ЛАБОРАТОРИЯ КАСПЕРСКОГО

Антивирус Касперского 6.0 для Windows Servers Enterprise Edition

РУКОВОДСТВО ПО УСТАНОВКЕ

АНТИВИРУС КАСПЕРСКОГО 6.0 ДЛЯ WINDOWS SERVERS ENTERPRISE EDITION

Руководство по установке

Тел., факс: +7 (495) 797-8700, +7 (495) 645-7939,
+7 (495) 956-7000
http://www.kaspersky.ru/

Дата редакции: сентябрь 2008 г.

Содержание

ГЛАВА 1. ВВЕДЕНИЕ

Это руководство описывает установку приложения Антивирус Касперского 6.0 для Windows Servers Enterprise Edition (далее – Антивирус).

Антивирус защищает серверы на платформе Microsoft Windows от угроз, проникающих посредством файлового обмена. Он предназначен для использования в локальных сетях средних и крупных организаций.

Вы можете устанавливать Антивирус на серверах, выполняющих разные функции: на серверах терминалов и принт-серверах, на серверах приложений и контроллерах доменов, а также на файловых серверах – они более других подвержены заражению, так как обмениваются файлами с рабочими станциями пользователей.

Вы можете устанавливать Антивирус на серверах, объединенных в кластер. Установите Антивирус на каждый узел кластера.

Вы можете устанавливать Антивирус как с помощью мастера установки, так и с помощью запуска из командной строки *msi*-файла инсталляционного пакета. Вы также можете выполнить централизованную удаленную установку Антивируса через групповые политики Active Directory или с помощью задачи удаленной установки Kaspersky Administration Kit.

Перед тем как начать установку Антивируса, спланируйте ее. Определите, как вам будет удобнее управлять Антивирусом в зависимости от архитектуры сети, какие программные компоненты Антивируса вам потребуется установить для выбранной схемы управления. Определите, потребуется ли вам задавать специальные параметры установки Антивируса или вы будете использовать параметры установки по умолчанию; будут ли параметры установки едиными для всех серверов или индивидуальными для каждого сервера. Выберите способ установки (Глава 4 на стр. 34).

Глава 3 содержит общие сведения об установке Антивируса: в ней перечислены требования к компьютеру для установки Антивируса, описаны файлы комплекта поставки, программные компоненты, которые вы можете установить, параметры установки и специальные ключи службы Windows Installer для установки Антивируса из командной строки. В этой главе указано местоположение и название файла журнала установки / удаления и описаны изменения в системе после установки.

Главы 4 – 7 содержат инструкции по установке Антивируса разными способами; в них также описана последующая настройка Антивируса (см. разделы *Действия после установки*).

После установки Антивируса не требуется перезагрузка сервера. Если вы выполняете добавление или удаление компонентов, восстанавливаете Ан-

тивирус или удаляете его, перезагрузка сервера может потребоваться. Однако вы можете отложить перезагрузку.

После того как вы установите Антивирус, вы можете проверить его работоспособность. Глава 9 рассказывает о том, как это выполнить с помощью специального тестового вируса EICAR.

Если у вас возникли вопросы об Антивирусе, ответы на которые вы не нашли в этом документе, вы можете обратиться к другим источникам информации (Глава 2 на стр. 8).

ГЛАВА 2. ПОЛУЧЕНИЕ ИНФОРМАЦИИ ОБ АНТИВИРУСЕ

Если у вас возникли вопросы по выбору, приобретению, установке или использованию Антивируса, вы можете быстро получить ответы на них.

«Лаборатория Касперского» располагает многими источниками информации о приложении, и вы можете выбрать наиболее удобный для вас в зависимости от важности и срочности вопроса. Вы можете:

- найти ответ на свой вопрос самостоятельно (см. п. 2.1 на стр. 8);
- получить ответ от сотрудников Департамента продаж (см. п. 2.2 на стр. 10);
- получить ответ от специалиста Службы технической поддержки, если вы уже приобрели Антивирус (см. п. 2.3 на стр. 11);
- обсудить свой вопрос не только со специалистами «Лаборатории Касперского», но и с другими пользователями в разделе веб-форума, посвященном Антивирусу (см. п. 2.4 на стр. 13).

2.1. Источники информации для самостоятельного поиска

Вы можете обратиться к следующим источникам информации о приложении:

- странице приложения на веб-сайте «Лаборатории Касперского»;
- странице приложения на веб-сайте Службы технической поддержки (в Базе знаний);
- электронной справочной системе;
- документации.

Страница на веб-сайте «Лаборатории Касперского»

http://www.kaspersky.ru/kaspersky_anti-virus_windows_server_enterprise

На этой странице вы получите общую информацию о приложении, его возможностях и особенностях. Вы можете приобрести приложение или продлить срок его использования в нашем электронном магазине.

Страница на веб-сайте Службы технической поддержки (База знаний)

http://support.kaspersky.ru/win_serv_ee_6mp2

На этой странице вы найдете статьи, опубликованные специалистами Службы технической поддержки.

Эти статьи содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы по приобретению, установке и использованию приложения. Они сгруппированы по темам, таким как «Работа с файлами ключей», «Настройка обновлений баз» или «Устранение сбоев в работе». Статьи могут отвечать на вопросы, которые относятся не только к этому приложению, но и к другим продуктам «Лаборатории Касперского»; они могут содержать новости Службы технической поддержки в целом.

Электронная справочная система

В комплект поставки приложения входит файл полной справки.

Полная справка содержит информацию о том, как с помощью консоли Антивируса в MMC управлять защитой компьютера: просматривать состояние защиты, выполнять проверку различных областей компьютера, выполнять другие задачи. В ней содержится информация о том, как управлять приложением из командной строки, использовать счетчики производительности Антивируса, счетчики и ловушки протокола SNMP.

Чтобы открыть полную справку, в консоли Антивируса выберите команду **Вызов справки** в меню **Справка**.

Если у вас возникнет вопрос по отдельному окну приложения, вы можете обратиться к контекстной справке.

Чтобы открыть контекстную справку, нажмите на кнопку **Справка** в интересующем вас окне или на клавишу **<F1>**.

Документация

Комплект документов к приложению содержит большую часть информации, необходимой для работы с ним. Он состоит из следующих документов:

- **Типовые схемы применения**. Этот документ рассказывает о применении Антивируса в сети предприятия.
- **Сравнение с Антивирусом Касперского 6.0 для Windows Servers**. Этот документ перечисляет характеристики Антивиру-

са, которые отличают его от Антивируса Касперского 6.0 для Windows Servers.

- **Руководство по установке** содержит требования к компьютеру для установки Антивируса, инструкции по установке и активации Антивируса, проверке его работоспособности и первоначальной настройке.
- **Руководство администратора** (этот документ) содержит информацию о том, как работать с консолью Антивируса в MMC, управлять Антивирусом из приложения Kaspersky Administration Kit и из командной строки, использовать счетчики производительности Антивируса и счетчики и ловушки для протокола SNMP.

Файлы с этими документами в формате PDF входят в комплект поставки Антивируса.

Вы можете загрузить файлы документов со страницы приложения на сайте «Лаборатории Касперского».

После установки консоли Антивируса вы можете открыть руководство администратора из меню **Пуск**.

2.2. Обращение в Департамент продаж

Если у вас возникли вопросы по выбору или приобретению Антивируса или продлению срока его использования, вы можете поговорить с сотрудниками Департамента продаж в нашем центральном офисе в Москве по телефонам:

+7 (495) 797-87-00, **+7 (495) 645-79-39**, **+7 (495) 956-70-00**.

Обслуживание ведется на русском и английском языках.

Вы можете задать вопрос сотрудникам Департамента продаж по электронной почте, по адресу sales@kaspersky.com.

В департаменте продаж вы можете получить консультацию по управлению защитой сети предприятия, внедрению приложения в сети или использованию его совместно с другими приложениями.

2.3. Обращение в Службу технической поддержки

Если вы уже приобрели приложение, вы можете получить информацию о нем от специалистов Службы технической поддержки по телефону или через интернет.

Специалисты Службы технической поддержки ответят на ваш вопрос по установке и использованию приложения и помогут устранить последствия работы вредоносных программ, если ваш компьютер уже был заражен.

Техническая поддержка по телефону

Если проблема срочная, вы всегда можете позвонить в Службу технической поддержки в нашем офисе в Москве по телефонам:

+7 (495) 797-87-07, **+7 (495) 645-79-29** или **+7 (495) 956-87-08**.

Мы оказываем техническую поддержку пользователям приложений «Лаборатории Касперского» круглосуточно, на русском и английском языках.

Если вы хотите поговорить со специалистом, который занимается именно приложением Антивирус Касперского 6.0 для Windows Servers Enterprise Edition, звоните в рабочие дни, с 10 до 18:30 часов по московскому времени (GMT +3).

Сообщите специалисту Службы технической поддержки **код активации** приложения или **серийный номер ключа** (вы можете посмотреть его узле **Ключи** консоли Антивируса, в свойствах установленного ключа).

Электронный запрос в Службу технической поддержки (для зарегистрированных пользователей)

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

Вы можете отправить свой запрос на русском, английском, немецком, французском или испанском языке.

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

Примечание

Если вы еще не являетесь зарегистрированным пользователем приложений «Лаборатории Касперского», вы можете заполнить регистрационную форму на странице:

https://support.kaspersky.com/ru/PersonalCabinet/Registration/Form/.

При регистрации укажите **код активации** приложения или **серийный номер ключа** (вы можете посмотреть его узле **Ключи** консоли Антивируса, в свойствах установленного ключа).

Вы получите ответ на свой запрос от специалиста Службы технической поддержки по электронному адресу, который вы укажете в нем, и в своем **Персональном кабинете**

https://support.kaspersky.com/ru/PersonalCabinet.

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

- **Тип запроса**. Вопросы, которые пользователи задают наиболее часто, выделены в отдельные темы, например, «Проблема установки/удаления продукта» или «Проблема поиска/удаления вирусов». Если вы не найдете подходящей темы, выберите «Общий вопрос».
- **Название продукта**: Антивирус Касперского 6.0 для Windows Servers Enterprise Edition.
- **Текст запроса**. Опишите как можно подробнее возникшую проблему.
- **Номер клиента и пароль**. Введите номер клиента и пароль, которые вы получили при регистрации на веб-сайте Службы технической поддержки.
- **Электронный адрес**. По этому адресу специалисты Службы технической поддержки перешлют ответ на ваш запрос.

2.4. Обсуждение приложений «Лаборатории Касперского» на веб-форуме

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

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

Вы можете, например, обсудить различные схемы внедрения приложения в организации или варианты его настройки.

ГЛАВА 3. ОБЩАЯ ИНФОРМАЦИЯ

В этой главе содержатся следующие сведения:

- требования к защищаемому серверу для установки Антивируса (см. п. 3.1 на стр. 14);
- требования к компьютеру, с которого будет осуществляться управление Антивирусом через консоль в MMC (см. п. 3.2 на стр. 17);
- состав комплекта поставки (см. п. 3.3 на стр. 19);
- описание программных компонентов Антивируса и их коды для службы Windows Installer. Вы можете использовать коды программных компонентов, чтобы изменить набор устанавливаемых компонентов при установке Антивируса из командной строки (см. п. 3.4 на стр. 21);
- параметры установки и удаления, их значения по умолчанию и ключи, которые вы можете использовать для задания параметров при установке или удалении Антивируса из командной строки (см. п. 3.5 на стр. 24);
- местоположение и название файла журнала установки / удаления Антивируса (см. п. 3.6 на стр. 34);
- изменения в системе после установки Антивируса (см. п. 3.7 на стр. 34);
- процессы Антивируса (см. п. 3.8 на стр. 39).

3.1. Требования к защищаемому серверу

В этом разделе приводятся аппаратные и программные требования к защищаемому серверу.

Примечание

Перед установкой Антивируса удалите с защищаемого сервера другие антивирусные приложения, включая Антивирус Касперского 5.0 для Windows Servers и Антивирус Касперского 6.0 для Windows Servers.

Аппаратные требования защищаемому серверу

Общие требования:

- x86-совместимые системы в однопроцессорной и многопроцессорной конфигурации (например, Intel Xeon Processor и Intel Xeon Processor MP with Hyper Threading); x86-64-совместимые системы в однопроцессорной и многопроцессорной конфигурации (например, Intel Xeon Processor и Intel Xeon Processor MP with EM64T и Hyper Threading);
- дисковое пространство:
  - для установки всех программных компонентов – 70 МБ;
  - для хранения объектов на карантине и в резервном хранилище – 400 МБ (рекомендуется);
  - для хранения отчетов – 100 МБ (рекомендуется).

Минимальная конфигурация:

- процессор Intel Pentium II с частотой 400 МГц или выше;
- объем оперативной памяти – 256 МБ.

Рекомендуемая конфигурация:

- процессор Intel Xeon с частотой 3,2 ГГц или выше;
- объем оперативной памяти – 1-2 ГБ.

Программные требования к защищаемому серверу

Вы можете установить Антивирус на сервере под управлением операционной системы Microsoft Windows 32-разрядной или 64-разрядной версии.

На сервере должна быть установлена одна из следующих 32-разрядных версий Microsoft Windows:

- Microsoft Windows 2000 Server с накопительным пакетом обновлений 1 к пакету обновлений 4 (Service Pack 4 + Rollup 1);
- Microsoft Windows 2000 Advanced Server с накопительным пакетом обновлений 1 к пакету обновлений 4 (Service Pack 4 + Rollup 1);

- Microsoft Windows Server 2003 Standard Edition с пакетом обновлений 1 или выше;
- Microsoft Windows Server 2003 Enterprise Edition с пакетом обновлений 1 или выше;
- Microsoft Windows Server 2003 Datacenter Edition с пакетом обновлений 1 или выше;
- Microsoft Windows Server 2003 R2 Standard Edition или выше;
- Microsoft Windows Server 2003 R2 Enterprise Edition или выше;
- Microsoft Windows Server 2003 R2 Datacenter Edition или выше;
- Microsoft Windows Storage Server 2003 R2 или выше;
- Microsoft Windows Server 2008 Standard Edition;
- Microsoft Windows Server 2008 Enterprise Edition;
- Microsoft Windows Server 2008 Datacenter Edition.

Для установки и работы Антивируса на компьютере под управлением Microsoft Windows 32-разрядной версии требуется наличие Microsoft Windows Installer 3.1.

Или на сервере должна быть установлена одна из следующих 64-разрядных версий Microsoft Windows:

- Microsoft Windows Server 2003 x64 Standard Edition;
- Microsoft Windows Server 2003 x64 Enterprise Edition;
- Microsoft Windows Server 2003 x64 Datacenter Edition;
- Microsoft Windows Server 2003 R2 Standard x64 Edition;
- Microsoft Windows Server 2003 R2 Enterprise x64 Edition;
- Microsoft Windows Server 2003 R2 Datacenter x64 Edition;
- Microsoft Windows Server 2008 x64 Standard Edition;
- Microsoft Windows Server 2008 x64 Enterprise Edition;
- Microsoft Windows Server 2008 x64 Datacenter Edition.

Для установки и работы Антивируса на компьютере под управлением Microsoft Windows 64-разрядной версии требуется наличие Microsoft Windows Installer 3.1.

Вы можете установить Антивирус на следующих терминальных серверах:

- Microsoft Terminal на базе Windows 2008 Server;

- Microsoft Terminal на базе Windows 2003 Server;
- Microsoft Terminal на базе Windows 2000 Server;
- Citrix Metaframe XPe FR 3;
- Citrix Presentation Server 3.0;
- Citrix Presentation Server 4.0;
- Citrix Presentation Server 4.5.

3.2. Требования к компьютеру, с которого будет осуществляться управление Антивирусом через консоль в ММС

В этом разделе перечислены аппаратные и программные требования к компьютеру для установки набора компонентов «Средства администрирования» (содержит консоль Антивируса в ММС).

Аппаратные требования

Рекомендуемый объем оперативной памяти – 128 МБ или более

Свободное дисковое пространство – 30 МБ.

Программные требования

На компьютере должна быть установлена одна из следующих 32-разрядных версий Microsoft Windows:

- Microsoft Windows 2000 Server с пакетом обновлений 4;
- Microsoft Windows 2000 Advanced Server с пакетом обновлений 4;
- Microsoft Windows Server 2003 Standard Edition с пакетом обновлений 1 или выше;
- Microsoft Windows Server 2003 Enterprise Edition с пакетом обновлений 1 или выше;
- Microsoft Windows Server 2003 Datacenter Edition с пакетом обновлений 1 или выше;

- Microsoft Windows Server 2003 R2 Standard Edition с пакетом обновлений 1 или выше;
- Microsoft Windows Server 2003 R2 Enterprise Edition с пакетом обновлений 1 или выше;
- Microsoft Windows Server 2003 R2 Datacenter Edition с пакетом обновлений 1 или выше;
- Microsoft Windows Server 2008 Standard Edition;
- Microsoft Windows Server 2008 Enterprise Edition;
- Microsoft Windows Server 2008 Datacenter Edition;
- Microsoft Windows 2000 Professional с пакетом обновлений 1 или выше;
- Microsoft Windows XP Professional, Microsoft Windows XP Professional с пакетом обновлений 1 или выше;
- Microsoft Windows Vista x86 Editions.

Для установки и работы Антивируса на компьютере под управлением Microsoft Windows 32-разрядной версии требуется наличие Microsoft Windows Installer 3.1, Microsoft Management Console версии 1.2 или выше.

Или на компьютере должна быть установлена одна из следующих 64-разрядных версий Microsoft Windows:

- Microsoft Windows Server 2003 x64 Standard Edition;
- Microsoft Windows Server 2003 x64 Enterprise Edition;
- Microsoft Windows Server 2003 x64 Datacenter Edition;
- Microsoft Windows Server 2003 R2 Standard x64 Edition;
- Microsoft Windows Server 2003 R2 Enterprise x64 Edition;
- Microsoft Windows Server 2003 R2 Datacenter x64 Edition;
- Microsoft Windows Server 2008 x64 Standard Edition;
- Microsoft Windows Server 2008 x64 Enterprise Edition;
- Microsoft Windows Server 2008 x64 Datacenter Edition;
- Microsoft Windows XP Professional x64 Edition, Microsoft Windows XP Professional x64 Edition с пакетом обновлений 1 или выше;
- Microsoft Windows Vista x64 Editions.

Для установки и работы Антивируса на компьютере под управлением Microsoft Windows 64-разрядной версии требуется наличие Microsoft Windows Installer 3.1.

3.3. Состав комплекта поставки

В комплект поставки входит приложение-приветствие, из окна которого вы можете запустить мастер установки Антивируса или его консоли в MMC, открыть руководство по установке Антивируса, страницу Антивируса на веб-сайте «Лаборатории Касперского», веб-сайт Службы технической поддержки.

Остальные файлы комплекта поставки хранятся в двух папках: x86\ и x64\. В папке x86\ помещаются файлы для установки Антивируса на сервере с 32-разрядной версией Microsoft Windows; в папке x64\ – для установки на сервере с 64-разрядной версией Microsoft Windows.

Каждая папка для установки Антивируса в Windows одной разрядности содержит вложенные папки server\ и client\:

- папка server\ содержит файлы для установки компонентов защиты Антивируса;
- папка client\ содержит файлы для установки консоли Антивируса в MMC (набор компонентов «Средства администрирования»).

Назначение файлов комплекта поставки Антивируса описано в следующей таблице.

Таблица 1. Файлы комплекта поставки Антивируса

Файл	**Назначение**
setup.exe	Файл запуска приложения-приветствия
setup\	В этой папке хранятся файлы приложения-приветствия.
kav6.0_wseeinstallguideru.pdf	«Руководство по установке» (этот документ)
kav6.0_wseeadminguide.pdf	«Руководство администратора»; документ Adobe Acrobat
kav6.0_wseecomparisonru.pdf	«Сравнение с Антивирусом Касперского 6.0 для Windows Servers»; документ Adobe Acrobat

Файл	Назначение
kav6.0_wseeappschemesru.pdf	«Типовые схемы применения»; документ Adobe Acrobat
autorun.inf	Файл автозапуска файла setup.exe
x86(x64)\server\setup.exe	Мастер установки Антивируса на защищаемом сервере; запускает файл инсталляционного пакета kavws.msi с указанными в мастере параметрами установки.
x86(x64)\server\kavws.msi	Инсталляционный пакет службы Windows Installer; устанавливает Антивирус на защищаемом сервере.
x86(x64)\server\kavws.kpd	Файл с описанием инсталляционного пакета для удаленной установки Антивируса через Kaspersky Administration Kit; имеет расширение .kpd (Kaspersky Package Definition). Этот файл содержит название инсталляционного пакета, общую информацию об Антивирусе (номер версии и дату выпуска) и описание кодов возврата программы установки. Этот файл может также содержать ключи командной строки, которые изменяют параметры установки в msi-файле инсталляционного пакета.
x86(x64)\server\release_notes.txt	Файл «Release Notes»
x86(x64)\client\setup.exe	Мастер установки набора компонентов «Средства администрирования» (в него входит консоль Антивируса в MMC); запускает файл инсталляционного пакета kavwstools.msi с указанными в мастере параметрами установки.
x86(x64)\client\kavwstools.msi	Инсталляционный пакет службы Windows Installer; устанавливает на компьютере консоль Антивируса в MMC для управления Антивирусом.
x86(x64)\client\release_notes_tools.txt	Файл «Release Notes» для набора компонентов «Средства администрирования»

Файл	Назначение
x86(x64) \plugin\klcfginst.exe	Программа установки плагина управления Антивирусом через Kaspersky Administration Kit. Установите плагин на каждый компьютер, на котором установлена Консоль администрирования Kaspersky Administration Kit, если вы планируете управлять Антивирусом через нее.
x86\plugin\release_notes.txt	Файл «Release Notes» для плагина управления Антивирусом через Kaspersky Administration Kit
x86\MSI\WindowsInstaller-KB893803-v2-x86.exe	Мастер установки Microsoft Windows Installer 3.1 v2 Redistributable. Если служба Windows Installer отсутствует на компьютере или установлена служба Windows Installer ранней версии, установите Windows Installer 3.1 перед установкой Антивируса (консоли Антивируса в MMC).

Примечание

Вы можете запускать файлы комплекта поставки с установочного компакт-диска. Если вы предварительно скопировали файлы на локальный диск, убедитесь, что сохранена структура файлов комплекта поставки.

3.4. Программные компоненты Антивируса и их коды для службы Windows Installer

По умолчанию файл \server\kavws.msi устанавливает все программные компоненты Антивируса (см. п. 3.4.1 на стр. 22); файл \client\kavwstools.msi устанавливает все программные компоненты набора «Средства администрирования» (см. п. 3.4.2 на стр. 23).

В следующих пунктах приводятся коды программных компонентов для службы Windows Installer. Вы можете использовать эти коды, чтобы задать список устанавливаемых компонентов при установке Антивируса из командной строки.

3.4.1. Программные компоненты Антивируса

В таблице 2 содержатся коды и описание программных компонентов Антивируса.

Таблица 2. Описание программных компонентов Антивируса

Компонент	Код	Выполняет функции
Антивирус Касперского 6.0	Core	Устанавливает системные файлы Антивируса и файлы, реализующие задачи проверки по требованию (однократная полная или выборочная проверка объектов файловой системы сервера на наличие угроз). Если, устанавливая Антивирус из командной строки, вы укажете другие компоненты Антивируса, не указывая компонент Core, компонент Core будет установлен автоматически.
Постоянная защита файлов	Oas	Реализует задачу **Постоянная защита файлов** (проверка объектов защищаемого сервера при доступе к ним) и функцию **Блокирование доступа с компьютеров**.
Проверка скриптов	ScriptChecker	Реализует задачу **Проверка скриптов** (проверка программного кода скриптов, созданных по технологиям Microsoft Windows Script Technologies, при попытке их выполнения).
Модуль интеграции с Агентом администрирования Kaspersky Administration Kit	AKIntegration	Обеспечивает связь Антивируса с Агентом администрирования Kaspersky Administration Kit. Установите этот компонент на защищаемом сервере, если вы планируете управлять Антивирусом через Kaspersky Administration Kit.

Компонент	Код	Выполняет функции
Набор счетчиков производительности приложения «Системный монитор»	PerfMonCounters	Устанавливает набор счетчиков производительности приложения «Системный монитор». Эти счетчики позволяют измерять производительность Антивируса и локализовать возможные узкие места на сервере при совместной работе Антивируса с другими приложениями.
Поддержка SNMP-протокола	SnmpSupport	Публикует счетчики и ловушки Антивируса через службу Simple Network Management Protocol (SNMP) Microsoft Windows. Вы можете установить этот компонент на защищаемом сервере, только если Служба Microsoft SNMP установлена на сервере.
Приложение панели задач	TrayApp	Отображает значок Антивируса в области уведомлений панели задач защищаемого сервера. Значок Антивируса показывает состояние постоянной защиты сервера, позволяет открыть консоль Антивируса в MMC (если установлена), окно **О программе**.
Утилита командной строки	Shell	Позволяет управлять Антивирусом из командной строки защищаемого сервера.

3.4.2. Программные компоненты набора *Средства администрирования*

В таблице 3 содержатся коды и описание программных компонентов набора «Средства администрирования».

Таблица 3. Описание программных компонентов средств администрирования

Компонент	Код	Выполняет функции
Оснастка Антивируса в MMC	Core	Устанавливает оснастку для управления Антивирусом через консоль MMC; msc-файл консоли Антивируса сохраняется в папке с файлами Антивируса. Если, устанавливая набор «Средства администрирования» из командной строки, вы укажете другие компоненты набора, не указывая компонент Core, компонент Core будет установлен автоматически.
Справка	Help	chm-файл справки; сохраняется в папке с файлами Антивируса. Вы можете открыть файл справки из меню **Пуск**.
Документация	Docs	Документы Adobe Acrobat «Руководство администратора» и «Руководство по установке»; сохраняются в папке Антивируса; вы можете открыть их из меню **Пуск**.

3.5. Параметры установки и удаления и их ключи для службы Windows Installer

В следующих таблицах описаны параметры установки и удаления Антивируса и их значения по умолчанию, указаны специальные ключи для изменения значений параметров установки и их возможные значения. Вы можете использовать эти ключи вместе со стандартными ключами команды msiexec службы Windows Installer при установке Антивируса из командной строки.

Таблица 4. Параметры установки и их ключи в Windows Installer

Параметр	**Значение по умолчанию**	**Ключ Windows Installer и его значения**	**Описание**
Проверка активных процессов и загрузочных секторов локальных дисков перед установкой (**Проверить компьютер на вирусы**)	Не выполнять проверку	PRESCAN=<значение> **0** – не выполнять проверку перед установкой (по умолчанию); **1** – выполнять проверку перед установкой.	Рекомендуется выполнить проверку активных процессов и загрузочных секторов локальных дисков перед установкой, поскольку наличие вредоносного кода в этих областях компьютера может помешать успешной установке Антивируса. Проверка может занять несколько минут. Если во время проверки будут обнаружены зараженные или подозрительные процессы, они будут удалены из памяти компьютера (исполняемые файлы процессов не удаляются). В этом случае информация в работающих приложениях может быть потеряна. Поэтому рекомендуется перед началом установки закрыть все работающие приложения.

Параметр	Значение по умолчанию	Ключ Windows Installer и его значения	Описание
Папка назначения	Антивирус: %Program-Files%\Kaspersky Lab\Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition\ * Средства администрирования: %Program-Files%\Kaspersky Lab\Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition Admins Tools\ * * В Microsoft Windows 64-разрядной версии папка называется %ProgramFiles(x86)%	INSTALLDIR=<полный путь к папке>	Папка, в которой будут сохранены файлы Антивируса при его установке. Вы можете указать другую папку.

Параметр	**Значение по умолчанию**	**Ключ Windows Installer и его значения**	**Описание**
Запуск постоянной защиты файлов и проверки скриптов при запуске Антивируса (**Включить постоянную защиту после установки**)	Запустить	RUNRTP=<значение> **1** – запустить; **0** – не запускать.	Включите этот параметр, чтобы запустить постоянную защиту файлов и проверку скриптов при запуске Антивируса (рекомендуется).

Параметр	Значение по умолчанию	Ключ Windows Installer и его значения	Описание
Исключения из проверки, рекомендуемые корпорацией Майкрософт (**Добавить к исключениям файлы, рекомендованные Microsoft**)	Исключать	ADDMSEXCLUSION=<значение> **1** – исключать; **0** – не исключать.	В задаче **Постоянная защита файлов** исключает из области защиты объекты на сервере, которые рекомендует исключать корпорация Майкрософт. Некоторые программы на сервере могут работать нестабильно, когда антивирусное приложение перехватывает или изменяет файлы, к которым эти приложения обращаются. К таким программам корпорация Майкрософт относит, например, некоторые приложения контроллеров доменов. Майкрософт рекомендует исключать из постоянной защиты файлы этих приложений как неподверженные заражению. Вы можете просмотреть список этих файлов на веб-узле корпорации Майкрософт www.microsoft.com/rus/, код статьи: KB822158.

Параметр	Значение по умолчанию	Ключ Windows Installer и его значения	Описание
Исключение из обработки программ удаленного администрирования (**Добавить к исключениям угрозы по маске not-a-virus:RemoteAdmin***)	Не добавлять к исключениям угрозы по маске not-a-virus:RemoteAdmin*	RADMINEXCLUSION=<значение> **1 – добавить к исключениям угрозы по маске not-a-virus:RemoteAdmin***. Антивирус не будет выполнять никаких действий над объектами, содержащими угрозы с маской названия not-a-virus:RemoteAdmin*: **0 – не добавлять к исключениям угрозы по маске not-a-virus:RemoteAdmin***. Антивирус будет выполнять действия над объектами, содержащими угрозы с маской названия not-a-virus:RemoteAdmin*.	Антивирус, как и большинство других антивирусных приложений, относит код утилит удаленного администрирования Remote Administrator к потенциально опасным программам. Когда вы запускаете утилиту Remote Administrator, Антивирус обнаруживает в ней угрозу и удаляет с диска сервера ее исполняемый модуль. Антивирус присваивает угрозе в этих утилитах название not-a-virus:RemoteAdmin*. Если вы планируете использовать утилиты удаленного администрирования после установки Антивируса, вы можете исключить указанную угрозу из обработки Антивирусом с помощью параметра установки **Добавить к исключениям угрозы по маске not-a-virus:RemoteAdmin***. Вы можете исключить утилиты удаленного администрирования из обработки в задаче **Постоянная защита файлов** и задачах проверки по требованию и после установки Антивируса. Добавьте угрозу not-a-virus:RemoteAdmin* в доверенную зону Антивируса и примените доверенную зону в нужных задачах (см. документ «Антивирус Касперского 6.0 для Windows Servers Enterprise Edition. Руководство администратора»).

Параметр	Значение по умолчанию	Ключ Windows Installer и его значения	Описание
Путь к устанавливаемому ключу (**Ключ**)	Папка комплекта поставки \server\	LICENSEKEYPATH=<имя файла ключа и полный путь к нему> Если вы сохранили файл ключа в сетевой папке, укажите полный путь к файлу в формате UNC (Universal Naming Convention).	По умолчанию программа установки пытается найти файл ключа с расширением .key в папке server\ комплекта поставки. Если в папке \server\ хранится несколько файлов ключа, программа установки выбирает файл, ключ в котором имеет самую позднюю дату, после которой он становится недействительным. Вы можете предварительно сохранить файл ключа в папке \server\ или указать другой путь к файлу ключа с помощью параметра установки **Ключ**. Вы можете установить ключ не во время установки Антивируса, а после ее окончания с помощью выбранного вами средства администрирования, например, через консоль Антивируса в MMC. Однако обратите внимание, что, если, устанавливая Антивирус, вы выбрали **Включить постоянную защиту после установки**, но не указали файл ключа, Антивирус сразу после установки не начнет проверять объекты файловой системы сервера при доступе к ним. Подробнее о ключах Антивируса читайте в документе «Антивирус Касперского 6.0 для Windows Servers Enterprise Edition. Руководство администратора».

Параметр	**Значение по умолчанию**	**Ключ Windows Installer и его значения**	**Описание**
Путь к конфигурационному файлу	Не указан	CONFIGPATH=<имя конфигурационного файла и полный путь к нему>	Антивирус импортирует параметры из указанного ключом конфигурационного XML-файла, созданного в Антивирусе Касперского 6.0 для Windows Servers Enterprise Edition текущей версии, версии 6.0.0.454 или версии 6.0.1.511. Антивирус не импортирует из конфигурационного файла пароли, например, пароли учетных записей для запуска задач или пароли для соединения с прокси-сервером. После импорта параметров вам нужно ввести все пароли вручную. Если вы не укажете этот ключ, после установки Антивирус начнет работать с параметрами по умолчанию.

Параметр	Значение по умолчанию	Ключ Windows Installer и его значения	Описание
Разрешение сетевых соединений для консоли Антивируса Касперского	Выключен	ADDWFEXCLUSION=<значение> **1** – разрешать; **0** – не разрешать.	Используйте этот параметр, если вы устанавливаете консоль Антивируса в MMC (набор **Средства администрирования**) не на защищаемом сервере, а на другом компьютере, который работает под управлением Microsoft Windows XP с пакетом обновлений SP2 или под управлением Microsoft Windows Vista. С помощью этой консоли вы сможете управлять защитой сервера удаленно. В брандмауэре Microsoft Windows компьютера будет открыт TCP-порт 135, разрешены сетевые соединения для исполняемого файла процесса удаленного управления Антивирусом kavfsrcn.exe и открыт доступ к приложениям DCOM. После завершения установки добавьте пользователей, которые будут управлять Антивирусом удаленно, в группу **KAVWSEE Administrators** на сервере и, если сервер работает под управлением Microsoft Windows Server 2008, разрешите на нем сетевые соединения для службы управления Антивирусом Касперского (файл kavfsgt.exe). См. инструкции в п. 5.1.2.2 на стр. 70.

Таблица 5. Параметры удаления и их ключи в Windows Installer

Параметр	**Значение по умолчанию**	**Описание, ключи Windows Installer и их значения**
Восстановление содержимого карантина	Удалить	RESTOREQTN =<значение> **0** – удалить содержимое карантина; **1** – восстановить содержимое карантина в папку, указанную параметром RESTOREPATH
Восстановление содержимого резервного хранилища	Удалить	RESTOREBCK =<значение> **0** – удалить содержимое резервного хранилища; **1** – восстановить содержимое резервного хранилища в папку, указанную параметром RESTOREPATH
Папка для восстановленных объектов	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\Uninstall	RESTOREPATH=<полный путь к папке> Восстановленные объекты будут сохранены в папке, указанной этим параметром: Объекты из карантина будут сохранены во вложенной папке \Quarantine\. Объекты из резервного хранилища – во вложенной папке \Backup\.

3.6. Журнал установки и удаления Антивируса

Если вы выполняете установку или удаление Антивируса с помощью мастера установки / удаления (запускаете файл \server\setup.exe или \client\setup.exe), служба Windows Installer создает журнал установки (удаления) в режиме записи «полный вывод». Файл журнала с именем kav6wsee_install_<uid>.log" (где <uid> – уникальный восьмизначный идентификатор журнала) сохраняется в папке %temp% пользователя, с правами которого был запущен файл setup.exe.

Примечание

Если папка %temp% не определена для пользователя, с правами которого был запущен файл setup.exe, файл журнала не создается.

Если вы выполняете установку или удаление Антивируса из командной строки, то по умолчанию журнал установки не создается.

Чтобы выполнить установку Антивируса с созданием файла журнала kavws.log на диске C:\, выполните следующую команду:

```
msiexec /i kavws.msi /l*v C:\kavws.log /qn
```

3.7. Изменения в системе после установки Антивируса

При установке Антивируса и консоли Антивируса в MMC (набора «Средства администрирования») служба Windows Installer выполняет на компьютере следующие изменения:

- создает папки Антивируса на защищаемом сервере и компьютере, на котором установлена консоль Антивируса в MMC;
- регистрирует службы Антивируса;
- создает группу пользователей Антивируса;
- регистрирует ключи Антивируса в системном реестре.

Эти изменения описаны ниже.

Папки Антивируса

Таблица 6. Папки Антивируса на защищаемом сервере

Папка	Содержит
%Папка Антивируса%; по умолчанию: • в Microsoft Windows 32-разрядной версии – %Program-Files%\Kaspersky Lab\Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition\; • в Microsoft Windows 64-разрядной версии – %Program-Files(x86)%\Kaspersky Lab\Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition\	Исполняемые файлы Антивируса (папка назначения, указанная при установке)
%Папка Антивируса%**mibs**	Файлы Management Information Base (MIB); содержат описание счетчиков и ловушек, публикуемых Антивирусом по протоколу SMNP
%Папка Антивируса%**x64**	64-разрядные версии исполняемых файлов Антивируса (папка создается только при установке Антивируса в Microsoft Windows 64-разрядной версии)
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0**Data**\ %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0**Settings**\ %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0**Dskm**\	Служебные файлы Антивируса
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0**Update**\	Файлы с параметрами источников обновлений

Папка	Содержит
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0**Update\Distribution**\	Обновления баз и программных модулей, полученные с помощью задачи **Копирование обновлений** (папка создается при первом получении обновлений с помощью задачи **Копирование обновлений**)
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0**Reports**\	Отчеты о выполнении задач и журнал системного аудита
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0**Bases\Current**\	Набор баз, используемый в текущий момент
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0**Bases\Backup**\	Резервная копия баз; перезаписывается при каждом обновлении баз
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0\Bases**Temp**\	Временные файлы, создаваемые во время выполнения задач обновления
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0**Quarantine**\	Объекты на карантине (папка по умолчанию)
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0**Backup**\	Объекты в резервном хранилище (папка по умолчанию)
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\6.0**Restored**\	Объекты, восстановленные из резервного хранилища и карантина (папка для восстановленных объектов по умолчанию)

Таблица 7. Папки, создаваемые при установке консоли Антивируса в ММС

Папка	Содержит
%Папка Антивируса%; по умолчанию: • в Microsoft Windows 32-разрядной версии – %Program-Files%\Kaspersky Lab\Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition\; • в Microsoft Windows 64-разрядной версии – %Program-Files(x86)%\Kaspersky Lab\Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition\	Файлы набора «Средства администрирования» (папка назначения, указанная при установке консоли Антивируса в ММС);

Службы Антивируса

Все службы Антивируса кроме службы управления Антивирусом запускаются под учетной записью **Локальная система** (**System**) в Microsoft Windows всех версий. Служба управления Антивирусом в Microsoft Windows 2003 и выше (включая 64-разрядные версии) запускается под учетной записью **Сетевая служба** (**Network Service**).

Таблица 8. Службы Антивируса

Служба	Назначение
Служба Антивируса Касперского (Kaspersky Anti-Virus Service)	Основная служба Антивируса; управляет задачами и рабочими процессами Антивируса
Служба управления Антивирусом Касперского (Kaspersky Anti-Virus Management Service)	Служба управления Антивирусом через консоль в ММС
Служба диспетчера перехватов скриптов (Script Interceptor Dispatcher)	Служба проверки скриптов

Группы Антивируса

Таблица 9. Группы Антивируса

Группа	Назначение
KAVWSEE Administrators	Группа на защищаемом сервере, пользователи которой имеют полный доступ к Службе управления Антивирусом, а также доступ ко всем функциям Антивируса.

Ключи системного реестра

Таблица 10. Ключи системного реестра

Ключ	Назначение
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFS]	Параметры службы Антивируса Касперского
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Anti-Virus]	Параметры журнала событий Антивируса (Event Log)
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsscs]	Параметры службы диспетчера перехватов скриптов
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]	Параметры службы управления Антивирусом Касперского
В Microsoft Windows 32-разрядной версии: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Anti-Virus\Performance] В Microsoft Windows 64-разрядной версии: [[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Anti-Virus x64\Performance].	Параметры счетчиков производительности
В Microsoft Windows 32-разрядной версии: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\KAVFSEE\SnmpAgent] В Microsoft Windows 64-разрядной версии: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\KAVFSEE\SnmpAgent]	Параметры компонента «Поддержка SNMP-протокола»

Ключ	Назначение
В Microsoft Windows 32-разрядной версии: HKEY_LOCAL_MACHINE\Software\KasperskyLab\KAVFSEE\6.0\Trace\ В Microsoft Windows 64-разрядной версии: HKEY_LOCAL_MACHINE\Software\Wow6432Node\KasperskyLab\KAVFSEE\6.0\Trace\	Параметры журнала трассировки
В Microsoft Windows 32-разрядной версии: HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\KAVFSEE\6.0\CrashDump\ В Microsoft Windows 64-разрядной версии: HKEY_LOCAL_MACHINE\Software\Wow6432Node\KasperskyLab\KAVFSEE\6.0\CrashDump\	Параметры дампов

3.8. Процессы Антивируса

Антивирус запускает процессы, описанные в следующих таблицах.

Таблица 11. Процессы Антивируса

Имя файла	Назначение
kavfs.exe	Процесс службы Антивируса Касперского
kavfswp.exe	Рабочий процесс Антивируса
kavfsscs.exe	Процесс службы диспетчера перехватов скриптов
kavtray.exe	Процесс приложения панели задач
Kavfsgt.exe	Процесс службы управления Антивирусом Касперского
kavshell.exe	Процесс утилиты командной строки
kavfsrcn.exe	Процесс удаленного управления Антивирусом

ГЛАВА 4. ПЛАНИРОВАНИЕ УСТАНОВКИ

Перед тем как начать установку Антивируса, спланируйте ее, выполнив следующие шаги:

Таблица 12.Планирование установки

Шаг	Действие
Шаг 1	Определите, какие средства администрирования вы будете использовать для управления Антивирусом и его настройки (см. п. 4.1 на стр. 40).
Шаг 2	Определите, какие программные компоненты вам нужно установить (см. п. 3.4 на стр. 21).
Шаг 3	Выберите способ установки (см. п. 4.2 на стр. 41), а затем выполните установку Антивируса выбранным способом.

4.1. Выбор способа управления

Определите, какие средства администрирования вы будете использовать для управления Антивирусом и его настройки. В качестве средств администрирования Антивируса вы можете использовать консоль Антивируса в MMC, командную строку защищаемого сервера и приложение Kaspersky Administration Kit.

Консоль Антивируса в MMC

Консоль Антивируса в MMC представляет собой изолированную оснастку MMC. Вы можете управлять Антивирусом через консоль в MMC, установленную на защищаемом сервере или другом компьютере в сети.

Вы можете добавить в одну консоль Антивируса несколько экземпляров оснастки, чтобы управлять защитой нескольких серверов, на которых установлен Антивирус.

Консоль Антивируса в MMC входит в набор компонентов «Средства администрирования».

Командная строка защищаемого сервера

Вы можете управлять Антивирусом из командной строки защищаемого сервера.

Утилита командной строки входит в набор программных компонентов Антивируса.

Kaspersky Administration Kit

Если вы используете приложение Kaspersky Administration Kit для централизованного управления антивирусной защитой компьютеров в вашей организации, то вы можете управлять Антивирусом через Консоль администрирования Kaspersky Administration Kit.

Набор программных компонентов Антивируса включает компонент «Модуль интеграции с Агентом администрирования Kaspersky Administration Kit». Он обеспечивает связь Антивируса с Агентом администрирования (подробнее о программных компонентах Антивируса читайте в п. 3.4 на стр. 21). Установите Модуль интеграции с Агентом администрирования Kaspersky Administration Kit на защищаемом сервере.

На каждый защищаемый сервер установите Агент администрирования Kaspersky Administration Kit, который будет обеспечивать взаимодействие между Антивирусом на сервере и Сервером администрирования Kaspersky Administration Kit. Файл установки Агента администрирования входит в комплект поставки Kaspersky Administration Kit.

Дополнительно на компьютер, на котором установлена Консоль администрирования Kaspersky Administration Kit, установите плагин управления Антивирусом из Консоли администрирования. Он обеспечивает интерфейс управления Антивирусом через Kaspersky Administration Kit. Файл установки плагина, \plugin\klcfginst.exe, входит в комплект поставки Антивируса.

4.2. Выбор способа установки

Вы определили, какие программные компоненты вам нужно установить (см. п. 3.4 на стр. 21).

Теперь выберите способ установки в зависимости от того,

- какова архитектура сети;
- потребуется ли вам задать специальные параметры установки Антивируса или вы будете использовать параметры установки по умолчанию;

- будут ли параметры установки едиными для всех серверов или индивидуальными для каждого сервера.

Список параметров установки по умолчанию приводится в п. 3.5 на стр. 24.

Вы можете установить Антивирус как с помощью мастера установки, так и с помощью запуска из командной строки *msi*-файла инсталляционного пакета. Вы можете выполнить централизованную удаленную установку Антивируса через групповые политики Active Directory или с помощью задачи удаленной установки Kaspersky Administration Kit.

Запуск мастера установки

С помощью мастера установки вы можете установить:

- из файла \server\setup.exe комплекта поставки – программные компоненты Антивируса на каждом сервере, который вы хотите защищать (см. п. 5.1.1 на стр. 45);
- из файла \client\setup.exe – средства администрирования (консоль Антивируса в MMC) на компьютере, с которого вы хотите управлять Антивирусом (защищаемом сервере или другом компьютере в сети). См. п. 5.1.2 на стр. 60.

Вы должны входить в группу локальных администраторов на компьютере, на котором вы устанавливаете Антивирус.

Запуск msi-файла инсталляционного пакета из командной строки

По умолчанию файл \server\kavws.msi устанавливает все программные компоненты Антивируса на защищаемом сервере. Вы можете изменить список устанавливаемых компонентов и другие параметры установки с помощью стандартных ключей команды msiexec службы Windows Installer и специальных ключей Антивируса. Подготовив набор ключей для одного сервера, вы можете применить его на всех серверах, на которых вы хотите установить Антивирус с одинаковыми параметрами установки.

Вы можете установить консоль Антивируса в MMC на защищаемом сервере и / или рабочем месте администратора, выполнив файл \client\kavwstools.msi из командной строки этого компьютера.

Глава 6 на стр. 92 содержит примеры команд для установки Антивируса и консоли Антивируса в MMC.

Вы должны входить в группу локальных администраторов на компьютере, на котором вы выполняете установку из командной строки.

Централизованная установка через Kaspersky Administration Kit

Если вы используете приложение Kaspersky Administration Kit для управления антивирусной защитой компьютеров сети, вы можете установить Антивирус на нескольких серверах с помощью задачи удаленной установки Kaspersky Administration Kit.

Серверы, на которые хотите установить Антивирус через Kaspersky Administration Kit, могут находиться как в одном домене с Сервером администрирования, так и в другом домене, или вообще не принадлежать ни к одному домену.

Вы можете выполнить установку как при старте сервера, так и «на работающей системе», то есть без необходимости предварительно перезагружать сервер или выполнять вход в Microsoft Windows.

Глава 7 на стр. 98 содержит информацию о том, какими правами вы должны обладать, чтобы установить Антивирус таким способом, и как выполнить установку.

Централизованная установка через групповые политики Active Directory

Серверы, на которых вы устанавливаете Антивирус через групповые политики Active Directory, должны находиться в одном домене и в одной организационной единице. Установка выполняется при запуске сервера, перед входом в Microsoft Windows.

С помощью групповой политики Active Directory вы можете установить Антивирус на защищаемом сервере только с параметрами установки по умолчанию. Вы также можете установить консоль Антивируса на рабочем месте администратора.

Вы должны обладать правами администратора на контроллере домена, с которого вы планируете установить Антивирус. Вам не нужно регистрировать свою учетную запись на каждом из серверов.

Установку через групповые политики Active Directory описывает Глава 8 на стр. 112.

ГЛАВА 5. УСТАНОВКА И УДАЛЕНИЕ АНТИВИРУСА С ПОМОЩЬЮ МАСТЕРА УСТАНОВКИ / УДАЛЕНИЯ

В этой главе содержится следующая информация:

- установка Антивируса, установка консоли Антивируса в MMC (см. п. 5.1 на стр. 44);
- добавление или удаление компонентов, восстановление Антивируса (см. п. 5.2 на стр. 82);
- удаление Антивируса, удаление консоли Антивируса в MMC (см. п. 5.3 на стр. 86).

5.1. Установка с помощью мастера установки

В следующих разделах содержится информация о том, как установить Антивирус и консоль Антивируса в MMC и выполнить через консоль действия, рекомендованные после установки Антивируса. Выполните следующие шаги:

Таблица 13. Установка с помощью мастера установки

Шаг	Действие
Шаг 1	Установите Антивирус на каждом сервере, который вы хотите защищать (см. п. 5.1.1 на стр. 45).
Шаг 2	Установите средства администрирования (консоль Антивируса в MMC) на компьютерах, с которых вы планируете управлять Антивирусом (см. п. 5.1.2 на стр. 60);
Шаг 3	Выполните действия после установки Антивируса (см. п. 5.1.3 на стр. 76).

5.1.1. Установка Антивируса на защищаемом сервере

Перед установкой Антивируса выполните следующие действия:

- Убедитесь, что на сервере не установлены другие антивирусные приложения.
- Убедитесь, что у вас достаточно прав для установки Антивируса. Чтобы установить Антивирус, вы должны входить в группу локальных администраторов на компьютере, на котором вы запускаете мастер установки.

После того как вы выполните эти предварительные действия, перейдите к процедуре установки.

Чтобы установить Антивирус:

1. На компьютере, на котором вы хотите установить Антивирус, запустите файл приложения-приветствия setup.exe.

> **Примечание**:
>
> Вы можете запустить файл приложения-приветствия с установочного компакт-диска. Если вы предварительно скопировали файлы комплекта поставки на локальный диск, убедитесь, что сохранена структура файлов комплекта поставки.

2. В окне приложения-приветствия (см. рис. 1) щелкните на ссылке **Антивирус Касперского**.

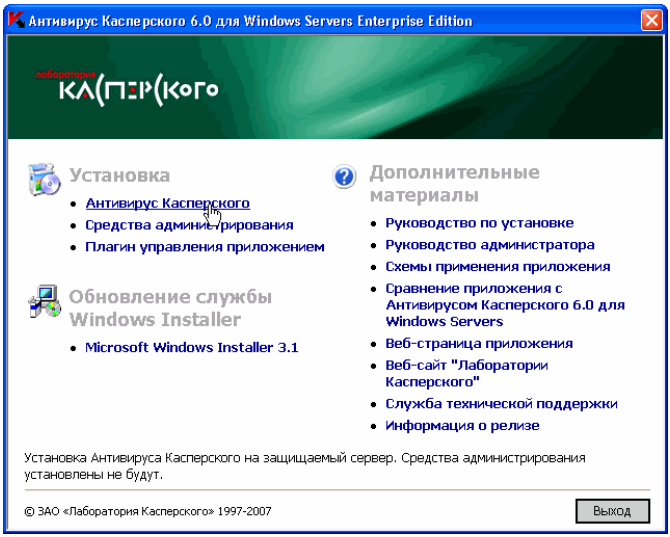

Рисунок 1. Окно приложения-приветствия

Откроется мастер установки Антивируса. Следуя его инструкциям, задайте параметры установки Антивируса. Описание параметров установки содержится в п. 3.5 на стр. 24.

Вы можете прервать установку Антивируса на любом шаге мастера установки. Для этого в окне мастера установки нажмите на кнопку **Отмена**.

3. В окне приветствия мастера установки (см. рис. 2) нажмите на кнопку **Далее**.

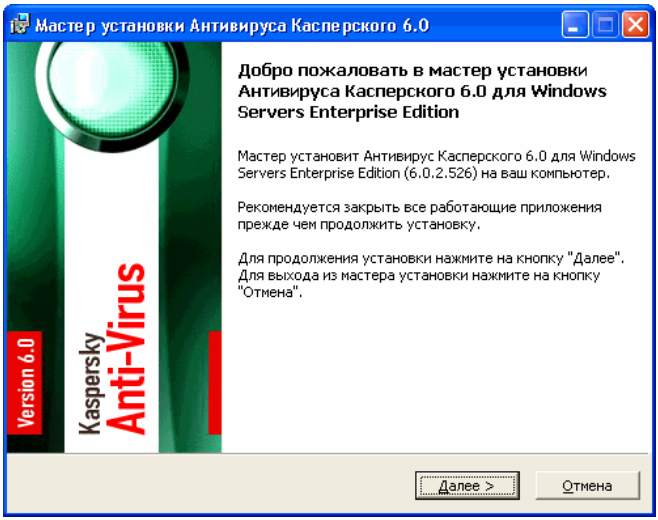

Рисунок 2. Окно приветствия мастера установки

4. В окне **Лицензионное соглашение** (см. рис. 3) ознакомьтесь с условиями лицензионного соглашения и установите флажок **Я принимаю условия лицензионного соглашения**, чтобы продолжить установку.

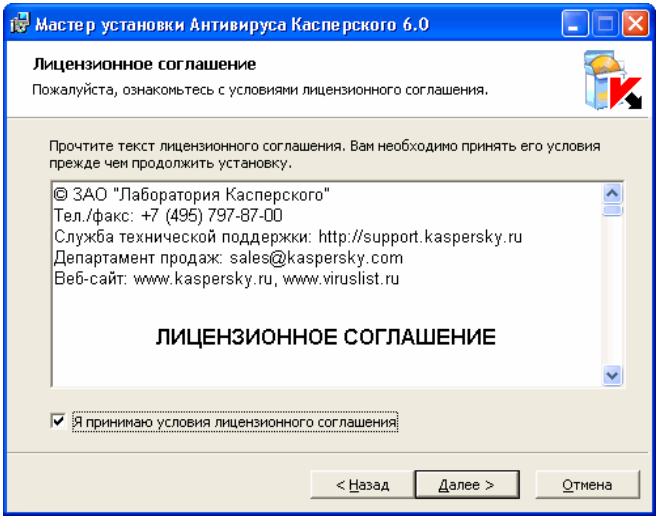

Рисунок 3. Окно **Лицензионное соглашение**

5. В окне **Антивирусная проверка перед установкой** (см. рис. 4), установите флажок **Проверить компьютер на вирусы**, чтобы проверить на наличие вирусов активные процессы и загрузочные секторы локальных дисков сервера (подробнее об этом параметре читайте в таблице 4 на стр. 25).

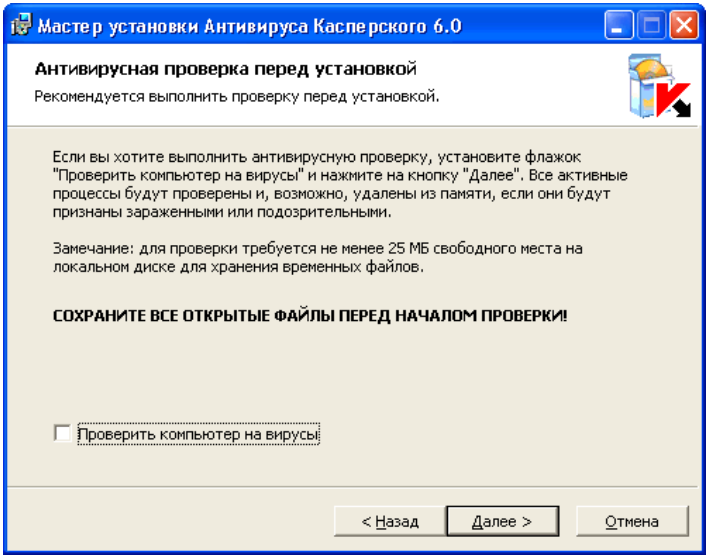

Рисунок 4. Окно **Антивирусная проверка перед установкой**

Чтобы прервать проверку, в окне **Выполняется проверка** нажмите на кнопку **Остановить**.

6. Если на предыдущем шаге вы выбрали **Проверить компьютер на вирусы**, по окончании проверки откроется окно с результатами антивирусной проверки (см. рис. 5). В нем вы можете просмотреть информацию о проверенных объектах сервера: общее количество проверенных объектов, количество обнаруженных типов угроз, количество обнаруженных зараженных и подозрительных объектов, количество зараженных или подозрительных процессов, которые Антивирус удалил из памяти, и количество зараженных или подозрительных процессов, которые Антивирусу не удалось удалить.

   Чтобы посмотреть, какие именно объекты были проверены, нажмите на кнопку **Список обработанных объектов**.

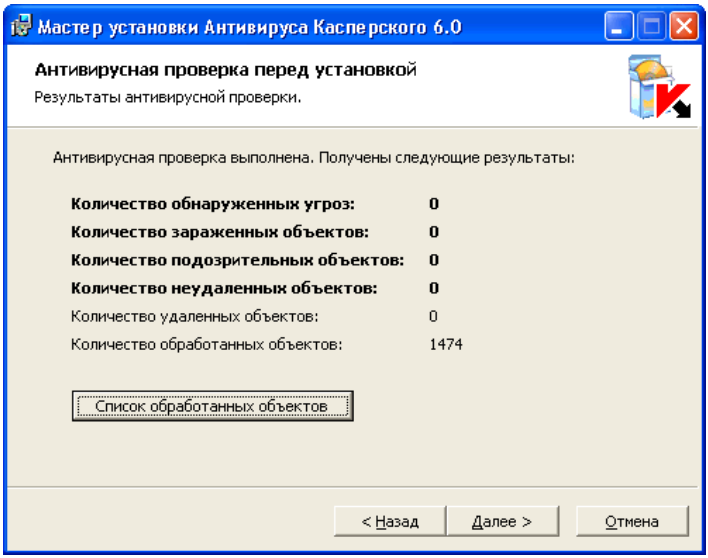

Рисунок 5. Окно результатов антивирусной проверки

7. В окне **Тип установки** (см. рис. 6) выберите один из следующих вариантов:

   - **Полная установка на сервер**, чтобы установить на сервер все программные компоненты Антивируса.

> **Примечание**
>
> Компонент **Поддержка SNMP-протокола** будет установлен на защищаемом сервере, только если на сервере установлена Служба SNMP Microsoft Windows.

- **Выборочная установка**, чтобы вручную выбрать компоненты из списка программных компонентов Антивируса (см. описание компонентов Антивируса в п. 3.4 на стр. 21).

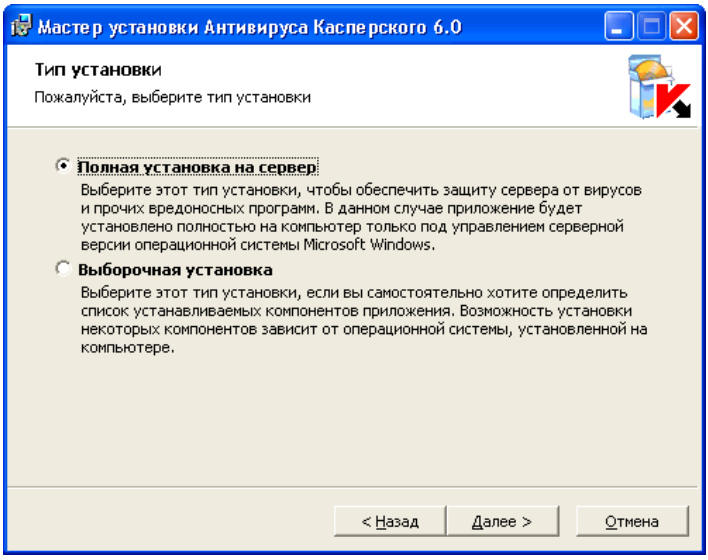

Рисунок 6. Окно **Тип установки**

Если компьютер не соответствует программным требованиям для установки компонентов Антивируса, мастер установки прекратит работу. Список программных требований приводится в п. 3.1 на стр. 14.

Если вы выбрали тип установки **Полная установка на сервер**, мастер установки проверит наличие на сервере программ, несовместимых с Антивирусом. Если мастер установки обнаружит несовместимую программу, он прекратит установку Антивируса. На экране появится сообщение, которое будет содержать список установленных на сервере несовместимых программ.

Если вы выбрали тип установки **Полная установка на сервер**, перейдите к шагу 9.

Если вы выбрали тип установки **Выборочная установка**, откроется окно **Выборочная установка** (см. рис. 7).

8. По умолчанию в окне отображаются все компоненты Антивируса (см. описание компонентов в п. 3.4 на стр. 21). Они включены в список устанавливаемых. Чтобы исключить компонент из списка, щелкните на компоненте и выберите ✕. Чтобы установить компо-

нент, щелкните на компоненте и выберите . Чтобы установить компонент и все его подкомпоненты, щелкните на компоненте и выберите .

Примечание

Вы можете исключить из списка компонент **Проверка по требованию** только вместе с набором компонентов **Антивирус Касперского 6.0**.

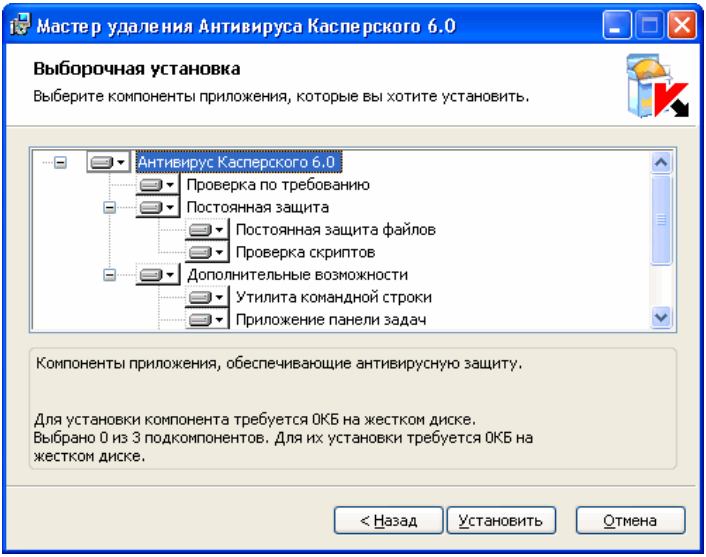

Рисунок 7. Окно **Выборочная установка**

Примечание

Вы можете установить компонент **Поддержка SNMP-протокола** Антивируса, только если на сервере установлена Служба SNMP Microsoft Windows. Если Служба SNMP на защищаемом сервере не установлена, компонент **Поддержка SNMP-протокола** Антивируса не отображается в списке программных компонентов в диалоговом окне **Выборочная установка**.

Чтобы отменить все изменения в окне **Выборочная установка**, нажмите на кнопку **Сбросить**. После того как вы укажете состав компонентов, нажмите на кнопку **Далее**.

Мастер установки проверит наличие на сервере программ, несовместимых с Антивирусом. Если он обнаружит несовместимую про-

грамму, то прекратит установку Антивируса. На экране появится сообщение, которое будет содержать список установленных на сервере несовместимых программ.

9. В окне **Выбор папки назначения** (см. рис. 8), если требуется, укажите другую папку, в которой будут сохранены файлы Антивируса (подробнее о параметре читайте в таблице 4 на стр. 25).

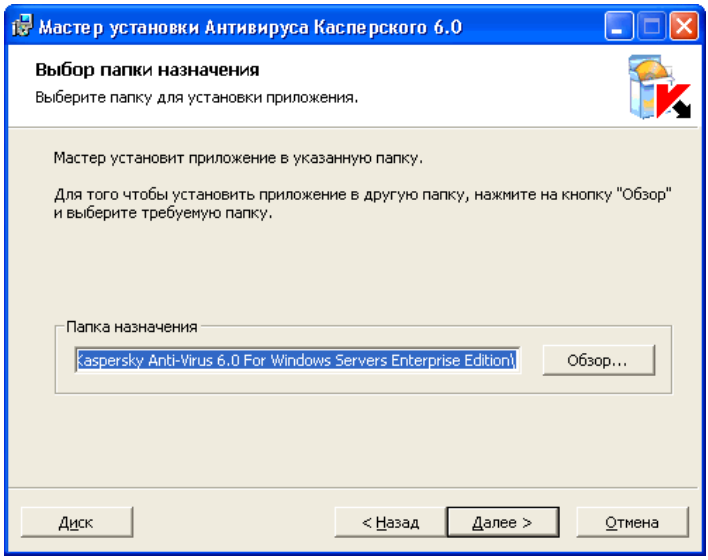

Рисунок 8. Окно **Выбор папки назначения**

После того как вы укажете папку на каком-либо из дисков компьютера, вы можете посмотреть, позволит ли размер свободного пространства на этом диске установить выбранные вами компоненты. Для этого нажмите на кнопку **Диск**.

Откроется окно **Доступное дисковое пространство** (см. рис. 9). В нем вы можете просмотреть доступный объем памяти на диске, на котором вы хотите установить выбранные компоненты Антивируса (**Доступно на диске**), а также объем памяти, требуемый для установки компонентов (**Требуется на диске**).

В окне **Доступное дисковое пространство** нажмите на кнопку **ОК**, чтобы закрыть его.

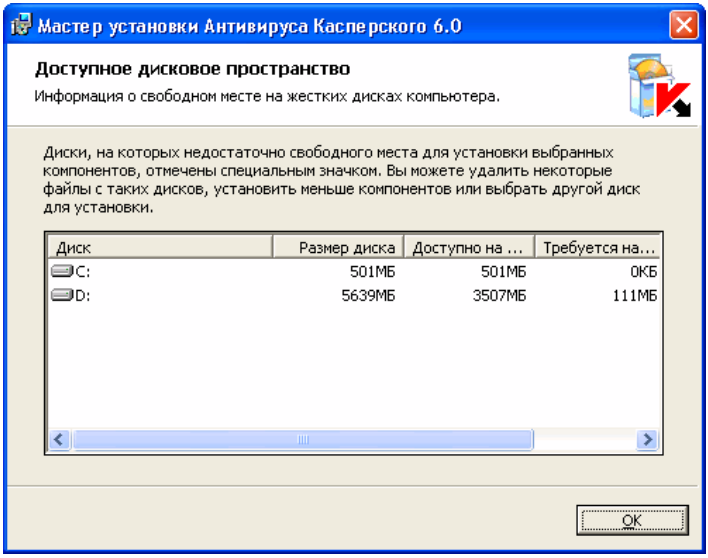

Рисунок 9. Окно **Доступное дисковое пространство**

Если места на выбранном диске недостаточно, освободите место на этом диске или в окне **Выбор папки назначения** укажите папку для файлов Антивируса на другом диске сервера.

10. В окне **Дополнительные параметры установки** (см. рис. 10) выберите:

    - включить / не включать постоянную защиту файлов и проверку скриптов после установки;
    - исключить / не исключать из области защиты объекты на сервере, которые рекомендует исключать корпорация Майкрософт.
    - добавить / не добавлять в список правил исключений доверенной зоны угрозы по маске not-a-virus:RemoteAdmin*.

Подробнее об этих параметрах установки читайте в таблице 4 на стр. 25.

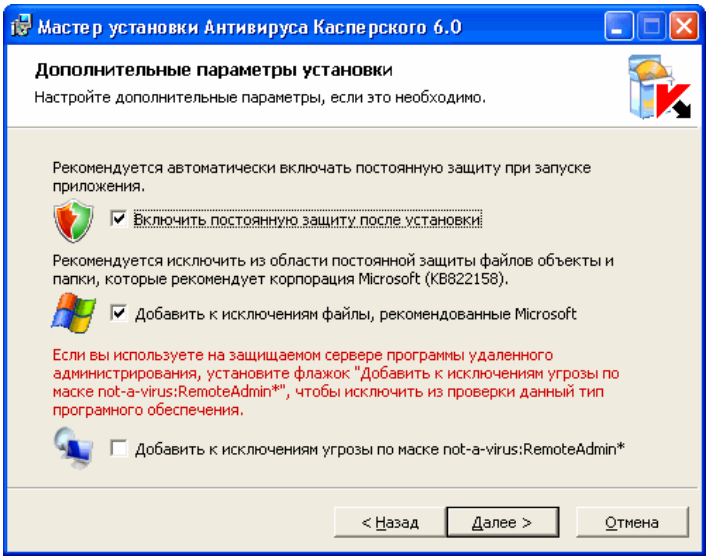

Рисунок 10. Окно **Дополнительные параметры установки**

11. Если вы хотите импортировать параметры Антивируса из существующего конфигурационного XML-файла, созданного в Антивирусе Касперского 6.0 для Windows Servers Enterprise Edition текущей версии, версии 6.0.0.454 или версии 6.0.1.511, укажите конфигурационный файл в окне **Импорт параметров из конфигурационного файла** (см. рис. 11).

    Подробнее о параметре читайте в таблице 4 на стр. 25.

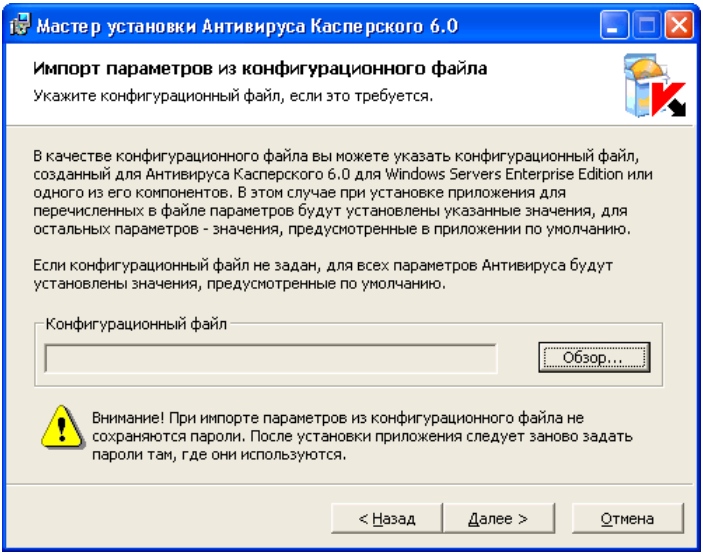

Рисунок 11. Окно **Импорт параметров из конфигурационного файла**

12. В окне мастера **Установка ключа** (см. рис. 12) укажите файл ключа Антивируса, который вы хотите установить (подробнее о параметре читайте в таблице 4 на стр. 25):

    - если вы предварительно сохранили файл ключа в папке \server\ комплекта поставки, имя этого файла отобразится в поле **Ключ**. Просмотрите информацию, которая содержится в файле ключа, в поле **Информация о ключе** и нажмите на кнопку **Далее**, чтобы установить ключ.
    - если вы хотите установить ключ, файл которого хранится в другой папке, укажите имя файла ключа и путь к нему.

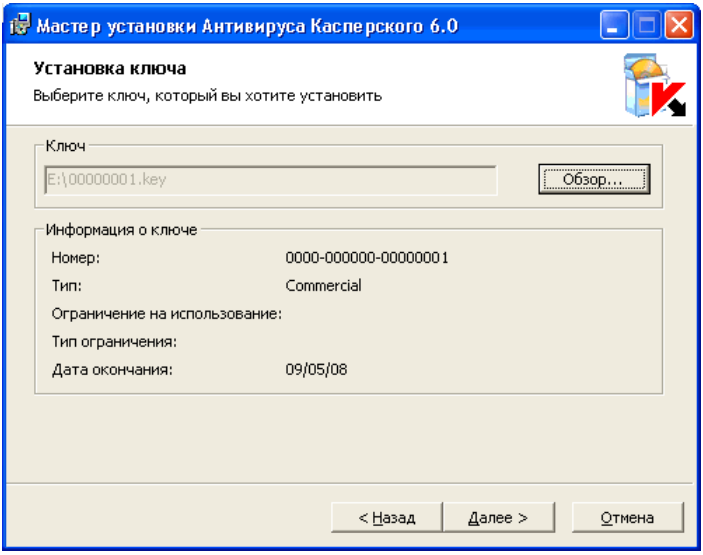

Рисунок 12. Окно **Установка ключа**

В окне **Установка ключа** отображается следующая информация об устанавливаемом ключе:

Поле	**Описание**
Номер	Серийный номер ключа
Тип	Тип ключа (для бета-тестирования, пробный или коммерческий)
Ограничение на использование	Количество объектов ограничения
Тип ограничения	Объекты ограничения
Дата окончания	Дата окончания срока действия ключа; рассчитывается Антивирусом; наступает, когда завершится период действия ключа с момента его активации, но не позднее даты, когда ключ становится недействительным

13. В окне **Готовность к установке** (см. рис. 13) нажмите на кнопку **Установить**.

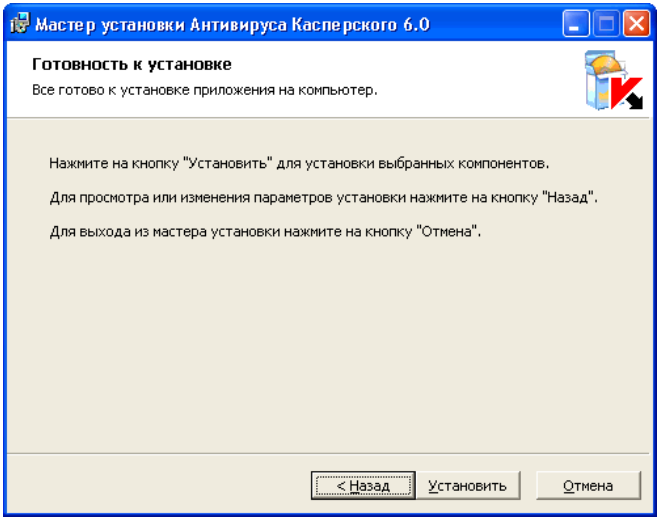

Рисунок 13. Окно **Готовность к установке**

Мастер приступит к установке компонентов Антивируса. Откроется окно **Выполняется установка** (см. рис. 14).

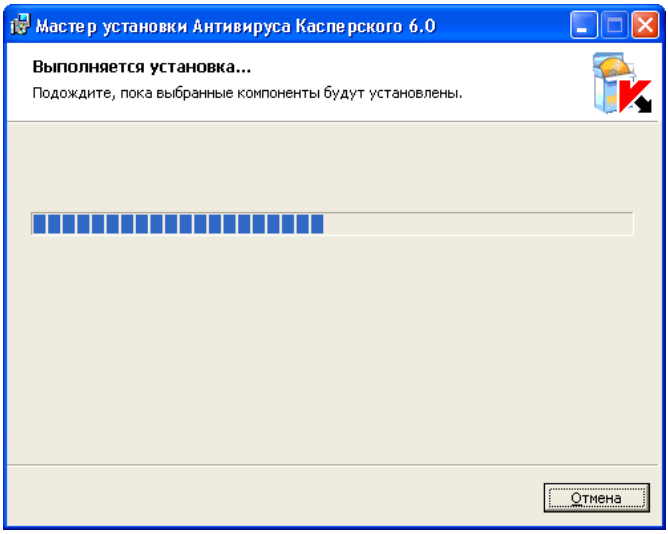

Рисунок 14. Окно **Выполняется установка**

14. В окне **Установка завершена** (см. рис. 15) нажмите на кнопку **ОК**.

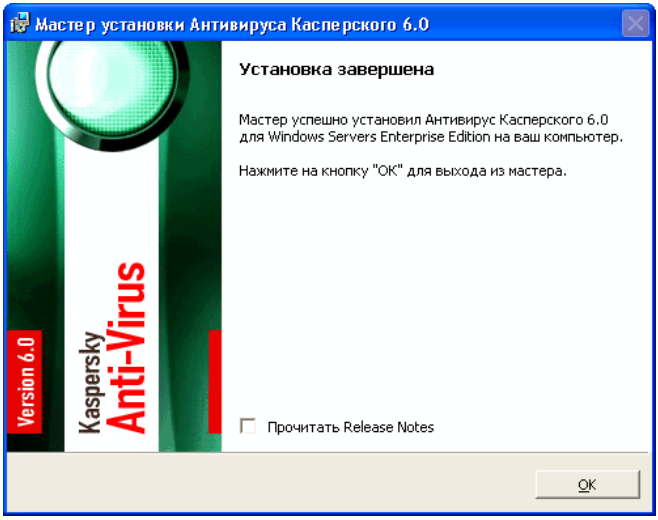

Рисунок 15. Окно **Установка завершена**

Как только установка завершится, Антивирус автоматически начнет выполнять свои функции, если вы установили ключ.

О том, какие действия рекомендуется выполнить после установки, см. п. 5.1.3 на стр. 76.

Глава 9 на стр. 116 содержит информацию о том, как проверить работу функций Антивируса перед его использованием.

5.1.2. Установка консоли Антивируса в ММС

Чтобы установить консоль Антивируса в ММС, выполните следующие шаги:

Таблица 14.Установка консоли Антивируса в ММС

Шаг	Действие
Шаг 1	С помощью мастера установки установите набор «Средства администрирования» на компьютер, с которого вы хотите управлять Антивирусом (см. п. 5.1.2.1 на стр. 60).
Шаг 2	Если вы установили набор «Средства администрирования» на другом компьютере, выполните дополнительную настройку, описанную в п. 5.1.2.2 на стр. 70.

5.1.2.1. Процедура установки консоли Антивируса в ММС

Чтобы установить консоль Антивируса в ММС:

1. Убедитесь, что у вас достаточно прав для установки.

   Чтобы установить консоль Антивируса в ММС, вы должны входить в группу локальных администраторов на компьютере, на котором вы запускаете мастер установки.

2. На компьютере, на котором вы хотите установить консоль Антивируса в ММС, запустите файл приложения-приветствия setup.exe.

   Примечание

   Вы можете запустить файл приложения-приветствия с установочного компакт-диска. Если вы предварительно скопировали файлы комплекта поставки на локальный диск, убедитесь, что сохранена структура файлов комплекта поставки.

3. В окне приложения-приветствия щелкните на ссылке **Средства администрирования** (см. рис. 16).

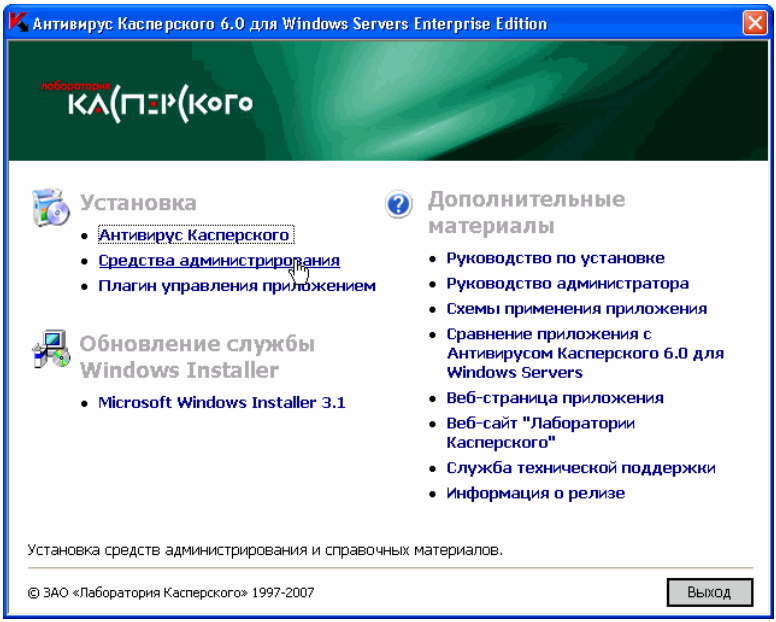

Рисунок 16. Окно приложения-приветствия

Откроется мастер установки. Следуя его инструкциям, задайте нужные параметры установки консоли Антивируса в ММС.

Вы можете прервать установку на любом шаге мастера. Для этого в окне мастера нажмите на кнопку **Отмена**.

4. В окне приветствия мастера установки (см. рис. 17) нажмите на кнопку **Далее**.

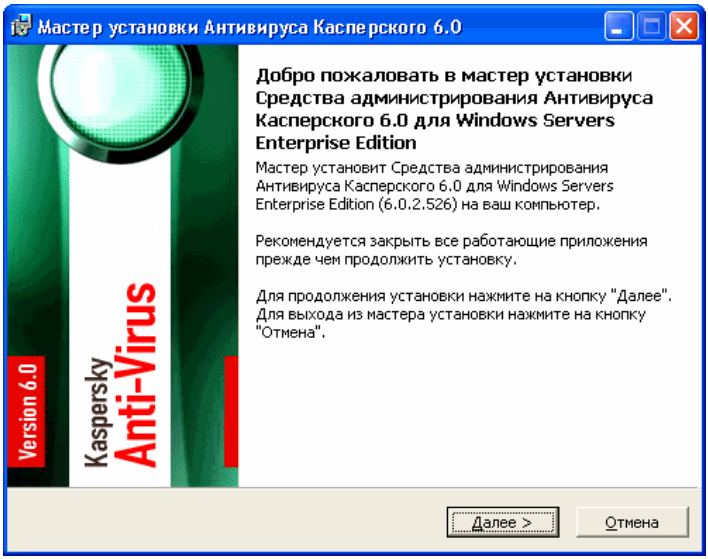

Рисунок 17. Окно приветствия мастера установки

5. В окне **Лицензионное соглашение** (см. рис. 18) ознакомьтесь с условиями лицензионного соглашения и установите флажок **Я принимаю условия лицензионного соглашения**, чтобы продолжить установку.

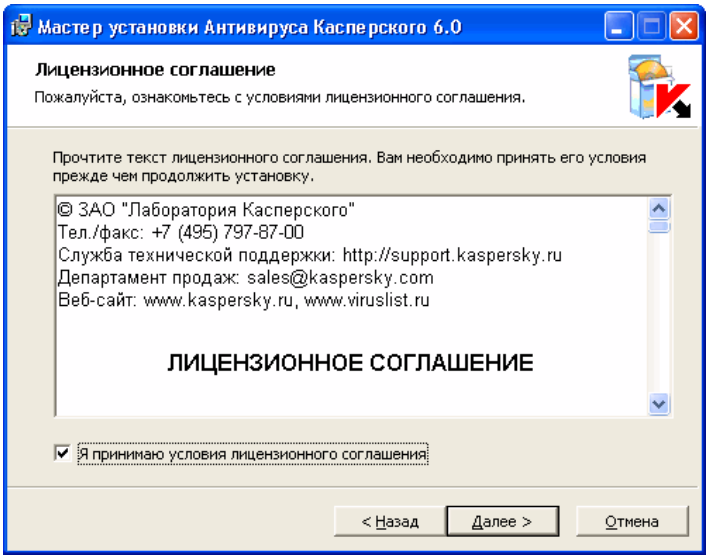

Рисунок 18. Окно **Лицензионное соглашение**

6. В окне **Тип установки** (см. рис. 19) выберите один из следующих вариантов:

   - **Полная установка**, чтобы установить на компьютер полный набор программных компонентов «Средства администрирования» (он включает консоль Антивируса в MMC, файл справки и файлы руководств; описание компонентов приводится в п. 3.4.1 на стр. 22).
   - **Выборочная установка**, чтобы вручную выбрать компоненты из списка.

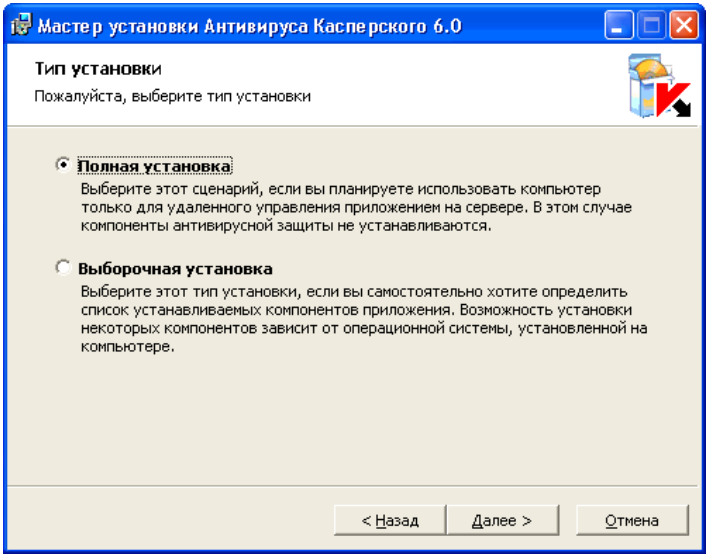

Рисунок 19. Окно **Тип установки**

Если компьютер не соответствует программным требованиям для установки компонентов, мастер установки прекратит работу. Список программных требований приводится в п. 3.2 на стр. 17.

Если вы выбрали тип установки **Полная установка**, перейдите к шагу 8.

7. Если вы выбрали тип установки **Выборочная установка**, откроется окно **Выборочная установка** (см. рис. 20). По умолчанию все компоненты набора «Средства администрирования» включены в список устанавливаемых. Чтобы исключить компонент из списка, щелкните на компоненте и выберите ✕. Чтобы установить компонент, щелкните на компоненте и выберите . Чтобы установить компонент и все его подкомпоненты, щелкните на компоненте и выберите .

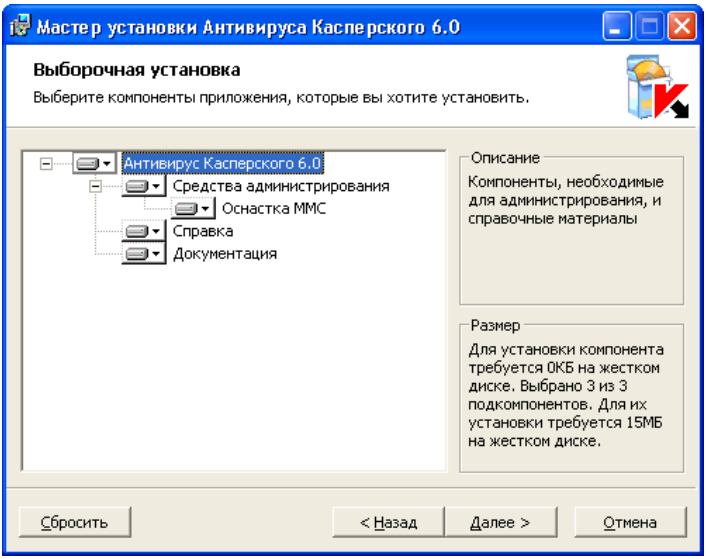

Рисунок 20. Окно **Выборочная установка**

Чтобы отменить все изменения в окне **Выборочная установка**, нажмите на кнопку **Сбросить**.

8. В окне **Выбор папки назначения** (см. рис. 21), если требуется, укажите другую папку, в которой будут сохранены устанавливаемые файлы.

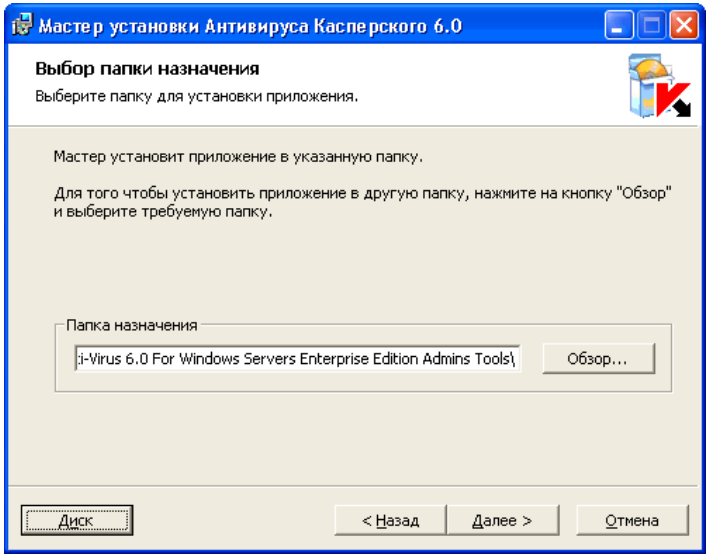

Рисунок 21. Окно **Выбор папки назначения**

После того как вы укажете папку на каком-либо из дисков компьютера, вы можете посмотреть, позволит ли размер свободного пространства на этом диске установить выбранные вами компоненты. Для этого нажмите на кнопку **Диск**.

Откроется окно **Доступное дисковое пространство** (см. рис. 22). В нем вы можете просмотреть доступный объем памяти на диске, на котором вы хотите установить выбранные компоненты (**Доступно на диске**), а также объем памяти, требуемый для их установки (**Требуется на диске**).

В окне **Доступное дисковое пространство** нажмите на кнопку **ОК**, чтобы закрыть его.

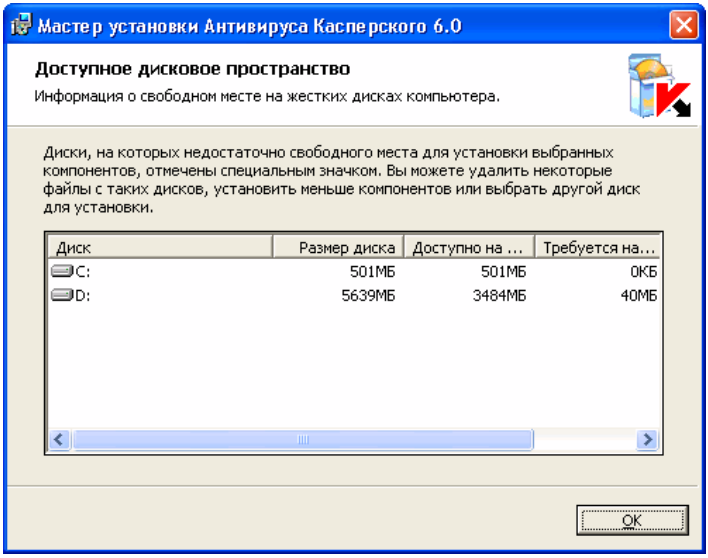

Рисунок 22. Окно **Доступное дисковое пространство**

Если места на выбранном диске недостаточно, освободите место на этом диске или в окне **Выбор папки назначения** укажите папку для файлов консоли Антивируса на другом диске компьютера.

9. Если вы планируете с помощью устанавливаемой консоли Антивируса в MMC управлять Антивирусом, установленным на другом компьютере, то в окне **Разрешение сетевых соединений** (см. рис. 23) установите флажок **Разрешить сетевые соединения для консоли Антивируса Касперского**.

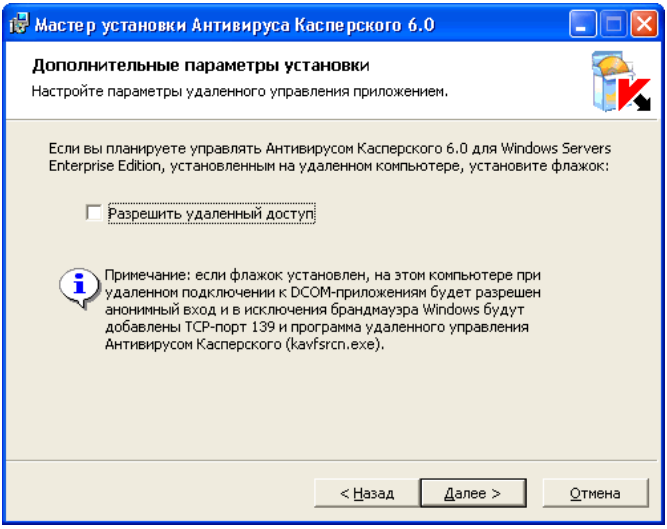

Рисунок 23. Окно **Разрешение сетевых соединений**

10. В окне **Готовность к установке** (см. рис. 24) нажмите на кнопку **Установить**.

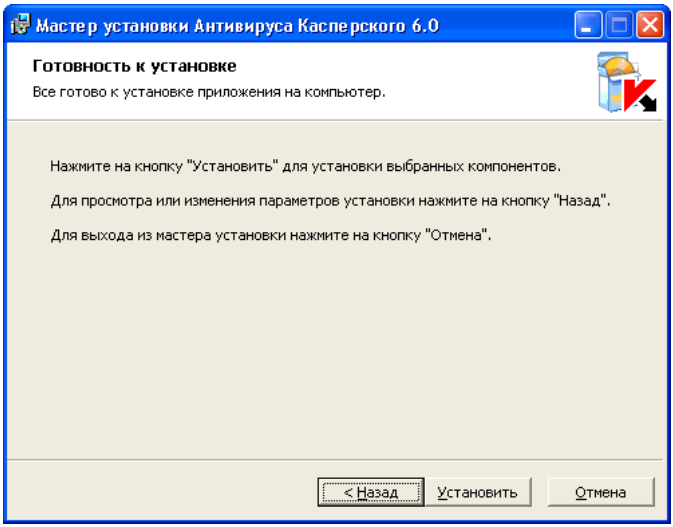

Рисунок 24. Окно **Готовность к установке**

Мастер приступит к установке выбранных компонентов. Откроется окно **Выполняется установка** (см. рис. 25).

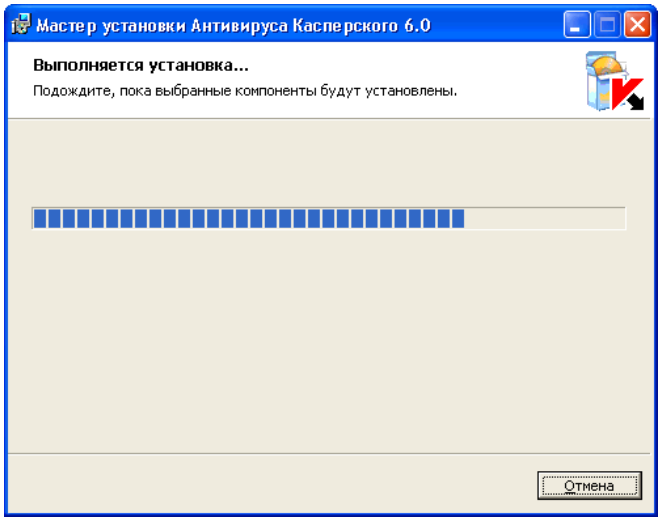

Рисунок 25. Окно **Выполняется установка**

11. В окне **Установка завершена** (см. рис. 26) нажмите на кнопку **ОК**.

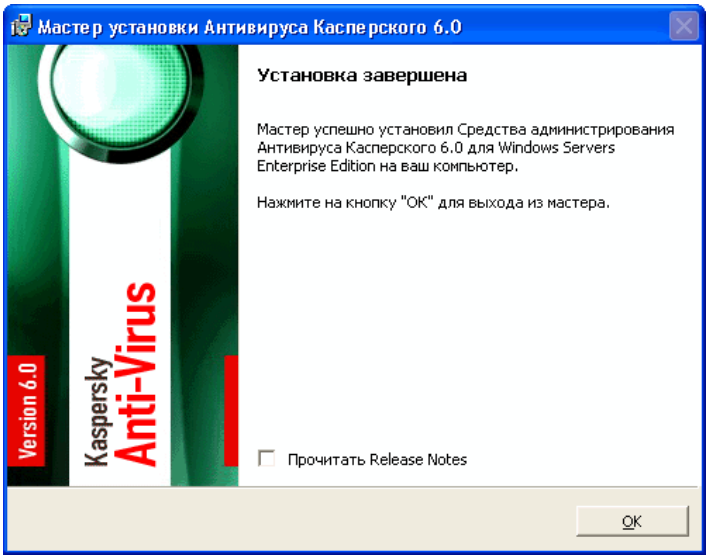

Рисунок 26. Окно **Установка завершена**

5.1.2.2. Дополнительная настройка после установки консоли Антивируса в ММС на другом компьютере

Если вы установили консоль Антивируса в ММС не на защищаемом сервере, а на другом компьютере, то для того, чтобы пользователи могли управлять Антивирусом на защищаемом сервере удаленно, выполните следующие действия:

- на защищаемом сервере добавьте пользователей Антивируса в группу **KAVWSEE Administrators** (см. п. 5.1.2.2.1 на стр. 71);
- если защищаемый сервер работает под управлением Microsoft Windows Server 2008, то на нем разрешите сетевые соединения для службы управления Антивирусом Касперского kavfsgt.exe (см. п. 5.1.2.2.2 на стр. 72);
- если удаленный компьютер работает под управлением Microsoft Windows XP с пакетом обновлений 1, выключите на нем брандмауэр Windows, чтобы открыть сетевые соединения для установленной на нем консоли Антивируса (см. п. 5.1.2.2.3 на стр. 73);

- если при установке консоли Антивируса в MMC на компьютере под управлением Microsoft Windows XP с пакетом обновлений 2 или под управлением Microsoft Windows Vista вы не включили параметр **Разрешить сетевые соединения для консоли Антивируса Касперского**, то вручную разрешите сетевые соединения для консоли через брандмауэр на этом компьютере (см. п. 5.1.2.2.4 на стр. 74).

5.1.2.2.1. Добавление пользователей Антивируса в группу KAVWSEE Administrators на защищаемом сервере

Чтобы управлять Антивирусом через консоль Антивируса в MMC, установленную на другом компьютере, пользователи Антивируса должны иметь полный доступ к *службе управления Антивирусом* (*Kaspersky Anti-Virus Management*) на защищаемом сервере. По умолчанию доступ к службе имеют пользователи, входящие в группу локальных администраторов на защищаемом сервере.

Примечание

О том, какие службы Антивирус регистрирует при установке, читайте в п. 3.7 на стр. 34

Вы можете предоставить доступ к службе управления Антивирусом учетным записям следующих типов:

- **учетной записи, зарегистрированной локально** на компьютере, на котором установлена консоль Антивируса. Чтобы установить соединение, на защищаемом сервере должна быть локально зарегистрирована учетная запись с такими же данными;
- **учетной записи, зарегистрированной в домене**, в котором зарегистрирован компьютер с установленной консолью Антивируса. Чтобы установить соединение, защищаемый сервер должен быть зарегистрирован или в этом же домене или в домене, который находится в доверительных отношениях с этим доменом.

Во время установки Антивирус регистрирует на защищаемом сервере группу **KAVWSEE Administrators**. Пользователям этой группы разрешен доступ к службе управления Антивирусом. Вы можете разрешать или запрещать пользователям доступ к службе управления Антивирусом, добавляя их в группу **KAVWSEE Administrators** или удаляя их из нее.

Чтобы разрешить или запретить доступ к службе управления Антивирусом:

1. На защищаемом сервере выберите **Пуск** → **Настройка** → **Панель управления**. В окне **Панель управления** выберите **Администрирование** → **Управление компьютером**.
2. В дереве консоли **Управление компьютером** разверните узел **Локальные пользователи и группы**, затем разверните узел **Группы**.
3. Дважды щелкните на группе **KAVWSEE Administrators** и в диалоговом окне **Свойства** выполните следующие действия:
   - чтобы разрешить пользователю удаленное управление Антивирусом с помощью консоли, добавьте его в группу **KAVWSEE Administrators**;
   - чтобы запретить пользователю удаленное управление Антивирусом с помощью консоли, исключите его из группы **KAVWSEE Administrators**.
4. Нажмите на кнопку **ОК** в диалоговом окне **Свойства**.

5.1.2.2.2. Разрешение на сервере под управлением Microsoft Windows Server 2008 сетевых соединений для службы управления Антивирусом Касперского

Чтобы устанавливать соединения между консолью и службой управления Антивирусом, вам нужно разрешить сетевые соединения через брандмауэр для службы управления Антивирусом Касперского на защищаемом сервере.

Чтобы разрешить сетевые соединения для службы управления Антивирусом Касперского:

1. На защищаемом сервере под управлением Microsoft Windows Server 2008 выберите **Пуск** → **Панель управления** → **Безопасность** → **Брандмауэр Windows**.
2. В окне **Параметры брандмауэра Windows** щелкните **Изменить параметры**.
3. На закладке **Исключения** в списке предустановленных исключений установите флажки **COM + Сетевой доступ**, **Windows Management Instrumentation (WMI)** и **Remote Administration**.

4. Нажмите на кнопку **Добавить программу**.
5. В диалоговом окне **Добавление программы** укажите файл kavfsgt.exe. Он хранится в папке, которую вы указали в качестве папки назначения при установке консоли Антивируса в MMC. По умолчанию полный путь к файлу следующий:
   - в Microsoft Windows 32-разрядной версии: %Program-Files%\Kaspersky Lab\Kaspersky Anti-Virus 6.0 For Windows Servers Enterprise Edition\kavfsgt.exe;
   - в Microsoft Windows 64-разрядной версии: %Program-Files(x86)%\Kaspersky Lab\Kaspersky Anti-Virus 6.0 For Windows Servers Enterprise Edition\kavfsgt.exe.
6. Нажмите на кнопку **ОК**.
7. Нажмите на кнопку **ОК** в диалоговом окне **Параметры брандмауэра Windows**.

5.1.2.2.3. Разрешение сетевых соединений для консоли Антивируса в MMC в Microsoft Windows XP с пакетом обновлений 1

Если компьютер, на котором установлена консоль Антивируса, работает под управлением Microsoft Windows XP с пакетом обновлений 1, вам нужно отключить брандмауэр Windows на этом компьютере, чтобы разрешить сетевые соединения для консоли:

1. На компьютере, на котором установлена консоль Антивируса в MMC, выберите **Пуск** → **Панель управления** → **Сетевые подключения**.
2. Откройте контекстное меню на названии сетевого подключения (например, **Local Area Connection**) и выберите команду **Свойства**.
3. В диалоговом окне **<Название сетевого подключения>: Свойства** на закладке **Дополнительно** снимите флажок **Защитить мое подключение к Интернету**.
4. Нажмите на кнопку **ОК**.

5.1.2.2.4. Разрешение сетевых соединений для консоли Антивируса в MMC в Microsoft Windows XP с пакетом обновлений 2 или Microsoft Windows Vista

Консоль Антивируса в MMC на удаленном компьютере использует протокол DCOM, чтобы получать информацию о событиях Антивируса (проверенных объектах, завершении задач и др.) от службы управления Антивирусом на защищаемом сервере.

Если компьютер, на котором установлена консоль, работает под управлением Microsoft Windows XP с пакетом обновлений 2 или Microsoft Windows Vista, вам нужно разрешить сетевые соединения через брандмауэр на этом компьютере, чтобы устанавливать соединения между консолью и службой управления Антивирусом.

Выполните следующие действия:

- убедитесь, что разрешен анонимный удаленный доступ к приложениям COM (но не удаленный запуск и активация приложений COM) и
- в брандмауэре Windows откройте TCP-порт 135 и разрешите сетевые соединения для исполняемого файла процесса удаленного управления Антивирусом kavfsrcn.exe.

  Через порт TCP 135 клиентский компьютер, на котором установлена консоль Антивируса в MMC, обменивается информацией с защищаемым сервером, на котором установлен Антивирус.

Чтобы разрешить анонимный удаленный доступ к приложениям COM:

1. На компьютере, на котором установлена консоль Антивируса в MMC, откройте консоль **Службы компонентов**: выберите **Пуск** → **Выполнить**, введите **dcomcnfg** и нажмите на кнопку **ОК**.
2. В консоли **Службы компонентов** компьютера разверните узел **Компьютеры**, откройте контекстное меню на узле **Мой компьютер** и выберите команду **Свойства**.
3. В диалоговом окне **Свойства** на закладке **Безопасность COM** нажмите на кнопку **Изменить ограничения** в группе параметров **Права доступа**.
4. В диалоговом окне **Разрешение на доступ** убедитесь, что для пользователя **ANONYMOUS LOGON** установлен флажок **Разрешить удаленный доступ**.

5. Нажмите на кнопку **ОК**.

Чтобы открыть в брандмауэре Windows TCP-порт 135 и разрешить сетевые соединения для исполняемого файла процесса удаленного управления Антивирусом:

1. На удаленном компьютере закройте консоль Антивируса в MMC.
2. Выполните одно из следующих действий:
   - в *Microsoft Windows XP с пакетом обновлений 2 или выше* выберите **Пуск** → **Панель управления** → **Брандмауэр Windows**.
   - в *Microsoft Windows Vista* выберите **Пуск** → **Панель управления** → **Брандмауэр Windows** и в окне **Брандмауэр Windows** щелкните **Изменить параметры**.
3. В диалоговом окне **Брандмауэр Windows** (**Параметры брандмауэра Windows**) на закладке **Исключения** нажмите на кнопку **Добавить порт**.
4. В поле **Имя** укажите имя порта **RPC(TCP/135)** или задайте другое имя, например, **DCOM Антивируса**, в поле **Номер порта** укажите номер порта: **135**.
5. Выберите протокол **TCP**.
6. Нажмите на кнопку **ОК**.
7. На закладке **Исключения** нажмите на кнопку **Добавить программу**.
8. В диалоговом окне **Добавление программы** укажите файл kavfsrcn.exe. Он хранится в папке, которую вы указали в качестве папки назначения при установке консоли Антивируса в MMC. По умолчанию полный путь к файлу следующий:
   - в Microsoft Windows 32-разрядной версии: %Program-Files%\Kaspersky Lab\Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition Admins Tools\kavfsrcn.exe;
   - в Microsoft Windows 64-разрядной версии: %Program-Files(x86)%\Kaspersky Lab\Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition Admins Tools\kavfsrcn.exe.
9. Нажмите на кнопку **ОК**.
10. Нажмите на кнопку **ОК** в диалоговом окне **Брандмауэр Windows** (**Параметры брандмауэра Windows**).

Примечание

Чтобы применить новые параметры соединения: если консоль Антивируса была открыта, когда вы выполняли настройку соединения между защищаемым сервером и компьютером, на котором консоль установлена, закройте консоль, подождите 30-60 секунд (пока завершится процесс удаленного управления Антивирусом kavfsrcn.exe), а затем снова запустите ее.

5.1.3. Действия после установки Антивируса

Антивирус начинает выполнять свои функции сразу после установки, если вы установили его ключ. Если, устанавливая Антивирус, вы выбрали **Включить постоянную защиту после установки**, Антивирус проверяет объекты файловой системы сервера при доступе к ним, а также проверяет программный код запускаемых скриптов. Каждую пятницу в 20:00 Антивирус выполняет задачу **Полная проверка компьютера**.

После установки Антивируса рекомендуется выполнить следующие действия:

- **настроить и запустить задачу обновления баз Антивируса**. После установки Антивирус проверяет объекты с использованием баз, которые входили в его состав при поставке. Рекомендуется сразу же обновить базы Антивируса. Для этого вам нужно настроить и запустить задачу **Обновление баз приложения**. Далее обновление баз будет выполняться каждый час согласно расписанию, установленному по умолчанию (см. п. 5.1.3.1 на стр. 76);
- **запустить полную проверку сервера**, если до установки Антивируса на защищаемом сервере не было установлено антивирусное приложение с включенной функцией постоянной защиты файлов (см. п. 5.1.3.2 на стр. 81).

Вы также можете настроить уведомления администратора о событиях Антивируса (см. документ «Антивирус Касперского 6.0 для Windows Servers Enterprise Edition. Руководство администратора»).

5.1.3.1. Настройка и запуск задачи обновления баз Антивируса

Выполните следующие действия: 1) в задаче **Обновление баз приложения** настройте соединение с источником обновлений – *HTTP- или FTP-*

серверами обновлений «Лаборатории Касперского» и 2) запустите задачу **Обновление баз приложения**.

*Чтобы настроить соединение с серверами обновлений «Лаборатории Касперского» в задаче **Обновление баз приложения**:*

1. Откройте консоль Антивируса в ММС: на компьютере, на котором вы установили набор «Средства администрирования», выберите **Пуск** → **Программы** → **Антивирус Касперского 6.0 для Windows Servers Enterprise Edition** → **Средства администрирования** → **Консоль Антивируса Касперского**.

   Примечание

   Если вы планируете добавлять в консоль Антивируса другие оснастки, откройте консоль в авторском режиме: выберите **Пуск** → **Программы** → **Антивирус Касперского 6.0 для Windows Servers Enterprise Edition** → **Средства администрирования**, откройте контекстное меню на приложении **Консоль Антивируса Касперского** и выберите **Автор**.

2. Если вы запустили консоль Антивируса не на защищаемом сервере, а на другом компьютере, подключитесь к защищаемому серверу: откройте контекстное меню на названии оснастки Антивируса, выберите команду **Подключиться к другому компьютеру**, затем в диалоговом окне **Выбор компьютера** выберите **Другой компьютер** и в поле ввода укажите сетевое имя защищаемого сервера.

   Примечание

   Если учетная запись, которую вы использовали для входа в soft Windows, не обладает правами доступа к службе управления Антивирусом на сервере, укажите учетную запись, которая ет этими правами. Подробнее о том, каким учетным записям вы можете предоставлять доступ к службе управления Антивирусом, читайте в п. 5.1.2.2.1 на стр. 71.

Откроется окно консоли Антивируса в ММС (см. рис. 27).

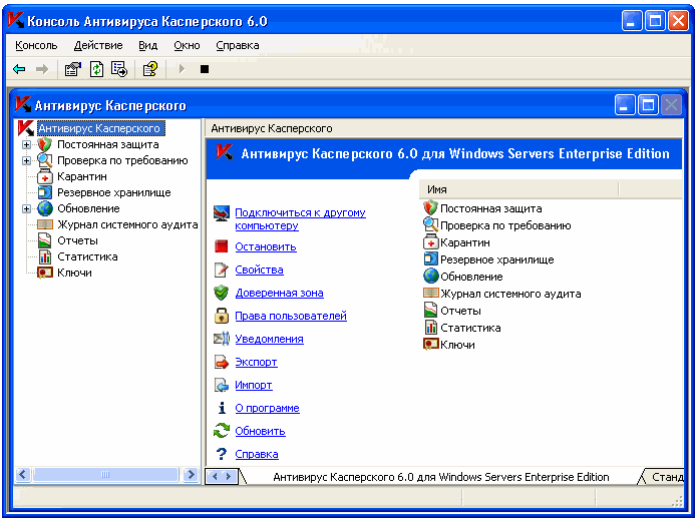

Рисунок 27. Окно консоли Антивируса в ММС

3. В дереве консоли выберите узел **Обновление**.
4. Откройте контекстное меню на задаче **Обновление баз приложения** и выберите команду **Свойства**.

5. В диалоговом окне **Свойства**: **Обновление** откройте закладку **Настройка соединения** (см. рис. 28).

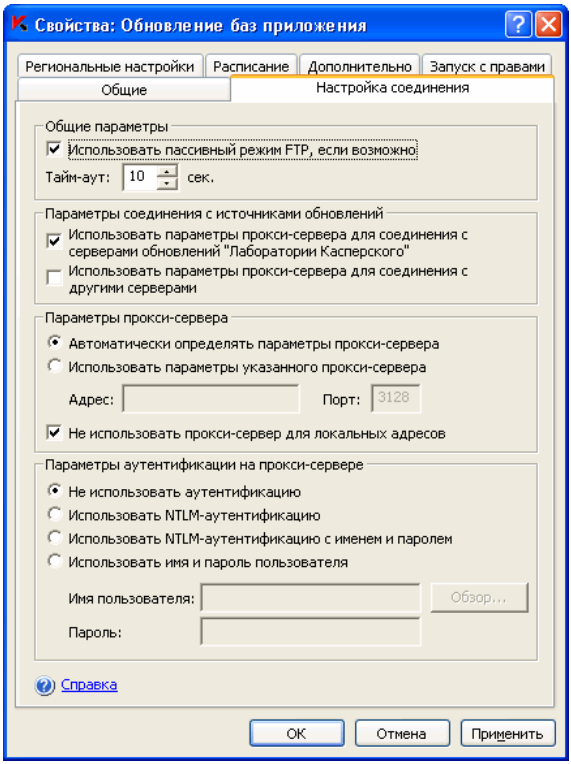

Рисунок 28. Закладка **Настройки соединения**

6. Выполните следующие действия:

   a) Если в вашей сети не настроен протокол Web Proxy Auto-Discovery Protocol (WPAD) для автоматического распознавания параметров прокси-сервера в локальной сети, укажите параметры прокси-сервера: в группе параметров **Параметры прокси-сервера** выберите **Использовать параметры указанного прокси-сервера**, в поле **Адрес** введите адрес, а в поле **Порт** – номер порта прокси-сервера.

б) Если в вашей сети требуется проверка подлинности при доступе к прокси-серверу, выберите нужный метод проверки подлинности в группе параметров **Параметры аутентификации на прокси-сервере**:

- **Использовать NTLM-аутентификацию**, если прокси-сервер поддерживает встроенную проверку подлинности Microsoft Windows (NTLM authentication). Антивирус будет использовать для доступа к прокси-серверу учетную запись, указанную в задаче (по умолчанию задача выполнится под учетной записью **Локальная система** (**SYSTEM**)).
- **Использовать NTLM-аутентификацию с именем и паролем**, если прокси-сервер поддерживает встроенную проверку подлинности Microsoft Windows. Антивирус будет использовать для доступа к прокси-серверу учетную запись, указанную вами.

  Введите имя и пароль пользователя или выберите пользователя в списке.
- **Использовать имя и пароль пользователя**, чтобы выбрать обычную проверку подлинности (Basic authentication). Введите имя и пароль пользователя или выберите пользователя в списке.

7. В диалоговом окне **Свойства**: **Обновление баз приложения** нажмите на кнопку **ОК**.

Вы настроили параметры соединения с источником обновлений в задаче **Обновление баз приложения**. Теперь запустите задачу.

*Чтобы запустить задачу **Обновление баз приложения**:*

1. В дереве консоли разверните узел **Обновление**.
2. Откройте контекстное меню на задаче **Обновление баз приложения** и выберите команду **Запустить**.

Задача будет запущена; в панели результатов отобразится статус задачи **Выполняется** (см. рис. 29).

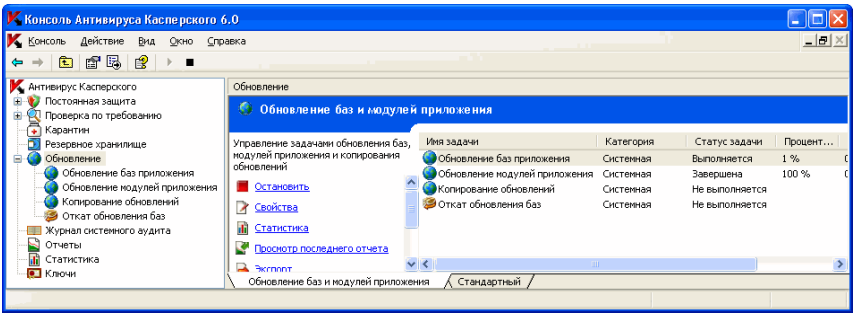

Рисунок 29. Задача **Обновление баз приложения** выполняется

После того как задача успешно завершится, вы сможете посмотреть дату выпуска последних установленных обновлений баз в узле **Статистика**.

5.1.3.2. Полная проверка сервера

После того как вы обновили базы Антивируса, проверьте сервер на наличие угроз с помощью задачи **Полная проверка компьютера**.

*Чтобы запустить задачу **Полная проверка компьютера**:*

1. Откройте консоль Антивируса в ММС (см. п. 5.1.3.1 на стр. 76).
2. В дереве консоли выберите узел **Проверка по требованию**.
3. Откройте контекстное меню на задаче **Полная проверка компьютера** и выберите команду **Запустить**.

Задача будет запущена; в панели результатов отобразится статус задачи **Выполняется**.

Выполнение задачи **Полная проверка компьютера** может занять длительное время.

Чтобы просмотреть сводный отчет о выполнении задачи:

1. В дереве консоли выберите узел **Отчеты**.
2. В панели результатов найдите строку-сводный отчет о задаче **Полная проверка компьютера**. Чтобы просмотреть подробный отчет о выполнении задачи, откройте контекстное меню на сводном отчете о задаче и выберите команду **Просмотреть отчет**. Подробнее об отчетах о выполнении задач читайте в документе

«Антивирус Касперского 6.0 для Windows Servers Enterprise Edition. Руководство администратора».

5.2. Добавление и удаление компонентов, восстановление Антивируса

Вы можете в любой момент добавить или удалить компоненты Антивируса.

Если в работе Антивируса возникли проблемы (Антивирус завершается аварийно; задачи завершаются аварийно или не запускаются), вы можете попробовать восстановить Антивирус. Вы можете выполнить восстановление, сохранив текущие значения параметров Антивируса, его функций и задач или выбрать режим, при котором все параметры Антивируса примут значения по умолчанию.

Во время работы мастера установки может потребоваться завершить работу Антивируса.

Чтобы добавить или удалить компоненты Антивируса или восстановить Антивирус:

1. В меню **Пуск** выберите **Все программы → Антивирус Касперского 6.0 для Windows Servers Enterprise Edition → Изменение или удаление**.
2. В окне **Изменение, восстановление или удаление** мастера установки (см. рис. 30) выполните следующие действия:
   - чтобы добавить или удалить отдельные компоненты Антивируса, выберите **Изменение состава компонентов приложения**;
   - чтобы восстановить Антивирус, выберите **Восстановление установленных компонентов**.

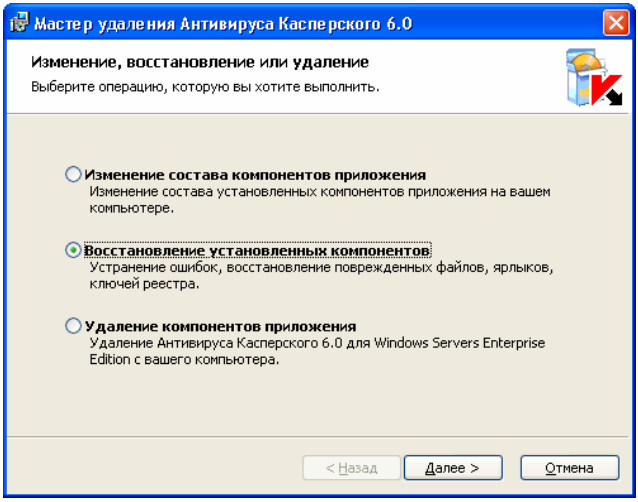

Рисунок 30. Окно **Изменение, восстановление или удаление**

3. Если вы выбрали **Восстановление установленных компонентов**, в одноименном окне (см. рис. 31) установите флажок **Восстановить рекомендуемые параметры работы приложения**, чтобы вернуть общим параметрам Антивируса, параметрам его функций и задач их значения по умолчанию.

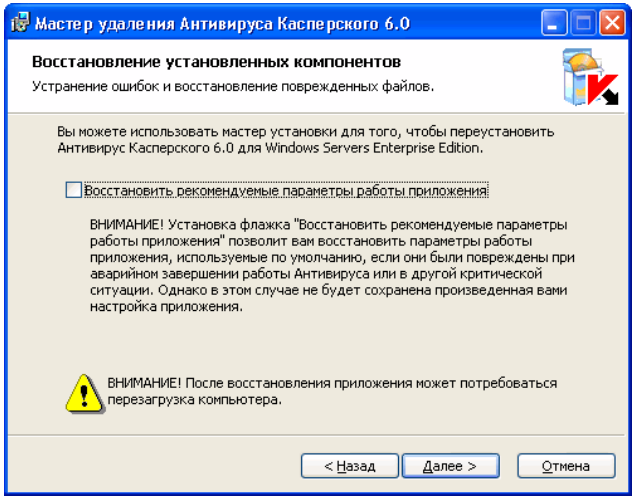

Рисунок 31. Окно **Восстановление установленных компонентов**

4. Если вы выбрали **Изменение состава компонентов приложения**, в окне **Выборочная установка** (см. рис. 32) укажите новый состав компонентов Антивируса (описание программных компонентов Антивируса приводится в п. 3.4 на стр. 21).

   По умолчанию все установленные компоненты будут установлены повторно. Чтобы удалить компонент, щелкните на компоненте и выберите ✕. Чтобы установить компонент, щелкните на компоненте и выберите . Чтобы установить компонент и все его подкомпоненты, щелкните на компоненте и выберите .

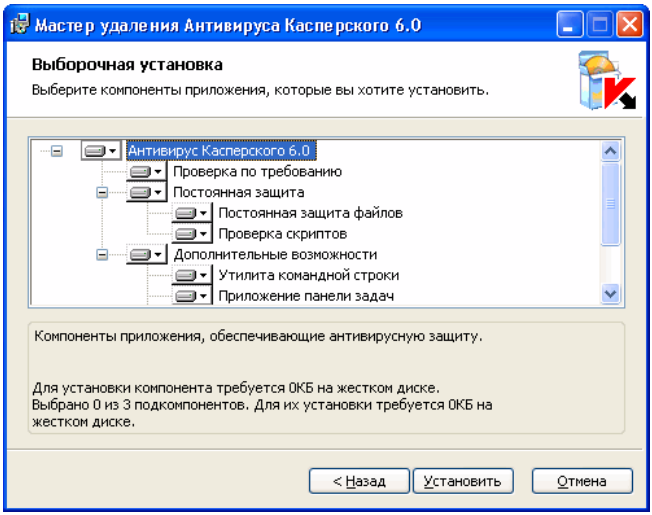

Рисунок 32. Окно **Выборочная установка**

5. В окне **Готовность к восстановлению** (или **Готовность к установке**, если вы выбрали изменение состава компонентов, см. рис. 33) нажмите на кнопку **Установить**, чтобы выполнить установку / восстановление.

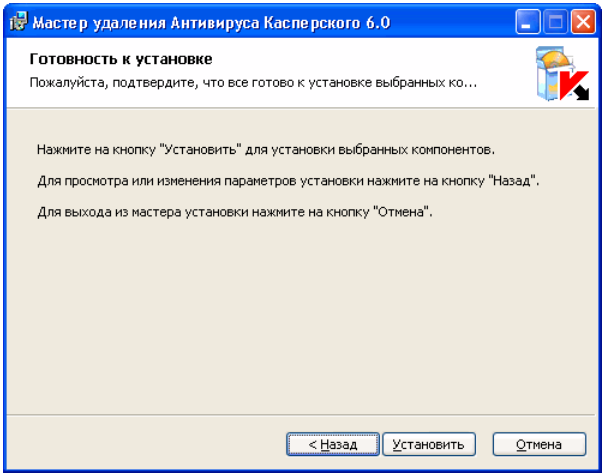

Рисунок 33. Окно **Готовность к установке**

6. Если после выполнения установки / восстановления потребуется перезагрузка сервера, в окне **Установка завершена** отобразится флажок **Перезагрузить компьютер сейчас** (см. рис. 34). Чтобы отложить перезагрузку, снимите флажок **Перезагрузить компьютер сейчас**.

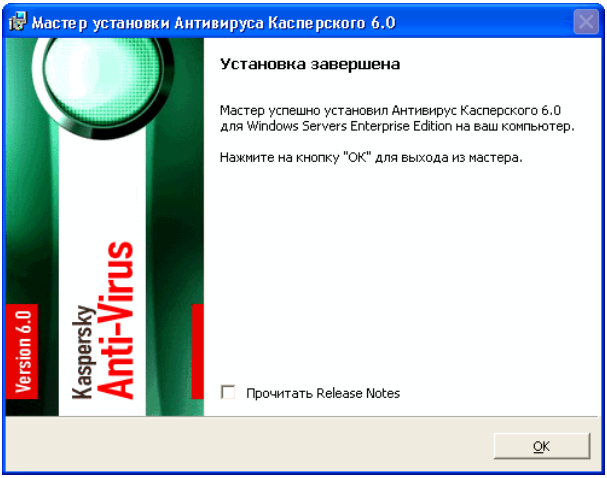

Рисунок 34. Окно **Установка завершена**

5.3. Удаление с помощью мастера установки / удаления

В этом разделе описано, как удалить с помощью мастера установки / удаления:

- Антивирус с защищаемого сервера (см. п. 5.3.1 на стр. 86);
- консоль Антивируса в MMC (набор «Средства администрирования») (см. п. 5.3.2 на стр. 90).

5.3.1. Удаление Антивируса с защищаемого сервера

Вы можете удалить Антивирус с защищаемого сервера с помощью мастера установки / удаления.

После удаления Антивируса с защищаемого сервера может потребоваться перезагрузка сервера. Вы можете отложить перезагрузку.

Чтобы удалить Антивирус:

1. В меню **Пуск** выберите **Все программы** → **Антивирус Касперского 6.0 для Windows Servers Enterprise Edition** → **Изменение или удаление Антивируса Касперского 6.0**.
2. В окне **Изменение, восстановление или удаление** мастера (см. рис. 35) выберите **Удаление компонентов приложения**.

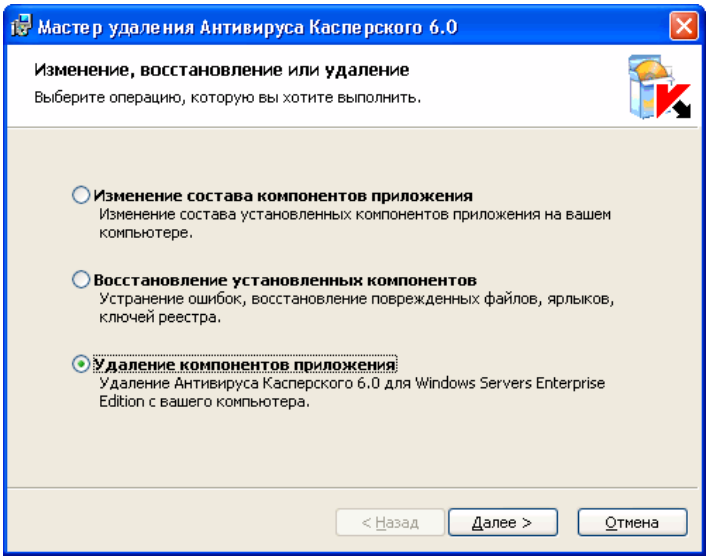

Рисунок 35. Окно **Изменение, восстановление или удаление**

3. В окне **Дополнительные параметры удаления** (см. рис. 36), если требуется, установите флажки, чтобы экспортировать содержимое карантина и содержимое резервного хранилища в специальную папку на сервере или другую указанную вами папку (подробнее об этих параметрах см. в таблице 5 на стр. 33).

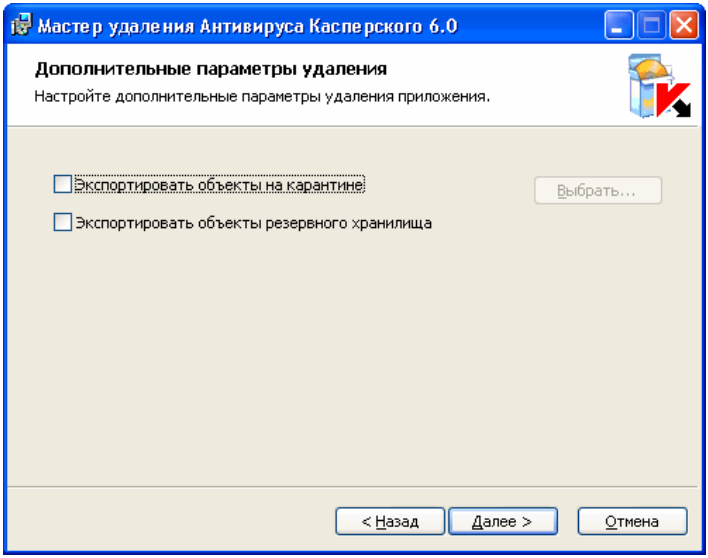

Рисунок 36. Окно **Дополнительные параметры удаления**

Примечание

Убедитесь, что отключена постоянная защита файлов в указанной вами папке.

4. В окне **Готовность к удалению** (см. рис. 37) нажмите на кнопку **Удалить**, чтобы удалить Антивирус.

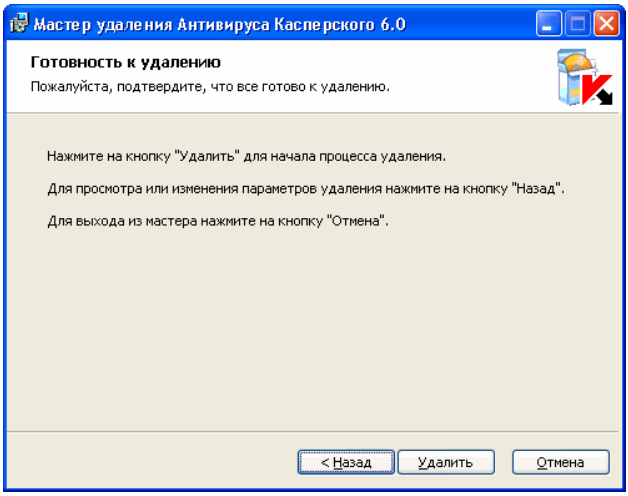

Рисунок 37. Окно **Готовность к удалению**

5. Если после удаления Антивируса потребуется перезагрузка сервера, в окне **Удаление завершено** отобразится флажок **Перезагрузить компьютер сейчас** (см. рис. 38). Чтобы отложить перезагрузку, снимите флажок **Перезагрузить компьютер сейчас**.

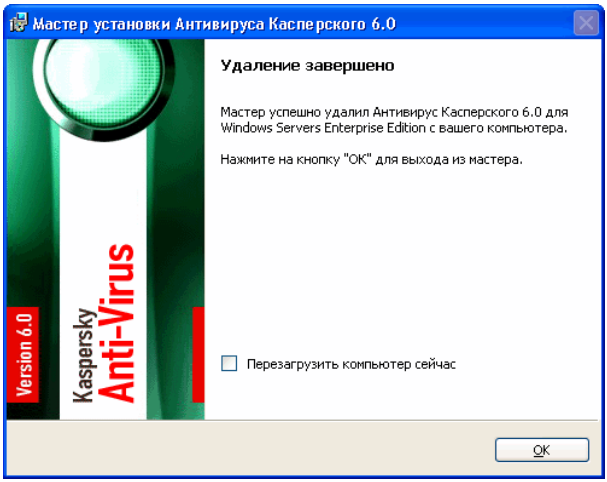

Рисунок 38. Окно **Удаление завершено**

6. В окне **Удаление завершено** нажмите на кнопку **ОК**.

5.3.2. Удаление консоли Антивируса в ММС

Вы можете удалить консоль Антивируса в ММС с компьютера с помощью мастера установки / удаления.

После удаления консоли перезагрузка не требуется.

Чтобы удалить консоль Антивируса в ММС:

1. В меню **Пуск** выберите **Все программы** → **Антивирус Касперского 6.0 для Windows Servers Enterprise Edition** → **Средства администрирования** → **Изменение или удаление**.
2. В окне **Изменение, восстановление или удаление** мастера (см. рис. 39) выберите **Удаление компонентов приложения**.

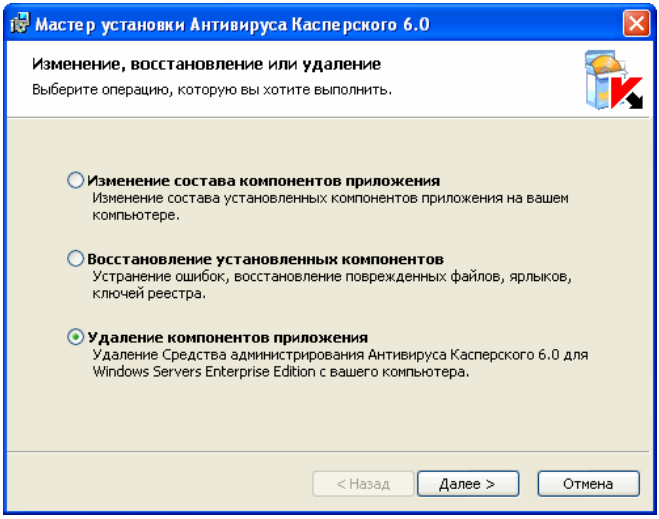

Рисунок 39. Окно **Изменение, восстановление или удаление**

3. В окне **Готовность к удалению** (см. рис. 40) нажмите на кнопку **Удалить**, чтобы удалить консоль Антивируса в ММС.

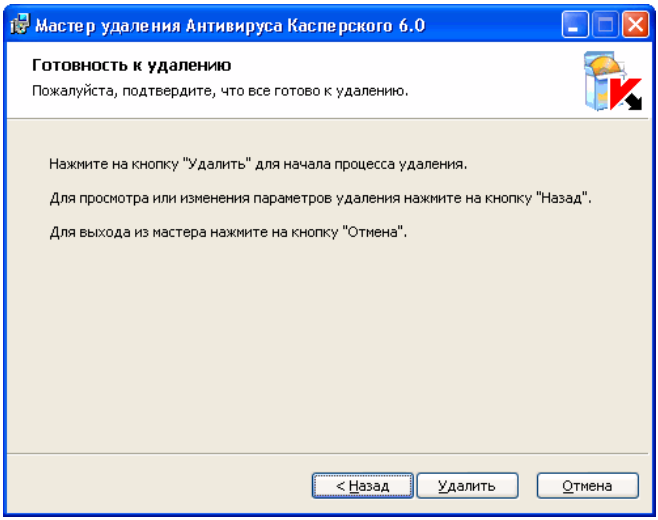

Рисунок 40. Окно **Готовность к удалению**

4. В окне **Удаление завершено** (см. рис. 41) нажмите на кнопку **ОК**.

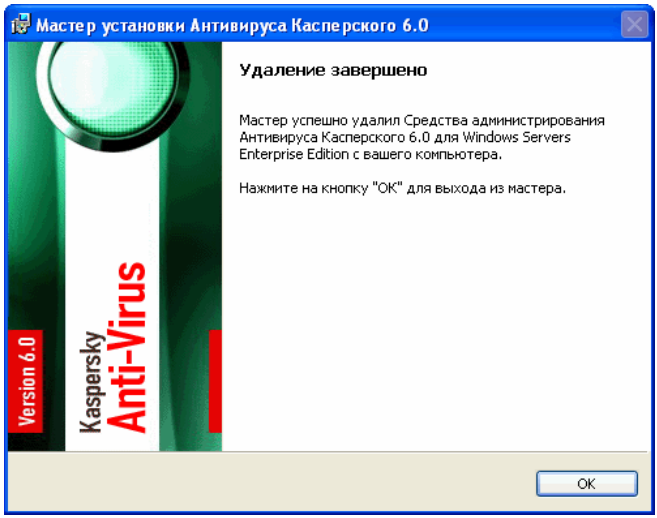

Рисунок 41. Окно **Удаление завершено**

ГЛАВА 6. УСТАНОВКА И УДАЛЕНИЕ АНТИВИРУСА ИЗ КОМАНДНОЙ СТРОКИ

В этой главе содержится следующая информация:

- об установке и удалении Антивируса из командной строки (см. п. 6.1 на стр. 92);
- примеры команд для установки Антивируса и действия после установки (см. п. 6.2 на стр. 93);
- примеры команд для добавления и удаления компонентов Антивируса (см. п. 6.3 на стр. 96);
- примеры команд для удаления Антивируса (см. п. 6.4 на стр. 97).

6.1. Об установке и удалении Антивируса из командной строки

Из командной строки защищаемого сервера вы можете устанавливать и удалять Антивирус, добавлять или удалять его компоненты, выполняя файл инсталляционного пакета \server\kavws.msi с помощью команды msiexec службы Windows Installer и ее стандартных ключей, а также специальных ключей Антивируса.

Выполняя файл \client\kavwstools.msi, вы можете установить набор «Средства администрирования» (консоль Антивируса в MMC), чтобы управлять Антивирусом на защищаемом сервере локально или удаленно.

О том, как использовать стандартные команды и ключи службы Windows Installer, см. документацию, предоставляемую корпорацией Майкрософт.

Примечание

Чтобы установить Антивирус на компьютере, вы должны входить в группу его локальных администраторов.

Если вы запустите на защищаемом сервере файл \server\kavws.msi без дополнительных ключей, Антивирус будет установлен с параметрами установки по умолчанию, перечисленными в таблице 4 на стр. 25.

По умолчанию устанавливаются все программные компоненты Антивируса. Вы можете задать набор устанавливаемых компонентов с помощью ключа ADDLOCAL, перечислив в качестве его значений коды выбранных компонентов или наборов компонентов (описание программных компонентов Антивируса и их коды приводятся в п. 3.4 на стр. 21).

6.2. Установка Антивируса

В этом разделе содержится следующая информация:

- примеры команд для установки Антивируса (см. п. 6.2.1 на стр. 93);
- действия после установки Антивируса (см. п. 6.2.2 на стр. 95).

6.2.1. Примеры команд для установки Антивируса

В этом разделе приводятся примеры команд для установки Антивируса с помощью выполнения из командной строки *msi*-файла и файла запуска инсталляционного пакета setup.exe.

Примечание

На компьютере под управлением Microsoft Windows 32-разрядной версии запускайте файлы из папки x86\ комплекта поставки, а на компьютере под управлением Microsoft Windows 64-разрядной версии запускайте файлы из папки x64\ комплекта поставки.

Примеры команд установки Антивируса из файла setup.exe

Выполните следующие файлы:

- setup.exe из папки \x86(x64)\server – для установки Антивируса;
- setup.exe из папки \x86(x64)\client – для установки консоли Антивируса в MMC.

Чтобы установить все программные компоненты Антивируса с параметрами установки по умолчанию в неинтерактивном режиме (см. описание компонентов в п. 3.4.1 на стр. 22, п. 3.4.2 на стр. 23):

```
\x86\server\setup.exe /s
```

или

```
\x64\server\setup.exe /s
```

Чтобы установить Антивирус со следующими компонентами и параметрами установки, указанными ключом /p:

- установить только компоненты **Постоянная защита файлов** и **Проверка по требованию**, без компонента **Проверка скриптов** (см. описание параметров и их ключи в таблице 4 на стр. 25);
- не запускать постоянную защиту файлов и проверку скриптов при запуске Антивируса;
- не исключать из проверки файлы, рекомендованные к исключению корпорацией Microsoft;

выполните следующую команду:

```
\x86\server\setup.exe /p"ADDLOCAL=Oas RUNRTP=0
ADDMSEXCLUSION=0"
```

или

```
\x64\server\setup.exe /p"ADDLOCAL=Oas RUNRTP=0
ADDMSEXCLUSION=0"
```

Чтобы установить Антивирус, сохранив файл журнала установки с именем kavws.log в папке, в которой хранится msi-файл инсталляционного пакета Антивируса:

```
\x86\server\setup.exe /l kavws.log
```

или

```
\x64\server\setup.exe /l kavws.log
```

Примеры команд для установки из msi-файла

Выполните следующие файлы:

- kavws.msi – для установки Антивируса;
- kavwstools.msi – для установки консоли Антивируса в MMC.

Чтобы установить Антивирус с параметрами установки по умолчанию; в режиме без взаимодействия с пользователем:

```
msiexec /i kavws.msi /qn
```

Чтобы установить Антивирус с параметрами установки по умолчанию; показать интерфейс установки:

```
msiexec /i kavws.msi /qf
```

Чтобы установить Антивирус с ключом из файла C:\0000000A.key:

```
msiexec /i kavws.msi LICENSEKEYPATH=C:\0000000A.key /qn
```

Чтобы установить Антивирус с предварительной проверкой активных процессов и загрузочных секторов локальных дисков компьютера:

```
msiexec /i kavws.msi PRESCAN=1 /qn
```

Чтобы установить Антивирус, сохранив его файлы в папке назначения C:\WSEE:

```
msiexec /i kavws.msi INSTALLDIR=C:\WSEE /qn
```

Чтобы установить Антивирус; сохранить файл журнала установки с именем kavws.log в папке, в которой хранится msi-файл инсталляционного пакета Антивируса:

```
msiexec /i kavws.msi /l*v kavws.log /qn
```

Чтобы установить консоль Антивируса в ММС:

```
msiexec /i kavwstools.msi /qn
```

6.2.2. Действия после установки Антивируса

Если, устанавливая Антивирус, вы указали файл ключа и выбрали **Включить постоянную защиту**, сразу после установки Антивирус проверяет объекты файловой системы сервера при доступе к ним, а также проверяет программный код запускаемых скриптов. Каждую пятницу в 20:00 Антивирус запускает полную проверку сервера.

После установки Антивируса рекомендуется выполнить следующие действия:

- **запустить задачу обновления баз Антивируса**. После установки Антивирус проверяет объекты с использованием баз, которые входили в его состав при поставке. Рекомендуется сразу же обновить базы Антивируса. Для этого вам нужно запустить задачу **Обновление баз приложения**. Далее обновление баз будет выполняться каждый час согласно расписанию, установленному по умолчанию.

  Вы можете запустить задачу **Обновление баз приложения**, выполнив следующую команду:

  ```
  KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080
  /AUTHTYPE:1 /PROXYUSER:inetuser /PROXYPWD:123456
  ```

  – чтобы получить обновления баз Антивируса с серверов обновлений «Лаборатории Касперского»; соединиться с источником обновлений через прокси-сервер (адрес прокси-сервера:

proxy.company.com, порт: 8080); использовать для доступа к серверу встроенную проверку подлинности Microsoft Windows (NTLM-authentication) под учетной записью (имя пользователя: inetuser; пароль: 123456).

Подробнее об управлении Антивирусом из командной строки читайте в документе «Антивирус Касперского 6.0 для Windows Servers Enterprise Edition. Руководство администратора».

- **запустить полную проверку сервера**, если перед установкой Антивируса на защищаемом сервере не было установлено антивирусного приложения с включенной функцией постоянной защиты файлов.

  Например, вы можете выполнить следующую команду:

  `KAVSHELL FULLSCAN /W:fullscan.log` – чтобы выполнить задачу проверки по требованию **Полная проверка компьютера**; сохранить отчет о событиях задачи в файле fullscan.log в текущей папке.

  Полная проверка сервера может занять длительное время.

- **настроить уведомления администратора о событиях Антивируса** (см. документ «Антивирус Касперского 6.0 для Windows Servers Enterprise Edition. Руководство администратора»).

6.3. Добавление и удаление компонентов. Примеры команд

Если Антивирус уже установлен и вы выполняете добавление компонентов, перечислите в списке значений ключа ADDLOCAL не только коды компонентов, которые вы хотите установить, но и коды компонентов, которые уже установлены. Иначе уже установленные компоненты будут удалены.

Описание программных компонентов Антивируса и их коды приводятся в п. 3.4 на стр. 21.

Примечание

Компонент «Антивирус Касперского 6.0» (Core) устанавливается автоматически. Вам нет необходимости указывать его в списке значений ключа ADDLOCAL, добавляя или удаляя компоненты Антивируса.

Чтобы добавить компонент «Проверка скриптов» (ScriptChecker) к установленным компонентам «Антивирус Касперского 6.0» (Core) и «Постоянная защита» (Oas), выполните следующую строку:

```
msiexec /i kavws.msi ADDLOCAL=Oas,ScriptChecker /qn
```

или

```
\x86\server\setup.exe /s /p"ADDLOCAL=Oas,ScriptChecker"
\x64\server\setup.exe /s /p"ADDLOCAL=Oas,ScriptChecker"
```

6.4. Удаление Антивируса. Примеры команд

Из командной строки вы можете удалить Антивирус с компьютера.

Чтобы удалить Антивирус с защищаемого сервера:

```
msiexec /x kavws.msi
```

Чтобы удалить консоль Антивируса в MMC:

```
msiexec /x kavwstools.msi
```

ГЛАВА 7. УСТАНОВКА И УДАЛЕНИЕ АНТИВИРУСА ЧЕРЕЗ KASPERSKY ADMINISTRATION KIT

В этой главе содержится следующая информация:

- общие сведения об установке Антивируса через Kaspersky Administration Kit (см. п. 7.1 на стр. 98);
- права, необходимые для установки или удаления Антивируса (см. п. на 7.2 стр. 99);
- установка Антивируса (см. п. 7.3 на стр. 100);
- установка консоли Антивируса в MMC (см. п. 7.4 на стр. 110);
- действия после установки Антивируса (см. п. 7.3.2 на стр. 103);
- удаление Антивируса (см. п. 7.5 на стр. 111).

7.1. Общие сведения об установке через Kaspersky Administration Kit

С помощью Консоли администрирования Kaspersky Administration Kit вы можете установить Антивирус:

- **на любое количество компьютеров**;

  Компьютеры, на которые вы хотите установить Антивирус, могут быть как в одном домене с Сервером администрирования Kaspersky Administration Kit, так и в другом домене или вообще не принадлежать ни к одному домену.

- **создав и запустив групповую или глобальную задачу удаленной установки**;

Антивирус будет установлен на компьютерах с одинаковыми параметрами установки, указанными вами в задаче.

Вы можете объединить серверы в одну группу администрирования, и создать *групповую* задачу для установки Антивируса на серверах этой группы.

Или вы можете создать *глобальную* задачу удаленной установки. При ее создании вам нужно будет сформировать список компьютеров, на которые Антивирус будет установлен.

- **на основе файла инсталляционного пакета server\kavws.kpd, который входит в комплект поставки Антивируса**.

Вы можете выполнить удаленную установку Антивируса на сервере, не вмешиваясь в работу сервера, то есть без необходимости предварительно перезагружать его или выполнять вход в Microsoft Windows. Этот метод установки называется **Форсированная установка**. Вы также можете выполнить удаленную установку Антивируса на сервер при входе пользователя сервера в Microsoft Windows. Этот метод установки называется **Установка с помощью сценария запуска**. Вы можете установить Антивирус этим методом, если все компьютеры находятся в одном домене (не обязательно в одном домене с Сервером администрирования), указав в задаче удаленной установки учетную запись с правами **Администратор домена** (**Domain Admin**).

7.2. Права для установки или удаления Антивируса

Учетная запись, которую вы укажете в задаче удаленной установки (удаления), должна входить в группу локальных администраторов на каждом из защищаемых серверов во всех случаях, кроме следующих:

- на компьютерах, на которых вы хотите установить Антивирус, уже установлен Агент администрирования Kaspersky Administration Kit (не зависимо от того, в каком домене находятся компьютеры и принадлежат ли они к какому-либо домену);

> **Примечание**
>
> Если Агент администрирования еще не установлен на серверах, то вы можете установить его вместе с Антивирусом с помощью задачи удаленной установки. Для установки Агента администрирования учетная запись, которую вы укажете в задаче, должна входить в группу локальных администраторов на каждом из серверов.

- все компьютеры, на которые вы хотите установить Антивирус, находятся в одном домене с Сервером администрирования и Сервер администрирования зарегистрирован под учетной записью **Администратор домена** (**Domain Admin**) (если она обладает правами локального администратора на компьютерах домена).

В указанных выше случаях в задаче удаленной установки выберите **Учетная запись по умолчанию**.

7.3. Установка Антивируса через Kaspersky Administration Kit

В этом разделе содержится следующая информация:

- процедура установки Антивируса (см. п. 7.3.1 на стр. 100);
- действия после установки (см. п. 7.3.2 на стр. 103).

7.3.1. Процедура установки Антивируса

В этом разделе приводится краткая инструкция по установке Антивируса с помощью задачи удаленной установки Kaspersky Administration Kit.

Примечание

Подробнее о том, как создать инсталляционный пакет и задачу удаленной установки, см. документ «Kaspersky Administration Kit. Руководство по внедрению».

Если вы планируете в дальнейшем управлять Антивирусом через Kaspersky Administration Kit:

- на компьютере, на котором установлена Консоль администрирования Kaspersky Administration Kit, установите плагин управления Антивирусом (файл \plugin\klcfginst.exe комплекта поставки Антивируса);
- если на защищаемых серверах не установлен Агент администрирования Kaspersky Administration Kit, вы можете установить его вместе с Антивирусом в задаче удаленной установки.

Вы также можете предварительно объединить серверы в группу администрирования, чтобы в дальнейшем управлять параметрами защиты с помощью групповых политик Kaspersky Administration Kit.

Чтобы установить Антивирус с помощью задачи удаленной установки (краткая инструкция):

1. В Консоли администрирования в узле **Удаленная установка** создайте новый инсталляционный пакет, указав в качестве файла инсталляционного пакета файл kavws.kpd комплекта поставки.

2. Если требуется, в свойствах созданного инсталляционного пакета измените набор устанавливаемых компонентов Антивируса и / или параметры установки. По умолчанию будут установлены все программные компоненты Антивируса (см. п. 3.4.1 на стр. 22) с параметрами установки, описанными в п. 3.5 на стр. 24.

   В консоли администрирования выберите узел **Удаленная установка**, в панели результатов откройте контекстное меню на созданном инсталляционном пакете Антивируса и выберите команду **Свойства**. В диалоговом окне **Инсталляционный пакет** на закладке **Настройка** (см. рис. 42) выполните следующие действия:

   а) В группе параметров **Устанавливаемые компоненты** установите флажки рядом с названиями компонентов Антивируса, которые вы хотите установить.

   б) Чтобы указать папку назначения, отличную от папки, установленной по умолчанию, укажите имя папки и путь к ней в поле **Папка назначения**.

      Путь к папке назначения может содержать переменные окружения. Если указанной папки не существует на сервере, она будет создана. Подробнее о параметре читайте в таблице 4 на стр. 25.

   в) В группе параметров **Дополнительные параметры** выберите:

      - выполнить / не выполнять антивирусную проверку компьютеров перед установкой;
      - включить / не включать постоянную защиту файлов и проверку скриптов после установки;
      - исключить / не исключать из области защиты объекты на сервере, которые рекомендует исключать корпорация Майкрософт;
      - добавить / не добавлять в список правил исключений доверенной зоны угрозы с маской названия not-a-virus:RemoteAdmin*.

   г) Если вы хотите импортировать параметры Антивируса из существующего конфигурационного XML-файла, созданного в Антивирусе Касперского 6.0 для Windows Servers Enterprise

Edition текущей версии, версии 6.0.0.454 или версии 6.0.1.511, укажите конфигурационный файл в поле **Конфигурационный файл**.

Подробнее о параметре читайте в таблице 4 на стр. 25.

д) В диалоговом окне **Инсталляционный пакет** нажмите на кнопку **ОК**.

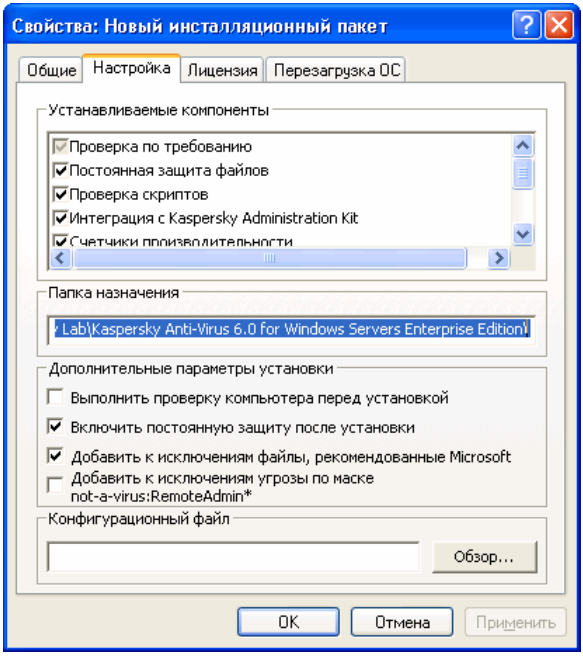

Рисунок 42. Диалоговое окно **Свойства инсталляционного пакета**, закладка **Настройка**

3. Создайте задачу удаленной установки Антивируса на выбранные компьютеры (группу). В задаче:

   - выберите инсталляционный пакет Антивируса, созданный на основе файла kavws.kpd;
   - если вы планируете в дальнейшем управлять Антивирусом через Kaspersky Administration Kit и Агент администрирования Kaspersky Administration Kit еще не установлен на серверах, вы можете установить его сейчас: в окне **Дополнительно** мастера установите флажок **Установить совместно с Агентом администрирования**.

- выберите нужный метод установки:
  - чтобы выполнить установку без необходимости предварительно перезагружать сервер или выполнять вход в Microsoft Windows, укажите метод установки **Форсированная установка**;
  - чтобы выполнить установку при входе пользователя сервера в Microsoft Windows, укажите метод установки **Установка с помощью сценария запуска**;

> **Примечание**
>
> Вы можете выполнить установку методом **Установка с помощью сценария запуска**, только если все компьютеры, на которые вы хотите установить Антивирус, находятся в одном домене (не обязательно в одном домене с Сервером администрирования), указав в задаче удаленной установки учетную запись с правами **Администратор домена** (**Domain Admin**).

- если вы выбрали режим **Установка с помощью сценария запуска**, в окне **Настройки** укажите пользователей компьютеров, при входе которых в Microsoft Windows будет выполняться установка Антивируса;
- в окне **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача. Если вы выбрали режим **Установка с помощью сценария запуска**, укажите учетную запись с правами **Администратор домена** (**Domain Admin**): под этой учетной записью Kaspersky Administration Kit изменит сценарий запуска компьютеров пользователей, указанных вами в окне **Настройки**.

4. Запустите созданную задачу удаленной установки. Антивирус будет установлен на указанные в задаче компьютеры.

О том, какие действия рекомендуется выполнить после завершения установки, см. п. 7.3.2 на стр. 103.

О том, как проверить работу функций Антивируса перед его использованием, рассказывает Глава 9 на стр. 116.

7.3.2. Действия после установки Антивируса

После установки Антивируса рекомендуется обновить базы Антивируса на серверах, а также выполнить полную проверку серверов, если до установки

Антивируса на серверах не были установлены антивирусные приложения с включенной функцией постоянной защиты файлов. Вы можете выполнить следующие шаги.

Таблица 15. Действия после установки Антивируса через Kaspersky Administration Kit

Шаг	Действие
Шаг 1	Создайте новую политику для группы серверов: в мастере создания новой политики установите в качестве источника обновлений Сервер администрирования, определите единые параметры безопасности для задач проверки по требованию (см. п. 7.3.2.1 на стр. 104).
Шаг 2	В свойствах созданной политики на закладке **Системные задачи** отключите запуск по расписанию системных задач проверки по требованию на серверах группы (см. п. 7.3.2.2 на стр. 105).
Шаг 3	Создайте групповую задачу **Обновление баз приложения** (см. п. 7.3.2.3 на стр. 106). Запустите ее. Перед запуском задачи убедитесь, что приложение Kaspersky Administration Kit получает обновления баз типов «Сигнатуры угроз» и «Дополнительный список отозванных лицензий»: в Консоли Администрирования откройте контекстное меню на узле **Обновление**, выберите команду **Параметры получения обновлений** и нажмите на кнопку **Состав обновлений** в диалоговом окне **Свойства**, чтобы открыть диалоговое окно **Состав обновлений**.
Шаг 4	Создайте групповую задачу проверки по требованию со статусом «Задача полной проверки компьютера» (см. п. 7.3.2.4 на стр. 108). Приложение Kaspersky Administration Kit будет оценивать состояние безопасности каждого сервера группы по результатам выполнения этой задачи, а не системной задачи **Полная проверка компьютера**. Запустите задачу.

Вы можете также настроить уведомления администратора о событиях Антивируса (см. документ «Антивирус Касперского 6.0 для Windows Servers Enterprise Edition. Руководство администратора»).

7.3.2.1. Создание политики

Чтобы создать политику для группы серверов, на которых установлен Антивирус:

1. Предварительно объедините защищаемые серверы в группу администрирования.

2. В дереве Консоли администрирования разверните узел **Группы**, а затем разверните группу администрирования, для серверов которой вы хотите создать политику.
3. В контекстном меню вложенного узла **Политики** выберите команду **Создать → Политику**.

   Откроется окно мастера создания политик.
4. В окне **Имя политики** в поле ввода введите имя создаваемой политики (оно не может содержать символы **" * < : > ? \ / |**).
5. В окне **Приложение** в списке **Приложение** выберите **Антивирус Касперского 6.0 для Windows Servers Enterprise Edition**.
6. В окне **Создание политики** выберите **Активная политика**, чтобы политика вступила в действие сразу после ее создания.
7. В окне **Постоянная защита** нажмите на кнопку **Далее** (вы сможете определить параметры постоянной защиты в политике позже).
8. В окне **Проверка по требованию** установите замок  , чтобы определить политикой значения параметров безопасности в задачах проверки по требованию. По умолчанию установлен уровень безопасности **Рекомендуемый**.
9. В окне **Обновление** выберите **Сервер администрирования Kaspersky Administration Kit** в качестве источника обновлений и установите замок  .
10. Нажмите на кнопку **Завершить** в окне **Завершение работы мастера создания политики**.

7.3.2.2. Отключение запуска по расписанию системных задач проверки по требованию на серверах группы

Чтобы отключить запуск по расписанию системных задач проверки по требованию на серверах группы:

1. В дереве Консоли администрирования разверните узел **Группы**, разверните группу серверов, на которых вы установили Антивирус, и разверните вложенный узел **Политики**.
2. В панели результатов откройте контекстное меню на названии созданной политики и выберите команду **Свойства**.

3. В диалоговом окне **Свойства политики** откройте закладку **Системные задачи** и в группе параметров **Запуск системных задач** снимите флажок **Задачи проверки по требованию**.

4. Нажмите на кнопку **ОК**.

7.3.2.3. Создание и запуск групповой задачи *Обновление баз приложения*

После того как вы определили политикой источник обновлений, создайте групповую задачу **Обновление баз приложения** и запустите ее. Создавая задачу, вы можете настроить ее запуск по расписанию с частотой **Запускать задачу при получении обновлений сервером администрирования**.

Чтобы создать групповую задачу обновления баз:

1. Запустите мастер создания групповых задач: в дереве Консоли администрирования выберите группу, для серверов которой вы хотите создать задачу, откройте контекстное меню на вложенной папке **Групповые задачи** и выберите команду **Создать** → **Задачу**.

2. В окне **Имя задачи** мастера создания задач введите имя задачи, например, **Обновление баз на серверах группы**.

3. В окне **Приложение** в списке **Приложение** выберите **Антивирус Касперского 6.0 для Windows Servers Enterprise Edition**, в списке **Тип задачи** выберите тип создаваемой задачи **Обновление баз приложения**.

4. В окне **Расписание** (см. рис. 43) настройте запуск задачи сразу после получения обновлений сервером Администрирования: установите флажок **Запускать задачу по расписанию** и выберите **Запускать задачу при получении обновлений Сервером администрирования** в списке **Частота запуска**.

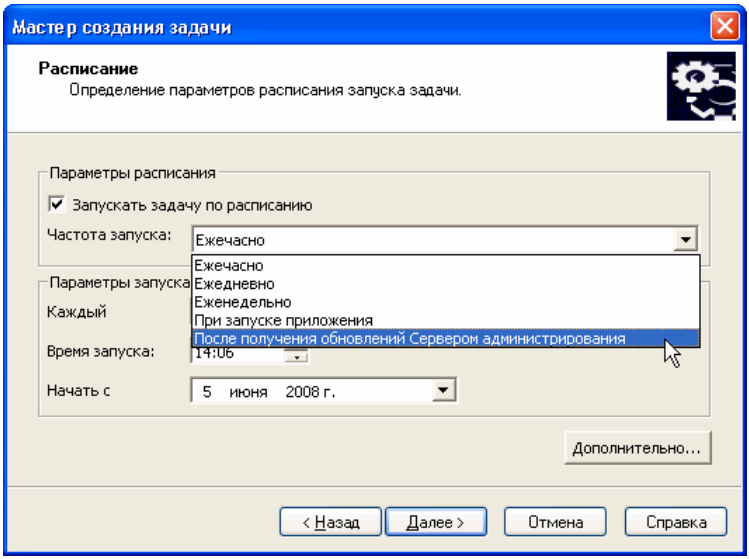

Рисунок 43. Окно **Расписание**

5. В окне **Завершение работы** мастера создания задач нажмите на кнопку **Готово**.

Созданная задача отобразится в диалоговом окне **Задачи**. Запустите ее.

Примечание

Перед запуском задачи убедитесь, что приложение Kaspersky Administration Kit получает обновления баз типов «Сигнатуры угроз» и «Дополнительный список отозванных лицензий»: в Консоли Администрирования откройте контекстное меню на узле **Обновление**, выберите команду **Параметры получения обновлений** и нажмите на кнопку **Состав обновлений** в диалоговом окне **Свойства**, чтобы открыть диалоговое окно **Состав обновлений**.

7.3.2.4. Создание и запуск групповой задачи проверки серверов и присвоение ей статуса «Задача полной проверки компьютера»

Чтобы создать групповую задачу полной проверки серверов в Консоли администрирования и присвоить ей статус «Задача полной проверки компьютера»:

1. Запустите мастер создания групповых задач: в дереве Консоли администрирования выберите группу, для серверов которой вы хотите создать задачу, откройте контекстное меню на вложенной папке **Групповые задачи** и выберите команду **Создать** → **Задачу**;
2. В окне **Имя задачи** мастера создания задач введите имя задачи, например, **Полная проверка серверов группы**.
3. В окне **Приложение** в списке **Приложение** выберите **Антивирус Касперского 6.0 для Windows Servers Enterprise Edition**; в группе параметров **Тип задачи** выберите тип создаваемой задачи: **Проверка по требованию**.
4. В окне **Область проверки** сформируйте область проверки.

   По умолчанию в область проверки входит предопределенная область **Мой компьютер**. Она включает все объекты файловой системы сервера (см. рис. 44).

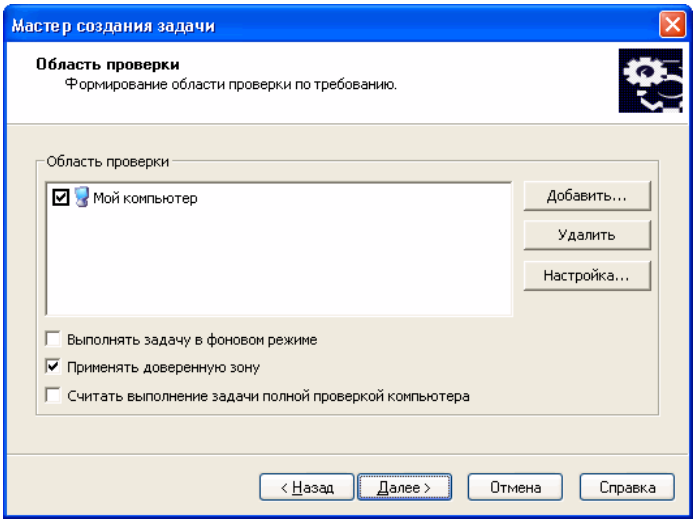

Рисунок 44. Окно **Настройка** мастера создания задач

5. В окне **Настройка** установите флажок **Считать выполнение задачи полной проверкой сервера**.

6. В окне **Расписание** настройте параметры расписания задачи:

   а) Установите флажок **Запускать задачу по расписанию**.

   б) Укажите частоту запуска задачи, например, чтобы выполнять задачу один раз в неделю, выберите **Еженедельно** в списке **Частота запуска** и укажите значение **1** в поле **Каждые <количество> недель** в группе параметров **Параметры запуска задачи**. Укажите, по каким дням недели будет запускаться задача (по умолчанию задача будет запускаться по понедельникам).

   в) В поле **Время запуска** укажите время запуска задачи.

   г) В поле **Начать с** укажите текущую дату в качестве даты начала действия расписания.

   д) Нажмите на кнопку **ОК**.

7. В окне **Завершение работы** мастера создания задач нажмите на кнопку **Готово**.

Созданная задача отобразится в диалоговом окне **Задачи**. Запустите ее.

7.4. Установка консоли Антивируса в ММС

В этом разделе приводится краткая инструкция по установке консоли Антивируса в ММС с помощью задачи удаленной установки Kaspersky Administration Kit.

Примечание

Подробнее о том, как создать инсталляционный пакет и задачу удаленной установки, см. документ «Kaspersky Administration Kit. Руководство по внедрению».

Чтобы установить консоль Антивируса в ММС с помощью задачи удаленной установки (краткая инструкция):

1. В Консоли администрирования в узле **Удаленная установка** создайте новый инсталляционный пакет на основе файла client\setup.exe. Создавая новый инсталляционный пакет:

   - в окне **Приложения** выберите **Создать инсталляционный пакет для приложения, указанного пользователем** и выберите файл client\setup.exe из папки комплекта поставки, соответствующей разрядности установленной Microsoft Windows (папка x86\ – для 32-разрядной Microsoft Windows; папка x64\ – для 64-разрядной Microsoft Windows).

     Если требуется, в поле **Параметры запуска исполняемого файла** измените состав устанавливаемых компонентов набора с помощью ключа ADDLOCAL службы Windows Installer (см. описание программных компонентов Антивируса в п. 3.4.1 на стр. 22) и измените папку назначения.

     Например, введите строку:

     ```
     /s /p"ADDLOCAL=Core
     INSTALLDIR=C:\KasperskyConsole"
     ```

     чтобы установить только консоль Антивируса в ММС, не устанавливая файл справки и документацию; сохранить файлы консоли Антивируса в папке C:\Kaspersky Console.

2. Создайте задачу удаленной установки консоли Антивируса на выбранные компьютеры (группу). В задаче:

   - выберите инсталляционный пакет, созданный на основе файла client\setup.exe.

- В окне **Метод установки** выберите метод установки:
  - чтобы выполнить установку без необходимости предварительно перезагружать сервер или выполнять вход в Microsoft Windows, выберите **Форсированная установка**;
  - чтобы выполнить установку при входе в Microsoft Windows, выберите **Установка с помощью сценария запуска**.

> **Примечание**
>
> Вы можете выполнить установку методом **Установка с помощью сценария запуска**, только если все компьютеры, на которые вы хотите установить Антивирус, находятся в одном домене (не обязательно в одном домене с Сервером администрирования), указав в задаче удаленной установки учетную запись с правами **Администратор домена** (**Domain Admin**).

- Если вы выбрали режим **Установка с помощью сценария запуска**, в окне **Настройки** укажите пользователей компьютеров, при входе которых в Microsoft Windows будет выполняться установка консоли.
- В окне **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача (если вы выбрали режим **Установка с помощью сценария запуска**, укажите учетную запись с правами **Администратор домена** (**Domain Admin**): под этой учетной записью Kaspersky Administration Kit изменит сценарий запуска компьютеров пользователей, указанных вами в окне **Настройки**).

3. Запустите созданную задачу удаленной установки. Консоль Антивируса в MMC будет установлена на указанные в задаче компьютеры.

7.5. Удаление Антивируса через Kaspersky Administration Kit

Чтобы удалить Антивирус, в Консоли администрирования Kaspersky Administration Kit создайте и запустите задачу удаления приложений.

В задаче выберите нужный метод удаления (так же, как вы выбирали метод установки; см. предыдущий пункт) и укажите учетную запись, под которой Сервер администрирования будет обращаться к компьютерам (см. п. 7.2 на стр. 99). Вы можете удалить Антивирус только с параметрами удаления по умолчанию (см. п. 3.5 на стр. 24).

ГЛАВА 8. УСТАНОВКА И УДАЛЕНИЕ АНТИВИРУСА ЧЕРЕЗ ГРУППОВЫЕ ПОЛИТИКИ ACTIVE DIRECTORY

В этой главе содержится следующая информация:

- установка Антивируса через групповые политики Active Directory (см. п. 8.1 на стр. 112);
- удаление Антивируса через групповые политики Active Directory (см. п. на 8.3 стр. 114).

8.1. Установка через групповые политики Active Directory

Вы можете установить Антивирус на многих серверах через новую или существующую групповую политику Active Directory. Таким же образом вы можете установить консоль Антивируса в MMC.

Чтобы установить Антивирус, используйте файл инсталляционного пакета kavws.msi, чтобы установить консоль Антивируса в MMC, используйте файл kavwstools.msi.

Компьютеры, на которых вы хотите установить Антивирус (консоль Антивируса в MMC), должны удовлетворять следующим условиям:

- все компьютеры должны быть в одном домене и в одной организационной единице;
- операционные системы на компьютерах должны быть одной разрядности (32-разрядные или 64-разрядные).

Примечание

Вы должны обладать правами администратора на контроллере домена, с которого вы планируете установить Антивирус или его консоль в MMC.

Общие рекомендации по установке:

- Предварительно проверьте настройки DNS-сервера. С помощью команды ping с каждого сервера свяжитесь с контроллером домена и наоборот, с контроллера домена свяжитесь с каждым сервером.
- Сохраните msi-файл инсталляционного пакета, соответствующий разрядности установленной версии Microsoft Windows, в папке общего доступа на контроллере домена, с которого вы будете устанавливать Антивирус на серверах. Вы можете сохранить файл в папке общего доступа по умолчанию на контроллере домена или создать новую.

Примечание

Подробнее о том, как выполнить следующие шаги, см. документацию, предоставляемую корпорацией Майкрософт.

Чтобы установить Антивирус (консоль Антивируса в MMC) (краткая инструкция):

1. На контроллере домена в консоли **Active Directory – пользователи и компьютеры** создайте новую политику для группы, в которую объединены серверы.
2. С помощью **Group Policy Object Editor** создайте новый инсталляционный пакет в узле **Конфигурация компьютеров**. Укажите путь к msi-файлу инсталляционного пакета Антивируса (консоли Антивируса в MMC) в формате UNC (Universal Naming Convention).
3. Установите флажок **Always install with elevated privileges** службы Windows Installer, как в узле **Конфигурация компьютеров**, так и в узле **Конфигурация пользователей** выбранной группы.
4. Примените изменения с помощью одной из следующих команд:
   - gpupdate /force – для Microsoft Windows 2003 и выше;
   - secedit /refreshpolicy machine_policy – для Microsoft Windows Server 2000.

Антивирус будет установлен на компьютерах группы после их перезагрузки, перед входом в Microsoft Windows.

8.2. Действия после установки Антивируса

После установки Антивируса на защищаемых серверах рекомендуется сразу обновить базы Антивируса и выполнить полную проверку сервера. Вы можете выполнить эти действия из консоли Антивируса в MMC (см. п. 5.1.3 на стр. 76).

Вы можете также настроить уведомления администратора о событиях Антивируса (см. документ «Антивирус Касперского 6.0 для Windows Servers Enterprise Edition. Руководство администратора»).

8.3. Удаление через групповые политики Active Directory

Если вы устанавливали Антивирус (консоль Антивируса в MMC) на компьютерах группы, используя групповую политику Active Directory, вы можете использовать эту политику, чтобы удалить Антивирус (консоль Антивируса в MMC).

Вы можете выполнить удаление только с параметрами удаления по умолчанию (они приводятся в п. 3.5 на стр. 24).

Примечание

Подробнее о том, как выполнить следующие шаги, см. документацию, предоставляемую корпорацией Майкрософт.

Чтобы удалить Антивирус (консоль Антивируса в MMC) (краткая инструкция):

1. На контроллере домена, в консоли **Active Directory – пользователи и компьютеры**, выберите организационную единицу, с компьютеров которой вы хотите удалить Антивирус или консоль Антивируса в MMC.
2. Выберите политику, созданную для установки Антивируса, и в **Редакторе групповых политик**, в узле **Software Installation** (**Конфигурация компьютеров** → **Конфигурация программ** → **Software Installation**) откройте контекстное меню на инсталляционном пакете Антивируса (консоли Антивируса в MMC) и выберите команду **Все задачи** → **Удалить**.

3. Выберите метод удаления **Немедленно удалить программу со всех компьютеров**.
4. Примените изменения с помощью одной из следующих команд:
   - gpupdate /force – для Microsoft Windows Server 2003 и выше;
   - secedit /refreshpolicy machine_policy – для Microsoft Windows Server 2000.

Антивирус будет удален с компьютеров после их перезагрузки, перед входом в Microsoft Windows.

ГЛАВА 9. ПРОВЕРКА РАБОТОСПОСОБНОСТИ АНТИВИРУСА. ИСПОЛЬЗОВАНИЕ ТЕСТОВОГО ВИРУСА EICAR

В этой главе содержится следующая информация:

- о тестовом вирусе EICAR (см. п. 9.1 на стр. 116);
- проверка функций Антивируса «Постоянная защита» и «Проверка по требованию» (см. п. 9.2 на стр. 118).

9.1. О тестовом вирусе EICAR

Тестовый вирус предназначен для проверки работы антивирусных приложений. Он разработан организацией The European Institute for Computer Antivirus Research (EICAR).

Примечание

Тестовый вирус не является вирусом и не содержит программного кода, который может нанести вред вашему компьютеру, но антивирусные приложения большинства производителей идентифицируют в нем угрозу.

Файл, который содержит тестовый вирус, называется eicar.com. Вы можете загрузить его со страницы http://www.eicar.org/anti_virus_test_file.htm сайта **EICAR**.

Примечание

Перед сохранением файла в папке на диске компьютера убедитесь, что постоянная антивирусная защита файлов в этой папке отключена.

Файл eicar.com содержит текстовую строку. При проверке файла Антивирус обнаруживает в этой текстовой строке «угрозу», присваивает файлу статус **Зараженный** и удаляет его. Информация об обнаруженной в файле угрозе

появляется в консоли MMC Антивируса, в подробном отчете о выполнении задачи.

Вы также можете использовать файл eicar.com, чтобы проверить, как Антивирус выполняет лечение зараженных объектов и как он обнаруживает подозрительные и потенциально опасные объекты. Для этого откройте файл с помощью текстового редактора, добавьте к началу текстовой строки в файле один из префиксов, перечисленных в таблице 16, и сохраните файл под новым именем, например, eicar_cure.com.

Примечание

Для того чтобы Антивирус обработал файл eicar.com с префиксом, установите параметр безопасности **Проверяемые объекты** в задаче Антивируса **Постоянная защита файлов** / задаче проверки по требованию в значение **Все объекты**. См. инструкцию в документе «Антивирус Касперского 6.0 для Windows Servers Enterprise Edition. Руководство администратора».

Таблица 16. Префиксы

Префикс	Статус файла после проверки и действие Антивируса
Без префикса	Антивирус присваивает объекту статус **Зараженный** и удаляет его.
SUSP–	Антивирус присваивает объекту статус **Подозрительный** (обнаружен с помощью эвристического анализатора) и удаляет его (подозрительные объекты не подвергаются лечению).
WARN–	Антивирус присваивает объекту статус **Подозрительный** (код объекта частично совпадает с кодом известной угрозы) и удаляет его (подозрительные объекты не подвергаются лечению).
CURE–	Антивирус присваивает объекту статус **Зараженный** и лечит его. Если лечение успешно, весь текст в файле заменяется словом «CURE».

9.2. Проверка функций Антивируса «Постоянная защита» и «Проверка по требованию»

После установки Антивируса вы можете проверить, как Антивирус обнаруживает объекты, содержащие вредоносный код. Для проверки вы можете использовать тестовый «вирус» **EICAR** (подробнее о тестовом вирусе **EICAR** – см. п. 9.1 на стр. 116).

В этом разделе рассказывается о том, как проверить функции Антивируса «Постоянная защита» и «Проверка по требованию» через консоль Антивируса в ММС.

Чтобы проверить функцию «Постоянная защита»:

1. Загрузите файл eicar.com со страницы сайта **EICAR** http://www.eicar.org/anti_virus_test_file.htm. Сохраните его в папке общего доступа на локальном диске любого из компьютеров локальной сети.

   Примечание

   Перед сохранением файла в папке убедитесь, что постоянная антивирусная защита файлов в этой папке отключена.

2. Если вы хотите также проверить работу уведомлений пользователей сети, убедитесь в том, что и на защищаемом сервере, и на компьютере, на котором вы сохранили файл eicar.com, включена Служба сообщений Microsoft Windows.

3. Откройте консоль Антивируса в ММС (подробнее о том, как открыть консоль Антивируса в ММС, читайте в п. 5.1.3.1 на стр. 76).

4. Если при установке Антивируса вы не выбрали **Включить постоянную защиту после установки**, то включите ее сейчас. Для этого в дереве консоли разверните узел **Постоянная защита**, откройте контекстное меню на узле **Постоянная защита файлов** и выберите команду **Запустить** (подробнее см. справку консоли Антивируса).

5. Скопируйте сохраненный файл eicar.com на локальный диск защищаемого сервера одним из следующих способов:

   - чтобы проверить работу уведомлений через окно Службы терминалов, скопируйте файл eicar.com на сервер, подключив-

шись к консоли сервера с помощью программы «Подключение к удаленному рабочему столу» (Remote Desktop Connection);

- чтобы проверить работу уведомлений через Службу сообщений Microsoft Windows, скопируйте файл eicar.com с компьютера, на котором вы его сохранили, через сетевое окружение этого компьютера.

Постоянная защита файлов работает должным образом, если:

- файл eicar.com удален с диска защищаемого сервера;
- в консоли Антивируса сводный отчет о выполнении задачи получил статус **Критический**  . В подробном отчете о выполнении задачи появилась строка с информацией об угрозе в файле eicar.com (чтобы просмотреть сводный отчет, в дереве консоли выберите узел **Отчеты**; чтобы просмотреть подробный отчет, откройте контекстное меню на сводном отчете о задаче **Постоянная защита файлов** и выберите команду **Просмотреть отчет**).
- появилось сообщение Службы сообщений Microsoft Windows на компьютере, с которого вы скопировали файл (Службы терминалов в терминальной сессии на сервере) следующего содержания: «**Антивирус Касперского заблокировал доступ к <путь к файлу eicar.com на сервере>\eicar.com на компьютере <сетевое имя сервера> в <время возникновения события>. Причина: Обнаружена угроза. Вирус: EICAR-Test-File. Имя пользователя объекта: <имя пользователя>. Имя компьютера пользователя объекта: <сетевое имя компьютера, с которого вы скопировали файл>**».

> **Примечание**
>
> Убедитесь, что Службы сообщений Microsoft Windows работает на компьютере, с которого вы скопировали файл eicar.com.

Чтобы проверить функцию «Проверка по требованию»:

1. Загрузите файл eicar.com со страницы сайта **EICAR**, http://www.eicar.org/anti_virus_test_file.htm. Сохраните его в папке общего доступа на локальном диске любого из компьютеров локальной сети.

> **Примечание**
>
> Перед сохранением файла в папку убедитесь, что постоянная антивирусная защита файлов в этой папке отключена.

2. Запустите консоль Антивируса в ММС.

3. В консоли Антивируса выполните следующие действия:

   а) В дереве консоли разверните узел **Проверка по требованию**.

   б) Щелкните на задаче **Полная проверка компьютера**.

   в) В панели результатов, в дереве файловых ресурсов сервера снимите флажок с узла **Мой компьютер**.

   г) Откройте контекстное меню на узле **Мой компьютер** и выберите команду **Добавить объект сетевого ресурса**. В дереве отобразится узел **Сетевое окружение** и вложенный узел для нового сетевого пути.

   д) Введите сетевой путь к файлу eicar.com на удаленном компьютере в формате UNC (Universal Naming Convention) и нажмите <**ENTER**>. Сетевой путь будет добавлен.

   е) Установите флажок, чтобы включить добавленный сетевой путь в область проверки.

   ж) Откройте контекстное меню на задаче **Полная проверка компьютера** и выберите команду **Запустить**.

Проверка по требованию работает должным образом, если:

- файл eicar.com удален с диска компьютера;
- в консоли Антивируса сводный отчет о выполнении задачи получил статус **Критический**  ; в подробном отчете о выполнении задачи появилась строка с информацией об угрозе в файле eicar.com (чтобы просмотреть сводный отчет, в дереве консоли выберите узел **Отчеты**, чтобы просмотреть подробный отчет, в узле **Отчеты** откройте контекстное меню на сводном отчете о задаче **Полная проверка компьютера** и выберите команду **Просмотреть отчет**).

ПРИЛОЖЕНИЕ А. ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

А.1. Общие сведения о 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, 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), F-Secure (Финляндия), Aladdin (Израиль), Sybari (США), G Data (Германия), Deerfield (США), Alt-N (США), Microworld (Индия), BorderWare (Канада).

Клиенты «Лаборатории Касперского» обеспечиваются широким спектром дополнительных услуг, гарантирующих бесперебойную работу продуктов и точное соответствие любым специфическим бизнес-требованиям. Мы проектируем, внедряем и сопровождаем корпоративные антивирусные комплексы. Наши базы обновляются каждый час. Мы обеспечиваем наших пользователей круглосуточной технической поддержкой на нескольких языках.

A.2. Другие разработки «Лаборатории Касперского»

Новостной Агент «Лаборатории Касперского»

Программа Новостной Агент предназначена для оперативной доставки новостей «Лаборатории Касперского», оповещения о «вирусной погоде» и появлении свежих новостей. С заданной периодичностью программа считывает с новостного сервера «Лаборатории Касперского» список доступных новостных каналов и содержащуюся в них информацию.

Новостной Агент также позволяет:

- визуализировать в области уведомлений панели задач состояние «вирусной погоды»;
- подписываться и отказываться от подписки на новостные каналы «Лаборатории Касперского»;
- получать с заданной периодичностью новости по каждому подписанному каналу; также осуществляется оповещение о появлении непрочитанных новостей;
- просматривать новости по подписанным каналам;
- просматривать списки каналов и их состояние;
- открывать в браузере страницы с подробным текстом новостей.

Новостной Агент работает под управлением операционной системы Microsoft Windows и может использоваться как отдельная программа, так и

входить в состав различных интегрированных решений «Лаборатории Касперского».

Kaspersky® OnLine Scanner

Программа представляет собой бесплатный сервис, доступный посетителям веб-сайта компании, позволяющий произвести эффективную антивирусную проверку компьютера в онлайн-режиме. Kaspersky OnLine Scanner выполняется в браузере. Таким образом, пользователи могут максимально оперативно получать ответ на вопросы, связанные с заражением вредоносными программами. В рамках проверки пользователь может:

- исключать архивы и почтовые базы из проверки;
- выбирать для проверки стандартные / расширенные базы;
- сохранять отчеты о результатах проверки в форматах txt и html.

Kaspersky® OnLine Scanner Pro

Программа представляет собой подписной сервис, доступный посетителям веб-сайта компании, позволяющий произвести эффективную антивирусную проверку компьютера и лечение зараженных файлов в онлайн-режиме. Kaspersky OnLine Scanner Pro выполняется в браузере. В рамках проверки пользователь может:

- исключать архивы и почтовые базы из проверки;
- выбирать для проверки стандартные / расширенные базы;
- лечить обнаруженные зараженные объекты;
- сохранять отчеты о результатах проверки в форматах txt и html.

Антивирус Касперского® 6.0

Антивирус Касперского 6.0 предназначен для защиты персонального компьютера от вредоносных программ, оптимально сочетая в себе традиционные методы защиты от вирусов с новыми проактивными технологиями.

Программа позволяет осуществлять комплексную антивирусную проверку, включающую в себя:

- антивирусную проверку почтового трафика на уровне протокола передачи данных (POP3, IMAP и NNTP для входящих сообщений и SMTP – для исходящих) независимо от используемой почтовой программы, а также проверку и лечение почтовых баз;
- антивирусную проверку интернет-трафика, поступающего по HTTP-протоколу, в режиме реального времени;
- антивирусную проверку любых отдельных файлов, папок и дисков. Также, используя предустановленную задачу проверки, можно за-

пустить анализ на присутствие вирусов только критических областей операционной системы и объектов, загружаемых при старте операционной системы Microsoft Windows.

Возможности проактивной защиты включают в себя:

- *Контроль изменений в файловой системе*. Программа позволяет создавать список приложений, компонентный состав которых будет контролироваться. Это помогает предотвратить нарушение целостности приложений вредоносными программами.
- *Наблюдение за процессами в оперативной памяти*. Антивирус Касперского 6.0 своевременно предупреждает пользователя в случае появления опасных, подозрительных или скрытых процессов, а также в случае несанкционированного изменения активных процессов.
- *Мониторинг изменений в реестре операционной системы* благодаря контролю состояния системного реестра.
- *Блокирование опасных макросов* Visual Basic for Applications в документах Microsoft Office.
- *Восстановление системы* после вредоносного воздействия программ-шпионов за счет фиксации всех изменений реестра и файловой системы компьютера и их отката по решению пользователя.

Kaspersky® Internet Security 6.0

Kaspersky Internet Security 6.0 – комплексное решение для защиты персонального компьютера от основных информационных угроз – вирусов, хакеров, спама и шпионских программ. Единый пользовательский интерфейс обеспечивает настройку и управление всеми компонентами решения.

Функции антивирусной защиты включают в себя:

- *антивирусную проверку почтового трафика* на уровне протокола передачи данных (POP3, IMAP и NNTP для входящих сообщений и SMTP для исходящих) независимо от используемой почтовой программы. Для популярных почтовых программ Microsoft Office Outlook, Microsoft Outlook Express и The Bat! предусмотрены плагины и лечение вирусов в почтовых базах;
- *проверку интернет-трафика*, поступающего по HTTP-протоколу, в режиме реального времени;
- *защиту файловой системы*: антивирусной проверке могут быть подвергнуты любые отдельные файлы, папки и диски. Также возможна проверка только критических областей операционной системы и объектов, загружаемых при старте операционной системы Microsoft Windows;

- *проактивную защиту*: программа осуществляет постоянное наблюдение за активностью приложений и процессов, запущенных в оперативной памяти компьютера, предотвращает опасные изменения файловой системы и реестра, а также восстанавливает систему после вредоносного воздействия.

Защита от интернет-мошенничества обеспечивается благодаря распознаванию фишинговых атак, что позволяет предотвратить утечку вашей конфиденциальной информации (в первую очередь паролей, номеров банковских счетов и карт, а также блокированию выполнения опасных скриптов на веб-страницах, всплывающих окон и рекламных баннеров). Функция *блокирования автоматического дозвона на платные ресурсы интернета* помогает идентифицировать программы, которые пытаются использовать ваш модем для скрытого соединения с платными телефонными сервисами, и блокировать их работу.

Kaspersky Internet Security 6.0 *фиксирует попытки сканирования портов вашего компьютера*, часто предшествующие сетевым атакам, и успешно отражает наиболее распространенные типы сетевых атак. На *основе заданных правил* программа осуществляет контроль всех сетевых взаимодействий, отслеживая все *входящие и исходящие пакеты данных*. Режим невидимости *предотвращает обнаружение компьютера извне*. При переключении в этот режим запрещается вся сетевая деятельность, кроме предусмотренных правилами исключений, которые определяются самим пользователем.

В программе применяется комплексный подход к фильтрации входящих почтовых сообщений на наличие спама:

- проверка по «черным» и «белым» спискам адресатов (включая адреса фишинговых сайтов);
- проверка фраз в тексте письма;
- анализ текста письма с помощью самообучающегося алгоритма;
- распознавание спама в виде изображений.

Антивирус Касперского® Mobile

Антивирус Касперского Mobile обеспечивает антивирусную защиту мобильных устройств, работающих под управлением операционных систем Symbian OS и Microsoft Windows Mobile. Программа позволяет осуществлять комплексную антивирусную проверку, включающую в себя:

- *проверку по требованию* памяти мобильного устройства, карт памяти, отдельной папки либо конкретного файла. При обнаружении зараженного объекта он помещается на карантин или удаляется;

- *постоянную защиту*: автоматически проверяются все входящие или изменяющиеся объекты, а также файлы при попытке доступа к ним;
- *защиту от sms- и mms-спама*.

Антивирус Касперского для файловых серверов

Программный продукт обеспечивает надежную защиту файловых систем серверов под управлением операционных систем Microsoft Windows, Novell NetWare, Linux и Samba от всех видов вредоносных программ. В состав программного продукта входят следующие приложения «Лаборатории Касперского»:

- Kaspersky Administration Kit.
- Антивирус Касперского для Windows Server.
- Антивирус Касперского для Linux File Server.
- Антивирус Касперского для Novell Netware.
- Антивирус Касперского для Samba Server.

Преимущества и функциональные возможности:

- *защита файловых систем серверов в режиме реального времени*: все файлы серверов проверяются при попытке их открытия и сохранения на сервере.
- *предотвращение вирусных эпидемий*;
- *проверка по требованию* всей файловой системы или отдельных ее папок и файлов;
- *применение технологий оптимизации* при проверке объектов файловой системы сервера;
- *восстановление системы после заражения*;
- *масштабируемость программного продукта* в пределах доступных ресурсов системы;
- *соблюдение баланса загрузки системы*;
- *формирование списка доверенных процессов*, чья активность на сервере не подвергается контролю со стороны программного продукта;
- *удаленное управление* программным продуктом, включающее централизованную установку, настройку и управление;

- *хранение резервных копий зараженных и удаленных объектов* на тот случай, если потребуется их восстановление;
- *изоляция подозрительных объектов* в специальном хранилище;
- *оповещения о событиях* в работе программного продукта администратора системы;
- *ведение детальных отчетов*;
- *автоматическое обновление баз* программного продукта.

Kaspersky Open Space Security

Kaspersky Open Space Security – это программный продукт, реализующий новый подход к безопасности современных корпоративных сетей любого масштаба, обеспечивающий централизованную защиту информационных систем, а также поддержку удаленных офисов и мобильных пользователей.

Программный продукт включает в себя четыре продукта:

- Kaspersky Work Space Security
- Kaspersky Business Space Security
- Kaspersky Enterprise Space Security
- Kaspersky Total Space Security

Рассмотрим подробнее каждый продукт.

Kaspersky WorkSpace Security – это приложение для централизованной защиты рабочих станций в корпоративной сети и за ее пределами от всех видов современных интернет-угроз: вирусов, шпионских программ, хакерских атак и спама.

Преимущества и функциональные возможности:

- целостная защита от вирусов, шпионских программ, хакерских атак и спама;
- *проактивная защита* от новых вредоносных программ, записи о которых еще не добавлены в базы;
- *персональный сетевой экран* с системой обнаружения вторжений и предупреждения сетевых атак;
- *отмена вредоносных изменений в системе*;
- *защита от фишинг-атак и нежелательной почтовой корреспонденции*;
- *динамическое перераспределение ресурсов* при полной проверке системы;

- *удаленное управление* программным продуктом, включающее централизованную установку, настройку и управление;
- *поддержка Cisco® NAC* (Network Admission Control);
- *проверка электронной почты и интернет-трафика* в режиме реального времени;
- *блокирование всплывающих окон и рекламных баннеров* при работе в интернете;
- *безопасная работа в сетях любого типа*, включая Wi-Fi;
- *средства для создания диска аварийного восстановления*, позволяющего восстановить систему после вирусной атаки;
- *развитая система отчетов* о состоянии защиты;
- *автоматическое обновление баз*;
- *полноценная поддержка 64-битных операционных систем*;
- *оптимизация работы программного продукта на ноутбуках* (технология Intel® Centrino® Duo для мобильных ПК);
- *возможность удаленного лечения* (технология Intel® Active Management, компонент Intel® vPro™).

Kaspersky Business Space Security обеспечивает оптимальную защиту информационных ресурсов компании от современных интернет-угроз. Kaspersky Business Space Security защищает рабочие станции и файловые серверы от всех видов вирусов, троянских программ и червей, предотвращает вирусные эпидемии, а также обеспечивает сохранность информации и мгновенный доступ пользователей к сетевым ресурсам.

Преимущества и функциональные возможности:

- *удаленное управление* программным продуктом, включающее централизованную установку, настройку и управление;
- *поддержка Cisco® NAC* (Network Admission Control);
- *защита рабочих станций и файловых серверов от всех видов интернет-угроз*;
- *использование технологии iSwift для исключения повторных проверок* в рамках сети;
- *распределение нагрузки между процессорами сервера*;
- *изоляция подозрительных объектов* рабочих станций в специальном хранилище;

- *отмена вредоносных изменений в системе*;
- *масштабируемость программного продукта* в пределах доступных ресурсов системы;
- *проактивная защита* рабочих станций от новых вредоносных программ, записи о которых еще не добавлены в базы;
- *проверка электронной почты и интернет-трафика* в режиме реального времени;
- *персональный сетевой экран* с системой обнаружения вторжений и предупреждения сетевых атак;
- *защита при работе в беспроводных сетях* Wi-Fi;
- *технология самозащиты антивируса от вредоносных программ*;
- *изоляция подозрительных объектов* в специальном хранилище;
- *автоматическое обновление баз*.

Kaspersky Enterprise Space Security

Это приложение включает компоненты для защиты рабочих станций и серверов совместной работы от всех видов современных интернет-угроз, удаляет вирусы из потока электронной почты, обеспечивает сохранность информации и мгновенный безопасный доступ пользователей к сетевым ресурсам.

Преимущества и функциональные возможности:

- защита рабочих станций и серверов от вирусов, троянских программ и червей;
- защита почтовых серверов Sendmail, Qmail, Postfix и Exim;
- проверка всех сообщений на сервере Microsoft Exchange, включая общие папки;
- обработка сообщений, баз данных и других объектов серверов Lotus Domino;
- защита от фишинг-атак и нежелательной почтовой корреспонденции;
- предотвращение массовых рассылок и вирусных эпидемий;
- масштабируемость программного продукта в пределах доступных ресурсов системы;
- удаленное управление программным продуктом, включающее централизованную установку, настройку и управление;

- поддержка Cisco® NAC (Network Admission Control);
- проактивная защита рабочих станций от новых вредоносных программ, записи о которых еще не добавлены в базы;
- персональный сетевой экран с системой обнаружения вторжений и предупреждения сетевых атак;
- безопасная работа в беспроводных сетях Wi-Fi;
- проверка интернет-трафика в режиме реального времени;
- отмена вредоносных изменений в системе;
- динамическое перераспределение ресурсов при полной проверке системы;
- изоляция подозрительных объектов в специальном хранилище;
- система отчетов о состоянии системы защиты;
- автоматическое обновление баз.

Kaspersky Total Space Security

Это приложение контролирует все входящие и исходящие потоки данных – электронную почту, интернет-трафик и все сетевые взаимодействия. Продукт включает компоненты для защиты рабочих станций и мобильных устройств, обеспечивает мгновенный и безопасный доступ пользователей к информационным ресурсам компании и сети Интернет, а также гарантирует безопасные коммуникации по электронной почте.

Преимущества и функциональные возможности:

- *целостная защита от вирусов, шпионских программ, хакерских атак и спама* на всех уровнях корпоративной сети: от рабочих станций до интернет-шлюзов;
- *проактивная защита* рабочих станций от новых вредоносных программ, записи о которых еще не добавлены в базы;
- *защита почтовых серверов и серверов совместной работы*;
- *проверка интернет-трафика* (HTTP/FTP), поступающего в локальную сеть, в режиме реального времени;
- *масштабируемость программного продукта* в пределах доступных ресурсов системы;
- *блокирование доступа с зараженных рабочих станций*;
- *предотвращение вирусных эпидемий*;

- *централизованные отчеты о состоянии защиты*;
- *удаленное управление* программным продуктом, включающее централизованную установку, настройку и управление;
- *поддержка Cisco® NAC* (Network Admission Control);
- *поддержка аппаратных прокси-серверов*;
- *фильтрация интернет-трафика* по списку доверенных серверов, типам объектов и группам пользователей;
- *использование технологии iSwift для исключения повторных проверок* в рамках сети;
- *динамическое перераспределение ресурсов* при полной проверке системы;
- *персональный сетевой экран* с системой обнаружения вторжений и предупреждения сетевых атак;
- *безопасная работа пользователей в сетях любого типа*, включая WiFi;
- *защита от фишинг-атак и нежелательной почтовой корреспонденции*;
- *возможность удаленного лечения* (технология Intel® Active Management, компонент Intel® vPro™);
- *отмена вредоносных изменений в системе*;
- *технология самозащиты антивируса от вредоносных программ*;
- *полноценная поддержка 64-битных операционных систем*;
- автоматическое обновление баз.

Kaspersky Security для почтовых серверов

Программный продукт для защиты почтовых серверов и серверов совместной работы от вредоносных программ и спама. Продукт включает в себя приложения для защиты всех популярных почтовых серверов: Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix и Exim, а также позволяет организовать выделенный почтовый шлюз. В состав решения входят:

- Kaspersky Administration Kit;
- Kaspersky Mail Gateway;
- Антивирус Касперского для Lotus Notes/Domino;

- Антивирус Касперского для Microsoft Exchange;
- Антивирус Касперского для Linux Mail Server.

Среди его возможностей:

- *надежная защита от вредоносных и потенциально опасных программ*;
- *фильтрация нежелательной почтовой корреспонденции*;
- *проверка входящих и исходящих почтовых сообщений и вложений*;
- *антивирусная проверка всех сообщений на сервере Microsoft Exchange*, включая общие папки;
- *проверка сообщений, баз данных и других объектов серверов Lotus Notes/Domino*;
- *фильтрация сообщений* по типам вложений;
- *изоляция подозрительных объектов* в специальном хранилище;
- *удобная система управления* программным продуктом;
- *предотвращение вирусных эпидемий*;
- *мониторинг состояния системы защиты* с помощью уведомлений;
- *система отчетов* о работе приложения;
- *масштабируемость программного продукта* в пределах доступных ресурсов системы;
- *автоматическое обновление баз*.

Kaspersky Security для интернет-шлюзов

Программный продукт обеспечивает безопасный доступ к сети Интернет для всех сотрудников организации, автоматически удаляя вредоносные и потенциально опасные программы из потока данных, поступающего в сеть по протоколам HTTP/FTP. В состав продукта входят:

- Kaspersky Administration Kit;
- Антивирус Касперского для Proxy Server;
- Антивирус Касперского для Microsoft ISA Server;
- Антивирус Касперского для Check Point FireWall-1.

Среди его возможностей:

- *надежная защита от вредоносных и потенциально опасных программ*;

- *проверка интернет-трафика* (HTTP/FTP) в режиме реального времени;
- *фильтрация интернет-трафика* по списку доверенных серверов, типам объектов и группам пользователей;
- *изоляция подозрительных объектов* в специальном хранилище;
- *удобная система управления*;
- *система отчетов о работе приложения*;
- *поддержка аппаратных прокси-серверов*;
- *масштабируемость программного продукта* в пределах доступных ресурсов системы;
- *автоматическое обновление баз*.

Kaspersky® Anti-Spam

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

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

Высокая эффективность работы программы достигается благодаря ежедневному автоматическому обновлению баз контентной фильтрации образцами, предоставляемыми специалистами лингвистической лаборатории. Обновления баз выпускаются каждые 20 минут.

Антивирус Касперского® для MIMESweeper

Антивирус Касперского® для MIMESweeper обеспечивает высокоскоростную антивирусную проверку трафика на серверах, использующих Clearswift MIMEsweeper for SMTP / Clearswift MIMEsweeper for Exchange / Clearswift MIMEsweeper for Web.

Программа выполнена в виде плагина (модуля расширения) и осуществляет в режиме реального времени антивирусную проверку и обработку входящих и исходящих почтовых сообщений.

A.3. Наши координаты

Если у вас возникнут вопросы, вы можете обратиться к нашим дистрибьюторам или в ЗАО «Лаборатория Касперского». Вам будут предоставлены подробные консультации по телефону или электронной почте.

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 бизнес-продуктов:	+7 (495) 797-87-07, +7 (495) 645-79-29, +7 (495) 956-87-08 в рабочие дни с 10 до 18:30 часов по московскому времени (GMT +3)
Электронная система HelpDesk:	http://support.kaspersky.ru/helpdesk.html
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