

ЛАБОРАТОРИЯ КАСПЕРСКОГО

Антивирус Касперского 5.6 для
Microsoft ISA Server 2004/2006
Standard Edition

РУКОВОДСТВО
АДМИНИСТРАТОРА

АНТИВИРУС КАСПЕРСКОГО 5.6 ДЛЯ MICROSOFT ISA
SERVER 2004/2006 STANDARD EDITION

Руководство администратора

© ЗАО «Лаборатория Касперского»
Тел., факс: +7 (495) 797-8700, +7 (495) 645-7939, +7 (495) 956-7000
<http://www.kaspersky.ru>

Дата редакции: декабрь 2008 г.

Содержание

ГЛАВА 1. АНТИВИРУС КАСПЕРСКОГО® ДЛЯ MICROSOFT ISA SERVER.....	5
1.1. Аппаратные и программные требования к системе	6
1.2. Комплект поставки.....	7
1.2.1. Лицензионное соглашение	8
1.2.2. Регистрационная карточка	8
1.3. Сервис для зарегистрированных пользователей.....	9
ГЛАВА 2. ТИПИЧНАЯ СХЕМА РАЗВЕРТЫВАНИЯ ПРИЛОЖЕНИЯ	10
ГЛАВА 3. УСТАНОВКА ПРИЛОЖЕНИЯ	12
3.1. Настройка параметров ISA-сервера перед установкой приложения	12
3.2. Установка Антивируса Касперского.....	14
3.2.1. Первая установка.....	14
3.2.2. Повторная установка	19
3.3. Обновление версии.....	19
ГЛАВА 4. РАБОТА С АНТИВИРУСОМ КАСПЕРСКОГО.....	21
4.1. Параметры процесса проверки данных по умолчанию.....	21
4.2. Управление процессом проверки	24
4.2.1. Настройка общих параметров антивирусной проверки.....	25
4.2.1.1. Общие параметры работы приложения.....	25
4.2.1.2. Параметры проверки HTTP-потока данных	32
4.2.1.3. Параметры проверки FTP-потока данных.....	35
4.2.2. Управление группами клиентов	36
4.2.3. Ведение политик антивирусной проверки	41
4.2.3.1. Ведение списка доверенных серверов	46
4.2.3.2. Формирование списка непроверяемых объектов.....	48
4.3. Обновление антивирусных баз.....	48
4.3.1. Автоматическое обновление антивирусных баз по расписанию	51
4.3.2. Ручной запуск получения обновлений.....	51
4.4. Настройка параметров уведомлений пользователей	51
4.5. Проверка корректности работы Антивируса Касперского.....	53

4.6. Статистика и диагностика работы приложения	54
4.6.1. Сбор и просмотр статистической информации.....	54
4.6.2. Уведомление администратора посредством ISA Server Alerts	56
4.6.3. Настройка параметров диагностики работы приложения	57
4.7. Ограничения при работе с Антивирусом Касперского	59
4.8. Управление лицензионными ключами.....	60
4.8.1. Установка лицензионного ключа.....	61
4.8.2. Продление лицензии	63
4.8.3. Удаление лицензионного ключа	64
ГЛАВА 5. ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ.....	65
ПРИЛОЖЕНИЕ А. ГЛОССАРИЙ.....	70
ПРИЛОЖЕНИЕ В. ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО».....	71

ГЛАВА 1. АНТИВИРУС КАСПЕРСКОГО® ДЛЯ MICROSOFT ISA SERVER

Антивирус Касперского® для Microsoft ISA Server (далее также **Антивирус Касперского**) – 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 Microsoft 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 Microsoft ISA-сервер как плагины, а антивирусное ядро устанавливается в систему как служба.

Управление настройками антивирусной проверки осуществляется через специализированный интерфейс, представляющий собой оснастку Microsoft Management Console (далее MMC).

Примечание

Интерфейс администрирования Антивируса Касперского для Microsoft ISA Server может устанавливаться на отдельную станцию управления.

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;
- блокировка загрузки потока данных при невозможности лечения;
- 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 Microsoft Windows;
- управление лицензионными ключами.

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

- настраивать параметры антивирусной проверки и уведомлений пользователя об опасных событиях;
- создавать группы клиентов, объединяемые по сетевым принципам. Например, можно 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 доверенных серверов, трафик с которых не будет анализироваться на вирусы;
- формировать список объектов по типу, которые не будут подвергаться антивирусной проверке.

Антивирус Касперского поддерживает следующие протоколы передачи данных:

- HTTP 1.0 и 1.1 (RFC 2616);
- FTP (RFC 775, 959, 2389, Extensions to FTP);
- FTP over HTTP.

Примечание

Данные, передаваемые по другим протоколам и VPN-соединениям, Антивирусом Касперского не проверяются.

1.1. Аппаратные и программные требования к системе

Антивирус Касперского функционирует совместно с продуктом Microsoft Internet Security and Acceleration Server 2004/2006 Standard Edition на операционных системах Microsoft Windows 2000 с установленным Service Pack 4 и Microsoft Windows Server 2003.

Если на вашем сервере установлен Microsoft Internet Security and Acceleration Server 2006 Standard Edition, для работы Антивируса Касперского требуется платформа Microsoft Windows Server 2003 с установленным Service Pack 1.

Минимальные аппаратные требования для использования Антивируса Касперского:

- процессор Pentium III с тактовой частотой 550 МГц;
- 512 МБ оперативной памяти;
- 50 МБ свободного дискового пространства для установки приложения;
- 200 МБ свободного дискового пространства для очереди объектов, копируемых из интернета перед антивирусной проверкой.

Примечание

Необходимый объем свободного дискового пространства для временного хранения копируемых из интернета данных перед антивирусной проверкой определяется количеством трафика, проходящего через Microsoft ISA Server. Как правило, достаточно 500 МБ, однако при интенсивной загрузке из интернета файлов большого размера может потребоваться большее количество свободного дискового пространства.

1.2. Комплект поставки

Антивирус Касперского 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-диск, на котором записаны файлы программного продукта и документация в формате pdf.
- Руководство пользователя в печатном виде (если данная позиция была включена в заказ) или Руководство по продуктам.
- Лицензионный ключ, записанный на специальную дискету.
- Регистрационная карточка (с указанием серийного номера продукта).
- Лицензионное соглашение.

Примечание

Перед тем как распечатать конверт с компакт-диск (или с дискетами), внимательно ознакомьтесь с Лицензионным соглашением.

При покупке Антивируса Касперского в интернет-магазине вы копируете продукт с веб-сайта Лаборатории Касперского, в дистрибутив которого по-

мимо самого продукта включено также данное Руководство. Лицензионный ключ будет вам отправлен 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 продуктом дистрибьютору, у которого она была приобретена, и получить назад сумму, уплаченную за продукт. При этом конверт с установочным компакт-диск (или с дискетами) должен оставаться запечатанным.

Открывая запечатанный пакет с установочным компакт-диск (или с дискетами), 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 отрывной 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 действия лицензии. 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.

Приобретая лицензию, вы становитесь зарегистрированным пользователем программы и в течение срока действия лицензии можете получать следующие услуги:

- ежечасное обновление баз приложения и 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» на веб-сайте Службы технической поддержки (<http://support.kaspersky.ru/subscribe/>)).

Примечание

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

ГЛАВА 2. ТИПИЧНАЯ СХЕМА РАЗВЕРТЫВАНИЯ ПРИЛОЖЕНИЯ

Типичной схемой работы администратора ISA-сервера с большинством серверных 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 была установлена полная версия приложения Антивирус Касперского, а на компьютере администратора – только консоль администрирования. Единственным требованием к установке консоли администрирования Антивируса Касперского является наличие на компьютере средств администрирования ISA-сервера.

Примечание

Инсталляция отдельного компонента Антивируса Касперского выполняется посредством выборочной установки приложения (см. Глава 3 на стр. 12).

Установка Антивируса Касперского предусматривает встраивание в ISA-сервер следующих фильтров:

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

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

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

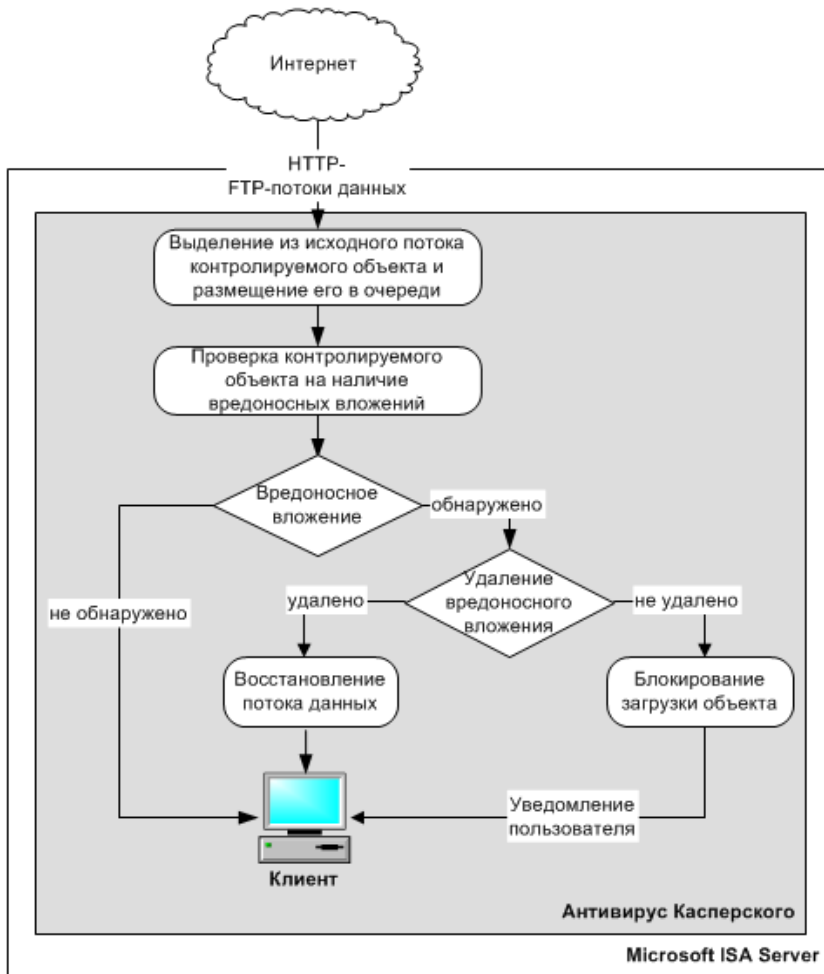


Рисунок 1. Схема обработки потока данных Антивирусом Касперского

ГЛАВА 3. УСТАНОВКА ПРИЛОЖЕНИЯ

Для корректной работы Антивируса Касперского необходимо до его установки правильно настроить стандартный фильтр ISA-сервера - *FTP Access Filter*.

Также если вы используете Microsoft Internet Security and Acceleration Server 2004 Service Pack 2 необходимо настроить поддержку декомпрессии HTTP-объектов.

3.1. Настройка параметров ISA-сервера перед установкой приложения

В Microsoft ISA Server существует стандартный фильтр, позволяющий контролировать передачу данных по протоколу FTP: *FTP Access Filter*. От состояния этого фильтра зависит функционирование Антивируса Касперского для Microsoft ISA Server.

Внимание!

Чтобы избежать отключения антивирусной защиты серверов, убедитесь, что *FTP Access Filter* активирован.

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

Чтобы настроить *FTP Access Filter*,

выберите в дереве главного окна **ISA Management** узел **Microsoft Security and Acceleration Server 2004/2006\<имя массива>\Configuration\Add-Ins**, а затем перейдите на закладку **Application Filters**.

Если фильтр отключен, то в списке он будет отмечен значком .

Совместно со стандартными фильтрами Microsoft ISA-сервера могут использоваться дополнительные фильтры сторонних производителей, которые могут повлиять на работоспособность приложения, если их параметры

будут препятствовать поступлению потока данных на вход фильтров Анти-вируса Касперского. Более того, в отдельных случаях возможно полное отключение Антивируса Касперского.

Кроме того, для корректного функционирования Антивируса Касперского на Microsoft ISA Server 2004 необходимо в настройках Microsoft ISA-сервера включить опцию, разрешающую распаковку трафика перед подачей его на обработку в Web-фильтры (поддержка сжатого контента).

Чтобы включить данную поддержку,

выберите в дереве главного окна **ISA Management** узел **Microsoft Security and Acceleration Server 2004\<имя массива>\Configuration\General**, а затем выберите в правой части окна ссылку **Define HTTP Compression Preferences**. В открывшемся окне **HTTP Compression** перейдите на закладку **Content Inspection** и установите флажок **Decompress incoming packets to allow ISA Server Web filters to inspect the content**.

Если вы предполагаете использовать функцию удаленного администрирования, необходимо дополнительно разрешить соединение консоли удаленного администрирования приложения с компьютером, на котором установлен Microsoft ISA Server, по протоколу TCP. Для этого программа установки автоматически создаст разрешающее правило **Разрешает удаленное администрирование Антивируса Касперского для Microsoft ISA Server (Allows Kaspersky Anti-Virus for Microsoft ISA Server Remote Management)**.

Внимание!

Для Microsoft ISA Server 2004 Standard Edition название правила будет указано только на английском языке!

По умолчанию это правило не будет активировано во время установки, что позволяет администратору проанализировать его в консоли управления Microsoft ISA Server до вступления правила в силу.

Внимание!

Для удаленного управления Антивирусом Касперского необходимо, чтобы компьютер, с которого осуществляется удаленное администрирование, обладал правом администрирования Microsoft ISA Server. Эта возможность регулируется встроенной системной политикой сетевого экрана Microsoft ISA Server Remote Management\Microsoft Management Console (MMC).

3.2. Установка Антивируса Касперского

Процедура установки Антивируса Касперского на ISA-сервер выполняется стандартно, как для большинства приложений Microsoft Windows.

Примечание

Прежде чем начать установку Антивируса Касперского, рекомендуется удалить антивирусные приложения других производителей, так как их совместное функционирование может привести к конфликту в работе приложений.

Установка приложения может быть запущена локально на ISA-сервере или через терминальную сессию. Можно выбрать как полную, так и выборочную установку продукта, а также восстановить некорректную установку Антивируса Касперского.

Внимание!

Для установки Антивируса Касперского 5.6 для Microsoft ISA Server 2004/2006 Standard Edition пользователь должен обладать правами администратора сервера.

В процессе установки Антивируса Касперского возможно возникновение ряда ошибок. Каждая из них приводит к завершению процедуры установки Антивируса Касперского. Во избежание возникновения ошибок до начала установки Антивируса Касперского убедитесь, что сервер соответствует всем предъявленным аппаратным и программным требованиям (подробнее см. п. 1.1 на стр. 6).

Примечание

В случае возникновения ошибок установки обратитесь в Службу технической поддержки. К письму приложите файл журнала **kav4isa.log**, расположенный в каталоге временных файлов (каталог указан в переменной окружения **%TEMP%**).

3.2.1. Первая установка

Шаг 1. Приветствие и лицензионное соглашение

На первых этапах установки Антивируса Касперского открываются окно приветствия и окно, содержащее лицензионное соглашение. Внимательно

прочтите текст лицензионного соглашения и примите его условия для продолжения установки.

Шаг 2. Информация о пользователе и выбор типа 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 Microsoft ISA-сервер необходимо выбрать полную установку приложения.

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

Внимание!

Минимальным требованием к установке консоли администрирования Антивируса Касперского для ISA-серверов является наличие установленных на компьютере Microsoft Windows 2000 (Service Pack 4 или выше) средств администрирования ISA-сервера.

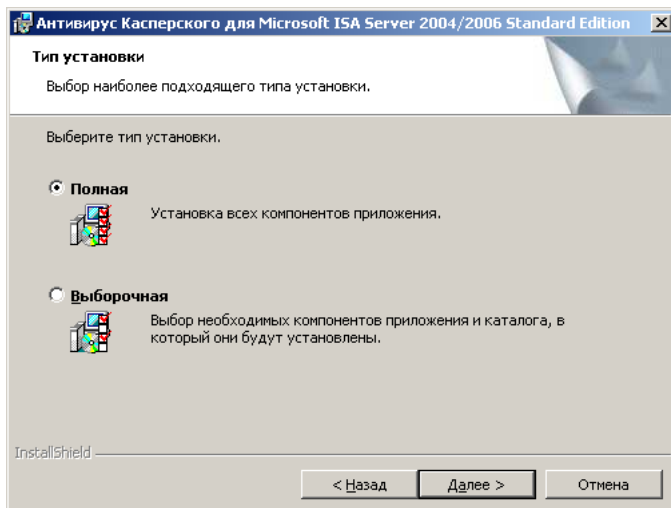


Рисунок 2. Выбор варианта установки

Шаг 3. Выбор компонентов приложения для установки

На данном этапе необходимо выбрать компоненты Антивируса Касперского, которые вы хотите установить на компьютер (см. рис. 3). Рекомендуем выполнить полную установку всех компонентов.

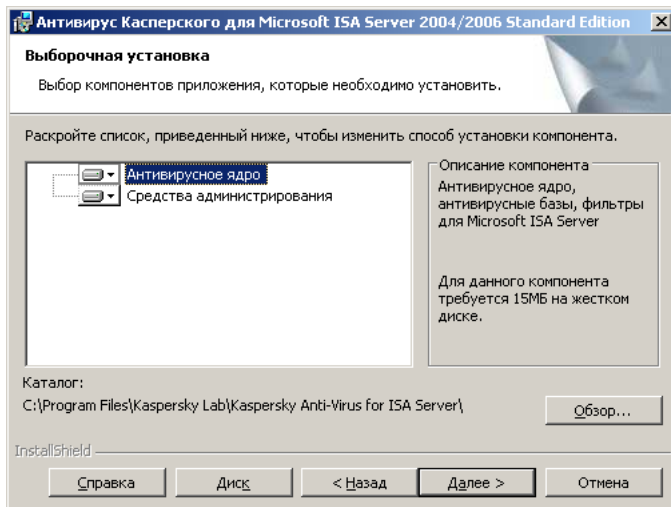


Рисунок 3. Выбор консоли администрирования для установки

Также при помощи кнопки **Обзор** можно изменить каталог установки антивирусного ядра и консоли администрирования.

Шаг 4. Параметры антивирусной проверки

На этом шаге установки приложения 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. Данный каталог должен соответствовать минимальным требованиям к объему свободного дискового пространства для временного хранения копируемых из интернета данных перед антивирусной проверкой (подробнее см. п. 1.1 на стр. 6).
- Каталог хранения антивирусных баз, используемых для поиска и лечения вирусов.
- Каталог хранения временных файлов, создаваемых во время работы приложения.

- Количество параллельно работающих экземпляров антивирусного ядра.

Примечание

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

- Количество объектов в очереди на проверку.

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

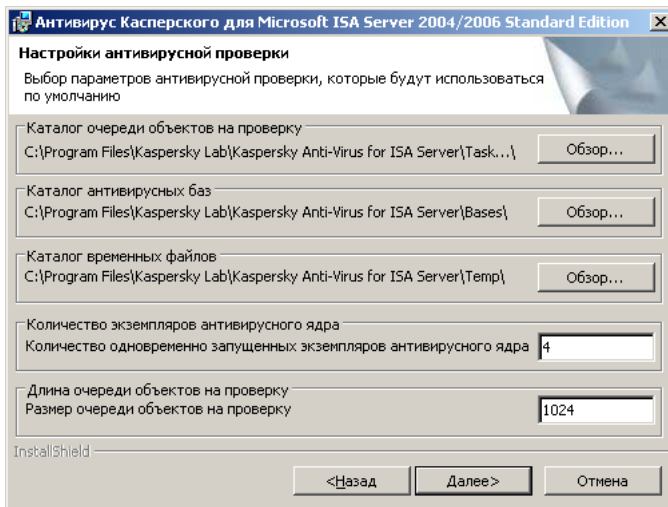


Рисунок 4. Параметры работы приложения, используемые по умолчанию

По окончании данного этапа будет запущен процесс копирования файлов приложения на компьютер и будут автоматически перезапущены службы Microsoft ISA Server¹.

¹ Службы Microsoft ISA Server не будут запущены, если они были остановлены перед установкой Антивируса Касперского.

Шаг 5. Завершение установки приложения

На этом шаге отображается информация об окончании процесса установки Антивируса Касперского.

Вы также можете запустить мастер установки лицензионных ключей приложения, установив соответствующий флажок (см. рис. 5). В этом случае по завершении работы программы установки откроется окно (см. рис. 6), в котором вы можете добавить / удалить файл лицензионного ключа.

Предусмотрена также возможность выполнения данной операции после установки приложения (подробнее см. п. 4.7 на стр. 59).

Внимание!

Без установленного лицензионного ключа Антивирус Касперского не будет осуществлять проверку трафика и обновление антивирусных баз будет недоступно.

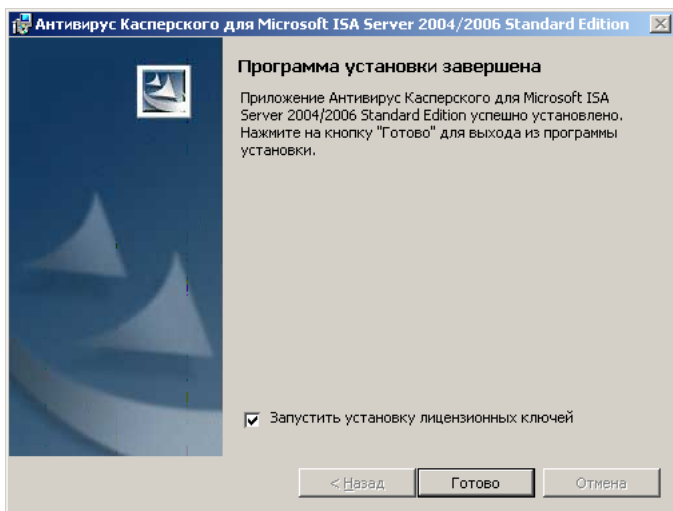


Рисунок 5. Завершение установки приложения

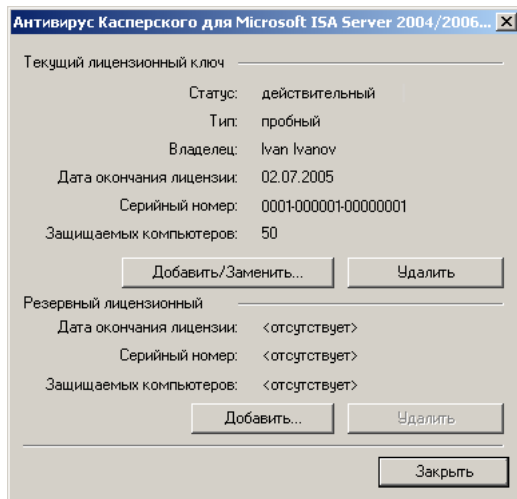


Рисунок 6. Выбор лицензионного ключа

3.2.2. Повторная установка

Повторная установка Антивируса Касперского выполняется в том случае, если первая установка приложения была выполнена некорректно, либо необходимо установить какой-либо отдельный компонент Антивируса Касперского.

*Для корректной установки приложения в открывшемся окне выберите вариант **Восстановить**.*

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

3.3. Обновление версии

Если на вашем сервере установлен Антивирус Касперского 5.5 для Microsoft ISA Server 2004, вы можете обновить его до версии Антивируса Касперского 5.6 для Microsoft ISA Server 2004/2006. Для обновления запустите программу установки (подробнее см. п. 3.2.1 на стр. 14). Программа обнаружит более раннюю версию приложения и выполнит ее обновление с сохранением настроек и типа установки (полная или выборочная установка).

При обновлении Microsoft ISA Server с версии 2004 Standard Edition до версии 2006 Standard Edition, Антивирус Касперского прекращает свою работу. Это связано с тем, что процедура обновления ISA-сервера не сохраняет регистрацию фильтров сторонних производителей. Для восстановления работоспособности приложения повторно установите (обновите) Антивирус Касперского.

Примечание

Если на вашем сервере был установлено приложение версии 5.6, то для установки в панели управления Microsoft Windows выберите пункт **Установка и удаление программ** → **Антивирус Касперского 5.6 для Microsoft ISA Server 2004/2006** и в его свойствах нажмите на кнопку **Исправить**.

Если на вашем сервере был установлено приложение версии 5.5, процедура обновления до версии 5.6 будет выполнена описанным выше образом.

ГЛАВА 4. РАБОТА С АНТИВИРУСОМ КАСПЕРСКОГО

Сразу же после установки приложения и перезапуска служб Microsoft ISA Server Антивирус Касперского готов к запуску процесса проверки потоков данных, поскольку необходимые общие параметры уже заданы. Антивирус Касперского может управляться:

- локально, если серверная часть (антивирусное ядро, антивирусные базы данных и фильтры для Microsoft ISA Server) и средства администрирования (консоль администрирования) приложения установлены на одном компьютере;
- удаленно, если серверная часть и средства администрирования установлены на разных компьютерах.

Обратите внимание, что для осуществления удаленного управления, необходимо чтобы доступ к серверу осуществлялся по следующим протоколам:

- протоколам, перечисленным в стандартной системной политике ISA-сервера **Разрешает удаленное управление с выбранных компьютеров с помощью консоли управления ММС**. Доступ по этим протоколам разрешается с помощью добавления удаленного компьютера в данную системную политику;
- по протоколу **Протокол удаленного администрирования Антивируса Касперского для Microsoft ISA Server**. Доступ по этому протоколу разрешается специальным правилом межсетевого экрана, которое создает программа установки Антивируса Касперского.

4.1. Параметры процесса проверки данных по умолчанию

Параметры процесса проверки размещены на закладках диалогового окна **Свойства Антивируса Касперского для Microsoft 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. 51):

- **Лечить HTTP-трафик** – включено.
- *Максимальное время проверки перед началом отправки данных клиенту, сек.* – 30 секунд.
- *Максимальный интервал между отправками данных клиенту, сек.* – 10 секунд.
- *Количество данных, не отправляемых клиенту до завершения проверки, %* – 10 %.
- *Разрешить дозагрузку файлов* – включено.
- *Сообщение, отправляемое клиенту, если произошла ошибка:*

```
<html>
<head>
<title>Kaspersky Anti-Virus for Microsoft ISA Serv-
er</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 Serv-
er</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. 35) содержится информация о *количестве данных, полученных сервером до того, как первый пакет с данными отправляется клиенту, КБ* – 128 килобайт.
- на закладке **Антивирус** (подробнее см. п. 4.2.1.1 на стр. 25) расположены параметры проверки:
 - **Проверять архивы.**

- **Проверять упакованные исполняемые файлы.**

Также на закладке осуществляется выбор типа используемых антивирусных баз.

- на закладке **Лицензирование** (подробнее см. п. 4.7 на стр. 59) указывается количество дней, в течение которых до окончания лицензии администратор ежедневно будет получать уведомление об истечении срока ее действия. Количество дней задается в поле *Уведомлять об истечении срока действия лицензии* и по умолчанию равняется семи дням. Уведомление выполняется посредством сообщений, выводящихся в системный журнал компьютера, на котором установлен Антивирус Касперского.
- на закладке **Обновление** (подробнее см. п. 4.3 на стр. 48) определяется ресурс для обновления антивирусных баз, настраивается процедура и частота ее выполнения. По умолчанию обновление выполняется каждые 3 часа с автоматически выбираемого сервера обновлений.

На закладке **Настройки** (подробнее см. п. 4.2.1 на стр. 25) диалогового окна свойств сервера также приводится набор рабочих каталогов Антивируса Касперского по умолчанию:

- **Каталог хранения антивирусных баз:**
.../Program Files/Kaspersky Lab/Kaspersky Anti-Virus for ISA Server/bases
- **Каталог очереди объектов на проверку:**
.../Program Files/Kaspersky Lab/Kaspersky Anti-Virus for ISA Server/TaskQueue
- **Каталог временных файлов:**
.../Program Files/Kaspersky Lab/Kaspersky Anti-Virus for ISA Server/Temp
- **Количество объектов очереди, кешируемых в памяти** – 128 объектов.
- **Размер буфера для кешируемого объекта** – 128 килобайт.
- **Количество одновременно запущенных экземпляров антивирусного ядра** – 4 экземпляра.
- **Количество экземпляров антивирусного ядра, резервируемых для проверки "быстрых" объектов** – 1 экземпляр.
- **Размер очереди объектов на проверку** – 1024 объекта.
- **Максимальное время проверки** – 1800 секунд.

4.2. Управление процессом проверки

Управление процессом проверки осуществляется через главное окно Антивируса Касперского, представленное на рис. 7.

В дереве приложения каждый узел сервера включает в себя узлы **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**. Можно изменить способ отображения на **Список**, воспользовавшись соответствующим пунктом контекстного меню, которое открывается по нажатию правой кнопки мыши в узле приложения² (см. рис. 8).

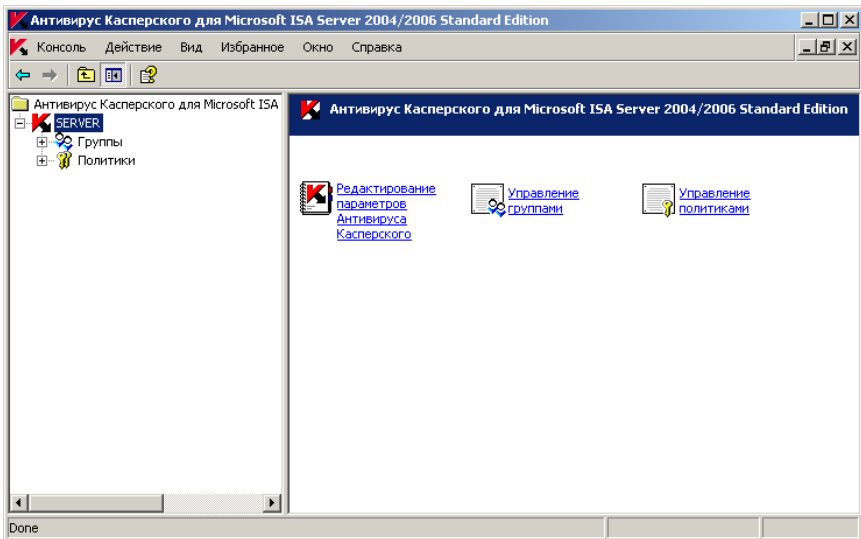


Рисунок 7. Главное диалоговое окно Антивируса Касперского для Microsoft ISA Server

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

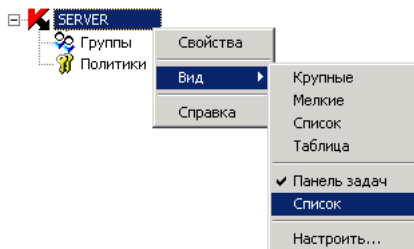


Рисунок 8. Контекстное меню

Для настройки параметров процесса управления используйте следующие возможности Антивируса Касперского:

- редактирование параметров антивирусной проверки для сервера, на котором установлено приложение Антивирус Касперского (см. п. 4.2.1 на стр. 25);
- определение новых правил антивирусной проверки, отличающихся от установленных по умолчанию, при помощи создания новой политики (см. п. 4.2.3 на стр. 41). В политике переопределяются параметры фильтрации трафика, а затем к созданной политике прикрепляется группа пользователей.

4.2.1. Настройка общих параметров антивирусной проверки

Администратор может изменять общие параметры антивирусной проверки по своему усмотрению.

Чтобы перейти к настройке общих параметров антивирусной проверки,

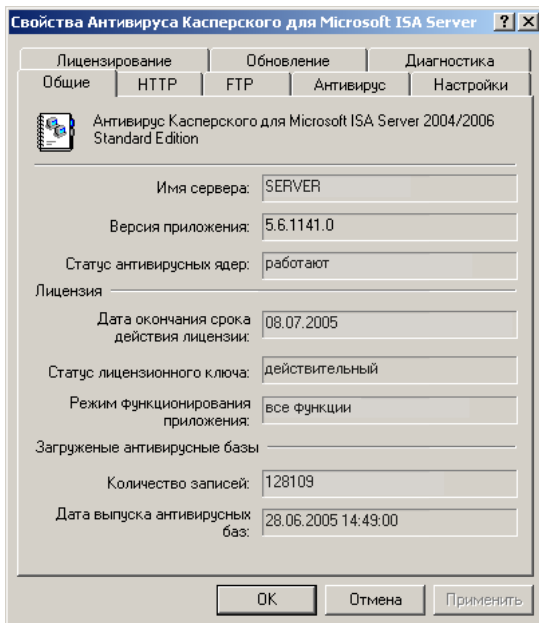
в главном окне приложения (см. рис. 7) выберите пункт **Редактирование параметров Антивируса Касперского**. Откроется диалоговое окно **Свойства Антивируса Касперского для Microsoft ISA Server**.

4.2.1.1. Общие параметры работы приложения

На закладке **Общие** (см. рис. 9) представлена информация о сервере:

- имя сервера;
- версия установленного приложения;
- статус антивирусных ядер;
- дата окончания срока действия лицензии;

- статус лицензионного ключа;
- режим функционирования приложения;
- количество записей в антивирусных базах;
- дата последнего обновления антивирусных баз.

Рисунок 9. Закладка **Общие**

На закладке **Антивирус** (см. рис. 10) сгруппированы общие параметры Антивируса Касперского.

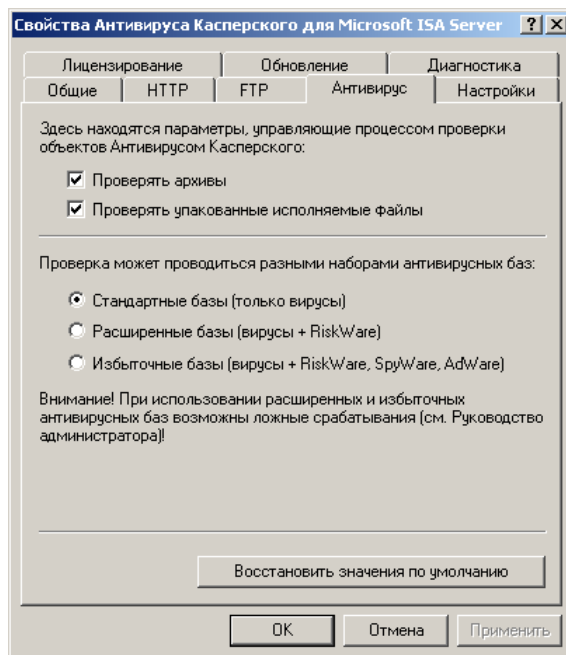


Рисунок 10. Закладка **Антивирус**

В верхней части закладки расположены параметры проверки (см. рис. 10):

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

Примечание

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.

Примечание

При проверке многотомных архивов каждый том воспринимается и обрабатывается Антивирусом Касперского как отдельный объект. В этом случае приложение сможет обнаружить вредоносный код, только если он целиком содержится в одном из томов. Если при частичной загрузке данных вирус будет разделен на части, Антивирус не сможет его найти. В такой ситуации не исключена вероятность распространения вредоносного кода после восстановления целостности объекта.

Многотомные архивы могут быть проверены после сохранения на диске другими приложениями Лаборатории Касперского, например, Антивирусом Касперского для Windows File Servers.

Внимание!

Антивирус Касперского не проверяет архивы, защищенные паролем!

- если необходимо проверять упакованные исполняемые файлы, установите соответствующий флажок.

Примечание

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

В нижней части закладки можно выбрать антивирусные базы, которые будут использоваться при проверке:

- *Стандартные базы (только вирусы)* – антивирусные базы, содержащие подробное описание всех существующих на данный момент вирусов, методов их обнаружения и лечения. Эти базы используются по умолчанию.
- *Расширенные базы (вирусы + RiskWare)* – антивирусные базы, которые помимо вирусов содержат также информацию о потенциально опасных программах (RiskWare). Подобные программы содержат уязвимости, которые могут использоваться для хакерских атак, внедрения неавторизованных программ и т.п.
- *Избыточные базы (вирусы + RiskWare, SpyWare, AdWare)* – наиболее полные антивирусные базы. Помимо описанной выше информации, они включают в себя также описания шпионских программ (SpyWare) и программ-распространителей рекламы (AdWare).

Шпионские программы позволяют несанкционированно получать персональную информацию (например, адреса посещаемых веб-сайтов, пароли, банковские реквизиты) и рассылать ее злоумышленникам.

Программы-распространители рекламы устанавливаются совместно с каким-либо программным обеспечением и в дальнейшем выводят рекламную информацию, либо отображая ее в дополнительных окнах, либо вынуждая пользователя посещать веб-сайт рекламодателя. Помимо того, что происходит навязывание рекламной информации, подобные программы также существенно загружают линии связи и увеличивают суммарный трафик.

Внимание!

При использовании расширенных и избыточных антивирусных баз в некоторых случаях возможно ложное срабатывание Антивируса Касперского при скачивании программного обеспечения, предназначенного для повышения уровня безопасности. Такими программами могут быть программы удаленного наблюдения, не имеющие своей программы установки.

Для обычного режима работы достаточно выбрать стандартные антивирусные базы. Расширенные и избыточные антивирусные базы используются для обеспечения более высокого уровня защиты информации. Использование более полных антивирусных баз приводит к увеличению затрат ресурсов на проверку данных.

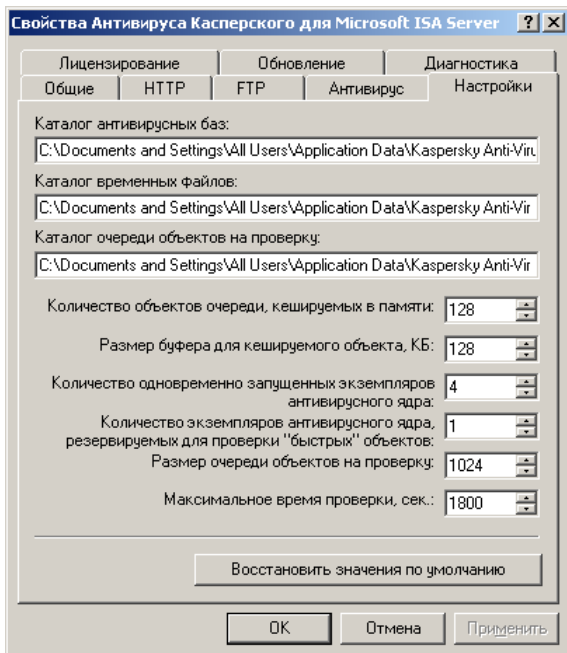
На закладке **Настройки** (см. рис. 11) можно изменять параметры Антивируса Касперского, влияющие на работу сервера.

В верхней части закладки расположены три поля, определяющие пути к рабочим каталогам Антивируса Касперского, установленные по умолчанию. Данные каталоги предназначены для:

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

Внимание!

Чтобы изменение пути к каталогу очереди объектов на проверку вступило в силу, необходимо перезапустить службу Microsoft ISA Server Control и службу Антивируса Касперского.

Рисунок 11. Закладка **Настройки****Внимание!**

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

В нижней части закладки вы можете настроить следующие параметры, влияющие на производительность Антивируса Касперского:

- **Количество объектов очереди, кешируемых в памяти.**
- **Размер буфера для кешируемого объекта, КБ.**
- **Количество одновременно загруженных экземпляров антивирусного ядра.**

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.

Примечание

Можно задать от 1 до 32 включительно одновременно работающих экземпляров антивирусного ядра. Рекомендуется задавать для каждого физического процессора по 4 экземпляра.

- **Количество экземпляров антивирусного ядра, резервируемых для проверки "быстрых" объектов.**

В этом поле можно указать количество экземпляров антивирусного ядра, резервируемых из общего числа загруженных ядер для прохождения рабочего ("быстрого") трафика. Это позволяет снизить влияние проверки больших объектов на пропускную способность Антивируса Касперского.

К "быстрым" объектам относятся только объекты HTTP-трафика, соответствующие следующим критериям:

- текстовые объекты размером менее 2 МБ;
 - графические объекты размером менее 2 МБ;
 - все остальные объекты (за исключением приложений) размером менее 256 КБ.
- **Размер очереди объектов на проверку.** В этом поле укажите максимальное количество объектов, которые могут быть одновременно размещены в рабочем каталоге для объектов, поставленных в очередь на антивирусную проверку.

Примечание

Может быть задана очередь размером от 1 до 16383 объектов включительно. Значение по умолчанию – 1024.

Примечание

Может быть задана очередь размером от 1 до 16383 объектов включительно. Значение по умолчанию – 1024.

Внимание!

Если очередь целиком заполнена, новый объект не будет проверен, будет признан незараженным и отправлен запросившему его клиенту.

Внимание!

При установке многочисленных соединений (более 1000 одновременно) с FTP или HTTP-сервером время проверки некоторых объектов, находящихся в очереди, может превысить тайм-аут сервера. В этом случае произойдет разрыв соединения с сервером, и эти объекты не будут доставлены запросившему их клиенту.

- **Максимальное время проверки, сек.** В этом поле укажите максимальное время, отведенное на проверку объекта.

Примечание

Может быть задано время от 1 до 86400 секунд включительно. Значение по умолчанию – 1800.

Внимание!

Если объект не удалось проверить в течение указанного времени, он будет признан незараженным и будет отправлен запросившему его клиенту.

Для восстановления параметров по умолчанию нажмите на кнопку **Восстановить значения по умолчанию**.

На закладке **Лицензирование** производится управление лицензионными ключами (подробнее см. п. 4.7 на стр. 59).

На закладке **Обновление** определяются опции обновления антивирусных баз (подробнее см. п. 4.3 на стр. 48).

На закладке **Диагностика** настраивается полнота информации, выводимой в журналах (подробнее см. п. 4.6.3 на стр. 57).

4.2.1.2. Параметры проверки HTTP-потока данных

На закладке **HTTP** (см. рис. 12) можно настраивать проверку HTTP-трафика, а также ограничения на работу приложения с потоком данных,

перемещаемых по HTTP-протоколу. Здесь же, при необходимости, редактируется текст информационных сообщений, передаваемых клиентам.

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

- установите флажок **Лечить HTTP-трафик**, если необходимо, чтобы Антивирус Касперского при обнаружении зараженного файла пытался его вылечить;

Примечание

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.

- укажите максимальное время задержки данных, проверяемых приложением, в поле **Максимальное время проверки перед началом отправки данных клиенту, сек.** 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 зараженный файл был обнаружен и вылечен до того, как пользователю был отправлен 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.

Внимание!

При повторном запросе проверка файла будет проведена только в том случае, если между первым и вторым запросом пройдет более 100 секунд. Если время между запросами менее 100 секунд, пользователь получит уведомление о зараженном файле, скопированное из кеша.

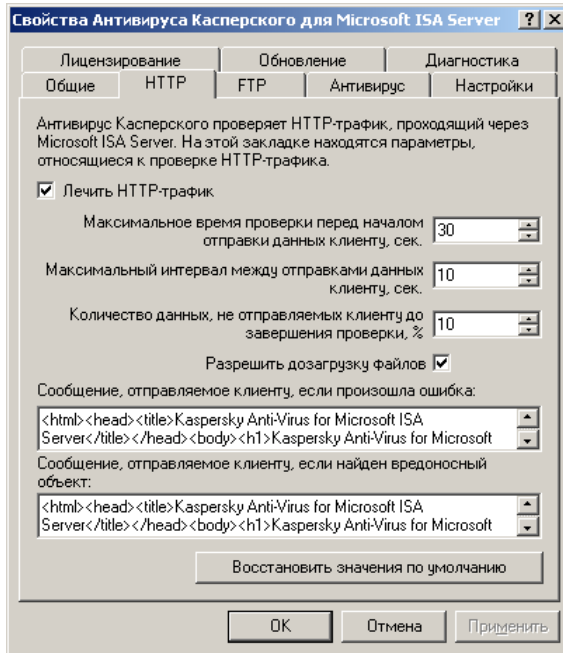


Рисунок 12. Закладка HTTP

- укажите время, в течение которого клиенту требуется отправить следующий пакет проверенных данных, запрашиваемый им, в поле **Максимальный интервал между отправками данных клиенту, сек.**;

Внимание!

Значение данного поля не должно превышать значения поля **Максимальное время проверки перед началом отправки данных клиенту, сек.**

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

Флаг **Разрешить дозагрузку файлов** включает / выключает дозагрузку запрашиваемых клиентами данных в случае, например, разрыва соединения при загрузке.

Внимание!

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 дозагрузке 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. 51.

В любой момент работы с параметрами можно вернуться к параметрам по умолчанию. Для этого нажмите на кнопку **Восстановить значения по умолчанию**.

4.2.1.3. Параметры проверки FTP-потока данных

На закладке **FTP** (см. рис. 13) регулируется проверка данных ISA-сервера, поступающих по протоколам FTP и FTP over HTTP.

Дополнительно к режиму антивирусной проверки можно 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 килобайт.

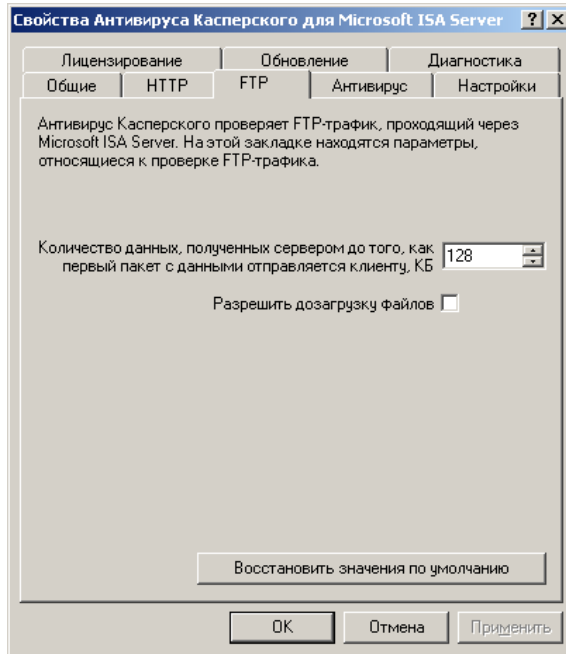


Рисунок 13. Закладка FTP

В любой момент работы с параметрами можно вернуться к параметрам по умолчанию. Для этого нажмите на кнопку **Восстановить значения по умолчанию**.

Внимание!

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 дозагрузке объекта вирус будет также разделен на части, не исключена вероятность его распространения после восстановления целостности объекта.

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.

Примечание

При установке приложения автоматически создается пользователь *default* и группа пользователей *default*, так как наличие хотя бы одной группы пользователей является необходимым условием для функционирования Антивируса Касперского.

Примечание

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

Внимание!

Удалить пользователя и группу по умолчанию нельзя!

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 параметры группы **Администраторы**.

В текущей 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 приложения (см. рис. 7) выберите **Управление группами**. Откроется окно **Управление группами клиентов Антивируса Касперского** (см. рис. 14).

Аналогичное действие выполняется при выборе в дереве сервера узла **Группы**.

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

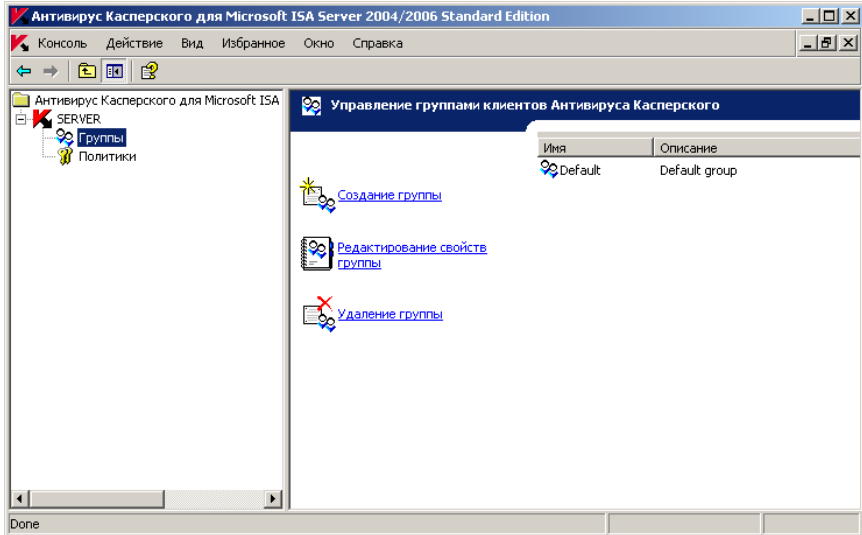


Рисунок 14. Диалоговое окно **Управление группами клиентов Антивируса Касперского**

Чтобы создать группу клиентов:

1. Выберите пункт **Создание группы**.
2. В окне **Создание группы** (см. рис. 15) введите название группы и ее описание.
3. В следующем диалоговом окне (см. рис. 16) нажмите на кнопку **Добавить**.
4. В диалоговом окне **Клиенты** (см. рис. 17) выберите клиента из списка существующих либо создайте нового, нажав на кнопку **Добавить**.
5. Если выбрано создание нового клиента, то в окне **Свойства клиента** (см. рис. 18) необходимо заполнить поле **Имя клиента** и выбрать для заполнения:
 - **Один IP-адрес**, если добавляется клиент с постоянным IP-адресом.
 - **Подсеть**, если клиент может быть задан идентификатором и маской подсети.
 - **Диапазон адресов**, если клиент задается пространством IP-адресов, ограниченным указанным диапазоном.

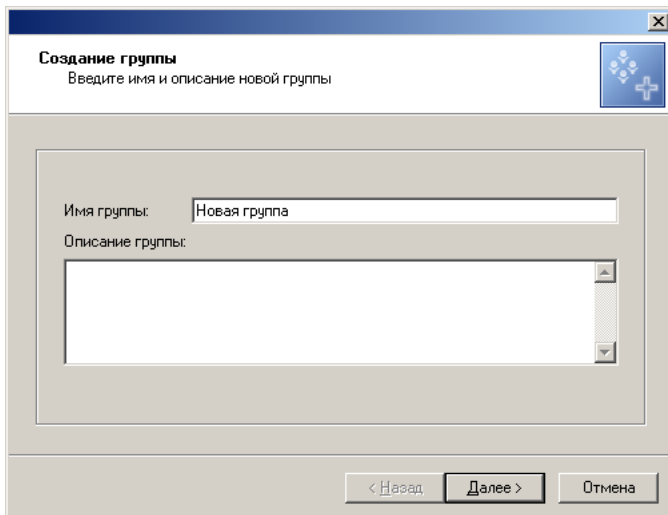


Рисунок 15. Создание новой группы

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

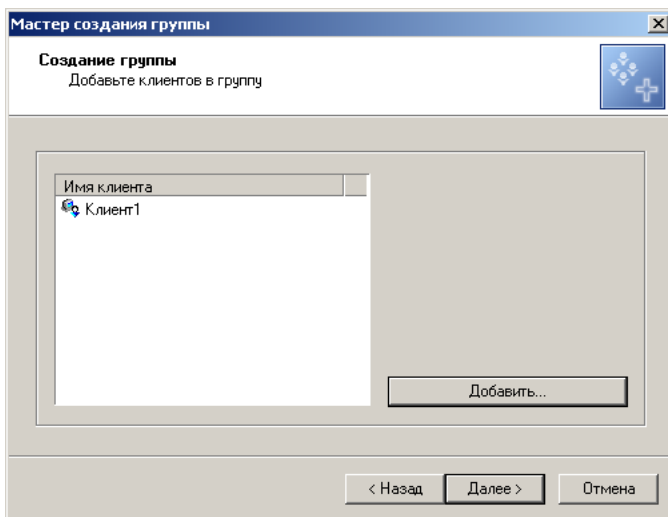


Рисунок 16. Добавление клиентов в новую группу

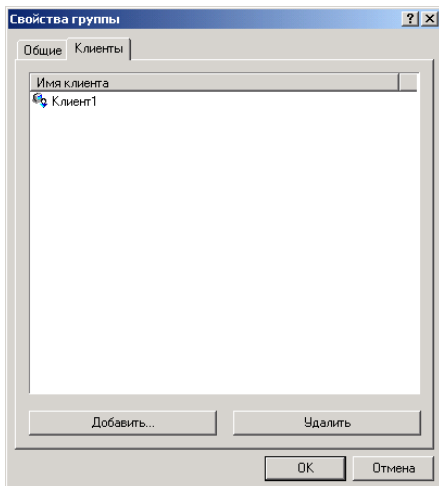
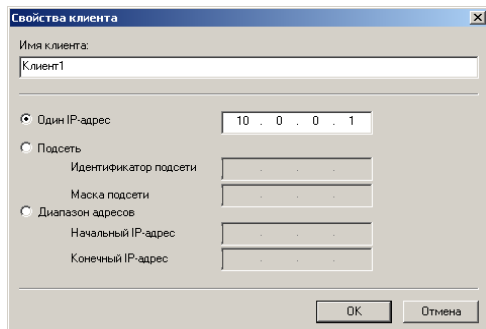
Рисунок 17. Диалоговое окно **Клиенты**

Рисунок 18. Добавление нового клиента в группу

Примечание

Вновь созданная группа сразу прикрепляется к политике *default*.

Чтобы изменить описание и список клиентов группы,

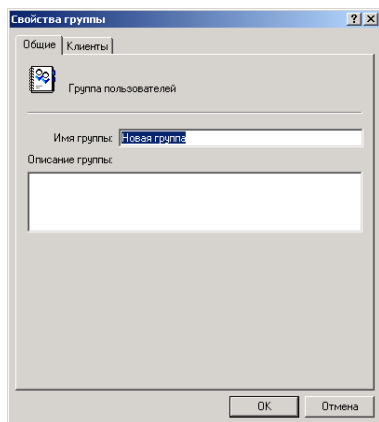
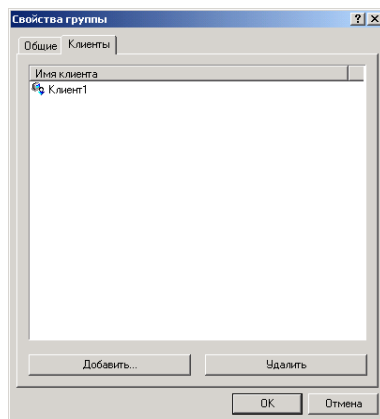
1. в окне **Управление группами клиентов Антивируса Касперского** (см. рис. 14) выделите нужную группу и выберите пункт **Редактирование свойств группы**.
2. В раскрывшемся окне **Свойства группы** на закладке **Общие** (см. рис. 19) можно переименовать группу и изменить ее описание. На закладке **Клиенты** (см. рис. 20) возможно добавление нового либо удаление существующего клиента из группы.

Примечание

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

Чтобы удалить группу,

в окне **Управление группами клиентов Антивируса Касперского** (см. рис. 14) выделите нужную группу и выберите пункт **Удаление группы**.

Рисунок 19. Закладка **Общие**Рисунок 20. 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.

Примечание

При установке приложения автоматически создается политика *default*, так как наличие хотя бы одной антивирусной политики является необходимым условием для функционирования Антивируса Касперского.

Внимание!

Удалить политику по умолчанию нельзя!

Примечание

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 приложения (см. рис. 7) выберите **Управление политиками**. Откроется окно **Управление политиками для Антивируса Касперского** (см. рис. 21).

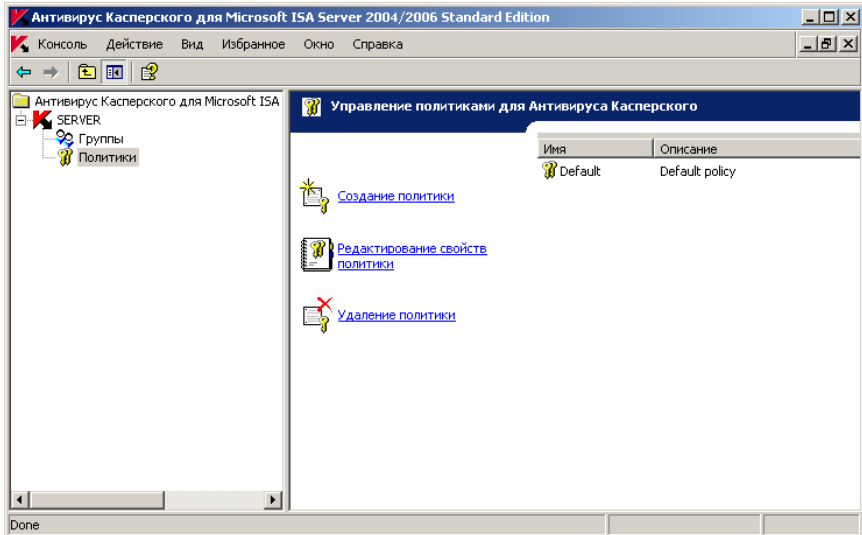


Рисунок 21. Диалоговое окно **Управление политиками для Антивируса Касперского**

Чтобы создать новую политику:

1. Воспользуйтесь ссылкой **Создание политики**.
2. В окне **Создание политики** (см. рис. 22) введите название политики и ее описание.
3. В следующем диалоговом окне (см. рис. 23) нажмите на кнопку **Добавить** и из раскрывающегося списка групп выберите ту группу клиентов, на которую будет распространяться новая политика.
4. В раскрывшемся диалоговом окне (см рис. 24) нажмите на кнопку **Добавить**, чтобы указать доверенные сервера. Входящий трафик для этих серверов не будет проверяться на вирусы. В окне **Доверенный сервер** (см. рис. 28) задайте описание сервера и его свойства (подробнее о доверенных серверах см. п. 4.2.3.1 на стр. 46). После того как будет сформирован список доверенных серверов, нажмите на кнопку **Далее**.

5. В следующем диалоговом окне (см. рис. 25) нажмите на кнопку **Добавить**, чтобы добавить тип объектов, которые не будут проверяться на вирусы (подробнее см. п. 4.2.3.2 на стр. 48).
6. После того как будет сформирован список типов, нажмите на кнопку **Готово**.

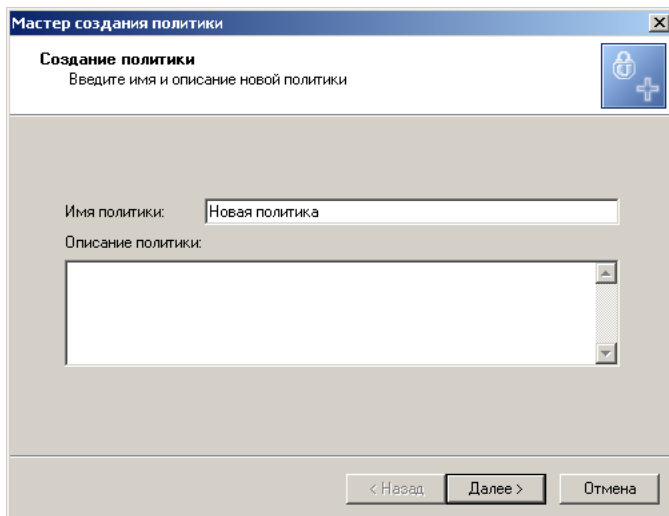


Рисунок 22. Создание новой политики

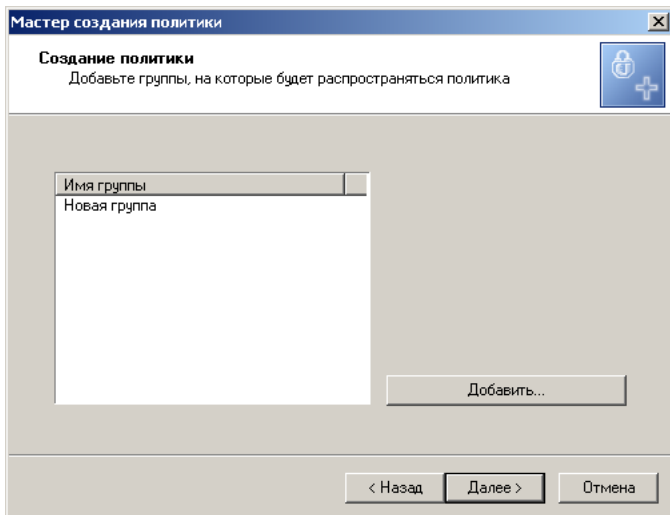


Рисунок 23. Добавление группы клиентов

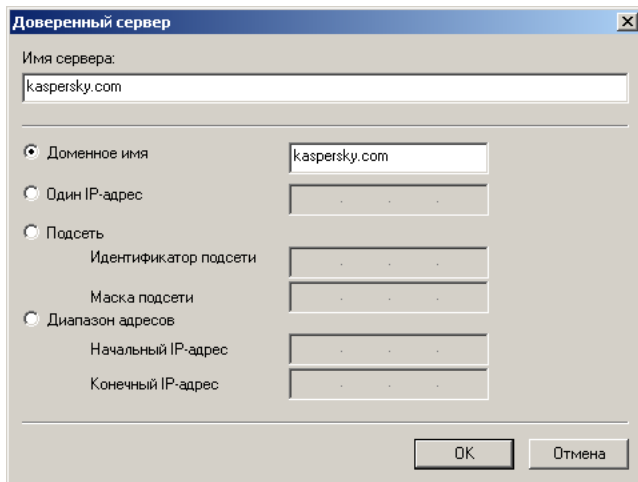


Рисунок 24. Добавление доверительных серверов

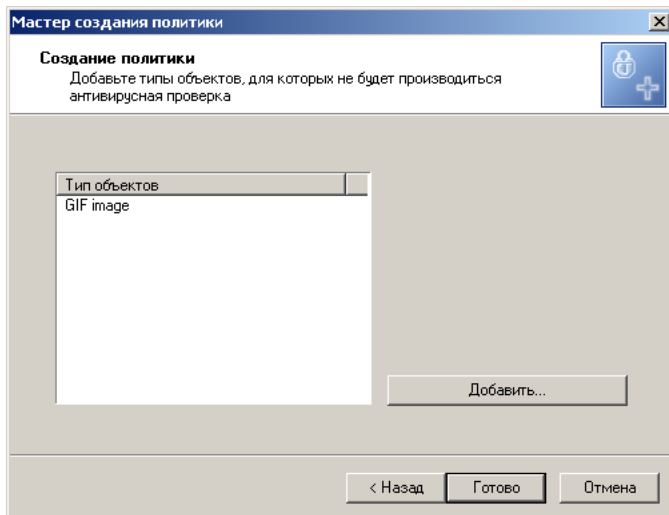


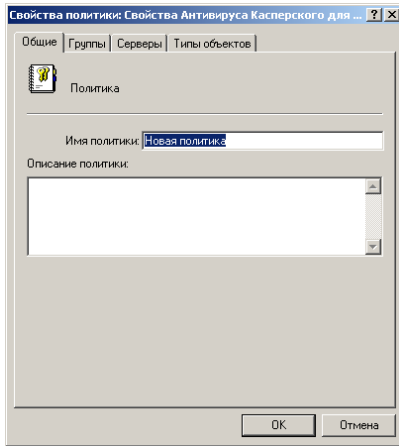
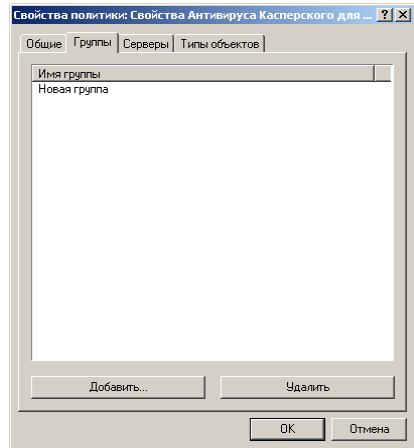
Рисунок 25. Добавление типа объекта

Чтобы редактировать свойства политики,

в окне **Управление политиками для Антивируса Касперского** (см. рис. 21) выделите нужную политику и выберите пункт **Редактирование политики**.

В раскрывшемся окне **Свойства политики** на закладке **Общие** (см. рис. 26) можно переименовать политику и изменить ее описание.

На закладке **Группы** (см. рис. 27) 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. Закладка **Общие**Рисунок 27. Закладка **Группы**

На закладках **Серверы** и **Типы объектов** осуществляется редактирование списков доверенных серверов и непроверяемых типов объектов для данной антивирусной политики.

Чтобы удалить политику,

в окне **Управление политиками для Антивируса Касперского** (см. рис. 21) выделите нужную политику и выберите **Удаление политики**.

Примечание

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 доверенных серверов

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

Управление списком доверенных серверов осуществляется на закладке **Серверы** диалогового окна свойств политики.

При добавлении доверенного сервера открывается диалоговое окно **Доверенный сервер** (см. рис. 28). Задать параметры доверенного сервера можно одним из четырех способов:

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

Чтобы удалить доверенный сервер из списка, нажмите на соответствующую кнопку на закладке Серверы.

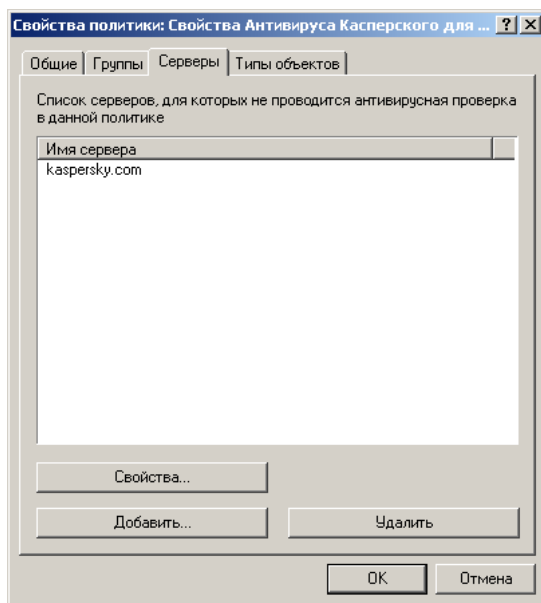


Рисунок 28. Добавление доверительного сервера

4.2.3.2. Формирование списка непроверяемых объектов

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

Управление списком типов осуществляется на закладке **Типы объектов** диалогового окна свойств редактируемой политики. При добавлении нового типа открывается диалоговое окно **Тип объектов** (см. рис. 29).

Примечание

В список непроверяемых объектов по умолчанию уже включены объекты типа **BMP, GIF и PNG**.

Если вы хотите, чтобы Антивирус Касперского не проверял объекты при потоковой передаче аудио- и видеоинформации, исключите из проверки объекты типа **Adobe flash video, Windows Media Streaming Protocol object и QuickTime video**.

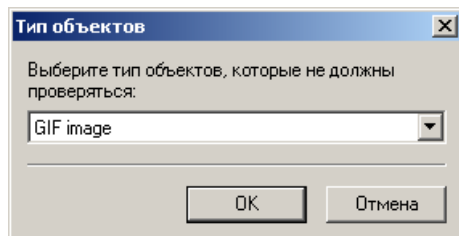


Рисунок 29. Добавление типа объекта

4.3. Обновление антивирусных баз

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

- интернет по FTP- или HTTP-протоколу с серверов обновлений Лаборатории Касперского;
- локальный или сетевой каталог.

Примечание

Антивирусные базы на серверах обновлений Лаборатории Касперского обновляются ежедневно.

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

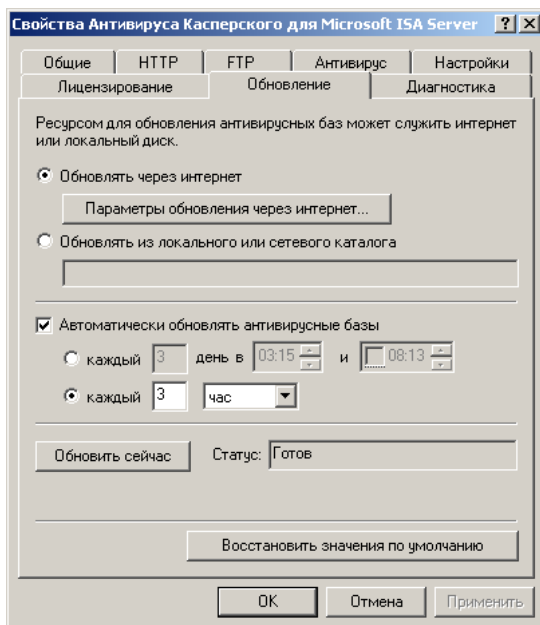


Рисунок 30. Задание параметров обновления антивирусных баз

Для настройки параметров обновления антивирусных баз через интернет выполните следующие действия:

1. Выберите в главном окне приложения пункт **Редактирование параметров Антивируса Касперского** и в открывшемся диалоговом окне **Свойства Антивируса Касперского для Microsoft ISA Server** выберите закладку **Обновление**.
2. На закладке **Обновление** антивирусных баз укажите источник обновления **Обновлять через интернет**.
3. Нажмите на кнопку **Параметры обновления через интернет**, чтобы указать сервер-ресурс получения обновлений.

4. В раскрывшемся диалоговом окне **Параметры обновления через интернет** (см. рис. 31):
 - выберите **Автоматически выбирать сервер обновлений**, если для получения обновлений вы хотите использовать выбранный приложением сервер;
 - выберите **Использовать указанный сервер**, если вы хотите самостоятельно определить сервер для получения обновлений. В поле ввода укажите адрес сервера.
5. 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 Microsoft ISA Server.
 - Выберите **Использовать другой прокси-сервер** и укажите в полях **Имя прокси-сервера** и **порт** прокси-сервера, отличный от локального прокси ISA-сервера.

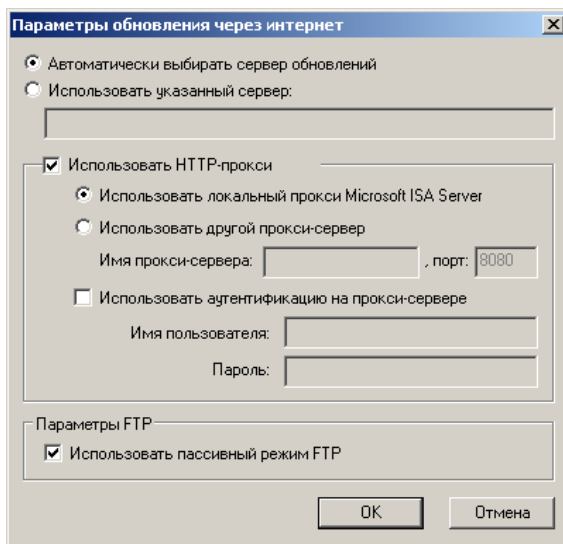


Рисунок 31. Настройка параметров сервера обновления антивирусных баз

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

Чтобы получить обновления антивирусных баз из локальной сети,

в окне **Обновление антивирусных баз** выберите способ обновления **Обновлять из локального или сетевого каталога** и в поле укажите полный путь к нему (см. рис. 31).

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 каждые 3 часа.

В следующих полях можно настроить частоту и время проведения обновлений антивирусных баз.

4.3.2. Ручной запуск получения обновлений

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

Примечание

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

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

4.4. Настройка параметров уведомлений пользователей

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

Примечание

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

Сообщение формируется в поле **Сообщение, отправляемое клиенту, если найден вредоносный объект** (см. рис. 12) 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. 12):

```
<html>
<head>
<title>Kaspersky Anti-Virus for Microsoft ISA Serv-
er</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.

Можно отредактировать сообщения, направляемые пользователю, на закладке **HTTP** диалогового окна **Свойства Антивируса Касперского для Microsoft ISA Server** (см. рис. 12). Максимальная длина сообщения – 10240 байт. Кодовая страница зависит от региональных параметров операционной системы. Например, если в региональных параметрах установлен русский язык, то кодовая страница сообщения будет *windows-1251*.

4.5. Проверка корректности работы Антивируса Касперского

После установки и настройки параметров Антивируса Касперского рекомендуется проверить правильность заданных параметров и корректность работы приложения с помощью тестового "вируса" и его модификаций.

Тестовый "вирус" был специально разработан организацией  (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 компьютеру, при этом большинство продуктов антивирусных компаний-производителей идентифицируют его как вирус.

Внимание!

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 Касперского обнаруживает его, идентифицирует как зараженный 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. 21) при попытке загрузить тестовый "вирус" соединение с ресурсом будет разорвано, и на экран будет выведено сообщение о том, что данный объект заражен вирусом *eicar*.

4.6. Статистика и диагностика работы приложения

Антивирус Касперского предоставляет возможность просматривать статистику своей работы посредством стандартных счетчиков производительности Microsoft Windows и редактировать способы уведомления администратора о важном событии. Также можно настраивать ведение журналов событий Антивируса Касперского, 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 Microsoft Windows, доступные через консоль **Производительность** (Пуск → Настройка → Панель управления → Администрирование → Системный монитор).

Чтобы выбрать, какие сведения будут отражаться в статистике:

1. Перейдите в окно **Добавить счетчики** (см. рис. 32) 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 **KAV for ISA**. 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**.

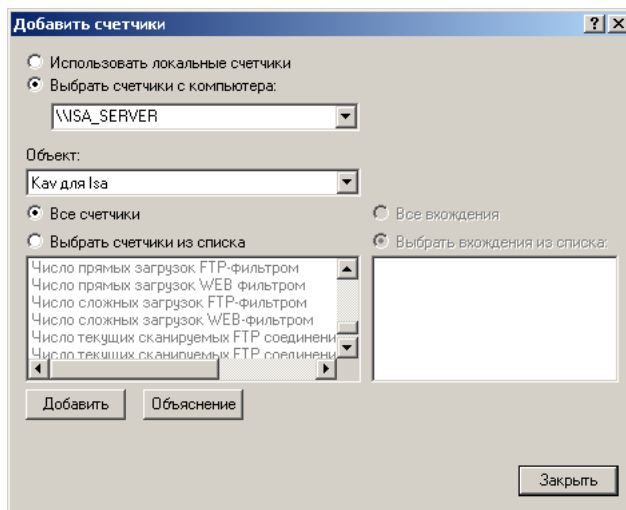


Рисунок 32. Настройка параметров отображения статистики

Внимание!

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

1. Просмотр статистики с удаленного компьютера также требует наличия следующих привилегий пользователя на том компьютере, где установлен Антивирус Касперского для Microsoft ISA Server:
 - права на чтение файлов:
 - %windir%\System32\PERFCxxx.DAT
 - %windir%\system32\PERFHxxx.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.

Примечание

Более подробную информацию о приведенном выше перечне привилегий можно найти в документации к Microsoft Windows Server 2000/2003.

По умолчанию данные права есть у пользователей, являющихся членами локальной группы **Администраторы** компьютера, на котором установлен Антивирус Касперского для Microsoft ISA Server.

3. Для удаленного просмотра статистики на сервере с установленным Антивирусом Касперского также должен быть:
 - запущен сервис **Служба удаленного управления реестром**;
 - доступ по NetBIOS (в свойствах сетевого подключения **Сетевое окружение → Свойства → Подключение к локальной сети → Свойства** должен быть установлен флажок **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 критических событиях, возникающих при работе какого-либо из установленных на ISA-сервере приложений.

Для Антивируса Касперского также предусмотрен ряд важных событий, возникновение которых требует реакции администратора системы, например, события *Антивирусные базы повреждены* (см. рис. 33), *Ошибка при загрузке антивирусных баз из источника обновления*, *Истекает срок действия лицензии* или *Обнаружен зараженный объект в HTTP-трафике*. Набор таких событий пополняет существующий список сразу после установки приложения на сервер. Способ уведомления для каждого из событий можно настроить самостоятельно.

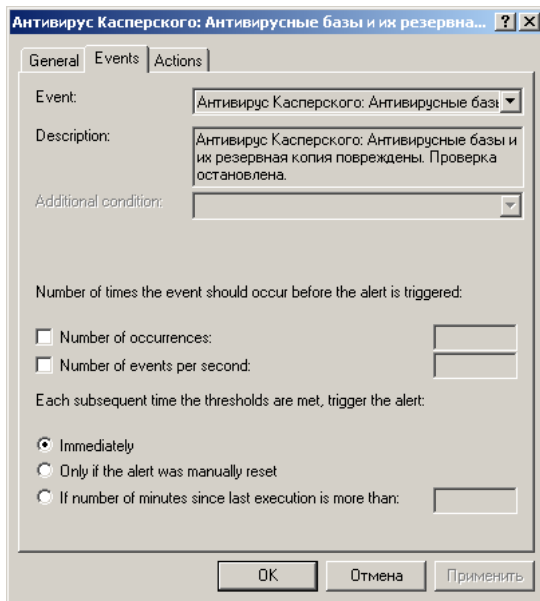


Рисунок 33. Настройка параметров уведомления администратора при возникновении важного события в работе приложения

4.6.3. Настройка параметров диагностики работы приложения

Антивирус Касперского позволяет проводить полную диагностику своей работы для любого из Microsoft ISA-серверов, на которых он установлен, и фиксировать ее результаты в следующих файлах журналов:

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

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

*virus***DATA**.log – журнал Антивируса Касперского, включающий информацию об обнаруженных вредоносных объектах.

Можно настроить полноту информации, выводимой в перечисленные выше журналы, в окне **Свойства сервера** на закладке **Диагностика** (см. рис. 34).

Примечание

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

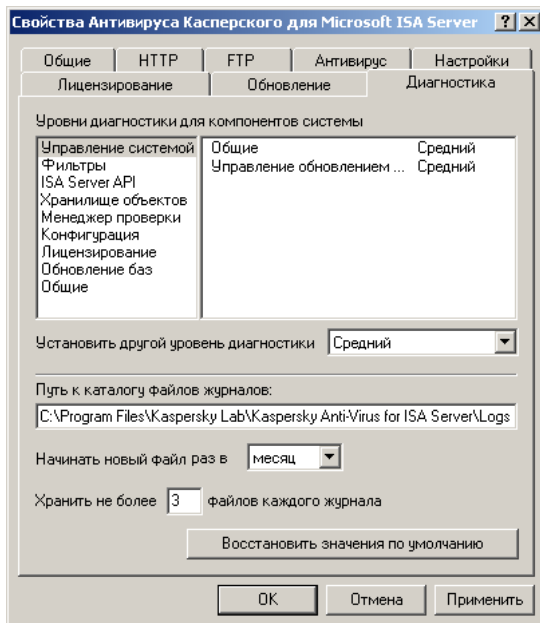


Рисунок 34. Параметры диагностики работы Антивируса Касперского

Все важные сообщения о работе Антивируса Касперского также выводятся в Системный журнал приложений операционной системы Microsoft 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 можно 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. На этом уровне диагностики может выводиться достаточно большое количество сообщений, что может привести к снижению производительности и быстрому заполнению дискового пространства. Рекомендуется включать его только для диагностики ошибок в работе приложения.

По умолчанию для всех сообщений установлен минимальный уровень детализации.

На этой же закладке можно настроить частоту формирования журналов и их количество.

В любой момент работы с параметрами можно вернуться к параметрам по умолчанию. Для этого нажмите на кнопку **Восстановить значения по умолчанию**.

4.7. Ограничения при работе с Антивирусом Касперского

Существует ряд параметров Антивируса Касперского, которые повышают удобство работы, но увеличивают риск проникновения вредоносных объектов в защищаемую сеть. К таким параметрам относятся:

- Возможность дозагрузки файлов по протоколу HTTP. Для повышения надежности антивирусной защиты не рекомендуется разрешать дозагрузку файлов. В противном случае части файла будут проходить антивирусную проверку как отдельные объекты. При этом сигнатура вредоносного объекта может быть разделена и не распознана Антивирусом Касперского.
- Уменьшение значения параметра **Максимальное время проверки**. Для объектов, проверяемых достаточно большой период времени (по причине большого размера объекта или низкой скорости загрузки с удаленного сервера), ограничение времени максимальной проверки может привести к тому, что объект не будет прове-

рен. Однако при этом объекту будет присвоен статус **Файл не заражен**.

- Уменьшение значений параметров **Максимальное время проверки перед началом отправки данных клиенту** и **Количество данных, полученных сервером до того, как первый пакет с данными отправляется клиенту** может привести к тому, что долго проверяемые объекты будут частично переданы клиенту до полного завершения проверки, что повышает риск проникновения в сеть вредоносных объектов.
- Уменьшение значения параметра **Количество данных, не отправляемых клиенту до завершения проверки**. Это может привести к тому, что при одновременной проверке и отправке файла увеличивается риск проникновения вируса.

Также существует также ряд ограничений, связанных с логикой работы Антивируса Касперского версии 5.6:

- Приложение проверяет только входящий http и ftp-трафик, маршрутизируемый с помощью ISA-сервера.
- Приложение не проверяет данные, запрашиваемые клиентом с серверов, опубликованных с помощью сервера ISA.
- Приложение не проверяет данные, копируемые клиентом на сервера, опубликованные с помощью сервера ISA.

4.8. Управление лицензионными ключами

Управление лицензионными ключами осуществляется на закладке **Лицензирование** диалогового окна **Свойства Антивируса Касперского для Microsoft ISA Server** (см. рис. 35).

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, и антивирусная проверка потоков данных будет недоступна.

Примечание

Дважды использовать пробный ключ невозможно!

Если лицензионный ключ отсутствует или не соответствует данному приложению, Антивирус Касперского 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 срока действия лицензии. Следовательно, не гарантируется защита данных от новых вирусов, появившихся после окончания срока действия лицензии.

Внимание!

Если после окончания срока действия лицензии в приложение будут подложены антивирусные базы, выпущенные позже даты истечения лицензии, Антивирус Касперского отреагирует на это действие как на нарушение лицензионного соглашения.

В результате антивирусная проверка будет отключена!

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

4.8.1. Установка лицензионного ключа

Для полнофункциональной работы Антивируса Касперского необходимо установить лицензионный ключ.

Чтобы установить лицензионный ключ,

на закладке **Лицензирование** (см. рис. 35) в поле **Текущий лицензионный ключ** нажмите на кнопку **Добавить/Заменить** и в открывшемся окне укажите файл действующего лицензионного ключа (*.key).

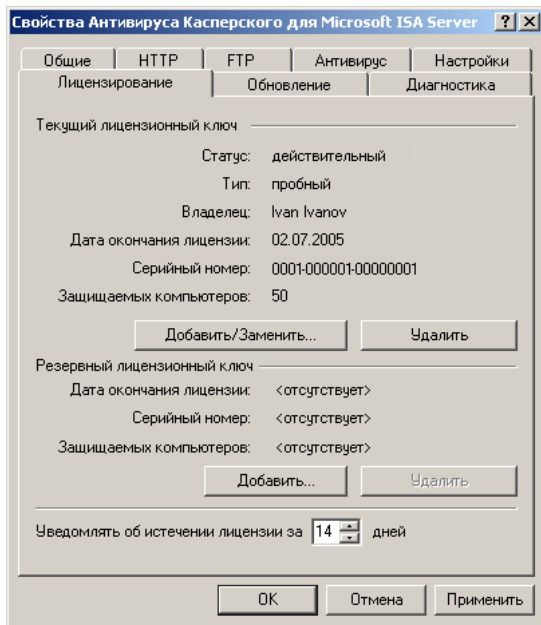


Рисунок 35. Управление лицензионными ключами

После добавления лицензионного ключа отобразится следующая информация о нем:

- статус лицензионного ключа;
- тип лицензионного ключа;
- владелец лицензии;
- дата окончания срока действия лицензии;
- серийный номер лицензионного ключа;
- количество защищаемых компьютеров.

Чтобы настроить время уведомления об истечении срока действия лицензии,

на закладке **Лицензирование** (см. рис. 35) укажите в соответствующем поле необходимое количество дней. Когда до истечения срока действия лицензионного ключа останется заданное количество дней, ежедневно в системном журнале компьютера, на котором установлен Антивирус Касперского, будет фиксироваться соответствующее сообщение. В нем будет указано оставшееся количество дней.

Примечание

Дату окончания срока действия лицензии также можно посмотреть на вкладке **Общие** (см. рис. 9) окна свойств Антивируса Касперского.

Существует возможность установки резервного ключа, который вступит в силу сразу по окончании действующего. Таким образом, вам удастся обеспечить непрерывную защиту сервера.

Для установки резервного ключа в поле **Резервный лицензионный ключ** нажмите на кнопку **Добавить** (см. рис. 35) и в открывшемся окне укажите файл резервного ключа (*.key).

После добавления резервного лицензионного ключа о нем отобразится следующая информация:

- дата окончания срока действия лицензии;
- серийный номер лицензионного ключа;
- количество защищаемых компьютеров.

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.

Внимание!

Невозможно установить более двух лицензионных ключей.

4.8.2. 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, обновление антивирусных баз будет недоступно, следовательно, мы не можем гарантировать стопроцентную антивирусную защиту.

Чтобы продлить лицензию на использование Антивируса Касперского, 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 **Интернет-магазин**. По факту оплаты по электронной почте бу-

дет отправлен лицензионный ключ. Полученный лицензионный ключ необходимо установить (подробнее см. п. 4.8.1 на с. 61).

Примечание

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**.

4.8.3. Удаление лицензионного ключа

При установке нового лицензионного ключа существует возможность самостоятельно удалить просроченный ключ, воспользовавшись соответствующей кнопкой на закладке **Лицензирование** (см. рис. 35).

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

ГЛАВА 5. ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ

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

Вопрос: возможно ли использование Антивируса Касперского с антивирусными продуктами других производителей?

Во избежание конфликтов мы рекомендуем удалять антивирусные продукты сторонних производителей до установки Антивируса Касперского.

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

Детектирование вирусов является 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.

В отличие от других антивирусов, сокращающих время проверки путем исключения из антивирусных баз более сложных в обнаружении или более редких (например, в географическом отношении) вирусов, а также более сложных в анализе форматов файлов (например, pdf), Лаборатория Касперского считает, что задача Антивируса – обеспечивать реальную антивирусную безопасность пользователей.

Антивирус Касперского позволяет опытному пользователю ускорить антивирусную проверку путем отключения антивирусной проверки различных типов файлов. Однако не стоит забывать, что это приводит к снижению уровня безопасности.

Антивирус Касперского распознает более 1200 форматов архивированных и сжатых файлов, а четыре формата лечит. Это очень важно для антивирусной безопасности, поскольку каждый из распознаваемых форматов может содержать исполняемый вредоносный код. Тем не менее, новая версия продукта работает быстрее, чем предыдущая, несмотря на ежедневное увеличение общего количества обнаруживаемых Антивирусом Касперского вирусов, а также постоянное увеличение количества распознаваемых форматов.

Вопрос: зачем нужен лицензионный ключ? Может ли мой Антивирус Касперского 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), 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 по-прежнему будет выполнять лечение зараженных объектов, но с использованием старых антивирусных баз.

При возникновении данной ситуации проинформируйте вашего системного администратора или обратитесь за продлением лицензии в компанию, где был приобретен Антивирус Касперского или непосредственно в ЗАО "Лаборатория Касперского".

Вопрос: отсутствует антивирусная проверка. Зараженные файлы свободно загружаются из сети. Почему?

Если возникла подобная проблема, проверьте следующее:

1. В приложении Антивирус Касперского зарегистрирован действующий лицензионный ключ.
2. Режим функционирования приложения можно узнать в окне свойств сервера на закладке **Общие**. Антивирусная проверка выполняется для режимов **полная функциональность** и **без обновлений**.
3. Если режим не соответствует указанному, необходимо добавить / продлить лицензию (см. п. 4.7 на стр. 59).
4. Убедитесь, что ваш браузер настроен таким образом, что все запросы проходят через антивирусный фильтр Антивируса Касперского.
5. Службы ISA-сервера были хотя бы раз перезапущены после установки Антивируса Касперского, так как ISA-сервер активирует новые фильтры только при старте своих служб.
6. Для решения данной проблемы убедитесь, что необходимые фильтры активированы в консоли администрирования и перезапустите службы из консоли Microsoft ISA Server.

7. Фильтры Антивируса Касперского инициализированы после старта служб ISA-сервера.
8. В этом случае в журнале работы приложения и в системном журнале должна появиться запись **Web / FTP-фильтр проинициализирован**.
9. Если соответствующая запись не появилась в журнале, обратитесь в Службу технической поддержки Лаборатории Касперского.
10. Проверьте корректность работы Антивируса с помощью тестового вируса (см. п. 4.5 на стр. 53).
11. Если тестовый вирус не распознается как зараженный объект, возможно, он берется из локального кеша вашего браузера. В этом случае воспользуйтесь командой браузера, позволяющей принудительно загрузить файл с сервера, минуя кеш.

Если в результате описанных действий не удалось решить проблему, пожалуйста, обратитесь в Службу технической поддержки Лаборатории Касперского.

Вопрос: Зачем нужны ежечасные обновления?

Еще несколько лет назад вирусы передавались на дискетах и для защиты компьютера достаточно было установить антивирусную программу и изредка обновлять антивирусные базы. Но последние вирусные эпидемии распространялись по миру всего за несколько часов, и установленный Антивирус со старыми базами может оказаться бессилён перед новой угрозой. Для того чтобы не стать жертвой новых вирусов, необходимо обновлять антивирусные базы ежедневно.

Лаборатория Касперского с каждым годом увеличивает частоту обновления антивирусных баз. Сейчас они обновляются ежечасно.

Дополнительной функцией является задача обновления программных модулей Антивируса, в которых исправляются обнаруженные уязвимости или предоставляются новые функциональные возможности.

Вопрос: Антивирусные базы не обновляются. Почему?

Чтобы найти причину, препятствующую обновлению антивирусных баз, сначала установите **Отладочный** уровень выдачи диагностических сообщений для всех категорий подсистем **Управление системой** и **Обновление баз** на закладке **Диагностика** (см. рис. 34). Затем вручную запустите обновление антивирусных баз и после завершения процесса проанализируйте журнал работы приложения (см. п. 4.6.1 на стр. 54).

Если установлено обновление антивирусных баз из интернета (см. рис. 30), то возможно не удастся установить соединение с сервером обновлений. В этом случае в журнале работы приложения будут содержаться

сообщения о неудачных попытках соединения с сервером или истекших тайм-аутах соединения. Проверьте параметры получения обновлений и ISA-сервера в следующем порядке:

1. Определите выбранный способ получения обновлений Антивируса Касперского:
 - локальный прокси ISA-сервера;
 - другой прокси-сервер (или получение обновлений напрямую, минуя прокси-сервер).

Эту информацию можно найти в окне **Параметры обновления через интернет**.

В случае обновления через локальный прокси ISA-сервера:

- Убедитесь, что соединение с серверами обновлений Лаборатории Касперского действительно возможно. Например, настройте аналогичным образом параметры браузера Internet Explorer на том же компьютере, где установлен Антивирус Касперского, и откройте любую веб-страницу.
- Проверьте режим аутентификации на прокси-сервере и при необходимости задайте имя пользователя / пароль в параметрах программы обновления Антивируса Касперского.

Внимание!

Процедура обновления антивирусных баз выполняется Антивирусом Касперского под учетной записью **LocalSystem**, которая без специальной настройки параметров имеет ограниченные права в локальной сети (подробнее см. п. 4.3 на стр. 48).

В случае обновления через другой прокси-сервер или напрямую убедитесь, что правила фильтрации Microsoft ISA Server Firewall разрешают обращения программы обновления (процесс **kavisasrv.exe**) в интернет.

2. Если установлено обновление из локального или сетевого каталога, то возможно возникновение следующих проблем:
 - отсутствие прав на доступ к указанному каталогу;
 - неправильно выложенные антивирусные базы.

Внимание!

Антивирусные базы необходимо выкладывать в сетевой каталог, обязательно сохраняя структуру каталогов сервера обновлений Лаборатории Касперского. В противном случае процедура обновления не обнаружит в указанном каталоге антивирусных баз.

Если в результате описанных действий не удалось решить проблему, пожалуйста, обратитесь в Службу технической поддержки Лаборатории Касперского.

Вопрос: может ли злоумышленник подменить антивирусные базы?

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 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 Microsoft ISA-сервер для доступа в интернет.

Консоль администрирования – специальное приложение, обеспечивающее пользовательский интерфейс для выполнения задач администрирования Антивируса Касперского.

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, в странах Бенилюкса, 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 четырехсот пятидесяти высококвалифицированных специалистов, десять из которых имеют дипломы MBA, шестнадцать – степени кандидатов наук. Ведущие вирусные аналитики «Лаборатории Касперского» являются членами престижной организации Computer Anti-virus Researcher's Organization (CARO).

Главная ценность компании – уникальные знания и опыт, накопленные ее сотрудниками в 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 систем, сетевых экранов и интернет-шлюзов, 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), 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. Наши базы обновляются каждый час. Мы обеспечиваем наших пользователей круглосуточной технической поддержкой на нескольких языках.

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, 123060, Москва, 1-й Волоколамский проезд, д.10, стр.1
Факс:	+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00
Экстренная круглосуточная помощь:	+7 (495) 797-87-07, +7 (495) 645-79-29, +7 (495) 956-87-08
Поддержка пользователей персональных и бизнес-продуктов:	+7 (495) 797-87-07, +7 (495) 645-79-29, +7 (495) 956-87-08 (с 10:00 до 18:30 по московскому времени) http://support.kaspersky.ru/helpdesk.html
Поддержка корпоративных пользователей:	Контактная информация предоставляется при покупке корпоративных продуктов в зависимости от пакета технической поддержки.
Веб-форум «Лаборатории Касперского»:	http://forum.kaspersky.com
Антивирусная лаборатория:	newvirus@kaspersky.com (только для отправки новых вирусов в архивированном виде)
Группа подготовки пользовательской документации:	docfeedback@kaspersky.com (только для отправки отзывов о документации и электронной справочной системе)
Департамент продаж:	+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00 sales@kaspersky.com

Общая информация:	+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00 info@kaspersky.com
WWW:	http://www.kaspersky.ru http://www.viruslist.ru