

ЛАБОРАТОРИЯ КАСПЕРСКОГО

Kaspersky[®] Administration Kit 6.0

РУКОВОДСТВО ПО
ВНЕДРЕНИЮ

KASPERSKY® ADMINISTRATION KIT 6.0

Руководство по внедрению

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

Дата редакции: сентябрь 2007 г.

Содержание

| | |
|---|----|
| ГЛАВА 1. KASPERSKY® ADMINISTRATION KIT | 5 |
| 1.1. Назначение, состав и основные функции..... | 5 |
| 1.2. Требования к аппаратному и программному обеспечению | 7 |
| 1.3. Комплект поставки..... | 9 |
| 1.4. Сервис для зарегистрированных пользователей..... | 9 |
| 1.5. Назначение документа | 10 |
| 1.6. Принятые обозначения..... | 11 |
| ГЛАВА 2. ТИПИЧНЫЕ СХЕМЫ РАЗВЕРТЫВАНИЯ АНТИВИРУСНОЙ ЗАЩИТЫ..... | 12 |
| 2.1. Схемы развертывания антивирусной защиты на компьютерах логической сети..... | 12 |
| 2.2. Схема построения системы централизованного управления антивирусной защитой..... | 13 |
| ГЛАВА 3. УСТАНОВКА KASPERSKY ADMINISTRATION KIT | 15 |
| 3.1. Установка MSDE с дистрибутива Kaspersky Administration Kit..... | 17 |
| 3.2. Установка Сервера администрирования и Консоли администрирования на локальном компьютере..... | 19 |
| 3.3. Удаление программных компонентов Kaspersky Administration Kit | 35 |
| 3.4. Обновление версии приложения | 36 |
| ГЛАВА 4. УСТАНОВКА И ДЕИНСТАЛЛЯЦИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА КОМПЬЮТЕРАХ | 37 |
| 4.1. Удаленная установка программного обеспечения | 39 |
| 4.1.1. Формирование инсталляционного пакета..... | 40 |
| 4.1.2. Просмотр и настройка параметров инсталляционного пакета | 43 |
| 4.1.3. Создание и настройка инсталляционного пакета для Агента администрирования..... | 47 |
| 4.1.4. Создание и настройка инсталляционного пакета для Сервера администрирования..... | 50 |
| 4.1.5. Создание задачи распространения инсталляционного пакета на подчиненные Серверы администрирования | 50 |

| | |
|---|-----|
| 4.1.6. Распространение инсталляционных пакетов в пределах группы с помощью агентов обновления | 52 |
| 4.1.7. Создание задачи удаленной установки | 55 |
| 4.1.8. Настройка задачи удаленной установки | 66 |
| 4.1.9. Удаленная установка приложений на подчиненные Серверы администрирования..... | 68 |
| 4.1.10. Удаленная деинсталляция программного обеспечения..... | 70 |
| 4.2. Мастер удаленной установки | 71 |
| 4.3. Локальная установка программного обеспечения..... | 75 |
| 4.3.1. Локальная установка Агента администрирования..... | 76 |
| 4.3.2. Локальная установка плагина управления приложением | 81 |
| 4.3.3. Установка приложений в неинтерактивном режиме..... | 81 |
| ПРИЛОЖЕНИЕ А. ГЛОССАРИЙ..... | 84 |
| ПРИЛОЖЕНИЕ В. ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»..... | 91 |
| В.1. Другие разработки «Лаборатории Касперского» | 92 |
| В.2. Наши координаты | 105 |

ГЛАВА 1. KASPERSKY® ADMINISTRATION KIT

1.1. Назначение, состав и основные функции

Приложение **Kaspersky® Administration Kit** предназначено для централизованного решения основных административных задач по управлению системой антивирусной безопасности компьютерной сети предприятия, построенной на основе приложений, входящих в состав продуктов компании Антивирус Касперского Business Optimal и Kaspersky Corporate Suite. Kaspersky Administration Kit поддерживает работу во всех сетевых конфигурациях, использующих протокол TCP/IP.

Приложение адресовано администраторам корпоративных компьютерных сетей, а также сотрудникам, отвечающим за антивирусную защиту компьютеров в организациях.

Приложение предоставляет администратору следующие возможности:

- Удаленная централизованная установка и удаление приложений, входящих в состав продуктов «Лаборатории Касперского», на компьютеры сети. Эта возможность позволяет администратору один раз скопировать на выделенный компьютер необходимый набор приложений «Лаборатории Касперского», и после этого проводить удаленную установку на компьютеры сети.
- Удаленное централизованное управление приложениями, входящими в состав продуктов «Лаборатории Касперского». Эта возможность позволяет создавать многоуровневую систему антивирусной защиты и управлять работой всех приложений с единого рабочего места администратора. Последнее особенно актуально для крупных организаций, в которых локальная сеть состоит из большого количества компьютеров и может охватывать несколько территориально разделенных зданий или помещений. Данная возможность включает в себя:
 - объединение компьютеров в *группы администрирования* в соответствии с выполняемыми функциями и набором установленных на них приложений;
 - централизованную настройку параметров работы приложения путем создания и применения *групповых политик*;

- индивидуальную настройку параметров работы приложения для отдельных компьютеров при помощи *настроек приложения*;
 - централизованное управление работой приложений путем создания и запуска *групповых и глобальных задач*;
 - построение индивидуальных схем работы приложений путем создания и запуска задач для набора компьютеров из различных групп администрирования.
- Автоматическое обновление антивирусных баз и модулей приложения на компьютерах. Эта возможность позволяет проводить централизованное обновление антивирусных баз для всех установленных приложений компании без непосредственного обращения каждого компьютера к интернет-серверу «Лаборатории Касперского». Обновление может происходить автоматически, по заданному администратором графику. Администратор может отслеживать распространение обновлений на клиентские компьютеры.
 - Система получения отчетности. Данная возможность позволяет осуществлять централизованный сбор статистики о работе всех установленных приложений компании, отслеживать корректность работы этих приложений и создавать отчеты на основании полученной информации. Администратор может создавать единый сетевой отчет о работе приложения, отчеты о работе приложений на каждом компьютере.
 - Механизм оповещения о событиях в работе приложений. Механизм рассылки уведомлений. Эта возможность позволяет администратору формировать список событий в работе приложений, при возникновении которых к нему будут поступать уведомления. Например, в числе таких событий может быть обнаружение вируса или некорректное завершение процедуры обновления антивирусных баз на компьютере, обнаружение нового компьютера в сети.
 - Управление лицензиями. Данная возможность позволяет централизованно устанавливать лицензионные ключи ко всем установленным приложениям компании, отслеживать выполнение лицензионного соглашения (соответствие числа лицензий количеству работающих приложений в сети) и срок его окончания.
 - Совместная работа с Cisco Network Admission Control (NAC). Эта возможность позволяет задать соответствие между условиями антивирусной защиты компьютера и статусами Cisco NAC.

Приложение Kaspersky Administration Kit состоит из трех основных компонентов:

- **Сервер администрирования** осуществляет функции централизованного хранения информации об установленных в сети приложениях «Лаборатории Касперского» и управления ими.
- **Агент администрирования** осуществляет взаимодействие между Сервером администрирования и приложениями «Лаборатории Касперского», установленными на конкретном сетевом узле (рабочей станции или сервере). Данный компонент является единым для всех Windows-приложений из состава продуктов компании Антивирус Касперского Business Optimal и Kaspersky Corporate Suite. Для Novell- и Unix-приложений «Лаборатории Касперского» существуют отдельные версии Агента администрирования.
- **Консоль администрирования** предоставляет пользовательский интерфейс к административным сервисам Сервера и Агента. Консоль администрирования выполнена в виде компонента расширения к Microsoft Management Console (MMC).

1.2. Требования к аппаратному и программному обеспечению

Сервер администрирования

- Программные требования:
 - Microsoft Data Access Components (MDAC) версии 2.8 и выше;
 - MSDE 2000 с установленным Service Pack 3, или Microsoft SQL Server 2000 с установленным Service Pack 3¹ и выше, или MySQL версии 5.0.32, или Microsoft SQL 2005 и выше; или Microsoft SQL 2005 Express и выше;
 - Microsoft Windows 2000 с установленными Service Pack 1 и выше; Microsoft Windows XP Professional с установленным Service Pack 1 и выше; Microsoft Windows XP Professional x64 и выше; Microsoft Windows Server 2003 и выше; Microsoft

¹ Для установки MSDE вы можете воспользоваться входящим в состав поставки Kaspersky Administration Kit дистрибутивом.

Windows Server 2003 x64 и выше; Microsoft Windows NT4 с установленным Service Pack 6a и выше; Microsoft Windows Vista, Microsoft Windows Vista x64.

- Аппаратные требования:
 - процессор Intel Pentium III с частотой 800 МГц или выше;
 - объем оперативной памяти 128 МБ;
 - объем свободного места на диске 400 МБ.

Консоль администрирования

- Программные требования:
 - Microsoft Windows 2000 с установленным Service Pack 1 и выше; Microsoft Windows XP Professional с установленным Service Pack 1 и выше; Microsoft Windows XP Home Edition с установленным Service Pack 1 и выше; Microsoft Windows XP Professional x64 и выше; Microsoft Windows Server 2003 и выше; Microsoft Windows Server 2003 x64 и выше; Microsoft Windows NT4 с установленным Service Pack 6a и выше; Microsoft Windows Vista, Microsoft Windows Vista x64;
 - Microsoft Management Console версии 1.2 и выше;
 - при работе с Microsoft Windows NT4 требуется наличие установленного браузера Microsoft Internet Explorer 6.0.
- Аппаратные требования:
 - процессор Intel Pentium II с частотой 400 МГц или выше;
 - объем оперативной памяти 64 МБ;
 - объем свободного места на диске 10 МБ.

Агент администрирования

- Программные требования:
 - Для Windows-систем:

Microsoft Windows 98; Microsoft Windows ME; Microsoft Windows 2000 с установленным Service Pack 1 и выше; Microsoft Windows NT4 с установленным Service Pack 6a и выше; Microsoft Windows XP Professional с установленным Service Pack 1 и выше; Microsoft Windows XP Professional x64 и выше; Microsoft Windows Server 2003 и выше;

Microsoft Windows Server 2003 x64 и выше; Microsoft Windows Vista, Microsoft Windows Vista x64.

- Для Novell-систем:

Novell NetWare 6 SP3 и выше; Novell NetWare 6.5 SP3 и выше.
- Аппаратные требования:
 - Для Windows-систем:
 - процессор Intel Pentium с частотой 233 МГц или выше;
 - объем оперативной памяти 32 МБ;
 - объем свободного места на диске 10 МБ.
 - Для Novell-систем:
 - процессор Intel Pentium с частотой 233 МГц или выше;
 - объем оперативной памяти 12 МБ;
 - объем свободного места на диске 32 МБ.

1.3. Комплект поставки

Программный продукт бесплатно поставляется со всеми приложениями «Лаборатории Касперского», входящими в состав Антивируса Касперского Business Optimal и Kaspersky Corporate Suite (коробочный вариант), а также доступен для загрузки на веб-сайте «Лаборатории Касперского» (www.kaspersky.ru).

1.4. Сервис для зарегистрированных пользователей

ЗАО «Лаборатория Касперского» предлагает своим легальным пользователям большой комплекс услуг, позволяющих увеличить эффективность использования продуктов компании.

При приобретении лицензии на какой-либо из продуктов «Лаборатории Касперского», входящий в состав Антивируса Касперского Business Optimal

и Kaspersky Corporate Suite, вы становитесь зарегистрированным пользователем Kaspersky Administration Kit. После этого в течение срока действия лицензии вы получаете следующие услуги:

- предоставление новых версий данного программного продукта;
- консультации по вопросам, связанным с установкой, настройкой и эксплуатацией данного программного продукта, оказываемые по телефону и с помощью веб-формы;

При обращении в Службу технической поддержки указывайте информацию о лицензии приложения «Лаборатории Касперского», совместно с которым используется Kaspersky Administration Kit.

- оповещение о выходе новых программных продуктов «Лаборатории Касперского» и о новых вирусах, появляющихся в мире (данная услуга предоставляется пользователям, подписавшимся на рассылку новостей ЗАО «Лаборатория Касперского»).

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

1.5. Назначение документа

Данное руководство содержит описание установки компонентов Kaspersky Administration Kit, а также удаленной установки приложений в компьютерной сети простой конфигурации.

Основные понятия и общая схема работы с приложением приводятся в Руководстве администратора Kaspersky Administration Kit, пошаговое описание действий при работе с программой – в Справочном руководстве к Kaspersky Administration Kit.

С вопросами, которые пользователи чаще всего задают специалистам службы технической поддержки «Лаборатории Касперского», вы можете ознакомиться на нашем сайте в разделе **Сервис → Сайт технической поддержки**. Данный раздел содержит информацию по установке, настройке и функционированию программ «Лаборатории Касперского», а также по удалению с компьютера наиболее распространенных вирусов и лечению зараженных файлов.

1.6. Принятые обозначения

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

| Оформление | Смысловое назначение |
|---|---|
| Жирный шрифт | Названия меню, пунктов меню, окон, элементов диалоговых окон и т. п. |
| <i>Примечание.</i> | Дополнительная информация, примечания. |
| Внимание! | Информация, на которую следует обратить особое внимание. |
| <i>Чтобы выполнить действие,</i> 1. Шаг 1. 2. ... | Описание последовательности выполняемых пользователем шагов и возможных действий. |
| [ключ] – назначение ключа. | Ключи командной строки. |
| Текст информационных сообщений и командной строки | Текст конфигурационных файлов, информационных сообщений программы и командной строки. |

ГЛАВА 2. ТИПИЧНЫЕ СХЕМЫ РАЗВЕРТЫВАНИЯ АНТИВИРУСНОЙ ЗАЩИТЫ

2.1. Схемы развертывания антивирусной защиты на компьютерах логической сети

Существует два варианта развертывания системы антивирусной защиты, управляемой при помощи приложения Kaspersky Administration Kit:

- посредством удаленной централизованной установки приложений на клиентские компьютеры логической сети. При этом установка приложений и подключение к системе централизованного удаленного управления происходит автоматически, не требует какого-либо вмешательства со стороны администратора и позволяет устанавливать антивирусное программное обеспечение на любое количество клиентских компьютеров.
- путем локальной установки приложений на каждый клиентский компьютер. В этом случае установка необходимых компонентов на клиентские компьютеры и рабочее место администратора производится вручную, параметры подключения клиентов к Серверу задаются при установке Агента администрирования. Этот вариант развертывания можно порекомендовать, если невозможно провести удаленную централизованную установку.

Удаленная установка может быть использована для инсталляции любых приложений по выбору пользователя.

Однако следует помнить, что Kaspersky Administration Kit поддерживает управление только приложениями «Лаборатории Касперского», в состав дистрибутива которых входит специализированный компонент – плагин управления приложением.

2.2. Схема построения системы централизованного управления антивирусной защитой

Первым этапом построения системы централизованного управления антивирусной защитой сети предприятия при помощи программного комплекса Kaspersky Administration Kit является проектирование логической сети. На данном этапе необходимо принять следующие решения:

1. Выделить в сети изолированные участки и определить, какое количество Серверов администрирования потребуется установить. Использование иерархии Серверов администрирования позволит существенно уменьшить нагрузку каналов связи и увеличить надежность системы.
2. Какие компьютеры в составе сети предприятия будут выполнять функции главного Сервера администрирования и подчиненных Серверов, какие – рабочих мест администратора и клиентских компьютеров. Клиентскими компьютерами должны стать все компьютеры, на которые предполагается установить приложения «Лаборатории Касперского».
3. По какому признаку будет осуществляться объединение клиентских компьютеров в группы, и определить иерархию групп.
4. Какой вид развертывания системы антивирусной защиты будет использоваться: удаленная или локальная установка.

На следующем этапе администратор должен создать логическую сеть путем установки соответствующих программных компонентов Kaspersky Administration Kit на компьютеры сети, а именно:

1. Установить Серверы администрирования на компьютеры, входящие в состав сети предприятия.
2. Установить Консоль администрирования на компьютерах, с которых будет осуществляться управление.

3. Принять решение о назначении администраторов логической сети, определить какие еще категории пользователей будут работать с системой, и закрепить за каждой категорией перечень выполняемых функций.
4. Сформировать группы пользователей и предоставить каждой группе необходимые для выполнения возложенных на ее пользователей функций права доступа.

После этого необходимо создать иерархию Серверов администрирования и для каждого Сервера сформировать структуру логической сети: построить иерархию групп администрирования и провести распределение компьютеров в соответствующие группы.

На следующем этапе осуществляется установка на клиентские компьютеры компонента Агент администрирования, необходимых приложений «Лаборатории Касперского», а также на рабочее место администратора соответствующих плагинов управления приложениями.

При использовании удаленной установки Агент администрирования может быть установлен совместно с любым приложением. В этом случае отдельная установка Агента администрирования не требуется.

На заключительном этапе производится настройка установленных приложений посредством определения и применения групповых политик и создание необходимых задач.

Приложение предоставляет возможность создания системы централизованного управления антивирусной защитой с минимальными настройками с помощью мастера первоначальной настройки. При этом предлагается создать логическую сеть, идентичную доменной структуре Windows-сети, и формируется система антивирусной защиты с использованием Антивируса Касперского для Windows Workstations версий 5.0 и 6.0.

ГЛАВА 3. УСТАНОВКА KASPERSKY ADMINISTRATION KIT

Перед тем как начинать установку, необходимо убедиться, что аппаратное и программное обеспечение компьютера соответствует требованиям, предъявляемым к Серверу администрирования и рабочему месту администратора (см. п. 1.2 на стр. 7).

Для хранения информации Сервера администрирования используется MSDE (Microsoft Data Engine), MySQL-сервер или Microsoft SQL-сервер. Если в сети предприятия ни MSDE, ни SQL-сервер не установлен, вам необходимо установить один из них перед установкой Сервера администрирования. Для этого вы можете использовать имеющиеся у вас дистрибутивы. Для установки MSDE вы можете также воспользоваться дистрибутивом Kaspersky Administration Kit. Процедура установки MSDE с дистрибутива Kaspersky Administration Kit описана далее (см. п. 3.1 на стр. 17).

Для установки Kaspersky Administration Kit необходимо наличие прав локального администратора на компьютере, где осуществляется установка.

Программа установки предложит вам установить на компьютер, с которого она запущена, программные компоненты приложения Kaspersky Administration Kit – Сервер администрирования и Консоль администрирования. Такая конфигурация рекомендуется в начале формирования системы удаленного централизованного управления.

Для того чтобы в результате установки компоненты приложения работали корректно, на компьютерах должны быть открыты все необходимые порты. Список портов, которые используются приложением Kaspersky Administration Kit по умолчанию, представлен в таблице 1.

Таблица 1

| Номер порта | Протокол | Описание |
|--|-----------|--|
| Компьютер, на котором установлен Сервер администрирования | | |
| 13000 | TCP и UDP | С использованием SSL-протокола осуществляется: <ul style="list-style-type: none"> • получение данных с клиентских компьютеров; • подключение агентов обновления; • подключение подчиненных Серверов администрирования; • получение сообщений о выключении компьютеров. |
| 13292 | TCP | Используется для подключения мобильных устройств. ² |
| 14000 | TCP | Используется для: <ul style="list-style-type: none"> • получения данных с клиентских компьютеров; • подключения агентов обновления; • подключения подчиненных Серверов администрирования. |
| 18000 | HTTP | Используется для получения Сервером администрирования данных от сервера аутентификации Cisco NAC. |
| Компьютер, назначенный агентом обновления | | |
| 13000 | TCP | Используется для подключения клиентскими компьютерами. |

² Под мобильным устройством подразумевается устройство с установленным приложением Антивирус Касперского 6.0 Mobile Enterprise Edition.

| Номер порта | Протокол | Описание |
|---|----------|---|
| 13001 | TCP | Используется для подключения клиентскими компьютерами, если агентом обновления является компьютер с установленным Сервером администрирования. |
| 14000 | TCP | Используется для подключения клиентскими компьютерами. |
| 14001 | TCP | Используется для подключения клиентскими компьютерами, если агентом обновления является компьютер с установленным Сервером администрирования. |
| Клиентский компьютер с установленным Агентом администрирования | | |
| 15000 | UDP | Используется для получения запроса на подключение к Серверу администрирования. |

3.1. Установка MSDE с дистрибутива Kaspersky Administration Kit

До начала установки MSDE необходимо установить Microsoft Data Access Components (MDAC) версии 2.8 и выше (дистрибутив доступен на веб-сайте компании Microsoft).

Установка MSDE с дистрибутива Kaspersky Administration Kit на компьютер осуществляется локально.

Для того чтобы установить MSDE,

1. Запустите исполняемый файл, расположенный на дистрибутивном компакт-диске приложения Kaspersky Administration Kit в каталоге **MSDE2KSP3**. Мастер установки предложит вам провести настройку параметров и запустить ее. Следуйте его указаниям.
2. Первые шаги установки традиционны и состоят в распаковке с дистрибутива необходимых файлов и записи их на жесткий

диск вашего компьютера, проверки установки необходимого программного обеспечения, принятии лицензионного соглашения, а также вводе информации о пользователе и компании.

3. Далее в диалоговом окне **Каталог установки** определите:

- в поле **Программные модули** – каталог для установки программных файлов MSDE. По умолчанию это – **<Диск>:\Program Files\Microsoft SQL Server**. Если такого каталога нет, он будет создан автоматически.
- в поле **База данных** – каталог, который будет использоваться для размещения баз данных сервера MSDE. По умолчанию это также **<Диск>:\Program Files\Microsoft SQL Server**.

Выбор каталогов осуществляется при помощи кнопок **Обзор**.

4. После этого в диалоговом окне **Имя SQL-сервера** (см. рис. 1) установите имя, которое будет присвоено данному серверу.

По умолчанию имя не создается, для адресации к серверу будет использоваться имя компьютера, на котором он установлен.

Если вы хотите определить другое имя, снимите флажок **По умолчанию** и введите новое имя в поле **Имя SQL-сервера**.

По окончании настройки параметров вы можете ознакомиться с ними и запустить установку. В результате ее успешного завершения на вашем компьютере будет установлен MSDE.

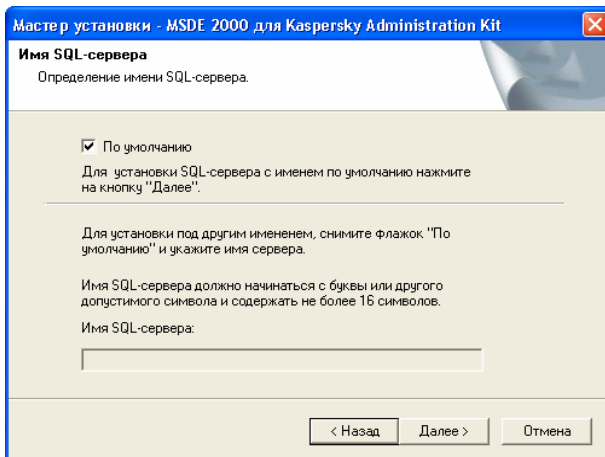


Рисунок 1. Выбор имени сервера

3.2. Установка Сервера администрирования и Консоли администрирования на локальном компьютере

В этом разделе описывается локальная установка Сервера и/или Консоли администрирования. Если в сети установлен хотя бы один Сервер администрирования, возможна установка последующих Серверов с помощью задачи удаленной установки методом форсированной установки (см. п. 4.1.7 на стр. 55). При формировании задачи следует использовать инсталляционный пакет Сервера администрирования (см. п. 4.1.4 на стр. 50).

Для того чтобы установить Сервер администрирования и/или Консоль администрирования на локальном компьютере,

1. Запустите исполняемый файл **setup.exe**, расположенный на дистрибутивном компакт-диске. Мастер установок предложит вам провести настройку параметров. Следуйте его указаниям.
2. На первых шагах мастер распакует с дистрибутива необходимые файлы и запишет их на жесткий диск вашего компьютера, предложит принять лицензионное соглашение и ввести информацию о пользователе и компании.

3. Далее определите каталог для установки компонентов. По умолчанию это **<Диск>:\Program Files\Kaspersky Lab\Kaspersky Administration Kit**. Если такого каталога нет, он будет создан автоматически. Смена каталога осуществляется при помощи кнопки **Обзор**.
4. После этого выберите компоненты Kaspersky Administration Kit, которые вы хотите установить (см. рис. 2):
 - **Сервер администрирования.** В этом случае также можно указать, требуется ли установка стандартных компонентов «Лаборатории Касперского» для работы с Cisco NAC. Если установка требуется, установите флажок **Posture Validation Server "Лаборатории Касперского" для Cisco NAC**. Настроить параметры взаимодействия с Cisco NAC можно будет в свойствах или в политике Сервера администрирования (подробнее см. Справочное руководство Kaspersky Administration Kit).
 - **Агент администрирования.**
 - **Консоль администрирования.**

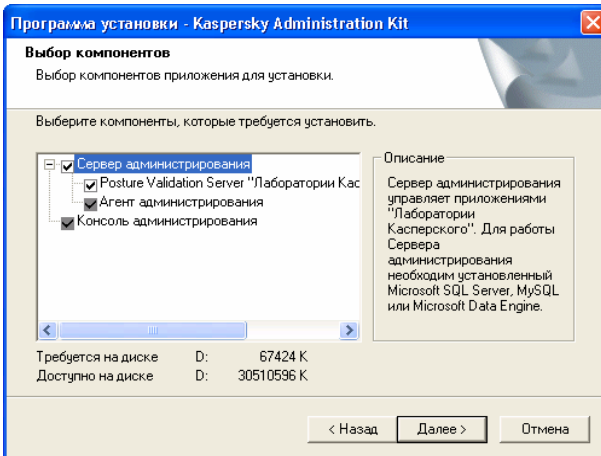


Рисунок 2. Выбор компонентов для установки

Установку Консоли и Агента администрирования отменить нельзя, они устанавливаются всегда. По умолчанию предусмотрена установка всех компонентов.

Вместе с компонентом Сервер администрирования на компьютер будет установлена серверная версия Агента администрирования. Его совместная установка с обычной версией Агента администрирования невозможна. Если данный компонент уже установлен на вашем компьютере, удалите его и запустите установку Сервера администрирования повторно.

Обратите внимание, что в диалоговом окне мастера приводится справочная информация:

- в правой части в поле **Описание** о выбранном компоненте;
- в нижней части о необходимом для установки выбранных компонентов объеме дискового пространства и объеме свободного пространства на заданном для установки диске компьютера.

Если вы выбрали только Консоль администрирования, дальнейшие шаги настройки параметров установки отсутствуют, и вы переходите на этап ознакомления с ними и запуска установки.

5. Если вы выбрали установку Сервера администрирования, на следующем этапе определите, под какой учетной записью будет запускаться Сервер администрирования как служба на данном компьютере (см. рис. 3).

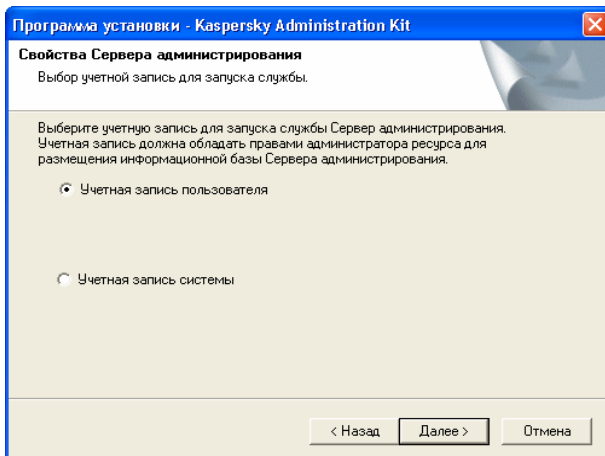


Рисунок 3. Выбор учетной записи

Вы можете выбрать один из двух вариантов:

- **Учетная запись пользователя** – Сервер администрирования будет запускаться под учетной записью пользователя, входящего в домен. В этом случае Сервер администрирования будет инициировать все операции с правами данной учетной записи, и на следующем этапе вам будет предложено определить пользователя, чья учетная запись будет использоваться.

Если в сети предприятия сформирована структура Windows-доменов, рекомендуется выбрать учетную запись администратора домена для запуска Сервера администрирования. Это позволит в дальнейшем избежать дополнительных настроек, например, задания учетной записи пользователя, обладающего правами администратора домена при создании задачи удаленной установки (см. п. 4.1.7 на стр. 55).

- **Учетная запись системы** – Сервер администрирования будет запускаться под учетной записью и с правами **Учетная запись системы**. В этом случае выбор пользователя не производится, и вы сразу перейдете на этап определения ресурса для размещения информационной базы Сервера администрирования (см. пункт 7 на стр. 24).

Для корректной работы Kaspersky Administration Kit необходимо, чтобы учетная запись для запуска Сервера администрирования обладала правами администратора ресурса для размещения информационной базы Сервера администрирования.

6. Если в качестве учетной записи для запуска Сервера администрирования вы выбрали учетную запись пользователя домена, вам будет предложено определить этого пользователя.

Для этого в окне мастера (см. рис. 4) в поле **Имя учетной записи** при помощи кнопки **Обзор** или вручную введите имя пользователя из числа зарегистрированных в текущем домене. После этого введите пароль пользователя, с которым он регистрируется в домене.

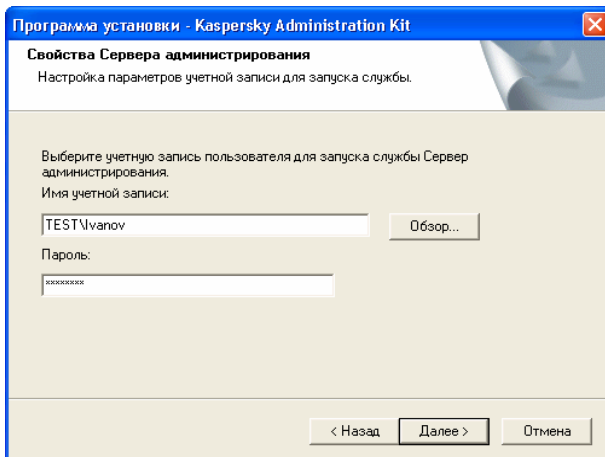


Рисунок 4. Выбор пользователя

В случае если вы выбрали пользователя, который не обладает правами администратора домена, Сервер администрирования будет запускаться под его учетной записью, однако функциональность Kaspersky Administration Kit будет несколько ограничена. Например, у него может не быть прав для выполнения задач удаленной установки с помощью сценария запуска (см. п. 4.1.7 на стр. 55) и проведения опроса некоторых доменов Windows-сети.

Для корректной работы Сервера администрирования учетная запись для его запуска должна входить в состав группы **Administrators** на компьютере с установленным Сервером администрирования, а также обладать следующими правами:

- Вход в качестве службы (Log on as a service);
- Работа в режиме операционной системы (Act as part of the operating system);
- Доступ к компьютеру из сети (Access this computer from the network);
- Замена маркера уровня процесса (Replace a process level token);
- Настройка квот памяти для процесса (Increase quotas/ Adjust memory quotas for a process).

Если выбранный вами пользователь является администратором домена, но не обладает перечисленными выше правами, они будут ему предоставлены (см. рис. 5).

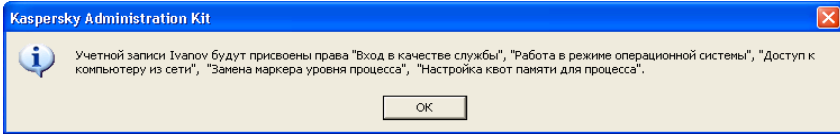


Рисунок 5. Сообщение о предоставлении пользователю прав

7. На следующем этапе вам будет предложено определить ресурс **Microsoft SQL-сервер (MSDE)** или **MySQL** (см. рис. 6), который будет использоваться для размещения информационной базы данных Сервера администрирования.

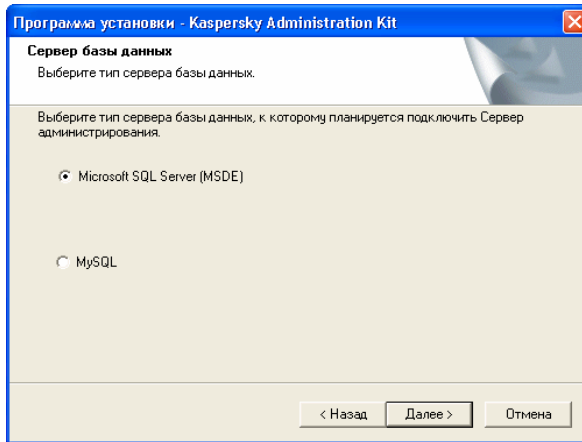


Рисунок 6. Выбор базы данных

8. Если на предыдущем этапе был выбран MSDE или Microsoft SQL-сервер, и вы планируете для работы Kaspersky Administration Kit использовать сервер, установленный в сети предприятия, укажите его имя в поле **Имя SQL-сервера** и задайте имя базы данных, которая будет создана для размещения информации Сервера администрирования, в поле **Имя базы данных SQL-сервера** (см. рис. 7). По умолчанию база данных создается под именем **KAV**.

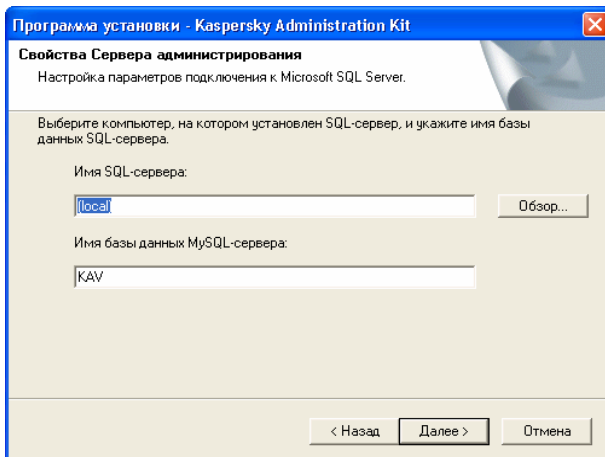


Рисунок 7. Выбор SQL-сервера

В поле **Имя SQL-сервера** автоматически проставляется значение (**local**), если SQL-сервер обнаружен на компьютере, с которого осуществляется установка Kaspersky Administration Kit. При помощи кнопки **Обзор** выводится список всех Microsoft SQL-серверов, установленных в сети.

Если Сервер администрирования будет запускаться под учетной записью локального администратора или под учетной записью системы кнопка **Обзор** не доступна.

Если на предыдущем этапе был выбран MySQL-сервер, в этом окне (см. рис. 8) укажите его имя в поле **Имя MySQL-сервера** (по умолчанию используется IP-адрес компьютера, на который устанавливается Kaspersky Administration Kit) и укажите порт для подключения в поле **Порт** (по умолчанию используется порт 3306). В поле **Имя базы данных MySQL-сервера** задайте имя базы данных, которая будет создана для размещения информации Сервера администрирования (по умолчанию база данных создается под именем **KAV**).

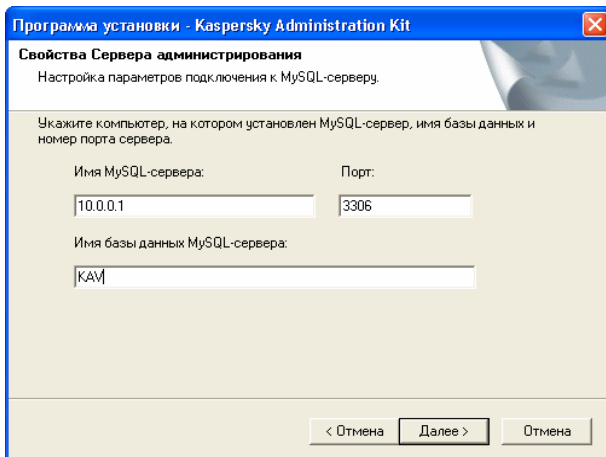


Рисунок 8. Выбор MySQL-сервера

Если в сети нет ни одного SQL-сервера или вы не можете их использовать, вам необходимо провести его установку (см. п. 3.1 на стр. 17).

Если вы хотите поставить SQL-сервер на тот компьютер, с которого производится установка Kaspersky Administration Kit, вам необходимо ее прервать и запустить снова после установки SQL-сервера.

Если установка будет проводиться на удаленный компьютер, прерывать работу мастера установки Kaspersky Administration Kit не требуется. Установите SQL-сервер и вернитесь к установке Kaspersky Administration Kit.

9. На данном шаге определите режим аутентификации, который будет использоваться при подключении Сервера администрирования к SQL-серверу.

Для MSDE или Microsoft SQL-сервер вы можете выбрать один из двух вариантов (см. рис. 9):

- **Режим аутентификации Microsoft Windows** – в этом случае при проверке прав будет использоваться учетная запись для запуска Сервера администрирования;
- **Режим аутентификации SQL-сервера** – в случае выбора данного варианта для проверки прав будет использоваться указанная ниже учетная запись. Заполните поля **Учетная запись**, **Пароль** и **Подтверждение пароля**.

Если база данных Сервера администрирования находится на другом компьютере, то при установке или обновлении Сервера администрирования необходимо использовать режим аутентификации SQL-сервера.

Программа установки - Kaspersky Administration Kit

Режим SQL-аутентификации
Выбор режима аутентификации.

Выберите режим аутентификации, который будет использоваться для подключения к Microsoft SQL Server. При выборе аутентификации SQL-сервера введите учетную запись, пароль и подтверждение пароля.

Режим аутентификации Microsoft Windows

Режим аутентификации SQL-сервера

Учетная запись:

Пароль:

Подтверждение пароля:

< Назад Далее > Отмена

Рисунок 9. Режим аутентификации на SQL-сервере

Для MySQL-сервера укажите учетную запись и пароль (см. рис. 10).

Программа установки - Kaspersky Administration Kit

Параметры MySQL-аутентификации
Задайте учетную запись MySQL-сервера.

Задайте учетную запись для подключения к MySQL-серверу, введите пароль и подтверждение пароля.

Учетная запись:

Пароль:

Подтверждение пароля:

< Назад Далее > Отмена

Рисунок 10. Режим аутентификации на MySQL-сервере

10. После этого (см. рис. 11) определите место размещения и название папки общего доступа, которая будет использоваться для:
- хранения файлов, необходимых для удаленной установки приложений (файлы копируются на Сервер администрирования при создании инсталляционных пакетов);
 - размещения обновлений, копируемых с источника обновлений на Сервер администрирования.

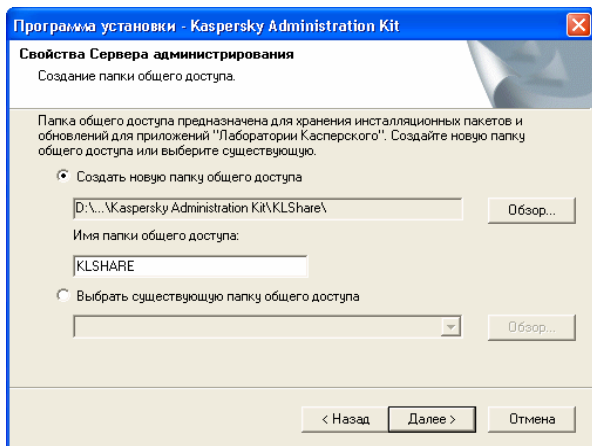


Рисунок 11. Создание папки общего доступа

К данному ресурсу будет открыт общий доступ на чтение для всех пользователей.

Вы можете выбрать один из двух вариантов:

- **Создать новую папку общего доступа** – для создания новой папки, при этом укажите путь к папке в расположенном ниже поле.
- **Выбрать существующую папку общего доступа** – для выбора папки общего доступа из числа уже существующих.

Папка общего доступа может размещаться как локально на компьютере, с которого производится установка, так и удаленно, на любом из компьютеров, входящих в состав сети предприятия. Вы можете указать папку общего доступа как с помощью кнопки **Обзор**, так и вручную, введя в соответствующем поле UNC-путь (например, \\server\KLSHare).

По умолчанию создается локальная папка **KLShare** в каталоге, заданном для установки программных компонентов Kaspersky Administration Kit.

11. В следующем окне мастера задайте адрес Сервера администрирования (см. рис. 12) с помощью:

- DNS-имени. Этот вариант используется в том случае, когда в сети присутствует DNS-сервер, и клиентские компьютеры могут получить с его помощью адрес Сервера администрирования.
- NetBIOS-имени. Этот вариант используется, если клиентские компьютеры получают адрес Сервера администрирования с помощью протокола NetBIOS, или в сети присутствует WINS-сервер.
- IP-адреса. Этот вариант используется, если Сервер администрирования имеет статический IP-адрес, и в дальнейшем он не будет изменяться.

При необходимости установите флажок **Разрешить службу имен NetBIOS в Анти-Хакере Антивируса Касперского 6.0**. В этом случае в Анти-Хакере Антивируса Касперского версии 6.0, установленном на компьютере, будет открыт UDP-порт 137, используемый для получения IP-адреса Сервера администрирования.

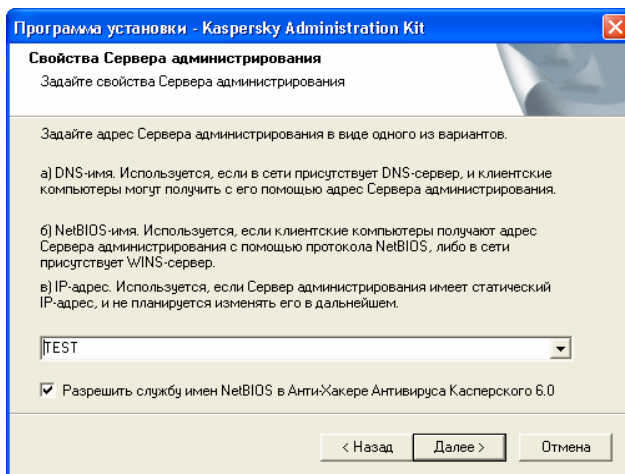


Рисунок 12. Адрес Сервера администрирования

12. После этого установите параметры подключения к Серверу администрирования (см. рис. 13):

- номер порта, по которому будет осуществляться подключение к Серверу администрирования. По умолчанию используется **14000** порт, если он занят, вы можете его изменить.
- номер SSL-порта, по которому будет осуществляться защищенное подключение к Серверу администрирования с использованием протокола SSL. По умолчанию это **13000** порт.

Если Сервер администрирования работает под управлением ОС Microsoft Windows XP с Service Pack 2, то встроенный межсетевой экран блокирует TCP-порты с номерами 13000 и 14000. Поэтому для обеспечения доступа на компьютере, на котором установлен Сервер администрирования, эти порты необходимо открыть вручную.

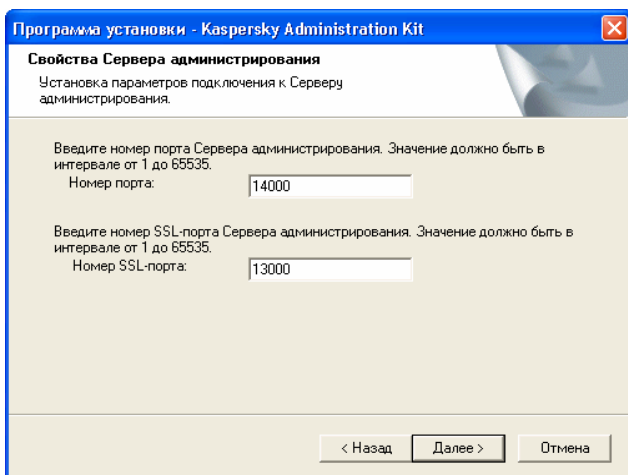


Рисунок 13. Параметры подключения к Серверу администрирования

13. В этом окне мастера (см. рис. 14) определите, как будет создаваться сертификат для аутентификации устанавливаемого Сервера администрирования.

Предусмотрено два варианта:

- **Создать новый сертификат** – выберите данный вариант, если вы устанавливаете новый Сервер администрирования. Для того чтобы в дальнейшем, в случае необходимо-

сти, было проще восстановить данные и структуру логической сети этого Сервера, сохраните резервную копию сертификата. Для этого установите флажок **Создать резервную копию сертификата**.

- **Восстановить сертификат из резервной копии** – выберите данный вариант, если вы восстанавливаете Сервер администрирования при отсутствии резервной копии. В этом случае будет возможно восстановить данные и структуру логической сети предыдущего Сервера администрирования.

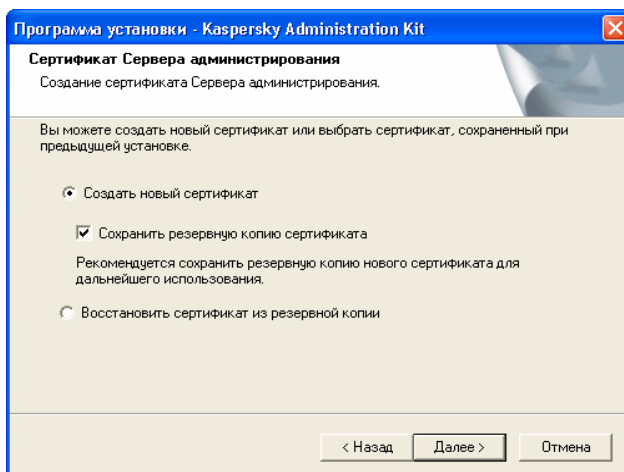


Рисунок 14. Выбор способа получения сертификата Сервера администрирования

14. Если на предыдущем шаге вы выбрали создание нового сертификата и сохранение его резервной копии в представленном окне (см. рис. 15) укажите:

- каталог для сохранения резервной копии файла сертификата;
- пароль, который будет использован для шифрования при создании сертификата и для расшифровки при его восстановлении из резервной копии;
- подтверждение пароля.

Полное восстановление данных Сервера администрирования в дальнейшем требует обязательного сохранения сертификата Сервера.

При восстановлении сертификата должен быть указан тот же пароль, что и при его резервном копировании. Если пароль указан неверно, сертификат восстановлен не будет.

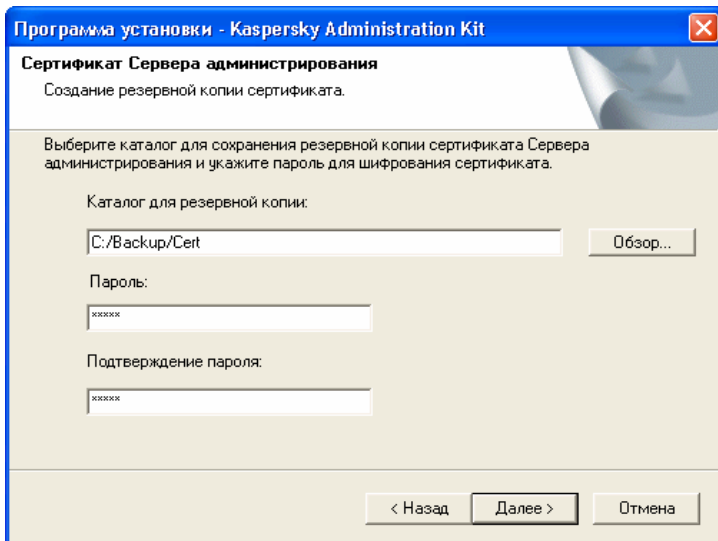


Рисунок 15. Выбор каталога для сохранения резервной копии сертификата

Если на предыдущем шаге был выбран вариант восстановления сертификата Сервера из резервной копии в представленном окне (см. рис. 16) укажите:

- каталог, в котором сохранена резервная копия файла сертификата;
- пароль, который был использован для шифрования при создании резервной копии сертификата.

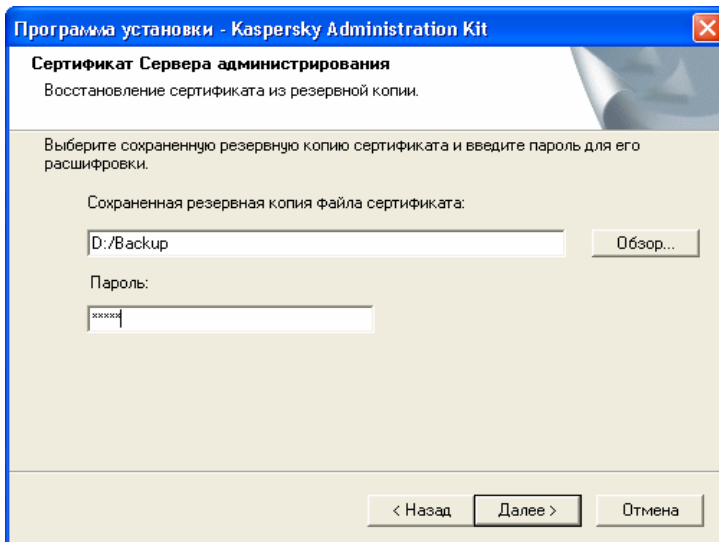


Рисунок 16. Выбор каталога размещения резервной копии сертификата

По окончании настройки параметров установки компонентов Kaspersky Administration Kit вы можете ознакомиться с ними и запустить установку.

В результате установки Консоли администрирования на вашем компьютере в меню **Пуск** → **Программы** → **Kaspersky Administration Kit** появится значок для ее запуска.

Сервер администрирования и Агент будут установлены на компьютере в качестве служб с атрибутами, указанными в таблице 2. В таблице также указаны атрибуты службы Posture Validation Server (PVS) «Лаборатории Касперского» для Cisco NAC, которая будет выполняться на компьютере, если соответствующий компонент был установлен совместно с Сервером администрирования.

Таблица 2

| Атрибут | Сервер администрирования | PVS «Лаборатории Касперского» для Cisco NAC | Агент администрирования |
|---|---|--|--------------------------------|
| Имя службы | CSAdminServer | nacserver | klagent |
| Выводимое имя службы | Kaspersky Administration Server | Kaspersky Lab Cisco NAC Posture Validation Server | Kaspersky Network Agent |
| Имя процесса в диспетчере задач Windows | klserver.exe | klnacserver.exe | klagent.exe |
| Тип запуска | Автоматически при старте операционной системы. | | |
| Учетная запись | Локальная система или указанная пользователем (см. п. 6 на стр. 22). | | |

Вместе с Сервером администрирования на компьютер будет установлена серверная версия Агента администрирования. Она входит в состав компонента Сервер администрирования, устанавливается и удаляется в его составе, и может взаимодействовать только с локально установленным Сервером администрирования. Настраивать параметры подключения Агента к Серверу администрирования не требуется, программно оно реализовано с учетом того, что компоненты установлены на одном компьютере. Эти параметры будут не доступны также в локальных настройках Агента администрирования на данном компьютере. Такая конфигурация позволяет избежать дополнительных настроек и возможных конфликтов в работе компонентов при их отдельной установке.

Серверная версия Агента администрирования устанавливается с теми же атрибутами и выполняет те же функции по управлению приложениями, что и стандартный Агент администрирования. На него будет действовать политика группы, в которую компьютер Сервера администрирования включен в качестве клиентского, будут создаваться и выполняться все задачи, предусмотренные для Агента администрирования, за исключением задачи смены Сервера.

Отдельная установка Агента администрирования на компьютер Сервера администрирования не требуется. Его функции выполняет серверная версия Агента.

Вы можете просматривать свойства служб **Kaspersky Administration Server**, **Kaspersky Network Agent** и **Kaspersky Lab Cisco NAC Posture Validation Server**, а также следить за их работой при помощи стандартных средств администрирования Windows – **Управление компьютером** → **Службы**. Информация о работе службы **Kaspersky Administration Server** фиксируется и сохраняется в системном журнале Windows на компьютере, где установлен Сервер администрирования, в отдельной ветви журнала **Kaspersky Event Log**.

На компьютере, где установлен Сервер администрирования, также создаются группы локальных пользователей **KLAdmins** и **KLOperators**. Если Сервер администрирования будет запускаться под учетной записью пользователя, входящего в домен, то группы **KLAdmins** и **KLOperators** добавляются в список групп доменных пользователей. Изменение состава групп осуществляется при помощи стандартных средств администрирования Windows.

3.3. Удаление программных компонентов Kaspersky Administration Kit

Удаление Kaspersky Administration Kit вы можете провести как с помощью команды **Удаление Kaspersky Administration Kit** в меню **Пуск** → **Программы** → **Kaspersky Administration Kit**, так и стандартными средствами установки и удаления программ Microsoft Windows. При этом запускается мастер, в результате работы которого с компьютера будут удалены все компоненты приложения (включая плагины). Если во время работы мастера вы не задали удаление папки общего доступа (**KLShare**), то после завершения всех связанных с ней задач удалите ее вручную.

При удалении вам будет предложено сохранить резервную копию Сервера администрирования.

3.4. Обновление версии приложения

Для обновления Kaspersky Administration Kit версий 4.x и 5.0 (Плановое обновление 1 и Плановое обновление 2) на более позднюю версию необходимо удалить предыдущую версию и установить новую, согласно описаниям, приведенным в данном Руководстве.

При обновлении версий 5.0 (Плановое обновление 3) и 6.0 на более новую версию поддерживается восстановление данных из резервной копии, сформированной более ранней версией приложения. При этом рекомендуется следующий порядок действий:

1. Создайте резервную копию данных установленного Сервера администрирования при помощи утилиты **klbackup.exe**. Данная утилита входит в состав дистрибутива Kaspersky Administration Kit и после установки компонента Сервер администрирования располагается в корне каталога установки. Обратите внимание на то, что для полного восстановления данных Сервера администрирования требуется сохранить сертификат сервера. Этот параметр является обязательным для утилиты **klbackup.exe**.
2. Запустите установку обновленной версии Kaspersky Administration Kit 6.0 на компьютере, где установлена предыдущая версия Сервера администрирования и/или Консоли. Выполните обновление компонента. При обновлении сохраняются и будут доступны в новой версии все данные и настройки предыдущей версии Сервера и/или Консоли администрирования. Поддерживается обратная совместимость между новой и старой версиями Сервера администрирования.
3. Для обновления установленного на компьютерах сети Агента администрирования, создайте групповую либо глобальную задачу установки более новой версии данного компонента. Запустите задачу на выполнение вручную либо по расписанию. После ее успешного завершения версия Агента администрирования будет обновлена.

В случае возникновения проблем при установке вы можете восстановить предыдущую версию Kaspersky Administration Kit, используя созданную перед обновлением резервную копию данных Сервера администрирования.

Если установлен хотя бы один Сервер администрирования, обновление других Серверов можно проводить с помощью задачи удаленной установки, в которой используется инсталляционный пакет Сервера администрирования (подробнее см. п. 4.1.4 на стр. 50).

ГЛАВА 4. УСТАНОВКА И ДЕИНСТАЛЛЯЦИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА КОМПЬЮТЕРАХ

Перед тем как начинать установку, необходимо убедиться, что аппаратное и программное обеспечение компьютеров соответствует предъявляемым требованиям (см. п. 1.2 на стр. 7).

Kaspersky Administration Kit позволяет устанавливать и удалять приложения «Лаборатории Касперского» на компьютеры следующими способами:

- централизованно и удаленно через Консоль администрирования;
- локально, на каждый компьютер отдельно.

Связь Сервера администрирования с клиентскими компьютерами обеспечивает компонент Агент администрирования. Поэтому он должен быть установлен на каждом компьютере, который будет подключен к системе удаленного централизованного управления перед установкой антивирусных приложений. При централизованной установке приложений через Консоль администрирования Агент может быть установлен совместно с одним из приложений.

На компьютере, где установлен Сервер администрирования, в качестве Агента может использоваться только серверная версия этого компонента. Она входит в состав Сервера администрирования и устанавливается и удаляется вместе с ним (см. п. 3.2 на стр. 19).
Устанавливать Агент администрирования на этот компьютер не требуется.

Установка Агента администрирования осуществляется точно так же, как и установка приложений, и может быть проведена как удаленно, так и локально.

Агенты администрирования могут различаться в зависимости от приложений «Лаборатории Касперского», для совместной работы с которыми они должны быть установлены. В некоторых случаях возможна только локальная установка Агента администрирования (подробнее см. в

Руководства к соответствующим приложениям). Агент администрирования устанавливается на клиентский компьютер один раз.

Интерфейс управления приложениями при помощи Kaspersky Administration Kit обеспечивают соответствующие плагины управления. Поэтому для получения доступа к интерфейсу управления приложением соответствующий плагин должен быть установлен на рабочее место администратора. При удаленной установке он устанавливается автоматически при создании первого инсталляционного пакета для соответствующего приложения. При локальной установке на клиентском компьютере плагин управления должен быть установлен администратором вручную.

В текущей версии Kaspersky Administration Kit поддерживается удаленное управление следующими приложениями компании «Лаборатория Касперского»:

- защита рабочих станций и файловых серверов:
 - Антивирус Касперского 5.0 для Windows File Servers;
 - Антивирус Касперского 6.0 для Windows Servers;
 - Антивирус Касперского 5.0 для Windows Workstations;
 - Антивирус Касперского 6.0 для Windows Workstations;
 - Антивирус Касперского 5.0 Second Opinion Solution;
 - Антивирус Касперского 5.7 для Novell NetWare;
 - Антивирус Касперского Mobile 6.0 Enterprise Edition;
 - Антивирус Касперского 6.0 для Windows Servers Enterprise Edition.
- защита периметра:
 - Антивирус Касперского 5.6 для Microsoft ISA Server 2000 Enterprise Edition.
- защита почтовых систем:
 - Антивирус Касперского 5.5 для Microsoft Exchange Server 2000/2003, Плановое обновление 1;
 - Kaspersky Security 5.5 для Microsoft Exchange Server 2003, Плановое обновление 1.

Подробную информацию об управлении перечисленными приложениями через Kaspersky Administration Kit см. в Руководствах к соответствующим приложениям.

4.1. Удаленная установка программного обеспечения

Удаленная установка может быть выполнена с рабочего места администратора в главном окне программы Kaspersky Administration Kit.

Некоторые приложения «Лаборатории Касперского» могут быть установлены на клиентские компьютеры только локально (подробнее см. в Руководствах к соответствующим приложениям). При этом удаленное управление этими приложениями с помощью Kaspersky Administration Kit будет доступно.

Для удаленной установки программного обеспечения:

1. Сформируйте инсталляционный пакет (см. п. 4.1.1 на стр. 40). В его состав будут включены необходимые для установки приложения файлы, а также файлы с описанием параметров самого инсталляционного пакета.
2. Создайте задачу удаленной установки (см. п. 4.1.7 на стр. 55).

Для установки приложения на всех компьютерах логической сети или нескольких групп администрирования, либо на конкретных компьютерах из различных групп следует создать глобальную задачу удаленной установки.

Для установки программного обеспечения на все клиентские компьютеры какой-либо группы администрирования (все вложенных в нее групп и подчиненные Серверы) следует создать групповую задачу удаленной установки.

Вы можете воспользоваться мастером удаленной установки (см. п. 4.2 на стр. 71) для создания как групповой, так и для глобальной задачи.

Сформированная вами задача будет запускаться на выполнение в соответствии со своим расписанием. Параметры работы приложения на каждом клиентском компьютере устанавливаются в соответствии с политикой группы и настройками данного приложения по умолчанию.

Вы можете прервать процедуру установки, остановив выполнение задачи вручную.

Все сформированные для Сервера администрирования инсталляционные пакеты размещаются в дереве консоли в специальном контейнере – узле

Удаленная установка. На Сервере администрирования инсталляционные пакеты хранятся в заданной папке общего доступа в служебном каталоге **Packages**.

Вы можете просматривать свойства инсталляционного пакета, изменять его название и настройки в диалоговом окне **Свойства: <Название пакета >** (см. рис. 20). Данное окно открывается при помощи команды **Свойства** контекстного меню или аналогичного пункта в меню **Действие**.

Сформированные инсталляционные пакеты могут быть распространены на подчиненные Серверы администрирования (см. п. 4.1.5 на стр. 50) и на компьютеры в пределах группы с помощью агентов обновления (см. п. 4.1.6 на стр. 52).

Один и тот же инсталляционный пакет может быть многократно использован для создания задач удаленной установки.

Установка приложений может быть выполнена также в неинтерактивном режиме (подробнее см. п. 4.3.3 на стр. 81).

4.1.1. Формирование инсталляционного пакета

Для того чтобы сформировать инсталляционный пакет:

1. Подключитесь к нужному Серверу администрирования.
2. Выберите в дереве консоли узел **Удаленная установка**, откройте контекстное меню и выберите команду **Создать** → **Инсталляционный пакет** или воспользуйтесь аналогичным пунктом в меню **Действие**. В результате запускается мастер, следуйте его указаниям.
3. Вам будет предложено задать имя инсталляционного пакета, а на следующем шаге указать приложение для установки (см. рис. 17).

Если вы устанавливаете приложение, для которого предусмотрена возможность удаленной установки через Kaspersky Administration Kit, то из раскрывающегося списка выберите вариант: **Создать инсталляционный пакет для приложения «Лаборатории Касперского»**. При помощи кнопки **Обзор** выберите файл с описанием приложения (файл имеет расширение **.kpd** и входит в состав дистрибутива всех приложений компании, для которых предусмотрено удаленное управление через Kaspersky Administration Kit) или самораспаковывающийся архив приложения «Лаборатории Касперского» (файл имеет

расширение **.exe** и доступен для скачивания на веб-сайте «Лаборатории Касперского»). В результате автоматически заполняются поля с именем приложения и номером версии.

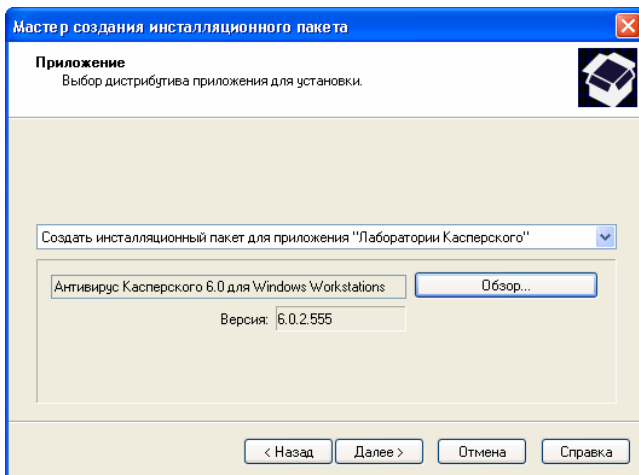


Рисунок 17. Создание инсталляционного пакета. Выбор приложения для установки

Настройки инсталляционного пакета создаются по умолчанию и соответствуют приложению, выбранному для установки. Вы можете их изменять после создания пакета в окне просмотра его свойств (см. п. 4.1.2 на стр. 43).

При создании инсталляционного пакета для установки других приложений (см. рис. 18):

- из раскрывающегося списка выберите: **Создать инсталляционный пакет для приложения, указанного пользователем**;
- укажите путь к дистрибутиву приложения при помощи кнопки **Обзор**;
- установите флажок **Копировать весь каталог в инсталляционный пакет**, если в пакет нужно включить все содержимое каталога, в котором размещен файл дистрибутива;
- укажите параметры запуска исполняемого файла в представленной строке ввода, если они потребуются для установки приложения (например, запуск в неинтерактивном режиме с помощью ключа **/s**).

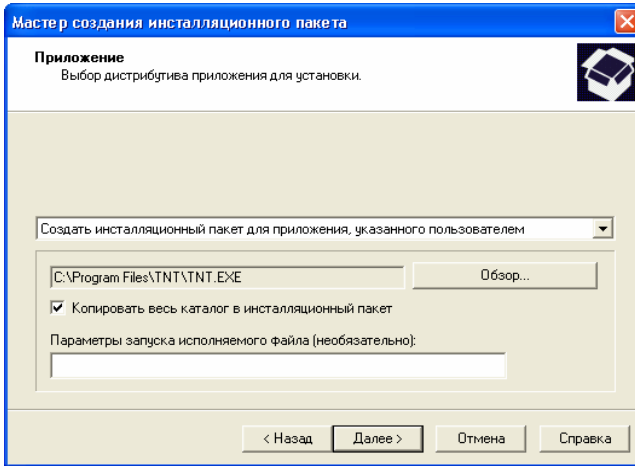


Рисунок 18. Создание инсталляционного пакета для установки приложения, указанного пользователем

4. В следующем окне мастера (см. рис. 19) вы можете указать лицензионный ключ, который будет входить в состав инсталляционного пакета. Для этого нажмите на кнопку **Обзор** и выберите необходимый файл лицензионного ключа (файл имеет расширение **.key**).

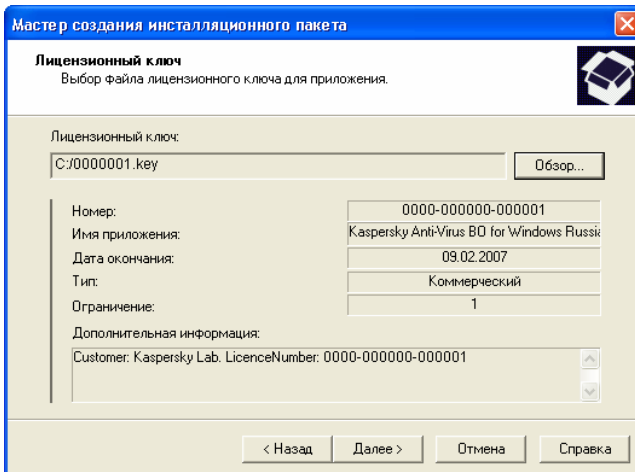


Рисунок 19. Создание инсталляционного пакета. Выбор лицензионного ключа

Если вы не хотите включать лицензионный ключ в состав инсталляционного пакета, просто нажмите на кнопку **Далее**.

При формировании инсталляционного пакета для Сервера и Агента администрирования, указывать лицензионный ключ не требуется.

5. После этого на Сервер администрирования в папку общего доступа загружается необходимый набор файлов для установки заданного приложения на клиентские компьютеры и осуществляется проверка наличия на рабочем месте администратора плагина управления выбранным приложением. Если плагин не установлен или его версия более ранняя, чем у входящего в состав дистрибутива, то производится установка или замена.

По окончании работы мастера сформированный инсталляционный пакет будет добавлен в состав узла **Удаленная установка** и представлен в панели результатов.

4.1.2. Просмотр и настройка параметров инсталляционного пакета

Для просмотра свойств инсталляционного пакета, изменения его названия и настроек:

разверните в дереве консоли узел **Удаленная установка**, выберите в панели результатов нужный инсталляционный пакет и воспользуйтесь командой **Свойства** контекстного меню либо аналогичной командой в меню **Действие**.

В результате открывается окно **Свойства <Имя инсталляционного пакета>** (см. рис. 20), состоящее из закладок: **Общие**, **Настройки**, **Лицензии** и **Перезагрузка ОС**.

Закладка **Общие** (см. рис. 20) содержит общую информацию о пакете:

- название пакета;
- имя и версию приложения, для установки которого пакет сформирован;
- размер пакета;
- дату создания.

Закладка **Настройки** (см. рис. 21) содержит настройки инсталляционного пакета, соответствующие приложению, для установки которого пакет сформирован. Данные настройки формируются по умолчанию на этапе создания пакета, в случае необходимости вы можете их изменить.

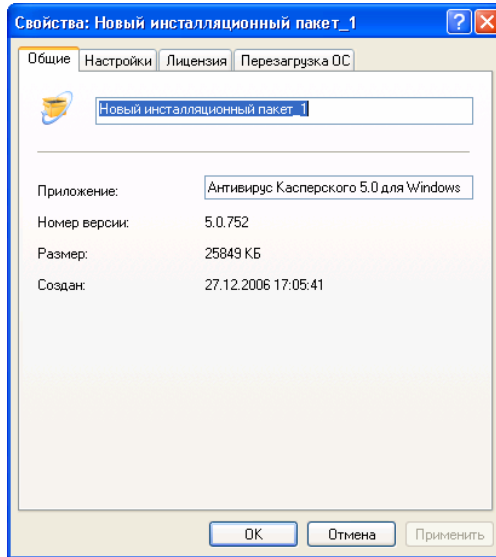


Рисунок 20. Окно просмотра свойств инсталляционного пакета.
Закладка **Общие**

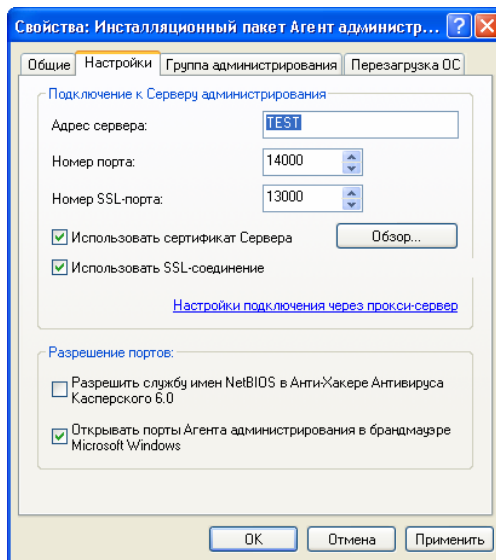


Рисунок 21. Окно просмотра свойств инсталляционного пакета.
Закладка **Настройки**

Закладка **Лицензия** (см. рис. 22) содержит общую информацию о лицензии, соответствующей приложению, для установки которого пакет сформирован.

Закладка **Лицензия** отсутствует в свойствах инсталляционного пакета Агента и Сервера администрирования.

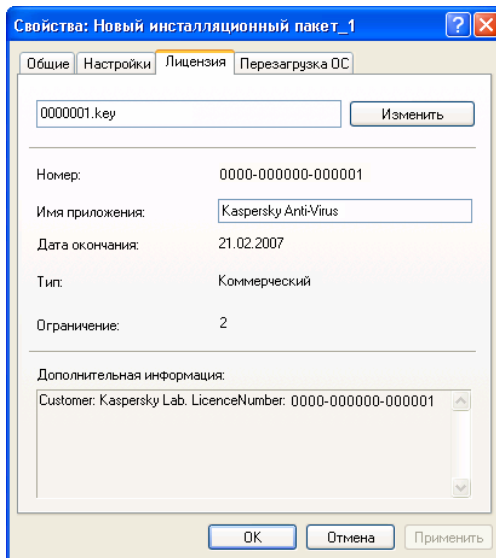


Рисунок 22. Окно просмотра свойств инсталляционного пакета.
Закладка **Лицензия**

На закладке **Переагрузка ОС** (см. рис. 23) вы можете определить действия, которые следует предпринять, если после установки приложения потребуются перезагрузка компьютера. Вы можете выбрать один из вариантов:

- **Не перезагружать операционную систему.**
- **При необходимости перезагрузить операционную систему автоматически** – при этом операционная система будет перезагружена только в случае необходимости.
- **Запросить у пользователя** – в случае выбора данного варианта, вы можете:
 - сформировать информационное сообщение, которое будет выводиться для уведомления пользователя о не-

обходимости перезагрузки операционной системы, в представленном поле ввода;

- установить периодичность повторных уведомлений о необходимости перезагрузки в случае отказа, установив флажок **Повторять запрос каждые (мин.)** и указав интервал вывода сообщения;
- задать автоматическую перезагрузку операционной системы компьютера, если она не будет выполнена пользователем в течение указанного временного интервала, начиная с момента установки приложения. Для этого установите флажок **Форсировать перезагрузку через (мин.)** и укажите величину временного интервала.

Если вы хотите, чтобы при необходимости выполнялась перезагрузка заблокированного компьютера, установите флажок **Закрывать работающие приложения автоматически**. По умолчанию флажок снят.

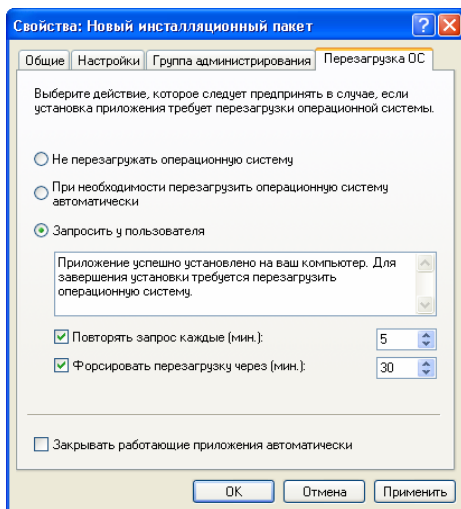


Рисунок 23. Окно просмотра свойств инсталляционного пакета.
Закладка **Перезагрузка ОС**

4.1.3. Создание и настройка инсталляционного пакета для Агента администрирования

Инсталляционный пакет для удаленной установки Агента администрирования не нужно создавать вручную. Он формируется автоматически при установке приложения Kaspersky Administration Kit и располагается в узле **Удаленная установка**.

Если пакет для удаленной установки Агента администрирования был удален, то для его повторного формирования в качестве файла с описанием следует выбрать файл **knagent.kpd**, расположенный в каталоге **NetAgent** дистрибутива Kaspersky Administration Kit.

В настройках инсталляционного пакета для Агента администрирования представлен минимальный набор параметров, необходимый для обеспечения работоспособности компонента сразу после его установки. Значение параметров соответствуют настройкам приложения по умолчанию. В случае необходимости вы можете их изменить на закладках **Настройки** и **Группа администрирования** в окне просмотра свойств инсталляционного пакета.

На закладке **Настройка** (см. рис. 21) представлены параметры, в соответствии с которыми Агент после установки на клиентские компьютеры будет подключаться к Серверу администрирования (по умолчанию при создании проставляются значения, текущего Сервера):

- Адрес компьютера, на котором установлен Сервер администрирования.
- Номер порта, по которому осуществляется незащищенное подключение к Серверу администрирования. По умолчанию используется **14000** порт, если он занят, вы можете его изменить.
- Номер порта, по которому осуществляется защищенное подключение к Серверу администрирования с использованием протокола SSL. По умолчанию это **13000** порт.

Допускается использование только десятичной формы записи.

- Файл сертификата для аутентификации доступа к Серверу администрирования. Значение этого параметра определяет флажок **Использовать сертификат Сервера**.

Если флажок не установлен (по умолчанию), файл сертификата будет получен автоматически с Сервера администрирования при первом подключении к нему Агента.

Если флажок **Использовать сертификат Сервера** установлен, аутентификация будет выполняться на основании указанного при помощи кнопки **Обзор** файла сертификата. Этот файл имеет расширение **.cer** и размещается на Сервере администрирования в каталоге **Cert** каталога установки Kaspersky Administration Kit. Вы можете изменить файл сертификата, выбрав нужный с помощью кнопки **Обзор**.

- Какой порт будет использоваться при подключении Агента администрирования к Серверу: простой или защищенный. Значение параметра определяет флажок **Использовать SSL-соединение**. Если флажок установлен, соединение производится через защищенный порт с использованием SSL-протокола, если снят – через незащищенный.
- Параметры подключения через прокси-сервер. Если при подключении Агента администрирования к Серверу будет использоваться прокси-сервер, щелкните по гиперссылке **Настройки подключения через прокси-сервер**. В открывшемся окне установите флажок **Использовать прокси-сервер** и введите адрес прокси-сервера, имя пользователя и пароль.
- Открытие UDP-порта 137, используемого для получения IP-адреса Сервера администрирования, в Анти-Хакере Антивируса Касперского версии 6.0. Для этого установите флажок **Разрешить службу имен NetBIOS в Анти-Хакере Антивируса Касперского 6.0**.
- Добавление UDP-порта, необходимого для работы Агента администрирования, в список исключений сетевого экрана Microsoft Windows. Для этого установите флажок **Открывать порты Агента администрирования в брандмауэре Microsoft Windows**.

После установки Агента администрирования вы сможете изменять значение параметров подключения к Серверу администрирования через политику и настройки приложения.

При повторной удаленной установке Агента администрирования на клиентский компьютер значения параметров подключения к Серверу и сертификат Сервера администрирования заменяются новыми.

На закладке **Группа администрирования** (см. рис. 24) определяется подгруппа группы **Сеть**, в которую будут добавлены компьютеры после установки на них Агента администрирования. Вы можете выбрать один из вариантов:

- добавить компьютеры в папки, **Соответствующие положению компьютера в Windows-сети**: домену или рабочей группе (вариант выбран по умолчанию),
- добавить все компьютеры **В группу**, заданную в поле ввода. В случае выбора этого варианта введите имя папки в расположенном ниже поле. Если в группе **Сеть** такой папки нет, она будет создана (вы также можете указать имя любой из существующих в группе **Сеть** папок).

В заданную папку будут размещаться все обнаруженные в сети компьютеры, даже если ранее компьютер был обнаружен Сервером администрирования и размещен в папку, соответствующую его положению в сети до установки Агента администрирования.

После установки Агента администрирования вы не сможете изменить папку для размещения компьютеров в группе **Сеть**, данный параметр не входит в состав политики и настроек приложения.

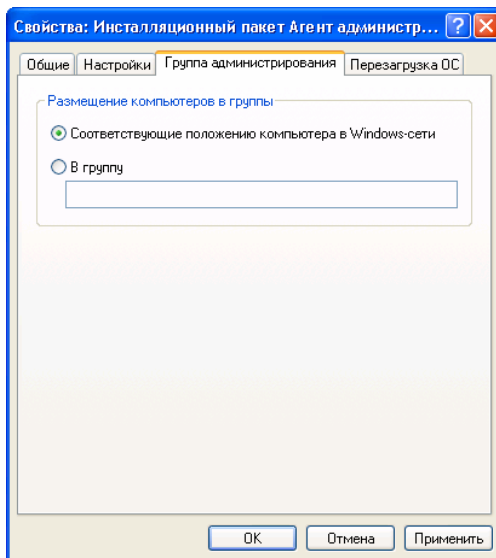


Рисунок 24. Окно просмотра свойств инсталляционного пакета Агента администрирования. Закладка **Группа администрирования**

Агент администрирования устанавливается на компьютер в качестве службы со следующим набором атрибутов:

- имя службы **KLNAgent**;
- выводимое имя **Kaspersky Network Agent**;
- с автоматическим типом запуска, при старте операционной системы;
- с учетной записью **Локальная система**.

Вы можете просматривать свойства службы **Kaspersky Network Agent**, запускать, останавливать и следить за работой при помощи стандартных средств администрирования Windows – **Управление компьютером / Службы**.

4.1.4. Создание и настройка инсталляционного пакета для Сервера администрирования

При создании инсталляционного пакета Сервера администрирования в качестве файла с описанием следует выбрать файл **ak6.kpd**, расположенный в корневом каталоге дистрибутива Kaspersky Administration Kit.

Настройки инсталляционного пакета Сервера администрирования представлены двумя закладками: **Общие** (см. рис. 20) и **Перезагрузка ОС** (см. рис. 23). Все остальные настройки соответствуют настройкам Сервера администрирования по умолчанию.

4.1.5. Создание задачи распространения инсталляционного пакета на подчиненные Серверы администрирования

Для того чтобы сформировать задачу распространения инсталляционного пакета на подчиненные Серверы администрирования:

1. Подключитесь к нужному Серверу администрирования.
2. Выберите в дереве консоли узел **Глобальные задачи**, откройте контекстное меню и выберите команду **Создать** → **Задачу** или воспользуйтесь аналогичным пунктом в

меню **Действие**. В результате запускается мастер, следуйте его указаниям.

3. Для приложения Kaspersky Administration Kit выберите тип задачи **Распространение инсталляционного пакета**.
4. В следующем окне мастера (см. рис. 25) выберите, какие инсталляционные пакеты следует распространять. Выберите один из вариантов:
 - **Все инсталляционные пакеты**.
 - **Выбранные инсталляционные пакеты**. В этом случае в таблице ниже установите флажки рядом с названиями нужных инсталляционных пакетов.

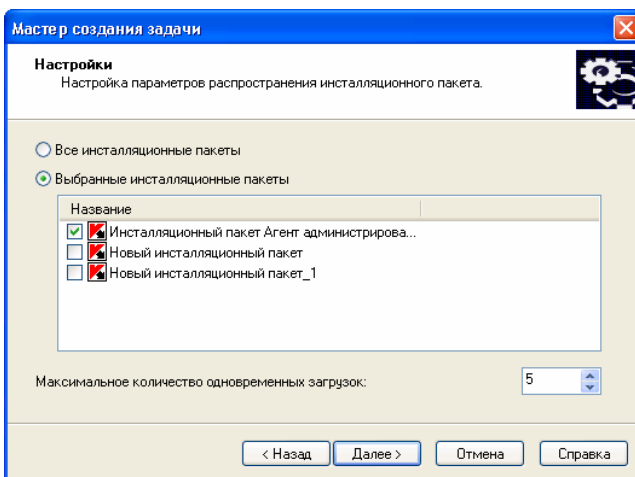


Рисунок 25. Формирование набора инсталляционных пакетов

В поле **Максимальное количество одновременных загрузок** укажите нужное значение.

5. В следующем окне мастера (см. рис. 26) установите флажки рядом с именами подчиненных Серверов администрирования, на которые требуется распространять инсталляционные пакеты.
6. В следующем окне мастера укажите расписание запуска задачи (подробнее см. п. 4.1.7 на стр. 55).
7. Для завершения работы мастера нажмите на кнопку **Готово**.

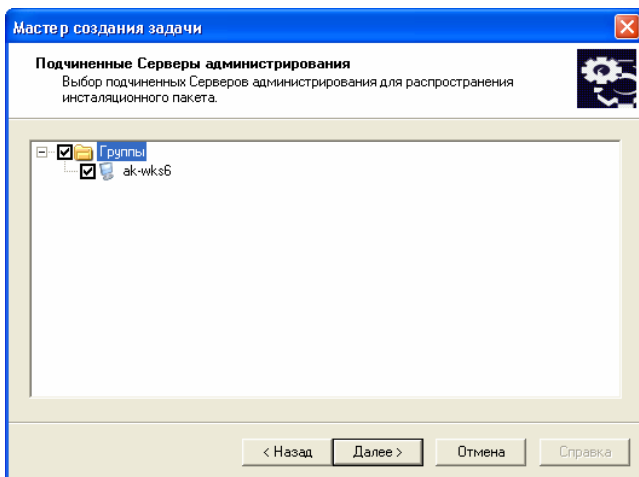


Рисунок 26. Выбор подчиненных Серверов администрирования

4.1.6. Распространение инсталляционных пакетов в пределах группы с помощью агентов обновления

Для распространения инсталляционных пакетов в пределах группы можно использовать агенты обновления. Агенты обновления получают инсталляционные пакеты и обновления с Сервера администрирования и сохраняют их в каталоге установки приложения «Лаборатории Касперского».

Изменять местоположение каталога, содержащего обновления и инсталляционные пакеты, и ограничивать его размер нельзя.

В дальнейшем инсталляционные пакеты распространяются на клиентские компьютеры с помощью многоадресной рассылки. Рассылка новых инсталляционных пакетов в пределах группы производится один раз. Если в момент рассылки клиентский компьютер был отключен от логической сети предприятия, то при запуске задачи установки Агент администрирования автоматически скачивает необходимый инсталляционный пакет с агента обновления.

Для того чтобы сформировать список агентов обновления и настроить их для распространения инсталляционных пакетов на компьютеры в пределах группы,

1. Подключитесь к нужному Серверу администрирования.
2. Выберите в дереве консоли нужную группу, откройте контекстное меню и выберите команду **Свойства** или воспользуйтесь аналогичным пунктом в меню **Действие**.
3. В открывшемся окне свойств группы на закладке **Агенты обновления** (см. рис. 27) с помощью кнопок **Добавить** и **Удалить** сформируйте список компьютеров, которые будут выполнять роль агентов обновления в пределах группы.

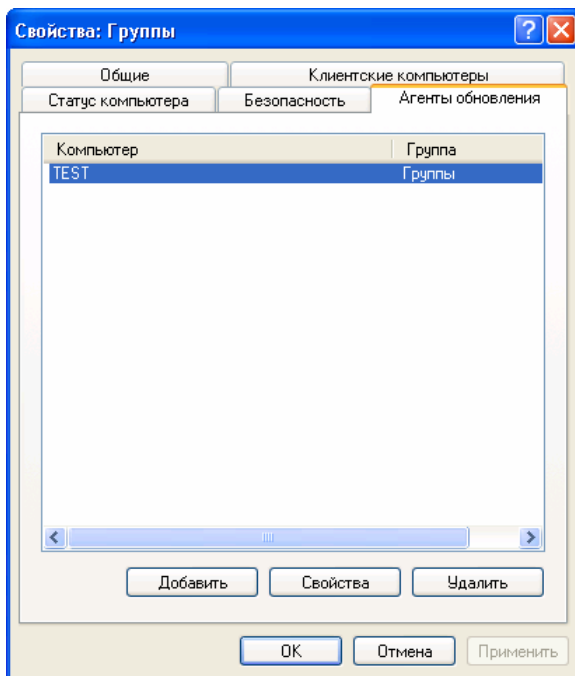


Рисунок 27. Окно свойств группы.
Закладка **Агенты обновления**

4. Отредактируйте настройки агента обновления. Для этого выберите агента в списке и нажмите на кнопку **Свойства**. В открывшемся окне **<Имя агента обновления> свойства** (см. рис. 28):
 - укажите номер порта, по которому осуществляется подключение клиентского компьютера к агенту обновления. По умолчанию используется **14001** порт, если он занят, вы можете его изменить;
 - укажите номер порта, по которому осуществляется защищенное подключение клиентского компьютера к агенту обновления с использованием протокола SSL. По умолчанию это **13001** порт.
 - установите флажок **Использовать многоадресную IP-рассылку** и заполните поля **Адрес IP-рассылки** и **Номер порта IP-рассылки**.

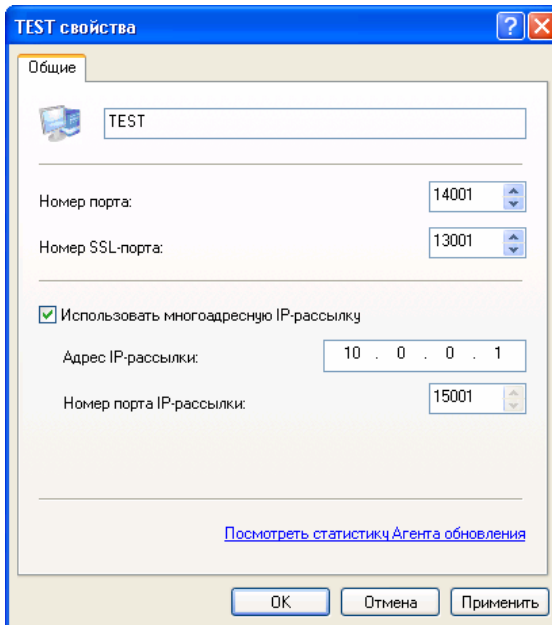


Рисунок 28. Окно свойств агента обновления

5. Нажмите на кнопку **Применить** или **OK**.

4.1.7. Создание задачи удаленной установки

При выполнении задачи удаленная установка программного обеспечения на клиентские компьютеры осуществляется одним из двух методов: методом **форсированной установки** или **установки с помощью сценария запуска**.

Форсированная установка позволяет провести удаленную установку программного обеспечения на конкретные клиентские компьютеры логической сети. При запуске задачи Сервер администрирования копирует из папки общего доступа набор файлов для установки приложения на каждый клиентский компьютер во временный каталог и производит запуск программы установки на каждом из них. Для успешного выполнения задачи методом форсированной установки Сервер администрирования должен обладать правами локальных администраторов на клиентских компьютерах логической сети. Данный метод рекомендуется для установки приложений на компьютеры, работающие под управлением операционных систем Microsoft Windows NT/2000/2003/XP, в которых поддерживается такая возможность, либо на компьютеры под управлением Microsoft Windows 98/Me, на которых установлен Агент администрирования.

В случае если соединение Сервера администрирования и клиентского компьютера осуществляется через интернет или защищено межсетевым экраном, использовать папки общего доступа для передачи данных невозможно. В этом случае доставку необходимых для установки приложения файлов на клиентский компьютер может осуществлять Агент администрирования. Установка Агента администрирования на такие компьютеры проводится локально.

Второй метод – **установка с помощью сценария запуска** – позволяет закрепить запуск задачи удаленной установки за конкретной учетной записью пользователя (нескольких пользователей). В результате выполнения задачи в сценарии запуска для заданных пользователей вносится запись о запуске программы установки, расположенной в папке общего доступа Сервера администрирования. Для успешного выполнения задачи учетная запись, под которой она запускается, либо Сервер администрирования должны обладать правом на изменение сценариев запуска в базе данных контроллера домена. Таким правом обладает администратор домена, т.о. задача или весь Сервер администрирования должны запускаться с правами этого пользователя. В результате при регистрации пользователя в домене предпринимается попытка провести установку приложения на клиентском компьютере, с которого пользователь

зарегистрировался. Данный метод рекомендуется для установки приложений компании на компьютеры, работающие под управлением операционных систем Microsoft Windows 98/Me.

Для успешного выполнения задачи удаленной установки с помощью сценария запуска пользователя, для которых вносятся изменения в сценарии, должны обладать правами локального администратора на своих компьютерах.

Групповые задачи удаленной установки программного обеспечения на клиентские компьютеры выполняются только методом форсированной установки. При создании глобальной задачи, вы можете выбрать необходимый вам метод: форсированная установка или установка с помощью сценария запуска.

Для создания глобальной задачи удаленной установки с помощью метода форсированной установки:

1. Подключитесь к нужному Серверу администрирования.
2. Выберите в дереве консоли узел **Глобальные задачи**, откройте контекстное меню и выберите команду **Создать / Задачу** или воспользуйтесь аналогичным пунктом в меню **Действие**. В результате запускается мастер создания задачи, следуйте его указаниям.
3. Определите имя задачи.
4. При выборе приложения и определении типа задачи (см. рис. 29) установите значения **Kaspersky Administration Kit** и **Удаленная установка приложения** соответственно.
5. После этого укажите инсталляционный пакет, установка которого будет проводиться при выполнении данной задачи (см. рис. 30). Выберите нужный из числа пакетов, сформированных для данного Сервера администрирования, либо создайте новый при помощи кнопки **Новый**.

Некоторые приложения, управление которыми осуществляется с помощью Kaspersky Administration Kit, могут быть установлены на компьютеры только локально. Подробную информацию см. в Руководствах к соответствующим приложениям.

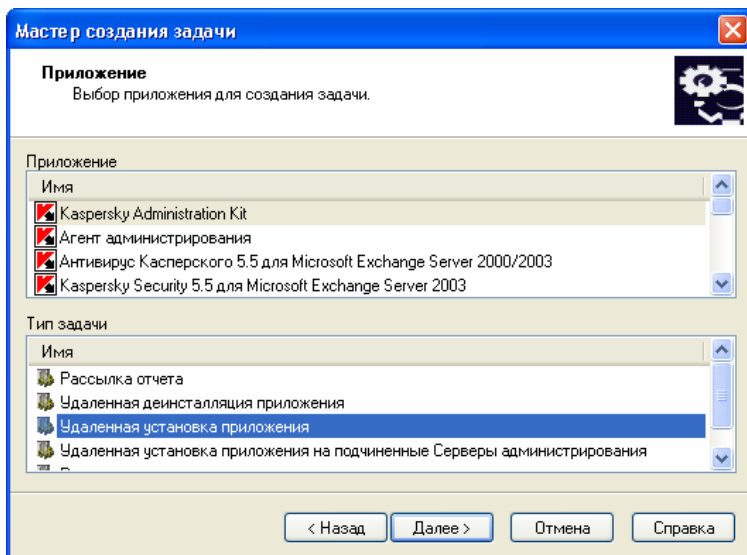


Рисунок 29. Определение типа задачи

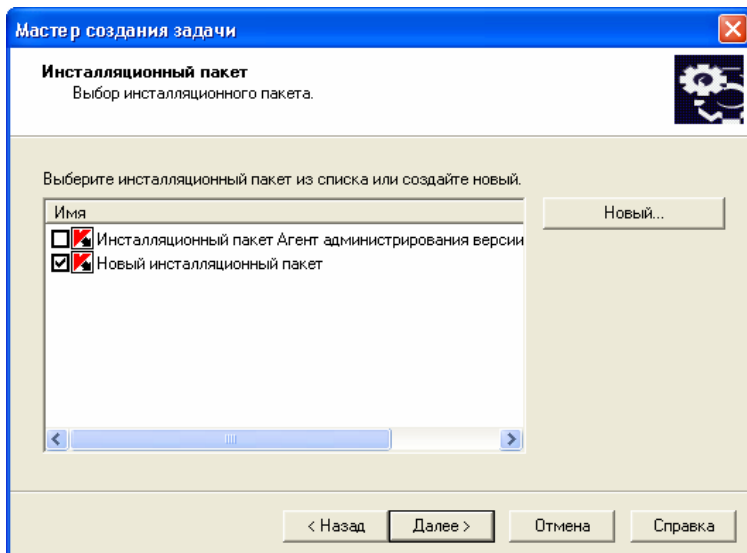


Рисунок 30. Выбор инсталляционного пакета для установки

6. На данном этапе выберите вариант **Форсированная установка** (см. рис. 31).

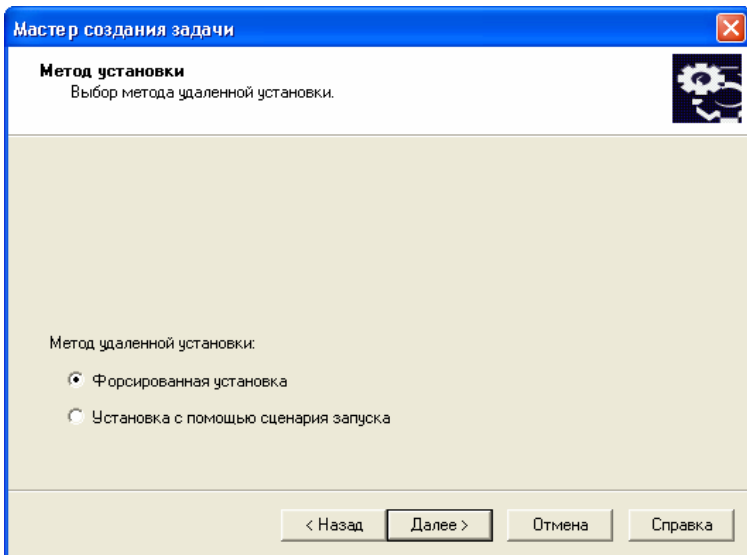


Рисунок 31. Выбор метода установки

7. В этом окне мастера (см. рис. 32) вам будет предложено определить дополнительные параметры установки:

- Нужно ли переустанавливать приложение, если оно уже установлено на компьютере.

Установите флажок **Не устанавливать приложение, если оно уже установлено** для того, чтобы повторная установка не проводилась (по умолчанию флажок установлен). В этом случае для тех компьютеров, где приложение уже установлено локально или в результате предыдущего запуска задачи удаленной установки по расписанию, задача запускаться не будет.

Если флажок снят, задача удаленной установки будет запускаться по расписанию до тех пор, пока не будет исчерпано количество попыток установки.

- Задать способ доставки необходимых для установки приложения файлов на клиентские компьютеры.

Для этого в группе полей **Загрузка инсталляционного пакета** выполните:

- Установите флажок **Средствами Microsoft Windows из папки общего доступа** для того, чтобы передача необходимых для установки приложения файлов на клиентские компьютеры осуществлялась средствами Windows через папки общего доступа (по умолчанию флажок установлен).
 - Установите флажок **С помощью Агента администрирования** для того, чтобы доставку файлов на клиентские компьютеры осуществлял установленный на каждом из них Агент администрирования (по умолчанию флажок установлен).
 - Укажите максимальное число клиентских компьютеров, которые могут одновременно скачивать информацию с Сервера администрирования в поле **Максимальное количество одновременных загрузок**.
- Установить количество попыток провести установку при запуске задачи по расписанию, установив нужное значение в поле **Количество попыток**. Повторные попытки предпринимаются в случае возникновения ошибок в ходе выполнения предыдущей установки.

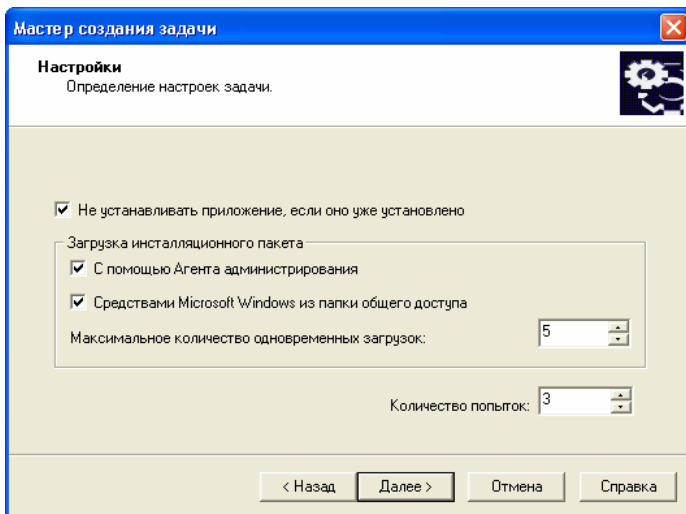


Рисунок 32. Дополнительные параметры установки

8. На этом шаге (см. рис. 33) вам будет предложено установить совместно с приложением Агент администрирования.

Мы рекомендуем вам воспользоваться совместной установкой для уменьшения нагрузки на Сервер администрирования. Для этого установите флажок **Установить совместно с Агентом администрирования** и установите флажок рядом с именем нужного инсталляционного пакета. При необходимости создайте новый инсталляционный пакет с помощью кнопки **Создать**.

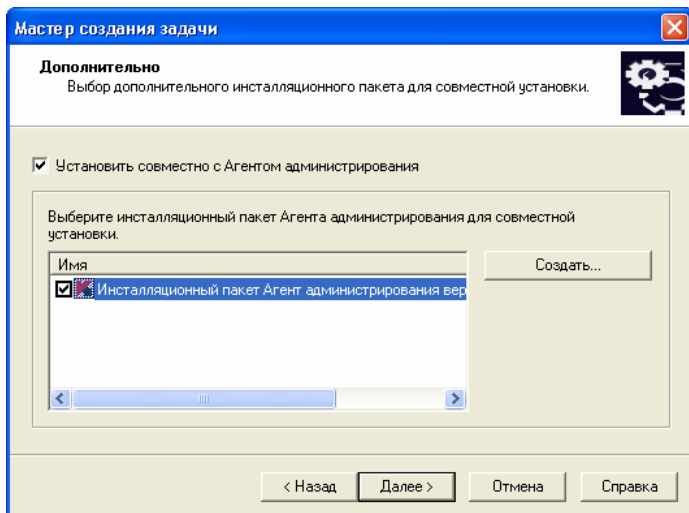


Рисунок 33. Выбор совместной установки с Агентом администрирования

9. Определите способ выбора компьютеров, для которых будет создана задача (см. рис. 34):

- **На основании данных, полученных в ходе опроса Windows-сети.** В этом случае выбор компьютеров для установки производится на основании данных, получаемых Сервером администрирования при опросе Windows-сети предприятия.
- **На основании адресов (IP-адрес, NetBIOS- или DNS-имя), вводимых вручную.** В этом случае компьютеры для установки будут выбираться вручную.

Если выбор компьютеров будет проводиться на основании данных, полученных в ходе опроса Windows-сети, то формирование списка производится в окне мастера (см. рис. 35) и осу-

ществляется так же, как при добавлении компьютеров в состав логической сети (подробнее см. Справочное руководство для Kaspersky Administration Kit). Вы можете выбрать как клиентские компьютеры логической сети, (папка **Группы**) так и компьютеры, не включенные еще в ее состав (папка **Сеть**).

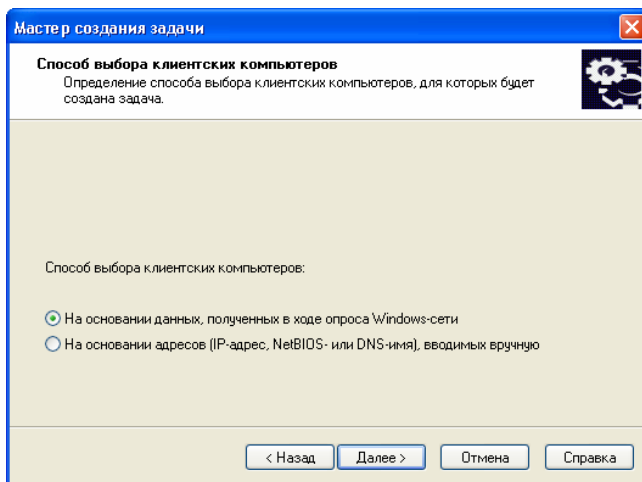


Рисунок 34. Определение способа выбора клиентских компьютеров

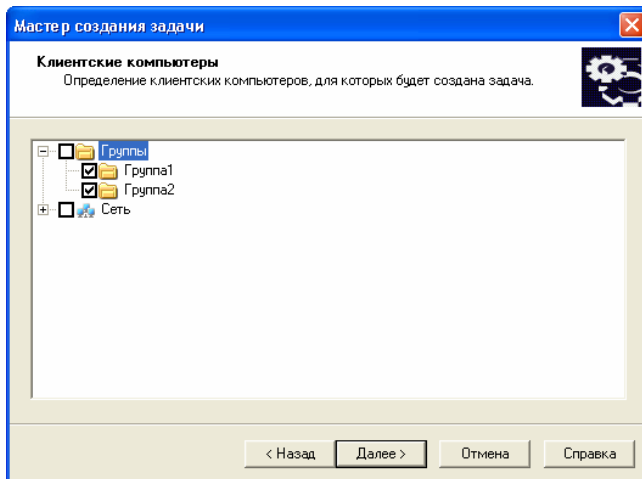


Рисунок 35. Формирование списка компьютеров для установки на основании данных Windows-сети

Если выбор компьютеров будет проводиться вручную, то формирование списка осуществляется за счет ввода NetBIOS- или DNS-имен, IP-адресов (или диапазона IP-адресов) компьютеров, либо импортом списка из *txt*-файла, в котором каждый адрес должен быть указан с новой строки (см. рис. 36).

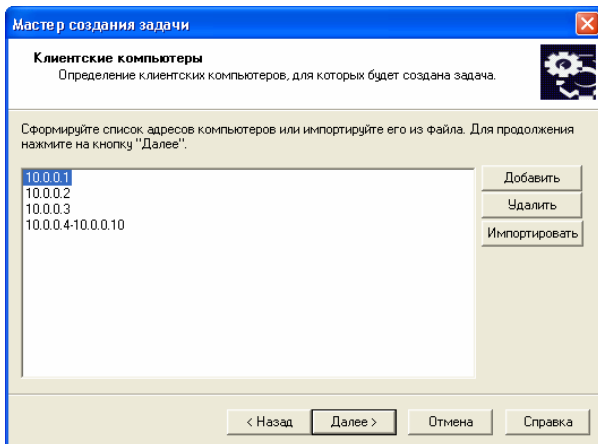


Рисунок 36. Формирование списка компьютеров для установки на основании IP-адресов

10. В следующем окне мастера укажите, под какой учетной записью будет запускаться задача удаленной установки на компьютерах (см. рис. 37).

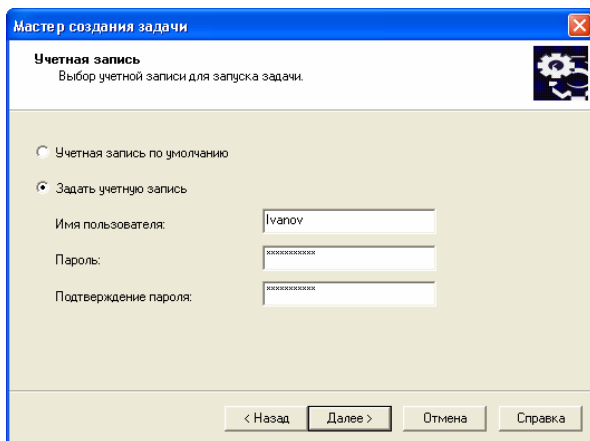


Рисунок 37. Выбор учетной записи

Учетная запись должна обладать правами администратора на всех компьютерах, где планируется провести удаленную установку программного обеспечения.

При установке программного обеспечения на компьютеры, входящие в состав различных доменов, необходимо наличие доверительных отношений между этими доменами и доменом, в котором работает Сервер администрирования.

Выберите один из вариантов:

- **Учетная запись по умолчанию** – если Сервер администрирования запускается под учетной записью пользователя домена (см. п. 3.2 на стр. 19) и она обладает необходимыми правами для установки программного обеспечения.
- **Задать учетную запись** – если Сервер администрирования запускается под учетной записью системы, или учетная запись Сервера администрирования не обладает правами на запуск задач удаленной установки.

Для удаленной установки программного обеспечения на компьютеры, не входящие в состав домена, следует запускать задачу удаленной установки под учетной записью пользователя, обладающего правами администратора на этих компьютерах.

В представленных ниже полях укажите атрибуты пользователя, учетная запись которого удовлетворяет необходимым условиям.

11. Далее составьте расписание запуска задачи (см. рис. 38).

- В раскрывающемся списке **Запуск по расписанию** выберите нужный режим запуска задачи:
 - **Вручную**
 - **Каждый N час.**
 - **Ежедневно.**
 - **Еженедельно.**
 - **Ежемесячно.**
 - **Один раз** (в этом случае запуск задачи удаленной установки на компьютерах будет осуществлен только один раз независимо от того, с каким результатом закончится ее выполнение).

- **Немедленно** (сразу после создания задачи, по завершению работы мастера).
- **По завершении другой задачи** (в этом случае задача удаленной установки будет запускаться только после завершения работы указанной задачи).
- Проведите настройку параметров расписания в группе полей, соответствующих выбранному режиму (подробнее см. Справочное руководство для Kaspersky Administration Kit).

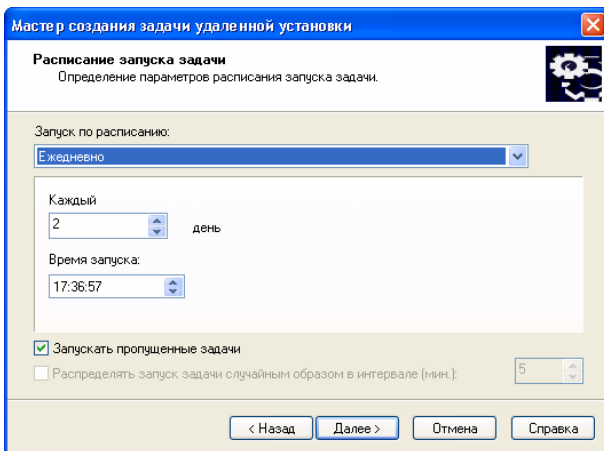


Рисунок 38. Ежедневный запуск задачи

Для создания глобальной задачи удаленной установки с помощью сценария запуска:

1. Подключитесь к нужному Серверу администрирования.
2. Выберите в дереве консоли узел **Глобальные задачи**, откройте контекстное меню и выберите команду **Создать / Задачу** или воспользуйтесь аналогичным пунктом в меню **Действие**. В результате запускается мастер создания задачи, следуйте его указаниям.
3. Определите имя задачи.
4. При выборе приложения и определении типа задачи (см. рис. 29) установите значения **Kaspersky Administration Kit** и **Удаленная установка приложения** соответственно.
5. В следующем окне (см. рис. 30) укажите инсталляционный пакет для установки. Это выполняется так же, как и при использовании метода форсированной установки (см. выше).

- После этого выберите вариант **Установка с помощью сценария запуска** (см. рис. 31).
- В следующем окне мастера (см. рис. 39) выберите учетные записи пользователей, для которых необходимо внести изменения в сценарии запуска.

Во время запуска задачи установки Kaspersky Administration Kit проверяет, назначен ли сценарий запуска каким-либо еще пользователям помимо выбранных. Если да, то установка не будет произведена. При этом в отчет будет записана информация о соответствующей ошибке.

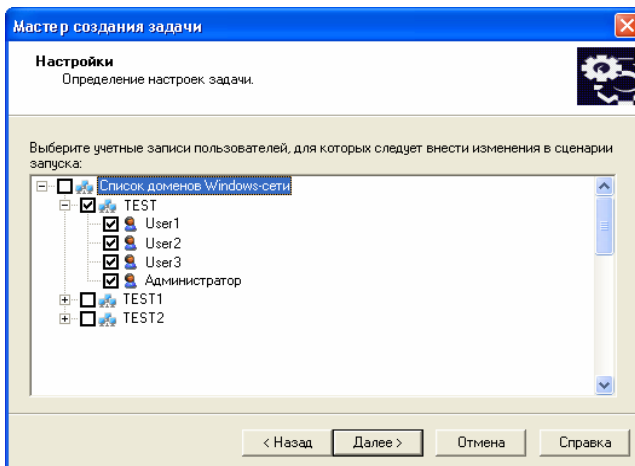


Рисунок 39. Выбор учетных записей

- На следующем шаге мастера (см. рис. 37), так же, как и при использовании метода форсированной установки (см. выше), укажите учетную запись, под которой будет запускаться задача удаленной установки на клиентских компьютерах.
- В окне **Расписание запуска задачи** (см. рис. 38) сформируйте расписание так же, как оно формируется для задачи форсированной установки (см. выше).

По окончании работы мастера сформированная задача удаленной установки будет добавлена в состав узла **Глобальные задачи** и представлена в панели результатов. В случае необходимости вы можете вносить изменения в ее настройки (подробнее см. п. 4.1.8 на стр. 66).

Для этого,

выберите в дереве консоли узел **Удаленная установка**, выделите в панели результатов нужный вам инсталляционный пакет, откройте контекстное меню и выберите команду **Установить** или воспользуйтесь аналогичным пунктом в меню **Действие**. В результате запускается мастер создания задачи удаленной установки, описанный выше, однако в нем опущены шаги выбора типа задачи и инсталляционного пакета. Следуйте указаниям мастера.

Также можно запустить мастер создания групповой задачи удаленной установки.

Для этого,

выберите в дереве консоли узел **Группы**, откройте контекстное меню и выберите команду **Установить** или воспользуйтесь аналогичным пунктом в меню **Действие**. В результате запускается мастер создания задачи удаленной установки, описанный выше, однако в нем опущены шаги выбора типа задачи и группы компьютеров. Следуйте указаниям мастера.

4.1.8. Настройка задачи удаленной установки

Настройка задачи удаленной установки осуществляется так же, как и настройка любой из задач (подробнее см. Справочное руководство для Kaspersky Administration Kit). Рассмотрим подробнее специфичные для данного типа задачи параметры, представленные на закладке **Настройки**.

В случае редактирования задачи, которая будет осуществлять удаленную форсированную установку (см. рис. 40), вы можете:

- определить, нужно ли переустанавливать приложение, если оно уже установлено на клиентском компьютере;
- задать способ доставки необходимых для установки приложения файлов на клиентские компьютеры и указать максимальное число одновременных соединений;
- установить количество попыток провести установку при запуске задачи по расписанию.

При настройке задачи удаленной установки с помощью сценария запуска на закладке **Настройки** вы можете изменить список учетных записей пользователей, для которых будут внесены изменения в сценарии запуска (см. рис. 41). Редактирование списка осуществляется при помощи кнопок **Добавить** и **Удалить**.

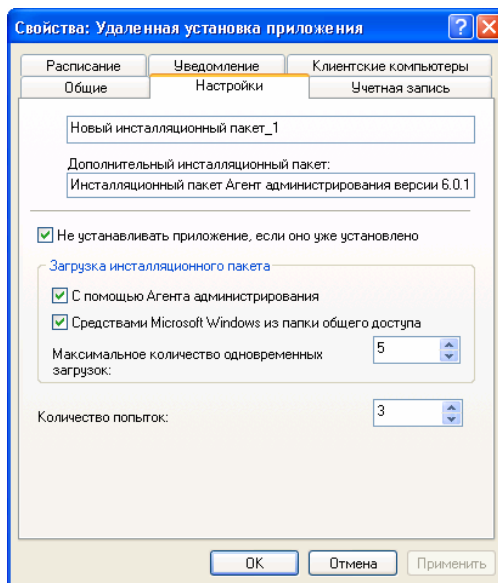


Рисунок 40. Настройка задачи удаленной установки.
Метод форсированной установки

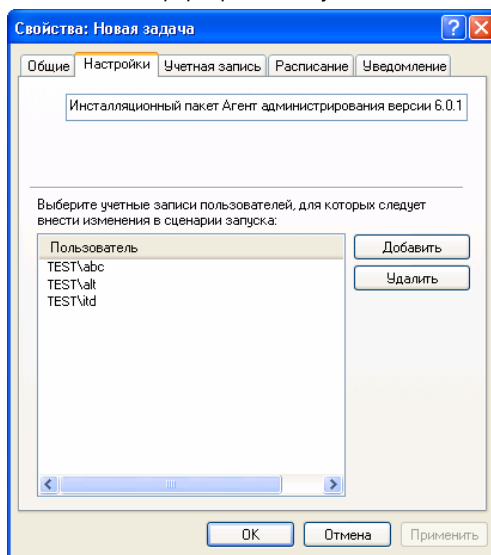


Рисунок 41. Настройка задачи удаленной установки с помощью сценария запуска

4.1.9. Удаленная установка приложений на подчиненные Серверы администрирования

С помощью этой задачи вы можете устанавливать и обновлять программное обеспечение на подчиненных Серверах администрирования.

До начала формирования задачи убедитесь в том, что соответствующий устанавливаемому приложению инсталляционный пакет находится на подчиненных Серверах администрирования. Если его там нет, распространите его с помощью задачи **Распространение инсталляционного пакета** (см. п. 4.1.5 на стр. 50).

Для создания задачи удаленной установки приложения на подчиненные Серверы администрирования:

1. Подключитесь к нужному Серверу администрирования.
2. Выберите в дереве консоли узел **Групповые задачи** (если вы хотите сформировать задачу для всех подчиненных Серверов группы) или **Глобальные задачи** (если вы хотите сформировать задачу для определенного набора подчиненных Серверов). Откройте контекстное меню и выберите команду **Создать / Задачу** или воспользуйтесь аналогичным пунктом в меню **Действие**. В результате запускается мастер создания задачи, следуйте его указаниям.
3. Определите имя задачи.
4. При выборе приложения и определении типа задачи (см. рис. 29) установите значения **Kaspersky Administration Kit** и **Удаленная установка приложения на подчиненные Серверы администрирования** соответственно.
5. После этого укажите инсталляционный пакет, установка которого будет проводиться при выполнении данной задачи (см. рис. 30).
6. В следующем окне (см. рис. 42), если необходимо, установите флажок **Не устанавливать приложение, если оно уже установлено**. При этом учитывается точная версия приложения.

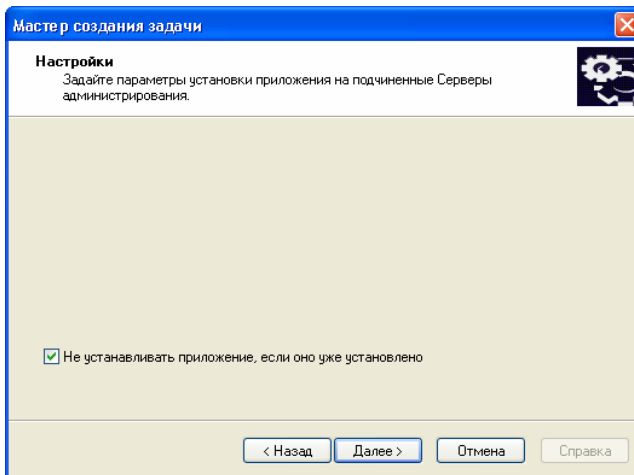


Рисунок 42. Настройка задачи удаленной установки приложения на подчиненные Серверы администрирования

7. Если формируется групповая задача, этот шаг отсутствует. Для глобальной задачи в окне **Подчиненные Серверы администрирования** (см. рис. 43) сформируйте набор подчиненных Серверов администрирования.

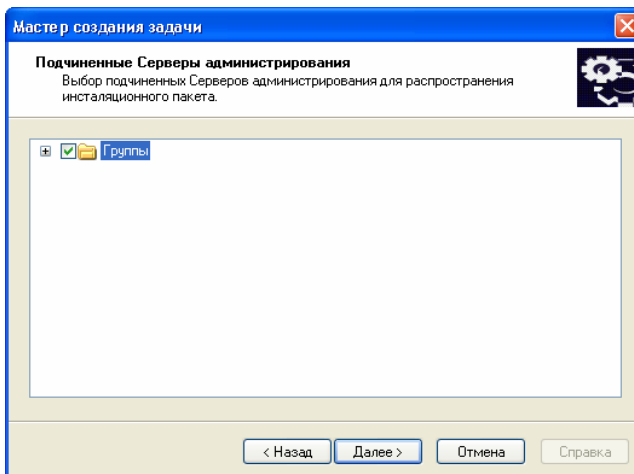


Рисунок 43. Формирование набора подчиненных Серверов администрирования

8. Сформируйте расписание запуска задачи (см. п. 4.1.7 на стр. 55).

При редактировании задачи запуска и остановки приложения (см. рис. 44) вы можете вносить изменения в описанные выше настройки.

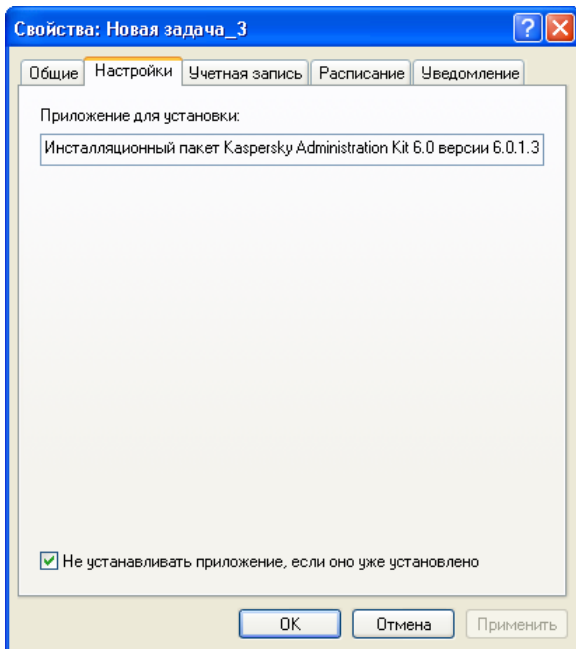


Рисунок 44. Задача удаленной установки приложения на подчиненные Серверы администрирования. Закладка **Настройки**

4.1.10. Удаленная деинсталляция программного обеспечения

Для того чтобы провести удаленную деинсталляцию программного обеспечения:

Создайте задачу аналогично задаче удаленной установки (см. п. 4.1.7 на стр. 55), при этом в качестве типа задачи выберите **Удаленная деинсталляция приложения** и в окне **Приложение** (см. рис. 45) в раскрывающемся списке **Приложение для деинсталляции** укажите нужное приложение «Лаборатории Касперского». Для того чтобы удалить стороннее приложение, установите флажок **Удалить стороннее приложение** и выберите приложение для удаления.

В раскрывающихся списках перечислены приложения, обнаруженные на компьютерах логической сети после установки на них Агента администрирования.

Сформированная вами задача будет запускаться на выполнение в соответствии со своим расписанием.

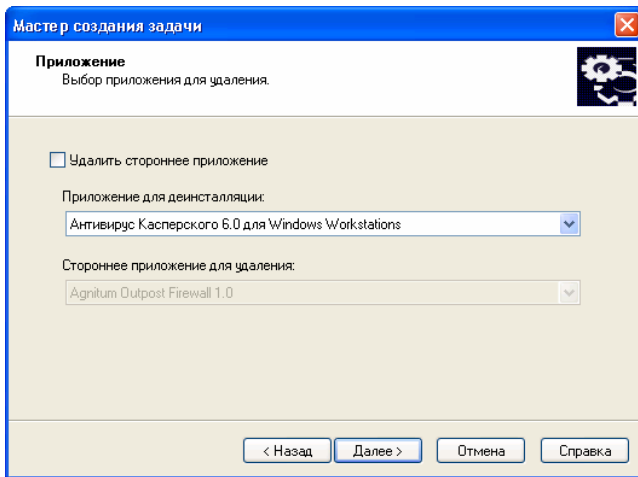


Рисунок 45. Выбор приложения для удаления

4.2. Мастер удаленной установки

Для установки приложений компании вы можете воспользоваться мастером удаленной установки. Мастер позволяет проводить удаленную установку приложений методом форсированной установки, как с использованием сформированных инсталляционных пакетов, так и непосредственно с дистрибутива.

В результате работы мастера осуществляется:

- создание инсталляционного пакета для установки приложения (если он не был создан раньше). Пакет размещается в узле **Удаленная установка** с именем, соответствующим названию и версии приложения и может быть использован для установки приложения в дальнейшем.
- создание и запуск глобальной или групповой задачи удаленной установки. Сформированная задача размещается в папке **Глобальные**

задачи или **Групповые задачи** группы, для которой она была создана и может быть запущена в дальнейшем вручную. Имя задачи соответствует имени пакета для установки приложения: **Установка <Имя выбранного инсталляционного пакета>**.

Для установки приложения с помощью мастера удаленной установки:

1. Подключитесь к нужному Серверу администрирования.
2. В главном окне программы Kaspersky Administration Kit выберите в дереве консоли узел, соответствующий нужному Серверу администрирования, откройте контекстное меню и выберите команду **Мастер удаленной установки** или воспользуйтесь аналогичным пунктом в меню **Действие**. В результате запускается мастер, следуйте его указаниям.
3. В открывшемся окне (см. рис. 46) укажите инсталляционный пакет, установка которого будет проводиться. Если вы проводите установку приложения с дистрибутива, и/или инсталляционный пакет не сформирован, сформируйте новый инсталляционный пакет. Для этого нажмите на кнопку **Новый**, в результате запускается мастер создания инсталляционного пакета (см. п. 4.1.1 на стр. 40).

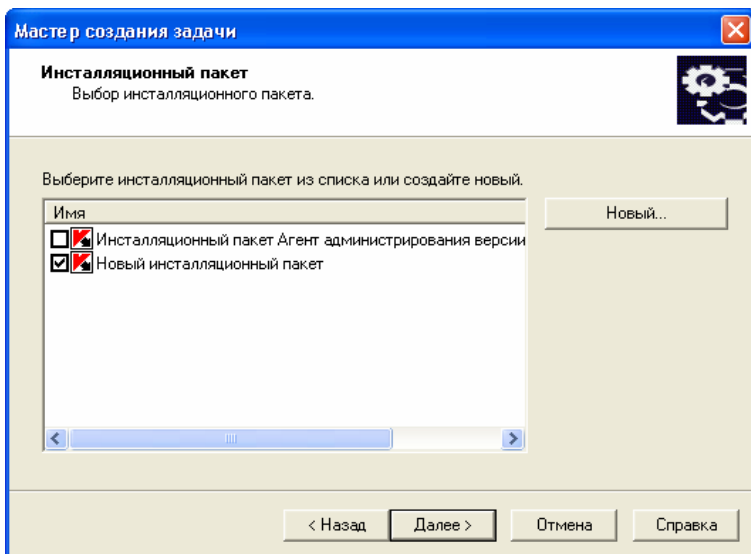


Рисунок 46. Выбор инсталляционного пакета

4. В следующем окне мастера при необходимости укажите инсталляционный пакет Агента администрирования для совместной установки (подробнее см. п. 4.1.7 на стр. 55).
5. В представленном окне мастера (см. рис. 47) определите на какие компьютеры будет выполняться установка приложения. Для этого выберите один из вариантов:
 - **Установить приложение на выбранные компьютеры**, в случае выбора данного варианта после завершения работы мастера будет сформирована глобальная задача удаленной установки приложения.
 - **Установить приложение на компьютеры в группе администрирования** – в результате работы мастера будет создана групповая задача.

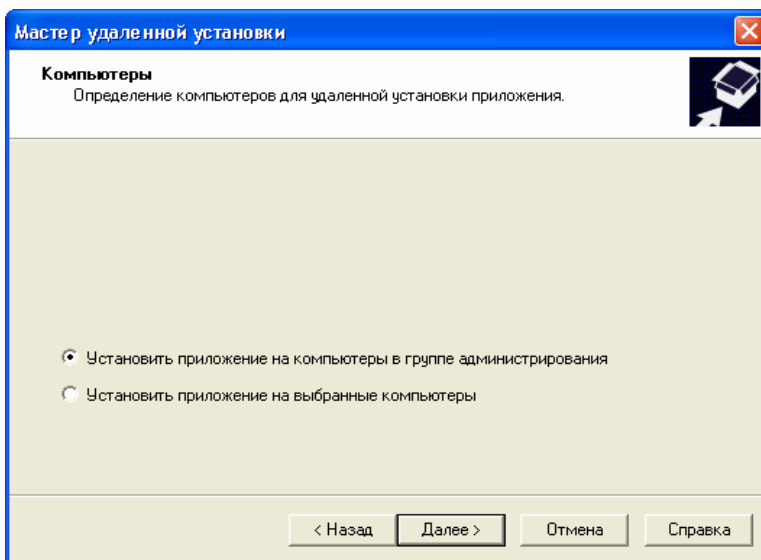


Рисунок 47. Выбор типа задачи

6. Далее, в случае создания групповой задачи, укажите группу, на компьютеры которой, будет проводиться удаленная установка (см. рис. 48), либо выберите компьютеры для установки. Если приложение должно быть установлено на все клиентские компьютеры логической сети, выберите группу **Группы**.

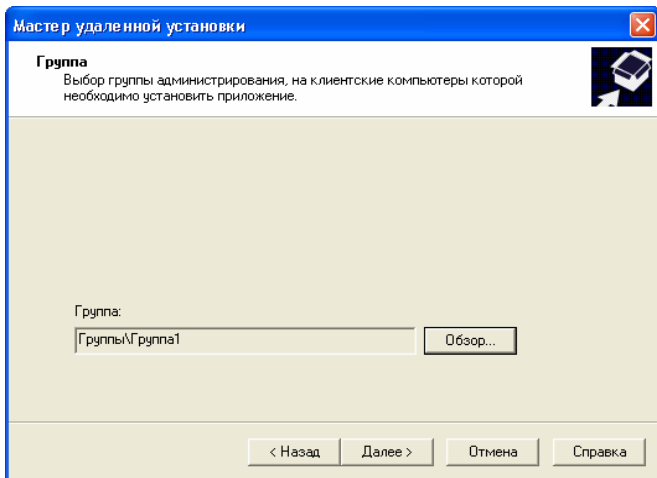


Рисунок 48. Выбор группы

7. Далее определите, под какой учетной записью будет запускаться задача удаленной установки на компьютерах (подробнее см. п. 4.1.7 на стр. 55).

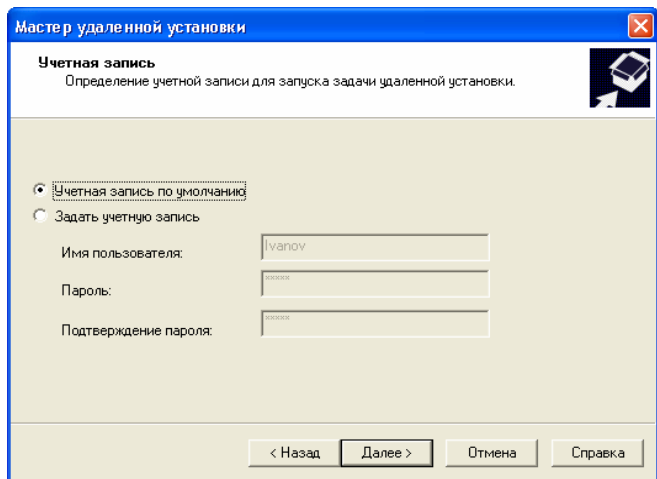


Рисунок 49. Выбор учетной записи пользователя

8. После этого появляется окно, в котором отображается процесс распространения и выполнения задачи удаленной установки на компьютерах выбранной группы (см. рис. 50). Вы перейти к

заключительному окну мастера, не дожидаясь окончания процесса. Для этого нажмите на кнопку **Далее**. Подробную информацию о результатах выполнения задачи на каждом компьютере вы можете посмотреть при помощи кнопки **Результаты**.

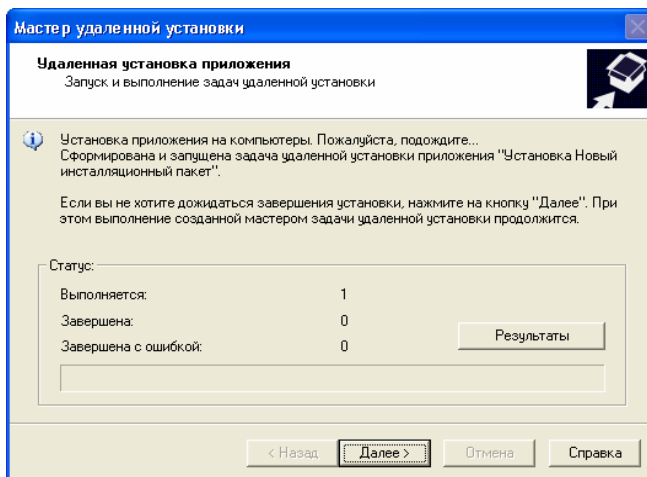


Рисунок 50. Выполнение задачи удаленной установки

4.3. Локальная установка программного обеспечения

Локальная установка осуществляется на каждом компьютере отдельно. Для ее проведения необходимо обладать правами администратора на локальном компьютере.

Ряд приложений, управление которыми осуществляется с помощью Kaspersky Administration Kit, могут быть установлены на компьютеры только локально. Подробную информацию см. в Руководствах к соответствующим приложениям.

Общий порядок установки программного обеспечения при локальном развертывании системы антивирусной защиты может быть следующим:

- установите Агент администрирования и настройте связь клиентского компьютера с Сервером администрирования (см. п. 4.3.1 на стр. 76);
- установите необходимые приложения на компьютеры, которые будут входить в систему антивирусной защиты, согласно описаниям, изложенным в соответствующих Руководствах;
- установите плагин управления для каждого из установленных приложений компании на рабочее место администратора (см. п. 4.3.2 на стр. 81).

Kaspersky Administration Kit поддерживает возможность локальной установки приложений в неинтерактивном режиме на основании формируемых при создании инсталляционного пакета файлов (см. п. 4.3.3 на стр. 81).

4.3.1. Локальная установка Агента администрирования

Для того чтобы установить Агент администрирования на компьютер локально:

1. Запустите исполняемый файл **setup.exe** (или **setup.msi**), расположенный на дистрибутивном компакт-диске приложения Kaspersky Administration Kit в каталоге **NetAgent**. Установка сопровождается мастером. Он предложит вам провести настройку параметров установки. Следуйте его указаниям.
2. Первые шаги установки традиционны и состоят в распаковке с дистрибутива необходимых файлов и записи их на жесткий диск вашего компьютера, принятии лицензионного соглашения, а также вводе информации о пользователе и компании.
3. Далее определите каталог для установки Агента администрирования. По умолчанию это **Program Files\Kaspersky Lab\NetworkAgent**. Если такого каталога нет, он будет создан автоматически. Смена каталога осуществляется при помощи кнопки **Обзор**.
4. В следующем окне мастера (см. рис. 51) необходимо настроить параметры подключения Агента администрирования к Серверу администрирования. Для этого определите:
 - адрес компьютера, на котором установлен или будет установлен Сервер администрирования. В качестве адреса компьютера можно использовать IP-адрес или имя компью-

тера в Windows-сети. Компьютер также можно выбрать с помощью кнопки **Обзор**.

- нужно ли открывать UDP-порта 137, используемый для получения IP-адреса Сервера администрирования, в Анти-Хакере Антивируса Касперского версии 6.0. Для этого установите флажок **Разрешить службу имен NetBIOS в Анти-Хакере Антивируса Касперского 6.0**.
- номер порта, по которому Агент администрирования будет подключаться к Серверу администрирования. По умолчанию используется **14000** порт, если он занят, вы можете его изменить. Допускается использование только десятичной формы записи.
- номер порта, по которому будет осуществляться подключение с использованием протокола SSL. По умолчанию используется **13000** порт, если он занят, вы можете его изменить. Допускается использование только десятичной формы записи. Для того чтобы подключение осуществлялось через защищенный порт (с использованием SSL протокола), установите флажок **Использовать SSL-соединение**.

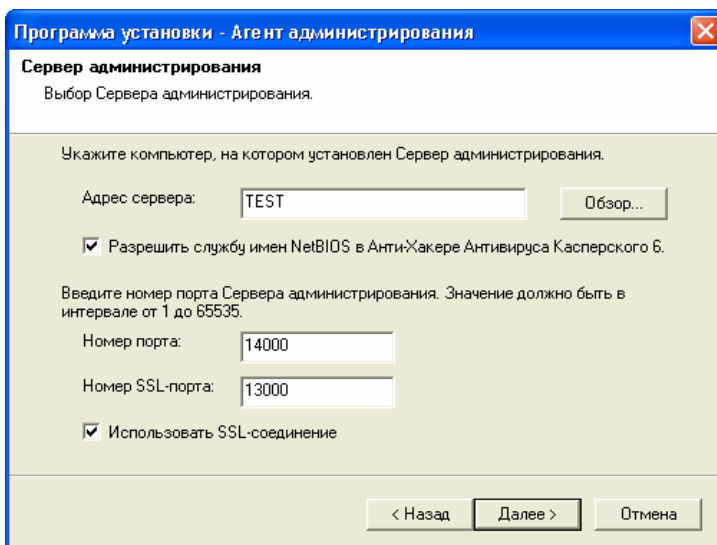


Рисунок 51. Настройка параметров подключения к Серверу администрирования

5. Если подключение Агента администрирования к Серверу будет выполняться через прокси-сервер, в представленном окне (см. рис. 52) настройте параметры подключения:
 - Установите флажок **Использовать прокси-сервер для соединения с Сервером администрирования** и введите адрес и номер порта для соединения с прокси-сервером. Допускается использование только десятичной формы записи (например, **Адрес прокси-сервера:** proxy.test.ru, **Порт:** 8080).
 - Если для доступа к прокси-серверу используется пароль, заполните поля **Имя пользователя** и **Пароль**.

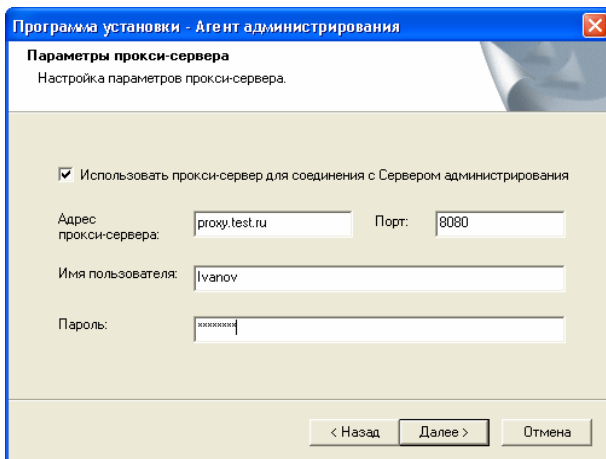
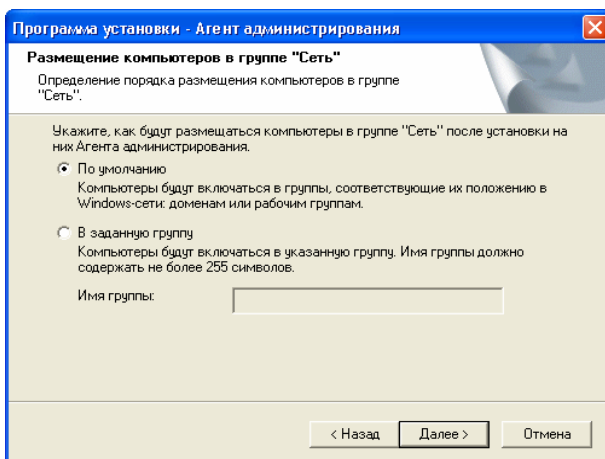


Рисунок 52. Настройка параметров подключения через прокси-сервер

Если прокси-сервер не используется, пропустите данный шаг, нажав на кнопку **Далее**.

6. После этого определите, в какую папку группы **Сеть** должен быть добавлен компьютер при его обнаружении Сервером администрирования в ходе опроса Windows-сети. Выберите один из следующих вариантов (см. рис. 53):
 - **По умолчанию** – компьютер будет включен в папку, соответствующую его положению в Windows-сети: домену или рабочей группе (данный вариант выбран по умолчанию);
 - **В заданную группу** – компьютер будет включен в состав папки, заданной в поле **Имя группы**. В случае выбора дан-

ного варианта введите имя папки. Если в группе **Сеть** такой папки нет, она будет создана (вы также можете указать имя любой из существующих в группе **Сеть** папок).



Рисунк 53. Определение группы размещения компьютеров в папке **Сеть**

7. На следующем этапе (см. рис. 54) укажите способ получения сертификата Сервера администрирования, к которому будет подключаться Агент. Выберите один из вариантов:

- **Получить с Сервера администрирования** – сертификат Сервера администрирования будет получен при первом подключении к нему Агента администрирования (данный вариант выбран по умолчанию).
- **Использовать существующий** – аутентификация Сервера администрирования будет осуществляться на основании сертификата, заданного администратором. В случае выбора данного варианта, укажите необходимый файл сертификата Сервера администрирования.

Файл сертификата имеет расширение **.cer** и размещается на Сервере администрирования в каталоге **Cert** каталога установки **Kaspersky Administration Kit**.

Вы можете скопировать файл сертификата в папку общего доступа или на дискету и использовать для установки Агента администрирования копию файла.

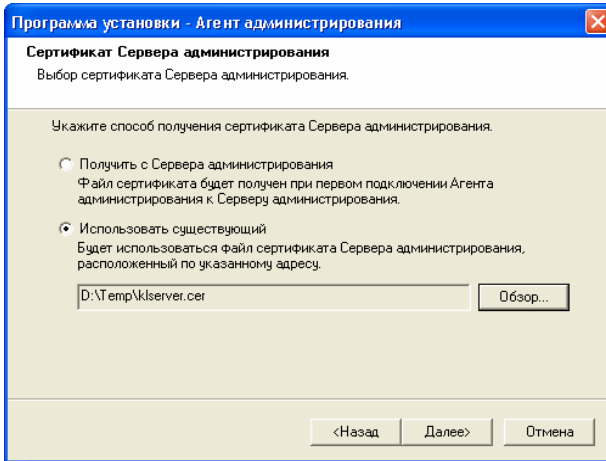


Рисунок 54. Выбор способа получения сертификата Сервера администрирования

- В заключительном окне мастера (см. рис. 55) вам будет предложено запустить Агент администрирования сразу же по окончании работы мастера. Если вы хотите, чтобы запуск состоялся позже, снимите установленный по умолчанию флажок **Запустить Агент администрирования**.

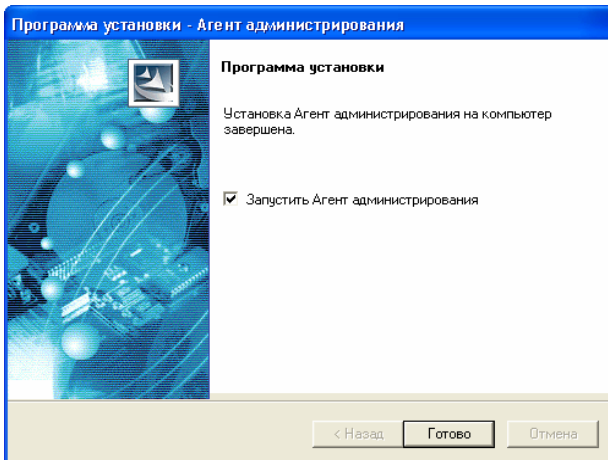


Рисунок 55. Настройка запуска Агента администрирования

По окончании работы мастера Агент администрирования будет установлен на вашем компьютере.

Вы можете просматривать свойства службы **Kaspersky Network Agent**, запускать, останавливать и следить за работой при помощи стандартных средств администрирования Windows – **Управление компьютером / Службы**.

Совместно с Агентом администрирования на компьютер всегда устанавливается плагин для работы с Cisco Network Admission Control (NAC). Этот плагин работает в том случае, когда на компьютере установлено приложение Cisco Trust Agent.

4.3.2. Локальная установка плагина управления приложением

Для того чтобы установить плагин управления приложением,

на компьютере, где установлена Консоль администрирования, запустите исполняемый файл **klcfginst.exe**, расположенный на дистрибутивном компакт-диске приложения. Данный файл входит в состав всех приложений, которые могут управляться при помощи Kaspersky Administration Kit. Установка сопровождается мастером и не требует каких-либо настроек.

Файл установки плагина управления для Агента администрирования **klcfginst.exe** расположен в каталоге **NetAgent** дистрибутивного пакета Kaspersky Administration Kit.

4.3.3. Установка приложений в неинтерактивном режиме

Для того чтобы провести установку приложения в неинтерактивном режиме:

1. Сформируйте необходимый инсталляционный пакет (см. п. 4.1.1 на стр. 40), если для приложения, установку которого вы хотите провести, инсталляционный пакет еще не создавался.

Инсталляционный пакет будет сохранен на Сервере администрирования в определенной на этапе установки Сервера администрирования папке общего доступа в служебном каталоге **Packages**. При этом каждому инсталляционному пакету соответствует своя вложенная папка.

2. При необходимости настройте параметры инсталляционного пакета (см. п. 4.1.2 на стр. 43).
3. Скопируйте всю папку, соответствующую нужному инсталляционному пакету, с Сервера администрирования на клиентский компьютер. Затем на клиентском компьютере откройте скопированную папку.

или

С клиентского компьютера откройте на Сервере администрирования папку общего доступа, соответствующую нужному инсталляционному пакету.

Если папка общего доступа расположена на компьютере с установленной операционной системой Microsoft Windows Vista, необходимо установить значение **Отключен** для параметра **Управление учетными записями пользователей: все администраторы работают в режиме одобрения администратором** (Пуск > Панель управления > Администрирование > Локальная политика безопасности > Параметры безопасности).

4. Затем сделайте следующее:
 - для Антивируса Касперского 6.0 для Windows Workstations, Антивирус Касперского 6.0 для Windows Servers и Kaspersky Administration Kit перейдите во вложенный каталог **exec** и запустите исполняемый файл (файл с расширением **.exe**) с ключом /s.
 - для остальных приложений «Лаборатории Касперского» запустите из открытой папки исполняемый файл (файл с расширением **.exe**) с ключом /s.

При установке приложения Kaspersky Administration Kit в неинтерактивном режиме можно использовать файл ответов. Этот файл содержит все параметры установки приложения и позволяет выполнять многократную установку приложения с одинаковыми параметрами.

Для того чтобы сформировать файл ответов для Kaspersky Administration Kit:

1. В командной строке перейдите в каталог, в котором расположен дистрибутив приложения Kaspersky Administration Kit, и запустите исполняемый файл с ключами /r и /f1"<путь к файлу>\setup.iss"³ (например, **setup.exe /r /f1"C:\setup.iss"**).
В результате на компьютере запустится мастер установки приложения.
2. Настройте параметры установки приложения, следуя указаниям мастера. Например, можно выбрать установку Сервера администрирования или только Консоли (см. п. 3.2 на стр. 19).

После окончания установки на компьютере будет установлена выбранная версия приложения Kaspersky Administration Kit, и в указанном каталоге будет сформирован файл ответов. Созданный файл ответов нужно скопировать в папку дистрибутива Kaspersky Administration Kit. Затем из этой папки следует создать инсталляционный пакет (см. п. 4.1.1 на стр. 40). После этого при установке Kaspersky Administration Kit в неинтерактивном режиме указанным выше способом автоматически будет использоваться конфигурация, заданная в файле ответов.

С помощью файла ответа можно обновлять версии приложения Kaspersky Administration Kit в неинтерактивном режиме. При этом он может использоваться только для обновления той же версии приложения, на которой он был создан.

³ Должен быть указан полный путь к файлу ответов.

ПРИЛОЖЕНИЕ А. ГЛОССАРИЙ

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

А

Агент администрирования – компонент приложения Kaspersky Administration Kit, осуществляющий взаимодействие между Сервером администрирования и приложениями «Лаборатории Касперского», установленными на конкретном сетевом узле (рабочей станции или сервере). Данный компонент является единым для всех Windows-приложений из состава продуктов компании Антивирус Касперского Business Optimal и Kaspersky Corporate Suite. Для Novell- и Unix-приложений «Лаборатории Касперского» существуют отдельные версии Агента администрирования.

Агенты обновления – компьютеры, представляющие собой промежуточные центры распространения обновлений и инсталляционных пакетов в пределах группы администрирования.

Администратор логической сети – пользователь, осуществляющий установку, настройку и обслуживание приложения Kaspersky Administration Kit, а также удаленное управление приложениями «Лаборатории Касперского» на компьютерах логической сети.

Антивирусные базы – базы данных, формируемые специалистами «Лаборатории Касперского» и содержащие подробное описание всех существующих на текущий момент вирусов, способов их обнаружения и лечения. На основании записей антивирусных баз осуществляется поиск вирусов и лечение зараженных объектов. Антивирусные базы размещаются на сайтах «Лаборатории Касперского» и регулярно обновляются по мере появления новых вирусов. Доступ к обновлениям предоставляется зарегистрированным пользователям «Лаборатории Касперского». Для повышения качества обнаружения вирусов мы рекомендуем регулярно копировать обновления антивирусных баз.

В

Восстановление – восстановление данных Сервера администрирования при помощи утилиты резервного копирования на основании информации, сохраненной в резервном хранилище. Утилита позволяет восстанавливать:

- информационную базу Сервера администрирования (политики, задачи, настройки приложения, сохраненные на Сервере администрирования события);
- конфигурационную информацию о структуре логической сети и клиентских компьютерах;
- хранилище дистрибутивов программ для удаленной установки (содержимое папок Packages, Uninstall, Updates);
- сертификат Сервера администрирования.

Г

Группа администрирования – набор компьютеров, объединенных в соответствии с выполняемыми функциями и устанавливаемым на них набором приложений «Лаборатории Касперского». Группировка осуществляется для удобства управления всеми компьютерами как единым целым. Группа может включать в состав другие группы. В группе могут быть созданы групповые политики для каждого из установленных в группе приложений и сформированы групповые задачи.

Глобальная задача – задача, определенная для набора клиентских компьютеров из произвольных групп администрирования логической сети и выполняемая на них.

Групповая задача – задача, определенная для группы и выполняемая на всех клиентских компьютерах данной группы администрирования.

Групповая политика – набор параметров работы приложения в группе администрирования при управлении через Kaspersky Administration Kit. Для разных групп параметры работы приложения могут быть различны. Для каждого приложения определяется своя собственная политика. Политика включает в себя параметры полной настройки всей функциональности приложения.

Д

Доступные обновления – Service Packs, которые содержат набор срочных обновлений, собранных за некоторый временной промежуток, а также изменения в архитектуре приложения.

З

Задача – именованное действие, выполняемое приложением «Лаборатории Касперского».

И

Инсталляционный пакет – набор файлов, формируемый для осуществления удаленной установки приложений «Лаборатории Касперского» на клиентские компьютеры логической сети. Инсталляционный пакет создается на основании специального файла с расширением **.kpd**, входящего в состав дистрибутива приложения, и содержит минимальный набор параметров, необходимых для обеспечения работоспособности приложения сразу после установки. Значение параметров соответствуют настройкам приложения по умолчанию.

К

Клиент Сервера администрирования (или клиентский компьютер) – компьютер, сервер или рабочая станция, на котором установлен Агент администрирования и управляемые приложения «Лаборатории Касперского».

Консоль администрирования – компонент приложения Kaspersky Administration Kit, предоставляющий пользовательский интерфейс к административным сервисам Сервера администрирования и Агента администрирования.

Л

Лицензионный ключ – файл с расширением ***.key**, который является вашим личным «ключом», необходимым для работы с приложениями «Лаборатории Касперского». Лицензионный ключ включен в поставку продукта, если вы приобрели его у дистрибьюторов «Лаборатории Касперского», или присылается вам по почте, если продукт был приобретен в интернет-магазине.

Локальная задача – задача определенная и выполняющаяся на отдельном клиентском компьютере.

Н

Настройки задачи – параметры работы приложения, специфичные для каждого типа задач.

Настройки приложения – набор параметров работы приложения, общий для всех типов его задач.

Непосредственное управление приложением – управление приложением через локальный интерфейс.

О

Обновление – процедура замены/ добавления новых файлов (антивирусных баз или программных модулей приложения), получаемых с серверов обновлений «Лаборатории Касперского».

Оператор логической сети – пользователь, который осуществляет наблюдение за состоянием и работой системы антивирусной защиты, управляемой при помощи Kaspersky Administration Kit.

П

Плагин управления приложением – специализированный компонент, предоставляющий интерфейс для удаленного управления работой приложения через Консоль администрирования. Плагин управления для каждого приложения свой и входит в состав всех приложений «Лаборатории Касперского», управление которыми может осуществляться при помощи Kaspersky Administration Kit.

Политика – см. **Групповая политика**.

Порог вирусной активности – число обнаруженных вирусов в течение ограниченного временного интервала, превышение которого будет считаться повышением вирусной активности и возникновением события **Вирусная атака**. Данная характеристика имеет большое значение в периоды вирусных эпидемий и позволяет администратору своевременно реагировать на возникающие угрозы вирусных атак.

Р

Резервный лицензионный ключ – лицензионный ключ, установленный для работы приложения «Лаборатории Касперского», но не активизированный. В зависимости от настроек активизация ключа может проходить автоматически после истечения срока действия текущего ключа или вручную.

Резервное копирование – копирование данных Сервера администрирования для резервного хранения и последующего восстановления, осуществляемое при помощи утилиты резервного копирования. Утилита позволяет сохранять:

- информационную базу Сервера администрирования (политики, задачи, настройки приложения, сохраненные на Сервере администрирования события);
- конфигурационную информацию о структуре логической сети и клиентских компьютерах;
- хранилище дистрибутивов программ для удаленной установки (содержимое папок Packages, Uninstall, Updates);
- сертификат Сервера администрирования.

Рабочее место администратора – компьютер, на котором установлен компонент Kaspersky Administration Kit Консоль администрирования. С него осуществляется построение и управление системой централизованной антивирусной защитой сети предприятия, сформированной на базе приложений «Лаборатории Касперского».

С

Статус антивирусной защиты – текущее состояние антивирусной защиты, характеризующее степень защищенности компьютера.

Сервер администрирования – компонент приложения Kaspersky Administration Kit, осуществляющий функции централизованного хранения информации об установленных в сети предприятия приложениях «Лаборатории Касперского» и управления ими.

Сертификат Сервера администрирования – сертификат на основании которого осуществляется аутентификация Сервера администрирования при подключении к нему Консоли администрирования и обмене информацией с клиентскими компьютерами. Сертификат Сервера администрирования создается при установке Сервера администрирования и хранится в каталоге установки программы в папке **Cert**.

Срок действия лицензии – период времени, в течение которого вам предоставляется возможность использовать полную функциональность Антивируса Касперского. Срок действия лицензии определяется лицензионным ключом, и, как правило, составляет календарный год со дня установки ключа. После окончания действия лицензии функциональность продукта сокращается.

Сервера обновлений «Лаборатории Касперского» – список http- и ftp-серверов «Лаборатории Касперского», откуда Антивирус Касперского копирует антивирусные базы на ваш компьютер.

Стороннее приложение – антивирусное приложение стороннего производителя или приложение «Лаборатории Касперского», не поддерживающее управление через Kaspersky Administration Kit.

Т

Текущий лицензионный ключ – лицензионный ключ, установленный и использующийся в данный временной период для работы приложения «Лаборатории Касперского». Он определяет срок действия лицензии и лицензионную политику в отношении продукта.

У

Удаленная установка – установка приложений «Лаборатории Касперского» при помощи сервисов, предоставляемых приложением Kaspersky Administration Kit.

Уровень важности события – характеристика события, зафиксированного в работе приложения «Лаборатории Касперского». Существуют четыре уровня важности:

- **Критическое событие.**
- **Отказ функционирования.**
- **Предупреждение.**
- **Информационное сообщение.**

События одного и того же типа могут иметь различные уровни важности, в зависимости от ситуации, при которой событие произошло.

Установка с помощью сценария запуска – метод удаленной установки приложений «Лаборатории Касперского», который позволяет закрепить запуск задачи удаленной установки за конкретной учетной записью пользователя (нескольких пользователей). При регистрации пользователя в домене предпринимается попытка провести установку приложения на клиентском компьютере, с которого пользователь зарегистрировался. Данный метод рекомендуется для установки приложений компании на компьютеры, работающие под управлением операционных систем Microsoft Windows 98/Me.

Ф

Форсированная установка – метод удаленной установки приложений «Лаборатории Касперского», который позволяет провести удаленную установку программного обеспечения на конкретные клиентские компьютеры логической сети. Для успешного выполнения задачи методом форсированной установки учетная запись для запуска задачи должна обладать правами на удаленный запуск приложений на клиентских компьютерах логической сети. Данный метод рекомендуется для установки приложений на компьютеры, работающие под управлением операционных систем Microsoft Windows NT/2000/2003/XP, в которых поддерживается такая возможность, либо на компьютеры под управлением Microsoft Windows 98/Me, на которых установлен Агент администрирования.

Х

Хранилище резервных копий – специальный каталог для сохранения копий данных Сервера администрирования, создаваемых при помощи утилиты резервного копирования.

Ц

Централизованное управление приложением – управление приложением при помощи сервисов администрирования, предоставляемых Kaspersky Administration Kit.

К

Kaspersky Administration Kit – приложение, входящее в состав продуктов Антивирус Касперского Business Optimal и Kaspersky Corporate Suite и предназначенное для централизованного решения основных административных задач по управлению системой антивирусной безопасности компьютерной сети предприятия, построенной на основе приложений «Лаборатории Касперского».

ПРИЛОЖЕНИЕ В. ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

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

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

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

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

Годы упорной работы позволили компании стать лидером в разработке технологий защиты от вирусов. «Лаборатория Касперского» первой разработала многие современные стандарты антивирусных программ. Основной продукт компании, Антивирус Касперского®, обеспечивает надежную защиту всех объектов вирусных атак: рабочих станций, файловых серверов, почтовых систем, сетевых экранов и интернет-шлюзов, карманных компьютеров. Удобные средства управления дают пользователям возможность максимально автоматизировать антивирусную защиту компьютеров и корпоративных сетей. Многие западные разработчики используют в своих продуктах программное ядро Антивируса Касперского®, например, такие как: Nokia ICG (США), 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.

В.1. 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 системной панели 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 непосредственно 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 непосредственно 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® 7.0

Антивирус Касперского 7.0 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 запустить 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 7.0 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.
- *Контроль скрытых процессов* позволяет бороться с сокрытием вредоносного кода в операционной системе с использованием технологий rootkit.
- *Эвристический анализатор.* При проверке какой-либо программы анализатор эмулирует ее исполнение и протоколирует все ее подозрительные действия, например, открытие или запись в файл, перехват векторов прерываний и т.д. На основе этого протокола принимается решение о возможном заражении программы вирусом. Эмуляция происходит в искусственной изолированной среде, что исключает возможность заражения компьютера.
- *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 7.0

Kaspersky Internet Security 7.0 – 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 дозвола на платные ресурсы интернета* помогает идентифицировать программы, которые пытаются использовать ваш модем для скрытого соединения с платными телефонными сервисами, и блокировать их работу. Модуль *Защита конфиденциальных данных* обеспечивает защиту от несанкционированного доступа и передачи информации личного характера. Компонент *Родительский контроль* обеспечивает контроль доступа пользователей компьютера к интернет-ресурсам.

Kaspersky Internet Security 7.0 *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 потребуются 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 продукт 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

Программный продукт 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

Решение 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.

В.2. Наши координаты

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

| | |
|--|--|
| Адрес: | Россия, 123060, Москва, 1-й Волоколамский проезд, д.10, стр.1 |
| Факс: | +7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00 |
| Экстренная круглосуточная помощь: | +7 (495) 797-87-07, +7 (495) 645-79-29, +7 (495) 956-87-08 |
| Поддержка пользователей персональных и бизнес-продуктов: | +7 (495) 797-87-07, +7 (495) 645-79-29, +7 (495) 956-87-08 (с 10 до 19 часов) http://support.kaspersky.ru/helpdesk.html |
| Поддержка корпоративных пользователей: | контактная информация предоставляется при покупке корпоративных продуктов в зависимости от пакета технической поддержки. |
| Веб-форум «Лаборатории Касперского»: | http://forum.kaspersky.com |
| Антивирусная лаборатория: | newvirus@kaspersky.com (только для отправки новых вирусов в архивированном виде) |
| Группа подготовки пользовательской документации: | docfeedback@kaspersky.com (только для отправки отзывов о документации и электронной справочной системе) |
| Департамент продаж: | +7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00 sales@kaspersky.com |

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