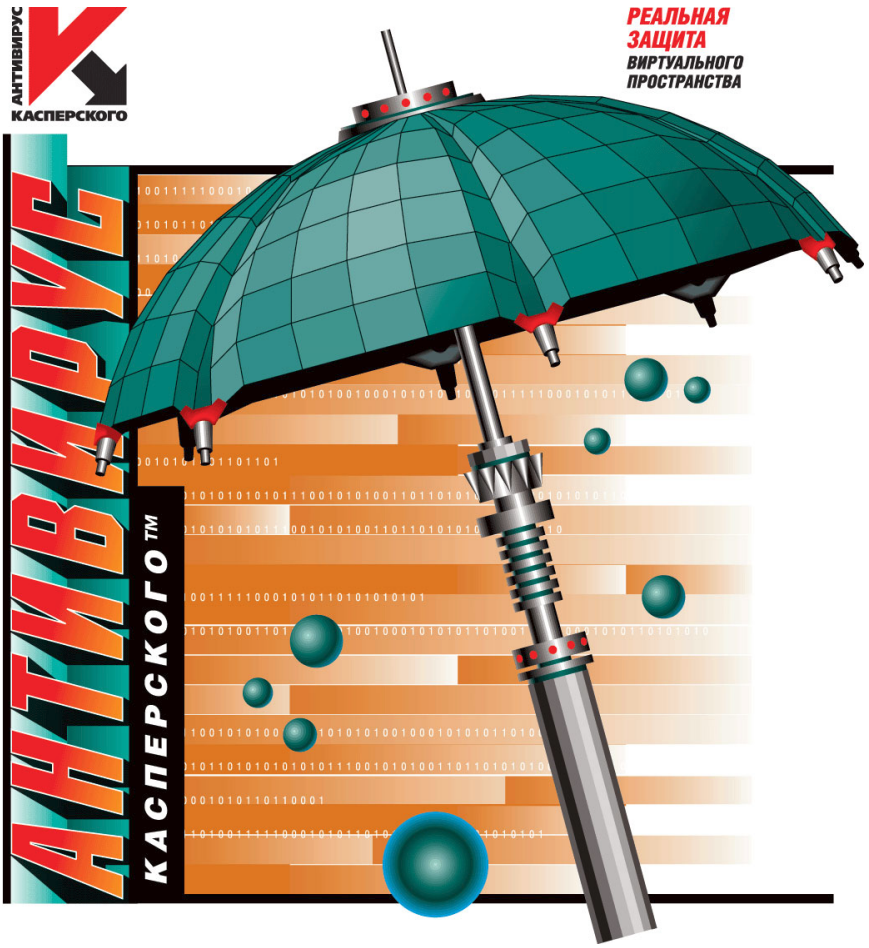
ЛАБОРАТОРИЯ КАСПЕРСКОГО



Антивирус Касперского® 5.1 для Microsoft ISA Server

Руководство администратора

АНТИВИРУС КАСПЕРСКОГО® 5.1 ДЛЯ MS ISA SERVER

Руководство администратора

Тел., факс +7 (095) 797-87-00
http://www.kaspersky.ru

Дата редакции: июль 2004 года

Содержание

ГЛАВА 1. АНТИВИРУС КАСПЕРСКОГО® ДЛЯ MS ISA SERVER

Антивирус Касперского® для Microsoft ISA Server (далее также **Антивирус Касперского® для ISA-серверов**) – это система антивирусного контроля над файлами, перемещаемыми по протоколам HTTP и FTP через брандмауэр Microsoft Internet Security and Acceleration Server, обеспечивающая высокий уровень защиты корпоративных сетей от проникновения вредоносных программ.

Антивирус Касперского для MS ISA-серверов выполняет функции фильтра, который перехватывает данные, передаваемые по протоколам HTTP и FTP, выделяет из них контролируемые объекты, анализирует их на присутствие вирусов и блокирует проникновение в локальную сеть зараженных файлов и веб-документов.

В состав приложения входят фильтры потоков данных и антивирусное ядро.

Фильтры интегрируются в MS ISA-сервер как плагины, а антивирусное ядро устанавливается в систему как служба.

Управление процессом антивирусной проверки осуществляется через специализированный интерфейс, встроенный в ISA Microsoft Management Console (далее MMC).

Приложение обеспечивает выполнение следующих функций:

- антивирусная проверка и обработка потоков данных, поступающих из сети Интернет;
- генерация потока данных из вылеченных файлов для передачи клиенту, запросившему поток;
- обновление антивирусных баз через интернет, как автоматическое с заданным расписанием обновления, так и в ручном режиме;
- сбор статистической информации о работе приложения и просмотр статистики через стандартные механизмы операционной системы Windows;
- управление лицензионными ключами.

Кроме того, Антивирус Касперского для MS ISA-серверов позволяет:

- настраивать параметры антивирусной проверки, уведомлений пользователя об опасных событиях;
- создавать группы пользователей, объединяемые по сетевым принципам. Например, вы можете использовать административное деление на отделы с последующим определением настроек антивирусной защиты для каждой из созданных групп, что может ускорить процесс антивирусной проверки;
- вести для одной или нескольких групп пользователей список доверительных серверов, трафик с которых не будет анализироваться на предмет наличия вирусов;
- формировать список типов объектов, которые не будут подвергаться антивирусной проверке.

Антивирус Касперского поддерживает следующие протоколы передачи данных:

- HTTP 1.0 и 1.1 (RFC 2616);
- FTP (RFC 959, 2389, Extensions to FTP);
- FTP over HTTP.

1.1. Аппаратные и программные требования к системе

Антивирус Касперского для MS ISA-серверов функционирует совместно с продуктом Microsoft® Internet Security and Acceleration Server 2000 с установленным Service Pack 1 или выше на следующих платформах:

- Microsoft® Windows 2003 Server.
- Microsoft® Windows 2000 Server с установленным Service Pack 3 или выше.
- Microsoft® Windows 2000 Advanced Server с установленным Service Pack 3 или выше.

В данной версии не поддерживается совместная работа с MS ISA-серверами, работающими в режиме массива серверов (Array Member).

Минимальные аппаратные требования для использования Антивируса Касперского для MS ISA-серверов:

- процессор Pentium II с тактовой частотой 300 МГц;

- 256 МБ свободной оперативной памяти;
- не менее 20 МБ свободного дискового пространства для установки приложения;
- не менее 200 МБ свободного дискового пространства для временного хранения копируемых из интернета данных перед антивирусной проверкой.

1.2. Комплект поставки

Программный продукт вы можете приобрести у наших дистрибьюторов (коробочный вариант), а также в одном из интернет-магазинов (например, www.kaspersky.ru, раздел **Электронный магазин**).

Если вы приобретаете продукт в коробке, то в комплект поставки программного продукта входят:

- запечатанный конверт с установочным компакт-диском, на котором записаны файлы программного продукта;
- руководство пользователя;
- лицензионный ключ, записанный на дискету;
- регистрационная карточка (с указанием серийного номера продукта);
- лицензионное соглашение.

Перед тем как распечатать конверт с компакт-диском, внимательно ознакомьтесь с лицензионным соглашением.

При покупке продукта в интернет-магазине вы копируете продукт с веб-сайта "Лаборатории Касперского", в дистрибутив которого помимо самого продукта включено также данное руководство. Лицензионный ключ либо включен в дистрибутив, либо отправляется вам по электронной почте по факту оплаты.

1.2.1. Лицензионное соглашение

Лицензионное соглашение – это юридическое соглашение между вами и ЗАО "Лаборатория Касперского", в котором указано, на каких условиях вы можете пользоваться приобретенным вами программным продуктом.

Внимательно прочитайте лицензионное соглашение!

Если вы не согласны с условиями лицензионного соглашения, вы можете вернуть коробку с Антивирусом Касперского дистрибьютору, у которого она была приобретена, и получить назад сумму, уплаченную за подписку. При этом конверт с установочным компакт-диском должен оставаться запечатанным.

Открывая запечатанный пакет с установочным компакт-диском или устанавливая продукт на компьютер, вы тем самым принимаете все условия лицензионного соглашения.

1.2.2. Регистрационная карточка

Пожалуйста, заполните отрывной корешок регистрационной карточки, по возможности наиболее полно указав свои координаты: фамилию, имя, отчество (полностью), телефон, адрес электронной почты (если она есть), и отправьте ее дистрибьютору, у которого вы приобрели программный продукт.

Если впоследствии у вас изменится почтовый/электронный адрес или телефон, пожалуйста, сообщите об этом в организацию, куда был отправлен корешок регистрационной карточки.

Регистрационная карточка является документом, на основании которого вы приобретаете статус зарегистрированного пользователя нашей компании. Это дает вам право на техническую поддержку в течение срока подписки. Кроме того, зарегистрированным пользователям, подписавшимся на рассылку новостей ЗАО "Лаборатория Касперского", высылается информация о выходе новых программных продуктов.

1.3. Сервис для зарегистрированных пользователей

ЗАО "Лаборатория Касперского" предлагает своим легальным пользователям большой комплекс услуг, позволяющих увеличить эффективность использования Антивируса Касперского.

Приобретя подписку, вы становитесь зарегистрированным пользователем программы и в течение срока действия подписки получаете следующие услуги:

- предоставление новых версий данного программного продукта;

- консультации по вопросам, связанным с установкой, настройкой и эксплуатацией данного программного продукта, оказываемые по телефону и электронной почте;
- оповещение о выходе новых программных продуктов Лаборатории Касперского и о новых вирусах, появляющихся в мире (данная услуга предоставляется пользователям, подписавшимся на рассылку новостей ЗАО "Лаборатория Касперского").

Консультации по вопросам функционирования и использования операционных систем, а также работы различных технологий не проводятся.

1.4. Принятые обозначения

Текст документации выделяется различными элементами оформления в зависимости от его смыслового назначения. В расположенной ниже таблице приведены используемые условные обозначения.

Оформление	Смысловое назначение
Жирный шрифт	Названия меню, пунктов меню, окон, элементов диалоговых окон и т. п.
 Примечание.	Дополнительная информация, примечания.
 Внимание!	Информация, на которую следует обратить особое внимание.
 *Чтобы выполнить действие,* 1. Шаг 1. 2. …	Описание последовательности выполняемых пользователем шагов и возможных действий.
`Текст информационных сообщений и командной строки`	Текст конфигурационных файл, информационных сообщений программы и командной строки.

ГЛАВА 2. ТИПИЧНАЯ СХЕМА РАЗВЕРТЫВАНИЯ ПРИЛОЖЕНИЯ

Типичной схемой работы администратора ISA-сервера с большинством его приложений и фильтров является следующая: администратор устанавливает приложение на ISA-сервер, а компонент его администрирования – на удаленный компьютер (как правило, рабочее место администратора).

Для такой организации работы с Антивирусом Касперского необходимо, чтобы на ISA-сервере было установлено полное приложение Антивирус Касперского, а на компьютере администратора – только его консоль администрирования. Единственным требованием к установке консоли администрирования Антивируса Касперского для ISA-серверов является наличие на компьютере средств администрирования самого ISA-сервера.

Инсталляция отдельного компонента Антивируса Касперского выполняется посредством выборочной установки приложения (см. Глава 3 на стр. 13).

В процессе установки приложения автоматически определяется режим работы ISA-сервера. Рассмотрим подробнее возможные режимы и особенности инсталляции и работы Антивируса Касперского для каждого из них.

В руководстве к ISA-серверам описаны три возможных режима работы:

- Firewall;
- Proxy;
- Integrated.

ISA-сервер, работающий в режиме **Firewall**, функционирует в качестве брандмауэра, который обеспечивает защиту внутренней корпоративной сети от различных типов угроз из сети Интернет и использует разнообразные средства повышения безопасности. В том числе это и фильтры IP-пакетов, фильтры каналов и фильтры приложений. Функциональность, связанная с кешированием проходящей информации, в данном режиме отключена.

В режиме **Proxy** ISA-сервер выполняет функции сервера кеширования, маршрутизации запросов и планирования загрузки данных для

эффективной последующей обработки запросов клиента. В данном режиме ISA-сервер функции брандмауэра не выполняет.

Режим **Integrated** позволяет использовать ISA-сервер одновременно и для защиты внутренней сети, и как сервер кеширования. Кроме того, в данном режиме возможно использование ISA-сервера только как Proxy либо только как Firewall.

При установке Антивируса Касперского режим работы ISA-сервера определяется автоматически. В зависимости от этого устанавливается различный набор фильтров потоков данных.

Установка Антивируса Касперского предусматривает добавление в систему следующих фильтров:

- **FTP-фильтр Антивируса Касперского**;
- **Web-фильтр Антивируса Касперского**;
- **HTTP-фильтр Антивируса Касперского**.

В таблице 1 представлены варианты выбора устанавливаемых фильтров для трех режимов работы ISA-сервера.

Таблица 1

Фильтр	Proxy	Firewall	Integrated
FTP-фильтр Антивируса Касперского	–	Да	Да
Web-фильтр Антивируса Касперского	Да	Да[1]	Да
HTTP-фильтр Антивируса Касперского	–	Да	–

После установки Антивируса Касперского перечисленные выше фильтры будут доступны для управления через интерфейс администрирования ISA-сервера.

При работе ISA-сервера в режиме Firewall **Web-фильтр Антивируса Касперского** устанавливается в отключенном состоянии, поскольку предполагается, что все клиенты используют ISA-сервер как брэндмауэр, не обращаясь напрямую к прокси-серверу. Если клиенты обращаются

[1] Фильтр устанавливается в отключенном состоянии.

напрямую к прокси-серверу (например, настроив свои браузеры для работы с прокси), то после установки приложения следует включить **Web-фильтр Антивируса Касперского**, чтобы проходящий через прокси-сервер трафик подвергался антивирусной проверке.

В случае переустановки ISA-сервера с выбором другого режима работы требуется переустановить и Антивирус Касперского, определив необходимые для данного режима работы фильтры.

Технологический процесс обработки исходного потока данных, представленный на рис. 1, является общим для всех возможных схем развертывания Антивируса Касперского.

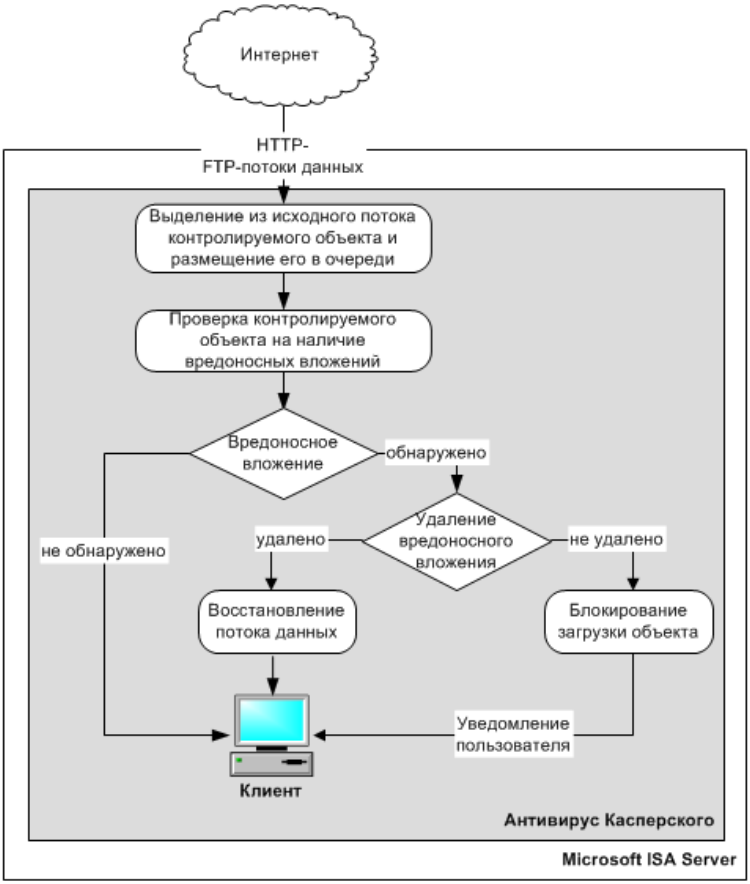


Рисунок 1. Схема обработки потока данных Антивирусом Касперского

ГЛАВА 3. УСТАНОВКА ПРИЛОЖЕНИЯ

Для корректной установки Антивируса Касперского необходимо правильно настроить ряд фильтров ISA-сервера и только после этого инсталлировать приложение в систему.

3.1. Настройка ISA-сервера перед установкой приложения

В консоли MS ISA-сервера предусмотрен ряд стандартных фильтров, которые позволяют контролировать входящие потоки данных. Для протоколов HTTP – это **HTTP Redirector Filter**. Протоколы FTP контролируются через **FTP Access Filter** (не используется в режиме Proxy).

Антивирус Касперского для MS ISA-серверов использует настройки по умолчанию указанных фильтров, чтобы получать исходный поток данных для его последующей проверки.

Перед тем как устанавливать Антивирус Касперского для ISA-серверов, убедитесь, что стандартные фильтры HTTP Redirector Filter и FTP Access Filter не отключены или не перенаправляют потоки данных, минуя антивирусную фильтрацию. Это может привести к отключению антивирусной защиты сервера!

Управление фильтрами потоков осуществляется через стандартное окно управления **ISA Management**.

Чтобы настроить HTTP Redirector Filter и FTP Access Filter,

выберите в дереве главного окна **ISA Management** узел **Extensions**, а затем папку **Application Filters**.

Если один из вышеназванных фильтров отключен, то в списке фильтров он будет отмечен значком  .

Чтобы включить фильтр,

1. Выберите в списке нужный фильтр и откройте диалоговое окно свойств фильтра.
2. Для *FTP Access Filter* в диалоговом окне **FTP Access Filter Properties** выберите **Enable this filter**.
3. Для *HTTP Redirector Filter* в диалоговом окне **HTTP Redirector Filter Properties** на закладке **General** выберите **Enable this filter**. Затем на закладке **Options** выберите **Send to requested Web server**, если MS ISA-сервер работает в режиме Firewall. Это позволит потокам данных, передаваемым по HTTP-протоколу, поступать на вход соответствующих фильтров Антивируса Касперского.

Если вы выбрали **Send to local Web Proxy server** при работе ISA-сервера в режиме Firewall, и включили использование фильтра **Kaspersky Anti-Virus Web Filter**, рекомендуем вам отключить фильтр **Kaspersky Anti-Virus HTTP Application Filter** во избежание двойной проверки трафика: при прохождении через **HTTP Redirector Filter** и через локальный прокси-сервер.

Совместно со стандартными фильтрами MS ISA-сервера могут использоваться дополнительные фильтры сторонних производителей, которые могут повлиять на работоспособность приложения, если их настройки будут препятствовать поступлению потока данных на вход фильтров Антивируса Каперского для ISA-серверов. Более того, в отдельных случаях возможно полное отключение Антивируса Касперского.

3.2. Установка Антивируса Касперского

Процедура установки Антивируса Касперского на ISA-сервер выполняется стандартно для большинства Windows-приложений. Вы можете выбирать как полную, так и выборочную установку продукта, а также восстанавливать некорректную установку Антивируса.

3.2.1. Первая установка

Шаг 1. Приветствие и Лицензионное соглашение

На первых этапах установки Антивируса Касперского открывается приветственное окно и окно, содержащее лицензионное соглашение. Внимательно прочтите текст соглашения и примите его условия для продолжения установки.

Шаг 2. Информация о пользователе и выбор варианта установки

На этом шаге автоматически определяется информация о пользователе согласно указанной в реестре операционной системы и предлагается на выбор вариант установки: полная или выборочная (см. рис. 2). При установке всего приложения Антивирус Касперского (антивирусное ядро, средства администрирования и т.д.) на MS ISA-сервер вам необходимо выбрать полную установку приложения.

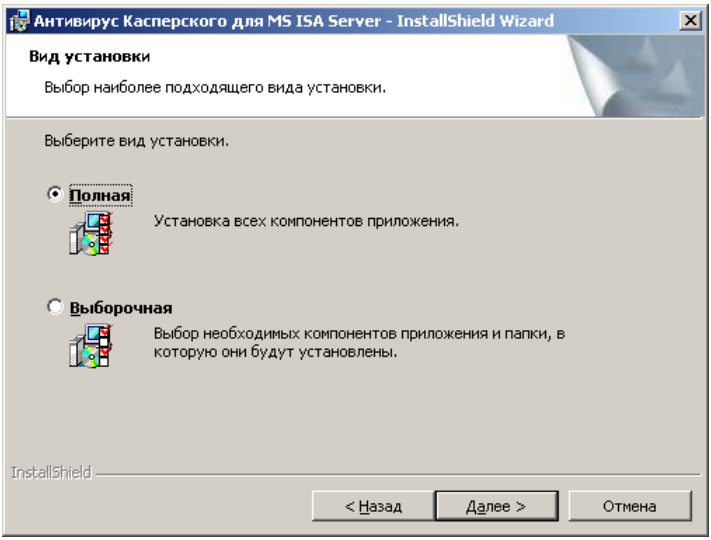


Рисунок 2. Выбор варианта установки

В случае, если необходимо установить отдельный компонент Антивируса, воспользуйтесь выборочной установкой. Например, для удаленного управления Антивирусом Касперского необходимо установить на компьютер администратора только консоль администрирования.

Необходимым требованием к установке консоли администрирования Антивируса Касперского для ISA-серверов является наличие установленных на компьютере средств администрирования самого ISA-сервера.

Шаг 3. Выбор компонентов приложения для установки

На данном этапе вам необходимо выбрать компонент Антивируса Касперского, который вы хотите установить на компьютер (см. рис. 3).

Как правило, это средства администрирования, которые встраиваются в Microsoft Management Console для управления Антивирусом Касперского.

Вы также можете изменить каталог расположения консоли администрирования.

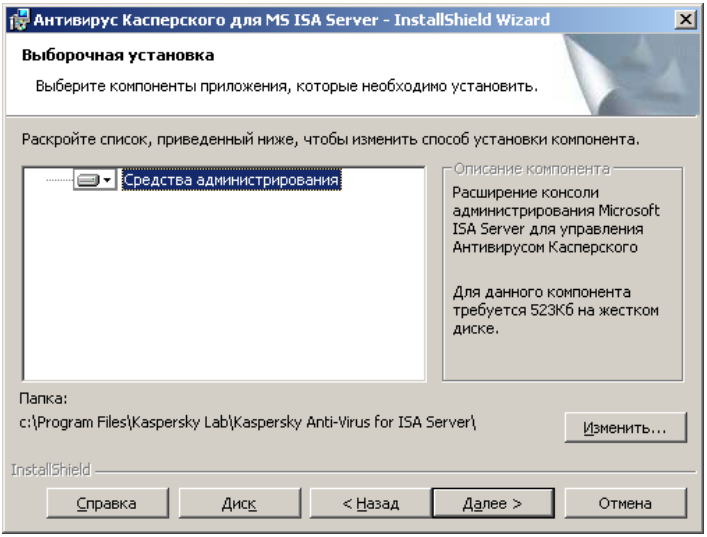


Рисунок 3. Выбор консоли администрирования для установки

Шаг 4. Настройки антивирусного ядра

На этом шаге установки продукта определяются значения параметров антивирусной защиты, которые затем будут использоваться как значения по умолчанию (см. рис. 4). Такими параметрами являются:

- Каталог файловой системы для хранения очереди объектов на проверку.

Рекомендуется разместить данный каталог на диске, содержащем не менее 200 Мбайт свободного пространства.

- Количество объектов на проверку.
- Каталог хранения антивирусных баз, используемых при поиске и лечении вирусов.
- Каталог для хранения временных файлов, создаваемых во время работы приложения.
- Количество параллельно работающих экземпляров антивирусного ядра.

Рекомендуем вам для повышения скорости антивирусной проверки и обработки объектов устанавливать по 4 экземпляра антивирусного ядра на один физический процессор. Так, например, если сервер работает на двух процессорах, рекомендуется задать 8 экземпляров антивирусного ядра.

Для каждого из перечисленных параметров уже предусмотрены значения по умолчанию. Если вы хотите изменить текущие значения, воспользуйтесь соответствующими кнопками или полями ввода.

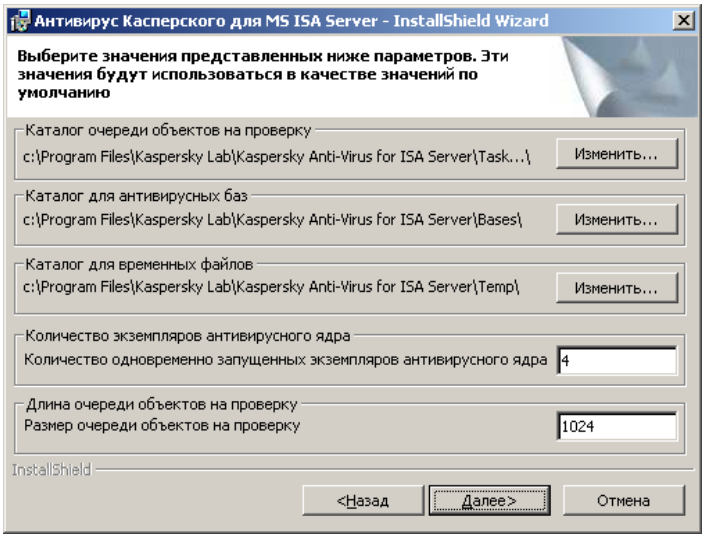


Рисунок 4. Параметры работы приложения, используемые по умолчанию

Сразу после данного этапа будет запущен процесс копирования файлов приложения на компьютер.

Шаг 5. Завершение установки приложения

Последним этапом установки Антивируса Касперского является перезагрузка службы MS ISA Server. Это необходимо для загрузки антивирусных фильтров приложения. Вы можете это сделать самостоятельно с консоли MS ISA Server, а также воспользоваться программой установки, установив соответствующий флажок(см. рис. 5).

Помните, что антивирусная защита ISA-сервера не будет запущена до тех пор, пока не будут перезагружены службы MS ISA Server.

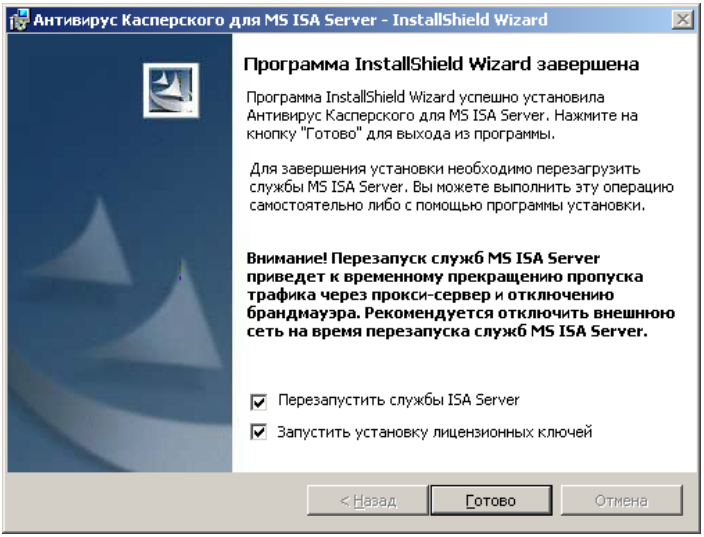


Рисунок 5. Завершение установки приложения

На данном этапе вы также можете запустить автоматическую инсталляцию лицензионных ключей приложения, установив соответствующий флажок. Без лицензионного ключа приложение не будет функционировать.

Предусмотрена также возможность выполнения данной операции после установки приложения (подробнее см. п. 4.6.2 на стр. 51).

3.2.2. Повторная установка

Повторная установка Антивируса Касперского для ISA-серверов выполняется в том случае, если первая установка приложения была

выполнена некорректно, либо если вы хотите установить какой-либо отдельный компонент Антивируса.

*Для корректной установки приложения в открывшемся окне (см. рис. 6) выберите вариант **Исправить**.*

В этом случае будет осуществлен повтор предыдущей установки Антивируса Касперского. Так, если предыдущая установка была выборочной, то и повторная установка в режиме **Исправить** также будет выполняться выборочно.

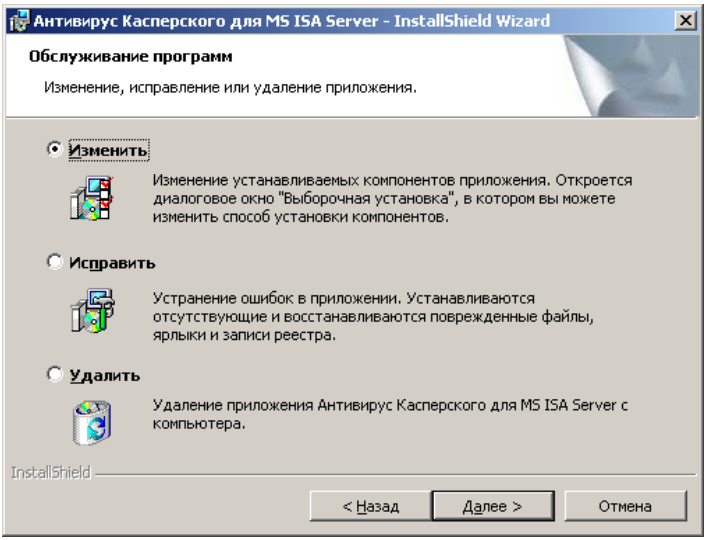


Рисунок 6. Выбор режима повторной установки приложения

*Для установки отдельного компонента приложения на компьютер выберите режим **Изменить**.*

После этого будет открыто окно выборочной установки (см. рис. 3). Далее последовательность действий идентична первой установке.

3.2.3. Возможные проблемы при установке приложения

В процессе установки Антивируса Касперского возможно возникновение ряда ошибок. Каждая из них приводит к завершению процедуры установки Антивируса Касперского.

Рассмотрим подробнее наиболее типичные ошибки и причины их возникновения.

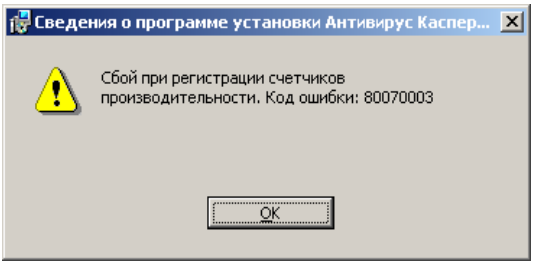


Рисунок 7. Ошибка регистрации счетчиков

Данная ошибка возникает том случае, если при установке Антивируса не удается зарегистрировать счетчики производительности. Такие счетчики используются в Windows 2000 для просмотра статистики данных приложения.

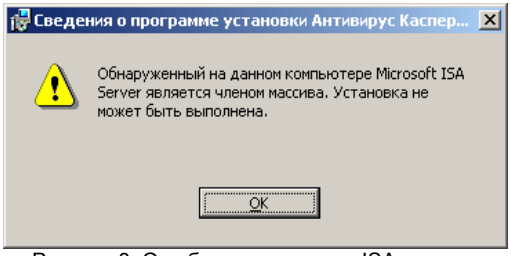


Рисунок 8. Ошибка установки на ISA-сервер, являющийся членом массива данных

Такая ошибка возникает в том случае если ISA-сервер, на который выполняется установка приложения, входит в массив серверов. Установка на такой сервер не может быть выполнена, поскольку Антивирус Касперского для ISA-серверов не поддерживает этот режим работы ISA-сервера.

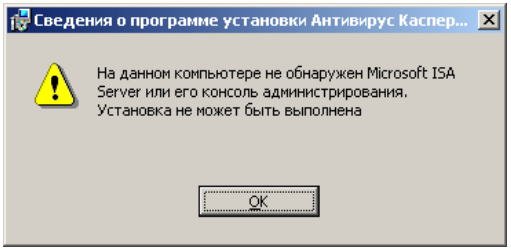


Рисунок 9. Отсутствие необходимого программного обеспечения

Если на экране появилось такое уведомление, убедитесь, что сервер удовлетворяет программным требованиям, необходимым для установки Антивируса.

Описанные выше ошибки – лишь некоторые из возможных при установке приложения. Любая критичная ошибка, как правило, приводит к прекращению установки. Во избежание возникновения ошибок убедитесь до начала установки Антивируса Касперского, что ваш сервер соответствует всем предъявленным аппаратным и программным требованиям (см. п. 1.1 на стр. 6).

ГЛАВА 4. РАБОТА С АНТИВИРУСОМ КАСПЕРСКОГО ДЛЯ ISA SERVER

Инсталляционный пакет устанавливает Антивирус Касперского в соответствии с текущим режимом работы ISA-сервера. Сразу же после установки приложение готово к запуску процесса проверки потоков данных, поскольку необходимые для проверки общие параметры уже заданы.

В установленном приложении автоматически создается пользователь default, группа пользователей default и политика default, так как наличие хотя бы одной группы пользователей и одной антивирусной политики, назначаемой этой группе, является необходимым условием для функционирования Антивируса Касперского. Удалять пользователя, группу и политику по умолчанию нельзя!

4.1. Настройки процесса проверки данных по умолчанию

Параметры процесса проверки размещены на закладках диалогового окна **Свойства Антивируса Касперского для ISA Server**. По умолчанию заданы значения следующих полей:

- на закладке **HTTP** формируются ограничения на работу приложения (подробнее см. п. 4.2.1.2 на стр. 28) и тексты информационных сообщений (см. п. 4.4 на стр. 46):
    - *Максимальное время проверки первого пакета данных в секундах* – 30 секунд;
    - *Максимальный интервал между отправками данных клиенту в секундах* – 10 секунд;
    - *Количество данных в процентах, не отправляемый клиенту до завершения проверки* – 10 %;
    - *Разрешить дозагрузку файлов* – включено.

- *Сообщение, отправляемое клиенту, если произошла ошибка*:

```
<html>
<head>
<title>Kaspersky Anti-Virus for Microsoft ISA
Server</title>
</head>
<body>
<h1>Kaspersky Anti-Virus for Microsoft ISA
Server</h1>
<p>Internal Scanner Error "%ERR_TEXT%"
(%ERR%)</p>
</body>
</html>
```

- *Сообщение, отправляемое клиенту, если найден вредоносный объект*:

```
<html>
<head>
<title>Kaspersky Anti-Virus for Microsoft ISA
Server</title>
</head>
<body>
<h1>Kaspersky Anti-Virus for Microsoft ISA
Server</h1>
<p>The requested URL "%URL%" is infected with
%VIRUSNAME% virus</p>
</body>
</html>
```

- на закладке **FTP** (подробнее см. п. 4.2.1.3 на стр. 31) содержится информация о *количестве данных, полученных сервером до того, как первый пакет с данными отправляется клиенту, кбайт* – 8 килобайт;

- на закладке **Антивирус** (подробнее см. п. 4.2.1.1 на стр. 26) приводится набор рабочих каталогов Антивируса Касперского для ISA-серверов:

  - *Каталог для хранения антивирусных баз:*
    C:/Program Files/Kaspersky Lab/KAV for ISA/bases
  - *Каталог для очереди объектов на проверку*:
    C:/Program Files/Kaspersky Lab/KAV for ISA/TaskQueue
  - *Каталог для временных файлов*:
    C:/Program Files/Kaspersky Lab/KAV for ISA/Temp

- *Количество одновременно запущенных экземпляров антивирусного ядра* – 4 экземпляра;
- *Размер очереди объектов на проверку* – 1024 объекта;
- *Параметры проверки*:
  - *Лечить объекты, если возможно*.
  - *Проверять архивы*.
  - *Проверять упакованные исполняемые файлы*.

- на закладке **Лицензирование** (подробнее см. п. 4.6.2 на стр. 51) указывается количество дней, в течение которых до окончания лицензии администратор будет уведомляться об истечении срока ее действия. Количество дней задается в поле *Уведомлять об истечении срока действия лицензии* и равняется по умолчанию семи дням. Уведомление выполняется посредством сообщений, выводящихся в системный журнал компьютера, на котором установлен Антивирус Касперского для ISA-серверов.
- на закладке **Обновление** (подробнее см. п. 4.3 на стр. 43) определяется ресурс для обновления антивирусных баз, настраивается процедура и частота ее выполнения. По умолчанию обновление выполняется ежедневно в 23:15 с автоматически выбираемого сервера обновлений.

4.2. Управление процессом проверки

При установке консоль администрирования Антивируса Касперского встраивается в MMC.

Управление процессом проверки осуществляется через главное окно Антивируса Касперского для ISA-серверов, представленное на рис. 10.

Дерево приложения включает в себя два узла: **Группы** и **Политики**.

Способ отображения узлов в правой части главного окна может корректироваться. По умолчанию узлы приложения и все возможные операции с ними отображаются в виде **Панели задач**. Вы можете изменить способ отображения на **Список**, воспользовавшись соответствующим

пунктом контекстного меню, которое открывается по щелчку правой кнопки мыши на узле MMC **Антивирус Каспеского**[2] (см. рис. 11).

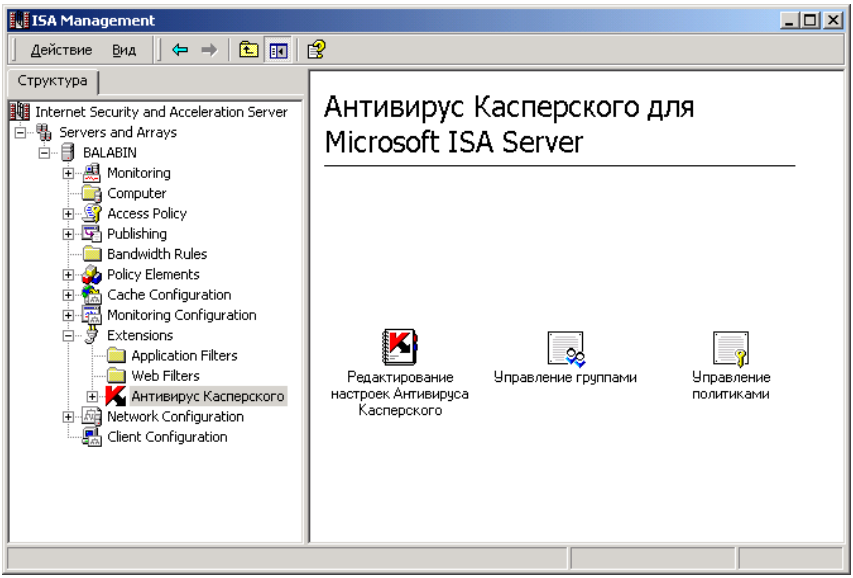


Рисунок 10. Главное диалоговое окно Антивируса Касперского для MS ISA Server

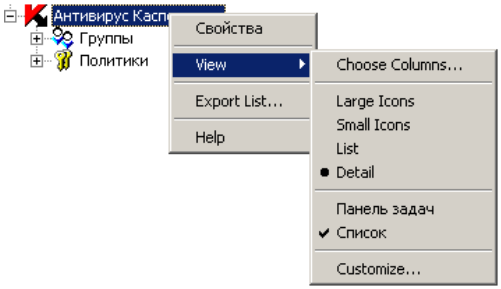


Рисунок 11. Контекстное меню

Для настройки процесса управления используйте следующие возможности Антивируса Касперского:

[2] Далее в документации приводится описание работы с элементами главного окна, отображаемыми в виде Панели задач.

- редактирование общих параметров, влияющих на работу Антивируса Касперского в целом, включая все политики антивирусной проверки (см. п. 4.2.1 на стр. 26);
- определение новых правил антивирусной проверки, отличных от установленных по умолчанию, при помощи создания новой политики (см. п. 4.2.3 на стр. 36). В политике переопределяются настройки фильтрации трафика, а затем к созданной политике прикрепляют группу пользователей.

4.2.1. Настройка общих параметров антивирусной проверки

Администратор может изменять настройки общих параметров антивирусной проверки по своему усмотрению.

Чтобы перейти к настройкам общих параметров антивирусной проверки,

выберите в главном окне приложения пункт **Редактирование настроек Антивируса Касперского**. Откроется диалоговое окно **Свойства Антивируса Касперского для ISA Server**.

Общие параметры антивирусной проверки расположены на закладках **Антивирус**, **HTTP** и **FTP**.

4.2.1.1. Общие параметры работы приложения

На закладке **Антивирус** (см. рис. 12) вы можете изменять настройки Антивируса Касперского, влияющие на работу приложения в целом.

В верхней части закладки расположены три поля, в которых вы можете отредактировать пути к рабочим каталогам Антивируса Касперского, установленные по умолчанию. Данные каталоги предназначены для:

- хранения антивирусных баз, используемых при антивирусной проверке;
- размещения объектов в очередь на проверку. В этом каталоге хранятся объекты, которые ждут проверки либо проверяются, либо уже проверены и готовы к отправке к клиенту;
- размещения временных файлов. При включенной проверке архивов и упакованных исполняемых файлов Антивирус Касперского разме-

щает распакованные файлы во временном каталоге. После проверки временные файлы удаляются.

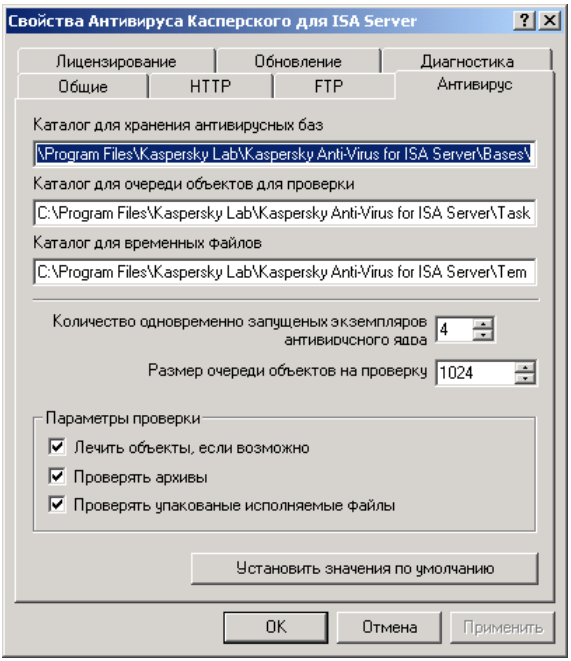


Рисунок 12. Закладка **Антивирус**

Совместно с Антивирусом Касперского для MS ISA-серверов могут использоваться дополнительные антивирусные программы для антивирусного контроля над файловой системой компьютера (например, Антивирус Касперского для Microsoft NT Server). В этом случае для корректной работы Антивируса Касперского для MS ISA-серверов необходимо настроить подобные антивирусные программы так, чтобы рабочие каталоги Антивируса Касперского для очереди объектов и временных файлов не подвергались антивирусной проверке.

Для увеличения пропускной способности Антивируса Касперского при обработке больших потоков данных предусмотрено формирование нескольких одновременно работающих экземпляров антивирусного ядра приложения. По умолчанию при старте Антивируса Касперского формируются и параллельно работают четыре экземпляра антивирусного ядра.

Чтобы изменить количество одновременно запущенных копий,

укажите необходимое число в поле **Количество одновременно запущенных экземпляров антивирусного ядра**.

Вы можете задать до 32 включительно одновременно работающих экземпляров антивирусного ядра. Мы рекомендуем вам создавать на каждом физическом процессоре по 4 экземпляра.

Чтобы изменить размер очереди объектов, проверяемых приложением,

в поле **Размер очереди объектов на проверку** укажите максимальное количество объектов, которые могут быть одновременно размещены в рабочем каталоге для объектов, поставленных в очередь на антивирусную проверку.

В нижней части закладки расположены **Параметры проверки** (см. рис. 12):

- если вы хотите, чтобы Антивирус Касперского при обнаружении инфицированного файла пытался его вылечить, установите флажок **Лечить объекты, если возможно**;

Возможно лечение только тех файлов, которые передаются по HTTP-протоколу. При обнаружении зараженного файла, пересылаемого по FTP-протоколу, Антивирус Касперского без попытки лечения блокирует доступ к зараженному объекту.

- если вы хотите включить механизм распаковки архивов для проверки заархивированных файлов, установите флажок **Проверять архивы**;

Если механизм распаковки архивов отключен, архивы будут проверяться как обычные файлы. В этом случае могут быть обнаружены только те вирусы, которые внедрились уже в файл архива. Антивирус Касперского не проверяет архивы, защищенные паролем!

- если вы хотите проверять упакованные исполняемые файлы, установите соответствующий флажок **Проверять упакованные исполняемые файлы**.

Как и в случае с архивами, если данный параметр проверки отключен, то исполняемые файлы будут проверяться как неупакованные, и вирус может быть обнаружен, только если он внедрился в уже упакованный файл.

Поскольку все эти режимы могут увеличить затраты ресурсов на антивирусную проверку данных, то это сказывается на увеличении времени задержки файлов перед отправкой пользователю.

4.2.1.2. Параметры проверки HTTP-потока данных

На закладке **HTTP** (см. рис. 13) вы можете настраивать проверку HTTP-трафика, а также ограничения на работу приложения с потоком данных, перемещаемых по HTTP-протоколу. Здесь же при необходимости редактируются тексты информационных сообщений, передаваемых клиентам.

В первых трех полях задайте параметры, контролирующие работу Антивируса Касперского с HTTP-трафиком:

- укажите максимальное время задержки данных, проверяемых приложением, в поле **Максимальное время проверки первого пакета данных в секундах**. В пределах этого времени данные проверяются, после проверки преобразуются в поток и направляются клиенту, запросившему их. Этот параметр существенно влияет на то, что происходит с зараженным файлом в случае его обнаружения:
    - если инфицированный файл был обнаружен и вылечен до того, как пользователю отправился первый пакет с данными, содержащими часть данного файла, то пользователь получает преобразованный вылеченный файл;
    - если зараженный файл обнаружен Антивирусом Касперского уже после того, как пользователю был отправлен первый пакет с данными, содержащими часть этого файла, то соединение будет разорвано. Но при повторном запросе данного файла пользователь сразу же получит уведомление о том, что запрашиваемый файл был заражен.

При повторном запросе пользователь получит уведомление о зараженном файле только в том случае, если между первым и вторым запросом пройдет не более 100 секунд. В данной версии приложения откорректировать значение этого параметра невозможно.

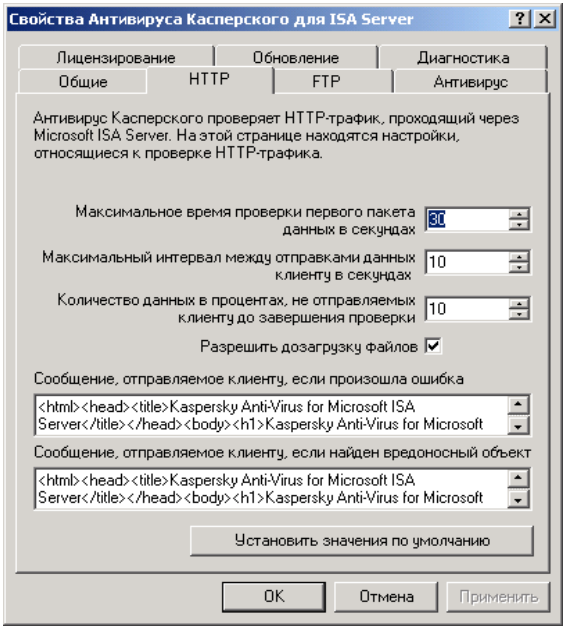


Рисунок 13. Закладка **HTTP**

- укажите время, в течение которого к клиенту должен отправиться следующий пакет проверенных данных, запрашиваемый им, в поле **Максимальный интервал между отправками данных клиенту в секундах**;

Значение данного поля не должно превышать значения поля **Максимальное время проверки первого пакета данных в секундах**.

- задайте в процентах объем данных, накапливаемых Антивирусом Касперского для анализа и проверки, в поле **Количество данных в процентах, не оправляемый клиенту до завершения проверки**.

Флаг **Разрешить дозагрузку файлов** регулирует возможность дозагрузки запрашиваемых клиентами данных в случае, напрмер, разрыва соединения при загрузке.

Следует, однако, помнить о том, что Антивирус Касперского сможет обнаружить вредоносный код только в том случае, если он будет полностью присутствовать в любой части загружаемого частями объекта. В случае если при частичной загрузке объекта вирус будет также разделен на части,

не исключена вероятность его распространения после восстановления целостности объекта.

О полях, в которых формируются сообщения, отправляемые пользователю, см. подробнее в п. 4.4 на стр. 46.

В любой момент работы с настройками вы можете вернуться к настройкам по умолчанию. Для этого нажмите на соответствующую кнопку.

4.2.1.3. Параметры проверки FTP-потока данных

На закладке **FTP** (см. рис. 14) регулируется проверка данных ISA-сервера, поступающих по протоколам FTP и FTP over HTTP.

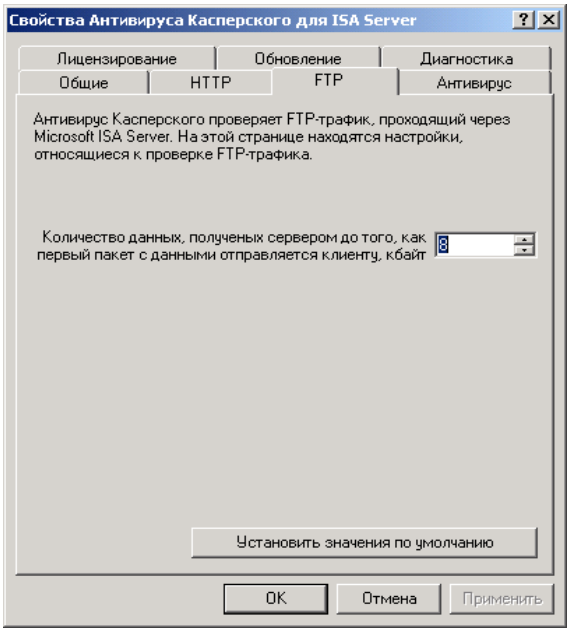


Рисунок 14. Закладка **FTP**

Дополнительно к режиму антивирусной проверки вы можете установить количество накапливаемых для анализа данных, полученных сервером по FTP-протоколу. После того, как указанный объем данных будет получен сервером, начинается отправка данных клиенту. Максимальное значение этого поля – 1024 Кбайт.

В любой момент работы с настройками вы можете вернуться к настройкам по умолчанию. Для этого нажмите на соответствующую кнопку.

4.2.2. Управление группами клиентов

В каждую группу включены клиенты внутренней сети, к которым могут быть применены одинаковые политики. Каждый клиент может входить в одну или несколько групп.

К клиентам группы default автоматически относятся все клиенты ISA-сервера, не внесенные ни в какую другую группу.

Если клиент входит одновременно в несколько групп, то для него производится антивирусная проверка в соответствии с группой, обладающей наименее строгими условиями проверки.

Например, клиент входит в группу **Бухгалтерия**, для которой производится проверка запрашиваемого потока данных, и в группу **Администраторы**, для которой проверка аналогичного потока данных не производится. В этом случае при антивирусной проверке данного клиента будут использоваться настройки группы **Администраторы**.

В настоящей версии Антивируса Касперского клиенты задаются IP-адресом либо группой IP-адресов. Клиентами, задаваемыми конкретным IP-адресом, могут быть компьютеры с установленными сетевыми сервисами и постоянным IP-адресом. Например, это могут быть почтовые сервера. Для клиентов сети, не имеющих постоянного IP-адреса, возможно создание одного клиента, который будет задан адресом подсети и маской подсети.

Чтобы перейти к списку групп,

в главном окне Антивируса Касперского выберите **Управление группами**. Откроется окно **Управление группами клиентов Антивируса Касперского** (см. рис. 15).

Вы также можете перейти в окно управления группами клиентов, выбрав в дереве приложения узел **Группы**.

Администратор может переименовывать имеющиеся группы, менять их описания, создавать новые и удалять ненужные группы.

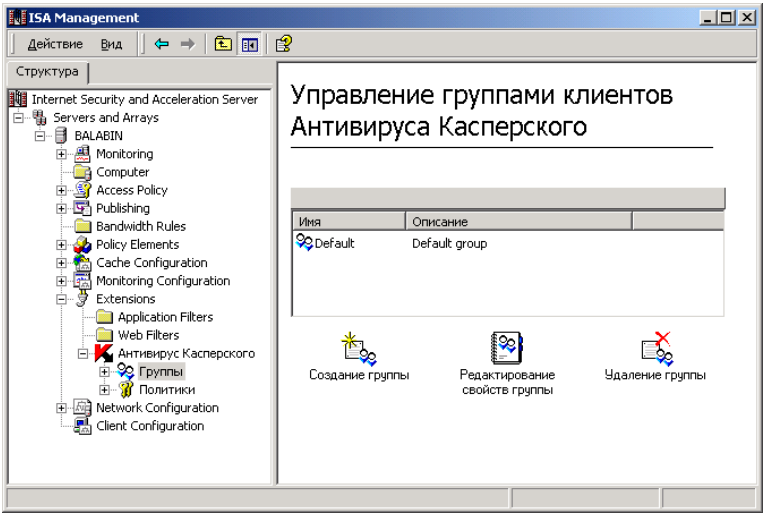


Рисунок 15. Диалоговое окно **Управление группами клиентов Антивируса Касперского**

Чтобы создать группу клиентов:

1. Выберите пункт **Создание группы**.
2. В окне **Создание группы** (см. рис. 16) введите название группы и ее описание.
3. В следующем диалоговом окне (см. рис. 17) нажмите на кнопку **Добавить клиентов…**
4. В диалоговом окне **Клиенты** (см. рис. 18) выберите клиента из списка существующих либо создайте нового, нажав на кнопку **Новый…**
5. Если вы выбрали создание нового клиента, то в окне **Свойства клиента** (см. рис. 19) заполните поле **Название клиента** и выберите для заполнения:
   - **Один IP-адрес**, если добавляется клиент с постоянным IP-адресом;
   - **Подсеть**, если клиент может быть задан маской подсети;
   - **Диапазон адресов**, если клиент задается пространством IP-адресов, ограниченным указанным диапазоном.

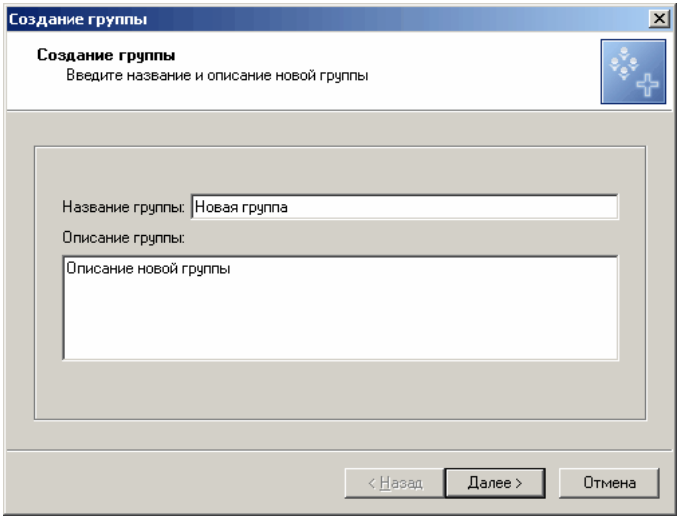


Рисунок 16. Создание новой группы

6. После того, как нужные клиенты будут включены в группу, завершите создание группы, нажав на кнопку **Готово**.

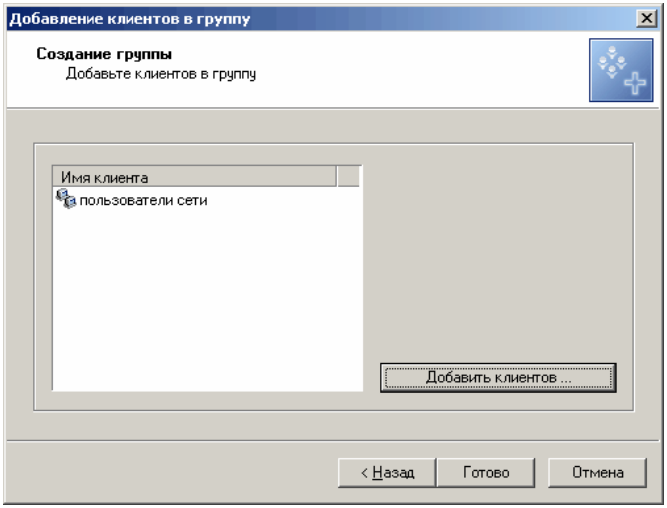


Рисунок 17. Добавление клиентов в новую группу

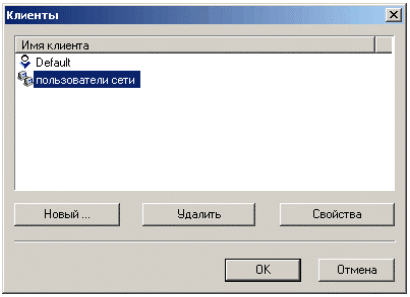


Рисунок 18. Диалоговое окно **Клиенты**

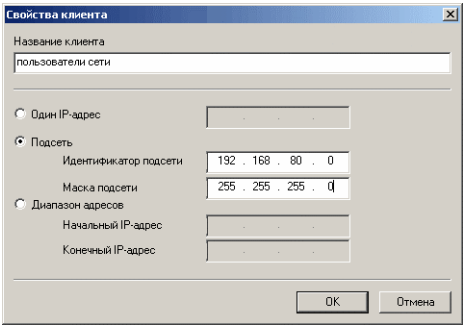


Рисунок 19. Добавление нового клиента в группу

Вновь созданная группа сразу прикрепляется к политике default.

Чтобы изменить описание и состав клиентов групп,

в окне **Управление группами клиентов Антивируса Касперского** (см. рис. 15) выделите нужную группу и выберите пункт **Редактирование свойств группы**.

В раскрывшемся окне на закладке **Общие** (см. рис. 20) вы можете переименовать группу и изменить ее описание. На закладке **Клиенты** (см. рис. 21) возможно добавление нового либо удаление существующего клиента из группы.

При удалении существующего клиента информация о нем удаляется только из редактируемой группы.

Чтобы удалить группу,

в окне **Управление группами клиентов Антивируса Касперского** (см. рис. 15) выделите нужную группу и выберите пункт **Удаление группы**.

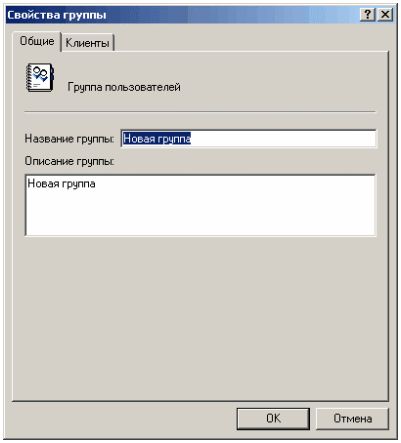


Рисунок 20. Закладка **Общие**

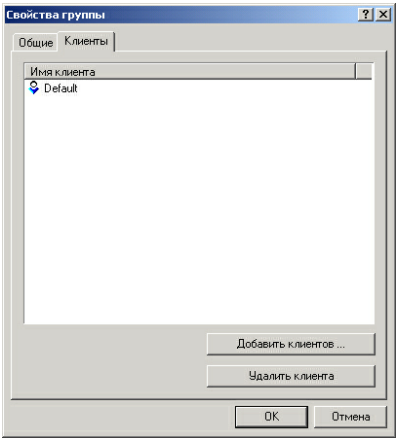


Рисунок 21. Закладка **Клиенты**

4.2.3. Ведение политик антивирусной проверки

Для каждой группы клиентов может быть задана своя политика. В политиках определяются дополнительные параметры фильтрации входящего потока данных, которые позволяют задавать различные правила для разных групп клиентов и тем самым могут ускорить процесс антивирусной проверки.

Каждой группе может быть назначена только одна политика. Например, если группа **Администраторы** входит в политику **Администраторы**, то она не может входить в другую политику.

Чтобы перейти к списку политик,

в главном окне Антивируса Касперского выберите **Управление политиками**. Откроется окно **Управление политиками для Антивируса Касперского** (см. рис. 22).

Вы также можете перейти в окно управления политиками, выбрав в дереве приложения узел **Политики**.

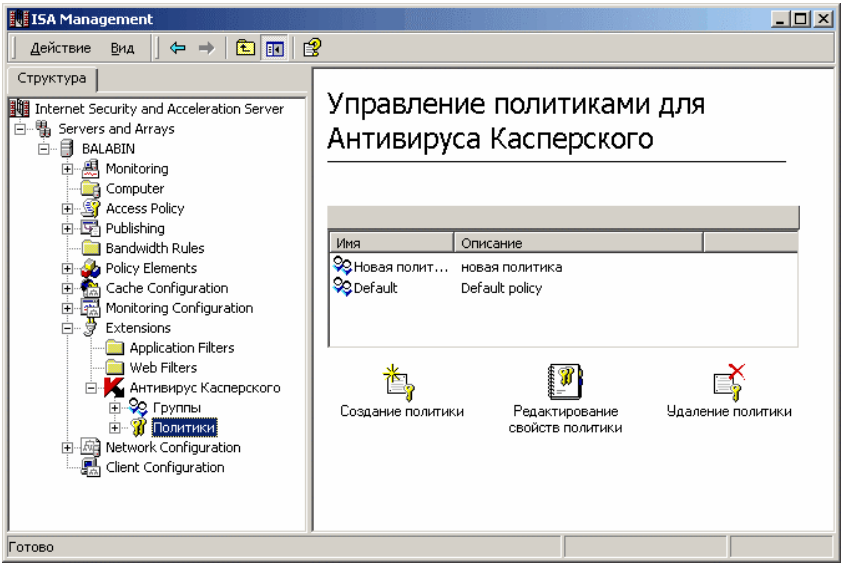


Рисунок 22. Диалоговое окно **Управление политиками для Антивируса Касперского**

Чтобы создать новую политику:

1. Выберите пункт **Создание политики**.
2. В окне **Создание политики** (см. рис. 23) введите название политики и ее описание.
3. В следующем диалоговом окне (см. рис. 24) нажмите на кнопку **Добавить группу** и из раскрывающегося списка групп выберите ту группу клиентов, на которую будет распространяться новая политика.
4. В раскрывшемся диалоговом окне (см рис. 25) нажмите на кнопку **Добавить сервер**, чтобы указать доверительные сервера, для входящего трафика с которых не будет производиться антивирусная проверка. В окне **Доверительный сервер** (см. рис. 31) задайте описание сервера и его свойства (подробнее о доверительных серверах см. п. 4.2.3.1 на стр. 41). После того, как будет сформирован список доверительных серверов, нажмите на кнопку **Далее**.

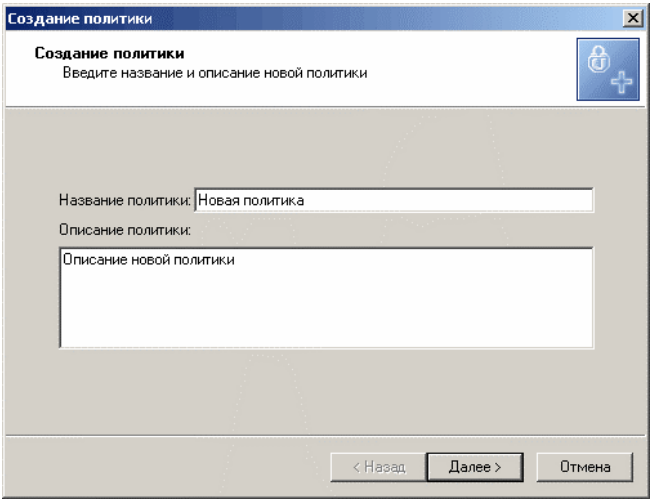


Рисунок 23. Создание новой политики

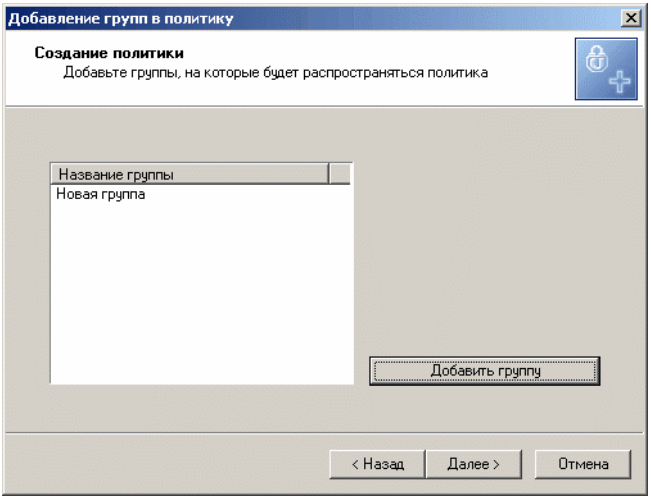


Рисунок 24. Добавление группы клиентов

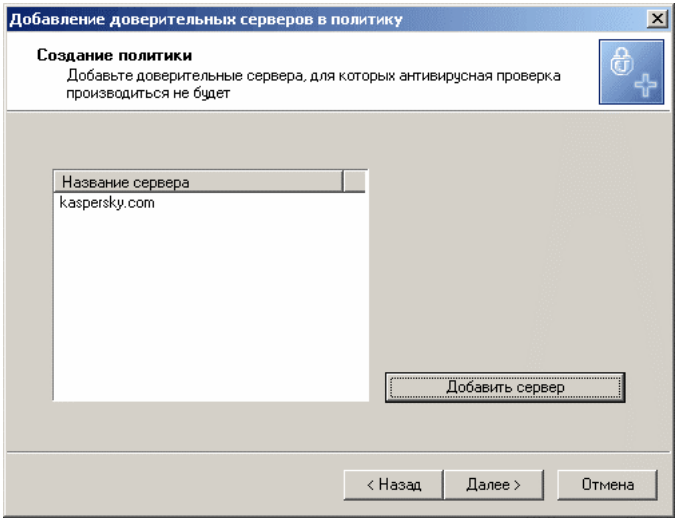


Рисунок 25. Добавление доверительных серверов

5. В следующем диалоговом окне (см. рис. 26) нажмите на кнопку **Добавить тип объектов**, чтобы добавить тип объектов, для которых не будет производиться антивирусная проверка (подробнее см. п. 4.2.3.2 на стр. 42).

6. После того, как будет сформирован список типов, нажмите на кнопку **Готово**.

Чтобы редактировать свойства политики,

в окне **Управление политиками для Антивируса Касперского** (см. рис. 22) выделите нужную политику и выберите пункт **Редактирование политики**.

В раскрывшемся окне на закладке **Общие** (см. рис. 27) вы можете переименовать политику и изменить ее описание.

На закладке **Группы** (см. рис. 28) возможно изменение списка групп, на которые распространяется данная антивирусная политика, добавление новой группы в список групп либо удаление из списка одной из групп.

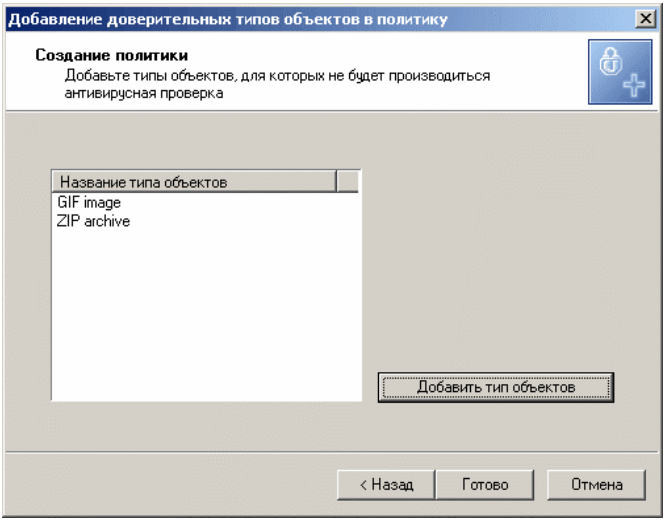


Рисунок 26. Добавление типа объекта

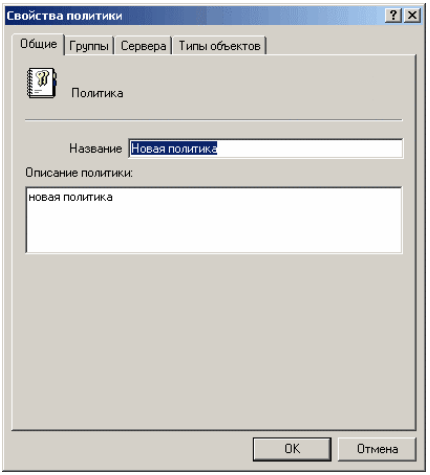


Рисунок 27. Закладка **Общие**

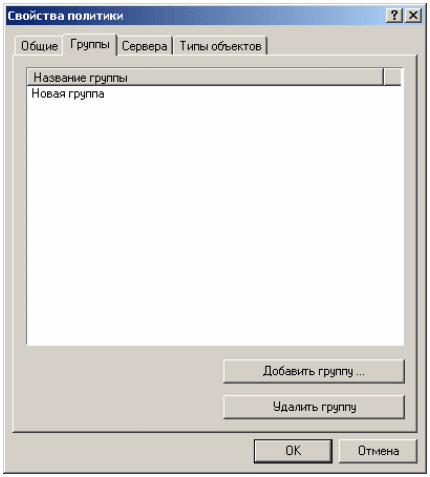


Рисунок 28. Закладка **Группы**

На закладках **Сервера** (см. рис. 29) и **Типы объектов** (см. рис. 30) осуществляется редактирование списков доверительных серверов и непроверяемых типов объектов для данной антивирусной политики.

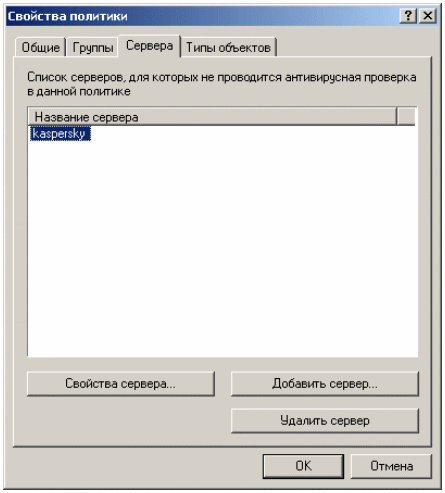


Рисунок 29. Закладка **Сервера**

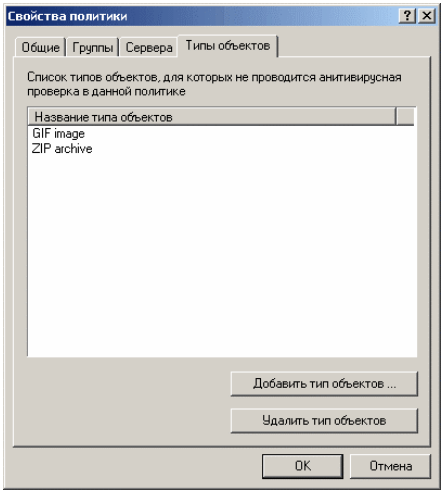


Рисунок 30. Закладка **Типы объектов**

Чтобы удалить политику,

в окне **Управление политиками для Антивируса Касперского** (см. рис. 22) выделите нужную политику и выберите пункт **Удаление политики**.

После удаления политики, все группы клиентов, для которых удаляемая политика определяла параметры антивирусной проверки, автоматически прикрепляются к политике default.

4.2.3.1. Ведение списка доверительных серверов

Для каждой политики администратор может задать список доверительных серверов, входящий трафик с которых не будет подвергаться антивирусной проверке. В такой список включаются те сервера, трафику с которых мы доверяем, поскольку слишком мала вероятность наличия в нем вредоносных объектов. Чем больше список доверительных серверов в политике, тем меньше степень вмешательства Антивируса Касперского в потоки данных, которые запрашивают клиенты групп, относящихся к данной политике.

Управление списком доверительных серверов осуществляется на закладке **Сервера** (см. рис. 29) диалогового окна свойств политики.

При добавлении доверительного сервера открывается диалоговое окно **Доверительный сервер** (см. рис. 31). Вы можете задать параметры доверительного сервера одним из четырех способов:

- доменным именем сервера;
- IP-адресом сервера;
- подсетью;
- группой IP-адресов, ограниченных указанным диапазоном.

*Чтобы удалить доверительный сервер из списка, нажмите соответствующую кнопку на закладке **Сервера** (см. рис. 29).*

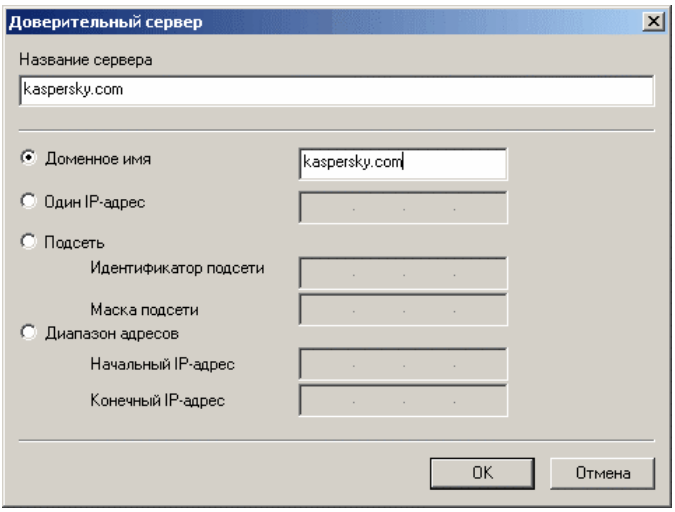


Рисунок 31. Добавление доверительного сервера

4.2.3.2. Формирование списка непроверяемых объектов

Как и формирование списков доверительных серверов, задание типов объектов, которые не будут подвергаться антивирусной проверке, позволяют снизить нагрузку на ISA-сервер.

Управление списком типов осуществляется на закладке **Типы объектов** (см. рис. 30) диалогового окна свойств редактируемой политики. При добавлении нового типа открывается диалоговое окно **Тип объектов** (см. рис. 32).

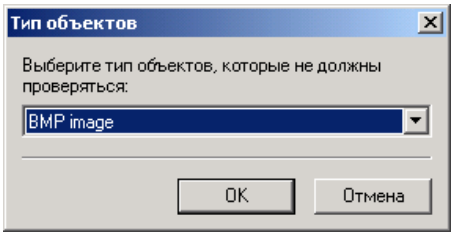


Рисунок 32. Добавление типа объекта

4.3. Обновление антивирусных баз

Обновление антивирусных баз может выполняться автоматически с заданным периодом обновления и вручную администратором. Возможны два способа получения антивирусных баз:

- через интернет по FTP- или HTTP-протоколу с серверов обновлений Лаборатории Касперского;
- из локальной или сетевой папки.

Управление обновлением антивирусных баз осуществляется на закладке **Обновление** диалогового окна **Свойства Антивируса Касперского для ISA Server** (см. рис. 33). По умолчанию включено ежедневное обновление с серверов Лаборатории Касперского.

Для настройки обновления антивирусных баз через интернет выполните следующие действия:

1. Выберите способ обновления **Обновлять через интернет**.
2. Нажмите на кнопку **Настройки обновления через интернет…**, чтобы указать сервер-ресурс получения обновлений.

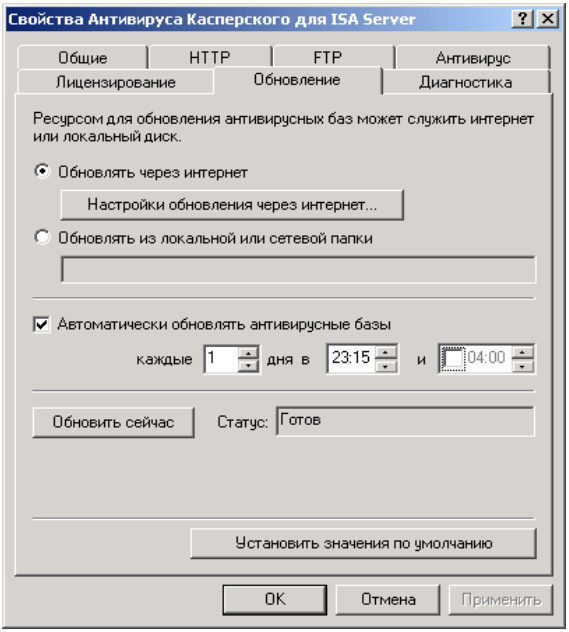


Рисунок 33. Задание параметров обновления антивирусных баз

3. В раскрывшемся диалоговом окне (см. рис. 34):

   - выберите **Автоматически выбирать сервер обновлений**, если для получения обновлений вы хотите использовать случайным образом выбранный приложением сервер;
   - выберите **Использовать указанный сервер**, если вы хотите самостоятельно определить сервер для получения обновлений. В поле ввода укажите адрес сервера.

4. В разделе **Использовать HTTP-прокси** настройте параметры HTTP прокси-сервера, если таковой используется в системе:

   - Выберите **Использовать локальный прокси ISA-сервера**, чтобы приложение при обновлении антивирусных баз через интернет использовало локальный прокси-сервер MS ISA Server.
   - Выберите **Использовать другой прокси-сервер** и явно укажите в полях **Имя прокси-сервера** и **порт** прокси-сервер, отличный от локального прокси ISA-сервера.

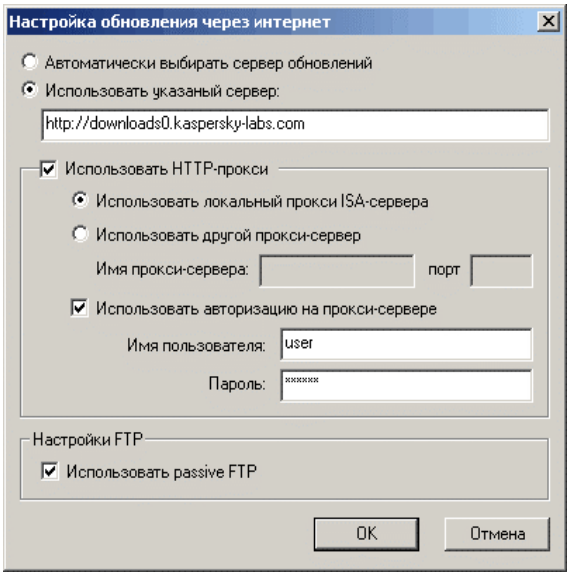


Рисунок 34. Настройка обновления через интернет

5. В разделе **Настройки FTP** установите соответствующий флажок, чтобы использовать пассивный режим работы FTP-сервера при загрузке обновлений по FTP.

Чтобы получать обновления антивирусных баз из локальной сети,

выберите способ обновления **Обновлять из локальной или сетевой папки** и в поле укажите полный путь к ней.

4.3.1. Автоматическое обновление антивирусных баз по расписанию

*Чтобы включить автоматическое обновление, установите флажок **Автоматически обновлять антивирусные базы**.*

Обновление антивирусных баз происходит в заданный администратором ISA-сервера период. По умолчанию задано обновление ежедневно в 23:15.

В следующих трех полях (см. рис. 33) вы можете настроить частоту и время проведения обновлений антивирусных баз.

4.3.2. Ручной запуск получения обновлений

На закладке **Обновление** вы также можете осуществить ручной запуск получения обновлений в соответствии с заданными настройками, нажав на кнопку **Обновить сейчас**.

Вы можете провести ручное обновление независимо от того, включен или выключен автоматический режим обновления антивирусных баз.

В поле **Статус** выводится текущее состояние обновления.

4.4. Настройка уведомлений пользователей

Если приложение обнаруживает в потоке данных инфицированный файл, который невозможно вылечить, соединение разрывается, и пользователь, запросивший эти данные, получает HTML-сообщение об обнаружении вируса.

Сообщения формируются только в том случае, если вредоносный объект был обнаружен **Web-фильтом Антивируса Касперского** или **HTTP-фильтром Антивируса Касперского**.

Сообщение формируется в поле **Сообщение, отправляемое клиенту, если найден вредоносный объект** (см. рис. 13) и по умолчанию содержит следующую информацию:

```
<html>
<head>
<title>Kaspersky Anti-Virus for Microsoft ISA Server</title>
</head>
<body>
<h1>Kaspersky Anti-Virus for Microsoft ISA Server</h1>
<p>The requested URL "%URL%" is infected with %VIRUSNAME%
virus</p>
</body>
</html>
```

В тексте сообщения используются расширяемые переменные:

- `%URL%` – адрес интернет-ресурса, запрашиваемый пользователем;
- `%VIRUSNAME%` – имя вируса, которым заражен поток.

В случае если при выполнении запроса возникла внутрисистемная ошибка, пользователю, запросившему данные, отправляется следующее HTML-сообщение, сформированное в поле **Сообщение, отправляемое клиенту, если произошла ошибка** на закладке **HTTP** окна свойств Антивируса Касперского (см. рис. 13):

```
<html>
<head>
<title>Kaspersky Anti-Virus for Microsoft ISA Server</title>
</head>
<body>
<h1>Kaspersky Anti-Virus for Microsoft ISA Server</h1>
<p>Internal Scanner Error "%ERR_TEXT%" (%ERR%)</p>
</body>
</html>
```

В тексте используются следующие расширяемые переменные:

- `%ERR_TEXT%` – текстовое описание ошибки;
- `%ERR%` – код ошибки.

Вы можете отредактировать сообщения, направляемые пользователю, на закладке **HTTP** диалогового окна **Свойства Антивируса Касперского для ISA-сервера** (см. рис. 13). Максимальная длина сообщения – 10240 байт. Кодовая страница – win1251.

4.5. Проверка корректности работы Антивируса

После установки и настройки Антивируса Касперского мы рекомендуем вам проверить правильность настроек и корректность работы приложения с помощью тестового "вируса" и его модификаций.

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.

При попытке загрузки тестового "вируса" Антивирус обнаруживает его, идентифицирует как инфицированный объект, не подвергающийся лечению, и выполняет действие, установленное администратором для такого объекта. Так, в случае действия настроек по умолчанию (см. п. 4.1 на стр. 22) при попытке загрузить тестовый "вирус" соединение с ресурсрм будет разорвано, и на экран будет выведено сообщение о том, что данный объект заражен вирусом *eicar*.

4.6. Статистика и диагностика работы программы

Антивирус Касперского предоставляет возможность просматривать статистику своей работы посредством стандартных счетчиков производительности и редактировать способы уведомления администратора о важном событии. Также вы можете настраивать журнализацию событий Антивируса Касперского в формируемых им журналах, чтобы на любом этапе антивирусной фильтрации потоков данных осуществлять диагностику его работы.

В данном разделе Руководства мы подробнее остановимся на каждой из перечисленных возможностей.

4.6.1. Сбор и просмотр статистической информации

Просмотр и управление сбором статистической информации о работе Антивируса Касперского осуществляется через стандартные счетчики производительности Windows, доступные через консоль **Производительность** (**Пуск → Настройка → Панель управления → Администрирование → Системный монитор**).

Оценка работы приложения проводится по следующим параметрам:

- всего вылеченных объектов;
- всего зараженных (невылеченных) объектов;

- всего испорченных объектов;
- всего непроверенных объектов;
- всего ошибок проверки;
- всего подозрительных объектов;
- всего прерванных проверок;
- всего проверено объектов;
- всего чистых объектов;
- длина очереди задания;
- объем обработанного Антивирусом Касперского трафика в Кбайтах.
- число обычных, прямых и сложных загрузок данных каждым из фильтров Антивируса Касперского (FTP- , HTTP- и Web-фильтр).

Чтобы выбрать, какие сведения будут отражаться в статистике:

1. Перейдите в диалоговое окно **Добавить счетчики** (см. рис. 35) и выберите **Использовать локальные счетчики**, если администрирование ISA-сервера осуществляется непосредственно на сервере с установленной системой, либо **Выбрать счетчики с компьютера**, если администрирование ISA-сервера осуществляется через удаленный доступ с рабочего места администратора.
2. Из раскрывающегося списка **Объект** выберите объект **KL4ISA**. В нижнем левом поле появится список всех возможных параметров, по которым осуществляется сбор статистической информации о работе приложения:
    - Выберите **Все счетчики**, если хотите просматривать статистику по всем параметрам работы Антивируса Касперского и нажмите на кнопку **Добавить**.
    - Выберите **Выбрать счетчики из списка**, если хотите просматривать информацию только по нескольким параметрам работы приложения. Затем выберите из списка нужный счетчик и нажмите на кнопку **Добавить**.

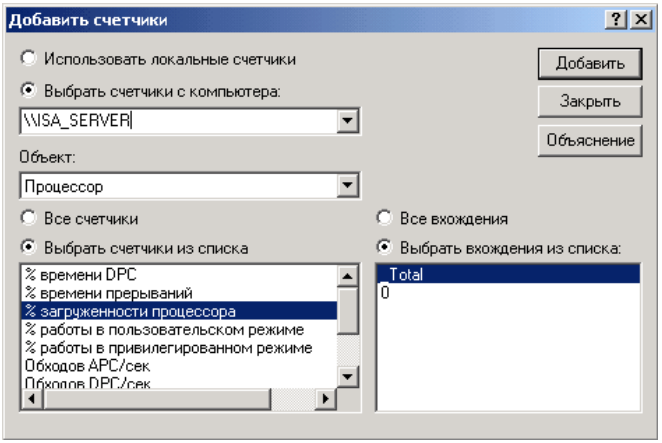


Рисунок 35. Настройка отображения статистики

Следующие настройки обычно требуются только для просмотра счетчиков производительности с удаленного компьютера!

3. Просмотр статистики с удаленного компьютера также требует наличия следующих привилегий пользователя на том компьютере, где установлен Антивирус Касперского для MS ISA Server:

   - права на чтение файлов:

     `%windir%\System32\PERFC`*xxx*`.DAT`
     `%windir%\system32\PERFH`*xxx*`.DAT`

   - права на чтение разделов реестра:

     `HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Perflib`

     `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\Winreg`

   - права на чтение и запись разделов реестра:

     `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Anti-Virus KL for MS ISA`

   - системные привилегии (назначаются в **Панель управления → Администрирование → Локальная политика безопасности → Параметры безопасности → Локальные политики → Назначение прав пользователя**) на:

     - профилирование загруженности системы;

- профилирование одного процесса.

Приведенный выше перечень привилегий описан в статье Microsoft Knowledge Base Q158438
http://support.microsoft.com/default.aspx?kbid=158438
По умолчанию данные права есть у пользователей, являющихся членами локальной группы **Администраторы** компьютера, на котором установлен Антивирус Касперского для MS ISA Server.

4. Для удаленного просмотра статистики на сервере с установленным Антивирусом Касперского для MS ISA Server также должен быть:
   - запущен сервис **Служба удаленного управления реестром**;
   - должен быть доступ по NetBIOS (в свойствах сетевого подключения **Сетевое окружение → Свойства → Подключение к локальной сети → Свойства** должен быть установлен флаг Служба доступа к файлам и принтерам сетей Microsoft).

4.6.2. Уведомление администратора посредством ISA Server Alerts

Системные средства ISA Server Alerts позволяют различными способами (запись в системный журнал, уведомление почтовым сообщением и т.д.) информировать администратора о событиях исключительной важности, возникающих при работе какого-либо их установленных на ISA-сервере приложений.

Для Антивируса Касперского также предусмторен ряд важных событий, возникновение которых требует немедленной реакции администратора системы. Например, событие *До истечения лицензии осталось 14 дней* (см. рис. 36). Набор таких событий пополняет существующий список сразу после установки приложения на сервер. Способ уведомления для каждого из событий вы можете настроить самостоятельно.

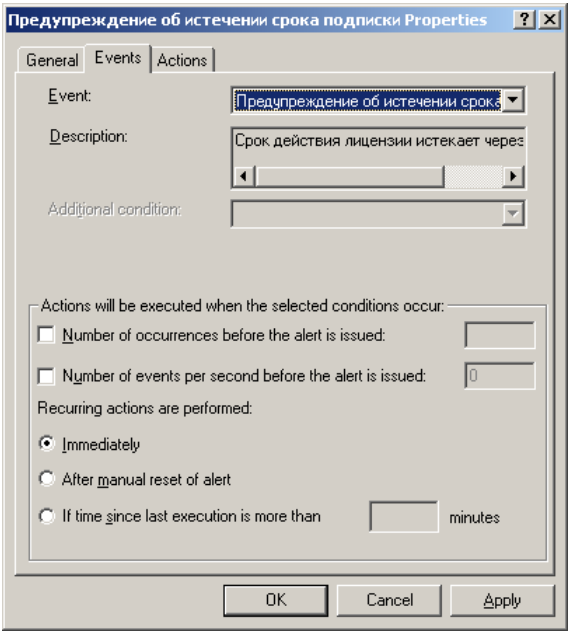


Рисунок 36. Настройка уведомления администратора при возникновении важного события в работе приложения

4.6.3. Настройка диагностики работы программы

Антивирус Касперского позволяет проводить полную диагностику своей работы и фиксировать ее результаты в следующих файлах журналов:

kavisaДАТА.log – журнал Антивируса Касперского, содержащий информацию о работе приложения в заданном вами объеме на определенную дату. В качестве *ДАТА* в названии файла приводится дата его создания в формате *ГодМесяцЧисло*. Например: *kavisa20040410.log*.

В случае если в момент дополнения журнала он будет, например, открыт администратором на редактирование, Антивирус Касперского сформирует новый файл с дополнительным постфиксом к его имени. Например: *kavisa20040410_1.log*.

viruslogДАТА.log – журнал Антивируса Касперского, включающий информацию об обнаруженнных вредоносных объектах.

Вы можете настроить полноту информации, выводимой в перечисленные выше журналы, на закладке **Диагностика** (см. рис. 37).

Время возникновения событий, фиксируемых в перечисленных выше журналах, приводится в формате *Universal Coordinated Time* (UTC).

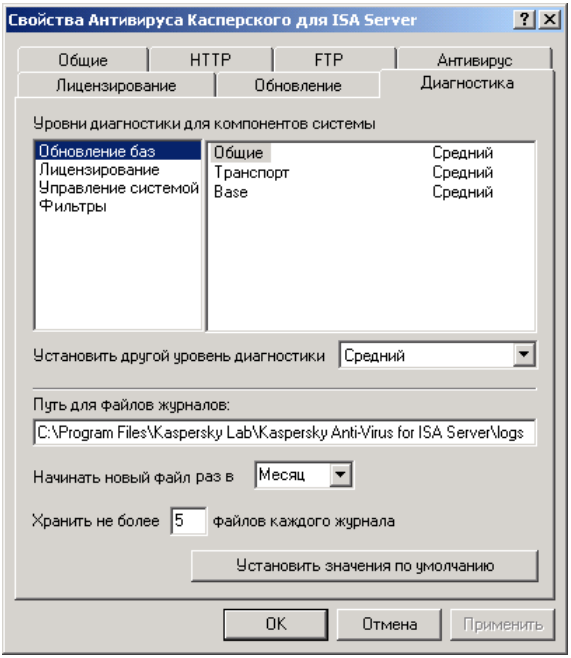


Рисунок 37. Параметры диагностики работы Антивируса Касперского

Все важные сообщения о работе Антивируса Касперского также выводятся в Системный журнал приложений операционной системы Windows.

В левой части окна приведены все возможные задачи (Обновление баз, Лицензирование и т.д), в правой части – классификация сообщений, которые формируются Антивирусом Касперского по выбранной задаче, и уровень их детализации.

Для любой из классификаций сообщений вы можете выбрать уровень детализации:

- **Не выводить** – не записывать в журналы никакой информации.
- **Минимальный** – фиксировать в журналах только основные события (например, запуск и остановка приложения и т.д.).

- **Средний** – записывать помимо основных событий ряд дополнительных, характеризующих работу Антивируса более детально (например, сообщение об ошибке соединения с сервером обновлений).
- **Максимальный** – выводить в журналы максимально полную информацию о работе приложения, за исключением отладочных сообщений.
- **Отладочный** – записывать в журналы всю информацию, в том числе и отладочную.

Здесь же вы можете настроить частоту формирования журналов и их количество.

4.7. Управление лицензионными ключами

Управление лицензионными ключами осуществляется на закладке **Лицензирование** диалогового окна **Свойства Антивируса Касперского для ISA Server** (см. рис. 38).

Лицензионный ключ необходим для полнофункциональной работы Антивируса Касперского.

Если вы еще не решились на приобретение Антивируса Касперского, мы можем предоставить вам пробный лицензионный ключ (trial-key), который будет работать в течение двух недель или месяца. По истечении данного срока ключ будет заблокирован. Вы не сможете осуществлять антивирусную проверку потоков данных.

Дважды использовать пробный ключ невозможно!

Если лицензионный ключ к Антивирусу Касперского для ISA-серверов отсутствует или не соответствует данному приложению, Антивирус не работает.

По истечении срока действия лицензии Антивирус Касперского сохраняет свою функциональность за исключением возможности обновления антивирусных баз. Потоки данных по-прежнему подвергаются антивирусной фильтрации, но только на основе антивирусных баз, актуальных на дату окончания лицензии. Следовательно, мы не можем гарантировать защиты данных от новых вирусов, появившихся после окончания лицензии.

Даже если базы будут вручную скопированы с сайтов Лаборатории Касперского и выложены в соответствующий каталог на сервере, Антивирус Касперского не будет использовать такие базы.

Если лицензионный ключ не включен в поставку продукта, обратитесь к дистрибьютору, у которого вы приобрели Антивирус Касперского.

4.7.1. Продление лицензии

Если срок действия лицензии истек, для восстановления полной функциональности приложения вам нужно продлить лицензию, то есть приобрести новый лицензионный ключ. Пока вы не продлите лицензию, Антивирус Касперского не сможет обновлять антивирусные базы, следовательно, мы не можем гарантировать вам стопроцентную антивирусную защиту.

Чтобы продлить лицензию на использование Антивируса Касперского, вам необходимо:

связаться с компанией, у которой вы купили продукт, и приобрести продление лицензии на использование Антивируса Касперского.

или:

продлить 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**. По факту оплаты вам будет отправлен лицензионный ключ по электронной почте, адрес которой был указан вами в форме заказа.

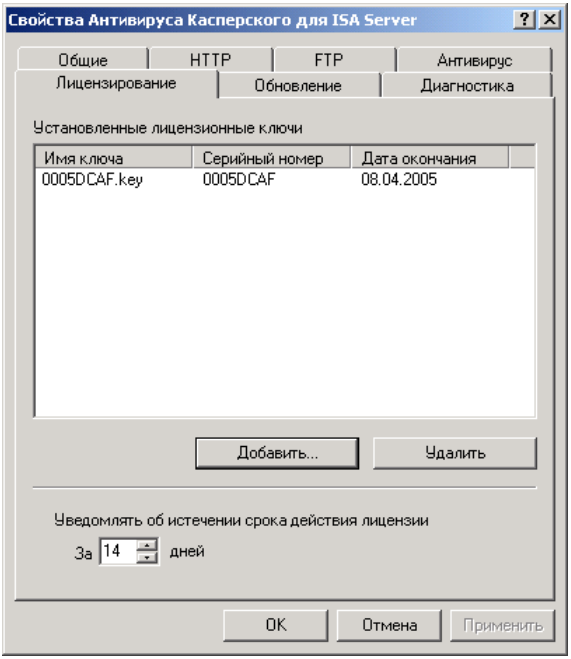


Рисунок 38. Управление лицензионными ключами

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

Чтобы установить новый лицензионный ключ,

нажмите на кнопку **Добавить** и в открывшемся окне укажите файл действующего ключа (*.key).

Чтобы настроить время уведомления об истечении срока действия лицензии,

укажите в соответствующем поле необходимое число дней. Когда до истечения срока действия лицензионного ключа останется указанное количество дней, ежедневно в течение указанного периода в системном журнале компьютера, на котором установлен Антивирус Касперского для ISA-серверов, будет фиксироваться соответст-

вующее сообщение. В нем будет указано оставшееся количества дней.

Дату окончания срока действия лицензии вы также можете посмотреть на закладке **Общие** главного окна Антивируса Касперского для ISA-серверов.

Существует возможность установки резервного ключа, который вступит в силу сразу по окончании действующего. Таким образом вам удастся избежать пробелов в антивирусной защите сервера.

Для установки резервного ключа нажмите на кнопку **Добавить** и в открывшемся окне укажите файл резервного ключа (*.key).

Если вы заранее позаботились об установке резервного ключа, то по окончании срока действия лицензии он автоматически становится действующим, а просроченный ключ удаляется. Таким образом, автоматически выполняется продление лицензии.

Невозможно установить более двух лицензионных ключей.

Итак, в списке лицензионных ключей действующий ключ всегда будет первым, а резервный – вторым.

4.7.2. Удаление лицензионного ключа

При установке нового лицензионного ключа вы можете самостоятельно удалить просроченный ключ, воспользовавшись соответствующей кнопкой на закладке **Лицензирование** (см. рис. 38).

Если же установлены два ключа – действующий и резервный – и вы хотите удалить действующий ключ еще до окончания его действия, то вместе с действующим будет удален и резервный.

ГЛАВА 5. ВОЗМОЖНЫЕ ВОПРОСЫ ПРИ РАБОТЕ С ПРИЛОЖЕНИЕМ

В данной главе мы осветим наиболее часто задаваемые пользователями вопросы по установке, настройке и работе Антивируса Касперского и постараемся ответить на них наиболее подробно.

Вопрос: почему Антивирус Касперского вызывает определенное снижение производительности сервера и ощутимо нагружает процессор?

Детектирование вирусов является в чистом виде вычислительной (математической) задачей, связанной с анализом структур, подсчетом контрольных сумм и математическими преобразованиями данных. Поэтому основным ресурсом, который потребляется антивирусом в процессе работы, является процессорное время. При этом каждый новый вирус, добавленный в антивирусную базу, увеличивает общее время проверки. Это вынужденная плата за надежность и безопасность ваших данных.

В отличие от других антивирусов, урезающих время проверки путем исключения из антивирусных баз более сложных в детектировании или более редких (в том месте, где географически расположена компания-производитель) вирусов, а также более сложных в анализе форматов файлов (например, pdf), Лаборатория Касперского считает, что задача антивируса – обеспечивать реальную, а не мнимую, антивирусную безопасность пользователей, поскольку нельзя быть защищенным наполовину. При этом быть "частично защищенным" хуже, чем не быть защищенным вообще (поскольку в этом случае пользователь принимает меры предосторожности самостоятельно).

Антивирус Касперского позволяет пользователю чувствовать себя максимально защищенным. Безусловно, Антивирус Касперского позволяет опытному пользователю ускорить антивирусную проверку в ущерб общей безопасности путем отключения антивирусной проверки различных типов файлов, но мы не рекомендуем этого делать, если пользователь хочет чувствовать себя максимально защищенным.

Вопрос: зачем нужен лицензионный ключ? Может ли мой Антивирус работать без него?

Без лицензионного ключа Антивирус Касперского не работает.

Если вы еще не решились на приобретение Антивируса Касперского, мы можем предоставить вам пробный ключ (trial-key), который будет работать в течение двух недель или месяца. По истечении данного срока ключ будет заблокирован.

Вопрос: что произойдет, когда истечет лицензия на использование продукта?

По истечении срока действия лицензии на использование Антивируса Касперского продукт будет продолжать работу, но использование новых антивирусных баз станет невозможным. Антивирус попрежнему будет выполнять лечение инфицированных объектов, но с использованием старых антивирусных баз.

Загрузка антивирусных баз с сайта Лаборатории Касперского посредством с помощью Антивируса Касперского будет невозможно. Даже если вы скопируете антивирусные базы без его использования, Антивирус Касперского не будет их использовать.

Следовательно, мы не можем гарантировать вам защиту от заражения новыми вирусами.

Вопрос: почему после установки приложение не выполняет проверку трафика?

Такая ситуация возникает в том случае, если сразу после установки приложения не были перезагружены службы MS ISA Server. Для решения данной проблемы достаточно их перезагрузить из консоли MS ISA Server.

Вопрос: после обновления антивирусных баз Антивирус Касперского не проверяет трафик. Почему?

Если время запуска обновления антивирусных баз (автоматического или ручного) приходится на время высокой нагрузки сервера (более 300 одновременных активных соединений), то возможно возникновение такой ситуации, когда приложение прекращает проверку трафика.

В данном случае вам следует перезапустить сервис **Антивирус Касперского для MS ISA Server** из консоли управления операционной системы Windows или из командной строки командами:

```
net stop kavisasrv
net start kavisasrv
```

Для того чтобы избежать проявления этой особенности функционирования, следует установить время автоматического обновления антивирусных баз (или проводить ручное обновление), когда сервер не загружен большим количеством запросов пользователей, например, в ночное время.

Вопрос: мой Антивирус не работает.

Что мне делать?

Мы рекомендуем обратиться к фирме, продавшей вам Антивирус Касперского или написать письмо в Службу технической поддержки (support@kaspersky.com).

Чтобы ваш запрос был обработан как можно скорее:

1. В заголовке сообщения укажите операционную систему вашего сервера, имя компонента, который вы не можете настроить, и проблему.
2. Пишите сообщения в виде plain text. Сообщения HTML-формата труднее читать.
3. В начале сообщения укажите точную версию операционной системы, дистрибутива Антивируса Касперского и номер вашей лицензии.
4. Кратко, но наиболее понятно опишите проблему. Помните, что Служба поддержки на момент чтения вашего письма ещё ничего не знает о вашей проблеме и сможет помочь вам, только полностью поняв и воспроизведя её.
5. Отправьте в Службу технической поддержки следующие данные, предварительно запаковав их в один архив:
   - файл отчета Антивируса Касперского (например, *updater.log*, *isavweb.log*);
   - лицензионный ключ.
6. Укажите примерный размер дневного трафика и бывают ли пики нагрузки.

Вопрос: может ли злоумышленник подменить антивирусные базы?

Злоумышленник может загрузить антивирусные базы с сайта Лаборатории Касперского и скопировать их в каталог хранения антивирусных баз, однако Антивирус Касперского не будет их использовать в процессе работы!

Все антивирусные базы имеют уникальную подпись, и при обращении к базам Антивирус Касперского проверяет ее. Если подпись не соответствует присвоенной в Лаборатории Касперского, и дата баз – более поздняя, чем день окончания лицензии на использование продукта, Антивирус Касперского не будет использовать такие базы.

ПРИЛОЖЕНИЕ А. ГЛОССАРИЙ

В документации встречаются термины и понятия, специфичные для области антивирусной защиты. Глоссарий представляет собой словарь определений данных понятий. Для удобства пользования статьи глоссария представлены в алфавитном порядке.

А

Антивирусные базы – базы данных, формируемые специалистами Лаборатории Касперского и содержащие подробное описание всех существующих на текущий момент вирусов, способов их обнаружения и лечения. Базы постоянно обновляются в Лаборатории Касперского по мере появления новых вирусов. Это требует от администратора проведения регулярного обновления антивирусных баз.

З

Зараженный (инфицированный) объект – объект, внутри которого содержится вредоносный код. Мы не рекомендуем вам работать с такими объектами, поскольку это может привести к заражению вашего компьютера.

И

Исходный поток данных – поток данных, передаваемый по протоколам HTTP и FTP.

К

Клиент – пользователь корпоративной сети, использующий MS ISA-сервер для доступа в интернет.

Консоль администратора – специальное приложение, обеспечивающее пользовательский интерфейс для выполнения задач администрирования Антивируса Касперского для MS ISA-серверов.

Контролируемый объект – любой файл, перемещаемый по протоколам HTTP и FTP через брандмауэр.

О

Обновление антивирусных баз – процедура замены/добавления новых антивирусных баз, получаемых с серверов обновлений Лаборатории Касперского.

ПРИЛОЖЕНИЕ В. ЗАО "ЛАБОРАТОРИЯ КАСПЕРСКОГО"

ЗАО "Лаборатория Касперского" была основана в 1997 г. Сегодня это самый известный в России разработчик широкого спектра программных продуктов для обеспечения информационной безопасности: систем защиты от вирусов, нежелательной почты (спама) и хакерских атак.

"Лаборатория Касперского" – международная компания. Центральный офис находится в России, открыты локальные офисы в Великобритании, Франции, Германии, Японии, Бенилюксе, Китае, Польше, Румынии и США (Калифорния). Во Франции открыто новое отделение компании – Европейский центр антивирусных исследований. Наша партнерская сеть объединяет более 500 компаний по всему миру.

"Лаборатория Касперского" сегодня – это более двухсотпятидесяти высококвалифицированных специалистов, девять из которых имеют дипломы MBA, пятнадцать – степени кандидатов наук и двое являются членами престижной организации Computer Anti-virus Researcher's Organization (CARO).

Главная ценность компании – уникальные знания и опыт, накопленные ее сотрудниками течение более чем четырнадцати лет непрерывной борьбы с вирусами. Благодаря постоянному анализу вирусной активности мы умеем предугадывать тенденции развития вредоносных программ и заблаговременно обеспечиваем пользователей надежной защитой от новых видов атак. Это преимущество – основа продуктов и услуг "Лаборатории Касперского". Мы всегда на шаг впереди конкурентов и предоставляем нашим заказчикам наилучшую защиту.

Годы упорной работы позволили компании стать лидером в разработке технологий защиты от вирусов. "Лаборатория Касперского" первой разработала многие современные стандарты антивирусных программ. Основной продукт компании, Антивирус Касперского, обеспечивает надежную защиту всех объектов вирусных атак: рабочих станций, файловых серверов, почтовых шлюзов, межсетевых экранов и карманных компьютеров. Удобные средства управления дают пользователям возможность максимально автоматизировать антивирусную защиту компьютеров и корпоративных сетей. Многие западные разработчики используют в своих продуктах программное ядро Антивируса Касперского™, например, такие как: Nokia ICG (США), F-Secure (Финляндия), Aladdin (Израиль), Sybari (США), G Data (Германия), Deerfield (США), Alt-N (США), Microworld (Индия), BorderWare (Канада).

Клиенты "Лаборатории Касперского" обеспечиваются широким спектром дополнительных услуг, гарантирующих бесперебойную работу продуктов и точное соответствие любым специфическим бизнес-требованиям. Мы проектируем, внедряем и сопровождаем корпоративные антивирусные комплексы. Наша антивирусная база обновляется каждые три часа. Мы обеспечиваем наших пользователей круглосуточной технической поддержкой на нескольких языках.

B.1. Другие разработки Лаборатории Касперского

Антивирус Касперского® Personal

Антивирус Касперского® Personal предназначен для антивирусной защиты персональных компьютеров, работающих под управлением операционных систем Windows 98/ME, 2000/NT/XP, от всех известных видов вирусов, включая потенциально опасное ПО. Программа осуществляет постоянный контроль всех источников проникновения вирусов – электронной почты, интернета, дискет, компакт-дисков и т.д. Уникальная система эвристического анализа данных эффективно нейтрализует неизвестные вирусы. Можно выделить следующие варианты работы программы (они могут использоваться как отдельно, так и в совокупности):

- **Постоянная защита компьютера** – проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов.
- **Проверка компьютера по требованию** – проверка и лечение как всего компьютера в целом, так и отдельных дисков, файлов или каталогов. Такую проверку вы можете запускать самостоятельно или настроить ее регулярный автоматический запуск.

Антивирус Касперского Personal теперь не проверяет повторно те объекты, которые были проанализированы во время предыдущей проверки и с тех пор не изменились, не только при постоянной защите, но и при проверке по требованию. Такая организация работы **заметно повышает скорость работы программы**.

Программа создает надежный барьер на пути проникновения вирусов через электронную почту. Антивирус Касперского Personal автоматически осуществляет проверку и лечение всей входящей и исходящей почтовые корреспонденции по протоколам POP3 и SMTP и эффективно обнаруживает вирусы в почтовых базах.

Программа поддерживает более семисот форматов архивированных и сжатых файлов и обеспечивает автоматическую антивирусную проверку их

содержимого, а также удаление вредоносного кода из архивных файлов формата **ZIP, CAB, RAR, AFJ**.

Простота настройки программы осуществляется за счет возможности выбора одного из трех предопределенных уровней: **Максимальная защита**, **Рекомендуемая защита** и **Максимальная скорость**.

Обновления антивирусных баз осуществляется каждые три часа, при этом обеспечивается их гарантированная доставка при разрыве или смене соединений с интернетом.

Антивирус Касперского® Personal Pro

Пакет разработан специально для полномасштабной антивирусной защиты домашних компьютеров, работающих под управлением операционных систем Windows 98/ME, Windows 2000/NT, Windows XP с бизнес-приложениями из состава MS Office 2000. Антивирус Касперского® Personal Pro включает программу загрузки ежедневных обновлений антивирусной базы и программных модулей. Уникальная система эвристического анализа данных второго поколения эффективно нейтрализует неизвестные вирусы. Простой и удобный пользовательский интерфейс позволяет быстро менять настройки и делает работу с программой максимально комфортной.

Антивирус Касперского® Personal Pro обеспечивает:

- **антивирусную проверку по требованию пользователя** локальных дисков;
- **автоматическую проверку в масштабе реального времени** на присутствие вирусов всех используемых файлов;
- **почтовый фильтр**, осуществляющий проверку входящих и исходящих почтовых сообщений в фоновом режиме;
- **поведенческий блокиратор**, гарантирующий стопроцентную защиту от макро-вирусов.

Kaspersky® Anti-Hacker

Программа Kaspersky® Anti-Hacker представляет собой персональный межсетевой экран, обеспечивающий полномасштабную защиту компьютера, работающего под управлением операционной системы Windows, от несанкционированного доступа к данным, а также от сетевых хакерских атак из локальной сети и интернета.

Kaspersky® Anti-Hacker отслеживает сетевую активность по протоколу TCP/IP для всех приложений на вашем компьютере. При обнаружении подозрительных действий какого-либо приложения программа информирует вас об этом, и, при необходимости, блокирует сетевой доступ этому приложению. В результате обеспечивается конфиденциальность информации, находящейся на вашем компьютере.

Благодаря технологии SmartStealth™ значительно затрудняется обнаружение компьютера извне: режим невидимости вашего компьютера обеспечивает защиту от хакерских атак, не оказывая никакого негативного влияния на вашу работу в интернете. Программа обеспечивает стандартную прозрачность и доступность информации.

Kaspersky® Anti-Hacker также блокирует наиболее распространенные сетевые хакерские атаки, отслеживает попытки сканирования портов.

Программа поддерживает упрощенное администрирование по пяти режимам безопасности. По умолчанию используется режим самообучения, который позволяет настроить систему безопасности в зависимости от вашей реакции на различные события. Данный режим позволяет сконфигурировать межсетевой экран под конкретного пользователя и конкретный компьютер.

Kaspersky® Security для PDA

Kaspersky® Security для PDA обеспечивает надежную антивирусную защиту данных, хранимых на КПК, работающих под управлением Palm OS или Windows CE, а также информации, переносимой с PC или любой карты расширения, ROM файлы и базы данных, В состав программы входит оптимальный набор средств антивирусной защиты:

- **антивирусный сканер**, обеспечивающий проверку информации (хранимой как на PDA, так и на картах расширения любого типа) по требованию пользователя;
- **антивирусный монитор**, осуществляющий перехват вирусных программ, передаваемых в процессе синхронизации с использованием технологии HotSync™ или с другими КПК.

Программа также обеспечивает защиту данных, хранящихся на карманном компьютере, от несанкционированного доступа путем шифрования доступа к самому устройству и ко всей информации, хранящейся на портативном компьютере и картах расширения.

Антивирус Касперского® Business Optimal

Программный комплекс представляет собой уникальное конфигурируемое решение антивирусной защиты для предприятий малого и среднего бизнеса.

Антивирус Касперского® Business Optimal обеспечивает полномасштабную антивирусную защиту[3]:

[3] В зависимости от типа поставки

- *рабочих станций* под управлением Windows 98/Me, Windows 2000/NT/XP Workstation, Linux.
- *файловых серверов* под управлением Windows NT 4.0 Server, Windows 2000 Server/Advanced Server, Windows 2003 Server, Novell Netware, FreeBSD и OpenBSD, Linux.
- *почтовых систем* Microsoft Exchange 5.5/2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail и Qmail.
- *интернет-шлюзов*: CheckPoint Firewall –1; MS ISA Server.

Антивирус Касперского® Business Optimal также включает систему централизованной установки и управления – Kaspersky® Administration Kit.

Вы можете самостоятельно выбрать антивирусные программы в соответствии с используемыми операционными системами и приложениями.

Kaspersky® Corporate Suite

Kaspersky® Corporate Suite – это интегрированная система, обеспечивающая информационную безопасность вашей корпоративной сети независимо от ее сложности и размера. Программные компоненты, входящие в состав комплекса, предназначены для защиты всех узлов сети компании. Они совместимы с большинством используемых сегодня операционных систем и программных приложений, объединены системой централизованного управления и обладают единым пользовательским интерфейсом. Программный комплекс обеспечивает создание системы защиты, полностью совместимой с системными требованиями вашей сети.

Kaspersky® Corporate Suite обеспечивает полномасштабную антивирусную защиту:

- *рабочих станций* под управлением Windows 98/Me, Windows 2000/NT/XP Workstations и Linux.
- *файловых серверов* под управлением Windows NT 4.0 Server, Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD, OpenBSD и Linux.
- *почтовых систем* Microsoft Exchange Server 5.5/2000/2003, Lotus Notes/Domino, Sendmail, Postfix, Exim и Qmail.
- *интернет-шлюзов*: CheckPoint Firewall –1; MS ISA Server.
- *карманных компьютеров*, работающих под управлением Windows CE и Palm OS.

Kaspersky® Corporate Suite также включает *систему централизованной установки и управления* – Kaspersky® Administration Kit.

Вы можете самостоятельно выбрать антивирусные программы в соответствии с используемыми операционными системами и приложениями.

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam – первый российский программный комплекс для защиты от нежелательных писем (спама) для предприятий средних и малых масштабов. Продукт сочетает революционные технологии лингвистического анализа текстов, все современные методы фильтрации электронной почты (включая RBL-списки и формальные признаки письма) и уникальный набор сервисов, которые позволяют пользователям распознать и уничтожить до девяноста пяти процентов нежелательного трафика.

Kaspersky® Anti-Spam представляет собой фильтр, который устанавливается на "входе" в сеть предприятия и проверяет входящий поток писем на предмет обнаружения спама. Продукт совместим с любой почтовой системой, используемой в сети заказчика, и может быть установлен как на уже существующий почтовый сервер, так и на выделенный.

Высокая эффективность работы программы достигается благодаря ежедневному автоматическому обновлению базы контентной фильтрации образцами, предоставляемыми специалистами лингвистической лаборатории.

Kaspersky® Anti-Spam Personal

Kaspersky® Anti-Spam Personal предназначен для защиты пользователей почтовых клиентов Microsoft Outlook и Microsoft Outlook Express от нежелательных писем (спама).

Программный пакет Kaspersky Anti-Spam Personal представляет собой мощный инструмент для обнаружения спама в потоке входящей электронной почты, поступающей по протоколам POP3 и IMAP4 (только для Microsoft Outlook).

Во время фильтрации проверяются все возможные атрибуты письма: адреса отправителя и получателя, его заголовки. Также используется *контентная фильтрация*, то есть анализируется содержание самого письма (включая заголовок *Subject*) и файлов вложений. Применяются уникальные лингвистические и эвристические алгоритмы.

Высокая эффективность работы программы достигается благодаря ежедневному автоматическому обновлению базы контентной фильтрации образцами, предоставляемыми специалистами лингвистической лаборатории.

В.2. Наши координаты

Если у вас возникнут какие-либо вопросы, вы можете обратиться к нашим дистрибьюторам или непосредственно в ЗАО "Лаборатория Касперского". Вам всегда будут предоставлены подробные консультации по телефону или электронной почте. На все ваши вопросы вы получите полные и исчерпывающие ответы.

Адрес:	Россия, 125363, Москва, ул. Героев Панфиловцев, 10	
Факс:	+7 (095) 797-8700	
Экстренная круглосуточная помощь	+7 (095) 797-8707 support@kaspersky.com	
Поддержка пользователей Business Optimal	+7 (095) 363-4205 (с 10 до 19 часов)	smb-support@kaspersky.com
Поддержка пользователей Corporate Suite	Телефоны и электронный адрес предоставляются при покупке Corporate Suite.	
Антивирусная лаборатория	newvirus@kaspersky.com (только для отправки новых вирусов в архивированном виде)	
Департамент продаж	+7 (095) 797-8700	sales@kaspersky.com
Департамент маркетинговых коммуникаций	+7 (095) 797-8700	info@kaspersky.com
WWW:	http://www.kaspersky.ru http://www.viruslist.com	