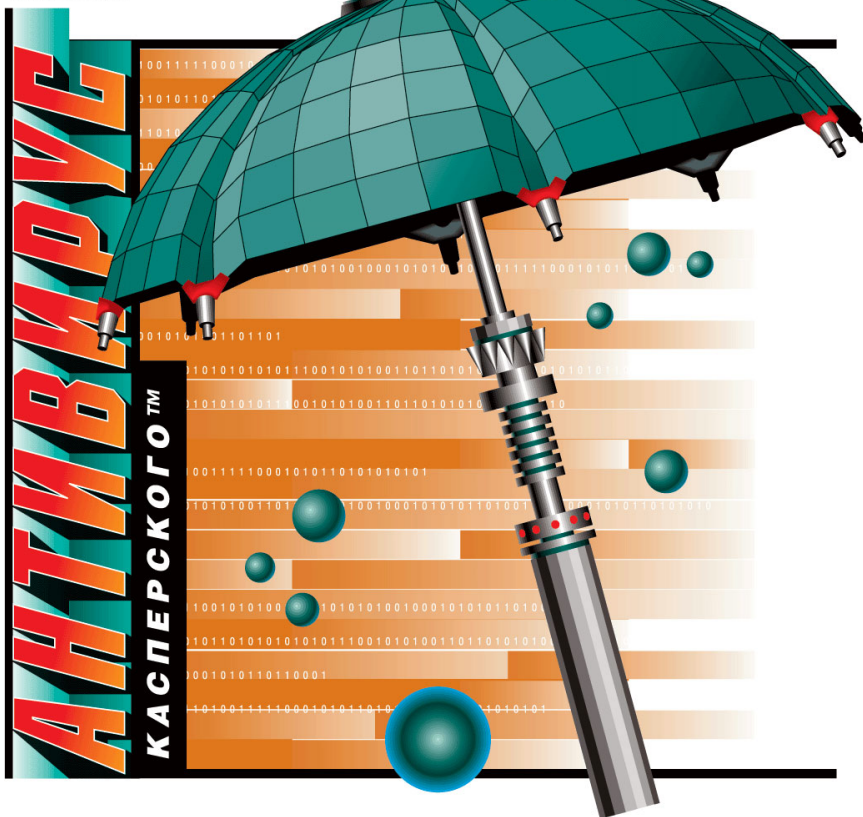


ЛАБОРАТОРИЯ КАСПЕРСКОГО



**РЕАЛЬНАЯ
ЗАЩИТА
ВИРТУАЛЬНОГО
ПРОСТРАНСТВА**



Kaspersky® Administration Kit 5.0

Начало работы

KASPERSKY® ADMINISTRATION KIT 5.0

Начало работы

© ЗАО "Лаборатория Касперского"
Тел., факс: +7 (495) 797-87-00
<http://www.kaspersky.ru/>

Дата редакции: декабрь 2005 г.

Содержание

ГЛАВА 1. ВВЕДЕНИЕ.....	4
ГЛАВА 2. НАЧАЛО РАБОТЫ	6
2.1. Установка MSDE 2000	7
2.2. Установка Сервера администрирования и Консоли администрирования.....	8
2.3. Первоначальная настройка антивирусной защиты.....	9
2.4. Создание группы администрирования	11
2.5. Удаленная установка Агента администрирования.....	11
2.6. Удаленная установка антивирусного приложения	13
2.7. Проверка корректности обновлений антивирусных баз на клиентских компьютерах.....	14
2.8. Настройка уведомлений.....	15
2.9. Проверка распространения уведомлений и задачи проверки по требованию.....	16
2.10. Получение отчетов.....	16
ГЛАВА 3. ПЕРЕХОД АНТИВИРУСНЫХ ПРИЛОЖЕНИЙ С ВЕРСИИ 4.X НА ВЕРСИЮ 5.X.....	18
ГЛАВА 4. ЗАКЛЮЧЕНИЕ.....	20
ПРИЛОЖЕНИЕ А. ЗАО "ЛАБОРАТОРИЯ КАСПЕРСКОГО"	21
А.1. Другие разработки Лаборатории Касперского	22
А.2. Наши координаты	27

ГЛАВА 1. ВВЕДЕНИЕ

В данном документе описываются шаги, с помощью которых администратор антивирусной безопасности предприятия может быстро начать работу с приложением **Kaspersky Administration Kit** и развернуть в своей сети антивирусную защиту на базе приложений Лаборатории Касперского.

Здесь подробно описывается простой сценарий форсированной установки, когда антивирусная защита разворачивается только на нескольких компьютерах. Для успешной установки необходимо, чтобы эти компьютеры работали под управлением операционных систем Microsoft Windows NT/2000/2003/XP.

В документе описывается также процедура перехода антивирусных приложений версий 4.x на приложения версии 5.x.



Подробная информация по приложению **Kaspersky Administration Kit** содержится в Руководстве администратора.

Приложение **Kaspersky Administration Kit** предназначено для управления системой антивирусной безопасности компьютерной сети предприятия. При помощи данного приложения администратор может:

- Проводить удаленную установку приложений антивирусной защиты предприятия.
- Осуществлять удаленное централизованное управление приложениями антивирусной защиты.
- Получать уведомления о критических событиях в работе приложений антивирусной защиты.
- Получать статистику и отчеты о работе приложений антивирусной защиты.

Приложение **Kaspersky Administration Kit** состоит из следующих основных компонентов:

- **Сервер администрирования** осуществляет централизованное управление приложениями Лаборатория Касперского, обеспечивающими антивирусную безопасность предприятия (Антивирус Касперского 5.0 для Windows Workstations, Антивирус Касперского 5.0 для File Servers). Сервер администрирования осуществляет функции централизованного хранения информации об антивирусной защите предприятия в базе данных MSDE 2000 либо MS SQL 2000. Базы

данных MSDE / Microsoft SQL 2000 с Service Pack 3 должны работать в сети предприятия до начала установки и работы Сервера администрирования. MSDE 2000 с установленным Service Pack 3 можно установить с дистрибутива Kaspersky Administration Kit 5.0.

- **Агент администрирования** устанавливается на клиентский компьютер (компьютер, который управляется Сервером администрирования и защищается приложениями Антивирус Касперского 5.0 для Windows Workstations или Антивирус Касперского 5.0 для File Servers). Агент администрирования осуществляет взаимодействие антивирусных приложений с Сервером администрирования: получает команды управления от Сервера администрирования и отправляет на Сервер администрирования информацию об антивирусной защите клиентского компьютера.
- **Консоль администрирования** предоставляет пользовательский интерфейс Kaspersky Administration Kit, позволяющий полностью использовать все функциональные возможности системы администрирования. Консоль администрирования выполнена в виде компонента расширения к Microsoft Management Console (MMC).

ГЛАВА 2. НАЧАЛО РАБОТЫ

Для того чтобы развернуть в сети предприятия систему антивирусной защиты, необходимо выполнить следующие действия:

1. Установить приложение MSDE 2000 с Service Pack 3 либо MS SQL 2000 с Service Pack 3 (см. п. 2.1 на стр. 7). Данное действие не требуется, если такой компонент уже установлен в сети предприятия.
2. Установить Сервер администрирования и Консоль администрирования (см. п. 2.2 на стр. 8).
3. Осуществить первоначальную настройку параметров и развернуть систему антивирусной защиты предприятия с помощью мастера первоначальной настройки (см. п. 2.3 на стр. 9).
4. Создать группы администрирования (см. п. 2.4 на стр. 11). Группы администрирования позволяют при помощи политик и групповых задач управлять набором клиентских компьютеров, входящих в группу, как единым целым.
5. Удаленно установить Агента администрирования на выбранные клиентские компьютеры для обеспечения взаимодействия антивирусных приложений с Сервером администрирования (см. п. 2.5 на стр. 11).
6. Удаленно установить приложения Антивирус Касперского 5.0 для Windows Workstations или Антивирус Касперского 5.0 для File Servers на выбранные клиентские компьютеры, если они не установлены ранее (см. п. 2.6 на стр. 13).
7. Проверить корректность работы задачи получения обновлений Сервером администрирования из интернета. Проверить корректность работы задачи обновления на клиентских компьютерах. Подробнее см. п. 2.7 на стр. 14.
8. Настроить параметры уведомлений о событиях в работе антивирусной защиты на клиентских компьютерах (см. п. 2.8 на стр. 15).
9. Запустить задачу проверки по требованию и проверить работу уведомлений о событиях в работе системы антивирусной безопасности на клиентских компьютерах (см. п. 2.9 на стр. 16).

10. Получить отчет о состоянии системы антивирусной защиты на клиентских компьютерах и о найденных вирусах (см. п. 2.10 на стр. 16).

Когда все эти действия будут выполнены, в компьютерной сети предприятия будет развернута система антивирусной защиты.

В последующих разделах документа перечисленные выше действия будут описаны более подробно.

2.1. Установка MSDE 2000

Данное действие можно пропустить, если в сети предприятия уже присутствует компонент MSDE 2000 с Service Pack 3 либо MS SQL 2000 с Service Pack 3.



Для того чтобы установить MSDE 2000 с дистрибутива Kaspersky Administration Kit,

1. Выберите компьютер, на котором будет установлена база данных Сервера администрирования. Обычно это тот же компьютер, на котором установлен Сервер администрирования.
2. Запустите на выбранном компьютере исполняемый файл **setup.exe**, расположенный на дистрибутивном компакт-диске приложения Kaspersky Administration Kit в каталоге **MSDE2KSP3**.
3. Следуйте указаниям мастера установки.

В результате на компьютере будет установлен MSDE 2000 и его Service Pack 3. Установленное приложение не требует никакого обслуживания или администрирования.



Использование MSDE, установленного с дистрибутива Kaspersky Administration Kit, возможно только для работы данного приложения.

В базе данных MSDE 2000 с установленным Service Pack 3 Сервер администрирования осуществляет функции централизованного хранения информации об антивирусной защите предприятия.

Резервное копирование данных Сервера администрирования осуществляется с помощью утилиты **klbackup**, входящей в состав дистрибутива Kaspersky Administration Kit (более подробную информацию

об утилите резервного копирования смотрите в Руководстве администратора).

2.2. Установка Сервера администрирования и Консоли администрирования

В процессе установки можно выбрать либо оба компонента, либо только Консоль администрирования. Установка Сервера администрирования без Консоли выбрать нельзя. По умолчанию предусмотрена установка обоих компонентов.

В случае необходимости можно установить Консоль администрирования на отдельный компьютер и управлять Сервером администрирования по сети.



Для того чтобы установить Сервер администрирования и/или Консоль администрирования,

1. Выберите компьютер, на котором будут установлены компоненты. Если в сети предприятия используется структура Windows-доменов, рекомендуется, чтобы компоненты были установлены на компьютер, входящий в домен.

Компьютер для установки Сервера администрирования и/или Консоли Kaspersky Administration Kit 5.x может быть тем же самым, на котором работает Сервер администрирования и/или Консоль версии 4.x. Компоненты версий 5.x и 4.x не зависят друг от друга и могут работать совместно на одном и том же компьютере.

Рекомендуется производить установку, обладая правами администратора домена. Это позволит автоматически создать группы **KLAdmins** и **KLOperators** и предоставить необходимые права учетной записи, под которой будет работать Сервер администрирования.

2. Запустите исполняемый файл **setup.exe**, расположенный на дистрибутивном компакт-диске.
3. Следуйте указаниям мастера установки.

В качестве учетной записи для Сервера администрирования рекомендуется выбрать учетную запись пользователя, обладающего правами администратора домена.

2.3. Первоначальная настройка антивирусной защиты




Для того чтобы осуществить первоначальную настройку параметров антивирусной защиты предприятия,

1. Запустите консоль администрирования с помощью меню **Пуск > Программы > Kaspersky Administration Kit > Kaspersky Administration Kit**.
2. Подключитесь к Серверу администрирования, выбрав соответствующий узел в дереве консоли и согласитесь принять сертификат данного Сервера администрирования.
3. Откройте контекстное меню Сервера администрирования и выберите команду **Мастер первоначальной настройки**.
4. Подождите, пока Сервер администрирования закончит опрос сети и обнаружит существующие в ней компьютеры.
5. Создайте группы администрирования одним из следующих способов:
 - Если система антивирусной защиты формируется для нескольких клиентских компьютеров, выберите способ **Создать логическую сеть вручную**. В этом случае вам нужно будет самостоятельно создать структуру логической сети.
 - Если установка осуществляется на все компьютеры предприятия, то группы администрирования могут быть созданы автоматически. В этом случае выберите один из следующих вариантов:
 - **Сформировать логическую сеть на основе Windows-сети**. В этом случае логическая сеть будет сформирована на основании структуры доменов и рабочих групп Windows (группы администрирования совпадают с доменами и рабочими группами Windows).
 - **Импортировать логическую сеть из предыдущей версии Kaspersky Administration Kit**. В этом случае логическая сеть будет сформирована на основании структуры логической сети Kaspersky Administration Kit 4.x.

6. Установите параметры рассылки уведомлений о работе антивирусной защиты. Вы сможете изменить эти параметры в дальнейшем в свойствах Сервера администрирования (более подробную информацию смотрите в Руководстве администратора).
7. Создайте политику для антивирусного приложения и несколько задач, которые позволят настроить в сети предприятия корректно работающую систему антивирусной защиты. Политики в приложении Kaspersky Administration Kit используются для определения общих параметров работы приложений в группах администрирования, задачи – для выполнения приложениями действий в группах администрирования.

Будут созданы следующие объекты:

- Политика верхнего уровня для антивирусного приложения с настройками по умолчанию. Позднее вы можете просматривать и изменять параметры политики. Чтобы значения, определенные в политике начали действовать на клиентских компьютерах и пользователь не мог их изменять, используйте символ  для этих параметров.

- Задача получения обновлений из интернета Сервером администрирования с настройками по умолчанию.

Данная задача получает обновления антивирусных баз и модулей приложения с серверов обновлений Лаборатории Касперского и помещает их в папку общего доступа, которая была задана при установке Сервера администрирования. Клиентские компьютеры могут получать обновления, используя папку общего доступа. Для настройки параметров получения обновлений с серверов обновлений Лаборатории Касперского нажмите на кнопку **Параметры** и задайте соответствующие параметры.

- Групповая задача верхнего уровня для обновлений антивирусных баз на клиентских компьютерах с настройками по умолчанию. Данная задача настроена таким образом, что клиентские компьютеры получают обновления из папки общего доступа, в который помещает полученные из интернета обновления Сервер администрирования.
- Групповая задача проверки по требованию для клиентских компьютеров с настройками по умолчанию.

2.4. Создание группы администрирования



Для того чтобы добавить новую группу в состав логической сети,

1. В дереве консоли или в панели результатов в папке **Группы** выберите папку, соответствующую группе, в состав которой должна входить новая группа. Откройте контекстное меню и выберите команду **Создать / Группу**. В результате запускается мастер создания новой группы. Следуйте его указаниям.
2. Переместите выбранные клиентские компьютеры в созданную группу администрирования из группы **Сеть**. Для этого используйте команды **Вырезать / Вставить** контекстного меню, либо просто перенесите с помощью мыши компьютеры из группы **Сеть** в созданную группу администрирования.

На выбранных клиентских компьютерах может работать Антивирус Касперского версии 4.x. Системы администрирования версий 4.x и 5.x работают независимо друг от друга. И в случае удаленной установки Антивируса Касперского версии 5.x поверх версии 4.x произойдет автоматическое удаление версии 4.x и установка вместо нее версии 5.x.

2.5. Удаленная установка Агента администрирования



Для того чтобы провести удаленную установку Агента администрирования,

1. Запустите мастер удаленной установки из контекстного меню Консоли администрирования.
2. Выберите для установки инсталляционный пакет Агента администрирования. Данный пакет создается при установке Сервера администрирования и содержит параметры, позволяющие Агенту администрирования подключиться к Серверу после проведения установки.

3. В качестве целевых клиентских компьютеров для установки укажите созданную группу администрирования.

В случае необходимости укажите имя и пароль администратора для доступа к клиентским компьютерам. Это необходимо, если учетная запись Сервера администрирования не обладает правами администратора для клиентских компьютеров.
4. На следующем шаге мастера будет создана и запущена групповая задача удаленной установки Агента администрирования для заданных клиентских компьютеров. В окне мастера вы можете наблюдать текущие результаты выполнения задачи и историю выполнения задачи для всех клиентских компьютеров.
5. После завершения установки Агента администрирования на все клиентские компьютеры и просмотра результатов закройте окно мастера удаленной установки.
6. Если вы хотите управлять антивирусной защитой клиентского компьютера в режиме реального времени, для того чтобы Сервер администрирования мог устанавливать соединение с Агентом администрирования в произвольный момент времени, на клиентском компьютере должен быть открыт UDP-порт номер 15000. Если открыть UDP-порт невозможно, установите флажок **Не разрывать соединение с Сервером администрирования** на закладке **Общие** в окне настройки параметров клиентского компьютера **Свойства: <Имя компьютера>**.

Чтобы убедиться, что установка прошла корректно, откройте окно свойств клиентских компьютеров. На закладке **Приложения** должно отобразиться приложение **Агент администрирования** со статусом **Выполняется**.

В случае если удаленная установка прошла успешно, а Агент администрирования не смог подключиться к Серверу администрирования, используйте утилиту **klagchk.exe**. Данная утилита входит в состав дистрибутива Агента администрирования и после его установки располагается в корне каталога установки компонента. При запуске из командной строки утилита предоставляет детальную диагностику параметров соединения с Сервером администрирования.

2.6. Удаленная установка антивирусного приложения

В данном разделе мы рассматриваем удаленную установку приложения Антивирус Касперского для Windows Workstations. Для других антивирусных приложений Лаборатории Касперского процедура установки аналогична.



Для того чтобы провести удаленную установку Антивируса Касперского для Windows Workstations,

1. Создайте инсталляционный пакет для удаленной установки приложения Антивирус Касперского для Windows Workstations с помощью мастера, запускаемого из контекстного меню узла **Удаленная установка**.

Необходимый для формирования инсталляционного пакета файл с расширением **.kpd** находится в корне дистрибутива приложения Антивирус Касперского для Windows Workstations. Там же находится файл лицензионного ключа, который используется при работе приложения Антивирус Касперского для Windows Workstations.

В случае необходимости измените параметры инсталляционного пакета. Например, рекомендуется разрешить автоматическую перезагрузку клиентского компьютера.

2. Запустите мастер удаленной установки из контекстного меню Консоли администрирования.
3. Проведите удаленную установку приложения Антивирус Касперского для Windows Workstation. Процедура удаленной установки приложения аналогична процедуре установки Агента администрирования (см. п. 2.5 на стр. 11). Возможна также установка Агента администрирования одновременно с Антивирусом Касперского для Windows Workstations.

Удаленную установку можно проводить на компьютеры, на которых установлено приложение Антивирус Касперского 4.x для Windows Workstations. В этом случае Антивирус Касперского версии 4.x будет автоматически удален и вместо него будет установлен Антивирус Касперского версии 5.x.

Чтобы убедиться, что установка прошла корректно, откройте окно свойств клиентских компьютеров. На закладке **Приложения** должно появиться

приложение **Антивирус Касперского для Windows Workstations** со статусом **Выполняется**. На закладке **Задачи** должна появиться задача постоянной защиты, выполняемая приложением Антивирус Касперского для Windows Workstations.

2.7. Проверка корректности обновлений антивирусных баз на клиентских компьютерах



Для того чтобы проверить корректность получения обновлений клиентскими компьютерами,

1. Запустите задачу **Получение обновлений Сервером администрирования**. Эта задача создается мастером первоначальной настройки и находится в узле **Задачи** верхнего уровня дерева консоли. Задача получит обновления с сервера обновлений Лаборатории Касперского и поместит их в папку общего доступа, заданную при установке Сервера. Дождитесь завершения выполнения задачи.

Результаты выполнения задачи можно просмотреть, нажав на кнопку **Результаты**.

В дереве консоли в узле **Обновления** появится информация о помещенных в папку общего доступа обновлениях.



Более подробную информацию о способах получения обновлений можно получить на веб-сайте Лаборатории Касперского (<http://www.kaspersky.ru/avupdates>).

2. Запустите групповую задачу обновления на клиентских компьютерах. Эта задача создается мастером первоначальной настройки и находится в папке **Задачи** узла **Группы**. Дождитесь завершения выполнения задачи.

Результаты выполнения задачи можно просмотреть, нажав на кнопку **Результаты**.

Задача, созданная мастером первоначальной настройки проводит обновление клиентских компьютеров с использованием соединения между

Сетевым агентом и Сервером администрирования. Поддерживаются также следующие способы обновления клиентских компьютеров:

- Из папки общего доступа на Сервере администрирования.
- С использованием HTTP-сервера.
- С использованием FTP-сервера.

Для корректного получения обновлений из папки общего доступа клиентские компьютеры должны обладать правами на чтение этой папки. Если это по каким-либо причинам невозможно, то для получения обновлений рекомендуется использовать FTP- или HTTP-сервер. В этом случае необходимо создать FTP- или HTTP-папку, которая указывает на подпапку **Updates** папки общего доступа, используемой Сервером администрирования (например, ftp://admserver/updates). После этого в параметрах групповой задачи получения обновлений клиентскими компьютерами в качестве источника обновлений требуется указать путь к этой папке (ftp://admserver/updates).


2.8. Настройка уведомлений



Для того чтобы настроить уведомления о событиях в работе системы антивирусной защиты,

1. Перейдите на закладку **События** в свойствах политики верхнего уровня для антивирусного приложения (например, Антивирус Касперского для Windows Workstations).
2. Выберите необходимые события и укажите для них способы получения уведомлений.

Для проверки распространения уведомлений (см. п. 2.9 на стр. 16) достаточно установить уведомление для события **Найден вирус**.

3. Используйте символ  для установленных вами параметров, чтобы применить настройки для всех клиентских компьютеров. Чтобы изменения вступили в силу нажмите на кнопку **Применить**.
4. Чтобы проверить корректность установленных параметров, вы можете вручную отправить сообщение. Для этого нажмите на кнопку **Проверить**. В результате по указанным в параметрах

адресам будут направлены сообщения, сформированные по заданному шаблону.

2.9. Проверка распространения уведомлений и задачи проверки по требованию



Для того чтобы проверить распространение уведомлений о событиях и работу задачи проверки по требованию,

1. Попробуйте скопировать на защищенный компьютер тестовый "вирус" **Eicar**. Вам будет отказано в операции копирования (если работает задача постоянной защиты файловой системы). Вы получите уведомление о найденном вирусе, и в узле **События** верхнего уровня дерева консоли появится соответствующая запись.



Тестовый "вирус" НЕ ЯВЛЯЕТСЯ ВИРУСОМ и не содержит программного кода, который может навредить вашему компьютеру, при этом большинство продуктов антивирусных компаний-производителей идентифицируют его как вирус. Загрузить тестовый "вирус" можно с официального сайта организации **EICAR**: http://www.eicar.org/anti_virus_test_file.htm.

2. Остановите задачу постоянной защиты файловой системы на клиентском компьютере и скопируйте "вирус" **Eicar** на клиентский компьютер. Снова включите задачу постоянной защиты файловой системы.
3. Запустите групповую задачу проверки по требованию клиентских компьютеров. В процессе выполнения задачи тестовый "вирус" будет обнаружен. Вы получите уведомление о найденном вирусе, и в узле **События** верхнего уровня дерева консоли появится соответствующая запись.

2.10. Получение отчетов

На основании данных, сохраняемых в журнале событий Kaspersky Administration Kit на Сервере администрирования, вы можете получать

отчеты о состоянии системы антивирусной защиты по заранее сформированным шаблонам. Шаблоны отчетов размещаются в узле **Отчеты** дерева консоли.

Предусмотрено семь стандартных шаблонов, соответствующих типам отчетов о состоянии системы антивирусной защиты:

- **Отчет о версиях антивирусных баз.**
- **Отчет об ошибках.**
- **Отчет о лицензионных ключах.**
- **Отчет о наиболее заражаемых клиентских компьютерах.**
- **Отчет об уровне антивирусной защиты.**
- **Отчет о версиях установленных приложений Лаборатории Касперского.**
- **Отчет о вирусной активности.**

Например, если вы создадите отчет о вирусной активности, вы увидите информацию обо всех случаях обнаружения вирусов, зарегистрированных приложением Kaspersky Administration Kit.

Если вы добавите в группу администрирования произвольный компьютер без установленного на нем Агента администрирования, то в отчете об уровне антивирусной защите будет содержаться информация о том, что на одном из компьютеров не установлена антивирусная защита.

ГЛАВА 3. ПЕРЕХОД АНТИВИРУСНЫХ ПРИЛОЖЕНИЙ С ВЕРСИИ 4.X НА ВЕРСИЮ 5.X

В данном разделе описывается процедура перехода с антивирусных приложений версии 4.x на приложения Антивирус Касперского 5.x для Windows Workstations и Антивирус Касперского 5.x для File Servers. Отдельные особенности перехода уже были частично описаны в предыдущих разделах, в данном же разделе сценарий перехода приводится полностью.

Kaspersky Administration Kit 5.x работает независимо от Kaspersky Administration Kit 4.x. При этом система администрирования версии 5.x используется только для управления приложениями версии 5.x, а система администрирования версии 4.x – для управления приложениями версии 4.x. Поэтому во время перехода в сети некоторое время будут работать одновременно обе версии.

Типичный сценарий перехода выглядит следующим образом:

1. В сети предприятия устанавливается Сервер администрирования версии 5.x. При этом он может устанавливаться на тот же компьютер, где уже работает Сервер администрирования версии 4.x.
2. Создается структура логической сети (группы администрирования) для приложений версии 5.x. При этом структура логической сети может быть импортирована из системы администрирования версии 4.x.
3. Создаются политики и групповые задачи для приложений версии 5.x в логической сети. Устанавливаются требуемые параметры антивирусной защиты для приложений. Устанавливаются правила обработки событий работы антивирусной защиты.
4. Определяются компьютеры, для которых будет происходить переход с версии 4.x на версию 5.x.
5. Создается инсталляционный пакет удаленной установки для приложений версии 5.x. Антивирусные приложения версии 5.x устанавливаются на выбранные компьютеры. При этом происходит

автоматическое удаление антивирусных приложений версии 4.x и установка антивирусных приложений версии 5.x.

6. Компьютеры, на которых произведена установка антивирусных приложений версии 5.x, добавляются в логическую структуру Сервера администрирования версии 5.x. Оставшиеся компьютеры продолжают управляться системой администрирования версии 4.x.

Постепенно вся антивирусная защита компании переводится на антивирусные приложения версии 5.x, которые управляются системой администрирования версии 5.x.

ГЛАВА 4. ЗАКЛЮЧЕНИЕ

Возможности системы администрирования Kaspersky Administration Kit гораздо шире, чем описано в данном документе. Здесь описан простой сценарий, который позволит вам начать работу с системой администрирования и развернуть в сети антивирусную защиту на нескольких компьютерах. Однако данный сценарий описывает все основные действия, которые требуются для надежной антивирусной защиты сети предприятия:

- Развертывание и настройка системы администрирования антивирусной защитой.
- Централизованное развертывание антивирусной защиты на клиентских компьютерах сети предприятия.
- Определение политик антивирусной защиты.
- Определение и проверка работы задач обновления антивирусных баз клиентских компьютеров.
- Проверка работы задачи постоянной защиты.
- Определение и запуск задачи проверки по требованию для клиентских компьютеров.
- Получение уведомлений о критических событиях в работе системы антивирусной защиты.
- Получение отчетов о статусе антивирусной защиты в сети.

ПРИЛОЖЕНИЕ А. ЗАО "ЛАБОРАТОРИЯ КАСПЕРСКОГО"

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

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

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

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

Годы упорной работы позволили компании стать лидером в разработке технологий защиты от вирусов. Лаборатория Касперского первой разработала многие современные стандарты антивирусных программ. Основной продукт компании, Антивирус Касперского®, обеспечивает надежную защиту всех объектов вирусных атак: рабочих станций, файловых серверов, почтовых систем, межсетевых 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. Наша антивирусная база обновляется каждые три часа. Мы обеспечиваем наших пользователей круглосуточной технической поддержкой на нескольких языках.

А.1. Другие разработки Лаборатории Касперского

Антивирус Касперского® Personal

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

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

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

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

Программа поддерживает более семисот форматов архивированных и сжатых файлов и обеспечивает автоматическую антивирусную проверку их содержимого, а также удаление вредоносного кода из архивных файлов формата ZIP, CAB, RAR, ARJ.

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

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

Антивирус Касперского® Personal Pro

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

Антивирус Касперского® Personal Pro обеспечивает:

- **антивирусную проверку по требованию пользователя** локальных дисков;
- **автоматическую проверку в масштабе реального времени** на присутствие вирусов всех используемых файлов;
- **почтовый фильтр** автоматически осуществляет проверку и лечение всей входящей и исходящей почтовой корреспонденции по протоколам POP3 и SMTP и эффективно обнаруживает вирусы в почтовых базах;
- **поведенческий блокиратор**, гарантирующий стопроцентную защиту от макро-вирусов приложений Microsoft Office;
- **антивирусную проверку** более 900 версий форматов архивированных и сжатых файлов и обеспечивает автоматическую антивирусную проверку их содержимого, а также удаление вредоносного кода из архивных файлов формата **ZIP, CAB, RAR, ARJ**.

Kaspersky® Anti-Hacker

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

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

этому приложению. В результате обеспечивается конфиденциальность информации, находящейся на вашем компьютере.

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

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

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

Kaspersky® Security для PDA

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

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

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

Антивирус Касперского® Business Optimal

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

Антивирус Касперского® Business Optimal обеспечивает полномасштабную антивирусную защиту¹:

¹ В зависимости от типа поставки

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

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

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

Kaspersky® Corporate Suite

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

Kaspersky® Corporate Suite обеспечивает полномасштабную антивирусную защиту:

- *рабочих станций* под управлением Windows 98/Me, Windows 2000/NT/XP Workstations и Linux.
- *файловых серверов* под управлением Windows NT 4.0 Server, Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD, OpenBSD, Linux и Samba Servers.
- *почтовых систем* Microsoft Exchange Server 5.5/2000/2003, Lotus Notes/Domino, Sendmail, Postfix, Exim и Qmail.
- *интернет-шлюзов*: CheckPoint Firewall –1; Microsoft ISA Server 2004 Enterprise Edition.
- *карманных компьютеров*, работающих под управлением Windows CE и Palm OS.

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

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

Kaspersky® Anti-Spam

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

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

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

Kaspersky® Anti-Spam Personal

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

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

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

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

Kaspersky Security® для Microsoft Exchange 2003

Kaspersky Security для Microsoft Exchange обеспечивает антивирусную проверку входящих, исходящих и хранящихся на сервере почтовых

сообщений, в том числе сообщений в общих папках, а также осуществляет фильтрацию нежелательной корреспонденции, используя интеллектуальные технологии распознавания спама в сочетании с технологиями компании Microsoft. Приложение проверяет все сообщения, поступающие на Exchange-сервер по SMTP-протоколу, на наличие вирусов, используя антивирусные технологии, применяемые Лабораторией Касперского, и признаков спама, используя фильтрацию по формальным признакам (почтовому адресу, IP-адресу, размеру письма, заголовку), а также анализируя содержимое письма и его вложений с помощью интеллектуальных технологий, включая уникальные графические сигнатуры для распознавания спама в виде изображений. Проверке подвергается как тело сообщения, так и прикрепленные файлы.

Kaspersky® Mail Gateway

Kaspersky® Mail Gateway – универсальное решение для комплексной защиты пользователей почтовой системы. Установленное между корпоративной сетью и сетью Интернет, приложение осуществляет проверку всех элементов электронного письма на присутствие вирусов и других вредоносных программ (Spyware, Adware, и т.д.), а также производит централизованную фильтрацию потока почтовых сообщений на предмет спама. Решение также содержит ряд дополнительных возможностей по фильтрации почтового трафика.

А.2. Наши координаты

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

Адрес:	Россия, 125363, Москва, ул. Героев Панфиловцев, 10	
Факс:	+7 (495) 797-8700	
Экстренная круглосуточная помощь	+7 (495) 797-8707 support@kaspersky.com	
Поддержка пользователей Business Optimal	+7 (495) 363-4205 (с 10 до 19 часов)	smb-support@kaspersky.com
Поддержка пользователей Corporate Suite	Телефоны и электронный адрес предоставляются при покупке Corporate Suite.	

Антивирусная лаборатория	newvirus@kaspersky.com (только для отправки новых вирусов в архивированном виде)	
Группа подготовки пользовательской документации	docfeedback@kaspersky.com (только для отправки отзывов о документации и электронной справочной системе)	
Департамент продаж	+7 (495) 797-8700	sales@kaspersky.com
Департамент маркетинговых коммуникаций	+7 (495) 797-8700	info@kaspersky.com
WWW:	http://www.kaspersky.ru http://www.viruslist.ru	