложено выполнить следующие действия:

1. Указать путь к файлу ключа.

2. Настроить параметры прокси-сервера, используемого для подключения к интернету, в формате

   `http://<IP-адрес прокси_сервера>:<порт>`

   или

   `http://<имя_пользователя>:<пароль>@<IP-адрес_прокси_сервера>:<порт>,`

   в зависимости от того, требует ли прокси-сервер аутентификации. Это значение используется компонентом обновления (keepup2date) для подключения к серверам Лаборатории Касперского и скачивания обновлений баз.

   Если вы не используете прокси-сервер для подключения к интернету, то задайте значение **no** для этого параметра.

3. Скопировать обновления баз с серверов Лаборатории Касперского. Укажите значение **yes** или **no**, в зависимости от того, хотите ли вы выполнить обновление сейчас. После копирования обновления вам будет предложено настроить автоматическое обновление баз. По умолчанию автоматическое обновление будет выполняться каждый час.

4. Настроить работу с Webmin.

5. Выполнить интеграцию Антивируса Касперского с прокси-сервером. Укажите одно из следующих значений:

   - **No integration**. В этом случае интеграция не выполняется.

- **Configure to work with remote proxy**. В этом случае вам будет предложено ввести адрес удаленного прокси-сервера в формате `<доменое имя|IP-адрес>:<порт>` или **cancel** для отмены интеграции. По умолчанию предлагается адрес 0.0.0.0:1344 (получать и отправлять данные с порта 1344 всех сетевых адаптеров).

- **Configure Squid manually**. В этом случае вам будет предложено выполнить интеграцию вручную. Укажите полный путь к конфигурационному файлу Squid, а затем – путь к исполняемому файлу Squid. После этого подтвердите необходимость интеграции с выбранным прокси-сервером, введя **yes**. Чтобы отказаться от интеграции, введите **no**.

- **Squid (<путь к конфигурационному файлу squid.conf>)**. В этом случае скрипт настройки Антивируса Касперского выполняет интеграцию автоматически.

Если вы отказались от интеграции с прокси-сервером на этом этапе, в дальнейшем вы можете запустить скрипт автоматической интеграции /opt/kaspersky/kav4proxy/lib/bin/setup/proxy_setup.pl.

По завершении процедуры первоначальной настройки на сервере под управлением Linux выполняется запуск службы Антивируса Касперского. В дальнейшем запуск службы происходит автоматически, при старте операционной системы.

На сервере под управлением FreeBSD необходимо запустить службу Антивируса Касперского и настроить ее автоматический запуск вручную.

Чтобы запустить службу Антивируса Касперского и включить ее автоматический запуск на FreeBSD, выполните следующие действия:

1. Добавьте в конфигурационный файл /etc/rc.conf строку `kav4proxy_enable="YES"`.

2. Выполните следующую команду:

   ```
   /usr/local/etc/rc.d/kav4proxy.sh start
   ```

РАБОТА С АНТИВИРУСОМ КАСПЕРСКОГО

Данная глава содержит описание решений типовых задач, возникающих при работе с Антивирусом Касперского, таких как обновление программы, управление лицензиями, обеспечение антивирусной защиты HTTP-трафика, настройка различных параметров антивирусной проверки для групп пользователей. Описанные в разделе задачи раскрывают основные возможности Антивируса Касперского, конкретная реализация конфигурации программы зависит от особенностей организации вашей сети и используемой политики безопасности.

В ЭТОМ РАЗДЕЛЕ

Обновление баз

При обработке объектов, запрашиваемых клиентами через прокси-сервер, Антивирус Касперского использует базы.

Антивирусные базы применяются для поиска и лечения зараженных объектов и содержат описание всех известных на настоящий момент вирусов и способов лечения пораженных ими объектов.

Для обновления баз в состав Антивируса Касперского входит компонент *keepup2date*. Источником обновлений являются сервера обновлений Лаборатории Касперского, такие, как:

http://downloads1.kaspersky-labs.com/

http://downloads2.kaspersky-labs.com/

ftp://downloads1.kaspersky-labs.com/

и другие.

Список адресов, с которых можно копировать обновления, определен в файле *updcfg.xml*, включенном в дистрибутив Антивируса Касперского.

При подключении через прокси-сервер компонент keepup2date поддерживает Basic-аутентификацию.

В процессе обновления компонент keepup2date обращается к списку, выбирает адрес и пытается скопировать с сервера антивирусные базы. Если получить обновления с выбранного адреса невозможно, то Антивирус Касперского обращается по следующему адресу и вновь пытается обновить базы.

Обновления антивирусных баз публикуются на серверах обновлений Лаборатории Касперского каждый час.

После подключения к серверу обновлений компонент keepup2date определяет, для каких баз доступны обновления и скачивает их.

Настоятельно рекомендуется настроить компонент keepup2date на обновление баз каждый час!

После успешного обновления выполняется команда, указанная в качестве значения параметра **PostUpdateCmd** секции `[updater.options]` конфигурационного файла. По умолчанию эта команда запустит автоматическую перезагрузку антивирусных баз. Некорректное изменение данного параметра может привести к тому, что программа либо не будет использовать обновленные базы, либо будет работать некорректно.

Все параметры компонента keepup2date сгруппированы в секциях `[updater.*]` конфигурационного файла.

Если структура вашей локальной сети достаточно сложная и вы используете несколько серверов с установленным на них Антивирусом Касперского, мы рекомендуем каждый час скачивать обновления с серверов обновлений, размещать их в некоторой сетевой директории, а для локальных серверов настроить копирование баз из этой директории (см. стр. 21).

Задача обновления может быть запущена автоматически при помощи программы **cron** (см. стр. 20) или же вручную из командной строки (см. стр. 21). Для запуска keepup2date необходимы права пользователя **root** или **kluser**.

АВТОМАТИЧЕСКОЕ ОБНОВЛЕНИЕ БАЗ

Вы можете спланировать регулярное автоматическое обновление баз при помощи сервиса **cron**. Настройка cron может быть осуществлена как вручную, так и при помощи специального скрипта keepup2date.sh, расположенного в директории /opt/kaspersky/kav4proxy/lib/bin/setup/.

- *Чтобы установить cron-задачу ежечасного обновления антивирусных баз, выполните следующую команду:*

```
# /opt/kaspersky/kav4proxy/lib/bin/setup/keepup2date.sh –install
```

- *Чтобы удалить cron-задачу ежечасного обновления антивирусных баз, выполните следующую команду:*

```
# /opt/kaspersky/kav4proxy/lib/bin/setup/keepup2date.sh –uninstall
```

Пример: вручную задать автоматическое обновление баз каждый час. В системном журнале фиксировать только ошибки, возникающие при работе компонента. Вести общий журнал по всем запускам задачи, на консоль никакой информации не выводить.

Для реализации поставленной задачи выполните следующие действия:

1. В конфигурационном файле Антивируса Касперского задайте соответствующие значения для параметров:

```
[updater.report]

Append=true

ReportLevel=1
```

2. Отредактируйте файл, задающий правила работы процесса cron (crontab -e), а именно: для пользователя root или kluser добавьте например следующую строку:

```
23 * * * * /opt/kaspersky/kav4proxy/bin/kav4proxy-keepup2date -q
```

Указанная настройка времени запуска cron-задачи (каждую двадцать третью минуту часа) является примерной. Рекомендуется задать собственные настройки времени запуска, что позволит избежать перегрузки серверов обновлений.

Разовое обновление баз

В любой момент времени вы можете запустить обновление баз программы из командной строки.

Пример: запустить обновление баз, сохранив результаты работы в файле keepup2date.log, в директории /var/log/kaspersky/kav4proxy/.

Для реализации поставленной задачи войдите в систему с правами пользователя root (или любого другого, имеющего права привилегированного пользователя) и в командной строке введите:

```
# /opt/kaspersky/kav4proxy/bin/kav4proxy-keepup2date -l \

/var/log/kaspersky/kav4proxy/keepup2date.log
```

Если вам необходимо обновить базы на нескольких серверах, удобнее вместо многократного получения баз через интернет получить базы с серверов обновлений один раз, сохранить их в сетевой директории, а затем смонтировать эту директорию в файловой системе каждого из серверов, на которых установлен Антивирус Касперского. Теперь достаточно запустить скрипт обновления, указав предварительно в качестве источника обновлений смонтированную директорию.

Пример: запустить обновление баз из локальной директории /home/kavuser/bases/. Результаты работы вывести в файл /tmp/updatesreport.log.

Для реализации поставленной задачи войдите в систему с правами пользователя root (или любого другого, имеющего права привилегированного пользователя) и выполните следующие действия:

1. Смонтируйте сетевую директорию, содержащую обновления антивирусных баз, в локальную директорию /home/kavuser/bases/.

2. В командной строке введите:

   ```
   # /opt/kaspersky/kav4proxy/bin/kav4proxy-keepup2date -l \

   /tmp/updatesreport.log -g /home/kavuser/bases
   ```

Также все подобные задачи вы можете решить удаленно, с помощью модуля программы Webmin.

Создание сетевой директории для хранения и копирования баз

Для того, чтобы обновления баз из сетевой директории для локальных серверов проходили корректно, вам необходимо создать в этой директории файловую структуру, аналогичную структуре серверов обновлений Лаборатории Касперского.

Пример: создать сетевую директорию, откуда локальные серверы сети будут обновлять антивирусные базы.

Для реализации поставленной задачи войдите в систему с правами пользователя root (или любого другого, имеющего права привилегированного пользователя) и выполните следующие действия:

1. Создайте локальную директорию и предоставьте доступ на запись в эту директорию пользователю **kluser**.

2. Запустите компонент keepup2date следующим образом:

   ```
   # /opt/kaspersky/kav4proxy/bin/kav4proxy-keepup2date -x <rdir>,
   ```

   где `<rdir>` – полный путь к созданной директории.

3. Предоставьте для локальных компьютеров сетевой доступ на чтение данной директории.

Управление лицензиями

Возможность использования Антивируса Касперского определяется наличием файла ключа. Файл ключа входит в комплект поставки и дает вам право использовать Антивирус Касперского со дня приобретения и установки файла ключа.

Проверка наличия установленной лицензии выполняется программой при каждом запуске и перезагрузке баз.

Если файл ключа не установлен или произошла ошибка при загрузке информации об используемой лицензии, Антивирус Касперского переходит в режим работы без лицензии. В данном режиме не выполняется антивирусная проверка объектов, передаваемых через прокси-сервер, и над всеми объектами выполняется действие, заданное параметром **LicenseErrorAction**.

По окончании срока действия лицензии функциональность программы сохраняется за исключением возможности обновления баз. Вы по-прежнему можете выполнять антивирусную проверку и обработку объектов, но используя базы, актуальные на дату окончания лицензии. Следовательно, вы не будете защищены от новых вирусов, появившихся после окончания действия лицензии.

Чтобы избежать заражения новыми вирусами, мы рекомендуем вам продлить лицензию на использование Антивируса Касперского.

Файл ключа дает вам право на использование Антивируса Касперского и содержит всю необходимую информацию, связанную с лицензией, которую вы приобрели, такую как: тип лицензии, дата окончания срока ее действия, информацию о дистрибьюторах и т.д.

Помимо прав на использование программы в течение срока действия лицензии вы приобретаете следующие возможности:

- круглосуточную техническую поддержку;
- ежечасное обновление баз;
- своевременное информирование о новых вирусах.

Поэтому крайне важно вовремя продлевать лицензию на использование Антивируса Касперского. Существует также возможность установить резервный ключ, который Антивирус Касперского начнет использовать по истечении срока действия активного файла ключа.

Просмотр информации о лицензии

Просматривать информацию об установленных файлах ключей вы можете в отчете о работе компонента kavicapserver. При старте kavicapserver загружает информацию о ключах и выводит ее в отчет. Файл отчета kavicapserver.log расположен в директории /var/log/kaspersky/kav4proxy/.

Более полная информация о состоянии файлов ключей может быть получена при помощи специального компонента licensemanager, входящего в состав Антивируса Касперского.

Вся информация о файлах ключей может быть выведена на консоль сервера или просмотрена удаленно с любого компьютера сети с помощью модуля программы Webmin.

➧ *Чтобы просмотреть информацию обо всех установленных файлах ключей, выполните следующую команду:*

```
# /opt/kaspersky/kav4proxy/bin/kav4proxy-licensemanager -s
```

На консоль сервера будет выведена информация подобного рода:

```
Kaspersky license manager for Linux. Version 5.5.85/RELEASE #59

(C) 1997-2012 Kaspersky Lab ZAO. All Rights Reserved.

Registered trademarks and service marks are the property of their respective owners.



License info:

Product name: Kaspersky Anti-Virus for xSP International Edition. 1000-1499 Mb of
traffic per day 1 year NFR Traffic Licence: Anti-Virus for Proxy Server

Invalid reason: Expired


Active key info:

Key file:        070C3064.key

Install date:    24-05-2012 UTC

Product name:    Kaspersky Anti-Virus for xSP International Edition. 1000-1499 Mb of
traffic per day 1 year NFR Traffic Licence: Anti-Virus for Proxy Server

Creation date:   03-11-2009 UTC

Expiration date: 03-11-2011 UTC

Serial:          0F92-0004AA-070C3064

Type:            Commercial

Count:           1024

Lifespan:        365

Objs:            3:1024
```

- *Чтобы просмотреть информацию о файле ключа, выполните следующую команду:*

```
# /opt/kaspersky/kav4proxy/bin/kav4proxy-licensemanager -k 070C2FB1.key,
```

где `070C2FB1.key` – имя файла ключа.

На консоль сервера будет выведена информация подобного рода:

```
Kaspersky license manager for Linux. Version 5.5.85/RELEASE #59

(C) 1997-2012 Kaspersky Lab ZAO. All Rights Reserved.

Registered trademarks and service marks are the property of their respective owners.

Product name:    Kaspersky Anti-Virus for xSP International Edition. 1000-1499 Mb of
traffic per day 1 year NFR Traffic Licence: Anti-Virus for Proxy Server

Creation date:   03-11-2009
```

```
Expiration date: 03-11-2011

Serial:          0F92-0004AA-070C2FB1

Type:            Commercial

Count:           250

Lifespan:        365

Objs:            3:250
```

- *Чтобы просмотреть подробную информацию о состоянии лицензии, выполните следующую команду:*

```
# /opt/kaspersky/kav4proxy/bin/kav4proxy-licensemanager -i
```

На консоль сервера будет выведена информация, зависящая от типа лицензии. Например, в случае использования лицензирования по трафику:

```
Kaspersky license manager for Linux. Version 5.5.85/RELEASE #59

(C) 1997-2012 Kaspersky Lab ZAO. All Rights Reserved.

Registered trademarks and service marks are the property of their respective owners.


Licensed traffic units: 250 (MB)

Traffic units used: 0 (MB)

Traffic units left: 250 (MB)
```

ПРОДЛЕНИЕ ЛИЦЕНЗИИ

Продление лицензии на использование Антивируса Касперского дает вам право на восстановление полной функциональности Антивируса Касперского. Возобновляется период действия дополнительных услуг (см. стр. 22).

Срок действия лицензии зависит от типа лицензирования, который вы выбрали, приобретая Антивирус Касперского, а также от продукта, в составе которого вы приобрели Антивирус Касперского.

- *Чтобы продлить лицензию на использование Антивируса Касперского, выполните одно из следующих действий:*

  - свяжитесь с компанией, у которой вы купили Антивирус Касперского, и продлите лицензию на использование Антивируса Касперского.

  - продлите лицензию непосредственно в Лаборатории Касперского, написав в Отдел продаж (sales@kaspersky.com) или заполнив соответствующую форму на нашем сайте (www.kaspersky.ru) в разделе **Электронный магазин** → **Продлить лицензию**. По факту оплаты вам будет отправлен файл ключа по электронной почте, адрес которой был указан вами в форме заказа.

Регулярно Лаборатория Касперского проводит акции, позволяющие продлевать лицензии на использование наших продуктов со значительными скидками. Следите за акциями на сайте Лаборатории Касперского в разделе **Продукты** → **Акции** и спецпредложения.

- *Чтобы установить новый файл ключа, выполните следующую команду:*

```
# /opt/kaspersky/kav4proxy/bin/kav4proxy-licensemanager -a 00053E3D.key,
```

где `00053E3D.key` – имя файла ключа.

В случае успешной установки файла ключа на консоль сервера будет выведена следующая информация:

```
Kaspersky license manager. Version 5.5.3/RELEASE

Copyright (C) Kaspersky Lab. 1997-2009.

Key file 00053E3D.key is successfully registered
```

После этого рекомендуем вам обновить базы.

Если вы хотите установить новый файл ключ до истечения срока действия текущего, вы можете добавить его в качестве резервного. Резервный файл ключ начинает свою работу после истечения срока действия активного файла ключа. Срок действия резервного файла ключа начинает отсчитываться с момента его активации. Можно установить только один резервный файл ключа.

Если вы установили два файла ключа (активный и резервный), то при запросе информации о лицензии на консоль сервера будет выводиться информация как об активном, так и о резервном файлах ключей.

УДАЛЕНИЕ ФАЙЛА КЛЮЧА

- *Чтобы удалить активный файл ключа, в командной строке введите:*

```
# /opt/kaspersky/kav4proxy/bin/kav4proxy-licensemanager -da
```

В случае успешного удаления на консоль сервера будет выведена следующая информация:

```
Kaspersky license manager. Version 5.5.3/RELEASE

Copyright (C) Kaspersky Lab. 1997-2009.

Active key was successfully removed
```

- *Чтобы удалить дополнительный файл ключа, в командной строке введите:*

```
# /opt/kaspersky/kav4proxy/bin/kav4proxy-licensemanager -dr
```

На консоль сервера будет выведена следующая информация:

```
Kaspersky license manager. Version 5.5.3/RELEASE

Copyright (C) Kaspersky Lab. 1997-2009.

Additional key was successfully removed
```

ИСПОЛЬЗОВАНИЕ УПРАВЛЯЮЩЕГО СКРИПТА

Управляющий скрипт kav4proxy, расположенный в директории /etc/init.d/, применяется для запуска, останова и выполнения перезагрузки Антивируса Касперского. Управляющий скрипт kav4proxy использует следующие ключи командной строки:

- **start** – запустить Антивирус Касперского. Если программа уже запущена, выполнение скрипта kav4proxy останавливается. Если программа не запущена, выполняется проверка конфигурационного файла и запуск Антивируса Касперского. Код возврата **0** сообщает об успешном старте.

- **stop** – остановить Антивирус Касперского. Перед остановкой выполняется проверка, запущена программа или нет (по ID процесса). Если программа запущена, выполняется сигнал SIGTERM. Если по истечении 30 секунд программа не будет остановлена, выполняется сигнал SIGKILL. Результатом успешного выполнения является код возврата **0**.

- **restart** – выполнить останов и запуск Антивируса Касперского в соответствии с ключами stop и start.
- **reload** – выполнить перезагрузку конфигурации и баз Антивируса Касперского посредством сигнала SIGHUP.
- **reload_avbase** – выполнить только перезагрузку баз и проверить корректность файла ключа.
- **stats** – выполнить запись показаний счетчиков статистики (см. стр. 37) в файл, а также переключить запись отчета в новый файл (см. стр. 38).

Обеспечение антивирусной защиты HTTP-трафика

Антивирус Касперского не проверяет данные, передаваемые по протоколу HTTPS.

Пример: настроить антивирусную проверку HTTP-трафика прокси-сервера, установленного на один сервер с Антивирусом Касперского, согласно следующим требованиям:

- использовать общие параметры антивирусной проверки для всех запросов;
- включить режим лечения зараженных объектов;
- отключить режим проверки почтовых баз;
- включить режимы проверки упакованных и архивных объектов;
- запретить доступ к зараженным, подозрительным и поврежденным объектам, а также объектам, содержащим код, похожий на код известного вируса;
- использовать режим partial при обработке запросов прокси-сервера;
- отключить антивирусную проверку объектов, запрашиваемых с веб-сервера www.example.com;
- сохранять статистические данные о результатах антивирусной проверки в файл /var/log/kaspersky/kav4proxy/statistic.

Чтобы реализовать поставленную задачу, выполните следующие действия:

1. Установите Антивирус Касперского на один сервер с прокси-сервером (см. стр. 13) и выполните постинсталляционную настройку (см. стр. 17).
2. Задайте следующие значения параметров конфигурационного файла kav4proxy.conf (значения параметров, не указанных в примере, оставьте без изменения):

```
[icapserver.filter]

ExcludeURL=^www\.example\.com\/.*



[icapserver.engine.options]

ScanPacked=true

ScanArchives=true

ScanMailBases=false
```

```
ScanMailPlain=false

Cure=true


[icapserver.actions]

InfectedAction=deny

SuspiciousAction=deny

WarningAction=deny

ErrorAction=skip

ProtectedAction=skip

CorruptedAction=skip


[icapserver.protocol]

AnswerMode=partial


[icapserver.statistics]

AVStatisticsFile=/var/log/kaspersky/kav4proxy/statistic
```

3. Перезапустите Антивирус Касперского, выполнив следующую команду:

```
# /etc/init.d/kav4proxy restart
```

Настройка параметров антивирусной проверки для групп пользователей

Пример, приведенный в предыдущем разделе (см. стр. 26), предполагает настройку общих параметров антивирусной обработки для всех запросов, производимых пользователями через прокси-сервер. Антивирус Касперского позволяет использовать группы для настройки различных параметров антивирусной проверки для отдельных пользователей.

Пример: настроить программу на выполнение антивирусной проверки HTTP-трафика согласно следующим требованиям:

- для группы **managers**, включающей в себя компьютеры, использующие IP-адреса подсети 192.168.1.0/255.255.255.0, задать следующие параметры антивирусной проверки:
  - отключить режимы проверки упакованных и архивных файлов, а также почтовых баз;
  - включить режим лечения зараженных объектов;
  - разрешить доступ только к незараженным и вылеченным объектам.
- для группы **sales**, включающей в себя компьютеры, использующие IP-адреса подсети 192.168.2.0/255.255.255.0, задать следующие параметры антивирусной проверки:

- выполнять проверку всех объектов;
- включить режим лечения зараженных объектов;
- запретить доступ к зараженным, подозрительным и поврежденным объектам, а также объектам, содержащим код, похожий на код известного вируса.

- для всех остальных пользователей задать следующие пара-метры антивирусной проверки:
  - отключить режим проверки почтовых баз;
  - отключить режим лечения зараженных объектов;
  - разрешить доступ только к объектам, получившим по результатам проверки статус *OK* (см. стр. 33).

Чтобы реализовать поставленную задачу, выполните следующие действия:

1. Создайте в конфигурационном файле kav4proxy.conf следующие секции, содержащие параметры антивирусной проверки для группы **managers**:

```
[icapserver.groups:managers]

Priority=1

ClientIP=192.168.1.0/255.255.255.0

URL=.*


[icapserver.engine.options:managers]

ScanPacked=false

ScanArchives=false

ScanMailBases=false

ScanMailPlain=false

Cure=true


[icapserver.actions:managers]

InfectedAction=deny

SuspiciousAction=deny

WarningAction=deny

ErrorAction=deny

ProtectedAction=deny

CorruptedAction=deny
```

2. Создайте в конфигурационном файле kav4proxy.conf следующие секции, содержащие параметры антивирусной проверки для группы **sales**:

```
[icapserver.groups:sales]
Priority=2
ClientIP=192.168.2.0/255.255.255.0
URL=.*

[icapserver.engine.options:sales]
ScanPacked=true
ScanArchives=true
ScanMailBases=true
ScanMailPlain=true
Cure=true

[icapserver.actions:sales]
InfectedAction=deny
SuspiciousAction=deny
WarningAction=deny
ErrorAction=skip
ProtectedAction=skip
CorruptedAction=deny
```

3. Задайте следующие значения параметров для группы по умолчанию:

```
[icapserver.engine.options]
ScanPacked=true
ScanArchives=true
ScanMailBases=false
ScanMailPlain=false
Cure=false

[icapserver.actions]
InfectedAction=deny
SuspiciousAction=deny
WarningAction=deny
```

```
ErrorAction=deny

ProtectedAction=deny

CorruptedAction=deny
```

4. Перезапустите Антивируса Касперского, выполнив следующую команду:

```
# /etc/init.d/kav4proxy restart
```

ДОПОЛНИТЕЛЬНАЯ НАСТРОЙКА АНТИВИРУСА КАСПЕРСКОГО

В этом разделе подробно освещена настройка основных параметров Антивируса Касперского. В отличие от необходимых настроек, выполняемых в процессе установки и постинсталляционной настройки, без которых использование Антивируса Касперского невозможно, дополнительная настройка осуществляются по усмотрению администратора. Она направлена на расширение возможностей Антивируса Касперского и его адаптацию согласно политике безопасности вашей компании.

В ЭТОМ РАЗДЕЛЕ

Создание групп

Использование групп позволяет администратору определить различные параметры антивирусной обработки объектов, запрашиваемых или передаваемых через прокси-сервер, для различных групп пользователей. Принадлежность запроса к той или иной группе определяется IP-адресом клиентского компьютера, запросившего объект через прокси-сервер, и URL запрашиваемого объекта.

Убедитесь, что в конфигурационном файле Squid параметру **icap_send_client_ip** присвоено значение **on**. Это значение указывает, что Squid выполняет передачу IP-адреса клиента Антивирусу Касперского.

Если параметры запроса не подпадают под область действия ни одной из групп, то Антивирус Касперского выполняет обработку объекта согласно правилам, заданным в группе по умолчанию.

Параметры каждой из групп расположены в следующих пяти секциях конфигурационного файла Антивируса Касперского:

- `[icapserver.groups:<имя группы>]` – содержит параметры, задающие область действия группы (IP-адреса клиентов, URL объектов) и ее приоритет;
- `[icapserver.filter:<имя группы>]` – содержит правила фильтрации для группы <имя группы>;

- [icapserver.engine.options:<имя группы>] – содержит параметры антивирусной проверки, согласно которым обрабатываются объекты, попадающие в область действия группы;

- [icapserver.actions:<имя группы>] – содержит параметры, определяющие действия Антивируса Касперского над объектами в зависимости от статуса, присвоенного им в процессе антивирусной проверки;

- [icapserver.notify:<имя группы>] – содержит параметры оповещения администратора о заблокированных объектах (в отношении которых было выполнено действие **deny**).

Параметры группы, используемой Антивирусом Касперского по умолчанию, расположены в секциях [icapserver.groups], [icapserver.filter], [icapserver.options], [icapserver.actions] и [icapserver.notify].

При создании новой группы нет необходимости определять все ее параметры. При отсутствии некоторых параметров (или секций) программа будет использовать значения по умолчанию.

Пример: создать группу **managers** для задания правил обработки запрашиваемых объектов от клиентских компьютеров, использующих подсеть 192.168.10.0/255.255.255.0. Для этой группы запрещать доступ ко всем объектам, кроме незараженных, вылеченных и защищенных паролем. Задать приоритет этой группы **2**. Для всех остальных параметров использовать значения по умолчанию.

Для реализации поставленной задачи войдите в систему с правами пользователя **root** (или любого другого, имеющего права привилегированного пользователя) и создайте следующие секции в конфигурационном файле kav4proxy.conf:

```
[icapserver.groups:managers]

Priority=2

ClientIP=192.168.10.0/255.255.255.0

URL=.*



[icapserver.engine.options:managers]

Cure=true



[icapserver.actions:managers]

ErrorAction=deny

ProtectedAction=skip
```

Параметры антивирусной проверки

Параметры антивирусного ядра, расположенные в секции [icapserver.engine.options:<имя группы>], задают следующие режимы проверки и лечения запрашиваемых объектов для соответствующей группы:

- **ScanPacked=true|false** – включает / отключает режим проверки упакованных файлов. При отключении этого режима все упакованные объекты считаются незараженными.

- **ScanArchives=true|false** – включает / отключает режим проверки объектов в архивах. При отключении этого режима все архивные файлы считаются незараженными.

- **ScanSFXArchives=true|false** – включает / отключает режим проверки самораспаковывающихся архивов (архивов, имеющих в своем составе исполняемый модуль распаковщик, self-extracting archives). При отключении этого режима все самораспаковывающиеся архивы считаются незараженными.

- **ScanMailBases=true|false** – включает / отключает режим проверки почтовых баз (запрашиваемых или передаваемых через прокси-сервер). При отключении этого режима все почтовые базы считаются незараженными.

- **ScanMailPlain=true|false** – включает / отключает режим проверки почтовых баз в формате plain text (запрашиваемых или передаваемых через прокси-сервер). При отключении этого режима все почтовые базы в виде plain text считаются незараженными.

- **UseAnalyzer=yes|no** – включает / отключает режим использования эвристического анализатора при антивирусной проверке.

- **HeuristicLevel=Recommended|Light|Deep|Medium** – устанавливает уровень детализации проверки с помощью эвристического анализатора. Уровень детализации обеспечивает баланс между тщательностью поиска новых угроз, степенью загрузки ресурсов операционной системы и временем проверки. Чем выше установлен уровень детализации проверки, тем больше ресурсов она потребует и больше времени займет. Возможные значения:

  - **Light** – наименее тщательная проверка, минимальная загрузка системы;

  - **Medium** – средняя глубина проверки, сбалансированная загрузка системы;

  - **Deep** – наиболее тщательная проверка, максимальная загрузка системы;

  - **Recommended** – рекомендуемое значение.

- **Cure=true|false** – включает / отключает режим лечения зараженных объектов. При отключении режима лечения программа не выполняет попыток вылечить зараженный объект.

- **MaxScanTime** – максимальное время проверки объекта. Если за указанное время проверка не завершена, объекту присваивается статус *ERROR*.

Выбор действий над проверенными объектами

Действие, применяемое Антивирусом Касперского в отношении проверенного объекта, определяется статусом, присвоенным ему в результате антивирусной проверки.

Антивирус Касперского использует следующие статусы:

- **OK** – объект успешно прошел проверку и не заражен;

- **INFECTED** – объект инфицирован и не может быть вылечен, либо лечение не проводилось;

- **CURED** – объект был инфицирован и успешно вылечен;

- **WARNING** – объект содержит код, похожий на код известного вируса;

- **SUSPICIOUS** – объект подозревается на заражение неизвестным вирусом;

- **PROTECTED** – объект защищен паролем и поэтому не может быть проверен;

- **CORRUPTED** – объект поврежден;

- **ERROR** – проверка объекта завершилась ошибкой.

Для определения действия, выполняемого Антивирусом Касперского в отношении объектов с определенным статусом, служат параметры, расположенные в секции `[icapserver.actions]` (для группы по умолчанию) и `[icapserver.actions:<имя группы>]` (для групп, созданных администратором):

- **InfectedAction** – действие над зараженным объектом, который не может быть вылечен, или лечение которого не проводилось.
- **SuspiciousAction** – действие над объектом, который подозревается на заражение неизвестным вирусом.
- **WarningAction** – действие над объектом, содержащим код, похожий на код известного вируса.
- **ErrorAction** – действие над объектом, получившим статус *ERROR*.
- **ProtectedAction** – действие над объектом, защищенным паролем.
- **CorruptedAction** – действие над поврежденным объектом.
- **CuredAction** – действие над вылеченным объектом.

В качестве значений перечисленных параметров, могут быть использованы следующие значения:

- **skip** – разрешить передачу объекта;
- **deny** – запретить передачу объекта, заменив его на соответствующий файл уведомления.

Если в отношении объекта используется действие **deny**, то в зависимости от статуса объекта, он будет заменен одним из следующих шаблонных файлов:

- **object_infected** – шаблон, содержащий уведомление об обнаружении зараженного объекта.
- **object_suspicious** – шаблон, содержащий уведомление об обнаружении объекта, подозреваемого на заражение неизвестным вирусом.
- **object_warning** – шаблон, содержащий уведомление об обнаружении объекта, содержащего код, похожий на код известного вируса.
- **object_protected** – шаблон, содержащий уведомление об обнаружении защищенного паролем объекта.
- **object_error** – шаблон, содержащий уведомление об обнаружении объекта, проверка которого завершилась ошибкой.
- **object_corrupted** – шаблон, содержащий уведомление об обнаружении поврежденного объекта.
- **object_cured** – шаблон, содержащий уведомление об обнаружении объекта, который был заражен и успешно вылечен.

У администратора есть возможность изменять текст этих шаблонов по своему усмотрению, в том числе добавляя специальные макросы (см. стр. 55).

Пример: задать для группы по умолчанию следующие действия над проверяемыми объектами:

- разрешить передачу объектов, получивших статус *CURED* и *PROTECTED*;
- запретить передачу всех остальных объектов.

Решение: для реализации поставленной задачи войдите в систему с правами пользователя **root** (или любого другого, имеющего права привилегированного пользователя) и задайте следующие значения параметров секции `[icapserver.actions]`:

```
[icapserver.actions]
```

```
CuredAction=skip

ProtectedAction=skip

InfectedAction=deny

SuspiciousAction=deny

WarningAction=deny

ErrorAction=deny

CorruptedAction=deny
```

Уведомление администратора

Каждый раз, когда к объекту, передаваемому через прокси сервер, применяется действие **deny**, Антивирус Касперского выполняет запуск специального скрипта. Пример такого скрипта находится по адресу: /opt/kaspersky/kav4proxy/share/examples/notify.sh. Для задания строки запуска скрипта служит параметр **NotifyScript**, расположенный в секции `[icapserver.notify:<имя группы>]` конфигурационного файла Антивируса Касперского.

Далее приводится пример создания скрипта уведомления и настройка программы для запуска скрипта.

Используя язык SHELL, администратор может создать собственные скрипты, которые будут выполняться каждый раз, когда по результатам проверки передача объекта через прокси-сервер будет заблокирована. При этом для каждой из созданных администратором групп может быть определен собственный скрипт уведомления (см. стр. 31).

- *Чтобы настроить программу на отправку уведомления о заблокированных объектах на почтовый адрес admin@test.local, выполните следующие действия:*

1. Создайте исполняемый скрипт-файл следующего содержания:

```
#!/bin/sh

recipients='admin@test.local'


action=%ACTION%

verdict=%VERDICT%


sendmail -t -i<<EOT

From: Kaspersky Anti-Virus For Linux Proxy Server <root@$HOSTNAME>

To: $recipients

Subject: $verdict object requested


Action applied: $action

Verdict: $verdict
```

```
Requested URL: %URL%

Client IP: %CLIENT_ADDR%


Found:

    Infected:  %VIRUS_LIST%

    Cured:     %CURED_LIST%

    Suspicious: %SUSP_LIST%

    Warnings:  %WARN_LIST%


This message generated by %PRODUCT% at %DATE% on $HOSTNAME

EOT
```

При создании скрипта допускается использование специальных макросов (см. стр. 55), таких как %URL%, %CLIENT_ADDR% и других, для указания дополнительных сведений.

2. Сохраните скрипт-файл и убедитесь, что он может быть выполнен пользователем **kluser**.

3. Укажите строку запуска скрипта в качестве значения параметра **NotifyScript**. Например, если скрипт был сохранен в файле /usr/local/bin/notify.sh, и его запуск должен выполняться при блокировании объектов, обрабатываемых по правилам группы по умолчанию, задайте следующее значение параметра **NotifyScript** в секции `[icapserver.notify]`:

```
[icapserver.notify]

NotifyScript=/usr/local/bin/notify.sh
```

Дистрибутив программы содержит набор шаблонов уведомлений, которые могут быть использованы при создании скриптов, в директории /opt/kaspersky/kav4proxy/share/notify.

РЕЖИМЫ РАБОТЫ ПРОГРАММЫ

В зависимости от состояния лицензии (см. раздел «Управление лицензиями» на стр. 22) и баз Антивирус Касперского может работать в одном из следующих режимов:

- **Основной режим** – полнофункциональный режим работы Антивируса Касперского. В этом режиме программа выполняет антивирусную проверку трафика прокси-сервера и, если задано, лечение зараженных объектов.

- **Без обновления** – режим, используемый Антивирусом Касперского после истечения срока действия используемой лицензии. В этом режиме Антивирус Касперского выполняет антивирусную проверку трафика прокси-сервера и, если задано, лечение зараженных объектов с использованием баз, актуальных на дату окончания лицензии.

- **Без лицензии** – режим, используемый Антивирусом Касперского в том случае, если не установлен файл ключа или произошла ошибка при загрузке информации об используемой лицензии. В этом режиме не выполняется антивирусная проверка трафика прокси-сервера, а ко всем объектам применяется действие, определенное параметром **LicenseErrorAction**.

- **Без антивирусных баз** – режим, используемый Антивирусом Касперского в том случае, если не установлены базы или произошла ошибка при загрузке баз. В этом режиме не выполняется антивирусная проверка трафика прокси-сервера, а ко всем объектам применяется действие, определенное параметром **BasesErrorAction**.

Режимы работы с прокси-сервером по ICAP-протоколу

Режим работы Антивируса Касперского с прокси-сервером определяется параметром **AnswerMode** в секции `[icapserver.protocol]` конфигурационного файла kav4proxy.conf, который может принимать следующие значения:

- **partial** – в этом режиме Антивирус Касперского с периодичностью, определяемой параметром **MaxSendDelayTime**, выполняет отправку прокси-серверу частей проверяемого объекта для дальнейшей передачи их пользователю. Последняя часть объекта передается пользователю лишь после завершения антивирусной проверки объекта, и только если согласно полученному статусу к объекту не применяется действие **deny**. Если к объекту применяется действие **deny**, то пользователю не высылается шаблонный файл (см. стр. 33), а соединение разрывается.

  Описанный режим удобен при скачивании файлов большого размера, так как при этом пользователь начинает получать объект еще до завершения антивирусной проверки, иначе пользователь может разорвать соединение, не дождавшись ответа.

- **complete** – в этом режиме Антивирус Касперского возвращает объект прокси-серверу для дальнейшей передачи его пользователю лишь после того, как он будет полностью загружен и проверен, и если согласно полученному статусу к объекту не применяется действие **deny**. Если по результатам антивирусной проверки к объекту применяется действие **deny**, то вместо запрошенного объекта пользователю возвращается шаблонный файл (см. стр. 33).

  При использовании режима **complete** следует учитывать, что после щелчка по объекту в браузере, пользователю не будет выведено окно с предложением сохранить объект или отменить загрузку до тех пор, пока объект не будет полностью загружен прокси-сервером и проверен Антивирусом Касперского. Отменить загрузку пользователь может, лишь закрыв окно браузера и разорвав тем самым соединение.

Ведение статистики работы программы

Антивирус Касперского предоставляет администратору два вида статистической информации:

- статистика по результатам антивирусной проверки и обработки;
- общая статистика работы Антивируса Касперского.

Для записи статистики антивирусной обработки может быть использован как локальный файл, так и сетевой сокет. Для того чтобы настроить Антивирус Касперского на запись статистики в локальный файл, укажите путь к этому файлу в качестве значения параметра **AVStatisticsFile**. Для задания сетевого сокета служит параметр **AVStatisticsAddress**.

Каждая строка в созданном файле статистики будет содержать информацию об одном проверенном объекте в следующем формате:

`<LEN><tab><RESULT><tab><METHOD><tab><ICAP_CLIENT_IP><tab>`
`<HTTP_USER_NAME><tab><HTTP_USER_IP><tab><URL>`, где `<tab>` – символ табуляции.

Значения каждого из параметров приведены в таблице ниже.

Таблица 1. Параметры статистики

Символическое имя	Значение
<LEN>	Длина запроса, в байтах.
<RESULT>	Результат антивирусной проверки объекта.
<METHOD>	Режим обработки ICAP-запроса (RESPMOD или REQMOD).
<ICAP_CLIENT_IP>	IP-адрес ICAP-клиента, запросившего объект.
<HTTP_USER_NAME>	Имя HTTP-пользователя, запросившего объект.
<HTTP_USER_IP>	IP-адрес HTTP-пользователя, запросившего объект.
<URL>	URL запрошенного объекта.

Если по каким-либо причинам вывод отчета об обработанном объекте невозможен, информация об объекте не фиксируется.

Помимо статистики антивирусной проверки Антивирус Касперского также использует специальные счетчики, предоставляющие статистическую информацию о работе Антивируса Касперского. Для вывода значений счетчиков в файл служит параметр **CounterStatisticsFile** конфигурационного файла программы. В указанном файле будут фиксироваться показания счетчиков, описанных в таблице ниже.

Таблица 2. Счетчики работы Антивируса Касперского

Счетчик	Описание
Total_requests	Общее количество обработанных запросов на проверку.
Infected_requests	Количество запросов, обработка которых выявила инфицированные или подозрительные объекты, а также объекты, содержащие код, похожий на код известного вируса.
Protected_requests	Количество запросов, обработка которых выявила защищенные объекты.
Error_requests	Количество запросов, обработка объектов которых завершилась ошибкой.
Proccessed_traffic	Общее количество обработанного трафика, включая служебный (в МБ).
Clean_traffic	Общее количество незараженного трафика (в МБ).
Infected_traffic	Общее количество зараженного трафика (в МБ).
Traffic_per_min	Среднее количество МБ в минуту.
Request_per_min	Среднее количество обработанных ICAP-запросов в минуту.
Engine_errors	Количество ошибок, возникших при работе антивирусного ядра.
Total_connections	Количество активных соединений с ICAP сервером.
Total_processes	Общее количество запущенных процессов обработки запросов пользователей.
Idle_processes	Количество процессов обработки запросов, находящихся в состоянии ожидания.

Параметры формирования отчета

Результаты работы Антивируса Касперского фиксируются в отчете, который выводится в лог-файл Антивируса Касперского в текстовом формате (параметр **ReportFileName** секции `[icapserver.report]`) или в системный журнал (**syslog**). Если значением параметра **ReportFileName** является пустая строка (**ReportFileName=**), информация о работе Антивируса Касперского не фиксируется.

Объем выводимой информации вы можете откорректировать путем изменения уровня детализации отчета (параметр **ReportLevel** в секции `[icapserver.report]`).

Уровень детализации представляет собой число, определяющее степень конкретизации информации о работе компонентов в отчете. Каждый последующий уровень включает в себя информацию предыдущего и некоторую дополнительную.

Возможные уровни детализации отчета перечислены в таблице ниже.

Таблица 3. Уровни детализации отчета

Уровень	Название уровня	Буквенное обозначение уровня	Значение
0	Fatal Errors	F	Информация только о критических ошибках (ошибках, которые приводят к завершению работы программы из-за невозможности выполнения каких-либо действий). Например, компонент заражен или произошла ошибка при инициализации, загрузке баз и файлов ключей.
1	Errors	E	Информация о прочих ошибках, в том числе и не приводящих к завершению работы компонентов; например, информация об ошибке проверки объекта.
2	Warning	W	Уведомления о событиях, в результате которых может произойти завершение работы программы (информация об истечении срока действия файла ключа, об отсутствии свободного места на диске).
3	Info, Notice	I	Важные сообщения информационного характера; например, информация о том, запущен ли компонент, путь к конфигурационному файлу, область проверки, информация о базах, о файлах ключей, результирующая статистика.
4	Activity	A	Сообщения о проверке файлов в соответствии с уровнем детализации отчета.
9	Debug	D	Все сообщения отладочного характера.

Информация о критических ошибках в работе компонента выводится всегда, вне зависимости от установленного уровня детализации. Оптимальным уровнем является уровень 4, который задан по умолчанию.

Сообщения информационного характера можно разделить на следующие виды:

- сообщения, связанные с антивирусной проверкой;
- сообщения, связанные с функционированием программы.

Например, при записи в отчет информации о результатах антивирусной проверки объекта будет использован следующий формат:

```
<DD-MM-YY HH:MM:SS> <REPORT_LEVEL> <METHOD> <ICAP_CLIENT_IP> <HTTP_USER_NAME>
<HTTP_USER_IP> <URL> <RESULT>
```

Значения каждого из параметров приведены в таблице 4.

Таблица 4. Параметры записи в отчете

Символическое имя	Значение
<DD-MM-YY HH:MM:SS>	Дата и время создания записи в формате, заданном параметрами **DateFormat** и **TimeFormat**.
<REPORT_LEVEL>	Буквенное обозначение уровня детализации отчета.
<METHOD>	Режим обработки ICAP-запроса (RESPMOD или REQMOD).
<ICAP_CLIENT_IP>	IP-адрес ICAP-клиента, запросившего объект.
<HTTP_USER_NAME>	Имя HTTP-пользователя, запросившего объект.
<HTTP_USER_IP>	IP-адрес HTTP-пользователя, запросившего объект.
<URL>	URL запрошенного объекта.
<RESULT>	Результат антивирусной проверки объекта.

Создание файлов дампа для обнаружения ошибок

Для того, чтобы эксперты Лаборатории Касперского помогли вам как можно быстрее выяснить причину сбоя в работе Антивируса Касперского, им понадобится файл дампа памяти. Файлы дампа памяти (иначе – файлы ядра) создаются во время аварийного завершения работы программы. Создание файлов дампа по умолчанию отключено.

Для включения создания файлов дампа задайте путь /var/log/kaspersky/kav4proxy/core/ в качестве значения параметра **CorePath** в секции `[icapserver.path]` конфигурационного файла Антивируса Касперского.

Удостоверьтесь, что раздел, на котором размещена директория /var/log/kaspersky/kav4proxy/core/ имеет достаточно свободного места для сохранения файлов дампа.

Для систем на базе FreeBSD также необходимо внести изменения в параметры ядра системы. Для этого введите следующую команду с полномочиями пользователя root:

```
# sysctl -w kern.sugid_coredump=1
```

После этого в случае аварийного завершения работы программы дамп памяти будет создан в директории /var/log/kaspersky/kav4proxy/core/.

Для систем на базе FreeBSD следует отключить создание файлов дампа после их использования и отменить все внесенные изменения в ядре системы. Для этого выполните следующую команду:

```
# sysctl -w kern.sugid_coredump=0
```

Настройки для приема интернет-радиостанций

Антивирусная проверка трафика, созданного интернет-радиостанциями, может прерывать поток данных или работу прокси-сервера. Это усложняет прослушивание радио через интернет. Для решения этой проблемы рекомендуется исключить такой трафик из проверки с помощью параметра **ExcludeMimeType**:

```
[icapserver.filter]
```

```
ExcludeMimeType=^audio/mpeg$

ExcludeMimeType=^application/vnd.ms.wms-hdr.asfv1$

ExcludeMimeType=^application/x-mms-framed$
```

Приведенные выше настройки позволяют исключить из проверки потоки данных в форматах MPEG, ASF и Microsoft Windows Media.

Оптимизация работы Антивируса Касперского

Работу Антивируса Касперского можно оптимизировать с целью уменьшения времени ответа пользователю и снижения нагрузки на сеть. Основными причинами снижения быстродействия являются:

- пересылка большого объема данных между прокси-сервером и Антивирусом Касперского;
- проверка всех типов объектов.

Для снижения нагрузки на сеть Антивирус Касперского поддерживает возможность ответа **204 No Content** (см. стр. 41).

Для предотвращения проверки некоторых типов объектов можно настроить исключения (см. стр. 41).

Снижение нагрузки на сеть

В ходе работы Антивируса Касперского возможны ситуации, когда объект, переданный с прокси-сервера, не требует модификации (например, объект незаражен). Если работа Антивируса Касперского с прокси-сервером организована в «полном» режиме (см. стр. 37), то проверенный объект будет передан прокси-серверу полностью.

Если же Антивирус Касперского работает в «частичном» режиме (см. стр. 37), а размер объекта достаточно мал, то проверка объекта может завершиться до истечения периода **MaxSendDelayTime**. В этом случае объект также будет передан прокси-серверу полностью.

Избежать ненужной пересылки данных можно с помощью использования ответа **204 No Content**. Для этого присвойте значение **true** параметру **Allow204** в секции `[icapserver.protocol]` конфигурационного файла Антивируса Касперского. После этого, если объект не был изменен в ходе антивирусной проверки, вместо полного объекта Антивирус Касперского отправит стандартный ответ **204 No Content**.

Настройка исключений

Одним из способов оптимизации работы Антивируса Касперского является настройка исключений из проверки. Возможна настройка трех типов исключений:

- по типу объекта;
- по адресу, с которого поступает объект;
- по размеру объекта.

В случае обработки исключения по адресу объекта, Антивирус Касперского проверяет адрес, с которого получен объект, на соответствие значению параметра **ExcludeURL** секции `[icapserver.filter]` конфигурационного файла программы. Если соответствие установлено, то антивирусная проверка не производится, и клиенту отправляется ответ **204 No Content**.

В случае обработки исключения по типу объекта, Антивирус Касперского анализирует тип полученного объекта (по значению **Content-Type**). Если значение параметра **ExcludeMimeType** секции `[icapserver.filter]` конфигурационного файла kav4proxy.conf совпадает со значением поля **Content-Type** объекта, то антивирусная проверка не производится, и клиенту отправляется ответ **204 No Content**.

В случае обработки исключения по размеру объекта Антивирус Касперского проверяет размер объекта (по значению поля **Content-Length** HTTP-заголовка). Если размер объекта превышает значение параметра **MaxReqLength** секции `[icapserver.filter]` конфигурационного файла kav4proxy.conf, то антивирусная проверка не производится, и клиенту отправляется ответ **204 No Content**.

Для полноценного использования исключений необходимо включить поддержку возможности preview. Эта возможность позволяет Антивирусу Касперского получить начало объекта вместо получения всего объекта целиком. На основании HTTP-заголовков, содержащихся в первой части объекта, Антивирус Касперского сможет эффективно выполнить фильтрацию объекта. В случае, если объект попадает под правила фильтрации, Антивирус Касперского останавливает дальнейшее получение объекта и посылает ответ **204 No Content**. Таким образом достигается существенное уменьшение трафика между прокси-сервером и Антивирусом Касперского, что позволяет повысить быстродействие.

Размер первой части объекта определяется параметром **PreviewSize**, который определен в секции `[icapserver.protocol]` конфигурационного файла kav4proxy.conf. Для включения возможности preview, необходимо соответствующим образом сконфигурировать прокси-сервер. Для Squid наличие режима preview определяется опцией icap_preview_enable, конфигурационного файла Squid.

УДАЛЕНИЕ ПРОГРАММЫ

- *Чтобы удалить Антивирус Касперского с сервера под управлением операционной системы Linux, выполните одно из следующих действий:*

  - для удаления Антивируса Касперского, установленного из rpm-пакета, в командной строке введите:

    ```
    # rpm -e <имя_дистрибутива>
    ```

  - для удаления Антивируса Касперского, установленного из deb-пакета, в командной строке введите:

    ```
    # dpkg -r <имя_дистрибутива>
    ```

- *Чтобы удалить Антивирус Касперского с сервера под управлением операционной системы FreeBSD, выполните следующую команду:*

  ```
  # pkg_delete <имя_дистрибутива>
  ```

Процедура удаления Антивируса Касперского выполняется автоматически и включает последовательное выполнение следующих действий:

1. Удаление cron-задачи обновления антивирусных баз из списка задач пользователя **kluser**.
2. Удаление изменений, внесенных в конфигурационный файл прокси-сервера, и перезапуск прокси-сервера.
3. Останов служб программы.
4. Откат регистрации автоматического запуска служб программы в системе.
5. Удаление временных файлов или директорий, созданных в процессе работы Антивируса Касперского.
6. Удаление файлов программы: удаляются все директории и файлы Антивируса Касперского, включая базы, устанавливаемые с пакетом. Исключением являются отчеты, конфигурационные файлы и директория резервного копирования, их удаление не производится.

ПРОВЕРКА КОРРЕКТНОСТИ НАСТРОЙКИ АНТИВИРУСА КАСПЕРСКОГО

После установки и настройки Антивируса Касперского вы можете проверить с помощью тестового «вируса» и его модификаций, правильно ли выполнена настройка параметров.

В ЭТОМ РАЗДЕЛЕ

Тестовый «вирус» EICAR и его модификации

Тестовый «вирус» был специально разработан организацией eicar (The European Institute for Computer Antivirus Research) для проверки работы антивирусных продуктов.

Тестовый «вирус» НЕ ЯВЛЯЕТСЯ ВИРУСОМ и не содержит программного кода, который может навредить вашему компьютеру, при этом большинство продуктов антивирусных компаний-производителей идентифицируют его как вирус.

Никогда не используйте в качестве проверки работоспособности антивирусного продукта настоящие вирусы!

Загрузить тестовый «вирус» можно с официального сайта организации **EICAR**: http://www.eicar.org/anti_virus_test_file.htm.

Перед загрузкой необходимо отключить антивирусную защиту, поскольку файл *anti_virus_test_file.htm* будет идентифицирован и обработан приложением как зараженный объект, перемещаемый по HTTP-протоколу.

Не забудьте включить антивирусную защиту сразу после загрузки тестового «вируса».

Приложение идентифицирует файл, загруженный с сайта компании **EICAR** как зараженный объект, содержащий **неподверженный лечению** вирус, и выполняет действие, установленное для такого объекта.

Вы также можете использовать модификации стандартного тестового «вируса» для проверки работы Антивируса Касперского. Для этого следует изменить содержание стандартного «вируса», добавив к нему один из префиксов (см. таблицу далее). Для создания модификаций тестового «вируса» может использоваться любой текстовый или гипертекстовый редактор, например, **Microsoft Блокнот**, **UltraEdit32**, и т. д.

Вы можете проверять корректность работы антивирусного приложения с помощью модифицированного «вируса» EICAR только при наличии антивирусных баз, датированных не ранее 24.10.2003 (кумулятивное обновление – Октябрь, 2003).

В первой графе приведены префиксы, которые следует добавить в начало строки стандартного тестового «вируса». Во второй графе перечислены все возможные значения статуса, присваиваемого Антивирусом Касперского объекту по результатам проверки. Третья графа содержит информацию об обработке приложением объектов с указанным статусом. Обращаем ваше внимание, что действия над объектами определяются значениями параметров Антивируса Касперского.

После добавления префикса к тестовому «вирусу» сохраните полученный файл, например, под именем: *eicar_dele.com*. Дайте аналогичные названия всем модифицированным «вирусам».

Таблица 5. Модификации тестового «вируса»

Префикс	Статус объекта	Информация об обработке объекта
Префикс отсутствует, стандартный тестовый «вирус».	**Зараженный**. Объект содержит код известного вируса. Лечение невозможно.	Антивирус Касперского идентифицирует данный объект как вирус, неподверженный лечению. При попытке лечения объекта возникает ошибка; применяется действие, установленное для неизлечимых объектов.
CORR–	**Поврежденный**.	Антивирус Касперского получил доступ к объекту, но не смог проверить его, поскольку объект поврежден (например, нарушена структура объекта, неверный формат файла).
WARN–	**Подозрительный**. Объект содержит код неизвестного вируса. Лечение невозможно.	Объект признан подозрительными с использованием эвристического анализатора. На момент обнаружения базы Антивируса Касперского не содержат описания процедуры лечения данного объекта.
	Подозрительный. Объект содержит модифицированный код известного вируса. Лечение невозможно.	Антивирус Касперского обнаружил частичное совпадение участка кода объекта с участком кода известного вируса. На момент обнаружения базы приложения не содержат описания процедуры лечения данного объекта.
ERRO–	**Ошибка проверки**.	При проверке объекта возникла ошибка. Антивирус Касперского не смог получить доступ к объекту: нарушена целостность объекта (например, нет конца многотомного архива) либо отсутствует связь с ним (если проверяется объект на сетевом ресурсе).
CURE–	**Зараженный**. Объект содержит код известного вируса. Излечим.	Объект содержит вирус, который может быть вылечен. Антивирус Касперского выполняет лечение объекта, при этом текст тела «вируса» изменяется на CURE.
DELE–	**Зараженный**. Объект содержит код известного вируса. Лечение невозможно.	Антивирус Касперского идентифицирует данный объект как вирус, неподверженный лечению. При попытке лечения объекта возникает ошибка; применяется действие, установленное для неизлечимых объектов.

Проверка корректности настройки антивирусной проверки HTTP-трафика

Приведенная ниже процедура проверки корректности настройки Антивируса Касперского требует наличия установленной утилиты wget.

Чтобы проверить, насколько корректно настроен Антивирус Касперского, выполните следующие действия:

1. Настройте параметры антивирусной проверки (см. стр. 26).

2. Задайте адрес прокси-сервера в конфигурационном файле утилиты wget (/etc/wgetrc (Linux), /usr/local/etc/wgetrc (FreeBSD)), например:

```
http_proxy = http://proxy.example.com:3128/
```

3. Попытайтесь загрузить тестовый «вирус» с официального сайта организации **EICAR**: http://www.eicar.org/anti_virus_test_file.htm.

   В результате загрузка файла будет запрещена и на консоли будет отображена подобная информация:

```
$ wget http://www.eicar.org/download/eicar.com

--2010-01-13 11:38:47--  http://www.eicar.org/download/eicar.com

Connecting to 172.16.0.1:8080... connected.

Proxy request sent, awaiting response... 403 Forbidden

2010-01-13 11:38:47 ERROR 403: Forbidden.
```

КОНФИГУРАЦИОННЫЙ ФАЙЛ АНТИВИРУСА КАСПЕРСКОГО

В этом разделе подробно рассматривается конфигурационный файл kav4proxy.conf, который используется для задания параметров работы Антивируса Касперского по умолчанию сразу после его установки на сервер.

Таблица 6. Параметры конфигурационного файла Антивируса Касперского

Параметр	**Описание**
Секция `[path]` содержит параметры, определяющие пути к важнейшим директориям для работы Антивируса Касперского.	
BasesPath=/var/opt/kaspersky/kav4proxy/bases	Полный путь к директории хранения баз Антивируса Касперского.
LicensePath=/var/opt/kaspersky/kav4proxy/licenses	Полный путь к директории хранения файлов ключей Антивируса Касперского.
TempPath=/tmp	Полный путь к директории хранения временных файлов Антивируса Касперского.
KLPluginsPath=/opt/kaspersky/kav4proxy/lib/ppl	Полный путь к директории хранения файлов библиотек Антивируса Касперского.
Секция `[options]` содержит параметры, определяющие пользователя и группу, с правами которых выполняется Антивирус Касперского.	
User=kluser	Имя пользователя, с правами которого выполняется Антивирус Касперского.
Group=klusers	Имя группы, с правами которой выполняется Антивирус Касперского.
Секция `[locale]` включает параметры, определяющие формат отображения даты и времени в отчетах и статистике работы Антивируса Касперского.	
DateFormat=%d-%m-%Y	Формат отображения даты в отчете о работе Антивируса Касперского.
TimeFormat=%H:%M:%S	Формат отображения времени в отчете.
Секция `[icapserver.network]` содержит сетевые настройки Антивируса Касперского.	

ListenAddress=localhost:1344	IP-адрес и порт на котором Антивирус Касперского ожидает запросы от прокси-сервера по протоколу ICAP.
	
	Перед изменением значения параметра **ListenAddress** остановите службу Антивируса Касперского с помощью следующей команды:
	
	для Linux:
	
	`# /etc/init.d/kav4proxy stop`
	
	для FreeBSD:
	
	`# /usr/local/etc/rc.d/kav4proxy stop`
	
	Чтобы запустить службу Антивируса Касперского, выполните следующую команду:

Параметр	Описание

	для Linux:
	
	`# /etc/init.d/kav4proxy start`
	
	для FreeBSD:
	
	`# /usr/local/etc/rc.d/kav4proxy start`

Timeout=0	Сетевой тайм-аут на взаимодействие по протоколу ICAP.
Секция `[icapserver.process]` содержит детальные настройки работы процессов Антивируса Касперского:	
MaxChildren=3	Максимальное количество запущенных дочерних процессов, выполняющих обработку запросов по протоколу ICAP.
IdleChildren=1	Максимальное количество запущенных дочерних процессов, находящихся в состоянии ожидания запроса по протоколу ICAP.
MaxReqsPerChild=0	Максимальное количество запросов на проверку объектов, которое может обработать дочерний процесс. После обработки указанного числа запросов дочерний процесс завершает свою работу и Антивирус Касперского запускает новый дочерний процесс.
MaxEnginesPerChild=2	Максимальное количество модулей проверки, одновременно используемых дочерними процессами для антивирусной проверки объектов. Большее количество модулей проверки позволяет быстрее выполнять антивирусную проверку объектов, но при этом оказывает влияние на производительность сервера. Учитывайте аппаратные возможности сервера при задании значения данного параметра.
Секция `[icapserver.protocol]` содержит параметры взаимодействия Антивируса Касперского с прокси-сервером по протоколу ICAP.	
AnswerMode=partial|complete	Режим взаимодействия с прокси-сервером. Значение **partial** определяет, что Антивирус Касперского разрешает передачу клиенту частей запрошенного объекта до того, как он будет полностью загружен из интернета и проверен. Значение **complete** определяет, что Антивирус Касперского разрешает передачу клиенту запрошенного объекта, только лишь после его полной загрузки и проверки. Значение по умолчанию: **partial**.
MaxSendDelayTime=10	Временной интервал (в секундах), определяющий периодичность отправки клиенту частей запрошенного объекта при использовании режима взаимодействия **partial**.
ReqModeServiceUrl=av/reqmod	URL ICAP-сервиса для проверки потока HTTP-запросов.

Параметр	Описание
RespModeServiceUrl=av/respmod	URL ICAP-сервиса для проверки потока HTTP-ответов.
PreviewSize=0	Размер preview-запроса. Если значение параметра равно **0**, то сервер не рекомендует отправлять ему preview-запросы.
MaxConnections=5000	Максимальное число соединений, допустимое для данного ICAP-сервера. Значение данного параметра возвращается клиенту в ответ на вызов метода OPTIONS. Если значение параметра равно **0**, то метод OPTIONS не возвращает максимальное число соединений.
Allow204	Режим использования ответа **204 No Content**. По умолчанию значение параметра **true**.
HTTPClientIpICAPHeader=X-Client-IP	Имя ICAP-заголовка, содержащего IP-адрес HTTP-клиента.
HTTPUserNameICAPHeader=X-Client-Username	Имя ICAP-заголовка, содержащего имя пользователя HTTP-клиента.
SendAVScanResult=true|false	Режим отправки информации об обнаруженной угрозе. Если значение параметра – **true**, в ICAP-ответ добавляется следующая информация: **X-Virus-ID** – имя обнаруженной угрозы, **X-Response-Info** – результате обработки запроса (blocked, filtered или passed). Значение по умолчанию: **false**.
Секция `[icapserver.statistics]` содержит параметры формирования статистики работы Антивируса Касперского.	
CounterStatisticsFile	Путь к файлу для записи значений счетчиков статистики.
AVStatisticsFile	Путь к файлу для записи статистики антивирусной проверки.
AVStatisticsAddress	Сетевой сокет для записи статистики антивирусной проверки.
Секция `[icapserver.report]` содержит параметры формирования отчетов Антивируса Касперского.	
ReportFileName=/var/log/kaspersky/kav4proxy/kavicapserver.log	Файл для записи отчета о работе Антивируса Касперского.
Buffered=true|false	Режим буферизации записи в файл отчета. Для включения режима установите **true** в качестве значения параметра. Значение по умолчанию: **false**.
ReportLevel=0|1|2|3|4|9	Уровень детализации отчета. Значение по умолчанию: **4**.
ShowOk=true|false	Режим фиксирования в отчете информации об объектах, в которых в результате проверки не был обнаружен вредоносный код. Значение по умолчанию: **true**.
Append=true|false	Режим формирования отчета, при котором файл отчета создается заново при каждом запуске Антивируса Касперского. Если вы хотите добавлять в существующий отчет новую информацию, а не перезаписывать ее, установите для параметра значение **true**. Значение по умолчанию: **true**.

ПАРАМЕТР	ОПИСАНИЕ
AVReportFileName=/var/log/kaspersky/kav4proxy/av_server_log	Имя файла отчета антивирусного ядра Антивируса Касперского.
AVReportLevel=0|1|2|3|4|9	Уровень детализации отчета Антивируса Касперского.
Секция `[icapserver.path]` содержит параметры, задающие пути к специальным файлам программы.	
PidFile=/var/run/kavicapserver.pid	Путь к PID-файлу Антивируса Касперского.
CorePath	Путь к директории хранения файлов дампа памяти, которые создаются в случае аварийного завершения работы Антивируса Касперского. Чтобы включить создание файлов дампа, задайте значение **/var/log/kaspersky/kav4proxy/core/**. По умолчанию значение параметра не задано (создание файлов дампа отключено).
Описанные далее секции содержат параметры антивирусной обработки для группы по умолчанию (см. стр. 31). Секция `[icapserver.groups]` содержит параметры группы по умолчанию.	
Priority	Приоритет группы. Если параметры запроса соответствуют нескольким группам, то обработка ведется по правилам группы с более высоким приоритетом. Значение по умолчанию: **0** (наивысший приоритет).
ClientIP	IP-адрес клиента, запросившего объект через прокси-сервер. Объекты, запрошенные с указанного IP-адреса, расположенные по адресу, заданному параметром URL, обрабатываются по правилам данной группы. Значение по умолчанию: **.***.
URL	URL запрашиваемого объекта. Объекты с заданным URL, запрошенные с IP-адреса, заданного параметром **ClientIP**, обрабатываются по правилам данной группы. Значение по умолчанию: **.***.
Секция `[icapserver.filter]` содержит параметры фильтрации для группы по умолчанию.	
ExcludeMimeType	Маска-исключение фильтрации по MIME-типу (до-пускается использование регулярных выражений). Антивирус Касперского не выполняет антивирусную проверку объектов, MIME-тип которых подпадает под действие заданной маски.
ExcludeURL	Маска-исключение фильтрации по URL (допускается использование регулярных выражений). Антивирус Касперского не выполняет антивирусную проверку объектов, URL которых подпадает под действие заданной маски.
MaxReqLength=0	Максимальный размер сканируемого объекта, в байтах.
Секция `[icapserver.engine.options]` содержит параметры антивирусной проверки для группы по умолчанию.	

Параметр	Описание
ScanPacked=true|false	Режим проверки упакованных файлов. Для отключения режима установите **false** в качестве значения параметра. Значение по умолчанию: **true**.
ScanArchives=true|false	Режим проверки объектов в архивах. Для отключения режима установите **false** в качестве значения параметра. Значение по умолчанию: **true**.
ScanSFXArchives=true|false	Режим проверки самораспаковывающихся архивов. Для отключения режима установите **false** в качестве значения параметра. Значение по умолчанию: **true**.
ScanMailBases=true|false	Режим проверки почтовых баз (запрашиваемых или передаваемых через прокси-сервер). Для отключения режима установите **false** в качестве значения параметра. Значение по умолчанию: **true**.
ScanMailPlain=true|false	Режим проверки почтовых баз в формате plain text (запрашиваемых или передаваемых через прокси-сервер). Для отключения режима установите **false** в качестве значения параметра. Значение по умолчанию: **true**.
UseAnalyzer=yes|no	Режим использования при антивирусной проверке эвристического анализатора. Эвристический анализатор проверяет типичные последовательности операций, позволяющие сделать вывод о природе файла с достаточной долей вероятности. Преимущество метода в том, что новые угрозы распознаются до того, как их активность станет известна вирусным аналитикам. Для отключения режима установите **no** в качестве значения параметра. Значение по умолчанию: **yes**.
HeuristicLevel=Recommended|Light|Deep|Medium	Уровень детализации проверки с помощью эвристического анализатора. Уровень детализации обеспечивает баланс между тщательностью поиска новых угроз, степенью загрузки ресурсов операционной системы и временем проверки. Чем выше установлен уровень детализации проверки, тем больше ресурсов она потребует и больше времени займет. Возможные значения: • **Light** – наименее тщательная проверка, минимальная загрузка системы; • **Medium** – средняя глубина проверки, сбалансированная загрузка системы; • **Deep** – наиболее тщательная проверка, максимальная загрузка системы; • **Recommended** – рекомендуемое значение. Значение по умолчанию: **Recommended**.
Cure=true|false	Режим лечения зараженных объектов. Для отключения режима установите **false** в качестве значения параметра. Значение по

Параметр	Описание
	умолчанию: **false**.
MaxScanTime	Максимальное время проверки объекта, в секундах. Если за указанное время проверка не завершена, объекту присваивается статус *ERROR*. Значение по умолчанию: **300**.
MaxNestingLevel=8	Максимальный уровень вложенности проверяемого объекта. Антивирус Касперского не проверяет объекты с уровнем вложенности, превышающим заданное значение.
Секция `[icapserver.actions]` содержит настройки действий над проверенными объектами для группы по умолчанию.	
CuredAction=skip|deny	Действие над вылеченным объектом. Значение по умолчанию: **skip**.
InfectedAction=skip|deny	Действие над зараженным объектом. Значение по умолчанию: **deny**.
SuspiciousAction=skip|deny	Действие над подозрительным объектом. Значение по умолчанию: **deny**.
WarningAction=skip|deny	Действие над объектом, содержащим код, похожий на код известного вируса. Значение по умолчанию: **deny**.
ErrorAction=skip|deny	Действие над объектом, проверка которого завершилась с ошибкой. Значение по умолчанию: **skip**.
ProtectedAction=skip|deny	Действие над объектом, защищенным паролем. Значение по умолчанию: **skip**.
CorruptedAction=skip|deny	Действие над поврежденным объектом. Значение по умолчанию: **skip**.
LicenseErrorAction=skip|deny	Действие над проверяемыми объектами, если Антивирусу Касперского не удалось загрузить информацию о лицензии. Значение по умолчанию: **skip**.
BasesErrorAction=skip|deny	Действие, выполняемое над объектами, если Антивирусу Касперского не удалось загрузить базы. Значение по умолчанию: **deny**.
MaxReqLengthAction=skip|deny	Действие над объектом, размер которого превышает заданный максимальный размер (**MaxReqLength**). Значение по умолчанию: **skip**.
PartialResponseAction=check|deny	Действие при обнаружении ответа сервера, содержащего часть объекта. Значение **check** разрешает проверку сообщения. Значение **deny** запрещает передачу ответа и сообщает об ошибке доступа. Значение по умолчанию: **check**.
PartialRequestAction=check|deny|reset	Действие при обнаружении запроса на выдачу части объекта. Значение **check** разрешает проверку запроса. Значение **deny** запрещает запрос и сообщает об ошибке доступа. Значение **reset** удаляет из запроса информацию о запросе части объекта и запрашивает объект целиком. Значение по

Параметр	Описание
	умолчанию: **check**.
Секция `[icapserver.notify]` содержит параметры оповещения для группы по умолчанию.	
NotifyTemplateDir	Директория расположения шаблонов оповещений.
NotifyScript	Скрипт, используемый Антивирусом Касперского для оповещения администратора.
Секция `[updater.path]` содержит параметры, определяющие пути к директориям, необходимым для работы утилиты **keepup2date**.	
BackUpPath	Полный путь к директории хранения резервной копии баз Антивируса Касперского. Значение по умолчанию: **/var/opt/kaspersky/kav4proxy/bases.backup**.
AVBasesTestPath	Полный путь к утилите проверки целостности баз Антивируса Касперского. Значение по умолчанию: **/opt/kaspersky/kav4proxy/lib/bin/avbasestest**.
Секция `[updater.options]` содержит параметры работы компонента **keepup2date**.	
KeepSilent=true|false	Режим вывода на консоль информации о работе компонента **keepup2date**. Для отключения режима присвойте параметру значение **true**. Значение по умолчанию: **false**.
ProxyAddress	Адрес используемого для соединения прокси-сервера. Значение параметра задается в виде `http://username:password@url:port`. В адресе прокси-сервера username и/или password могут отсутствовать. Если адрес не указан, то его значение берется из переменной окружения http_proxy.
UseProxy=true|false	Режим использования прокси-сервера при соединении с сервером обновлений «Лаборатории Касперского». Если значение параметра **false**, прокси-сервер не используется. Если значение параметра **true**, используется адрес прокси-сервера, определенный параметром **ProxyAddress**. Если значение параметра **ProxyAddress** не определено, будет использовано значение переменной окружения http_proxy. Если значение переменной окружения не определено, прокси-сервер не используется. Значение по умолчанию: **false**.
UseUpdateServerUrl=true|false	Режим использования обновления с адреса, определенного параметром **UpdateServerUrl**. Значение по умолчанию: **false**.
UseUpdateServerUrlOnly=true|false	Режим использования для обновления баз только адреса, указанного в настройке **Update-ServerUrl**. Если опции присвоено значение **false**, то в случае неудачной попытки обновления баз с адреса **UpdateServerUrl** будет использован другой адрес из списка серверов обновлений. Значение по умолчанию: **false**.
UpdateServerUrl=http://url/ **|** ftp://url/ **| /local_path/**	Адрес источника обновлений.

Параметр	Описание
PostUpdateCmd=/etc/init.d/kav4proxy reload_avbase	Команда, выполняемая сразу после успешного завершения обновления баз. Значение, указанное в конфигурационном файле, включенном в поставку Антивируса Касперского, запустит автоматическое перечитывание Антивирусом Касперского обновленных баз. Изменение значения этого параметра не рекомендуется.
RegionSettings=Russia	Код региона пользователя; применяется для выбора наиболее удобного для скачивания обновлений антивирусных баз сервера обновления «Лаборатории Касперского».
ConnectTimeout=30	Сетевой тайм-аут для обновления баз (в секундах). Если во время загрузки баз в течение указанного промежутка времени данные от сервера не приходят, производится выбор другого сервера из списка серверов обновлений «Лаборатории Касперского».
PassiveFtp=true|false	Режим использования для соединения passive FTP. Значение по умолчанию: **false**.
Секция `[updater.report]` содержит параметры формирования отчета о работе компонента **keepup2date**.	
Append=true|false	Режим добавления новых сообщений в файл отчета. Для отключения режима присвойте параметру значение **false**. Значение по умолчанию: **true**.
ReportFileName	Имя файла отчета, в котором фиксируются результаты работы компонента.
ReportLevel=0|1|2|3|4|9	Уровень детализации отчета. Значение по умолчанию: **4**.

МАКРОСЫ

Антивирус Касперского позволяет использовать специальные макросы в шаблонных файлах, отправляемых пользователю вместо объектов, доступ к которым был запрещен (см. стр. 33), а также в тексте скрипта уведомления (параметр **NotifyScript**). Описание этих макросов см. в таблице ниже.

Таблица 7. Макросы

Синтаксис макроса	Описание
%VIRUS_LIST%	Список вирусов, которыми заражен объект.
%WARN_LIST%	Список объектов, содержащих код, похожий на код известного вируса.
%SUSP_LIST%	Список объектов, подозреваемых на заражение неизвестным вирусом.
%CURED_LIST%	Список вылеченных вирусов.
%CLIENT_ADDR%	IP-адрес компьютера пользователя, запросившего объект.
%URL%	URL запрошенного объекта.
%ACTION%	Выполненное над объектом действие.
%VERDICT%	Статус объекта.
%PRODUCT%	Описание продукта.
%DATE%	Время создания сообщения.

КОДЫ ВОЗВРАТА КОМПОНЕНТА KAVICAPSERVER

Таблица 8. Коды возврата компонента kavicapserver

Код возврата	Значение
0	При запуске ошибок не выявлено.
30	Критическая системная ошибка.
65	Ошибка загрузки конфигурационного файла (файл не найден).
66	Ошибка в конфигурационном файле или параметрах командной строки.
70	Исполняемый файл компонента поврежден.

КЛЮЧИ КОМАНДНОЙ СТРОКИ КОМПОНЕНТА LICENSEMANAGER

Таблица 9. Ключи командной строки компонента licensemanager

Опции помощи	
-h	Вывести на консоль справочную информацию о ключах командной строки, поддерживаемых компонентом, и завершить работу компонента.
Опции работы с файлами ключей	
-s	Вывести на консоль информацию обо всех установленных файлах ключей
-c(C) <путь_к_файлу>	Использовать альтернативный конфигурационный файл <путь_к_файлу>.
-i	Вывести на консоль информацию о состоянии лицензируемого параметра.
-k <путь_к_файлу>	Вывести на консоль информацию об установленном файле ключа.
-a <путь_к_файлу>	Установить файл ключа.
-d <a|r>	Удалить активный / дополнительный файл ключа.

КОДЫ ВОЗВРАТА КОМПОНЕНТА LICENSEMANAGER

Таблица 10. Коды возврата компонента licensemanager

Код возврата	Значение
0	Компонент успешно завершил свою работу.
30	Критическая системная ошибка.
64	Ошибка лицензирования
65	Ошибка загрузки конфигурационного файла (файл не найден).
66	Ошибка в конфигурационном файле или параметрах командной строки.
70	Исполняемый файл компонента поврежден.

КЛЮЧИ КОМАНДНОЙ СТРОКИ КОМПОНЕНТА KEEPUP2DATE

Таблица 11. Ключи командной строки компонента keepup2date

Опции помощи	
-h	Вывести на консоль справочную информацию о ключах командной строки, поддерживаемых компонентом, и завершить работу компонента.
-v	Вывести на консоль версию программы и завершить работу компонента.
-s	Вывести список серверов обновлений с информацией об их регионах.
Опции обновления	
-c <путь_к_файлу>	Использовать альтернативный конфигурационный файл <путь_к_файлу>.
-u <директория>	Копировать обновление Антивируса Касперского в локальную директорию <директория>. В указанной директории создается структура, сходная со структурой сервера обновления, что позволяет локальным компьютерам производить обновление из данной директории.
-b <путь>	При обновлении создавать копию антивирусных баз, для которых найдены обновления, в директорию <путь>.
-t <путь>	Использовать директорию <путь> для хранения временных файлов.
-r	Отмена последнего обновления. Обновленные базы заменяются предыдущей версией.
-k	Отключить выполнение команды, заданной параметром PostUpdateCmd.
-d <путь_к_файлу>	Использовать pid-файл.
-g <url>	Использовать для обновления сервер с указанным URL.
-q	Отключение вывода информации о работе компонента.
-e	Отображать информацию только о критических ошибках.
Опции формирования отчета	
-l <путь_к_файлу>	Фиксировать результаты работы компонента в файле <путь_к_файлу>.

КОДЫ ВОЗВРАТА КОМПОНЕНТА KEEPUP2DATE

Таблица 12. Коды возврата компонента keepup2date

Код возврата	Значение
0	Обновления баз не требуется.
1	Обновление баз выполнено успешно.
10	Возникла критическая ошибка, процесс обновления прерывается.
12	Ошибка при выполнении отката к использованию прежних антивирусных баз. Откат прерван.
30	Не удалось запустить команду **PostUpdateCmd** после обновления баз.
60	Лицензионная информация отсутствует либо не найдено ни одного файла ключа по пути, указанному в конфигурационном файле.
75	Невозможно загрузить конфигурационный файл либо конфигурационный файл содержит ошибки.
128+код сигнала	Компонент завершил работу, получив сигнал с соответствующим кодом.

СХЕМА РАСПОЛОЖЕНИЯ ФАЙЛОВ АНТИВИРУСА КАСПЕРСКОГО

В дальнейшем в качестве примеров мы будем рассматривать названия компонентов, принятых при установке на сервер под управлением операционной системы Linux!

После установки Антивируса Касперского на сервер под управлением операционной системы Linux, при условии использования инсталляционных путей по умолчанию, файлы дистрибутива будут расположены следующим образом:

/etc/opt/kaspersky/kav4proxy.conf – конфигурационный файл, содержащий параметры работы Антивируса Касперского;

/opt/kaspersky/kav4proxy/bin/ – директория, содержащая исполняемые файлы компонентов Антивируса Касперского:

kav4proxy-keepup2date – утилита обновления баз Антивируса Касперского;

kav4proxy-licensemanager – утилита управления файлами ключей.

/opt/kaspersky/kav4proxy/lib/bin/avbasestest – утилита проверки корректности загруженных баз; используется компонентом keepup2date.

/etc/init.d/kav4proxy – скрипт для управления Антивирусом Касперского.

/opt/kaspersky/kav4proxy/lib/bin/setup/ – директория, содержащая скрипты, используемые для постинсталляционной настройки и удаления Антивируса Касперского:

postinstall.pl – скрипт постинсталляционной настройки Антивируса Касперского.

uninstall.pl – скрипт удаления Антивируса Касперского.

keepup2date.sh – скрипт настройки компонента keepup2date;

proxy_setup.pl – скрипт настройки прокси-сервера Squid на работу с Антивирусом Касперского.

/opt/kaspersky/kav4proxy/sbin/kav4proxy-kavicapserver – исполняемый файл основного модуля Антивируса Касперского.

/opt/kaspersky/kav4proxy/share/contrib/kav4proxy.wbm – модуль интеграции с Webmin.

/opt/kaspersky/kav4proxy/share/doc/ – директория хранения лицензий и документации по интеграции Антивируса Касперского:

LICENSE – лицензионное соглашение;

README-SQUID.txt – инструкция по интеграции Антивируса Касперского с прокси-сервером Squid.

/opt/kaspersky/kav4proxy/share/man/ – директория man-файлов.

Для подключения справочной системы Антивируса Касперского (manual pages) под операционной системой Linux воспользуйтесь следующей командой:

```
# export MANPATH="$MANPATH:/opt/kaspersky/kav4proxy/share/man/:".
```

/opt/kaspersky/kav4proxy/share/notify/ – директория хранения шаблонов уведомлений.

/opt/kaspersky/kav4proxy/share/examples/ – директория хранения примеров настройки Антивируса Касперского:

kav4proxy-default.conf – конфигурационный файл Антивируса Касперского с параметрами по умолчанию;

notify.sh – скрипт уведомления администратора.

/var/log/kaspersky/kav4proxy/ – директория хранения файлов журнала Антивируса Касперского.

После установки Антивируса Касперского на сервер под управлением операционной системы FreeBSD, при условии использования инсталляционных путей по умолчанию, файлы дистрибутива будут расположены следующим образом:

/usr/local/etc/kaspersky/kav4proxy.conf – конфигурационный файл, содержащий параметры работы Антивируса Касперского;

/usr/local/bin/ – директория, содержащая исполняемые файлы компонентов Антивируса Касперского:

kav4proxy-keepup2date – утилита обновления баз;

kav4proxy-licensemanager – утилита управления файлами ключей.

/usr/local/libexec/kaspersky/kav4proxy/avbasestest – утилита проверки корректности загруженных баз; используется компонентом keepup2date.

/usr/local/etc/rc.d/kav4proxy – скрипт для управления Антивирусом Касперского.

/usr/local/libexec/kaspersky/kav4proxy/setup/ – директория, содержащая скрипты, используемые для постинсталляционной настройки и удаления Антивируса Касперского:

postinstall.pl – скрипт постинсталляционной настройки Антивируса Касперского.

uninstall.pl – скрипт удаления Антивируса Касперского.

keepup2date.sh – скрипт настройки компонента keepup2date;

proxy_setup.pl – скрипт настройки прокси-сервера Squid на работу с Антивирусом Касперского.

/usr/local/sbin/kav4proxy-kavicapserver – исполняемый файл основного модуля Антивируса Касперского.

/usr/local/share/kav4proxy/contrib/kav4proxy.wbm – модуль интеграции с Webmin.

/usr/local/share/doc/kav4proxy/ – директория хранения лицензий и документации по интеграции Антивируса Касперского:

LICENSE – лицензионное соглашение;

README-SQUID.txt – инструкция по интеграции Антивируса Касперского с прокси-сервером Squid.

/usr/local/man/ – директория man-файлов.

Для подключения справочной системы Антивируса Касперского (manual pages) под операционной системой FreeBSD воспользуйтесь следующей командой:

```
# setenv MANPATH /usr/local/man.
```

/usr/local/share/kav4proxy/notify/ – директория хранения шаблонов уведомлений.

/usr/local/share/examples/kav4proxy/ – директория хранения примеров настройки Антивируса Касперского:

kav4proxy-default.conf – конфигурационный файл Антивируса Касперского с параметрами по умолчанию;

notify.sh – скрипт уведомления администратора.

/var/log/kaspersky/kav4proxy/ – директория хранения файлов журнала Антивируса Касперского.

ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

«Лаборатория Касперского» – известный в мире производитель систем защиты компьютеров от угроз: вирусов и других вредоносных программ, нежелательной почты (спама), сетевых и хакерских атак.

В 2008 году «Лаборатория Касперского» вошла в четверку ведущих мировых лидеров рынка программных решений для обеспечения информационной безопасности для конечных пользователей (рейтинг «IDC Worldwide Endpoint Security Revenue by Vendor»). По результатам исследования КОМКОН TGI-Russia 2009, «Лаборатория Касперского» – самый предпочитаемый производитель систем защиты для домашних пользователей в России.

«Лаборатория Касперского» основана в России в 1997 году. Сегодня «Лаборатория Касперского» – это международная группа компаний с центральным офисом в Москве и пятью региональными дивизионами, управляющими деятельностью компании в России, Западной и Восточной Европе, на Ближнем Востоке, в Африке, в Северной и Южной Америке, в Японии, Китае и других странах Азиатско-Тихоокеанского региона. В компании работает более 2000 квалифицированных специалистов.

Продукты. Продукты «Лаборатории Касперского» защищают как домашние компьютеры, так и компьютерные сети организаций.

Линейка персональных продуктов включает антивирусные приложения для настольных компьютеров и ноутбуков, для карманных компьютеров, смартфонов и других мобильных устройств.

Компания предлагает программы и сервисы для защиты рабочих станций, файловых и веб-серверов, почтовых шлюзов, сетевых экранов. Использование этих решений в сочетании с централизованными средствами управления позволяет построить и эксплуатировать эффективную автоматизированную защиту организации от компьютерных угроз. Продукты «Лаборатории Касперского» сертифицированы крупными тестовыми лабораториями, совместимы с программным обеспечением многих поставщиков программного обеспечения и оптимизированы для работы на многих аппаратных платформах.

Вирусные аналитики «Лаборатории Касперского» работают круглосуточно. Каждый день они находят сотни новых компьютерных угроз, создают средства их обнаружения и лечения и включают их в базы, используемые программами «Лаборатории Касперского». *Антивирусная база «Лаборатории Касперского» обновляется ежечасно*, *база Анти-Спама – каждые 5 минут*.

Технологии. Многие технологии, без которых трудно представить себе современный антивирус, впервые разработаны именно «Лабораторией Касперского». Не случайно программное ядро Антивируса Касперского используют в своих продуктах многие другие разработчики программ: среди них SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Israel), Clearswift (UK), CommuniGate Systems (USA), Critical Path (Ireland), D-Link (Taiwan), M86 Security (USA), GFI (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), NETASQ (France), NETGEAR (USA), Parallels (Russia), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Taiwan). Многие из инновационных технологий компании подтверждены патентами.

Достижения. За годы борьбы с компьютерными угрозами «Лаборатория Касперского» завоевала сотни наград. Например, в 2010 году Антивирус Касперского получил несколько высших наград Advanced+ в тестах, проведенных авторитетной австрийской антивирусной лабораторией AV-Comparatives. Но главная награда «Лаборатории Касперского» – это приверженность пользователей по всему миру. Продукты и технологии компании защищают более 300 миллионов пользователей. Количество организаций, являющихся ее клиентами, превышает 200 тысяч.

Веб-сайт «Лаборатории Касперского»:	http://www.kaspersky.ru
Вирусная энциклопедия:	http://www.securelist.com/ru/
Антивирусная лаборатория:	newvirus@kaspersky.com (только для отправки возможно зараженных файлов в архивированном виде)
	http://support.kaspersky.ru/virlab/helpdesk.html
	(для запросов вирусным аналитикам)
Веб-форум «Лаборатории Касперского»:	http://forum.kaspersky.com

ИНФОРМАЦИЯ О СТОРОННЕМ КОДЕ

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки программы.