ЛАБОРАТОРИЯ КАСПЕРСКОГО

Kaspersky® Administration Kit 6.0

СПРАВОЧНОЕ РУКОВОДСТВО

KASPERSKY® ADMINISTRATION KIT 6.0

Справочное руководство

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 8
1.1. Назначение документа 10
1.2. Принятые обозначения 10

ГЛАВА 2. УПРАВЛЕНИЕ ЛОГИЧЕСКОЙ СЕТЬЮ 12
2.1. Запуск программы. Подключение к Серверу администрирования 12
2.1.1. Запуск программы 12
2.1.2. Подключение к Серверу администрирования 12
2.1.3. Отключение от Сервера администрирования 15
2.1.4. Переключение между Серверами 15
2.1.5. Добавление Сервера в дерево консоли 16
2.1.6. Удаление Сервера из дерева консоли 16
2.2. Предоставление прав 17
2.2.1. Предоставление прав на работу с Сервером администрирования 17
2.2.2. Предоставление прав для группы 19
2.3. Просмотр информации о компьютерной сети. IP-подсети 20
2.3.1. Просмотр информации о компьютерной сети 20
2.3.2. Выбор способа отображения компьютерной сети 21
2.3.3. Создание IP-подсети 21
2.3.4. Просмотр и изменение параметров IP-подсети 22
2.3.5. Просмотр и изменение параметров группы Active Directory 25
2.4. Мастер первоначальной настройки 26
2.4.1. Работа с мастером первоначальной настройки 26
2.5. Создание, просмотр и изменение структуры логической сети 31
2.5.1. Просмотр информации о группах 31
2.5.2. Просмотр параметров группы и параметров взаимодействия клиентских компьютеров и Сервера администрирования 32
2.5.3. Просмотр информации о клиентском компьютере 36
2.5.4. Просмотр логической сети подчиненного Сервера 40
2.6. Группы 42
2.6.1. Добавление группы 42
2.6.2. Настройка параметров группы 42

2.6.3. Настройка автоматической установки программного обеспечения на новые компьютеры в группе ... 49
2.6.4. Перемещение группы ... 49
2.6.5. Изменение названия группы ... 50
2.6.6. Удаление группы ... 50
2.7. Клиентские компьютеры ... 50
2.7.1. Добавление компьютеров в логическую сеть ... 50
2.7.2. Автоматическое добавление новых компьютеров в группу ... 52
2.7.3. Перемещение клиентского компьютера в другую логическую сеть. Задача смены Сервера администрирования ... 53
2.7.4. Подключения клиентского компьютера к Серверу администрирования вручную. Утилита *klmover.exe* ... 56
2.7.5. Проверка соединения клиентского компьютера и Сервера администрирования вручную. Утилита *klnagchk.exe* ... 57
2.8. Подчиненные Серверы администрирования ... 59
2.8.1. Добавление подчиненного Сервера ... 59
2.8.2. Настройка параметров подключения подчиненного Сервера к главному ... 61

ГЛАВА 3. УДАЛЕННОЕ УПРАВЛЕНИЕ ПРИЛОЖЕНИЯМИ ... 63
3.1. Настройка параметров приложения ... 63
3.1.1. Управление политиками ... 63
3.1.1.1. Создание политики ... 63
3.1.1.2. Просмотр и настройка параметров политики ... 66
3.1.1.3. Отображение унаследованной политики в панели результатов вложенной группы ... 78
3.1.1.4. Активация политики ... 78
3.1.1.5. Активация политики по событию ... 79
3.1.1.6. Политика для мобильного пользователя ... 79
3.1.1.7. Удаление политики ... 80
3.1.1.8. Копирование политики ... 80
3.1.1.9. Настройка параметров политики Агента администрирования ... 81
3.1.1.10. Настройка параметров политики Сервера администрирования ... 85
3.1.1.11. Экспорт политики ... 89
3.1.1.12. Импорт политики ... 90
3.1.2. Локальные настройки приложения ... 90
3.1.2.1. Просмотр настроек приложения ... 90

3.1.2.2. Настройка параметров Сервера администрирования 94
3.1.2.3. Настройка параметров Агента администрирования..... 110
3.2. Управление работой приложений..... 111
3.2.1. Создание групповой задачи..... 111
3.2.2. Создание глобальной задачи 121
3.2.3. Создание локальной задачи 122
3.2.4. Просмотр и изменение настроек задачи..... 124
3.2.5. Отображение унаследованной групповой задачи в панели результатов вложенной группы 131
3.2.6. Автоматическая загрузка ОС клиентских компьютеров перед запуском задачи 131
3.2.7. Выключение компьютера после выполнения задачи..... 132
3.2.8. Ограничение времени выполнения задачи 132
3.2.9. Отключение запуска задачи по расписанию..... 132
3.2.10. Создание задачи запуска / остановки приложения 133
3.2.11. Экспорт задачи 134
3.2.12. Импорт задачи 135
3.2.13. Запуск / остановка задачи вручную..... 135
3.2.14. Приостановка / возобновление задачи вручную..... 135
3.2.15. Наблюдение за ходом выполнения задачи 136
3.2.16. Просмотр результатов выполнения задачи, хранящихся на Сервере администрирования 136
3.2.17. Настройка фильтра событий для групповой задачи 138
3.2.18. Настройка фильтра событий для выбранного компьютера 142
3.2.19. Отмена действия фильтра..... 143

ГЛАВА 4. ОБНОВЛЕНИЕ АНТИВИРУСНЫХ БАЗ И ПРОГРАММНЫХ МОДУЛЕЙ..... 144
4.1. Получение обновлений Сервером администрирования 144
4.1.1. Создание задачи получения обновлений Сервером администрирования..... 144
4.1.2. Настройка задачи получения обновлений Сервером администрирования..... 147
4.1.3. Просмотр списка обновлений..... 149
4.1.4. Просмотр свойств полученных обновлений..... 149
4.2. Автоматическое распространение обновлений..... 151
4.2.1. Автоматическое распространение обновлений на клиентские компьютеры 151

4.2.2. Автоматическое распространение обновлений на подчиненные Серверы ... 151
4.2.3. Формирование списка агентов обновления и их настройка ... 152

ГЛАВА 5. ОБСЛУЖИВАНИЕ ... 155
5.1. Продление лицензии ... 155
5.1.1. Просмотр информации об установленных лицензионных ключах ... 155
5.1.2. Просмотр информации о лицензионном ключе ... 155
5.1.3. Установка лицензионного ключа ... 157
5.1.4. Запуск мастера создания задачи установки лицензионного ключа ... 158
5.1.5. Создание и просмотр отчета о лицензионных ключах ... 159
5.2. Карантин и резервное хранилище ... 160
5.2.1. Просмотр свойств объекта, помещенного на карантин или в резервное хранилище ... 160
5.2.2. Удаление объекта из карантина или резервного хранилища ... 161
5.2.3. Восстановление объекта из карантина или резервного хранилища ... 162
5.2.4. Проверка карантинного каталога на клиентском компьютере ... 162
5.3. Журналы событий. Выборки событий ... 163
5.3.1. Просмотр журнала событий Kaspersky Administration Kit, хранящегося на Сервере администрирования ... 163
5.3.2. Создание выборки событий ... 164
5.3.3. Настройка выборки событий ... 165
5.3.4. Сохранение информации о событиях в файле ... 168
5.3.5. Удаление событий ... 169
5.4. Отчеты ... 169
5.4.1. Создание шаблона отчета ... 169
5.4.2. Просмотр и редактирование параметров шаблона отчета ... 172
5.4.3. Создание и просмотр отчета ... 176
5.4.4. Создание общих отчетов для подчиненных Серверов администрирования ... 178
5.4.5. Ограничение количества отображаемых в отчете записей ... 179
5.5. Отслеживание состояния антивирусной защиты с помощью информации в системном реестре ... 179
5.6. Поиск компьютеров ... 181
5.6.1. Поиск компьютеров ... 181
5.6.2. Сохранение результатов поиска компьютеров в текстовом файле ... 186
5.7. Выборки компьютеров ... 187
5.7.1. Создание выборки компьютеров ... 187

5.7.2. Настройка выборки компьютеров ... 187
5.8. Отслеживание вирусных эпидемий ... 193
5.8.1. Включение механизма распознавания вирусной атаки ... 193
5.8.2. Смена политики для приложения при регистрации события Вирусная атака ... 194
5.9. Резервное копирование и восстановление данных Сервера администрирования ... 195
5.9.1. Создание резервной копии данных Сервера администрирования ... 195
5.9.2. Восстановление данных Сервера администрирования из резервной копии ... 195
5.9.3. Задача резервного копирования данных ... 196
5.9.3.1. Создание задачи резервного копирования данных Сервера администрирования ... 196
5.9.3.2. Настройка задачи резервного копирования данных Сервера администрирования ... 198
5.9.4. Утилита резервного копирования данных ... 199
5.9.4.1. Создание резервной копии данных Сервера администрирования вручную. Утилита *klbackup* ... 199
5.9.4.2. Перенос Сервера администрирования на другой компьютер ... 201
5.9.4.3. Перенос базы Сервера администрирования на другой компьютер ... 202
5.10. Настройка совместной работы с Cisco Network Admission Control (NAC) ... 203

ПРИЛОЖЕНИЕ А. КАК ОБРАТИТЬСЯ В СЛУЖБУ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ ... 204

ПРИЛОЖЕНИЕ В. ГЛОССАРИЙ ... 206

ПРИЛОЖЕНИЕ С. ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО» ... 212
С.1. Другие разработки «Лаборатории Касперского» ... 213
С.2. Наши координаты ... 225

ГЛАВА 1. KASPERSKY® ADMINISTRATION KIT

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 приложений, входящих в состав продуктов «Лаборатории Касперского», на компьютеры, работающие под управлением операционных систем семейства Windows. Эта возможность позволяет администратору один раз скопировать на выделенный компьютер необходимый набор приложений «Лаборатории Касперского», и после этого проводить удаленную установку на компьютеры 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.
- Удаленное централизованное управление всеми приложениями, входящими в состав продуктов «Лаборатории Касперского», работающими на компьютерах под управлением операционной системы Windows. 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 почтовых 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.
- 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 предприятия 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).

1.1. Назначение документа

Данное руководство содержит назначение приложения Kaspersky Administration Kit и пошаговое описание предоставляемых им функций. Основные понятия и общая схема работы с приложением приводятся в Руководстве администратора 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.

1.2. Принятые обозначения

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

Оформление	Смысловое назначение
Жирный шрифт	Названия меню, пунктов меню, окон, элементов диалоговых окон и т. п.
Примечание.	Дополнительная информация, примечания.
Внимание!	Информация, на которую следует обратить особое внимание.

Оформление	Смысловое назначение
Чтобы выполнить действие, 1. Шаг 1. 2. …	Описание последовательности выполняемых пользователем шагов и возможных действий.
Вопрос:	Постановка задачи, примера для реализации возможностей программного продукта
[ключ] – назначение ключа.	Ключи командной строки.
`Текст информационных сообщений и командной строки`	Текст конфигурационных файлов, информационных сообщений программы и командной строки.

ГЛАВА 2. УПРАВЛЕНИЕ ЛОГИЧЕСКОЙ СЕТЬЮ

2.1. Запуск программы. Подключение к Серверу администрирования

2.1.1. Запуск программы

Для запуска программы:

выберите пункт **Kaspersky Administration Kit** в программной группе **Kaspersky Administration Kit** стандартного меню **Пуск / Программы**. Данная программная группа создается только на рабочих местах администраторов при установке компонента Консоль администрирования.

2.1.2. Подключение к Серверу администрирования

Для подключения к Серверу администрирования:

выберите в дереве консоли узел, соответствующий нужному Серверу.

В результате предпринимается попытка соединения с Сервером администрирования. Если в сети предприятия существует несколько Серверов администрирования, запрашивается последний из Серверов, с которым устанавливалось соединение во время предыдущего сеанса работы программы Kaspersky Administration Kit. Если программа запускается первый раз после установки, предполагается, что Сервер администрирования размещен на том же компьютере, что и Консоль администрирования, и производится попытка установить соединение с ним.

Если Сервер не обнаружен, вам будет предложено указать адрес Сервера вручную в диалоговом окне **Параметры подключения** (см. рис. 1). Адрес необходимого Сервера вводится в поле **Адрес сервера**. Вы можете указать IP-адрес или имя компьютера в сети Windows.

Для подключения к Серверу администрирования через порт, отличный от установленного по умолчанию, в поле **Адрес сервера** необходимо ввести значение в формате **<Имя сервера>:<Порт>**.

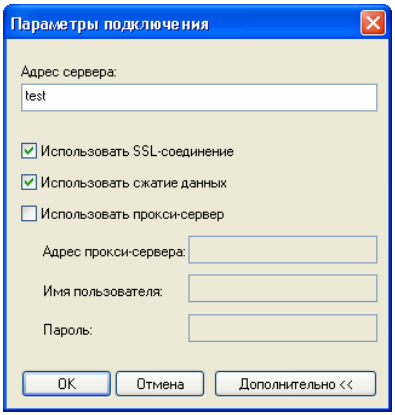

Рисунок 1. Установка соединения с Сервером администрирования

Нажав на кнопку **Дополнительно**, вы можете открыть/скрыть дополнительные параметры подключения:

- **Использовать SSL-соединение**. Установите этот флажок, чтобы включить использование протокола SSL для обмена информацией между Сервером администрирования и Консолью администрирования. Если вы хотите отключить использование протокола SSL, снимите флажок. Однако при этом уровень защищенности информации от изменения и перехвата значительно снижается.

- **Использовать сжатие данных**. Установите этот флажок для увеличения скорости передачи данных между Консолью администрирования и Сервером, сокращения объема передаваемой информации и уменьшения нагрузки на Сервер администрирования.

  При включении данного параметра может возрасти нагрузка на центральный процессор компьютера, на котором установлена Консоль администрирования.

- **Использовать прокси-сервер**. Установите этот флажок, если подключение к Серверу администрирования осуществляется через прокси-сервер. В поле **Адрес прокси-сервера** введите адрес для соединения с прокси-сервером. Заполните поля **Имя пользователя** и **Пароль**, если для доступа к прокси-серверу требуется аутентификация.

Далее производится проверка прав пользователя на подключение к Серверу администрирования, а в случае использования защищенного SSL-подключения сначала аутентификация Сервера администрирования, а после ее успешного завершения, проверка прав пользователя.

При аутентификации Сервера, если сертификат Сервера администрирования не совпадает с копией сертификата, хранящейся на рабочем месте администратора, а также при первом подключении, выводится запрос на подтверждение подключения к Серверу с заданным именем и получение нового сертификата (см. рис 2). Выберите один из вариантов:

- **Подключиться к Серверу администрирования и получить его сертификат** – продолжение подключения к Серверу администрирования и автоматического получения сертификата.
- **Повторить аутентификацию Сервера администрирования, используя сертификат** – определить сертификат Сервера вручную. В этом случае с помощью кнопки **Обзор** выберите файл сертификата. Он имеет расширение .**cer** и размещается на Сервере администрирования в каталоге **Cert** каталога установки Kaspersky Administration Kit. В результате будет проведена повторная аутентификация Сервера администрирования на основании указанного вами сертификата.

Вы можете скопировать файл сертификата в папку общего доступа или на дискету и использовать для настройки параметров доступа к Серверу копию этого файла.

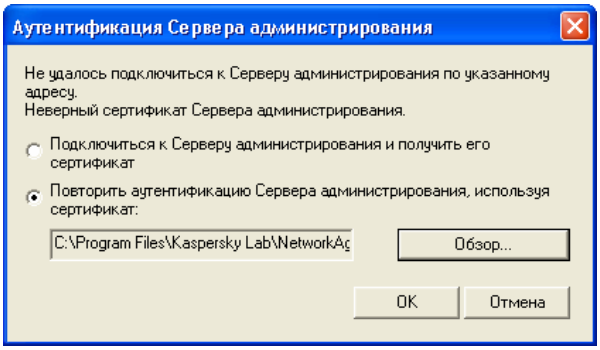

Рисунок 2. Запрос на подтверждение подключения к Серверу администрирования

Проверка прав пользователя осуществляется на основании Windows-аутентификации пользователя в сети. Если пользователь не обладает правами оператора (**KLOperators**) или администратора логической сети (**KLAdmins**) ему будет предложено пройти регистрацию для доступа Серверу администрирования (см. рис. 3). Введите в предложенной форме для регистрации учетную запись и пароль пользователя, обладающего правами оператора или администратора логической сети.

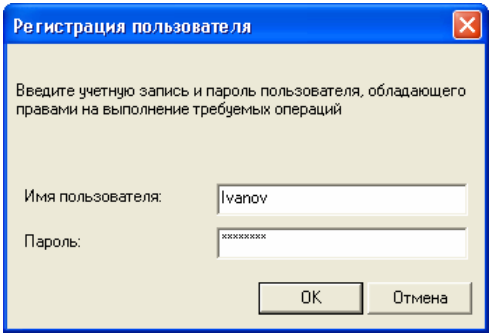

Рисунок 3. Регистрация пользователя для доступа к Серверу администрирования

В случае успешного соединения с Сервером администрирования структура логической сети данного Сервера и ее настройки появляются в дереве консоли.

2.1.3. Отключение от Сервера администрирования

Для того чтобы отключиться от Сервера администрирования:

выберите в дереве консоли узел **Сервер администрирования – <Имя компьютера>**, откройте контекстное меню и выберите команду **Отключиться от Сервера администрирования** или воспользуйтесь аналогичным пунктом в меню **Действие**.

2.1.4. Переключение между Серверами

Для того чтобы подключиться к другому Серверу администрирования,

в главном окне программы Kaspersky Administration Kit выберите в дереве консоли узел с именем нужного Сервера, откройте контекстное меню и выберите команду **Подключиться к Серверу админи-**

стрирования или воспользуйтесь аналогичным пунктом в меню **Действие**. В появившемся диалоговом окне **Параметры подключения** (см. рис. 1) введите имя Сервера, с логической сетью которого вы собираетесь работать (см. выше) и, в случае необходимости, определите, использовать SSL-протокол при связи с Сервером или нет (флажок **Использовать SSL-соединение**).

Пользователям, не обладающим правами администратора или оператора логической сети, будет отказано в доступе к Серверу администрирования.

В случае успешного соединения с Сервером содержание соответствующего узла обновляется.

2.1.5. Добавление Сервера в дерево консоли

Для того чтобы добавить в дерево консоли новый Сервер администрирования,

в главном окне программы Kaspersky Administration Kit выберите в дереве консоли узел **Kaspersky Administration Kit**, откройте контекстное меню и выберите команду **Создать/ Сервер администрирования** или воспользуйтесь аналогичным пунктом в меню **Действие**.

В результате в дереве консоли будет создан новый узел с именем **Сервер администрирования – <имя компьютера> (Не подключен)**, с которого вы можете подключиться к любому из установленных в сети Серверов администрирования.

2.1.6. Удаление Сервера из дерева консоли

Для того чтобы удалить Сервер администрирования из дерева консоли:

выберите в дереве консоли узел, соответствующий удаляемому Серверу администрирования, откройте контекстное меню и выберите команду **Удалить** или воспользуйтесь аналогичным пунктом в меню **Действие**.

2.2. Предоставление прав

2.2.1. Предоставление прав на работу с Сервером администрирования

Для предоставления прав на работу с логической сетью Сервера администрирования:

1. В главном окне программы Kaspersky Administration Kit выберите в дереве консоли узел, соответствующий нужному Серверу администрирования, откройте контекстное меню и выберите команду **Свойства** или воспользуйтесь аналогичным пунктом в меню **Действие**.
2. В открывшемся окне **Свойства: Сервер администрирования – <имя компьютера>** (см. рис. 4) выберите закладку **Безопасность**.

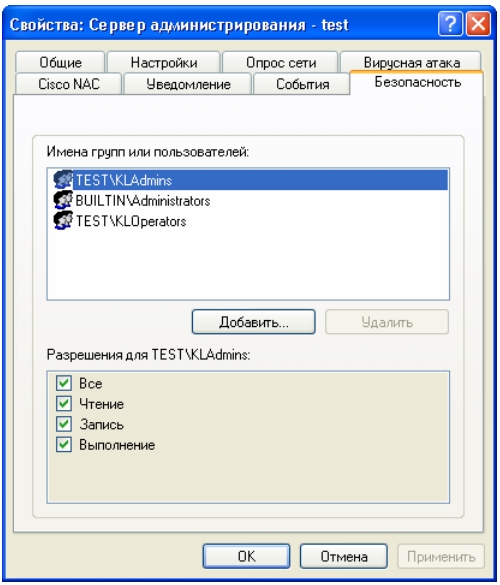

Рисунок 4. Предоставление прав доступа к Серверу администрирования

В верхней части закладки представлен список групп пользователей, зарегистрированных на компьютере, где установлена Консоль администрирования. В нижней части – перечень предусмотренных разрешений:

- **Все**: включает в себя все разрешения – **Чтение**, **Выполнение** и **Запись**.
- **Чтение**:
  - подключение к Серверу администрирования;
  - просмотр структуры логической сети (или группы администрирования);
  - просмотр значения параметров политик, задач и настроек приложения.
- **Выполнение**: запуск и остановка существующих групповых и глобальных задач; формирование отчетов.
- **Запись**:
  - создание логической сети, добавление в нее групп и клиентских компьютеров (или в группу администрирования);
  - установка на клиентские компьютеры компонента Агент администрирования;
  - создание и установка на клиентские компьютеры необходимых инсталляционных пакетов для антивирусных приложений компании, а также лицензионных ключей к ним;
  - обновление версии установленных на клиентских компьютерах приложений;
  - создание политик, задач для групп и отдельных компьютеров, изменение настроек приложения;
  - централизованное управление приложениями, получение отчетов об их работе при помощи сервисов, предоставляемых компонентами Сервер, Агент и Консоль администрирования;
  - предоставление пользователям и группам пользователей прав доступа к функциональности Kaspersky Administration Kit.

Для назначения прав выберите группу пользователей и проставьте флажки рядом с названиями предоставляемых разрешений. При установке флажка **Все** проставляются сразу все флажки.

Добавить новую группу или нового пользователя можно при помощи кнопки **Добавить**. При этом возможно добавление только групп пользователей и пользователей из числа зарегистрированных в домене.

3. После завершения настройки нажмите на кнопку **ОК** или **Применить**.

2.2.2. Предоставление прав для группы

Для предоставления прав на работу с группой администрирования:

1. Выберите в дереве консоли нужную группу администрирования, откройте контекстное меню и выберите команду **Свойства** или воспользуйтесь аналогичным пунктом в меню **Действие**.

2. В открывшемся окне **Свойства: <имя группы>** (см. рис. 5) выберите закладку **Безопасность**. Она аналогична закладке **Безопасность** окна настройки параметров Сервера администрирования.

   Права на работу с логической сетью и всеми входящими в ее состав объектами определяются в параметрах Сервера администрирования.

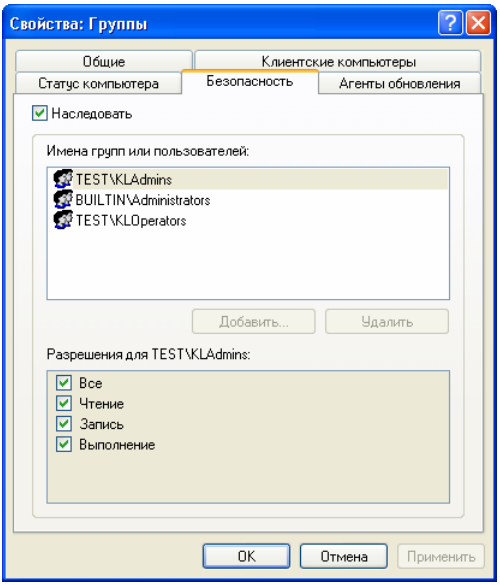

Рисунок 5. Предоставление прав доступа к группе администрирования

Для того чтобы установить для группы администрирования индивидуальные права доступа, отличные от заданных в параметрах Сервера администрирования, снимите флажок **Наследовать**.

3. После этого установите необходимые права доступа для представленных в списке пользователей и групп пользователей. Предоставление прав осуществляется так же, как и для Сервера администрирования.
4. После завершения настройки нажмите на кнопку **ОК** или **Применить**.

2.3. Просмотр информации о компьютерной сети. IP-подсети

2.3.1. Просмотр информации о компьютерной сети

Для просмотра информации о компьютерной сети, получаемой Сервером администрирования при регулярном опросе:

выберите в дереве консоли узел **Сеть**.

Информация о структуре сети и входящих в ее состав компьютерах, получается Сервером администрирования в ходе регулярных опросов Windows-сети и IP-подсетей, сформированных в компьютерной сети предприятия. По результатам этих опросов содержание папки **Сеть** обновляется.

После установки Kaspersky Administration Kit папка **Сеть** содержит иерархию папок, отображающих структуру доменов и рабочих групп Windows-сети предприятия. Каждая из папок на конечном уровне содержит перечень компьютеров соответствующего домена или рабочей группы, не включенных в состав логической сети. Список компьютеров отображается в панели результатов. При включении компьютера в какую-либо группу администрирования, информация о нем сразу же удаляется из папки. При исключении компьютера из состава логической сети, информация о нем вновь появляется в соответствующей папке узла **Сеть**.

Представленная в Консоли администрирования информация обновляется автоматически только для узлов.

Для обновления информации в панели результатов следует пользоваться клавишей **F5** либо командой **Обновить** в меню, контекстном меню или гиперссылкой **Обновить** на панели задач.

2.3.2. Выбор способа отображения компьютерной сети

*Чтобы выбрать способ отображения компьютерной сети при просмотре папки **Сеть**,*

выберите в дереве консоли узел **Сеть**, вызовите контекстное меню и выберите команду из группы **Вид**:

- **Домены** – для представления структуры компьютерной сети в виде иерархии папок, отображающих структуру доменов и рабочих групп Windows-сети предприятия. Каждая из папок на конечном уровне содержит перечень компьютеров соответствующего домена или рабочей группы, не включенных в состав логической сети.
- **Active Directory** – для отображения иерархии сети в соответствии со структурой Active Directory.
- **IP-подсети** – для представления компьютерной сети в виде IP-подсетей.

2.3.3. Создание IP-подсети

Для создания новой IP-подсети:

1. Выберите в дереве консоли узел **Сеть**, вызовите контекстное меню и выберите команду **Создать/IP-подсеть** или воспользуйтесь аналогичным пунктом в меню **Действие**.

   Команда **Создать/ IP-подсеть** доступна только при отображении папки **Сеть** в виде IP-подсетей.

2. В открывшемся окне **Новая IP-подсеть** (см. рис. 6) укажите значения для следующих параметров:
   - имя подсети;
   - способ описания подсети и значения соответствующих выбранному способу параметров.

Выберите один из вариантов:

- **Задать IP-подсеть адресом и маской подсети**; в этом случае в полях ввода укажите **Маску подсети** и **Адрес подсети**.
- **Задать IP-подсеть начальным и конечным IP-адресом**; после этого введите начальный и конечный IP-адреса.

- временной интервал, по истечении которого информация о неактивном компьютере будет удаляться из базы данных Сервера администрирования, в поле **Время действия IP-адреса (часов)**.

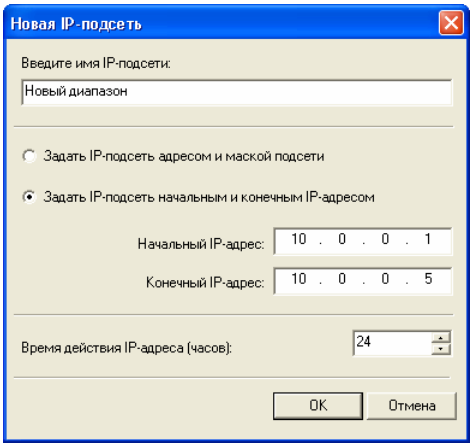

Рисунок 6. Создание новой IP-подсети

3. После окончания настройки параметров нажмите на кнопку **OK**.

2.3.4. Просмотр и изменение параметров IP-подсети

Для изменения параметров IP-подсети:

выберите в папке **Сеть** узел, соответствующий нужной подсети, вызовите контекстное меню и выберите команду **Свойства** или воспользуйтесь аналогичным пунктом в меню **Действие**.

В результате открывается диалоговое окно **Свойства: <Название подсети>**, состоящее из закладок **Общие** и **IP-диапазоны**.

На закладке **Общие** (см. рис. 7) вы можете:

- изменить имя подсети;
- определить будет Сервер администрирования автоматически перемещать новые входящие в данную подсеть компьютеры в состав логической сети. Для этого установите флажок **Добавить компьютер в состав группы** и выберите нужную группу администрирования при помощи кнопки **Выбрать**.
- изменить значение временного интервала, по истечении которого информация о неактивном компьютере будет удаляться из базы данных Сервера администрирования, в поле **Время действия IP-адреса (часов)**.
- разрешить или отменить регулярный опрос Сервером администрирования компьютеров данной подсети. Для того чтобы Сервер администрирования не опрашивал компьютеры при очередном опросе, снимите флажок **Разрешить опрос IP-подсети**.

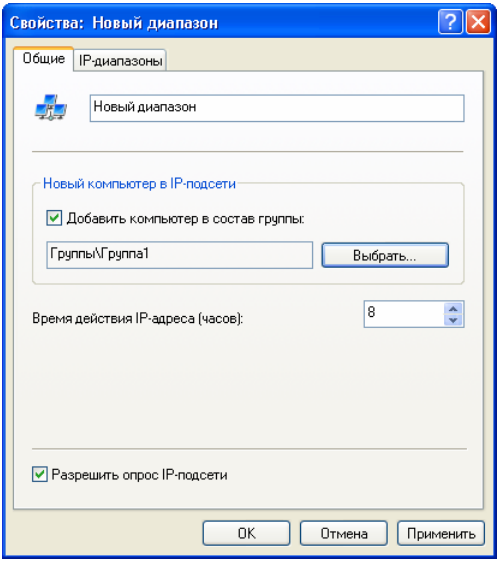

Рисунок 7. Просмотр параметров IP-подсети. Закладка **Общие**

На закладке **IP-диапазоны** (см. рис. 8) вы можете добавлять и удалять IP-диапазоны, определяющие подсеть, а также изменять параметры диапазонов:

- начальный и конечный IP-адреса диапазона;
- маску подсети и адрес подсети.

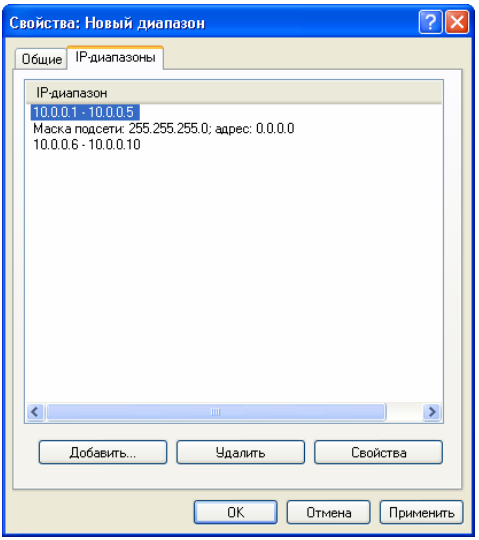

Рисунок 8. Просмотр параметров IP-подсети. Закладка **IP-диапазоны**

Для добавления IP-диапазона, определяющего подсеть, нажмите на кнопку **Добавить**. В открывшемся окне **IP-диапазон** (см. рис. 9) укажите способ описания диапазона и введите значения соответствующих выбранному способу параметров. Выберите один из вариантов:

- **Задать IP-подсеть адресом и маской подсети**, в этом случае в полях ввода укажите маску и адрес подсети.
- **Задать IP-подсеть начальным и конечным IP-адресом**, после этого введите начальный и конечный IP-адреса.

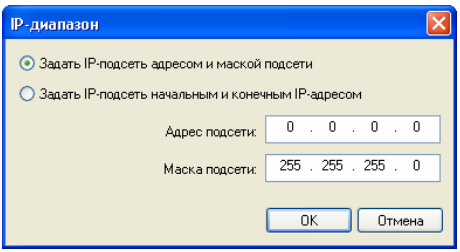

Рисунок 9. Добавление IP-диапазона

2.3.5. Просмотр и изменение параметров группы Active Directory

Для изменения параметров группы Active Directory:

выберите в папке **Сеть** узел, соответствующий нужной группе Active Directory, вызовите контекстное меню и выберите команду **Свойства** или воспользуйтесь аналогичным пунктом в меню **Действие**.

В результате открывается диалоговое окно **Свойства: <Название группы Active Directory>**, содержащее закладку **Общие** (см. рис. 10). На этой закладке вы можете определить, будет ли Сервер администрирования автоматически перемещать новые входящие в эту группу компьютеры в состав логической сети. Для этого установите флажок **Добавить компьютер в состав группы** и выберите нужную группу администрирования с помощью кнопки **Выбрать**.

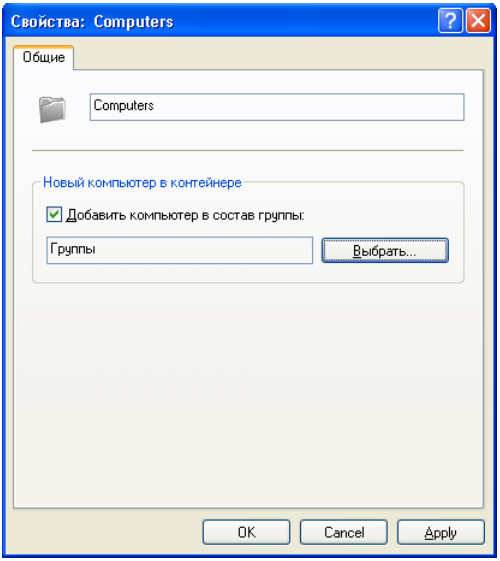

Рисунок 10. Просмотр параметров группы Active Directory. Закладка **Общие**

2.4. Мастер первоначальной настройки

2.4.1. Работа с мастером первоначальной настройки

Для создания системы централизованного управления антивирусной защитой с помощью мастера:

1. В главном окне программы Kaspersky Administration Kit выберите в дереве консоли узел, соответствующий нужному Серверу администрирования, откройте контекстное меню и выберите команду **Мастер первоначальной настройки** или воспользуйтесь аналогичным пунктом в меню **Действие**.
2. На первом этапе проводится опрос компьютерной сети и идентификация компьютеров в ней (см. рис. 11). По его результатам формируется служебная группа **Сеть** и составляется структура папки **Сеть**. Полученная информация будет использоваться при автоматическом создании логической сети. Для просмотра структуры компьютерной сети воспользуйтесь гиперссылкой **Просмотреть результаты опроса сети**. При помощи гиперссылки **Просмотреть введение в приложение** вы можете ознакомиться с описанием основных возможностей Kaspersky Administration Kit, не прерывая работу мастера.

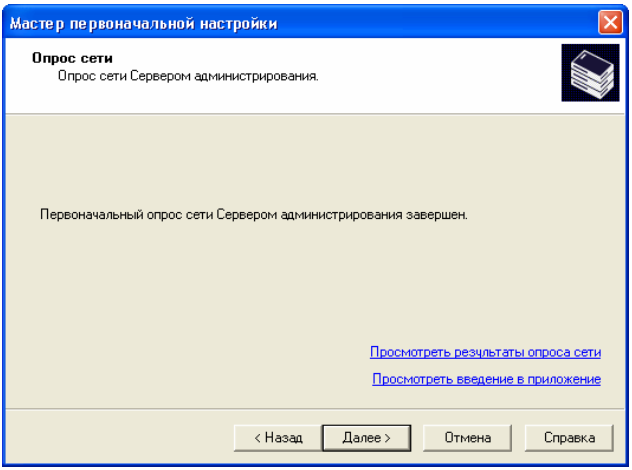

Рисунок 11. Опрос компьютерной сети

3. На данном этапе определите способ создания логической сети (см. рис. 12). Выберите:

   - **Сформировать логическую сеть на основе Windows-сети**, если вы хотите, чтобы логическая сеть была сформирована Сервером администрирования автоматически, на основе данных о структуре доменов и рабочих групп Windows-сети, представленных в группе **Сеть**.

     Если при создании логической сети мастером компьютер по каким-либо причинам не зафиксирован в группе **Сеть** (выключен, отключен от сети), он не будет добавлен в логическую сеть. Вы сможете сделать это позже вручную (см. п. 2.7.1 на стр. 50).

     Создание логической сети с помощью мастера первоначальной настройки не нарушает ее целостности: новые группы добавляются, а не замещают существующие; клиентский компьютер не может быть включен повторно, поскольку в группе **Сеть** содержится информация о компьютерах, не входящих в логическую сеть.

   - **Создать логическую сеть вручную**, если вы хотите создать логическую сеть позже вручную.

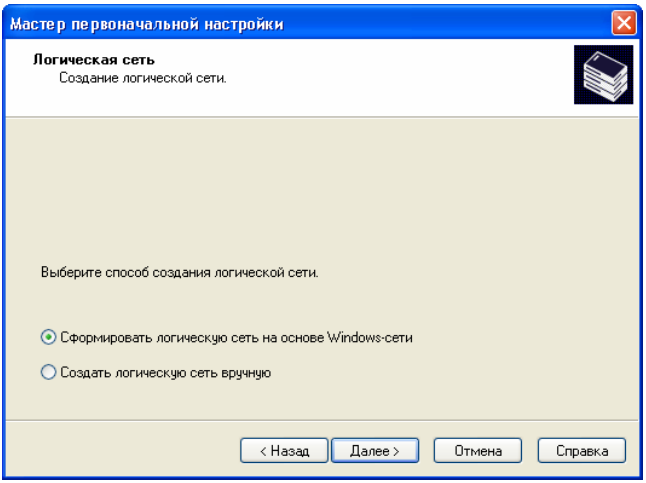

Рисунок 12. Выбор способа создания логической сети

4. В следующем окне мастера (см. рис. 13) установите параметры рассылки оповещений по электронной почте и средствами NET SEND о событиях, регистрируемых в работе приложений компании, и с помощью кнопки **Сообщение** сформируйте

шаблон сообщения (подробнее см. п. 3.1.1.2 на стр. 66). Эти настройки будут использоваться в качестве значений по умолчанию в политиках для приложений.

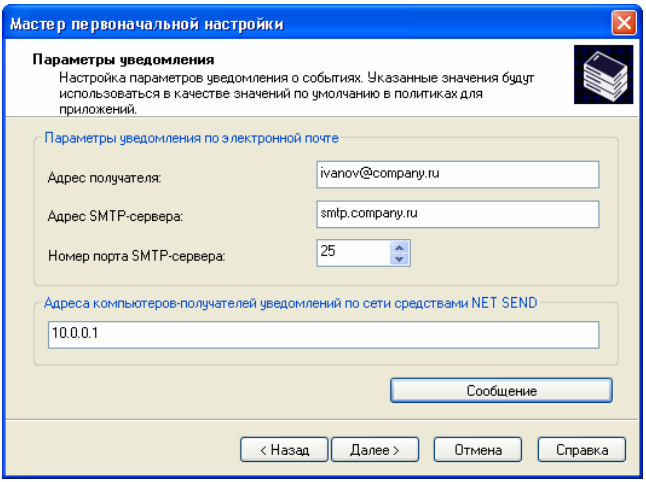

Рисунок 13. Настройка параметров рассылки оповещений

5. На следующем этапе производится настройка системы антивирусной защиты (см. рис. 14).

   Мастер первоначальной настройки формирует систему антивирусной защиты для клиентских компьютеров логической сети с использованием Антивируса Касперского для Windows Workstations версий 5.0 и 6.0. При этом Сервер администрирования создает политику и минимальный набор задач самого верхнего уровня иерархии для Антивируса Касперского для Windows Workstations версий 5.0 и 6.0, а также глобальные задачи получения обновлений Сервером администрирования и резервного копирования данных. Перечисленные объекты отображаются:

   - политики для Антивируса Касперского для Windows Workstations версий 5.0 и 6.0 в папке **Политики** группы **Группы** с именами **Политика Антивируса Касперского 5.0 для Windows Workstations** и **Политика Антивируса Касперского 6.0 для Windows Workstations** и настройками по умолчанию;

   - задача получения обновлений Сервером администрирования в узле **Глобальные задачи** дерева консоли с именем **Задача получения обновлений Сервером администрирования** и настройками по умолчанию;

- задачи обновления антивирусных баз для приложения Антивирус Касперского для Windows Workstations версий 5.0 и 6.0 в папке **Групповые задачи** группы **Группы** с именами **Задача обновления антивирусных баз и модулей приложения** и **Задача обновления (версия 6.0)** и настройками по умолчанию;

- задачи проверки по требованию для приложения Антивирус Касперского для Windows Workstations версий 5.0 и 6.0 в папке **Групповые задачи** группы **Группы** с именами **Задача проверки по требованию** и **Задача поиска вирусов (версия 6.0)** и настройками по умолчанию.

Политики для Антивируса Касперского для Windows Workstations версий 5.0 и 6.0 не создается, если в папке **Группы** политика для данного приложения уже существует.
Если групповые задачи для группы **Группы** и глобальная задача обновления с такими именами уже сформированы, они также не будут создаваться.

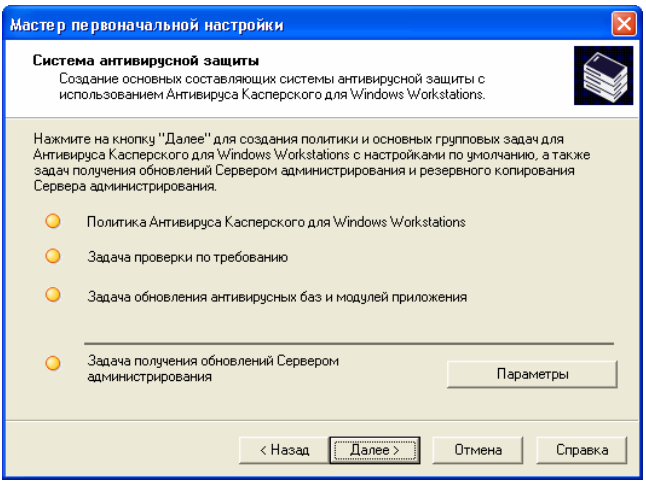

Рисунок 14. Мастер первоначальной настройки.
Настройка системы антивирусной защиты

В случае необходимости вы можете внести изменения в настройки задачи получения обновлений. Для этого нажмите на кнопку **Параметры** и в открывшемся окне установите необходимые значения (подробнее см. п. 4.1.2 на стр. 147).

Нажмите на кнопку **Далее**. Процесс создания политики и задач отображается в окне мастера. В случае возникновения ошибок выводятся соответствующие сообщения.

6. В следующем окне мастера (см. рис. 15) выберите:

   - **Запустить задачу получения обновления сейчас**. В этом случае по завершении работы мастера первоначальной настройки будет запущена задача получения обновлений Сервером администрирования.
   - **Запустить задачу получения обновлений по расписанию**. При этом процедура обновления будет запущена в соответствии с расписанием, заданным в настройках глобальной задачи с именем **Задача получения обновлений Сервером администрирования**.

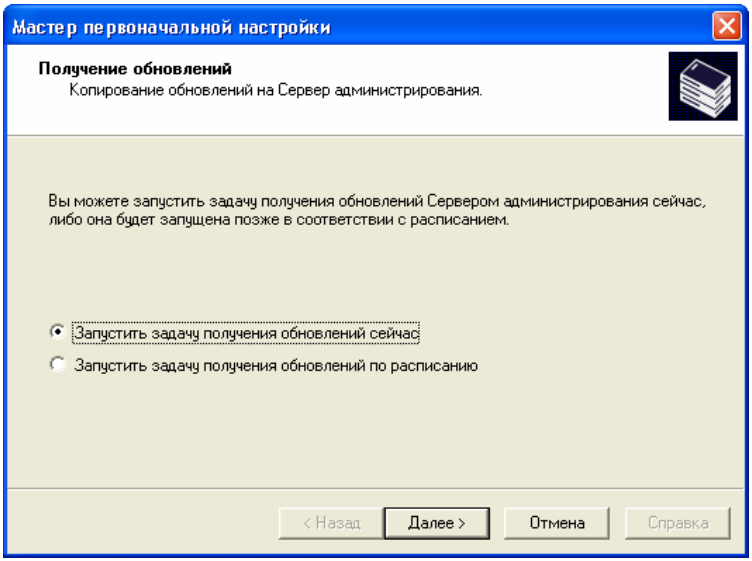

Рисунок 15. Мастер первоначальной настройки.
Настройка получения обновлений

7. В заключительном окне мастера вам будет предложено запустить **Мастер удаленной установки**. Вы можете воспользоваться мастером для установки Агента администрирования. Если вы не хотите устанавливать приложения сразу после окончания работы мастера первоначальной настройки, снимите флажок **Запустить Мастер удаленной установки**.

2.5. Создание, просмотр и изменение структуры логической сети

2.5.1. Просмотр информации о группах

Для просмотра информации о структуре группы, входящей в состав логической сети:

в папке **Группы** выберите папку с названием нужной вам группы. В результате перечень входящих в ее состав объектов будет представлен в панели результатов (вы также можете раскрыть содержание папки в дереве консоли):

- Для просмотра информации о групповых политиках выберите папку **Политики**. Если для группы были определены политики, они отображаются в панели результатов, иначе папка пуста.
- Для просмотра информации о групповых задачах, выберите папку **Групповые задачи**. Если для группы были созданы групповые задачи, они отображаются в панели результатов, иначе папка пуста.
- Для работы с логической сетью подчиненного Сервера администрирования выберите папку **Серверы администрирования**.
- Список клиентских компьютеров, включенных в состав группы, представлен в панели результатов.

Для обновления списка клиентских компьютеров в панели результатов следует пользоваться клавишей **F5** либо командой **Обновить** в меню, контекстном меню или гиперссылкой **Обновить** на панели задач.

2.5.2. Просмотр параметров группы и параметров взаимодействия клиентских компьютеров и Сервера администрирования

Для просмотра параметров группы и параметров взаимодействия Сервера администрирования с клиентскими компьютерами в составе группы:

в папке **Группы** выберите папку с названием нужной вам группы и воспользуйтесь командой **Свойства** контекстного меню или аналогичным пунктом в меню **Действие**. В результате в главном окне программы открывается диалоговое окно **Свойства: <Название группы>**, состоящее из закладок **Общие**, **Клиентские компьютеры**, **Статус компьютера**, **Безопасность** и **Агенты обновления**.

На закладке **Общие** (см. рис. 16) представлена следующая информация:

- название группы;
- название родительской группы, в состав которой входит данная группа (для группы **Группы** данное поле содержит имя Сервера администрирования, к логической сети которого она относится);
- статистическая информация о составе группы – количество вложенных групп и общее число клиентских компьютеров, включая клиентские компьютеры вложенных групп;
- дата создания группы;
- дата последнего изменения названия или атрибутов группы (поле содержит значение **<Неизвестно>**, если название и атрибуты группы не изменялись с момента создания).

При помощи кнопки **Обнулить счетчик вирусов** осуществляется сброс счетчика обнаруженных вирусов для всех клиентских компьютеров группы.

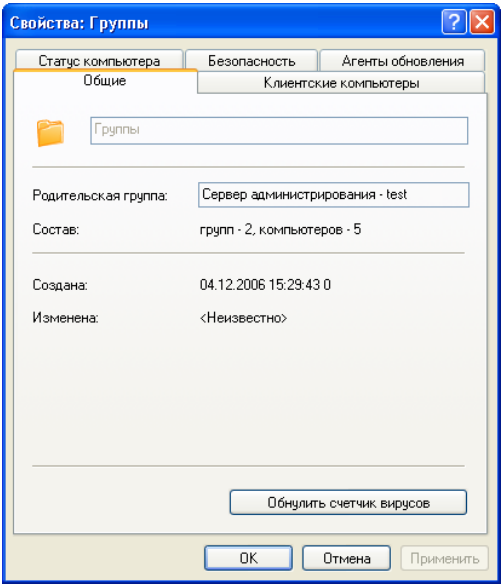

Рисунок 16. Закладка **Общие**

На закладке **Клиентские компьютеры** (см. рис. 17) отображается:

- в разделе **Новый клиентский компьютер в группе** – какие приложения будут автоматически установлены на вновь включенные в состав группы клиентские компьютеры. При этом рядом с именами инсталляционных пакетов нужных приложений установлены флажки.

  При отображении свойств группы **Сеть** и ее подгрупп (см. рис. 29) раздел **Новый компьютер в сети** содержит флажок **Добавить компьютер в состав группы**. Если он установлен, то вновь обнаруженные в составе Windows сети компьютеры автоматически включаются в состав логической сети в группу, название которой расположено ниже, в поле ввода.

- в разделе **Активность клиентского компьютера в сети** отображается реакция Сервера администрирования на отсутствие активности клиентских компьютеров в Windows-сети по истечении заданных интервалов времени: будут ли предприниматься какие-либо действия (например, оповещение администраторов логической сети) и проводиться удаление компьютеров из состава группы.

- Флажок **Перемещать компьютеры автоматически из домена, группы Active Directory или IP-подсети** определяет, будет ли Сервер администрирования автоматически добавлять в группу администрирования все клиентские компьютеры, обнаруженные при опросе сети.

  Чтобы автоматическое добавление выполнялось, установите флажок и укажите при помощи кнопки **Обзор** домен, группу Active Directory или IP-подсеть, из которой будут перемещаться компьютеры.

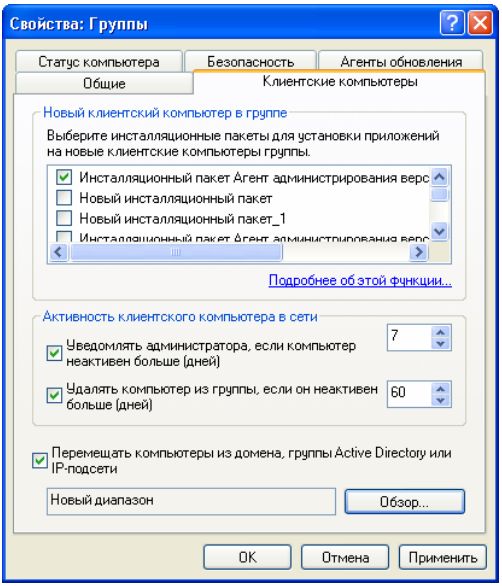

Рисунок 17. Закладка **Клиентские компьютеры**

На закладке **Статус компьютера** (см. рис. 18) представлены критерии диагностики состояния клиентских компьютеров на основании информации о статусе антивирусной защиты на компьютере и данных об активности клиентского компьютера в сети. Если хотя бы одно из этих условий выполняется, клиентскому компьютеру будет присваиваться один из статусов: **Критический** или **Предупреждение**. Если клиентский компьютер не подпадает ни под одно из перечисленных условий, то ему присваивается статус **OK**.

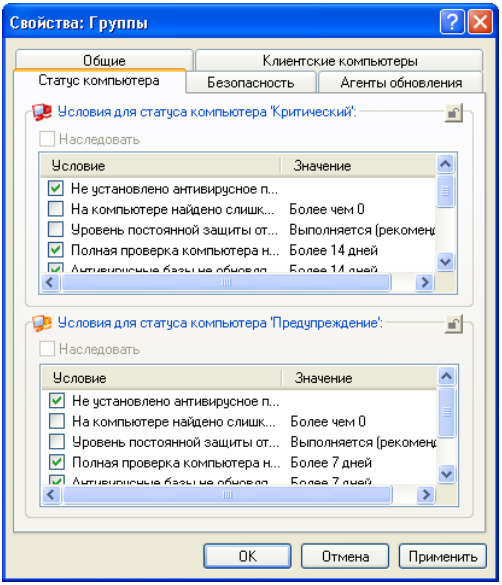

Рисунок 18. Закладка **Статус компьютера**

Для некоторых условий можно изменять пороговые значения. Для этого выберите необходимое условие в столбце **Условие**, и двойным щелчком мыши на нем откройте окно редактирования (см. рис. 19).

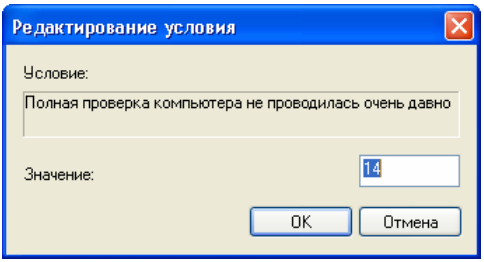

Рисунок 19. Редактирование условия выбора статуса компьютера

Например, можно установить максимальное количество дней, в течение которых клиентский компьютер не соединяется с Сервером администрирования. После истечения этого срока компьютеру будет присвоен статус **Критический**.

Если статус компьютера **OK**, то рядом с его именем, например, в панели результатов главного окна приложения, отображается зеленый значок – . Если статус компьютера **Предупреждение**, то отобра-

жается желтый значок – . Если статус компьютера **Критический**, то отображается красный значок – .

Критерии определения статуса клиентского компьютера устанавливаются в настройках группы предыдущего уровня иерархии и наследуются всеми группами логической сети. Для того чтобы установить отдельные критерии для группы, снимите флажок **Наследовать** и настройте параметры.

Закладка **Безопасность** (см. рис. 5) предназначена для настройки прав доступа к группе администрирования (см. п. 2.2.2 на стр. 19).

На закладке **Агенты обновления** (см. рис. 109) формируется список компьютеров, с помощью которых в пределах группы распространяются обновления и инсталляционные пакеты (см. п. 4.2.3 на стр. 152).

2.5.3. Просмотр информации о клиентском компьютере

Для просмотра информации о клиентском компьютере, включенном в состав логической сети:

в папке **Группы** выберите папку с названием группы, в состав которой входит клиентский компьютер. В результате перечень включенных в состав группы компьютеров будет представлен в панели результатов. Выберите компьютер, информацию о котором вам необходимо получить, и воспользуйтесь командой **Свойства** контекстного меню или аналогичным пунктом в меню **Действие**. В результате в главном окне программы открывается диалоговое окно **Свойства: <Имя компьютера>**, состоящее из нескольких закладок (см. рис. 20).

Чтобы найти нужный клиентский компьютер вы можете воспользоваться функцией поиска (см. п. 5.5 на стр. 179).

На закладке **Общие** (см. рис. 20) вы можете:

- просматривать сетевые параметры компьютера;
- получать информацию о компьютере в окне **Информация о системе** (см. рис. 21), раскрывающемся с помощью гиперссылки **О системе**. В этом окне на закладке **Всего** отображается общая информация о параметрах компьютера и установленной операционной системе, а на закладке **Сторонние приложения** – список установленных на компьютере сторонних приложений;

- изменять имя клиентского компьютера в логической сети (в общем случае его устанавливает Сервер администрирования, и оно совпадает с именем компьютера в Windows-сети);
- вносить собственное описание компьютера;
- определять характер соединения клиентского компьютера с Сервером администрирования при помощи флажка **Не разрывать соединение с Сервером администрирования**. Если флажок установлен, соединение между Сервером администрирования и клиентским компьютером непрерывное, если флажок не установлен (значение по умолчанию), клиентский компьютер подключается к Серверу администрирования только для синхронизации данных или передачи информации.

> Непрерывное соединение следует устанавливать только с наиболее важными клиентскими компьютерами, поскольку общее количество соединений, поддерживаемых Сервером администрирования одновременно, ограничено до нескольких сотен.

Вся информация предоставляется на основании данных, полученных в ходе последней синхронизации клиентского компьютера с Сервером администрирования.

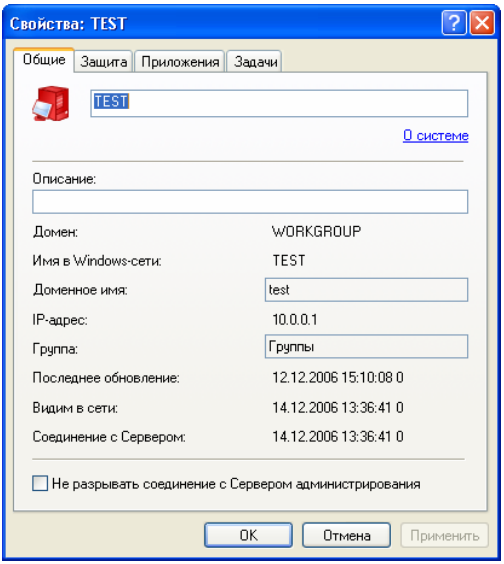

Рисунок 20. Просмотр свойств клиентского компьютера. Закладка **Общие**

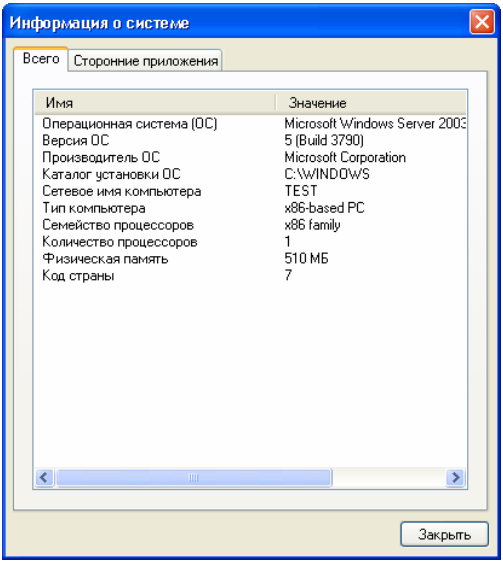

Рисунок 21. Окно просмотра свойств операционной системы клиентского компьютера

На закладке **Защита** (см. рис. 22) представлена информация о состоянии антивирусной защиты на клиентском компьютере. Отображаются следующие данные:

- **Статус постоянной защиты** – статус текущего состояния постоянной защиты клиентского компьютера.
- **Последняя проверка по требованию** – дата и время последней полной проверки клиентского компьютера на присутствие вирусов.
- **Обнаружено вирусов** – общее количество обнаруженных на клиентском компьютере вирусов (счетчик обнаруженных вирусов) со времени установки антивирусного приложения (первой проверки компьютера), либо последнего обнуления значения данной величины. Сброс значения осуществляется при помощи кнопки **Обнулить счетчик вирусов** либо аналогичного пункта контекстного меню или меню **Действие**.
- **Статус компьютера** – статус клиентского компьютера на основании установленных администратором критериев диагностики состояния антивирусной защиты на компьютере и активности компьютера в сети. В поле **Описание статуса компьютера** перечисляются условия, на основании которых клиентскому компьютеру присвоен один из статусов.

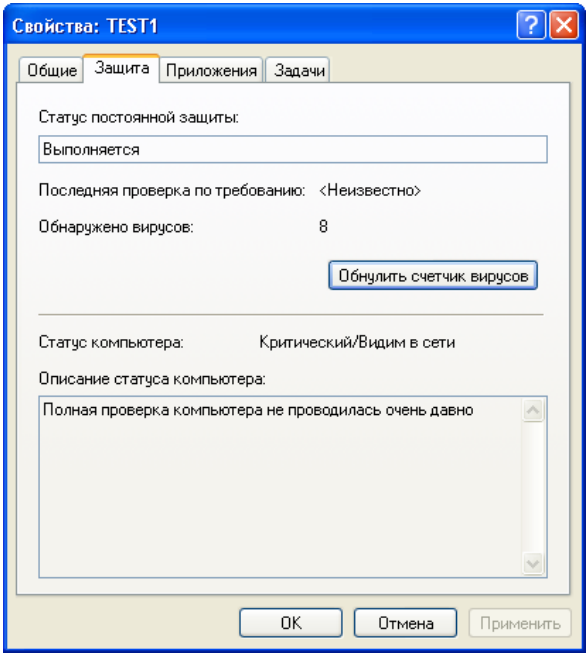

Рисунок 22. Просмотр свойств клиентского компьютера. Закладка **Защита**

На закладке **Приложения** (см. рис. 57) представлен полный список приложений «Лаборатории Касперского», установленных на клиентском компьютере. Вы можете просматривать общую информацию о каждом приложении, управлять его работой и осуществлять настройку (подробнее см. п. 3.1.2 на стр. 90).

На закладке **Задачи** (см. рис. 23) вы можете управлять задачами клиентского компьютера: просматривать список существующих, удалять, создавать новые, запускать и останавливать, изменять настройки задач, просматривать результаты их выполнения. Список задач предоставляется на основании данных, полученных в ходе последней синхронизации клиента с Сервером. Информация о статусе задач запрашивается Сервером администрирования с клиентского компьютера, в случае отсутствия связи статус не отображается.

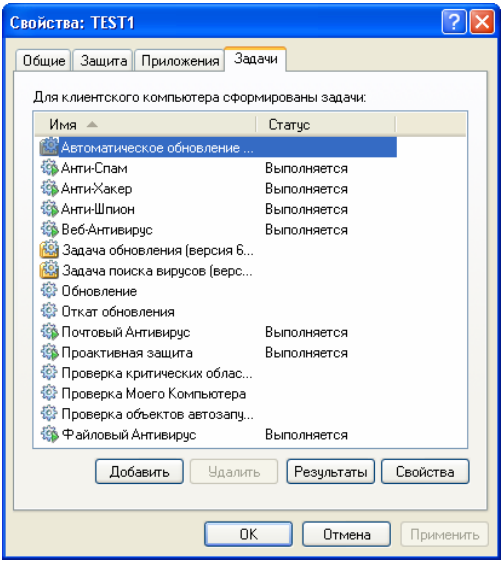

Рисунок 23. Просмотр свойств клиентского компьютера. Закладка **Задачи**

2.5.4. Просмотр логической сети подчиненного Сервера

Для просмотра логической сети подчиненного Сервера администрирования через логическую сеть главного Сервера подключите Консоль к подчиненному Серверу:

1. Выберите в дереве консоли главного Сервера администрирования в нужной вам групповой папке узел **Серверы администрирования**.
2. В узле **Серверы администрирования** выберите нужный подчиненный Сервер, вызовите контекстное меню и выберите команду **Подключиться к Серверу администрирования**. Вы можете также воспользоваться аналогичной командой в меню **Действие**.

В результате в Консоли администрирования отображается структура логической сети подчиненного Сервера администрирования. Далее вы можете просматривать структуру логической сети обычным способом (см. п. 2.5 на с. 31).

Подчиненный Сервер администрирования наследует с главного Сервера групповые задачи и политики той группы, в состав которой он входит. Унаследованные политики и задачи отображаются на подчиненном Сервере следующим образом:

- Рядом с именем политики, полученной с главного Сервера администрирования, отображается значок  . (Обычная иконка политики – ).
- Значения параметров унаследованной политики не доступны для изменения на подчиненном Сервере.
- Параметры, запрещенные к изменению в унаследованной политике не доступны для изменения (значок ) во всех политиках приложения на подчиненном Сервере и используют значения, заданные в унаследованной политике.
- Значения параметров, не закрытых «замком» в унаследованной политике, можно изменять в политиках подчиненного Сервера (значок ). Если параметр разрешен для изменения в политике подчиненного Сервера, его также можно будет изменить в настройках приложения (см. п. 3.1.1.2 на стр. 66) и настройках задачи (см. п. 3.2.4 на стр. 124).
- Рядом с именем групповой задачи, полученной с главного Сервера администрирования, отображается значок  . (Обычная иконка задачи –  .)

Политики и задачи, полученные с главного Сервера администрирования, на подчиненном Сервере не доступны для изменения.
Глобальные задачи и групповые задачи удаленной установки на подчиненные Серверы не передаются.

Для просмотра логической сети подчиненного Сервера напрямую через Консоль

добавьте компьютер, на котором установлен подчиненный Сервер администрирования, в дерево консоли в качестве нового Сервера (см. п. 2.8.1 на стр. 59), и подключитесь к нему (см. п. 2.1.2 на стр. 12).

2.6. Группы

2.6.1. Добавление группы

Чтобы создать группу:

1. В дереве консоли или в панели результатов в папке **Группы** выберите папку, соответствующую группе, в состав которой должна входить новая группа. Если вы создаете группу верхнего уровня иерархии, выберите папку **Группы**.
2. Откройте контекстное меню и выберите команду **Создать / Группу** или воспользуйтесь аналогичным пунктом в меню **Действие**.
3. В открывшемся окне введите имя группы (см. рис. 117) и нажмите на кнопку **ОК**.

В результате в дереве консоли в узле **Группы** в составе указанной вами папки появляется новая папка с заданным именем. В ее состав автоматически будут включены вложенные папки **Политики**, **Групповые задачи** и **Серверы администрирования**. Их наполнение осуществляется на этапе определения политик группы, создания групповых задач и добавления подчиненных Серверов администрирования.

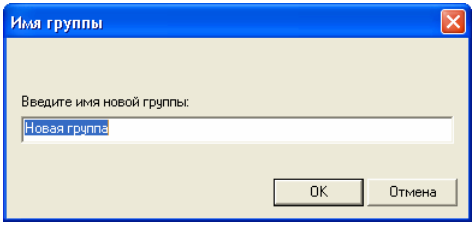

Рисунок 24. Создание группы

2.6.2. Настройка параметров группы

Чтобы настроить параметры группы:

1. Выберите в дереве консоли или в панели результатов нужную группу и воспользуйтесь командой **Свойства** контекстного меню или аналогичным пунктом в меню **Действие**.
2. В результате открывается окно настройки параметров группы (см. рис. 25), состоящее из закладок: **Общие**, **Клиентские компьютеры**, **Статус компьютера**, **Безопасность** и **Агенты обновления**.

На закладке **Общие** (см. рис. 25) вы можете изменить название группы. Название должно быть уникальным в пределах одного уровня иерархии папок (групп). Также представлена следующая информация:

- **Родительская группа**: название группы, в состав которой входит данная группа (для групп верхнего уровня иерархии данное поле содержит имя Сервера администрирования, к логической сети которого относится данная группа);
- **Состав**: статистическая информация о составе группы — количество вложенных групп и общее число клиентских компьютеров, включая клиентские компьютеры вложенных групп;
- **Создана**: дата создания группы;
- **Изменена**: дата последнего изменения названия или атрибутов группы (поле содержит значение **<Неизвестно>**, если название и атрибуты группы не изменялись).

По кнопке **Обнулить счетчик вирусов** вы можете сбросить счетчик обнаруженных вирусов для всех клиентских компьютеров группы.

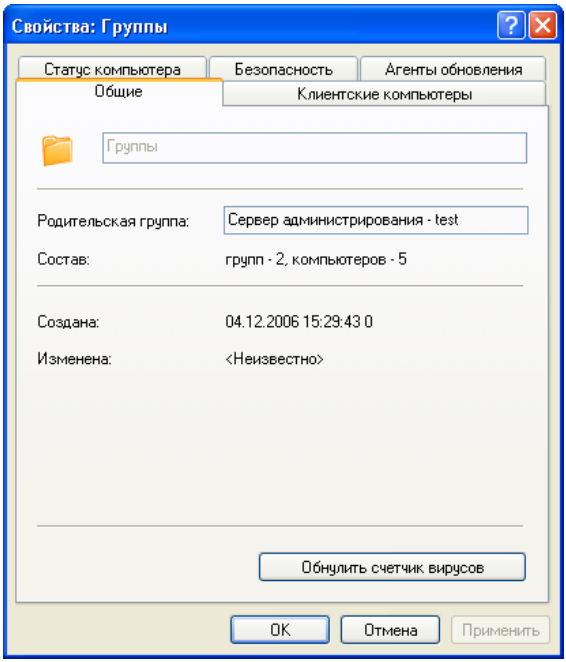

Рисунок 25. Настройка параметров группы.
Закладка **Общие**

На закладке **Клиентские компьютеры** (см. рис. 26) определяются следующие параметры:

- В разделе **Новый клиентский компьютер в группе** вы можете указать, какие инсталляционные пакеты использовать для автоматической удаленной установки приложений «Лаборатории Касперского» на вновь включенные в состав группы клиентские компьютеры. Если пакет используется, рядом с его названием установлен флажок. Для того чтобы автоматическая установка приложения не выполнялась, снимите флажок рядом с названием соответствующего инсталляционного пакета.

Для автоматической установки приложений «Лаборатории Касперского» на новые компьютеры, работающие под управлением операционных систем Microsoft Windows 98/ME, необходимо, чтобы на них был предварительно установлен Агент администрирования.

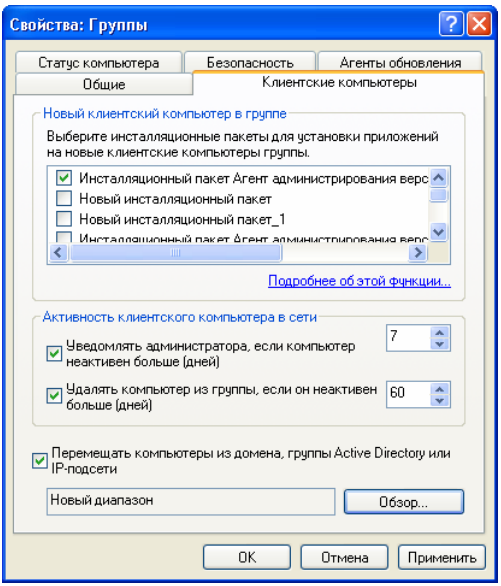

Рисунок 26. Настройка параметров группы. Закладка Клиентские компьютеры

- В разделе **Активность клиентского компьютера в сети** определите, как будет реагировать Сервер администрирования на отсутствие активности в сети клиентских ком-

пьютеров данной группы в течение некоторого временного интервала:

- если будут предприниматься какие-либо действия (например, оповещение администраторов логической сети), установите флажок **Уведомлять администратора, если компьютер не активен больше (дней)** и в поле справа проставьте количество дней. По истечении заданного периода Сервер администрирования выполнит необходимые действия.

  Уведомление производится в соответствии с параметрами, установленными в свойствах Сервера администрирования на закладке **Уведомление** (см. рис. 67).

- если клиентские компьютеры должны удаляться из состава группы, установите флажок **Удалить компьютер из группы, если он неактивен больше (дней)** и в поле справа проставьте количество дней. По истечении заданного периода клиентский компьютер будет автоматически удален из группы и перемещен в группу **Сеть**.

- Установите флажок **Перемещать компьютеры из домена, группы Active Directory или IP-подсети**, если необходимо, чтобы Сервер администрирования автоматически добавлял в группу администрирования все клиентские компьютеры, обнаруженные при опросе сети.

  С помощью кнопки **Обзор** укажите домен, группу Active Directory или IP-подсеть, из которой будут перемещаться компьютеры.

На закладке **Статус компьютера** (см. рис. 27) можно задать условия, при которых клиентскому компьютеру будет присваиваться один из статусов: **Критический** или **Предупреждение**. Если клиентский компьютер не подпадает ни под одно из перечисленных условий, то его статус соответствует **ОК**.

Для некоторых условий можно изменять пороговые значения. Для этого выберите необходимое условие в столбце **Условие**, и двойным щелчком мыши на нем откройте окно редактирования.

Например, можно установить максимальное количество дней, в течение которых клиентский компьютер не соединяется с Сервером администрирования. После истечения этого срока компьютеру будет присвоен статус **Критический**.

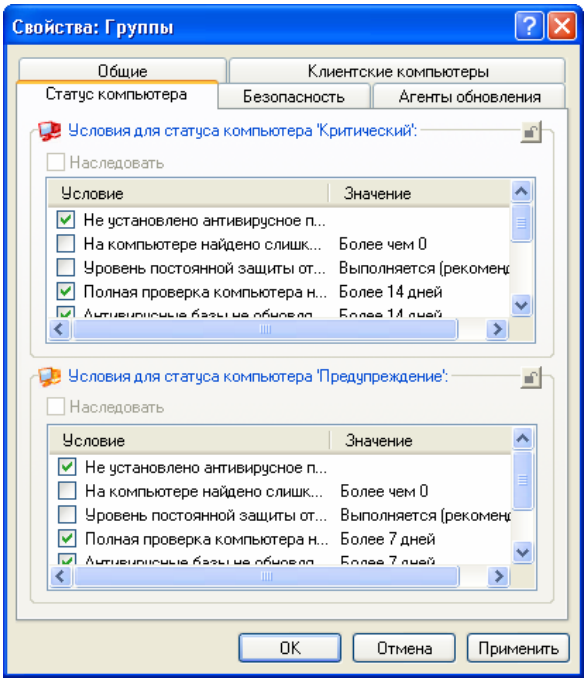

Рисунок 27. Настройка параметров группы.
Закладка **Статус компьютера**

Если статус компьютера соответствует **OK**, то рядом с его именем, например, в панели результатов главного окна приложения, отображается значок . Если статус компьютера **Предупреждение**, то отображается значок . Если статус компьютера **Критический**, то отображается значок .

Критерии определения статуса клиентского компьютера устанавливаются в настройках группы предыдущего уровня иерархии и наследуются всеми группами логической сети. Для того чтобы установить отдельные критерии для группы, снимите флажок **Наследовать** и настройте параметры. (Для групп верхнего уровня иерархии флажок **Наследовать** неактивен.)

На закладке **Безопасность** (см. рис. 28) определите права пользователей и групп пользователей на работу с группой администрирования.

Права на работу с логической сетью и всеми входящими в ее состав объектами определяются в параметрах Сервера адми-

нистрирования (см. п. 2.2 на стр. 17). Для того чтобы установить для группы администрирования индивидуальные права доступа, отличные от заданных в параметрах Сервера администрирования, снимите флажок **Наследовать**.

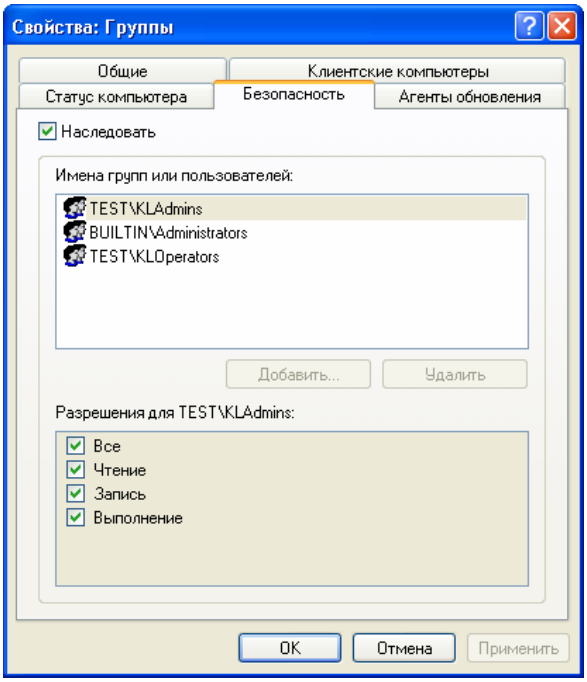

Рисунок 28. Настройка параметров группы.
Закладка **Безопасность**

В верхней части закладки представлен список групп пользователей, зарегистрированных на компьютере, где установлена Консоль администрирования. В нижней части — перечень предусмотренных разрешений:

- **Все**.
- **Чтение**:
  - подключение к Серверу администрирования;
  - просмотр структуры логической сети (или группы администрирования);
  - просмотр значения параметров политик, задач и настроек приложения.

- **Выполнение**: запуск и остановка существующих групповых и глобальных задач.
- **Запись**:
  - создание логической сети, добавление в нее групп и клиентских компьютеров (или в группу администрирования);
  - установка на клиентские компьютеры компонента Агент администрирования;
  - создание и установка на клиентские компьютеры необходимых инсталляционных пакетов для антивирусных приложений компании, а также лицензионных ключей к ним;
  - обновление версии установленных на клиентских компьютерах приложений;
  - создание политик, задач для групп и отдельных компьютеров, изменение настроек приложения;
  - централизованное управление приложениями, получение отчетов об их работе при помощи сервисов, предоставляемых компонентами Сервер, Агент и Консоль администрирования;
  - предоставление пользователям и группам пользователей прав доступа к функциональности Kaspersky Administration Kit.

Для назначения прав выберите группу пользователей и проставьте флажки рядом с названиями нужных разрешений. При установке флажка **Все** проставляются сразу все флажки.

Добавить новую группу или нового пользователя можно при помощи кнопки **Добавить**. При этом возможно добавление только групп пользователей и пользователей из числа зарегистрированных на компьютере Консоли администрирования. Для удаления группы или пользователя из списка используйте кнопку **Удалить**.

На закладке **Агенты обновления** (см. рис. 109) сформируйте, если необходимо, список компьютеров, с помощью которых будут распространяться обновления и инсталляционные пакеты в пределах группы (см. п. 4.2.3 на стр. 152). Использование агентов обновления позволяет снизить нагрузку на Серверы администрирования.

По окончании настройки для применения параметров группы нажмите на кнопку **Применить** или **ОК**.

2.6.3. Настройка автоматической установки программного обеспечения на новые компьютеры в группе

Для того чтобы на новые компьютеры группы автоматически устанавливались приложения «Лаборатории Касперского»,

1. В папке **Группы** выберите папку с названием нужной вам группы, откройте контекстное меню и выберите команду **Свойства** или воспользуйтесь аналогичным пунктом в меню **Действие**.
2. В открывшемся диалоговом окне **Свойства: <Название группы>** на закладке **Клиентские компьютеры** (см. рис. 17) в группе **Новый клиентский компьютер в группе** установите флажки рядом с названиями инсталляционных пакетов, которые должны быть использованы для автоматической установки программного обеспечения или снимите, если установку проводить не следует. По умолчанию автоматическая установка программного обеспечения не производится. Если флажки установлены, то для всех выбранных инсталляционных пакетов будут сформированы групповые задачи удаленной установки с именем **Установка <Имя выбранного инсталляционного пакета>**. Вы сможете запустить их вручную.

Для автоматической установки приложений «Лаборатории Касперского» на новые компьютеры, работающие под управлением операционных систем Microsoft Windows 98/ME, необходимо, чтобы на них был предварительно установлен Агент администрирования.

В дальнейшем вы можете изменить название группы, переместить ее в другую группу или удалить.

2.6.4. Перемещение группы

Для перемещения группы:

выберите перемещаемую папку в дереве консоли или в панели результатов и воспользуйтесь стандартными командами контекстного меню **Вырезать** / **Вставить** или аналогичными пунктами в меню **Действие**, либо мышью.

2.6.5. Изменение названия группы

Для того чтобы изменить название группы,

выберите папку группы в дереве консоли или в панели результатов, откройте контекстное меню и выберите команду **Свойства** либо воспользуйтесь аналогичным пунктом в меню **Действие**. В открывшемся диалоговом окне **Свойства: <Название группы>** на закладке **Общие** (см. рис. 16) измените название группы.

Вы не можете изменить название папки **Группы**, поскольку она является встроенным элементом Консоли администрирования.

2.6.6. Удаление группы

Чтобы удалить группу из состава логической сети,

выберите папку группы в дереве консоли или в панели результатов и воспользуйтесь командой **Удалить** контекстного меню либо аналогичным пунктом в меню **Действие**.

Группа может быть удалена, только если она не содержит подчиненных серверов, вложенных групп и клиентских компьютеров.

2.7. Клиентские компьютеры

2.7.1. Добавление компьютеров в логическую сеть

Для того чтобы включить компьютер/ компьютеры в состав логической сети,

1. В папке **Группы** выберите папку, соответствующую группе, в состав которой вы хотите добавить клиентский компьютер. Если вы добавляете клиентский компьютер на верхний уровень иерархии, выберите папку **Группы**.
2. Откройте контекстное меню и выберите команду **Создать / Компьютер** или воспользуйтесь аналогичным пунктом в меню **Действие**. В результате запускается мастер. Следуйте его указаниям.

3. Прежде всего, вам потребуется определить, каким способом будет проводиться добавление компьютера:

   - автоматически – на основании данных, получаемых Сервером администрирования при опросе Windows-сети предприятия (компьютер переводится в нужную группу из группы **Сеть**).

   - вручную – на основании данных, вводимых администратором. В этом случае достоверность и корректность информации проверяется для предотвращения конфликта имен и поддержания их уникальности. Если в базе данных Сервера администрирования есть информация о наличии этого компьютера в Windows-сети, компьютер включается в состав группы.

4. Далее вам будет предложено сформировать список компьютеров, включаемых в состав группы.

   Если вы выбрали автоматический способ добавления компьютеров, окно мастера содержит папку **Сеть**. Выберите компьютеры, которые необходимо включить в состав группы. Можно выбрать компьютеры из разных папок, можно выбрать сразу всю папку.

   Если вы выбрали способ добавления компьютеров вручную, вам будет предложено провести формирование списка адресов компьютеров, включаемых в состав группы. Вы можете сформировать список адресов в окне мастера при помощи кнопок **Добавить** и **Удалить**, либо импортировать из текстового файла при помощи кнопки **Импортировать**. В качестве адреса компьютера можно использовать IP-адрес (или диапазон IP-адресов) или имя компьютера в сети Windows. Для импорта списка из файла необходимо указать *txt*-файл с перечнем адресов добавляемых компьютеров. Каждый адрес должен располагаться на отдельной строке.

В случае успешного завершения работы мастера компьютеры включаются в состав группы и отображаются в панели результатов под именами, установленными для них Сервером администрирования.

Автоматическое добавление компьютера может быть также осуществлено при помощи мыши в главном окне программы Kaspersky Administration Kit путем перемещения компьютера из папки **Сеть** в папку логической сети.

2.7.2. Автоматическое добавление новых компьютеров в группу

Для того чтобы Сервер администрирования самостоятельно включал все вновь обнаруженные в Windows-сети компьютеры в состав определенной административной группы,

откройте окно просмотра свойств группы **Сеть** и выберите закладку **Клиентские компьютеры** (см. рис. 29). В разделе **Новый компьютер в сети** установите флажок **Добавить компьютер в состав группы** и при помощи кнопки **Обзор** укажите группу, в состав которой должны включаться компьютеры.

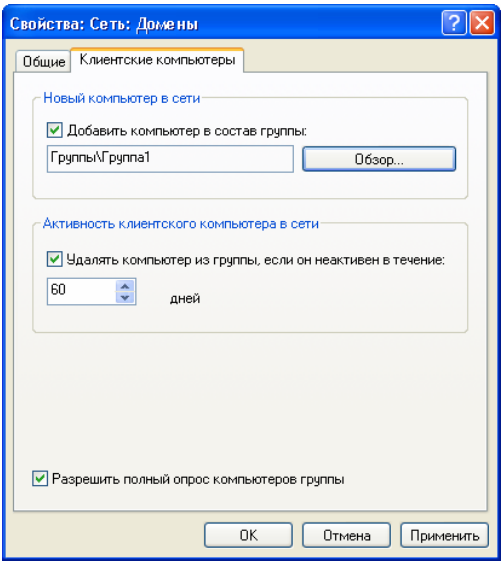

Рисунок 29. Просмотр свойств группы **Сеть**. Закладка **Клиентские компьютеры**

Вы можете переносить клиентские компьютеры из одной группы в другую, исключать из состава логической сети при помощи стандартных команд контекстного меню **Вырезать / Вставить** и **Удалить** или аналогичных пунктов в меню **Действие**. Удаленные из состава логической сети компьютеры перемещаются в группу **Сеть**.

Операция перемещения может быть также осуществлена при помощи мыши.

2.7.3. Перемещение клиентского компьютера в другую логическую сеть. Задача смены Сервера администрирования

Для создания задачи смены Сервера администрирования:

1. Подключитесь к Серверу администрирования, в состав логической сети которого входят переносимые компьютеры (см. п. 2.1 на стр. 12).
2. Запустите мастер создания групповой или глобальной задачи (подробнее см. п. 3.2.1 на стр. 111 или п. 3.2.2 на стр. 121).
3. При выборе приложения и определении типа задачи (см. рис. 30) выберите: **Агент администрирования** и **Смена Сервера администрирования**.

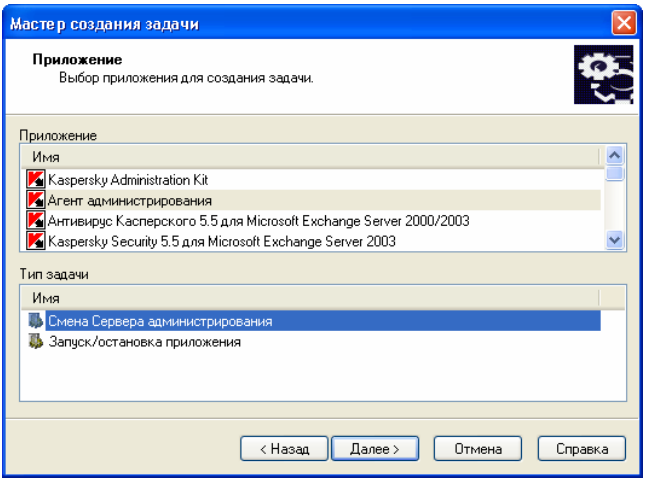

Рисунок 30. Выбор приложения для установки

4. На следующем этапе (см. рис. 31) определите значения параметров, которые будет использовать установленный на клиентских компьютерах Агент администрирования для подключения к новому Серверу.

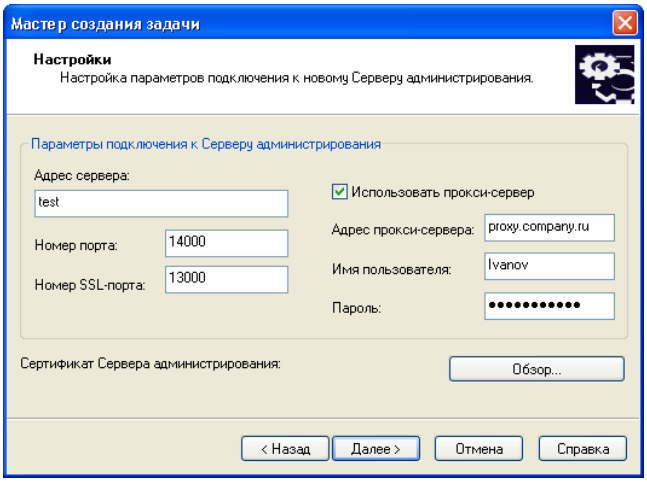

Рисунок 31. Определение Сервера и выбор сертификата

В группе полей **Параметры подключения к Серверу администрирования**:

- укажите адрес Сервера администрирования, в состав логической сети которого должны быть перенесены клиентские компьютеры. В качестве адреса компьютера можно использовать IP-адрес или имя компьютера в сети Windows.
- задайте номер порта, по которому будет осуществляться подключение к новому Серверу администрирования.
- задайте номер порта, по которому будет осуществляться защищенное подключение к новому Серверу администрирования (с использованием SSL-протокола).
- установите флажок **Использовать прокси-сервер**, если подключение к Серверу администрирования осуществляется через прокси-сервер. В поле **Адрес прокси-сервера** введите адрес прокси-сервера. Заполните поля **Имя пользователя** и **Пароль**, если для доступа к прокси-серверу требуется аутентификация.

После этого в поле **Сертификат Сервера администрирования** при помощи кнопки **Обзор** укажите файл сертификата для аутентификации доступа к новому Серверу администрирования.

Файл сертификата имеет расширение .**cer** и размещается на Сервере администрирования, на который перемещаются компьютеры, в папке **Cert** в каталоге установки Kaspersky Administration Kit. Вы можете скопировать файл сертификата в папку общего доступа или на дискету и использовать для настройки параметров доступа к Серверу копию файла.

Заданные на этом этапе параметры задачи вы сможете изменить на закладке **Настройки** (см. рис. 32) окна свойств задачи (подробнее о настройке задач см. п. 3.2.4 на стр. 124).

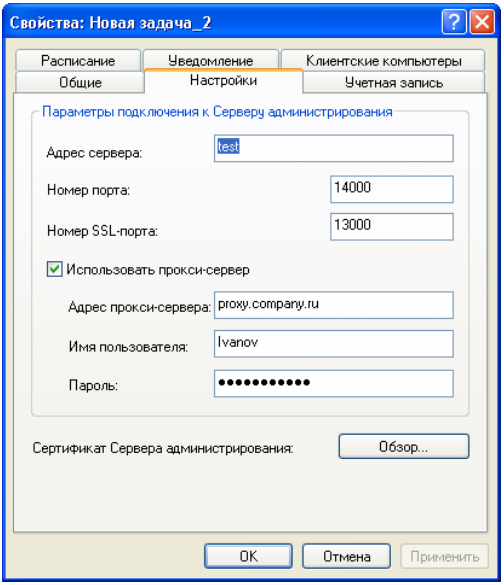

Рисунок 32. Просмотр параметров задачи смены Сервера администрирования

5. Если вы создаете глобальную задачу вам необходимо сформировать список клиентских компьютеров, на которых задача будет запускаться (см. п. 3.2.2 на стр. 121). Эти компьютеры в результате успешного выполнения задачи будут перенесены в состав логической сети заданного в настройках задачи Сервера администрирования и размещены в группе **Сеть**.

В случае групповой задачи к новому Серверу администрирования будет подключены все клиентские компьютеры этой группы.

Для клиентского компьютера с установленным Сервером администрирования задача смены Сервера создаваться и выполняться не будет.

6. На заключительном этапе сформируйте расписание запуска задачи (подробнее см. п. 3.2.1 на стр. 111).

2.7.4. Подключения клиентского компьютера к Серверу администрирования вручную. Утилита *klmover.exe*

Для подключения клиентского компьютера к Серверу администрирования:

на клиентском компьютере из командной строки запустите утилиту ***klmover.exe***, входящую в состав дистрибутива Агента администрирования.

После установки Агента администрирования данная утилита располагается в корне каталога установки компонента и при запуске из командной строки в зависимости от используемых ключей выполняет следующих действия:

- подключает Агент администрирования к Серверу администрирования с указанными параметрами;
- записывает в файл журнала событий или выводит на экран результаты выполнения операции.

Синтаксис утилиты:

- **`klmover [-logfile <имя файла>]` [1] `[-address <адрес сервера>] [-pn <номер порта>] [-ps <номер SSL-порта>] [-nossl] [-cert <путь к файлу сертификата>] [-silent] [-dupfix]`**

Описание ключей:

- **`-logfile <имя файла>`** – записать результаты выполнения утилиты в файл журнала; по умолчанию информация сохраняется в файле ***stdout.tx***; если ключ не используется, результаты и сообщения об ошибках выводятся на экран.

[1] В квадратных скобках приводятся необязательные ключи.

- **-address <адрес сервера>** – адрес Сервера администрирования для подключения; в качестве адреса может быть указан IP-адрес, NetBIOS или DNS-имя компьютера.
- **-pn <номер порта>** – номер порта, по которому будет осуществляться незащищенное подключение к Серверу администрирования; по умолчанию используется 14000 порт.
- **-ps <номер SSL-порта>** – номер SSL-порта, по которому будет осуществляться защищенное подключение к Серверу администрирования с использованием протокола SSL. По умолчанию это **13000** порт.
- **-nossl** – использовать незащищенное подключение к Серверу администрирования; если ключ не указан, подключение Агента к Серверу осуществляется по защищенному SSL-протоколу.
- **-cert <путь к файлу сертификата>** – использовать указанный файл сертификата для аутентификации доступа к новому Серверу администрирования. Если ключ не используется, Агент администрирования получит сертификат при первом подключении к Серверу администрирования.
- **-silent** – запустить утилиту на выполнение в неинтерактивном режиме; использование ключа может быть полезно, например, при запуске утилиты из сценария запуска при регистрации пользователя.
- **-dupfix** – данный ключ используется в случае, если установка Агента администрирования была выполнена не традиционным способом с использованием дистрибутива, а, например, путем восстановления из образа диска.

2.7.5. Проверка соединения клиентского компьютера и Сервера администрирования вручную. Утилита *klnagchk.exe*

Для проверки соединения клиентского компьютера и Сервера администрирования:

на клиентском компьютере из командной строки запустите утилиту ***klnagchk.exe***, входящую в состав дистрибутива Агента администрирования.

После установки Агента администрирования данная утилита располагается в корне каталога установки компонента и при запуске из командной строки в зависимости от используемых ключей выполняет следующих действия:

- выводит на экран или в файл журнала значения параметров подключения установленного на клиентском компьютере Агента администрирования к Серверу администрирования;
- записывает в файл журнала событий статистику Агента администрирования (с момента последнего запуска данного компонента) и результаты выполнения утилиты либо выводит информацию на экран;
- предпринимает попытку установить соединение Агента администрирования с Сервером администрирования;
- если соединение установить не удалось, посылает ICMP-пакет для проверки статуса компьютера, на котором установлен Сервер администрирования.

Синтаксис утилиты:

- **klnagchk [-logfile <имя файла>]** [2] **[-sp] [-savecert <путь к файлу сертификата>] [-restart]**

Описание ключей:

- **-logfile <имя файла>** – записать значения параметров подключения Агента администрирования к Серверу и результаты выполнения утилиты в файл журнала; по умолчанию информация сохраняется в файле ***stdout.tx***; если ключ не используется, параметры, результаты и сообщения об ошибках выводятся на экран.
- **-sp** – вывести пароль для аутентификации пользователя на прокси-сервере; параметр используется, если подключение к Серверу администрирования осуществляется через прокси-сервер.
- **-savecert <имя файла>** – сохранить сертификат для аутентификации доступа к Серверу администрирования в указанном файле.
- **-restart** – перезапустить Агент администрирования после завершения утилиты.

[2] В квадратных скобках приводятся необязательные ключи.

2.8. Подчиненные Серверы администрирования

2.8.1. Добавление подчиненного Сервера

Чтобы добавить в логическую сеть подчиненный Сервер администрирования,

1. Выберите в группе администрирования узел **Серверы администрирования**, откройте контекстное меню и выберите команду **Создать / Сервер администрирования**. Вы можете также воспользоваться аналогичной командой в меню **Действие**. В результате запускается мастер. Следуйте его указаниям.
2. Вам будет предложено определить имя подчиненного Сервера администрирования, введите его вручную. Под этим именем Сервер будет отображаться в группе администрирования. Имя должно быть уникальным в пределах одного уровня иерархии групп.
3. В следующем окне мастера вы можете указать сетевой адрес подчиненного Сервера администрирования. В этом случае главный Сервер администрирования отдает команду на подключение подчиненному Серверу, а также передает все необходимые атрибуты (сетевой адрес главного Сервера администрирования, имя подчиненного Сервера администрирования, сертификат главного Сервера администрирования).

   Если вы не хотите указывать сетевой адрес подчиненного Сервера администрирования, нажмите на кнопку **Далее**.
4. Укажите сертификат подчиненного Сервера администрирования. Для этого нажмите на кнопку **Обзор** и укажите путь к файлу сертификата.

5. Если на предыдущем шаге вы указали адрес подчиненного Сервера, на этом этапе вам будет предложено определить параметры подключения подчиненного Сервера администрирования к главному:

   - Укажите адрес главного Сервера администрирования. В качестве адреса компьютера можно использовать IP-адрес или имя компьютера в сети Windows.
   - Если подключение будет выполняться через прокси-сервер, настройте параметры подключения в группе полей **Параметры прокси-сервера**.

     Установите флажок **Использовать прокси-сервер**. В поле **Адрес прокси-сервера** введите адрес прокси-сервером. Заполните поля **Имя пользователя**, **Пароль** и **Подтверждение пароля**, если для доступа к прокси-серверу требуется аутентификация.

   Если адрес подчиненного сервера указан не был, данный шаг отсутствует.

8. На этом этапе выполняются следующие операции:

   - добавление информации о подчиненном Сервере в базу данных главного Сервера администрирования;
   - подключение Консоли администрирования к подчиненному Серверу;
   - настройка параметров подключения подчиненного Сервера администрирования к главному.

   Если адрес подчиненного Сервера указан не был, то после завершения мастера вам следует вручную:

   - подключить Консоль администрирования к подчиненному Серверу;
   - настроить параметры подключения подчиненного Сервера к главному.

   Нажмите на кнопку **Далее**. Процесс выполнения операций отображается в окне мастера. В случае возникновения ошибок выводятся соответствующие сообщения.

9. В заключительном окне мастера нажмите на кнопку **Готово**.

В результате работы мастера главный Сервер администрирования добавляет информацию о подчиненном Сервере в базу данных. Значок и имя подчиненного Сервера администрирования отображаются в папке **Серверы** в соответствующей группе администрирования.

2.8.2. Настройка параметров подключения подчиненного Сервера к главному

Чтобы настроить параметры подключения подчиненного Сервера к главному Серверу администрирования,

1. Добавьте подчиненный Сервер администрирования в дерево консоли в качестве управляемого Сервера администрирования (см. п. 2.8.1 на стр. 59).
2. В открывшемся окне **Свойства: Сервер администрирования <имя компьютера>** на закладке **Общие** воспользуйтесь ссылкой **Параметры иерархии серверов**.
3. В открывшемся окне **Параметры главного Сервера администрирования** (см. рис. 33) установите флажок **Данный Сервер администрирования является подчиненным**.

   После этого в группе полей **Подключение к главному Серверу администрирования**

   - Укажите адрес главного Сервера администрирования. В качестве адреса компьютера можно использовать IP-адрес или имя компьютера в сети Windows.

     Если подключение будет выполняться через прокси-сервер, установите флажок **Использовать прокси-сервер**. В поле **Адрес прокси-сервера** введите адрес для соединения с прокси-сервером. Заполните поля **Имя пользователя**, **Пароль** и **Подтверждение пароля**, если для доступа к прокси-серверу требуется аутентификация.

   Для применения настроек нажмите на кнопку **ОК** или **Применить**.
4. В окне **Свойства: Сервер администрирования <имя компьютера>** на закладке **Общие** нажмите на кнопку **Применить** или **ОК**.

В результате подчиненный Сервер администрирования соединяется с главным Сервером и получает от него все политики и задачи для группы, в которую включен подчиненный Сервер. После этого вы можете подключиться к подчиненному Серверу через главный Сервер из узла **Серверы администрирования**.

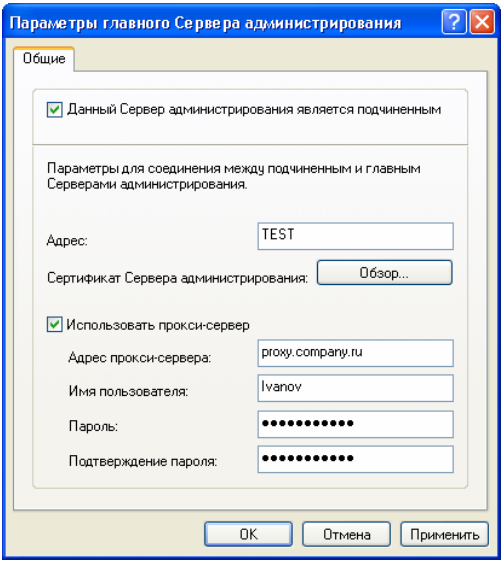

Рисунок 33. Настройка параметров подключения к главному Серверу администрирования

ГЛАВА 3. УДАЛЕННОЕ УПРАВЛЕНИЕ ПРИЛОЖЕНИЯМИ

3.1. Настройка параметров приложения

3.1.1. Управление политиками

3.1.1.1. Создание политики

Для того чтобы создать новую политику для группы,

1. В дереве консоли выберите группу, для которой вы будете определять политику, выберите входящую в ее состав папку **Политики**, откройте контекстное меню и выберите команду **Создать / Политику**, или воспользуйтесь аналогичным пунктом в меню **Действие**. В результате запускается мастер. Следуйте его указаниям.

2. Вам будет предложено задать имя политики и выбрать приложение, для которого она создается.

   Определение имени производится стандартным способом. Если вы зададите имя уже существующей политики, к нему автоматически будет добавлено окончание **_1**.

   Выбор приложения осуществляется (см. рис. 34) из раскрывающегося списка. В нем перечислены все приложения компании, для которых на рабочее место администратора установлены плагины управления.

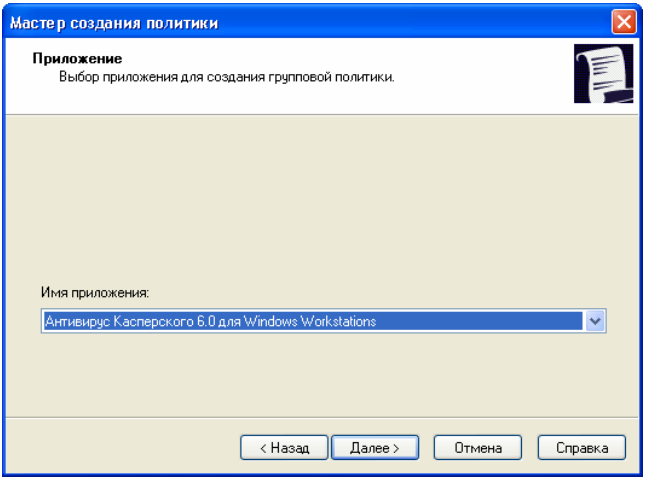

Рисунок 34. Создание политики. Выбор приложения

3. В следующем окне мастера (см. рис. 35) укажите статус политики. Выберите один из вариантов:

   - **Активная политика**. В этом случае создаваемая политика будет использоваться в качестве действующей для приложения.
   - **Неактивная политика**. При этом политика будет сохранена в узле **Политики**. По необходимости ее можно сделать действующей (см. п. 3.1.1.4 на стр. 78).
   - **Политика для мобильного пользователя**. Эта политика будет действовать при отключении компьютера от логической сети предприятия. Подобный тип политики доступен только для Антивируса Касперского для Windows Workstations версий 5.0 и 6.0, Антивируса Касперского 5.0 для Windows File Servers и Антивируса Касперского 6.0 для Windows Servers.

В группе для одного приложения может быть создано несколько политик, но действующей политикой может быть только одна из них.
При создании новой действующей политики предыдущая становится неактивной.

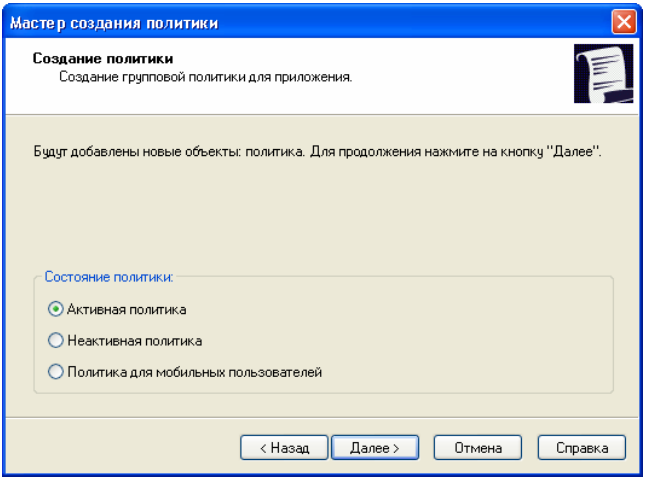

Рисунок 35. Создание политики. Активирование политики

4. Далее вам необходимо ознакомиться с общими настройками политики и провести настройку параметров, соответствующих выбранному приложению (см. рис. 36). Вы можете наложить запрет на дальнейшее изменение параметров в политиках вложенных групп, в настройках приложения и настройках задач. Параметры, входящие в политику, на изменение которых может быть наложен запрет, сопровождаются значком  . Для наложения запрета щелкните по нему левой кнопкой мыши. Значок изменится на  .

   Локальные настройки приложения имеют приоритет над настройками политики. Для того чтобы политика начала действовать на клиентских компьютерах, требуется запретить изменение необходимых параметров.

   На этапе создания политики производится настройка минимального набора параметров, без которых приложение не будет работать. Остальные значения устанавливаются по умолчанию и соответствуют значениям по умолчанию при локальной установке приложения. Вы можете внести изменения в политику путем ее редактирования (см. п. 3.1.1.2 на стр. 66).

   Подробное описание настройки политики для приложений приводится в Руководствах каждого из них.

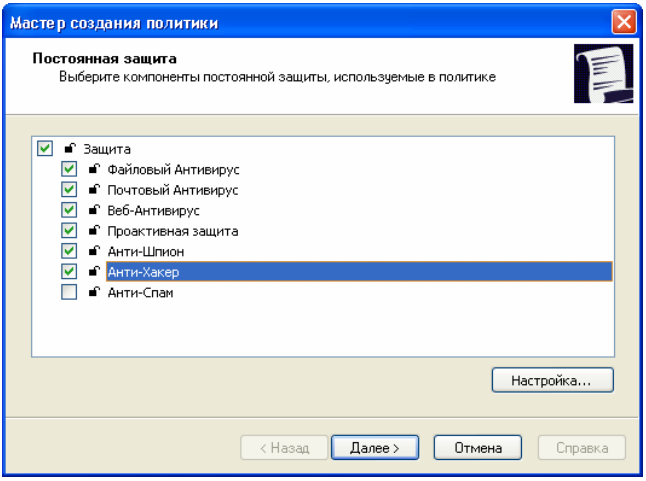

Рисунок 36. Создание политики для приложения Антивирус Касперского® 6.0 для Windows Workstations

5. В заключительном окне мастера нажмите на кнопку **Готово**.

После создания политики на клиентских компьютерах, для которых она сформирована, начинают действовать параметры, на изменение которых наложен запрет (установлен «замок»).

Для того чтобы настроить копирование параметров политики в настройки приложений и задач на клиентских компьютерах, необходимо произвести дополнительные настройки в окне **Дополнительно** (см. рис. 39).

3.1.1.2. Просмотр и настройка параметров политики

Для того чтобы просмотреть значения параметров групповой политики и/или внести в нее изменения,

в дереве консоли выберите необходимую группу, выберите входящую в ее состав папку **Политики**. После этого в панели результатов будет представлен список всех сформированных для данной группы политик. Выберите нужную политику, откройте контекстное меню и выберите команду **Свойства** или воспользуйтесь аналогичным пунктом в меню **Действие**.

В результате открывается окно настройки групповой политики для приложения **Свойства: <Имя политики>**, состоящее из нескольких закладок. Состав закладок для каждого приложения свой, подробное описание приводится в Руководствах каждого из них. Закладки **Общие**, **Применение**, **События** входят в состав окна настройки политики каждого приложения.

На закладке **Общие** (см. рис. 37) приведены общие сведения о политике:

- название политики;
- приложение, для которого создана политика (например, Антивирус Касперского 6.0 для Windows Workstations);
- версия приложения;
- дата и время создания политики;
- дата и время последнего редактирования политики;
- флажок **Активировать политику по событию** и список для выбора события, по которому политика активируется автоматически;
- раскрывающийся список **Состояние политики**, в котором можно указать, является политика действующей, неактивной или политикой для мобильного пользователя.

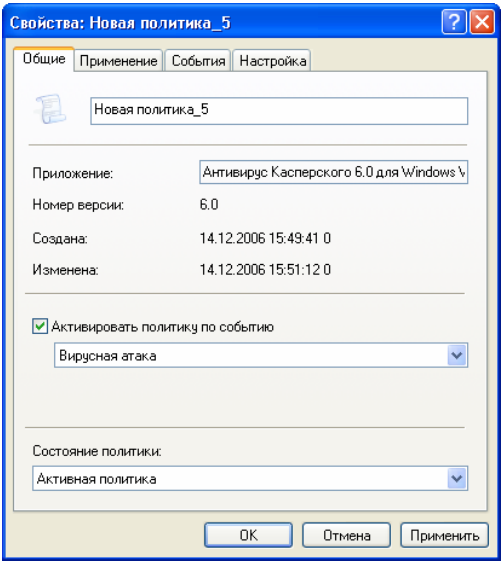

Рисунок 37. Редактирование политики. Закладка **Общие**

На данной закладке вы можете:

- изменить название политики;
- определить автоматическую активацию политики при наступлении события и выбрать это событие;
- задать состояние политики.

На закладке **Применение** (см. рис. 38) представлена справочная информация о результатах применения политики на клиентских компьютерах группы, при этом указано количество компьютеров:

- для которых политика была определена;
- на которых политика приведена в исполнение;
- на которых еще не приведена в исполнение;
- на которых политику применить не удалось.

В нижней части закладки **Применение** (см. рис. 38) вы можете настроить копирование параметров политики в настройки приложения и задач на клиентских компьютерах. Для этого щелкните по гиперссылке **Дополнительно** и в открывшемся окне (см. рис. 39) выберите один из следующих вариантов:

- **Не изменять параметры.** В этом случае для приложения будут применены только те параметры, рядом с которыми в настройках политики установлен значок  . Остальные параметры будут соответствовать локальным настройкам. Этот вариант установлен по умолчанию.

  После удаления политики или прекращения ее действия все локальные параметры приложения вернутся к тем значениям, которые действовали до применения политики.

- **Изменить обязательные параметры при первом применении политики**. В этом случае для приложения будут применены только те параметры, рядом с которыми в настройках политики установлен значок  .

  В этом случае после удаления политики или прекращения ее действия к исходным значениям вернутся только те параметры, редактирование которых не было запрещено в политике (т. е. для них был установлен значок ).

- **Изменять все параметры при первом применении политики.** В этом случае в соответствии с настройками политики будут изменены все локальные параметры.

  После удаления политики или прекращения ее действия приложение продолжит работу с настройками, заданными в политике. В дальнейшем их можно будет изменить вручную.

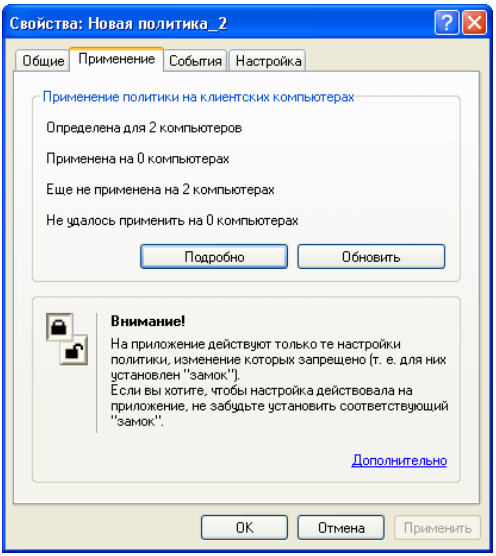

Рисунок 38. Редактирование политики. Закладка **Применение**

Изменения локальных параметров производится автоматически в соответствии с выбранным вариантом при первом применении политики на клиентском компьютере.

Если вы изменили какие-либо параметры политики и хотите повторно применить ее, нажмите на кнопку **Изменить сейчас**. При этом политика будет применена в соответствии с параметром, выбранным выше.

При применении политики на большом количестве клиентских компьютеров существенно возрастает нагрузка на Сервер администрирования и объем сетевого трафика.

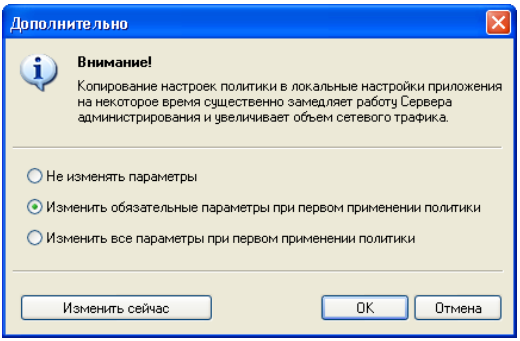

Рисунок 39. Настройка применения политики

Подробную информацию о результатах применения политики на каждом клиентском компьютере группы можно посмотреть в окне (см. рис. 40), которое открывается при помощи кнопки **Подробно**. В данном окне представлена таблица, состоящая из следующих столбцов:

- **Компьютер** – имя клиентского компьютера.
- **Домен** – название домена, к которому принадлежит компьютер.
- **Статус** – статус политики; столбец может содержать значение:
  - **Изменена** – на Сервере администрирования есть изменения по данной политике (изменены настройки), но они не синхронизированы с клиентским компьютером.
  - **Применена** – политика для приложения на данном компьютере успешно применена.
  - **Ожидает применения** – политика для приложения на данном компьютере еще не применялась.
  - **Не удалось применить** – политику на данном компьютере применить не удалось (компьютер выключен, соединение с компьютером не установлено, приложение не запущено или не установлено и т.п.).
- **Дата** – дата и время регистрации события.

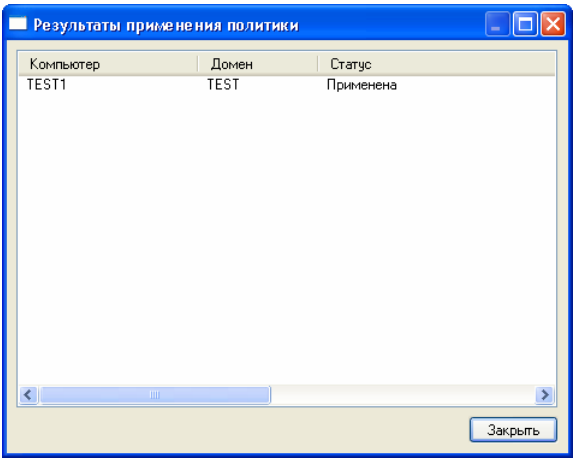

Рисунок 40. Результаты применения политики на клиентских компьютерах группы

На закладке **События** (см. рис. 41) представлены параметры, определяющие правила обработки событий, происходящих в работе приложения: какие события фиксируются, режим оповещения о них ад-

министратора и/или других пользователей и место хранения информации.

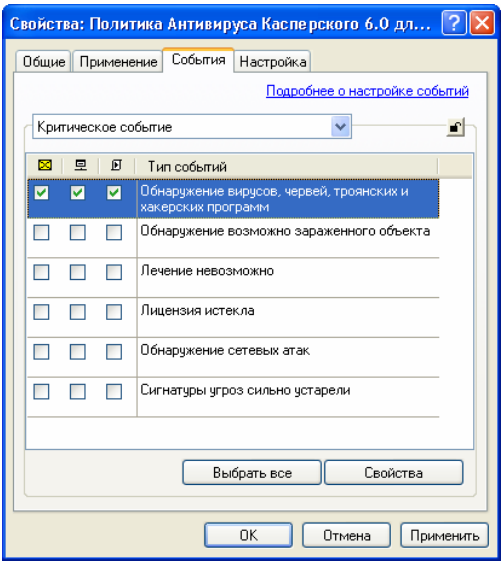

Рисунок 41. Редактирование политики. Закладка **События**

Непосредственно после создания политики значения параметров на закладке **События** соответствуют настройкам приложения по умолчанию. Данные параметры индивидуальны для каждого приложения, их подробное описание приводится в Руководствах к ним. В случае необходимости вы можете внести изменения в политику.

Для всех приложений компании предусмотрено четыре уровня важности событий, происходящих в их работе:

- **Критическое событие** (например, вирусная атака).
- **Отказ функционирования** (например, недоступна папка общего доступа).
- **Предупреждение** (например, клиентский компьютер слишком долго не проявляет активности в сети).
- **Информационное сообщение** (например, найден новый клиентский компьютер).

Настройка правил обработки событий осуществляется для каждого уровня важности отдельно:

1. Из раскрывающегося списка выберите уровень важности событий: **Критическое событие**, **Отказ функционирования**, **Предупреждение** или **Информационное сообщение**.
2. В результате выбора типы событий, которые могут иметь указанный уровень важности, будут представлены в расположенной ниже таблице. Перечень для каждого приложения индивидуален. Подробную информацию вы можете посмотреть в соответствующих Руководствах к приложениям. Выберите типы событий, информация о которых должна фиксироваться, при помощи клавиш <**Shift**> и <**Ctrl**>. Чтобы выбрать все типы событий, нажмите на кнопку **Выбрать все**.
3. Для того чтобы включить оповещение о выбранных событиях, задайте способы оповещения, установив флажки в соответствующих столбцах таблицы (– электронная почта, – средства NET SEND, – запуск исполняемого файла). Затем для выбранных типов событий нажмите на кнопку **Свойства** и перейдите на закладку **Уведомление** (см. рис. 42).

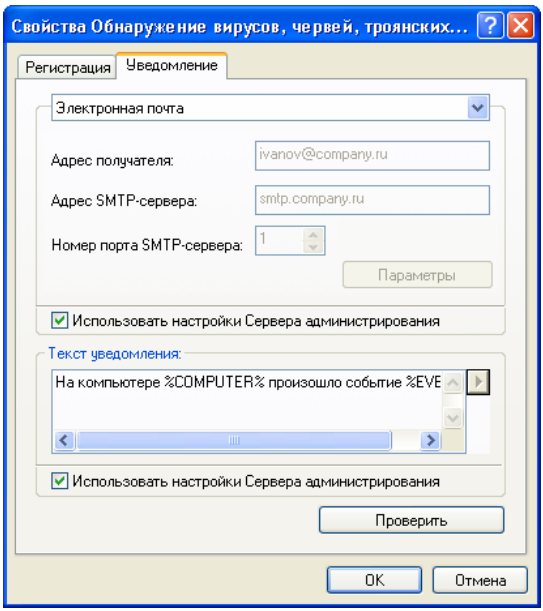

Рисунок 42. Редактирование свойств события. Закладка **Уведомление**

В верхней части закладки производится настройка способов оповещения. Если в этом блоке установлен флажок **Использовать настройки Сервера администрирования**, то по умолчанию используются значения, заданные в свойствах Сервера администрирования на закладке **Уведомление** (см. рис. 67). Чтобы изменить параметры оповещения, снимите флажок **Использовать настройки Сервера администрирования** и в раскрывающемся списке выберите:

- **Электронная почта** (см. рис. 42). В этом случае:
  - в поле **Адрес получателя** введите электронный адрес получателя уведомлений (допускается ввод нескольких адресов разделенных запятой или точкой с запятой);
  - в поле **Адрес SMTP-сервера** укажите адрес почтового сервера. В качестве адреса можно использовать IP-адрес или имя компьютера в сети Windows;
  - в поле **Номер порта SMTP-сервера** введите номер коммуникационного порта SMTP-сервера. По умолчанию используется порт 25;
  - отправителя и тему сообщения, которое будет доставляться в качестве уведомления. Для этого нажмите на кнопку **Параметры** и в открывшемся окне (см. рис. 43) заполните поля **От** и **Тема**. В этом же окне, если используется ESMTP-авторизация, в соответствующем разделе заполните поля **Имя пользователя** и **Пароль**.

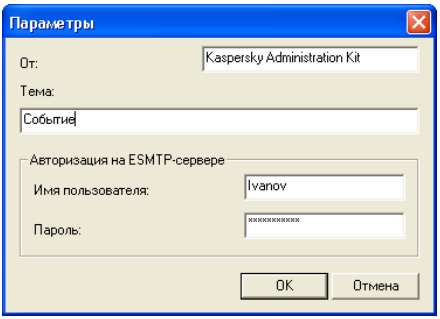

Рисунок 43. Формирование параметров рассылки уведомлений. Ввод отправителя и темы сообщения

- **NET SEND** (см. рис. 44). В этом случае в поле ниже укажите адреса компьютеров-получателей уведомлений по сети. В качестве адреса также можно использовать IP-адрес или имя компьютера в Windows-сети. Допускается ввод нескольких адресов разделенных запятой или точкой с запятой.

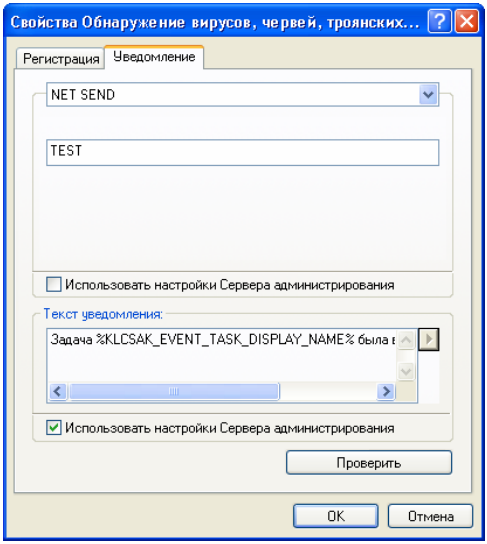

Рисунок 44. Настройка режима оповещений. Оповещение средствами NET SEND

- **Исполняемый файл для запуска** (см. рис. 44). В этом случае с помощью кнопки **Обзор** укажите исполняемый модуль для запуска при наступлении события.

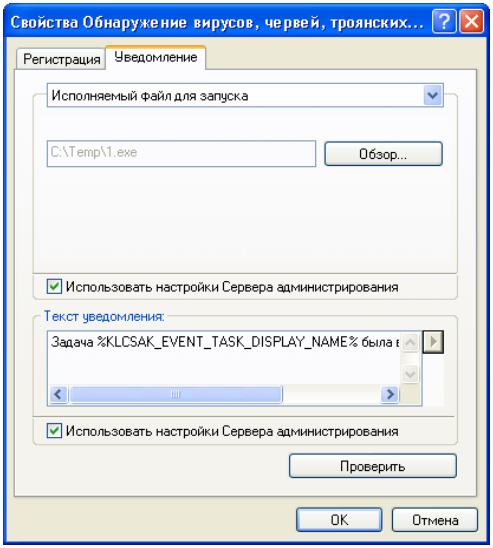

Рисунок 45. Настройка режима оповещений. Оповещение с помощью исполняемого файла

Имена переменных окружения исполняемого модуля совпадают с именами подстановочных параметров, используемых для формирования текста сообщения (см. ниже).

В нижней части закладки (см. рис. 42) введите текст сообщения, которое будет доставляться в качестве уведомления. Если в этом блоке установлен флажок **Использовать настройки Сервера администрирования**, то по умолчанию используется текст, заданный в свойствах Сервера администрирования на закладке **Уведомление** (см. рис. 67). Чтобы изменить текст сообщения, снимите флажок **Использовать настройки Сервера администрирования** и сформируйте новый текст.

В состав сообщения может включаться информация о зарегистрированном событии. Для этого следует вставить в шаблон соответствующие подстановочные параметры, выбрав необходимые из раскрывающегося с помощью кнопки  списка:

- **Уровень важности события**.
- **Компьютер-отправитель**.
- **Домен**.
- **Событие**.
- **Описание события**.
- **Время регистрации**.
- **Имя задачи**.
- **Приложение**.
- **Номер версии**.
- **IP-адрес**.
- **IP-адрес соединения**.

Чтобы проверить корректность установленных на этой закладке (см. рис. 42) параметров, вы можете вручную отправить сообщение. Для этого нажмите на кнопку **Проверить**. В результате откроется окно отправки тестового уведомления (см. рис. 46). При возникновении каких-либо ошибок отобразится подробная информация о них.

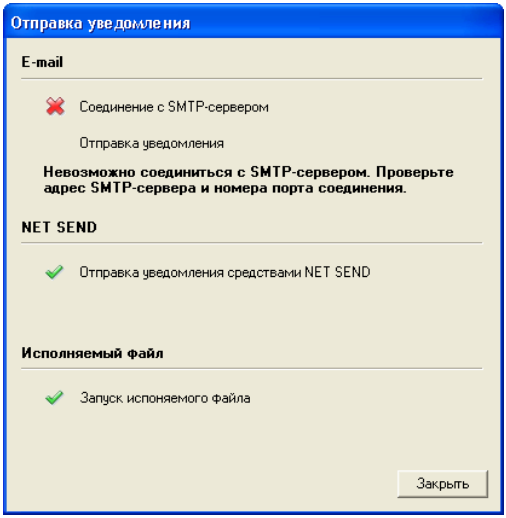

Рисунок 46. Формирование параметров рассылки уведомлений. Отправка тестового уведомления

4. Для того чтобы информация о событиях сохранялась в журналах событий, выберите типы событий, нажмите на кнопку **События**. Перейдите на закладку **Регистрация** (см. рис. 47) и установите следующие флажки:

   - **На Сервере администрирования в течение (дней)**, для того чтобы информация о событиях в работе приложений на всех клиентских компьютерах группы сохранялась централизованно на Сервере администрирования. В поле справа задайте количество дней, в течение которых она будет храниться. По истечении заданного периода с момента регистрации события информация о нем будет удалена. Просматривать информацию о событиях, хранящуюся на Сервере администрирования, вы можете с рабочего места администратора через Консоль администрирования. Она представлена в дереве консоли в узле **События**.
   - **Локально на клиентском компьютере**, для того чтобы информация о событиях сохранялась на каждом клиентском компьютере локально. В этом случае ее просмотр возможен только через локально установленную Консоль администрирования (контейнер **Локальный компьютер**).

     Эта возможность доступна только при работе с Антивирусом Касперского 5.0 для Windows File Servers.

- **В журнале событий Windows на клиентском компьютере**, для того чтобы информация о событиях сохранялась в системном журнале Windows на каждом клиентском компьютере локально.
- **В журнале событий Windows на Сервере администрирования**, для того чтобы информация о событиях в работе приложений на всех клиентских компьютерах группы сохранялась централизованно в системном журнале Windows компьютера Сервера администрирования.

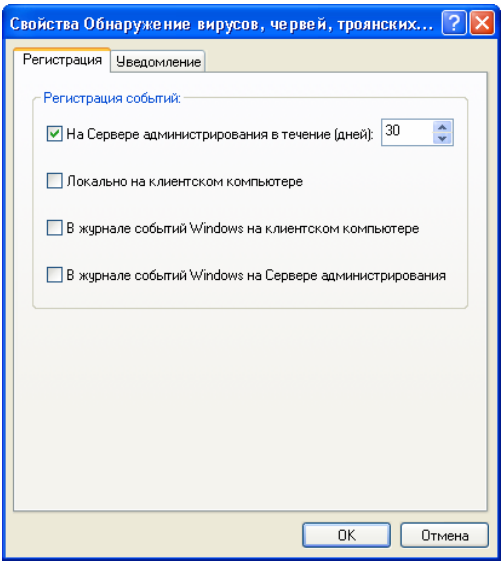

Рисунок 47. Настройка способов регистрации информации о событиях

Доступ к информации в журналах событий Windows будет осуществляться при помощи стандартного инструмента Windows просмотра и управления журналами **Просмотр событий**.

5. После установки всех необходимых параметров нажмите на кнопку **Применить** и выберите следующий уровень важности для настройки.

3.1.1.3. Отображение унаследованной политики в панели результатов вложенной группы

*Для того чтобы во вложенной группе в папке **Политики** отображались унаследованные политики:*

1. Выберите в панели результатов во вложенной группе папку **Политики**.
2. Откройте контекстное меню, выберите в нем пункт **Вид** и установите флажок **Унаследованные политики**.

В результате унаследованные политики отобразятся в панели результатов со значком  . Вы можете просматривать свойства унаследованный политик. Редактирование унаследованных политик доступно только в той группе, в которой они были созданы.

3.1.1.4. Активация политики

Для того чтобы групповая политика стала действующей политикой для приложения,

1. Выберите в панели результатов нужную групповую политику, откройте контекстное меню и выберите команду **Свойства** или воспользуйтесь аналогичным пунктом в меню **Действие**.
2. В открывшемся окне настройки групповой политики для приложения **Свойства: <Имя политики>** перейдите на закладку **Общие** (см. рис. 37).
3. В поле **Состояние политики** в раскрывающемся списке выберите **Активная политика**.

Чтобы сделать политику неактивной, выберите вариант **Неактивная политика**.

4. Нажмите на кнопку **Применить** или **ОК**.

3.1.1.5. Активация политики по событию

Для того чтобы групповая политика активировалась автоматически при наступлении события,

1. Выберите в панели результатов нужную групповую политику, откройте контекстное меню и выберите команду **Свойства** или воспользуйтесь аналогичным пунктом в меню **Действие**.
2. В открывшемся окне настройки групповой политики для приложения **Свойства: <Имя политики>** выберите закладку **Общие** (см. рис. 37).
3. Установите флажок **Активировать политику по событию** и выберите из раскрывающегося списка нужное событие (например, **Вирусная атака**).

Чтобы отменить автоматическое активирование политики по событию, флажок следует снять.

4. Нажмите на кнопку **Применить** или **ОК**.

В случае активации политики по событию вернуться к предыдущей политике можно только вручную.

После активации политика вступает в силу в соответствии с параметром, выбранном в окне **Дополнительно** (см. рис. 39).

3.1.1.6. Политика для мобильного пользователя

Подобный тип политики доступен только для Антивируса Касперского для Windows Workstations версий 5.0 и 6.0, Антивируса Касперского 5.0 для Windows File Servers и Антивируса Касперского 6.0 для Windows Servers.

Для того чтобы настроить применение групповой политики в случае отключения компьютера от логической сети,

1. Выберите в панели результатов нужную групповую политику, откройте контекстное меню и выберите команду **Свойства** или воспользуйтесь аналогичным пунктом в меню **Действие**.
2. В открывшемся окне настройки групповой политики для приложения **Свойства: <Имя политики>** перейдите на закладку **Общие** (см. рис. 37).

3. В поле **Состояние политики** в раскрывающемся списке выберите **Политика для мобильного пользователя**
4. Нажмите на кнопку **Применить** или **ОК**.

После активации политика для мобильного пользователя вступает в силу в соответствии с параметром, выбранном в окне **Дополнительно** (см. рис. 39).

3.1.1.7. Удаление политики

Чтобы удалить политику,

выберите в папке **Политики** в панели результатов соответствующую политику и воспользуйтесь командой **Удалить** контекстного меню либо аналогичным пунктом в меню **Действие**.

3.1.1.8. Копирование политики

Чтобы скопировать политику,

1. Выберите в папке **Политики** в панели результатов соответствующую политику и воспользуйтесь командой **Копировать** контекстного меню либо аналогичным пунктом в меню **Действие**.
2. Перейдите в папку **Политики** нужной группы (или останьтесь в той же папке) и воспользуйтесь командой контекстного меню **Вставить** либо аналогичным пунктом в меню **Действие**.

В результате политика копируется с сохранением всех параметров и распространяется на компьютеры группы, в которую она была перенесена. Если вы копируете политику в ту же папку, к ее имени автоматически будет добавлено окончание **_1**.

Активная политика при копировании становится неактивной. В случае необходимости вы можете сделать ее активной (см. п. 3.1.1.4 на стр. 78).

3.1.1.9. Настройка параметров политики Агента администрирования

При создании политики для Агента администрирования в окне **Настройки** (см. рис. 48) вы можете определять следующие настройки:

- В группе **Журнал событий** определите размер журнала событий, указав предельный объем файла с информацией в поле **Максимальный размер журнала событий, МБ**.
- Если вы хотите, чтобы информация об объектах, помещенных на компьютере на карантин или в резервное хранилище, автоматически передавалась на Сервер администрирования, установите соответствующие флажки в группе полей **Хранилища**.
- В группе **Пароль для удаления Агента администрирования** нажмите на кнопку **Изменить** и укажите пароль. Его необходимо будет указать в задаче удаленной деинсталляции Агента администрирования.

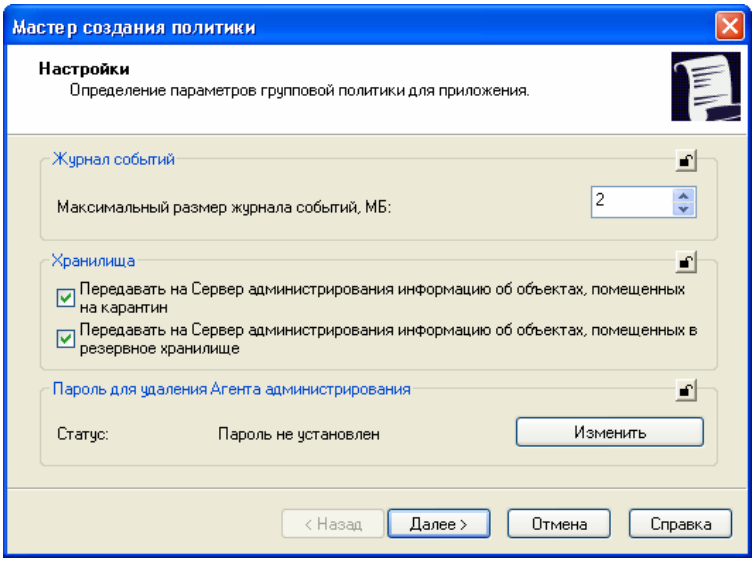

Рисунок 48. Создание политики для Агента администрирования
Окно **Настройки**

В окне **Сеть** (см. рис. 49) вы можете задать параметры подключения к Серверу администрирования:

- В поле **Подключение к Серверу администрирования** установите:
  - временной интервал в минутах, через который будет проводиться синхронизация данных клиентских компьютеров и Сервера администрирования в поле **Период синхронизации, мин**.
  - флажок **Использовать SSL-соединение**, если хотите, чтобы подключение осуществлялось через защищенный порт (с использованием SSL протокола).
  - флажок **Сжимать сетевой трафик** для увеличения скорости передачи данных Агентом администрирования, сокращения объема передаваемой информации и уменьшения нагрузки на Сервер администрирования.

    При включении данного параметра может возрасти нагрузка на центральный процессор клиентского компьютера.

- В поле **Порт Агента администрирования** разрешите подключение Сервера администрирования к клиентским компьютерам через UDP-порт и определите номер порта. Для открытия соединения через UDP-порт установите флажок **Использовать UDP-порт** и введите номер порта в поле **Номер UDP-порта**. По умолчанию это **15000** порт. В случае необходимости вы можете его изменить. Допускается использование только десятичной формы записи.

  Если клиентский компьютер работает под управлением операционной системы Microsoft Windows XP Service Pack 2, то встроенный межсетевой экран блокирует UDP-порт с номером 15000. Поэтому для доступа Сервера администрирования данный порт необходимо открыть вручную.

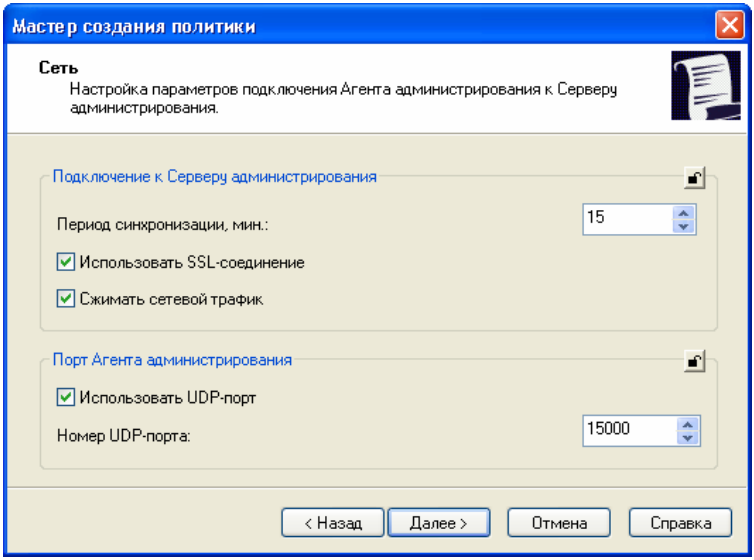

Рисунок 49. Создание политики для Агента администрирования
Окно **Сеть**

При редактировании политики для Агента администрирования вы можете вносить изменения на закладках **Настройки** (см. рис. 50) и **Сеть** (см. рис. 51).

Помимо настроек, задаваемых в мастере создания политики, на закладке **Сеть** (см. рис. 51) можно также:

- Установить флажок **Разрешить службу имен NetBIOS в Анти-Хакере Антивируса Касперского 6.0**. В этом случае в Анти-Хакере Антивируса Касперского версии 6.0 будет открыт UDP-порт 137, используемый для получения IP-адреса Сервера администрирования.
- Установить флажок **Открывать порты Агента администрирования в брандмауэре Microsoft Windows**. В результате в список исключений сетевого экрана Microsoft Windows будет добавлен UDP-порт, необходимый для работы Агента администрирования.

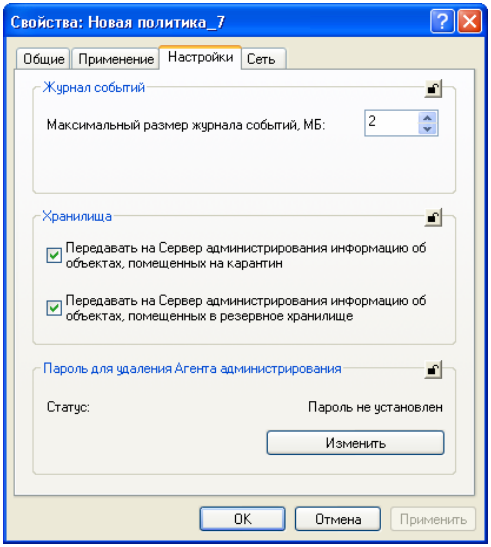

Рисунок 50. Редактирование политики для Агента администрирования
Закладка **Настройки**

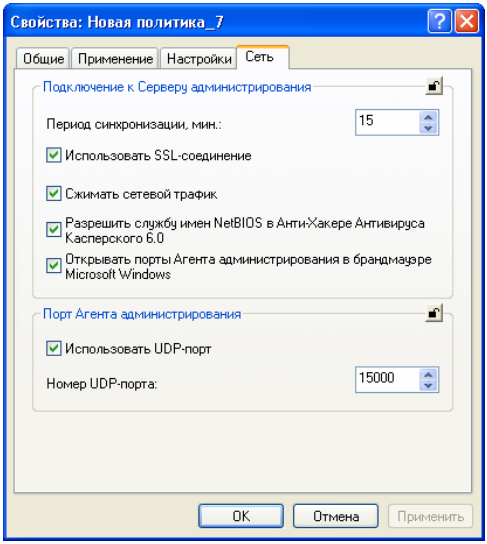

Рисунок 51. Редактирование политики для Агента администрирования
Закладка **Сеть**

3.1.1.10. Настройка параметров политики Сервера администрирования

При создании политики для Сервера администрирования в окне выбора приложения укажите **Kaspersky Administration Kit**. Далее в окне **Настройки** (см. рис. 52) вы можете определить следующее:

- В поле **Параметры подключения к Серверу администрирования**:
  - номер порта, по которому осуществляется 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.
- В поле **Максимальное количество событий, хранящихся в базе данных** укажите необходимое значение. По умолчанию оно составляет 400 000 записей.

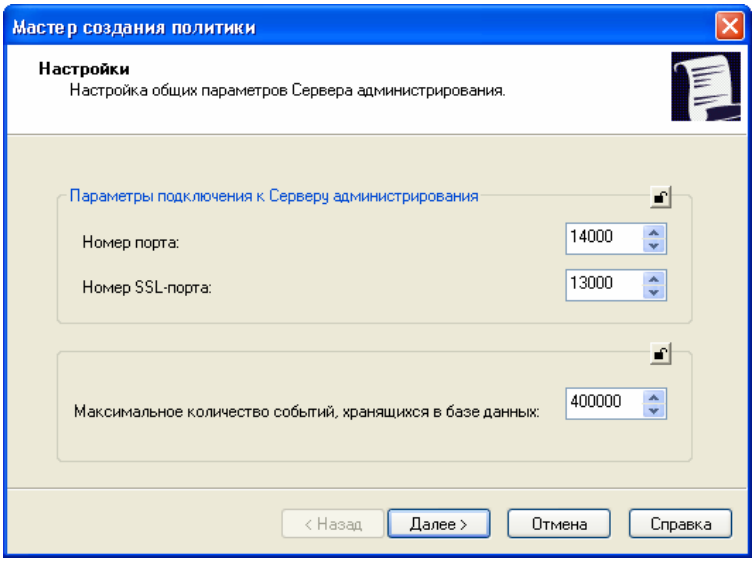

Рисунок 52. Создание политики для Сервера администрирования
Окно **Настройки**

В окне **Опрос сети** (см. рис. 53) вы можете задать параметры обновления Сервером администрирования информации о структуре сети:

- Чтобы включить автоматический опрос сети, в группе **Windows-сеть** установите флажок **Разрешить опрос**.
- Чтобы включить автоматический опрос IP-подсетей, в группе **IP-подсети** установите флажок **Разрешить опрос**. Сервер администрирования опрашивает подсети с периодичностью, указанной в поле **Период опроса, мин**. По умолчанию период опроса составляет 420 минут.
- Чтобы включить автоматический опрос сети в соответствии со структурой Active Directory, в группе **Active Directory** установите флажок **Разрешить опрос**.

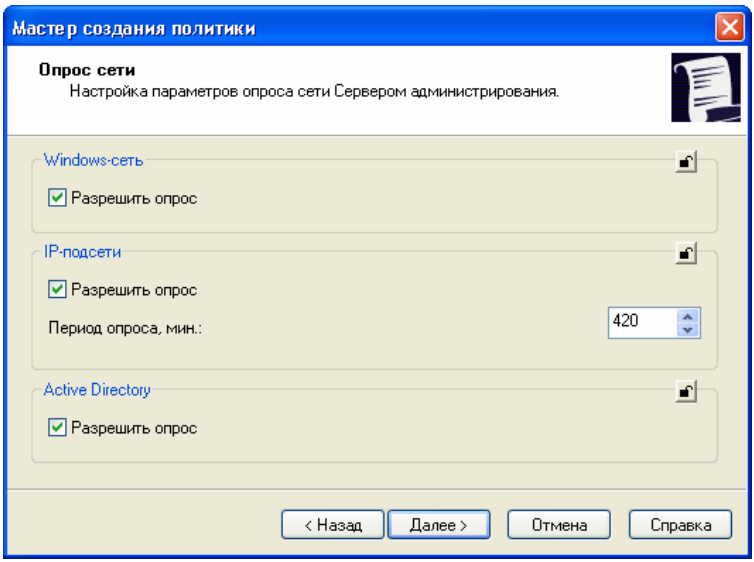

Рисунок 53. Создание политики для Сервера администрирования
Окно **Опрос сети**

Помимо настроек, заданных на этапе создания политики, вы можете изменять дополнительные параметры политики.

На закладке **Настройки** (см. рис. 54) в поле **Тайм-аут видимости компьютера, мин.** вы можете задать время, в течение которого клиентский компьютер считается видимым в сети после потери соединения с Сервером администрирования. По умолчанию интервал составляет 60 минут. По истечении заданного интервала Сервер администрирования будет считать клиентский компьютер неактивным.

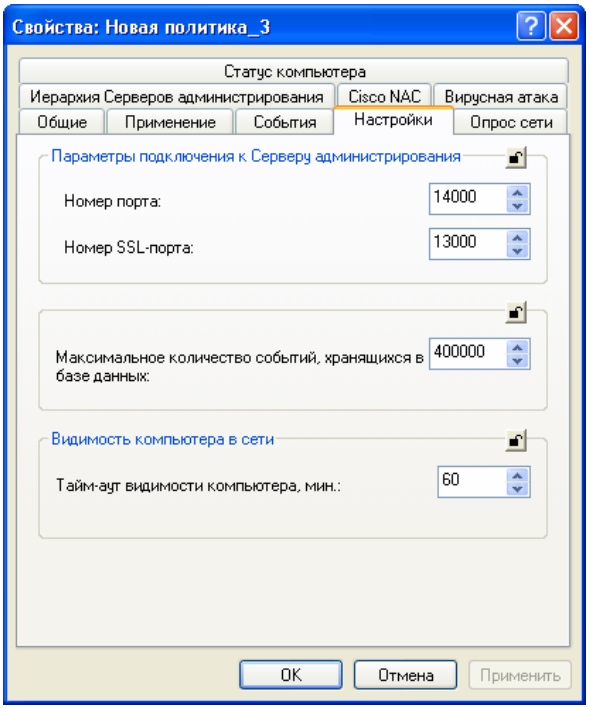

Рисунок 54. Редактирование политики для Сервера администрирования
Закладка **Настройки**

На закладке **Опрос сети** (см. рис. 55) вы можете задать:

- периоды опроса Windows-сети:
  - **Период быстрого опроса, мин**. С указанной периодичностью будет обновляться информация о списке компьютеров, подключенных к сети. По умолчанию период опроса составляет 15 минут.
  - **Период полного опроса, мин**. Через указанный промежуток времени будет полностью обновляться информация о компьютерах сети. По умолчанию период опроса составляет 60 минут.
- период опроса сети в соответствии со структурой Active Directory. Для этого в соответствующем блоке в поле **Период опроса, мин.** укажите необходимое значение. По умолчанию период опроса составляет 60 минут.

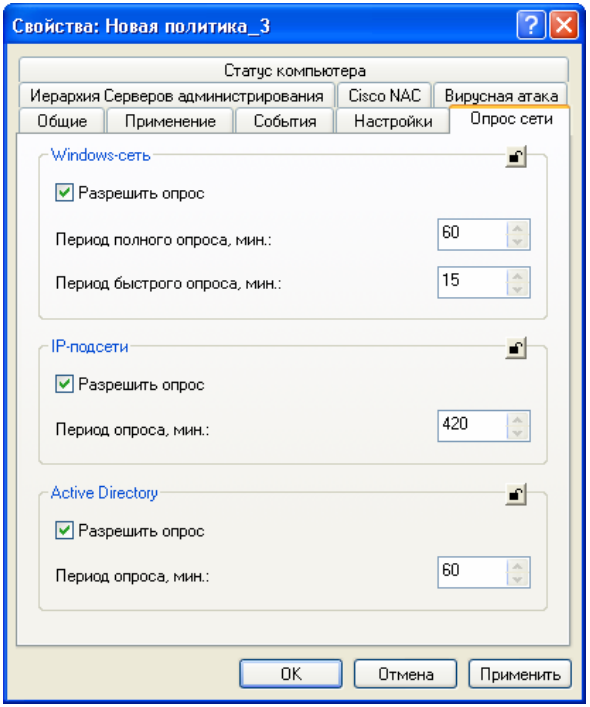

Рисунок 55. Редактирование политики для Сервера администрирования
Закладка **Опрос сети**

На закладке **Вирусная атака** вы можете настроить параметры генерации события **Вирусная атака** для каждого типа антивирусных приложений. Настройки этой закладки идентичны настройкам одноименной закладки в свойствах Сервера администрирования (см. рис. 70).

На закладке **Cisco NAC** вы можете задать соответствие условий антивирусной защиты статусам Cisco NAC. Настройки этой закладки идентичны настройкам одноименной закладки в свойствах Сервера администрирования (см. рис. 72).

На закладке **Иерархия Серверов администрирования** (см. рис. 56) вы можете разрешить или запретить редактирование параметров иерархии Серверов (см. рис. 64). Если флажок **Разрешить изменение настроек иерархии на подчиненных Серверах администрирования** снят, то администраторы подчиненных Серверов администрирования не смогут изменять назначенные главным Сервером параметры иерархии.

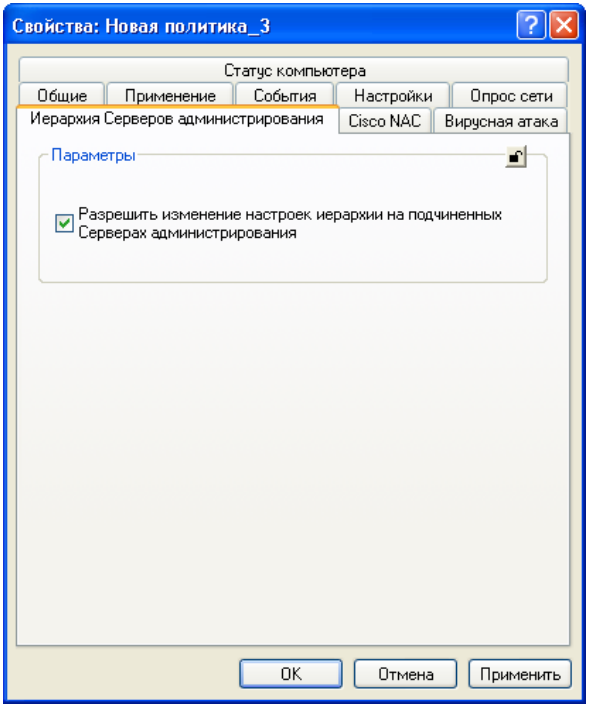

Рисунок 56. Редактирование политики для Сервера администрирования
Закладка **Иерархия Серверов администрирования**

3.1.1.11. Экспорт политики

Для того чтобы экспортировать политику,

в дереве консоли выберите необходимую группу, выберите входящую в ее состав папку **Политики**. После этого в панели результатов будет представлен список всех сформированных для данной группы политик. Выберите необходимую политику, откройте контекстное меню и выберите команду **Экспортировать** или воспользуйтесь аналогичным пунктом в меню **Действие**.

В открывшемся окне укажите имя файла и каталог, в который вы хотите сохранить политику. Нажмите на кнопку **Сохранить**.

3.1.1.12. Импорт политики

Для того чтобы импортировать политику,

в дереве консоли выберите необходимую группу. Откройте контекстное меню папки **Политики** и выберите команду **Все задачи / Импортировать** или воспользуйтесь аналогичным пунктом в меню **Действие**.

В открывшемся окне укажите путь к файлу, из которого вы хотите импортировать политику. Нажмите на кнопку **Открыть**.

3.1.2. Локальные настройки приложения

3.1.2.1. Просмотр настроек приложения

Для того чтобы ознакомиться с настройками приложения и/или внести необходимые изменения:

1. В папке **Группы** выберите папку с названием группы, в состав которой входит клиентский компьютер. В панели результатов выберите компьютер, для которого вам необходимо изменить настройки приложения, и воспользуйтесь командой **Свойства** контекстного меню или аналогичным пунктом в меню **Действие**.

2. В результате в главном окне программы открывается диалоговое окно **Свойства: <Имя компьютера>**, состоящее из нескольких закладок. Выберите закладку **Приложения** (см. рис. 57). На ней в виде таблицы представлен полный список приложений «Лаборатории Касперского», установленных на клиентском компьютере, и отображается краткая информация о каждом из них.

   Выберите нужное вам приложение. Вы можете:

   - просматривать список событий в работе приложения, произошедших на клиентском компьютере и зарегистрированных на Сервере администрирования, при помощи кнопки **События** (подробнее см. п. 5.3 на стр. 163).

   - просматривать текущую статистическую информацию о работе приложения при помощи кнопки **Статистика**. Данная информация запрашивается Сервером администрирования с клиентского компьютера, в случае отсутствия соединения выводится соответствующее сообщение.

- получать общую информацию о приложении и проводить его настройку при помощи кнопки **Свойства** в окне **Настройки приложения «<Название приложения>»** (см. рис. 58).

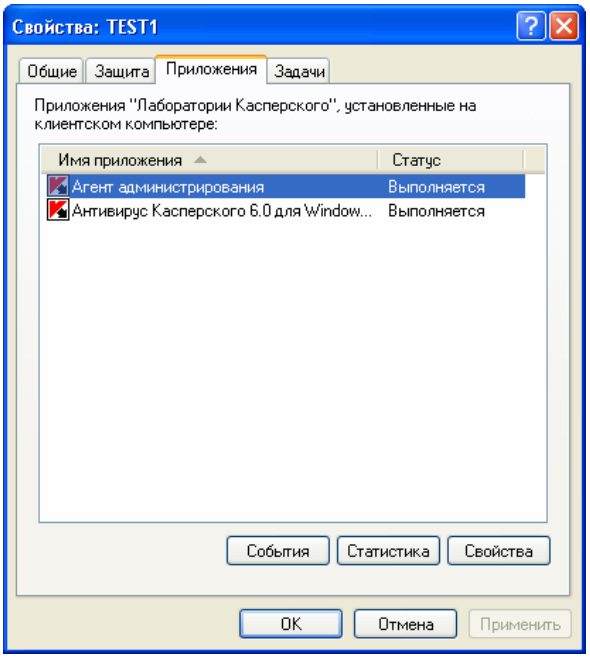

Рисунок 57. Окно просмотра свойств клиентского компьютера. Закладка **Приложения**

Окно **Параметры приложения «<Название приложения>»** состоит из нескольких закладок. Информация предоставляется на основании данных, полученных в ходе последней синхронизации клиентского компьютера с Сервером администрирования. Состав закладок для каждого приложения компании индивидуален, подробное описание приводится в соответствующих Руководствах. Закладки **Общие, Лицензии** и **События** входят в состав окна настройки для всех приложений.

На закладке **Общие** (см. рис. 58) вы можете просматривать общую информацию о приложении, запускать или останавливать его работу, а также знакомиться со свойствами установленного на рабочем месте администратора плагина управления приложением с помощью гиперссылки **Информация о плагине** (см. рис. 62).

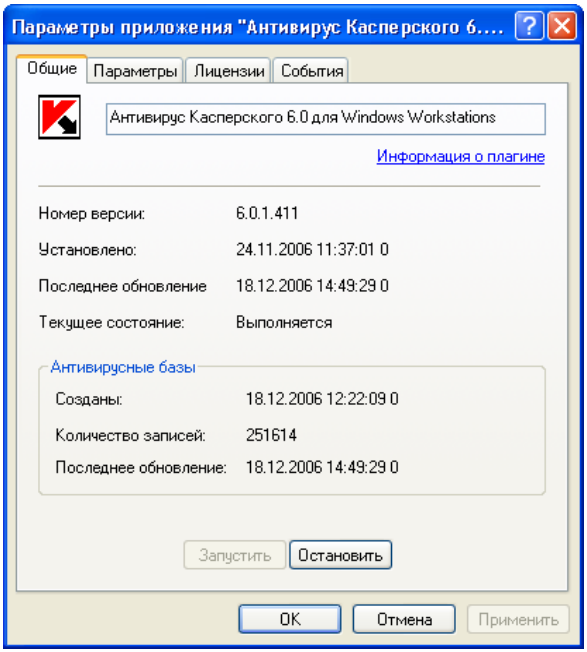

Рисунок 58. Окно настройки свойств приложения. Закладка **Общие**

На закладке **Лицензии** вы можете получать подробную информацию об установленных для приложения текущем и резервном лицензионных ключах (см. рис. 59).

В группе полей **Текущий лицензионный ключ** отображаются данные о текущем лицензионном ключе:

- **Номер** – серийный номер лицензионного ключа.
- **Тип** – тип установленного лицензионного ключа, например, **коммерческий**, **пробный**.
- **Дата активизации** – дата активизации ключа (дата, когда ключ стал текущим).
- **Дата окончания** – дата окончания срока действия лицензии.
- **Срок действия** – срок действия лицензионного ключа.
- **Ограничение** – лицензионные ограничения, заданные в ключе.

В группе полей **Резервный лицензионный ключ** отображаются данные о резервном лицензионном ключе:

- **Номер** – серийный номер лицензионного ключа.
- **Тип** – тип лицензионного ключа, например, **коммерческий**, **пробный**.
- **Срок действия** – срок действия лицензионного ключа.
- **Ограничение** – лицензионные ограничения, заданные в ключе.

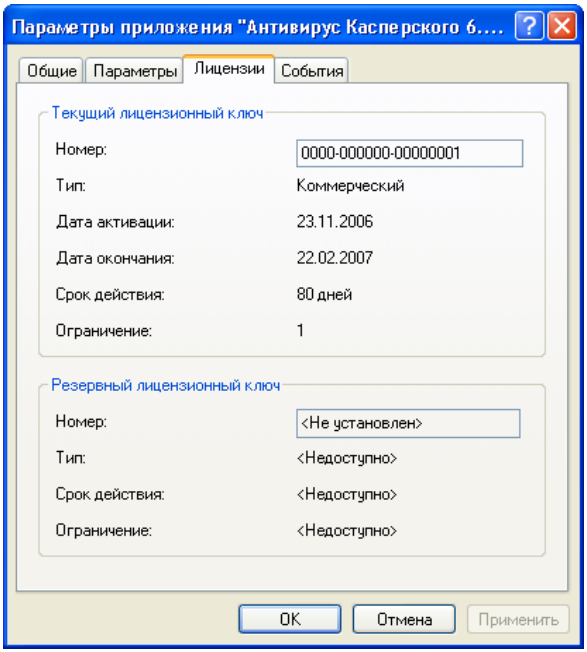

Рисунок 59. Окно настройки свойств приложения. Закладка **Лицензии**

На закладке **События** (см. рис. 60) представлены параметры, определяющие правила обработки событий в работе приложения на клиентском компьютере. Вы можете просматривать их и вносить необходимые изменения. Эта закладка полностью аналогична одноименной закладке окна настройки групповой политики для приложения (подробнее см. п. 3.1.1.2 на стр. 66).

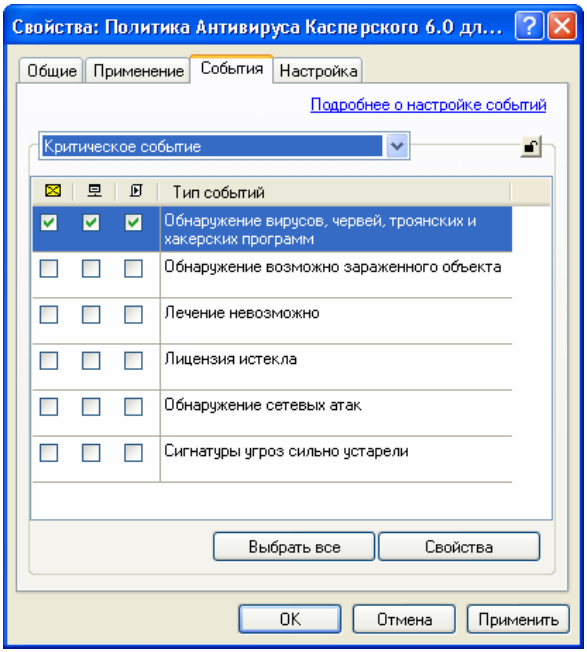

Рисунок 60. Настройка приложения.
Закладка **События**

3. Чтобы сохранить внесенные изменения нажмите на кнопку **Применить** или **ОК**.

3.1.2.2. Настройка параметров Сервера администрирования

Для просмотра настроек Сервера администрирования:

выберите в дереве консоли узел, соответствующий нужному Серверу администрирования, откройте контекстное меню и воспользуйтесь командой **Свойства** или аналогичным пунктом в меню **Действие**. В результате открывается диалоговое окно **Свойства: <Имя Сервера администрирования>**, в состав которого входят закладки **Общие**, **Настройки**, **События**, **Уведомление**, **Вирусная атака**, **Безопасность**, **Опрос сети**, **Cisco NAC**.

На закладке **Общие** (см. рис. 61) отображается следующая информация:

- название компонента Сервер администрирования и имя компьютера в Windows-сети, на который установлен компонент;
- номер установленной версии;
- путь к папке общего доступа, предназначенной для хранения файлов для удаленной установки приложений и размещения обновлений, копируемых с источника обновлений на Сервер администрирования.

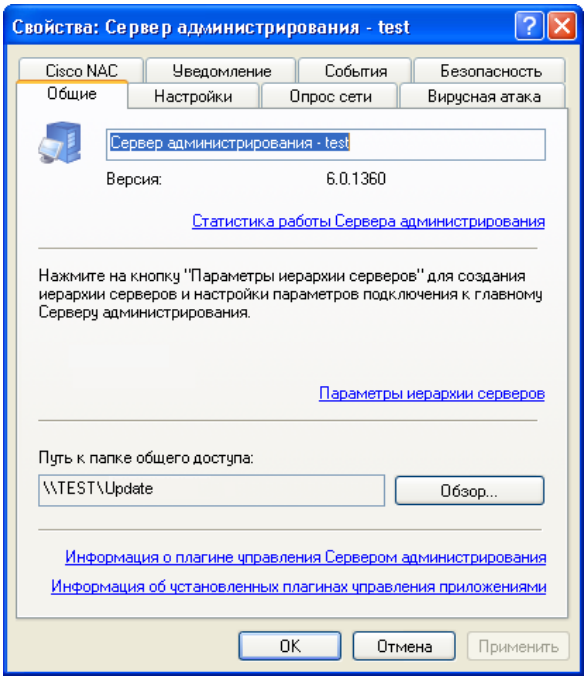

Рисунок 61. Просмотр свойств Сервера администрирования. Закладка **Общие**

Вы можете изменить путь к папке общего доступа при помощи кнопки **Обзор**.

Ссылка **Статистика работы Сервера администрирования** предназначена для вызова окна просмотра общей статистической информации Сервера администрирования.

С помощью ссылки **Информация о плагине управления Сервером администрирования** вызывается окно просмотра его свойств (см. рис. 62). Приводится следующая информация:

- имя и полный путь к файлу плагина управления,
- номер версии файла;
- сведения о правообладателе (**Kaspersky Lab**) и авторских правах;
- дата и время создания файла плагина управления.

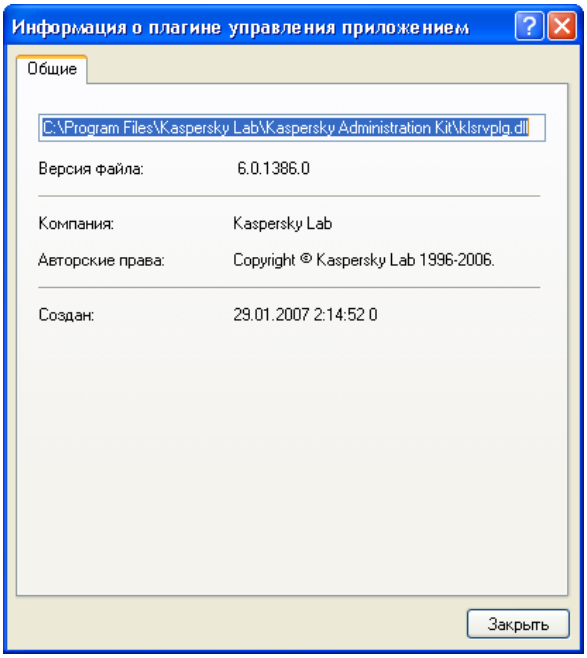

Рисунок 62. Окно просмотра свойств плагина управления приложением Сервер администрирования

С помощью ссылки **Информация об установленных плагинах управления приложениями** можно открыть окно со списком установленных на Сервере администрирования плагинов (см. рис. 63). Для каждого из них указаны название приложения и версия плагина. В этом окне, нажав на кнопку **Информация**, можно просмотреть подробную информацию о выбранном плагине управления приложением (см. рис. 62).

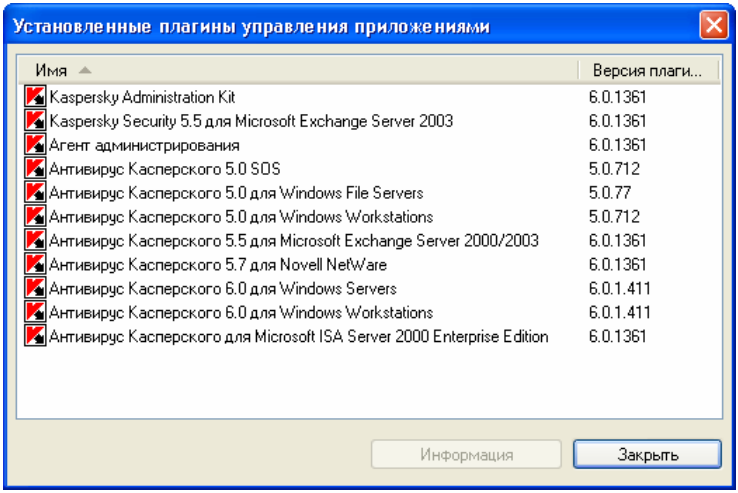

Рисунок 63. Список установленных на Сервере администрирования плагинов управления приложениями

Закладка также содержит ссылку **Параметры иерархии серверов** для вызова окна настройки параметров подчиненного Сервера администрирования (см. рис. 64). В окне можно произвести следующие настройки:

- указать, является ли Сервер администрирования подчиненным;
- задать адрес главного Сервера администрирования;
- указать или изменить путь к файлу сертификата главного Сервера администрирования;
- при необходимости задать параметры прокси-сервера для подключения к главному Серверу администрирования.

Эти параметры недоступны для редактирования, если в действующей политике Сервера администрирования снят флажок **Разрешить изменение настроек иерархии на подчиненных Серверах администрирования** (см. рис. 56).

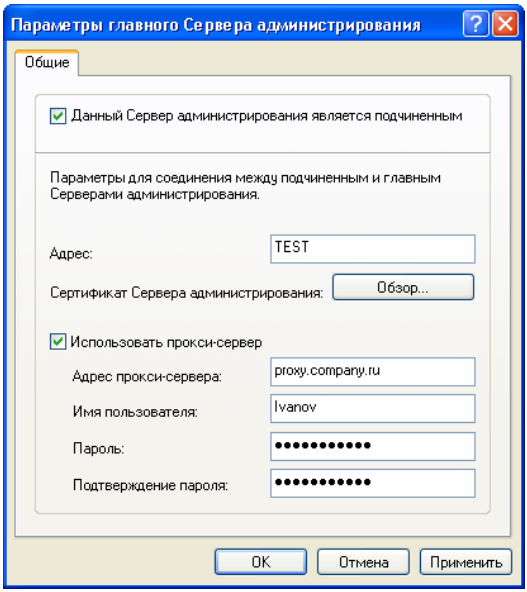

Рисунок 64. Окно настройки параметров подчиненного Сервера администрирования

На закладке **Настройки** (см. рис. 65) представлены настройки Сервера администрирования. Группа **Параметры подключения к Серверу администрирования** содержит:

- номер порта, по которому осуществляется 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.
- номер порта, по которому будет осуществляться подключение мобильных устройств[3] к Серверу администрирования. По умолчанию используется порт **13292**. Чтобы включить использование этого порта на Сервере администрирования, установите флажок **Открывать порт для мобильных устройств**.

[3] Под мобильным устройством подразумевается устройство с установленным приложением Антивирус Касперского 6.0 Mobile Enterprise Edition.

Вы также можете указать в соответствующем поле максимальное число событий, хранящихся в базе данных на Сервере администрирования.

В группе **Видимость компьютера в сети** в поле **Тайм-аут видимости компьютера, мин.** задается время, в течение которого клиентский компьютер считается видимым в сети после потери соединения с Сервером администрирования. По умолчанию интервал составляет 120 минут. По истечении заданного интервала Сервер администрирования будет считать клиентский компьютер неактивным. Если это необходимо, вы можете изменить значение данного параметра.

В случае необходимости вы можете изменить значения данных параметров.

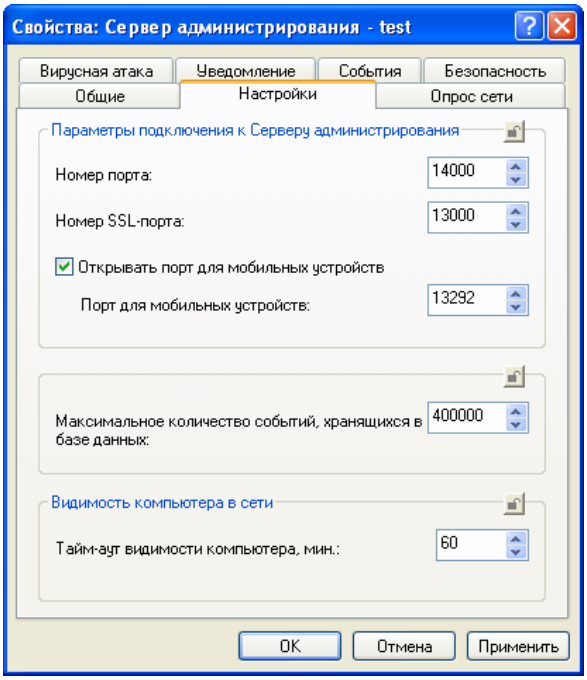

Рисунок 65. Просмотр свойств Сервера администрирования. Закладка **Настройки**

На закладке **События** (см. рис. 66) представлены параметры, определяющие правила обработки событий в работе Сервера администрирования. Данная закладка полностью аналогична одноименной закладке окна настройки свойств групповой политики (подробнее см. п. 3.1.1.2 на стр. 66).

Опишем подробнее события Сервера администрирования. Для Сервера администрирования, как и для других приложений «Лаборатории Касперского», управляемых при помощи Kaspersky Administration Kit, существуют четыре уровня важности событий: **Критическое событие**, **Отказ функционирования**, **Предупреждение**, **Информационное сообщение**.

Распределение типов событий в соответствии с уровнем их важности выглядит следующим образом:

- **Критическое событие**:
  - Превышено лицензионное ограничение для данного лицензионного ключа (например, количество клиентских компьютеров, на которые установлен лицензионный ключ, превышает заложенное в нем ограничение по компьютерам).
  - Вирусная атака (в логической сети превышен заданный порог вирусной активности).

    Реакция Сервера администрирования на событие **Вирусная атака** является крайне важной, особенно в период вирусных эпидемий и увеличения угрозы возникновения вирусных атак.
  - Потеряно соединение с клиентским компьютером (не удается установить соединение с Агентом администрирования на клиентском компьютере).
  - Статус компьютера «Критический» (при опросе сети найден компьютер с настройками, соответствующими статусу **Критический**).
- **Отказ функционирования**:
  - Нет свободного места на диске (отсутствует свободное место на диске, используемом для работы и хранения информации Сервера администрирования).
  - Недоступна папка общего доступа (недоступна папка, в которой хранятся обновления антивирусных баз и модулей приложений).
  - Недоступна информационная база Сервера администрирования.
  - Нет свободного места в информационной базе Сервера администрирования.

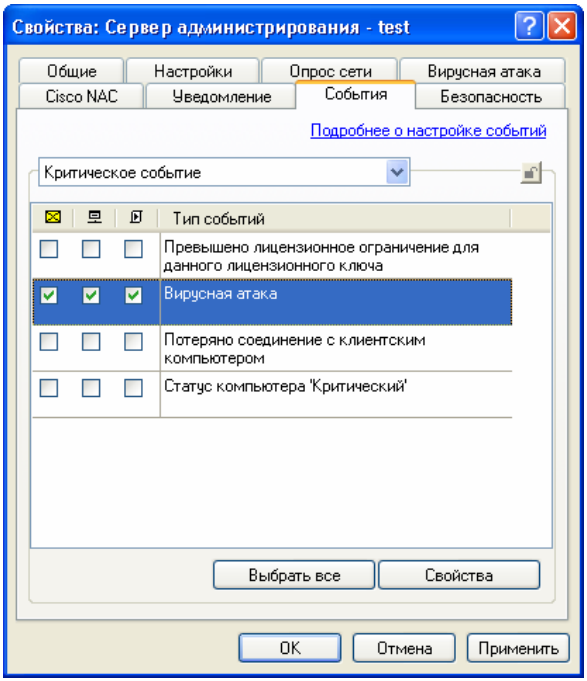

Рисунок 66. Просмотр свойств Сервера администрирования. Закладка **События**

- **Предупреждение**:
  - Превышено лицензионное ограничение для данного лицензионного ключа.
  - Клиентский компьютер слишком долго не проявляет активности в сети.
  - Конфликт имен клиентских компьютеров (не соблюдено правило уникальности имени клиентского компьютера в пределах одного уровня иерархии).
  - Осталось мало свободного места на дисках.
  - Мало свободного места в информационной базе Сервера администрирования.
  - Разорвано соединение с главным Сервером администрирования.

- Разорвано соединение с подчиненным Сервером администрирования.
- Статус компьютера «Предупреждение» (при опросе сети найден компьютер с настройками, соответствующими статусу **Предупреждение**).

- **Информационное сообщение**.
  - Лицензионное ограничение для данного лицензионного ключа использовано более чем на 90%.
  - Найден новый клиентский компьютер (при опросе сети найден новый клиентский компьютер).
  - Клиентский компьютер был автоматически добавлен в группу (новый клиентский компьютер был добавлен в группу в соответствии с параметрами группы **Сеть**).
  - Клиентский компьютер был удален из группы, поскольку слишком долго не проявлял активности в сети.
  - Установлено соединение с подчиненным Сервером администрирования.
  - Установлено соединение с главным Сервером администрирования.
  - Аудит: Подключение к Серверу администрирования.
  - Аудит: Изменение объекта.
  - Аудит: Изменение статуса объекта.
  - Аудит: Изменение параметров группы.

На закладке **Уведомление** (см. рис. 67) производится настройка параметров оповещения администратора и/или других пользователей о событиях, которые поступают на Сервер администрирования от управляемых приложений. Задайте:

- параметры отправки оповещений по электронной почте:
  - в поле **Адрес получателя** введите электронный адрес получателя уведомлений, допускается ввод нескольких адресов разделенных запятой или точкой с запятой;
  - в поле **Адрес SMTP-сервера** укажите адрес почтового сервера. В качестве адреса можно использовать IP-адрес или имя компьютера в сети Windows;
  - в поле **Номер порта SMTP-сервера** введите номер коммуникационного порта SMTP-сервера. По умолчанию используется порт 25.

- в поле **Компьютеры для уведомления средствами NET SEND** укажите адреса компьютеров-получателей уведомлений по сети. В качестве адреса также можно использовать IP-адрес или имя компьютера в Windows-сети. Допускается ввод нескольких адресов разделенных запятой или точкой с запятой.

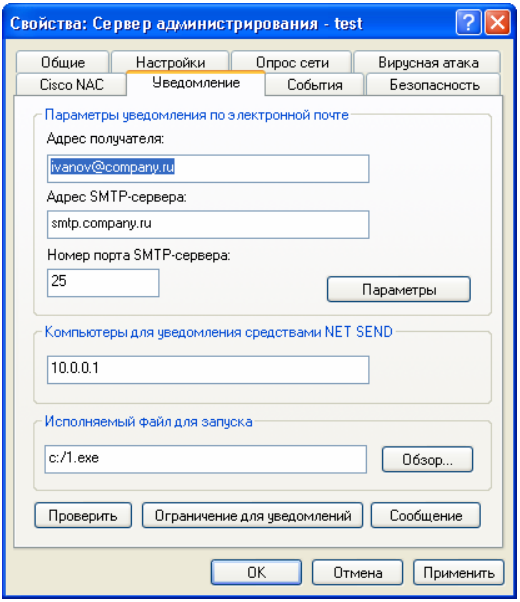

Рисунок 67. Просмотр свойств Сервера администрирования. Закладка **Уведомление**

- в группе **Исполняемый файл для запуска** с помощью кнопки **Обзор** укажите исполняемый модуль для запуска при наступлении события.

> Имена переменных окружения исполняемого модуля совпадают с именами подстановочных параметров, используемых для формирования текста сообщения (см. ниже).

- текст сообщения, которое будет доставляться в качестве уведомления. Для этого нажмите на кнопку **Сообщение** и в открывшемся окне (см. рис.68) сформируйте шаблон.

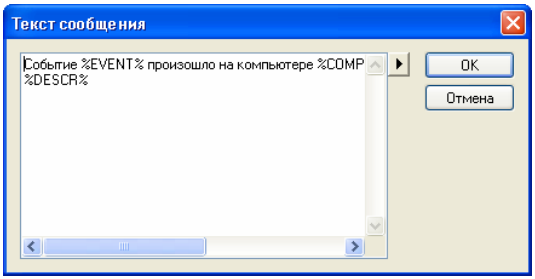

Рисунок 68. Формирование параметров рассылки уведомлений. Ввод текста сообщения

В состав сообщения может включаться информация о зарегистрированном событии. Для этого следует вставить в шаблон соответствующие подстановочные параметры, выбрав необходимые из раскрывающегося с помощью кнопки  списка (подробнее о подстановочных параметрах см. п. 3.1.1.2 на стр. 66).

- отправителя и тему сообщения, которое будет доставляться в качестве уведомления. Для этого нажмите на кнопку **Параметры** и в открывшемся окне (см. рис. 43) укажите необходимые параметры (подробнее см. п. 3.1.1.2 на стр. 66).

Для уменьшения нагрузки на Сервер вы можете ввести ограничение на количество оповещений, осуществляемых Сервером администрирования. Для этого нажмите на кнопку **Ограничение для уведомлений**, в открывшемся окне (см. рис. 69) установите флажок **Ограничить количество уведомлений** и определите критерии ограничения:

- максимальное количество оповещений, которое может сделать Сервер администрирования;
- допустимый временной интервал в минутах, в течение которого эти оповещения могут быть произведены.

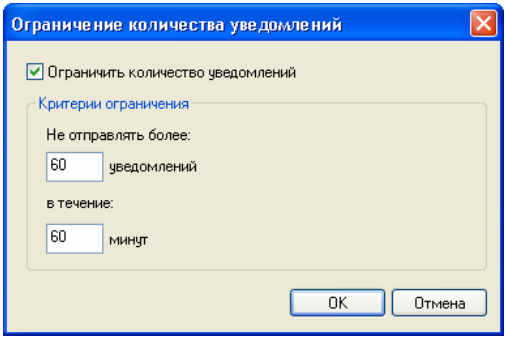

Рисунок 69. Ограничение количества оповещений

Данные настройки используются в политиках для приложений в качестве значений по умолчанию.

Чтобы проверить корректность установленных на этой закладке параметров, вы можете вручную отправить тестовое сообщение. Для этого нажмите на кнопку **Проверить**. В результате откроется окно отправки тестового уведомления (см. рис. 46). При возникновении каких-либо ошибок отобразится подробная информация о них.

На закладке **Вирусная атака** (см. рис. 70) вы можете определить число обнаруженных вирусов в течение ограниченного временного интервала, превышение которого будет считаться возникновением события **Вирусная атака**. Данная характеристика имеет очень большое значение в периоды вирусных эпидемий и позволяет администратору своевременно реагировать на возникающие угрозы вирусных атак.

Установите флажки рядом с нужными типами приложений:

- **Антивирусы для рабочих станций и файловых серверов**;
- **Антивирусы защиты периметра**;
- **Антивирусы для почтовых систем**.

Для каждого типа приложений задайте порог вирусной активности, превышение которого будет считаться возникновением события **Вирусная атака**:

- в поле **Вирусов** – количество обнаруженных приложениями этого типа в логической сети вирусов;
- в поле **В течение (мин.)** – временной интервал, в течение которого было обнаружено указанное выше количество вирусов.

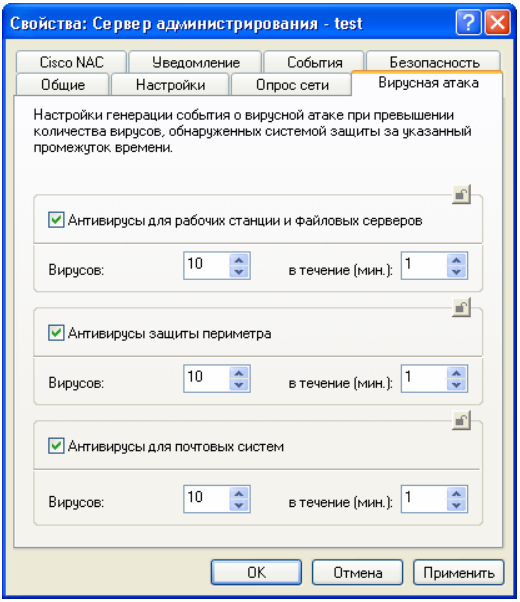

Рисунок 70. Просмотр свойств Сервера администрирования.
Закладка **Вирусная атака**

На закладке **Безопасность** (см. рис. 4) настраиваются права доступа к логической сети Сервера администрирования (см. п. 2.2.1 на стр. 17).

На закладке **Опрос сети** (см. рис. 71) представлены параметры опроса Сервером администрирования компьютерной сети.

В группе полей **Windows-сеть** задаются общие параметры опроса сети. Чтобы включить автоматический опрос сети, установите флажок **Разрешить опрос**. В полях ниже задайте:

- **Период быстрого опроса, мин**. С указанной периодичностью будет обновляться информация о списке NetBIOS-имен компьютеров всех доменов и рабочих групп сети. По умолчанию период опроса составляет 15 минут.
- **Период полного опроса, мин**. Через указанный промежуток времени будет полностью обновляться информация о компьютерах сети (операционная система, IP-адрес, DNS-имя и т. п.). По умолчанию период опроса составляет 60 минут.

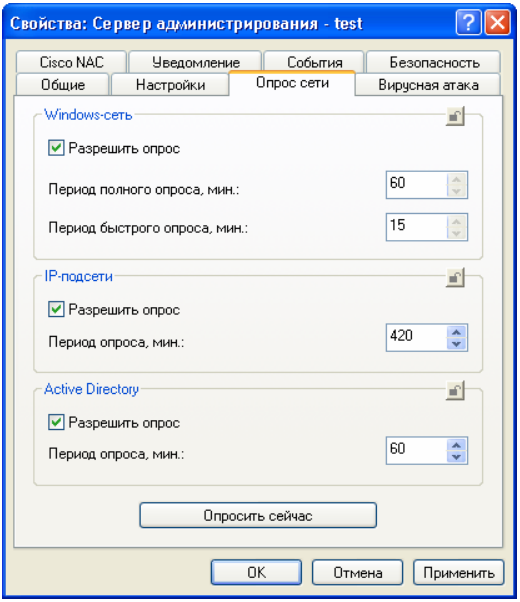

Рисунок 71. Просмотр свойств Сервера администрирования.
Закладка **Опрос сети**

Группа полей **IP-подсети** содержит параметры, определяющие опрос IP-подсетей. Если флажок **Разрешить опрос** установлен, Сервер администрирования опрашивает сформированные IP-диапазоны с помощью ICMP-пакетов и собирает полную информацию о компьютерах, входящих в диапазон. Опрос производится с периодичностью, указанной в поле **Период опроса, мин**. По умолчанию период опроса составляет 420 минут. Вы можете изменить интервал, установив другое значение, или отменить опрос, сняв флажок **Разрешить опрос**.

Группа полей **Active Directory** содержит параметры, определяющие опрос сети в соответствии со структурой организационных единиц Active Directory. При этом в базу данных Сервера администрирования записывается информация о структуре организационных единиц Active Directory, а также информация о DNS-именах компьютеров. Если флажок **Разрешить опрос** установлен, Сервер администрирования опрашивает сеть с периодичностью, указанной в поле **Период опроса, мин**. По умолчанию период опроса составляет 60 минут. Вы можете изменить интервал, установив другое значение, или отменить опрос, сняв флажок **Разрешить опрос**.

Нажмите на кнопку **Опросить сейчас**, чтобы вручную запустить полный опрос компьютерной сети.

На закладке **Cisco NAC** (см. рис. 72) содержатся параметры совместной работы Kaspersky Administration Kit и Cisco Network Admission Control (NAC). Здесь задается соответствие условий антивирусной защиты клиентского компьютера статусам Cisco NAC.

При работе с Cisco NAC Сервер администрирования играет роль стандартного компонента Posture Validation Server (PVS), который администратор может использовать для разрешения или запрета доступа компьютера в сеть (в зависимости от состояния антивирусной защиты).

В верхнем поле выбирается один из статусов компьютера Cisco NAC: **Healthy**, **Checkup**, **Quarantine** или **Infected**. В таблице ниже для каждого из этих статусов с помощью флажков задаются соответствующие им условия антивирусной защиты. Для некоторых условий можно изменять пороговые значения. Для этого выберите необходимое условие в столбце **Условие** и с помощью кнопки **Изменить** откройте окно редактирования (см. рис. 73). В этом окне в поле **Значение** задайте нужные параметры.

В поле **Номер PVS-порта** укажите номер порта Postrure Validation Server, через который идет обмен данными с сервером Cisco. По умолчанию используется порт 18000.

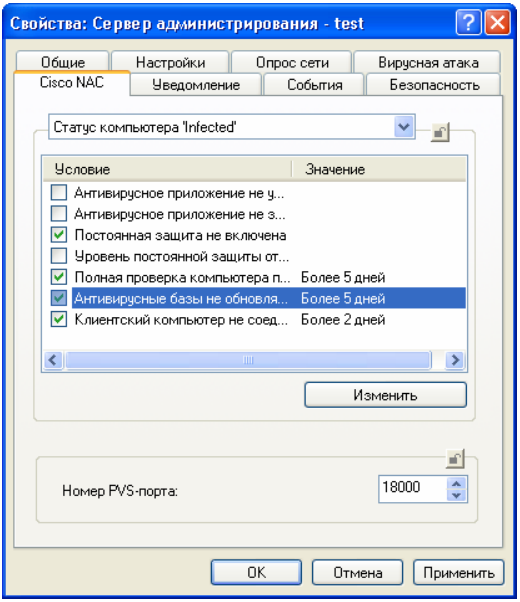

Рисунок 72. Просмотр свойств Сервера администрирования. Закладка **Cisco NAC**

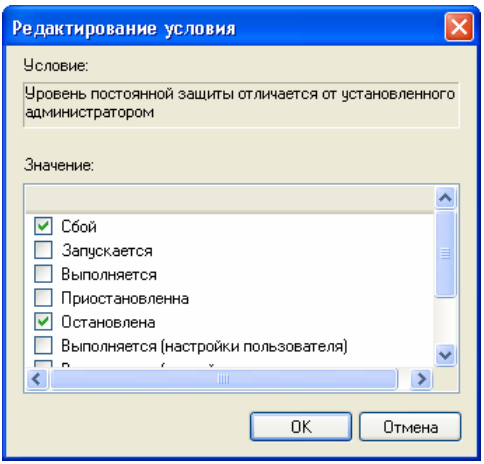

Рисунок 73. Редактирование условия выбора состояния антивирусной защиты компьютера

3.1.2.3. Настройка параметров Агента администрирования

Для просмотра настроек Агента администрирования, установленного на клиентском компьютере:

1. Выберите в панели результатов клиентский компьютер, откройте контекстное меню и выберите команду **Свойства** или воспользуйтесь аналогичной командой в меню **Действие**.
2. В открывшемся диалоговом окне перейдите на закладку **Приложения**.
3. В списке приложений, установленных на клиентском компьютере выберите **Агент администрирования** и нажмите на кнопку **Свойства**.

При работе с настройками Агента администрирования окно настройки помимо закладок **Общие** и **События** содержит закладки **Настройки** (см. рис. 74) и **Сеть** (см. рис. 75). Набор параметров, представленный на этих закладках, совпадает с параметрами, представленными на закладках **Настройки** и **Сеть** окна настройки политики для Агента администрирования (см. п. 3.1.1.9 на стр. 81).

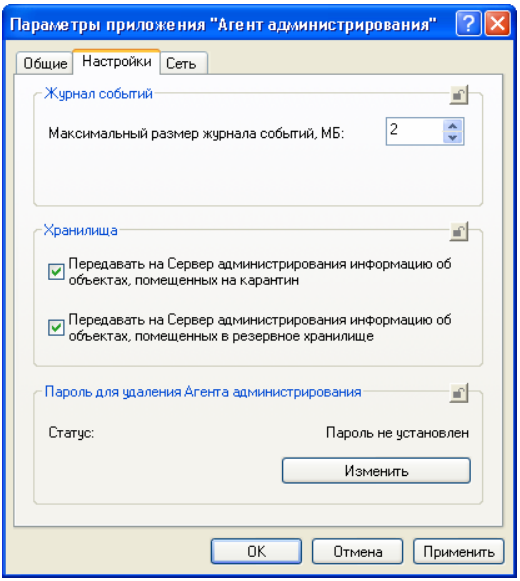

Рисунок 74. Окно настройки Агента администрирования. Закладка **Настройки**

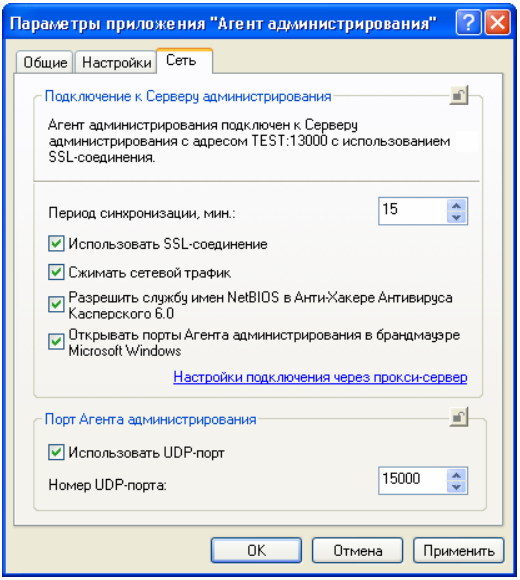

Рисунок 75. Окно настройки Агента администрирования.
Закладка **Сеть**

Для Агента администрирования, установленного на компьютере Сервера, доступна только закладка **Настройка** (см. рис. 74). Настраивать параметры подключения Агента к Серверу администрирования не требуется, они реализованы программно с учетом того, что компоненты установлены на одном компьютере.

3.2. Управление работой приложений

3.2.1. Создание групповой задачи

Для того чтобы создать новую групповую задачу,

1. В дереве консоли выберите группу, для которой вы будете создавать задачу, выберите входящую в ее состав папку **Групповые задачи**, откройте контекстное меню и выберите команду **Создать / Задачу** или воспользуйтесь аналогичным пунктом в меню **Действие**. В результате запускается мастер. Следуйте его указаниям.
2. Определите имя задачи. Если вы зададите имя уже существующей в данной группе задачи, к нему автоматически будет добавлено окончание **_1**.

3. После этого выберите приложение, для которого создается задача, и определите ее тип (см. рис. 76).

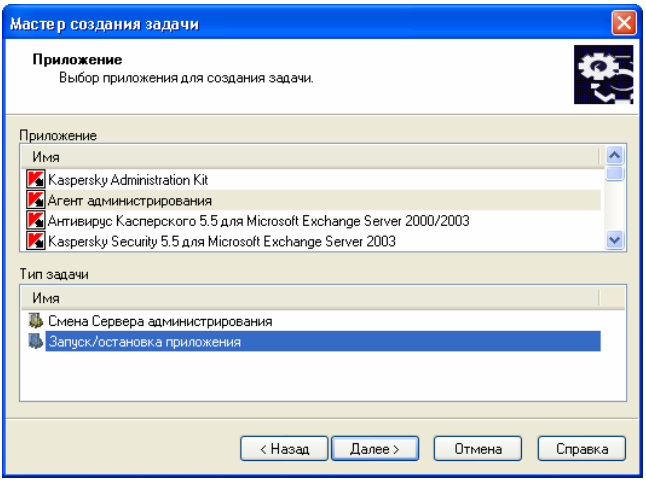

Рисунок 76. Создание задачи. Выбор приложения и типа задачи

Выбор приложения осуществляется из верхнего списка. В нем перечислены все приложения «Лаборатории Касперского», для которых на рабочее место администратора установлены плагины управления. Типы задач приводятся в нижнем списке и соответствуют выбранному приложению.

Если вы создаете задачу запуска или остановки приложения, в качестве приложения вам следует выбрать **Агент администрирования**, в качестве типа задачи – **Запуск / остановка приложения**.

4. Далее вам будет предложено провести настройку задачи в соответствии с выбранным приложением (см. рис. 77). Часть настроек определяется по умолчанию. Подробное описание настройки задач приводится в Руководствах к соответствующим приложениям.

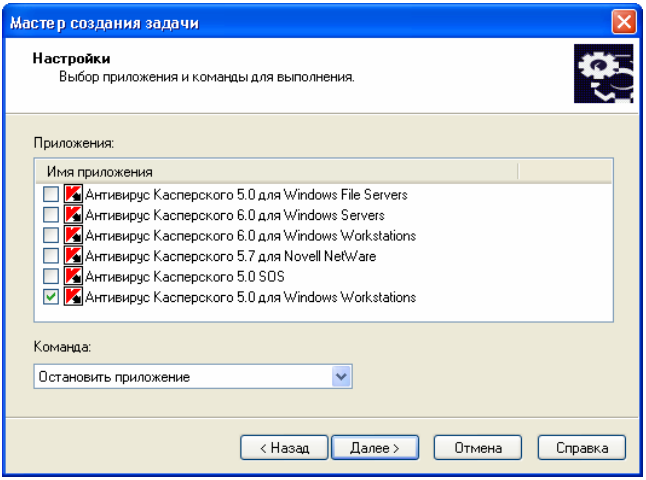

Рисунок 77. Настройка задачи

5. Далее составьте расписание запуска задачи.

   - В раскрывающемся списке **Запуск по расписанию** выберите нужный режим запуска задачи:

     - **Каждый N час**
     - **Ежедневно**.
     - **Еженедельно**.
     - **Ежемесячно**.
     - **Один раз**.
     - **При запуске приложения**.
     - **Вручную** – вручную из главного окна программы Kaspersky Administration Kit при помощи команды **Запустить** контекстного меню или аналогичного пункта в меню **Действие**.
     - **Немедленно** – сразу после создания задачи (по завершению работы мастера).
     - **При получении обновлений Сервером администрирования** – автоматически после получения Сервером администрирования обновлений.
     - **По завершении другой задачи**.
     - **При обнаружении вирусной атаки**.

Здесь перечислены все режимы запуска, используемые в задачах Kaspersky Administration Kit. В зависимости от выбранной задачи некоторые из указанных вариантов могут отсутствовать.

В задачах, создаваемых для приложений, управление которыми доступно через Kaspersky Administration Kit, могут присутствовать дополнительные режимы запуска. Подробную информацию о вариантах запуска задач см. в Руководствах соответствующих приложений.

- Проведите настройку параметров расписания в группе полей, соответствующих выбранному режиму.

  Если вы выбрали режим запуска задачи **Каждый N час** (см. рис. 78) определите:

  - Периодичность запуска задачи в поле **Каждый… час** и дату и время запуска в поле **Начать с**.

    Например, если в поле **Каждый… час** установлено значение 2, а в поле **Начать с** – 3 августа 2006 г. 15:00:00, задача будет запускаться каждые два часа, начиная с 15 часов 3 августа 2006 года.

    По умолчанию для периодичности устанавливается значение 6, в качестве даты и времени запуска автоматически проставляется текущая системная дата и время компьютера.

  - Порядок запуска задачи, если в заданное расписанием время клиентский компьютер недоступен (выключен, отключен от сети и т.п.) или приложение не запущено.

    Установите флажок **Запускать пропущенные задачи**, для того чтобы попытка запуска задачи предпринималась при очередном запуске приложения на данном клиентском компьютере. Для вариантов **Вручную**, **Один раз** и **Немедленно** в этом случае задача будет запущена сразу после появления компьютера в сети.

    Если данный флажок не установлен (по умолчанию) запуск задачи на клиентских компьютерах будет производиться только по расписанию, а для вариантов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских компьютерах.

  - Отклонение от заданного расписанием времени, в течение которого задача будет запущена на клиентских компьютерах. Данная возможность предусмотрена для того, чтобы разрешить проблему одновременного об-

ращения большого числа клиентских компьютеров к Серверу администрирования при запуске задачи.

Установите флажок **Распределить запуск задачи случайным образом в интервале (мин.)** и укажите время в минутах для того, чтобы обращение клиентских компьютеров при запуске задачи к Серверу администрирования происходило не одновременно, а в течение данного временного интервала с момента ее запуска.

По умолчанию данный флажок не установлен.

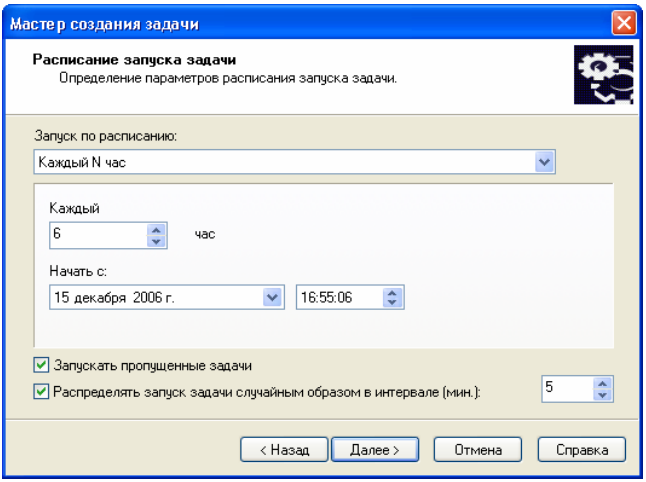

Рисунок 78. Запуск задачи **Каждый N час**

Если вы выбрали режим ежедневного запуска задачи (см. рис. 79) определите:

- Периодичность запуска задачи в полях **Каждый… день** и **Время запуска**.

  Например, если в поле **Каждый день** установлено значение 2, а в поле **Время запуска** – 15:00:00, задача будет запускаться один раз в два дня в 15 часов.

  По умолчанию для периодичности устанавливается значение 2, в качестве времени запуска автоматически проставляется текущее системное время компьютера.

- что делать, если на момент запуска задачи клиентский компьютер временно недоступен (см. описание выше).

- отклонение от заданного расписанием времени, в течение которого задача может запускаться на клиентских компьютерах (см. описание выше).

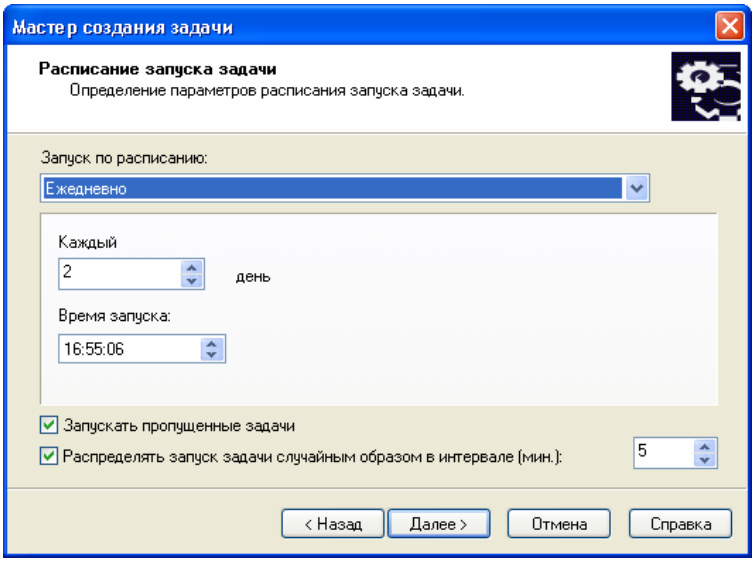

Рисунок 79. Ежедневный запуск задачи

Если вы выбрали режим еженедельного запуска задачи (см. рис. 80) определите:

- периодичность запуска задачи в полях **Каждый** и **Время запуска**. По умолчанию устанавливаются следующие значения данных полей: воскресенье, 18:00:00. Вы можете их изменить.

  Например, если в поле **Каждый** установлено значение **Воскресенье**, а в поле **Время запуска** – 15:00:00, задача будет запускаться каждое воскресенье в 15 часов.

- что делать, если на момент запуска задачи клиентский компьютер временно недоступен (см. описание выше).

- отклонение от заданного расписанием времени, в течение которого задача может запускаться на клиентских компьютерах (см. описание выше).

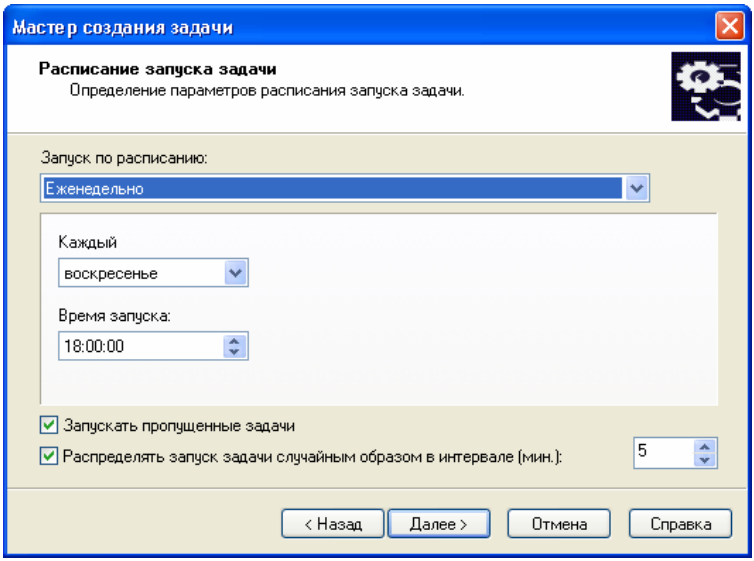

Рисунок 80. Еженедельный запуск задачи

Если вы выбрали режим ежемесячного запуска задачи (см. рис. 81) определите:

- периодичность запуска задачи, установив день и время запуска.

  Например, если в поле **Каждый… день месяца** установлено значение **20**, а в поле **Время запуска** – 15:00:00, задача будет запускаться каждый месяц двадцатого числа в 15 часов.

  По умолчанию в поле **Каждый… день месяца** установлено значение **1**, а в поле **Время запуска** – текущее системное время компьютера.

- что делать, если на момент запуска задачи клиентский компьютер временно недоступен (см. описание выше).

- отклонение от заданного расписанием времени, в течение которого задача может запускаться на клиентских компьютерах (см. описание выше).

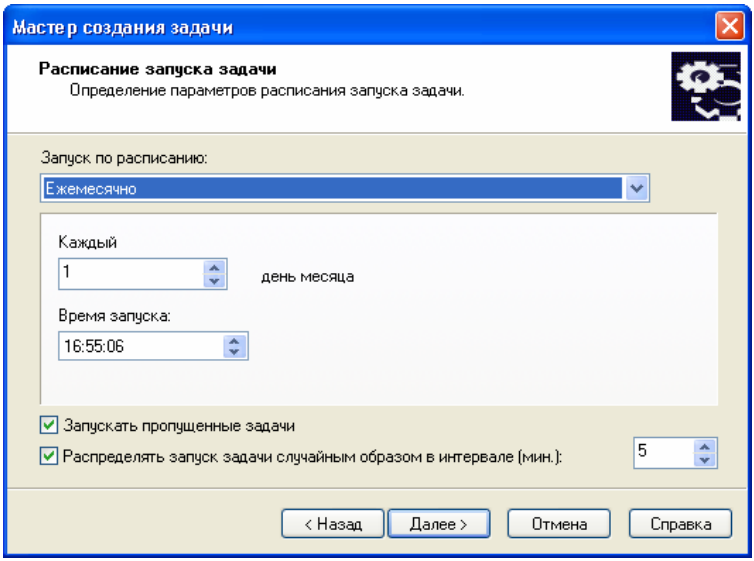

Рисунок 81. Ежемесячный запуск задачи

Если вы определили, что задача будет запускаться один раз (см. рис. 82), установите:

- дату ее запуска в поле **Дата запуска** и время – в поле **Время запуска**. Значения данных полей проставляются автоматически и соответствуют текущей системной дате и времени. Вы можете их изменить.
- что делать, если на момент запуска задачи клиентский компьютер временно недоступен (см. описание выше).
- отклонение от заданного расписанием времени, в течение которого задача может запускаться на клиентских компьютерах (см. описание выше).

Если вы выбрали режим запуска задачи вручную (см. рис. 83), при запуске приложения или сразу после создания задачи, установите:

- что делать, если на момент запуска задачи клиентский компьютер временно недоступен (см. описание выше).
- отклонение от заданного расписанием времени, в течение которого задача может запускаться на клиентских компьютерах (см. описание выше).

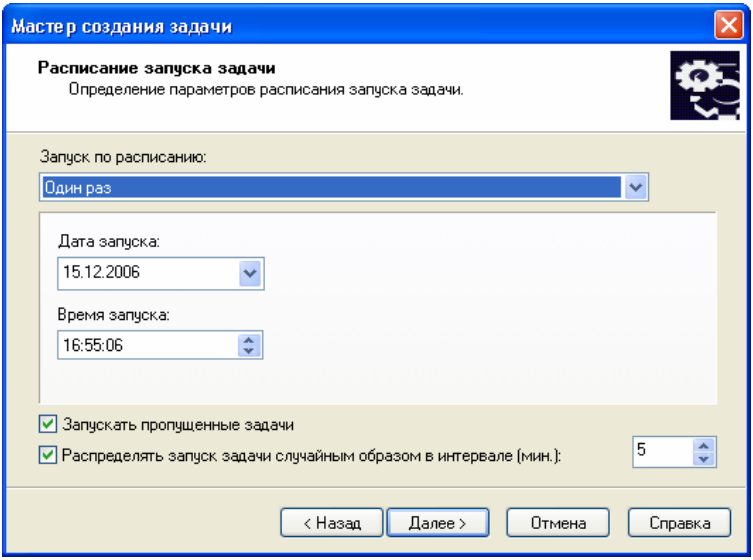

Рисунок 82. Запуск задачи один раз

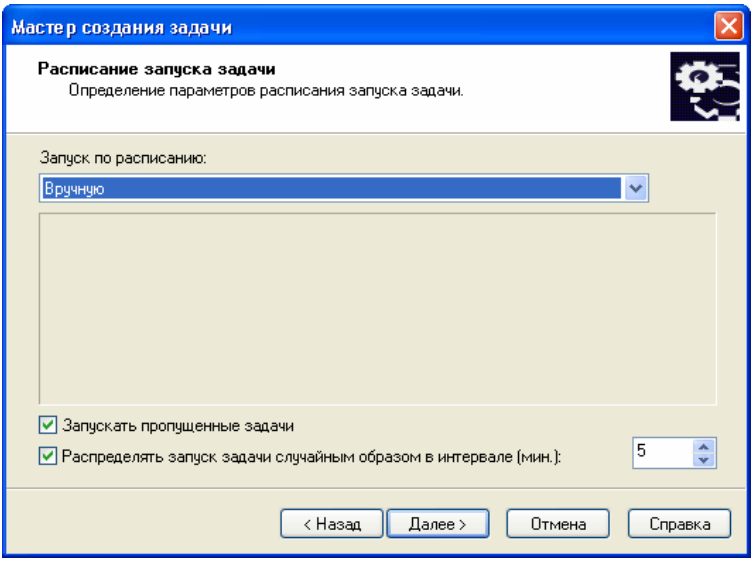

Рисунок 83. Запуск задачи вручную

Если вы определили, что задача будет запускаться после завершения другой задачи (см. рис. 84), задайте:

- задачу, после которой следует запускать текущую задачу. Для этого в поле **Имя задачи** с помощью кнопки **Обзор** выберите нужную задачу. В поле **Результат завершения** укажите для выбранной задачи вариант завершения: **Завершена успешно** или **Завершена с ошибкой**.
- что делать, если на момент запуска задачи клиентский компьютер временно недоступен (см. описание выше).

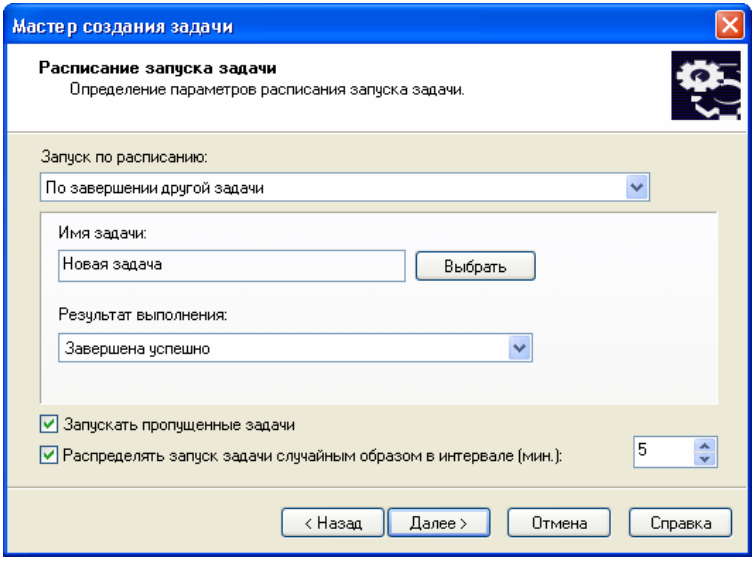

Рисунок 84. Запуск после завершения другой задачи

Если вы определили, что задача будет запускаться при обнаружении вирусной атаки (см. рис. 85), укажите:

- типы приложений, для которых следует учитывать событие **Вирусная атака** при запуске задачи. Для этого установите флажки рядом с нужными типами приложений.
- что делать, если на момент запуска задачи клиентский компьютер временно недоступен (см. описание выше).

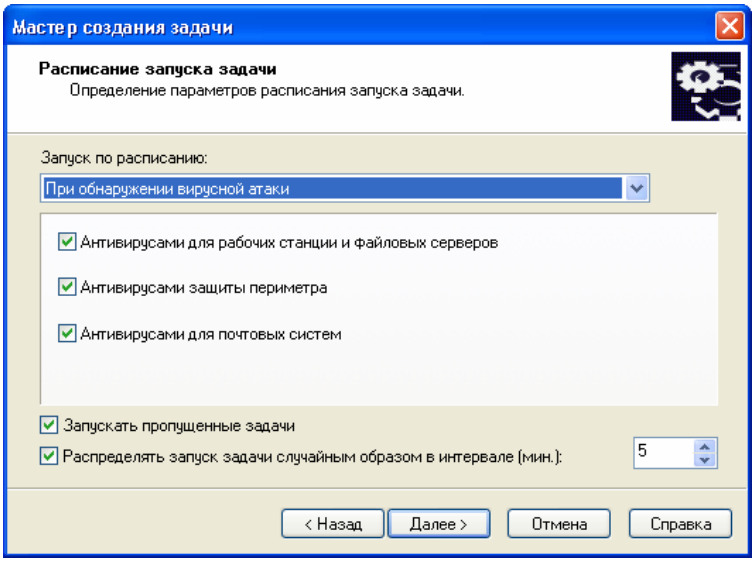

Рисунок 85. Запуск при обнаружении вирусной атаки

По окончании работы мастера задача будет добавлена в папку **Групповые задачи** соответствующей группы и представлена в панели результатов. В случае необходимости вы можете вносить изменения в настройки задачи (см. п. 3.2.4 на стр. 124).

3.2.2. Создание глобальной задачи

Для создания глобальной задачи:

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, аналогичный мастеру создания групповой задачи. Исключение составляет наличие этапа определения списка клиентских компьютеров из состава логической сети, для которых формируется глобальная задача (см. рис. 86).

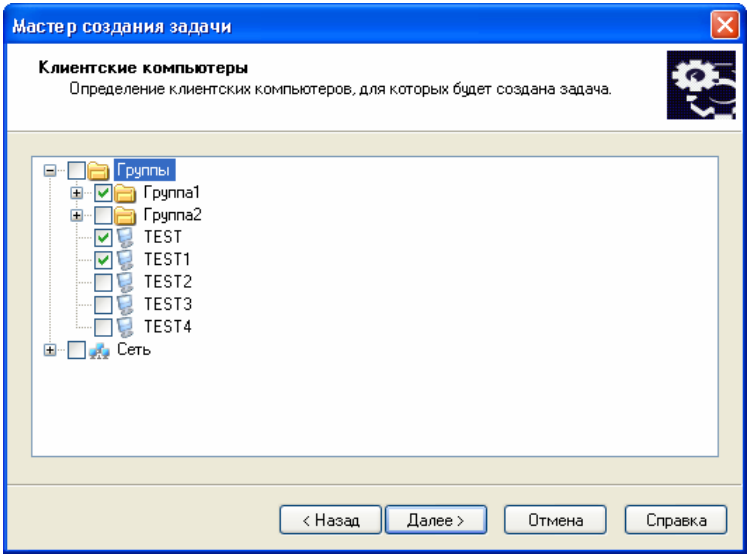

Рисунок 86. Создание глобальной задачи.
Формирование списка компьютеров для запуска

Выберите компьютеры из состава логической сети, на которых будет запускаться задача. Можно выбрать компьютеры из разных папок, можно выбрать папку целиком.

Глобальные задачи выполняются только для заданного набора компьютеров. Если в состав выбранной вами группы, будут добавлены новые клиентские компьютеры, для них данная задача выполняться не будет. Необходимо создать новую задачу или внести соответствующие изменения в настройки существующей.

По окончании работы мастера сформированная глобальная задача будет добавлена в состав узла **Глобальные задачи** дерева консоли и представлена в панели результатов. Над глобальными задачами можно производить все операции, определенные для групповых задач.

3.2.3. Создание локальной задачи

Чтобы создать локальную задачу для клиентского компьютера,

1. В папке **Группы** выберите папку с названием группы, в состав которой входит клиентский компьютер. В панели результатов выберите компьютер, для которого вам необходимо создать за-

дачу, и воспользуйтесь командой **Свойства** контекстного меню или аналогичным пунктом в меню **Действие**. В результате в главном окне программы открывается окно просмотра свойств клиентского компьютера **Свойства: <Имя компьютера>** (см. рис. 20).

2. Выберите закладку **Задачи** (см. рис. 87). На ней представлен полный перечень задач, сформированных для данного клиентского компьютера. Создание новой локальной задачи осуществляется при помощи кнопки **Добавить**, настройка задачи при помощи кнопки **Свойства**.

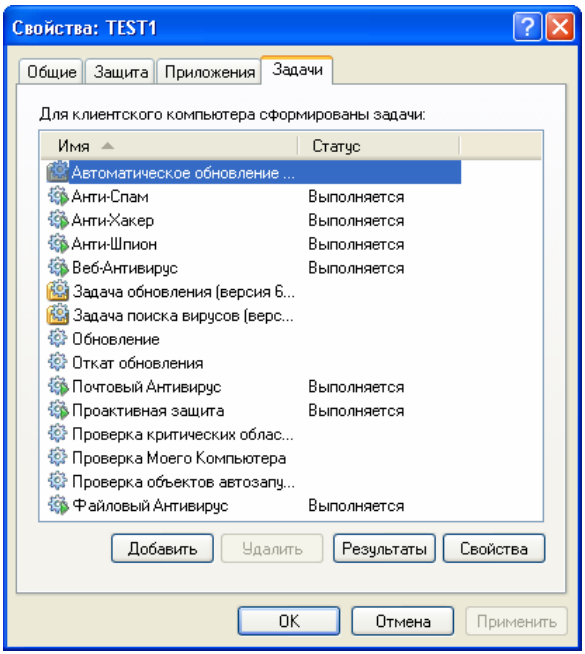

Рисунок 87. Создание локальной задачи. Закладка **Задачи**

Подробное описание создания и настройки локальной задачи приводится в Руководствах к соответствующим приложениям компании.

3.2.4. Просмотр и изменение настроек задачи

Для того чтобы просмотреть настройки задачи и /или внести в них изменения,

- в случае работы с групповой задачей выберите в дереве консоли необходимую группу, выберите входящую в ее состав папку **Групповые задачи**. После этого в панели результатов будет представлен список всех сформированных для данной группы задач. Выберите нужную, откройте контекстное меню и выберите команду **Свойства** или воспользуйтесь аналогичным пунктом в меню **Действие**.

- Если вам необходимо внести изменения в настройки глобальной задачи, выберите в дереве консоли узел **Глобальные задачи**, выберите в панели результатов необходимую задачу, откройте контекстное меню и выберите команду **Свойства** или воспользуйтесь аналогичным пунктом в меню **Действие**.

  В результате открывается окно настройки задачи **Свойства: <Имя задачи>**, состоящее из следующих закладок: **Общие**, **Настройки**, **Учетная запись**, **Расписание**, **Уведомление**. Окно настройки глобальной задачи содержит также закладку **Клиентские компьютеры**.

  В окне настройки задачи **Свойства: <Имя задачи>** представлены параметры, предусмотренные для задачи данного типа по умолчанию, либо определенные при последнем редактировании. Действие групповой политики для глобальных задач не отражается.
  Реальные значения параметров, с которыми задача будет выполняться, вы можете посмотреть в окне свойств конкретного клиентского компьютера **Свойства: <Имя компьютера>** на закладке **Задачи** (см. рис. 87).

  На закладке **Общие** (см. рис. 88) приведены общие сведения о задаче:

  - название задачи (в случае необходимости вы можете его изменить);
  - приложение, для которого создана задача (например, Антивирус Касперского 5.0 для Windows Workstations);
  - номер версии приложения;
  - тип задачи;
  - дата и время создания задачи;
  - последняя команда, произведенная вручную (**Запустить, Остановить, Приостановить, Возобновить**).

В нижней части закладки представлена информация, отображающая статистику результатов выполнения задачи на клиентских компьютерах группы (в случае глобальной задачи на компьютерах, для которых задача определена). С подробным описанием результатов выполнения задачи на клиентских компьютерах вы можете ознакомиться при помощи кнопки **Результаты** (подробнее см. п. 3.2.16 на стр. 136).

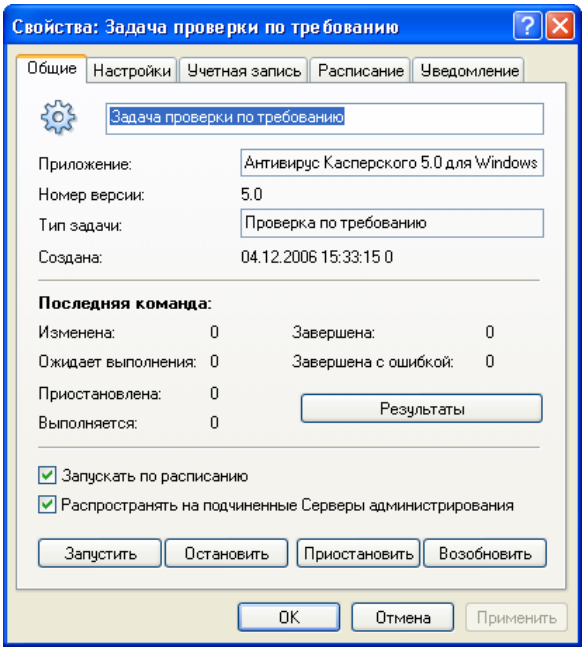

Рисунок 88. Редактирование настроек задачи. Закладка **Общие**

На закладке также расположены командные кнопки, при помощи которых вы можете осуществлять ручное управление процессом выполнения задачи: запускать, останавливать, приостанавливать, возобновлять.

Вы можете временно исключать задачу из числа запускаемых. Для этого снимите флажок **Запускать по расписанию**. В результате данная задача не удаляется, но ее запуск не производится до тех пор, пока флажок **Запускать по расписанию** не будет установлен вновь.

Чтобы задача была скопирована на подчиненные Серверы, установите флажок **Распространять на подчиненные Серверы администрирования**.

На закладке **Настройки** (см. рис. 89) представлены настройки задачи, специфичные для каждого приложения. Подробное описание данной закладки приводится в Руководствах для каждого приложения.

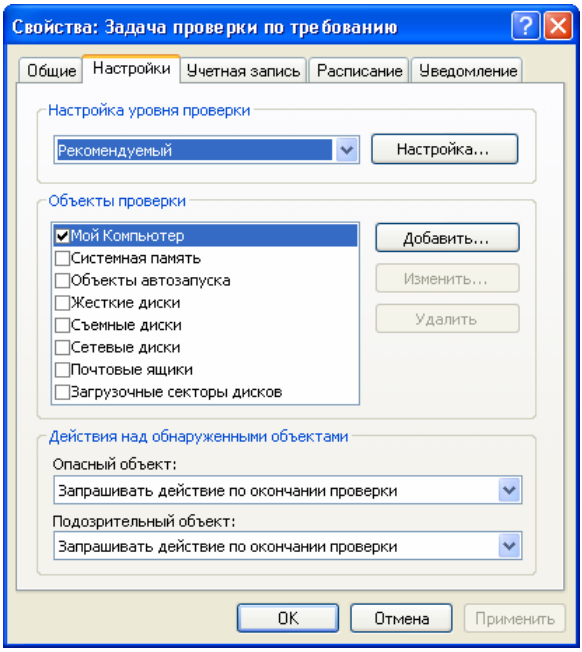

Рисунок 89. Редактирование настроек задачи. Закладка **Настройки**

На закладке **Учетная запись** (см. рис. 90) вы можете указать, под какой учетной записью запускать данную задачу. Вы можете выбрать:

- **Учетная запись по умолчанию**. В этом случае задача будет запускаться под учетной записью приложения, выполняющего данную задачу
- **Задать учетную запись**. В этом случае необходимо ввести данные учетной записи (имя пользователя и пароль), обладающей достаточными правами на доступ к объекту. Например, при выполнении задач проверки по требованию необходимы права на доступ к проверяемому объекту, а при выполнении задач обновления – права на доступ к папке общего доступа на Сервере администрирования или права авторизованного пользователя прокси-сервера.

Это дает возможность избежать ошибки при выполнении задач проверки по требованию и задач обновления, когда у пользователя, запустившего задачу, нет необходимых прав доступа.

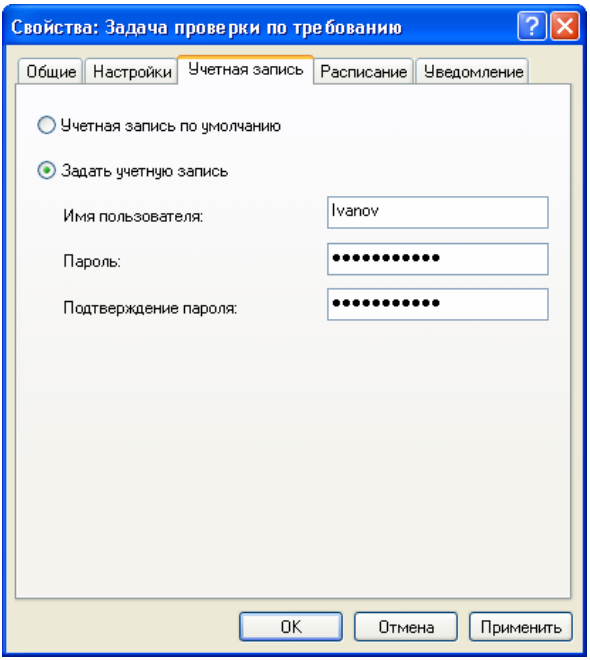

Рисунок 90. Редактирование настроек задачи. Закладка **Учетная запись**

На закладке **Расписание** (см. рис. 91) вы можете вносить изменения в параметры расписания задачи. Нажав на кнопку **Дополнительно**, вы можете:

- настроить автоматический запуск операционной системы на компьютерах, выключенных перед запуском задачи (подробнее см. п. 3.2.6 на стр. 131);
- установить выключение компьютера после выполнения задачи (см. п. 3.2.7 на стр. 132);
- ограничить время выполнения задачи (подробнее см. п. 3.2.8 на стр. 132).

Содержание закладки **Расписание** и работа с ней аналогичны окну настройки параметров расписания при создании задачи (см. п. 3.2.1 на стр. 111).

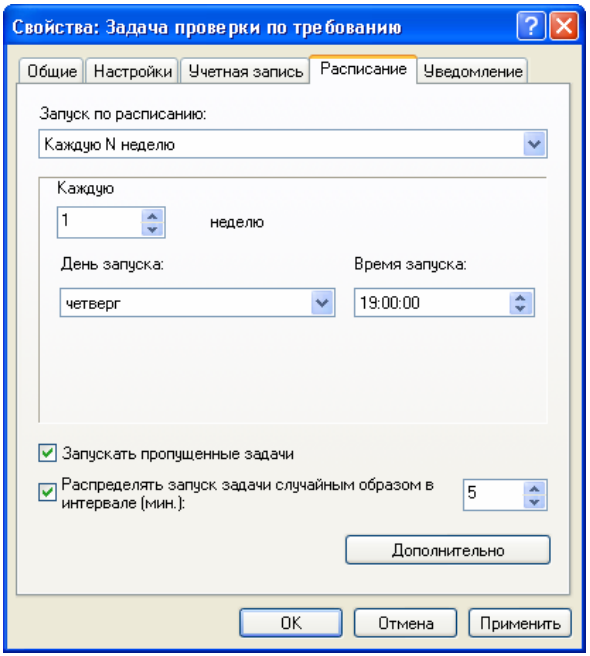

Рисунок 91. Редактирование настроек задачи. Закладка **Расписание**

На закладке **Уведомление** (см. рис. 92) вы можете проводить настройку и изменение параметров режима оповещения о результатах выполнении задачи:

- В группе полей **Сохранять информацию о результатах** определите место хранения информации о результатах, для этого установите:
  - флажок **Локально на клиентском компьютере**, чтобы информация сохранялась на каждом клиентском компьютере локально;

    Эта возможность доступна только при работе с Антивирусом Касперского 5.0 для Windows File Servers.

  - флажок **На Сервере администрирования в течение (дней)**, для того чтобы информация о результатах выполнения задачи на всех клиентских компьютерах сохранялась централизованно на Сервере администрирования, в поле справа задайте количество дней, в течение которых результаты выполнения задачи будут сохраняться на Сервере. По истечении заданного периода с момента регистрации результата информация о нем будет удалена.

- флажок **В журнале событий Windows на клиентском компьютере**, для того чтобы информация о событиях сохранялась в системном журнале Windows на каждом клиентском компьютере локально.
- флажок **В журнале событий Windows на Сервере администрирования**, для того чтобы информация о событиях в работе приложений на всех клиентских компьютерах группы сохранялась централизованно в системном журнале Windows компьютера Сервера администрирования.

В этом же поле выберите, какие события сохранять в журнале:

- **Сохранять все события**.
- **Сохранять события о ходе выполнения задачи**.
- **Сохранять только результат выполнения**.

- В группе **Уведомлять о результатах** укажите тип результатов выполнения задачи, о которых администратор и/или другие пользователи будут получать уведомления, определите способ и проведите настройку параметров оповещения.

  Для этого установите один или несколько флажков:

  - **Уведомлением по электронной почте** – отправка уведомлений через почтовый сервер.
  - **Уведомлением по сети средствами NET SEND** – отправка уведомлений по сети с помощью службы NET SEND.
  - **Запуском исполняемого файла** – запуск при наступлении событий на выполнение какой-либо программы или исполняемого файла.

  Настройка параметров производится так же как в окне свойств события на закладке **Уведомление** (см. рис. 42). По умолчанию используются значения, заданные в настройках Сервера администрирования (см. п. 3.1.1.2 на стр. 66).

  Если вы хотите получать уведомления только об ошибках, установите флажок **Уведомлять только об ошибках**.

Для глобальных задач в окне просмотра настроек представлена закладка **Клиентские компьютеры** (см. рис. 93). Она содержит перечень клиентских компьютеров логической сети, на которых данная задача выполняется. Вы можете вносить изменения в список, добавлять и удалять компьютеры.

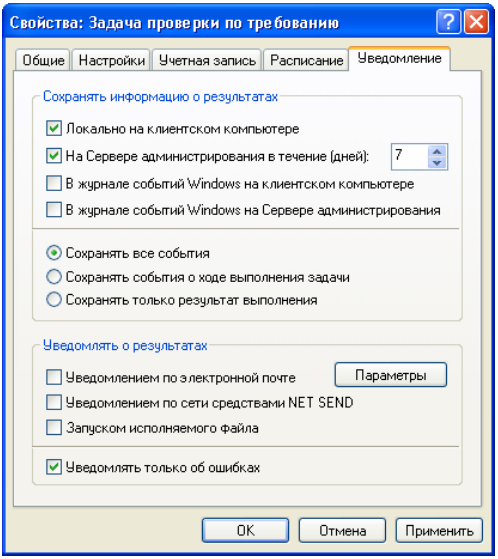

Рисунок 92. Редактирование настроек задачи.
Закладка **Уведомление**

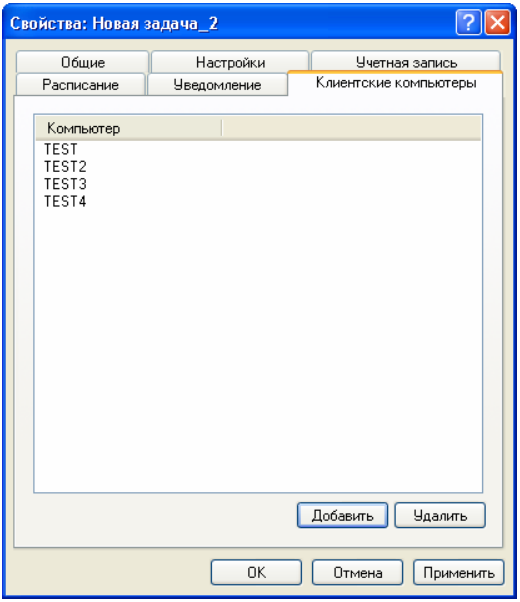

Рисунок 93. Редактирование настроек глобальной задачи.
Закладка **Клиентские компьютеры**

3.2.5. Отображение унаследованной групповой задачи в панели результатов вложенной группы

*Для того чтобы во вложенной группе в папке **Групповые задачи** отображались унаследованные политики:*

1. Выберите в панели результатов во вложенной группе папку **Групповые задачи**.
2. Откройте контекстное меню, выберите в нем пункт **Вид** и установите флажок **Унаследованные задачи**.

В результате унаследованные групповые задачи отобразятся в панели результатов со значком  . Вы можете просматривать свойства унаследованный групповых задач. Редактирование унаследованных групповых задач доступно только в той группе, в которой они были созданы.

3.2.6. Автоматическая загрузка ОС клиентских компьютеров перед запуском задачи

Для того чтобы задача выполнилась на компьютерах, выключенных в установленное в расписании время запуска,

в окне настройки задачи на закладке **Расписание** (см. рис. 91) нажмите на кнопку **Дополнительно**. В открывшемся окне (см. рис. 94) установите флажок **Активировать компьютер перед запуском задачи функцией Wake On Lan за (мин.)** и укажите время. В результате на компьютерах будет автоматически загружаться операционная система перед запуском задачи.

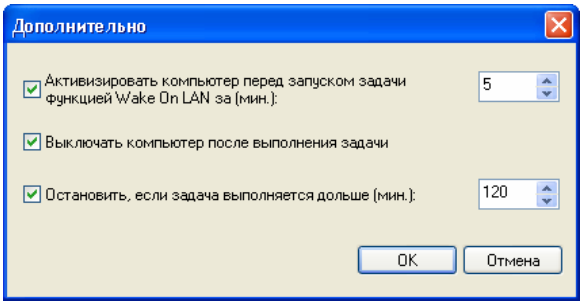

Рисунок 94. Окно **Дополнительно**

3.2.7. Выключение компьютера после выполнения задачи

Для того чтобы после выполнения задачи компьютер был выключен,

в окне настройки задачи на закладке **Расписание** (см. рис. 91) нажмите на кнопку **Дополнительно**. В открывшемся окне (см. рис. 94) установите флажок **Выключать компьютер после выполнения задачи**.

3.2.8. Ограничение времени выполнения задачи

Для ограничения времени выполнения задачи:

в окне настройки задачи на закладке **Расписание** (см. рис. 91) нажмите на кнопку **Дополнительно**. В открывшемся окне (см. рис. 94) установите флажок **Остановить, если задача выполняется дольше (мин.)** и укажите время в минутах, по истечении которого задача будет остановлена.

3.2.9. Отключение запуска задачи по расписанию

Чтобы отключить запуск задачи по расписанию:

в окне настройки задачи на закладке **Общие** (см. рис. 88) снимите флажок **Запускать по расписанию**. В результате задача останется в списке, но запускаться по расписанию не будет.

3.2.10. Создание задачи запуска / остановки приложения

Для того чтобы остановить / запустить приложения на клиентских компьютерах,

создайте групповую, глобальную или локальную задачу. При ее создании укажите следующие значения параметров:

- в качестве приложения выберите **Агент администрирования**, в качестве типа задачи – **Запуск/остановка приложения**.
- в окне **Параметры** (см. рис. 95) укажите приложения для остановки или запуска, установив флажки рядом с именами приложений в представленном списке. Определите действие задачи, выбрав нужный вариант из раскрывающегося списка в нижней части окна:
  - **Остановить приложение**.
  - **Запустить приложение**.

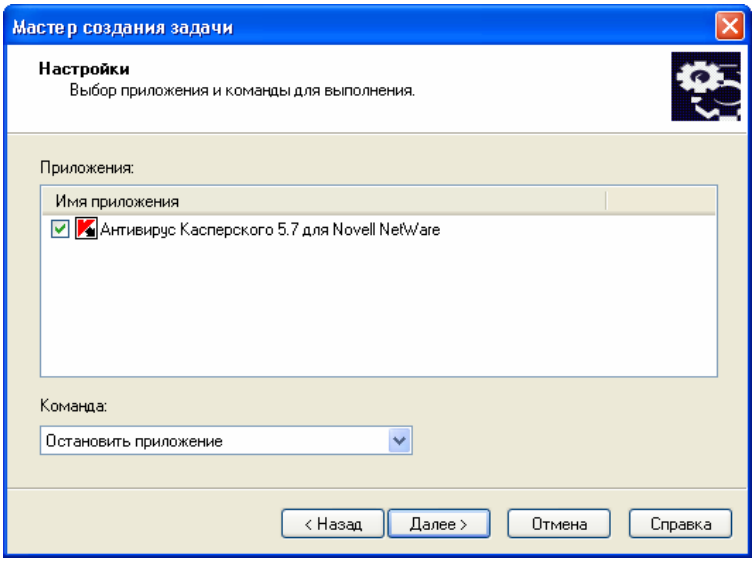

Рисунок 95. Задача запуска/остановки приложения.
Окно **Параметры**

При редактировании задачи запуска/остановки приложения (см. рис. 96) вы можете вносить изменения в описанные выше настройки.

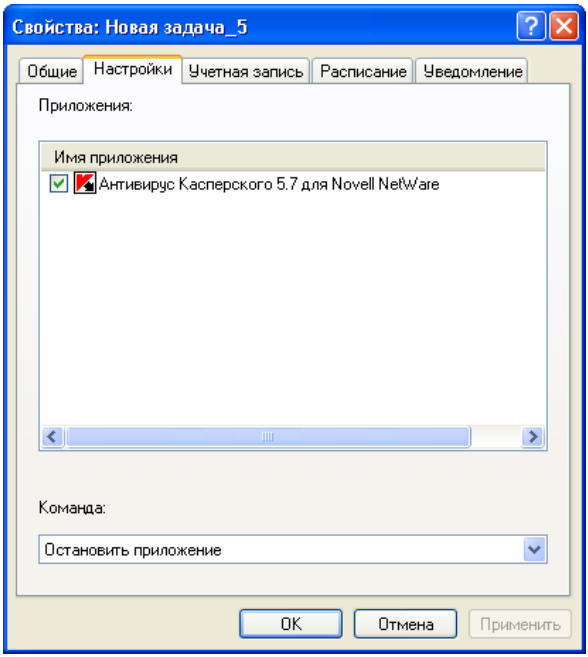

Рисунок 96. Редактирование задачи запуска/остановки приложения

3.2.11. Экспорт задачи

Для того чтобы экспортировать задачу из группы администрирования в файл,

в дереве консоли выберите необходимую группу, выберите входящую в ее состав папку **Групповые задачи**. После этого в панели результатов будет представлен список всех сформированных для данной группы задач. Выберите необходимую задачу, откройте контекстное меню и выберите команду **Экспортировать** или воспользуйтесь аналогичным пунктом в меню **Действие**.

В открывшемся окне укажите имя файла и каталог, в который вы хотите сохранить задачу. Нажмите на кнопку **Сохранить**.

3.2.12. Импорт задачи

Для того чтобы импортировать задачу из файла,

в дереве консоли выберите необходимую группу. Откройте контекстное меню папки **Групповые задачи** (**Глобальные задачи**) и выберите команду **Все задачи / Импортировать** или воспользуйтесь аналогичным пунктом в меню **Действие**.

В открывшемся окне укажите путь к файлу, из которого вы хотите импортировать задачу. Нажмите на кнопку **Открыть**.

3.2.13. Запуск / остановка задачи вручную

Для того чтобы запустить / остановить задачу вручную,

выберите необходимую задачу (групповую или глобальную) в панели результатов, откройте контекстное меню и выберите команду **Запустить / Остановить** или воспользуйтесь аналогичными пунктами в меню **Действие**.

3.2.14. Приостановка / возобновление задачи вручную

Для того чтобы приостановить / возобновить выполнение запущенной задачи,

выберите необходимую задачу (групповую или глобальную) в панели результатов, откройте контекстное меню и выберите команду **Приостановить / Возобновить** или воспользуйтесь аналогичными пунктами в меню **Действие**.

Аналогичные операции вы можете инициировать из окна настройки задачи на закладке **Общие** при помощи командных кнопок **Запустить**, **Остановить**, **Приостановить** и **Возобновить** (см. п. 3.2.4 на стр. 124).

Запуск задач на клиентском компьютере выполняется только в том случае, если запущено соответствующее приложение. При остановке приложения, выполнение всех запущенных задач прекращается.

3.2.15. Наблюдение за ходом выполнения задачи

Для наблюдения за ходом выполнения задачи:

откройте окно настройки интересующей вас задачи (см. п. 3.2.4 на стр. 124), выберите закладку **Общие** (см. рис. 88). В нижней части закладки представлена следующая информация:

- **Изменена** – число компьютеров, для которых есть изменения на Сервере администрирования по данной задаче (подана команда, изменены настройки), но они не синхронизированы с клиентским компьютером.
- **Будет запущена** – число компьютеров, на которых задача готова к запуску по расписанию и ее настройки синхронизированы с данными Сервера администрирования.
- **Приостановлена** – число компьютеров, на которых выполнение задачи приостановлено.
- **Выполняется** – число компьютеров, на которых задача выполняется.
- **Завершена** – число компьютеров, на которых выполнение задачи успешно завершено.
- **Завершена с ошибкой** – число компьютеров, на которых выполнение задачи завершилось с ошибкой.

Аналогичная информация по каждой задаче отображается в главном окне программы, при просмотре групповых или глобальных задач.

3.2.16. Просмотр результатов выполнения задачи, хранящихся на Сервере администрирования

Для того чтобы посмотреть результаты выполнения задачи, хранящиеся на Сервере администрирования:

откройте окно настройки интересующей вас задачи (см. п. 3.2.4 на стр. 124), выберите закладку **Общие** (см. рис. 88) и нажмите на кнопку **Результаты**.

В результате открывается окно **Результаты выполнения задачи** (см. рис. 97). В верхней части окна представлен список всех клиент-

ских компьютеров, для которых данная задача определена. Отображается следующая информация:

- **Клиентский компьютер** — имя клиентского компьютера, на котором определена задача.
- **Группа** — название группы администрирования, в состав которой входит клиентский компьютер.
- **Статус** — текущее состояние задачи.
- **Время** — дата и время регистрации последнего события.
- **Описание** — подробное описание текущего состояния задачи на клиентском компьютере.

В нижней части окна отображаются результаты выполнения задачи на выбранном клиентском компьютере:

- **Статус** — все изменения состояния задачи.
- **Время** — дата и время регистрации каждого события.
- **Описание** — подробное описание каждого события.

Информация, представленная в окне, включает в себя данные с подчиненных Серверов администрирования.

С помощью кнопки **Обновить** вы можете обновить информацию в каждой из таблиц.

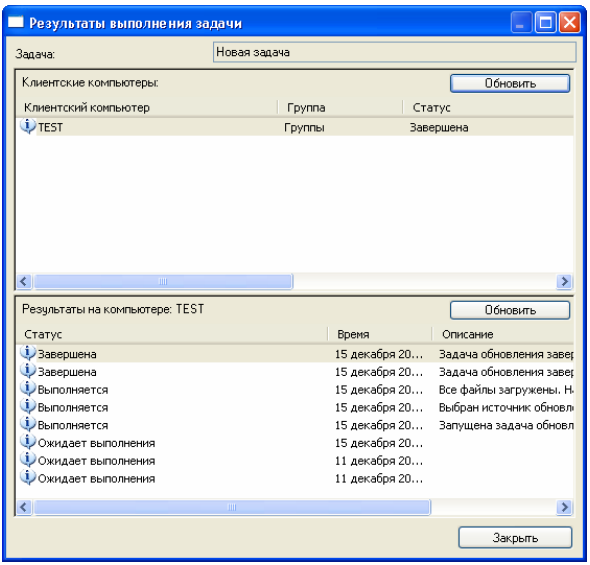

Рисунок 97. Просмотр результатов выполнения задачи, хранящихся на Сервере администрирования

С результатами выполнения задачи для каждого клиентского компьютера вы можете ознакомиться из окна просмотра его свойств **Свойства: <Имя компьютера>** на закладке **Задачи** при помощи кнопки **Результаты** (см. ниже). При этом предоставляется информация, хранящаяся на Сервере администрирования.

Просмотр информации о результатах выполнения задачи, хранящейся локально на клиентском компьютере, доступен только при работе с Антивирусом Касперского 5.0 для Windows File Servers и осуществляется через локально установленную на данном компьютере Консоль администрирования.

3.2.17. Настройка фильтра событий для групповой задачи

*Чтобы настроить фильтр для отображаемой в окне **Результаты выполнения задачи** информации:*

1. Воспользуйтесь командой **Фильтр** контекстного меню списка клиентских компьютеров. В результате открывается окно настройки фильтра (см. рис. 98). Настройте параметры фильтра.
2. На закладке **События** (см. рис. 98) выберите характеристики событий и результатов выполнения задач, которые должны отображаться в результате применения фильтра:
   - Выберите из раскрывающегося списка уровень важности событий.
   - Для того чтобы отображались результаты выполнения задач, выберите интересующий статус задачи в поле **Результаты выполнения задач**.
   - Для ограничения объема информации, представленной после применения фильтра, установите флажок **Ограничить количество отображаемых событий** и укажите максимальное количество строк таблицы.

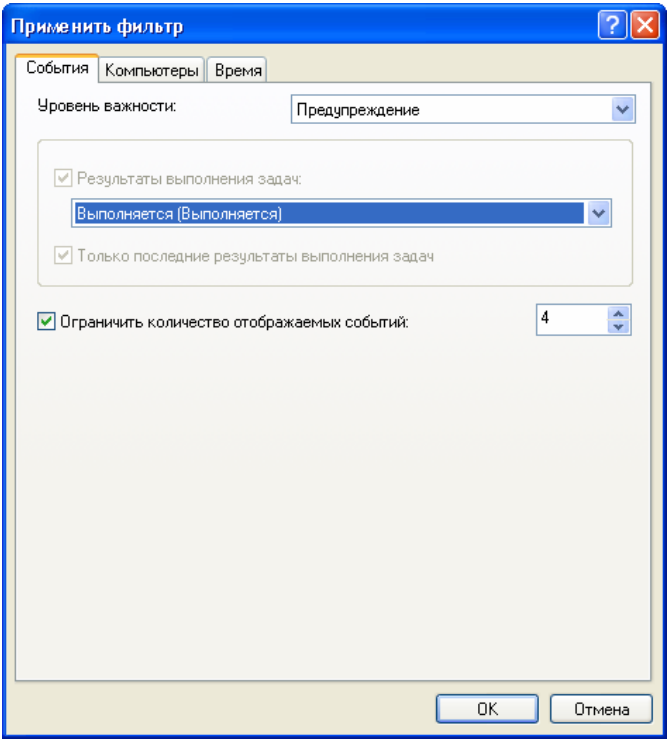

Рисунок 98. Настройка фильтра событий.
Закладка **События**

3. На закладке **Компьютеры** (см. рис. 99) определите, на каких компьютерах должны быть зарегистрированы события и результаты выполнения задач.

   Вы можете использовать следующие параметры:

   - **Имя компьютера** в логической сети;
   - **Имя компьютера в Windows-сети**;
   - **Группа администрирования**;
   - **Домен**;
   - **Диапазон IP-адресов** компьютеров. Для этого установите соответствующий флажок и введите начальный и конечный IP-адрес.

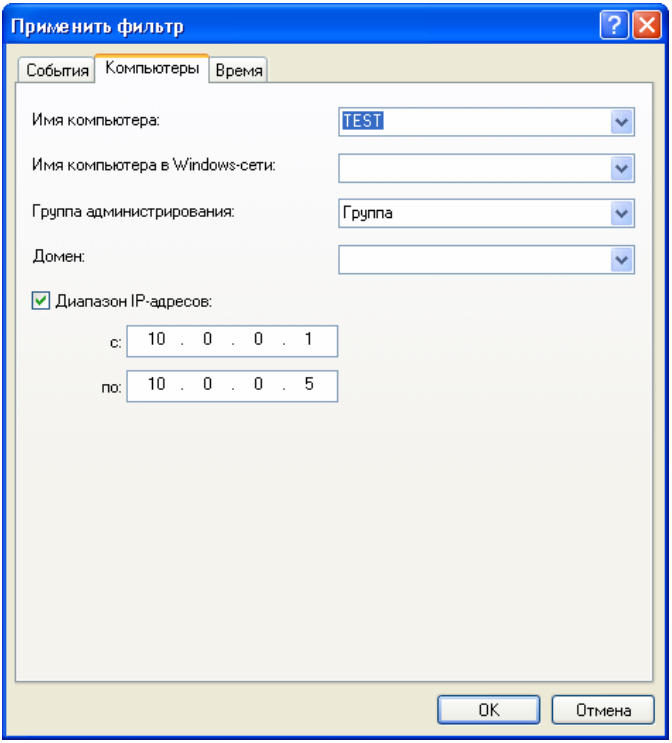

Рисунок 99. Настройка фильтра событий.
Закладка **Компьютеры**

4. На закладке **Время** (см. рис. 100) определите время регистрации событий и результатов выполнения задач.

   Вы можете выбрать следующие варианты:

   - **За период** и определить фиксированные даты начала и конца периода. Для этого в группах полей **С** и **по** соответственно выберите **События на дату** и установите точную дату и время. Если необходима вся зафиксированная информация, выберите **Первое событие** и **Последнее событие**.
   - **За последние дни** и указать количество дней.

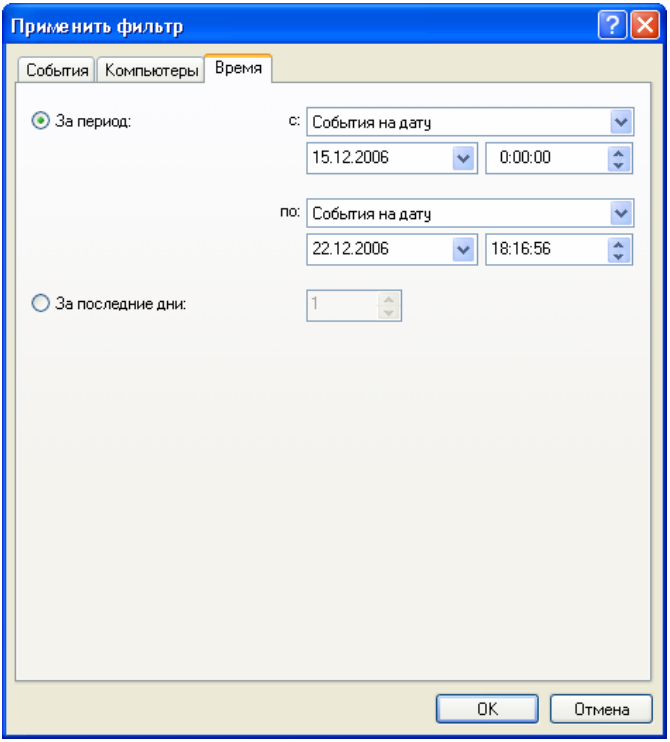

Рисунок 100. Настройка фильтра событий.
Закладка **Время**

5. По окончании настройки для применения фильтра нажмите на кнопку **OK**. В результате в окне **Результаты выполнения задач** будет представлена только информация, удовлетворяющая заданным параметрам.

3.2.18. Настройка фильтра событий для выбранного компьютера

*Чтобы настроить фильтр для отображаемой в окне **Результаты выполнения задачи** (см. рис. 97) информации:*

1. В контекстном меню выберите команду **Фильтр**. В результате открывается окно настройки фильтра (см. рис. 101).
2. Настройте параметры фильтра на закладках **События** (см. рис. 101) и **Время**.

   На закладке **События** (см. рис. 101) выберите характеристики событий и результатов выполнения задач, которые должны отображаться в результате применения фильтра:

   - В поле **Уровень важности** выберите из раскрывающегося списка уровень важности событий.

     Для каждого приложения определены типы событий, которые могут возникать во время его работы. Каждое событие имеет характеристику, отображающую уровень его важности. События одного и того же типа могут иметь различные уровни важности, в зависимости от ситуации, при которой событие произошло.

   - Для того чтобы в фильтр вошли только события определенного типа, установите флажок **События** и установите флажки рядом с названиями нужных типов событий. Если тип событий не указан, будут отображаться все типы событий.
   - Для того чтобы отображались результаты выполнения задач, установите флажок **Результаты выполнения задач** и выберите интересующий статус задачи.
   - Установите флажок **Только последние результаты выполнения задачи**, для того чтобы предоставлялась информация только о результатах последнего запуска задачи.
   - Для ограничения объема информации, представленной после применения фильтра, установите флажок **Ограничить количество отображаемых событий** и укажите максимальное количество строк таблицы.

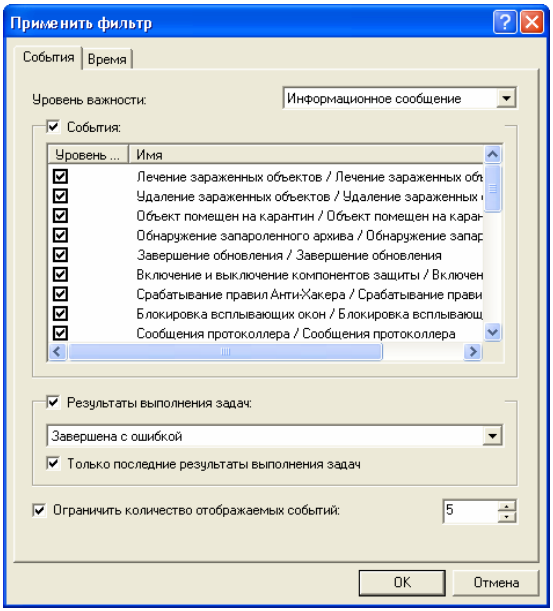

Рисунок 101. Настройка фильтра событий.
Закладка **События**

На закладке **Время** настройте параметры так же, как для групповой задачи (см. п. 3.2.17 на стр. 138). Закладка **Компьютеры** отсутствует, так как настройка фильтра осуществляется для уже выбранного компьютера.

3. По окончании настройки для применения фильтра нажмите на кнопку **OK**. В результате в окне **Результаты выполнения задач** будет представлена только информация, удовлетворяющая заданным параметрам.

3.2.19. Отмена действия фильтра

Для того чтобы отменить действие фильтра,

в контекстном меню выберите команду **Снять фильтр**.

ГЛАВА 4. ОБНОВЛЕНИЕ АНТИВИРУСНЫХ БАЗ И ПРОГРАММНЫХ МОДУЛЕЙ

4.1. Получение обновлений Сервером администрирования

4.1.1. Создание задачи получения обновлений Сервером администрирования

Задача получения обновлений Сервером администрирования является глобальной задачей (см. п. 3.2.2 на стр. 121). При ее создании в качестве приложения, для которого формируется задача, выберите **Kaspersky Administration Kit**, в качестве типа задачи – **Получение обновлений Сервером администрирования** (см. рис. 102).

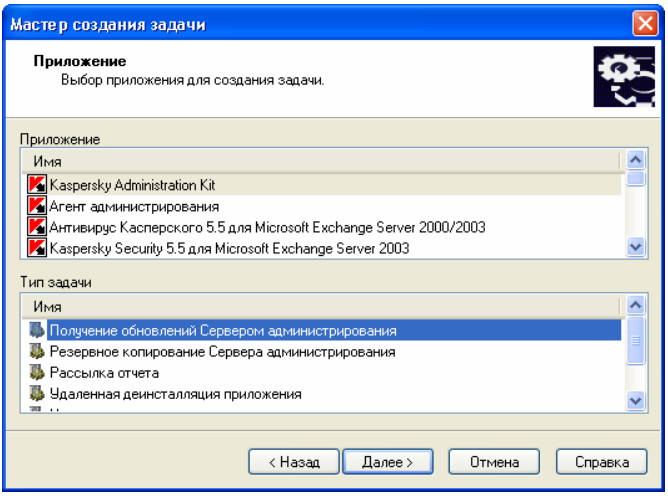

Рисунок 102. Создание задачи обновления. Выбор приложения и типа задачи

На этапе настройки параметров задачи (см. рис. 103) сформируйте список источников получения обновлений. При этом вы можете настроить параметры соединения с серверами обновлений, и определить будут автоматически запускаться задачи получения обновлений подчиненными Серверами администрирования после получения обновлений главным Сервером или нет.

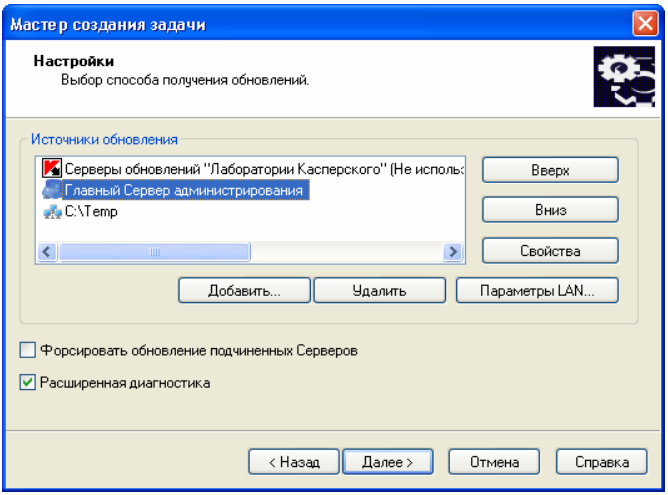

Рисунок 103. Создание задачи обновления.
Настройка параметров получения обновлений

Формирование списка источников получения обновлений выполняется с помощью кнопок **Добавить** и **Удалить**.

Чтобы добавить источник обновлений в список, нажмите на кнопку **Добавить** и в открывшемся окне **Свойства источника обновлений** (см. рис. 104) выберите один из вариантов:

- **Серверы обновлений «Лаборатории Касперского»** – для получения обновлений через интернет с FTP- и HTTP-серверов «Лаборатории Касперского». Изменить параметры прокси-сервера вы сможете в окне настройки задачи (см. рис. 106).
- **Главный Сервер администрирования** – для получения обновлений из папки общего доступа главного Сервера администрирования.
- **Каталог обновлений** – для получения обновлений из сетевого каталога. В случае выбора данного варианта укажите адрес размещения каталога с обновлениями.

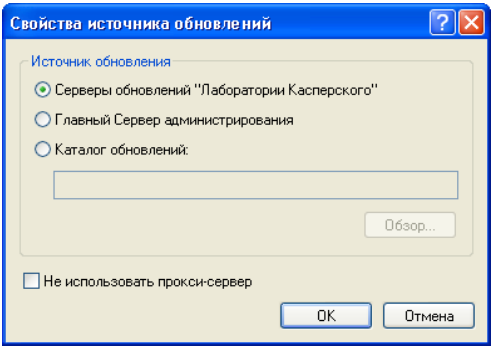

Рисунок 104. Настройка источника получения обновлений

Установите флажок **Не использовать прокси-сервер**, чтобы при соединении с источником обновлений прокси-сервер не использовался. Если флажок не установлен, прокси-сервер будет использоваться в соответствии с параметрами, заданными в окне **Параметры LAN**.

Антивирус Касперского будет производить обновление из перечисленных в списке источников в порядке их очередности. Если по какой-либо причине источник недоступен, обновление будет производиться из следующего по списку источника и т.д. Вы можете изменять очередность следования источников обновления в списке с помощью кнопок **Вверх**/ **Вниз**.

Для настройки соединения с серверами обновлений нажмите на кнопку **Параметры LAN** и установите необходимые значения параметров в открывшемся окне (см. рис. 105):

- Если подключение к источнику обновления осуществляется через прокси-сервер, установите флажок **Использовать прокси-сервер** и введите адрес и номер порта для соединения с прокси-сервером. Допускается использование только десятичной формы записи (например, **Адрес:** 125.2.19.1, **Номер порта:** 3128).
- Если для доступа к прокси-серверу используется пароль, определите параметры аутентификации прокси-пользователя. Для этого установите флажок **Аутентификация на прокси-сервере** и заполните поля **Имя пользователя** и **Пароль**.
- Установите флажок **Использовать пассивный режим FTP**, для того чтобы при обновлении по протоколу FTP использовался пассивный режим, или снимите флажок для использования активного режима. Мы рекомендуем использовать пассивный режим.
- В поле **Тайм-аут соединения, сек.** задайте время, отведенное на соединение с сервером обновления. Если соединение не произошло, по истечении заданного времени предпринимается попытка соединения со следующим сервером обновлений. Перебор производится

до тех пор, пока процесс соединения не завершится успешно, или пока не будут перебраны все доступные сервера обновлений.

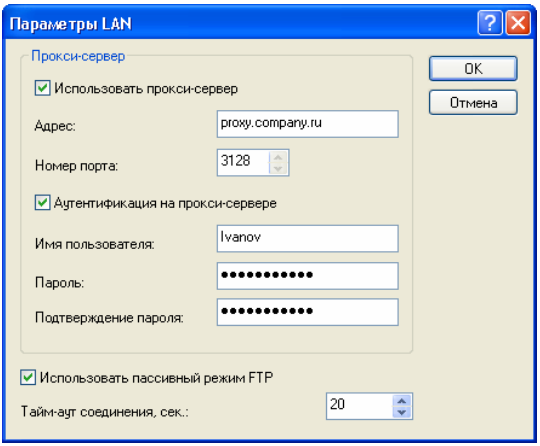

Рисунок 105. Настройка параметров соединения с серверами обновлений

Для того чтобы задачи получения обновлений подчиненными Серверами администрирования запускались автоматически сразу после получения обновлений главным Сервером, не зависимо от расписания, заданного в параметрах этих задач, установите флажок **Форсировать обновление подчиненных Серверов**.

Для того чтобы записывать в журнал подробную информацию о задаче, установите флажок **Расширенная диагностика**. Если флажок снят, то фиксируются только основные этапы выполнения задачи.

4.1.2. Настройка задачи получения обновлений Сервером администрирования

При редактировании параметров задачи обновления на закладке **Настройки** (см. рис. 106) вы можете вносить следующие изменения:

- переопределять список источников получения обновлений и настраивать параметры соединения с серверами обновлений в группе полей **Источники обновлений** (см. п. 4.1.1 на стр. 144).
- определять состав обновлений, копируемых с источника с помощью кнопки **Состав обновлений**. Нажмите на эту кнопку и в открывшемся

окне (см. рис. 107) с помощью флажков сформируйте нужный набор обновлений:

- **Загружать все доступные обновления**.
- **Загружать обновления для всех установленных в сети приложений «Лаборатории Касперского»**.
- если вы хотите выборочно копировать обновления антивирусных баз и программных модулей, в таблице в нижней части окна установите флажки рядом с названиями нужных типов обновлений.

Обновления антивирусных баз и программных модулей сохраняются на Сервере администрирования в заданной папке общего доступа.

- просматривать место расположения каталога для хранения обновлений, полученных с источника в поле **Каталог локального источника обновлений**.
- управлять автоматическим запуском задач получения обновлений подчиненными серверами администрирования при помощи флажка **Форсировать обновление подчиненных Серверов**;
- регулировать уровень детализации информации в журнале задачи с помощью флажка **Расширенная диагностика**.

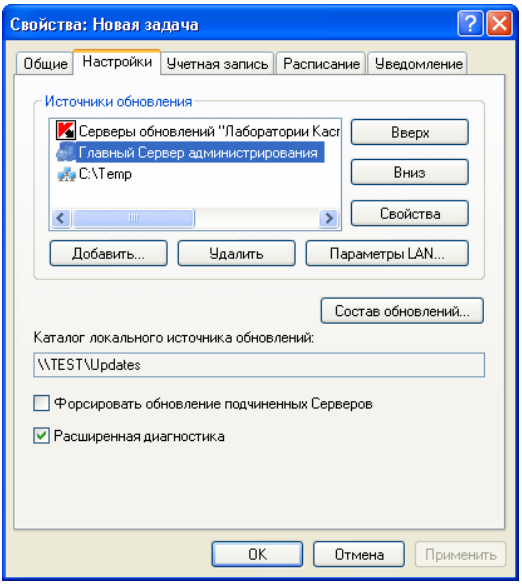

Рисунок 106. Настройка задачи обновления.
Закладка **Настройки**

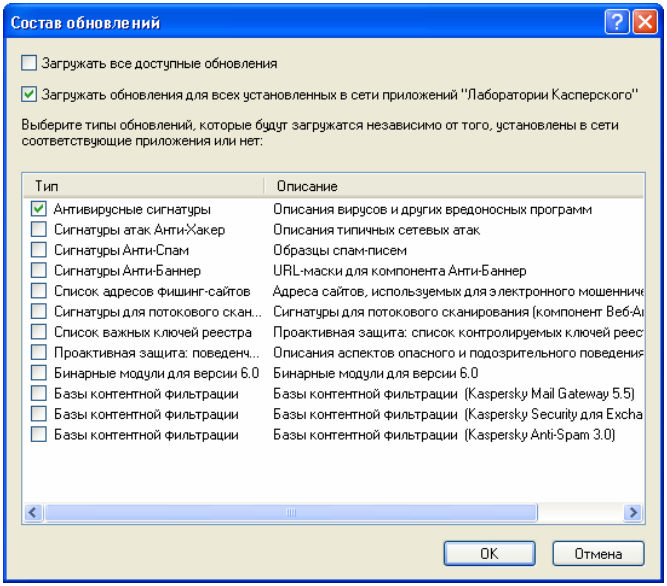

Рисунок 107. Выбор обновлений

4.1.3. Просмотр списка обновлений

Для просмотра полученных Сервером администрирования обновлений,

выберите в дереве консоли узел **Обновление**. Список сохраненных на Сервере администрирования обновлений представлен в панели результатов.

4.1.4. Просмотр свойств полученных обновлений

Для того чтобы просмотреть свойства обновления,

выберите необходимое обновление в панели результатов и воспользуйтесь командой **Свойства** контекстного меню или аналогичным пунктом в меню **Действие**. В результате загружается окно **Свойства: <Имя обновления>** (см. рис. 108).

На закладке **Общие** представлена следующая информация:

- имя обновления; для обновления антивирусных баз данное поле содержит значение **Антивирусные сигнатуры**;
- количество записей в антивирусных базах (данное поле отсутствует для обновлений модулей приложения);
- имя и версия приложения, для которого предназначено обновление;
- размер обновления, сохраненный на Сервере администрирования;
- дата, когда обновление было скопировано на Сервер администрирования;
- дата создания антивирусных баз.

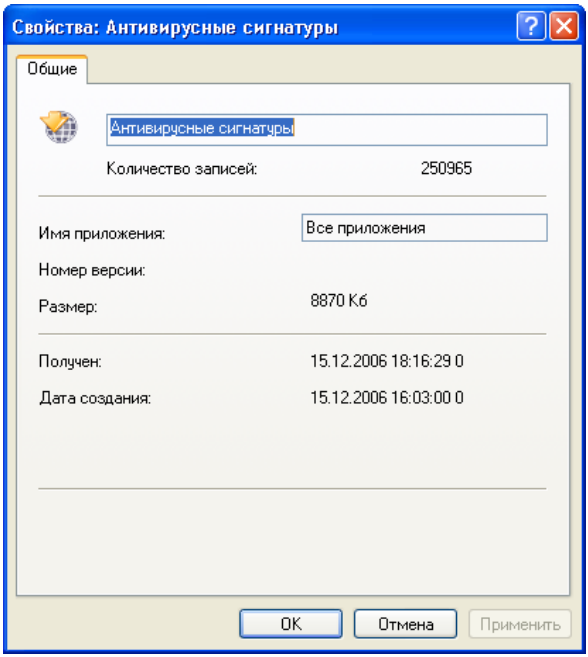

Рисунок 108. Просмотр свойств полученного обновления

4.2. Автоматическое распространение обновлений

4.2.1. Автоматическое распространение обновлений на клиентские компьютеры

Для того чтобы обновления, копируемые Сервером администрирования, сразу после получения автоматически распространялись на клиентские компьютеры,

в настройках задачи получения обновлений каким-либо приложением «Лаборатории Касперского» укажите в качестве источника обновлений Сервер администрирования и на закладке **Расписание** выберите вариант запуска **При получении обновлений Сервером администрирования**.

4.2.2. Автоматическое распространение обновлений на подчиненные Серверы

Для того чтобы обновления, копируемые главным Сервером администрирования, сразу после получения автоматически распространялись на подчиненные Сервера,

в настройках задачи получения обновлений Сервером администрирования (см. рис. 103 и рис. 106) установите флажок **Форсировать обновление подчиненных Серверов**.

В результате сразу после получения обновлений главным Сервером администрирования будут автоматически запускаться задачи получения обновлений подчиненными Серверами администрирования, не зависимо от расписания, установленного в параметрах этих задач.

4.2.3. Формирование списка агентов обновления и их настройка

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

в окне свойств группы (см. рис. 25) перейдите на закладку **Агенты обновления** (см. рис. 109). С помощью кнопок **Добавить** и **Удалить** сформируйте список компьютеров, которые будут выполнять роль агентов обновления в пределах группы.

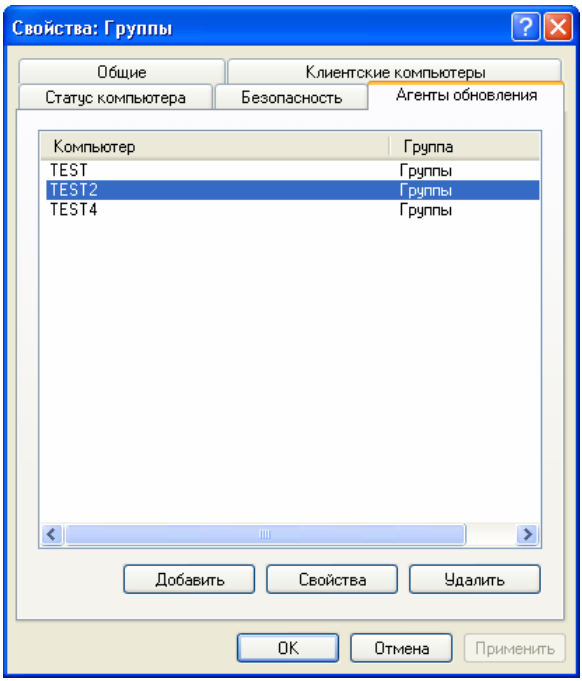

Рисунок 109. Окно свойств группы.
Закладка **Агенты обновления**

Для редактирования настроек агента обновления выберите агента в списке и нажмите на кнопку **Свойства**. В открывшемся окне **<Имя агента обновления> свойства** (см. рис. 110) вы можете:

- указать номер порта, по которому осуществляется подключение клиентского компьютера к агенту обновления. По умолчанию используется порт **14000**. Если он занят, вы можете его изменить;

  Если в качестве агента обновления указывается компьютер, на котором установлен Сервер администрирования, то по умолчанию для подключения используется порт **14001**.

- указать номер порта, по которому осуществляется защищенное подключение клиентского компьютера к агенту обновления с использованием протокола SSL. По умолчанию это порт **13000**.

  Если в качестве агента обновления указывается компьютер, на котором установлен Сервер администрирования, то по умолчанию для подключения с использованием SSL-протокола задается порт **13001**.

- включить использование многоадресной IP-рассылки для автоматического распространения инсталляционных пакетов на клиентские компьютеры в пределах группы. Для этого установите флажок **Использовать многоадресную IP-рассылку** и заполните поля **Адрес IP-рассылки** и **Номер порта IP-рассылки**. Подробную информацию о распространении инсталляционных пакетов с помощью агентов обновления см. в Руководстве по внедрению.

Чтобы просмотреть статистическую информацию агента обновления, щелкните по гиперссылке **Посмотреть статистику Агента обновления**.

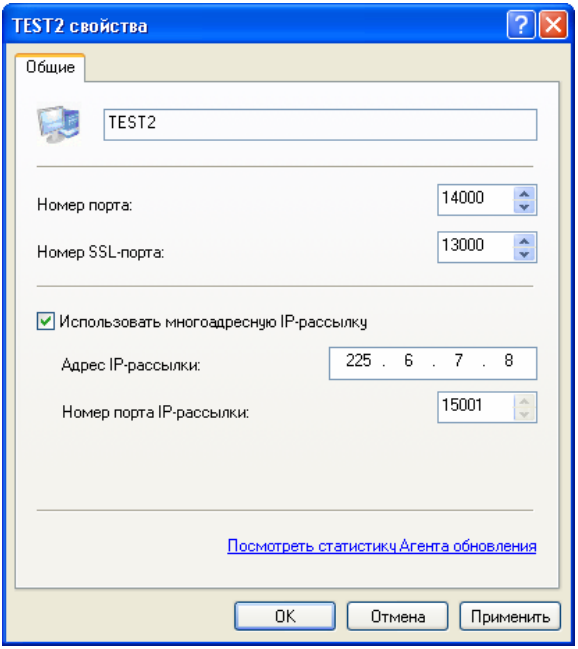

Рисунок 110. Окно свойств агента обновления

ГЛАВА 5. ОБСЛУЖИВАНИЕ

5.1. Продление лицензии

5.1.1. Просмотр информации об установленных лицензионных ключах

Для просмотра информации об установленных лицензионных ключах:

подключитесь к нужному Серверу администрирования (см. п. 2.1 на стр. 12) и выберите в дереве консоли узел **Лицензионные ключи**. После этого в панели результатов будет представлен перечень установленных на клиентских компьютерах лицензионных ключей.

По каждому из них приводится следующая информация:

- **Номер** – серийный номер лицензионного ключа.
- **Тип ключа** – тип установленного лицензионного ключа, например, **коммерческий**, **пробный**.
- **Ограничение** – лицензионные ограничения, заданные в ключе.
- **Срок действия** – срок действия лицензионного ключа.

5.1.2. Просмотр информации о лицензионном ключе

Для просмотра информации о конкретном лицензионном ключе:

выберите в панели результатов нужный лицензионный ключ и воспользуйтесь командой **Свойства** контекстного меню или аналогичным пунктом в меню **Действие**.

В результате открывается окно **Свойства: <серийный номер ключа>**, состоящее из закладок **Общие** и **Объекты** (см. рис. 111).

На закладке **Общие** (см. рис. 111) приводится следующая информация о ключе:

- серийный номер лицензионного ключа;
- тип ключа;
- срок действия;
- лицензионные ограничения, заданные в ключе.

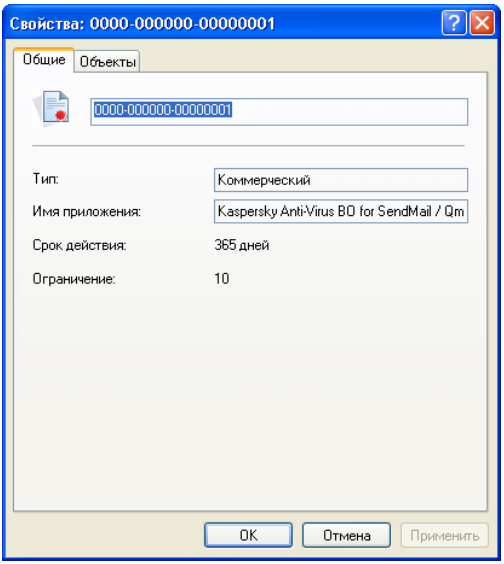

Рисунок 111. Свойства лицензионного ключа. Закладка **Общие**

На закладке **Объекты** (см. рис. 112) представлен список клиентских компьютеров, на которых данный ключ установлен. В нем приводится следующая информация:

- имя клиентского компьютера;
- группа администрирования;
- используется данный ключ в качестве текущего или нет;
- дата окончания ключа;
- дата активации ключа на клиентском компьютере.

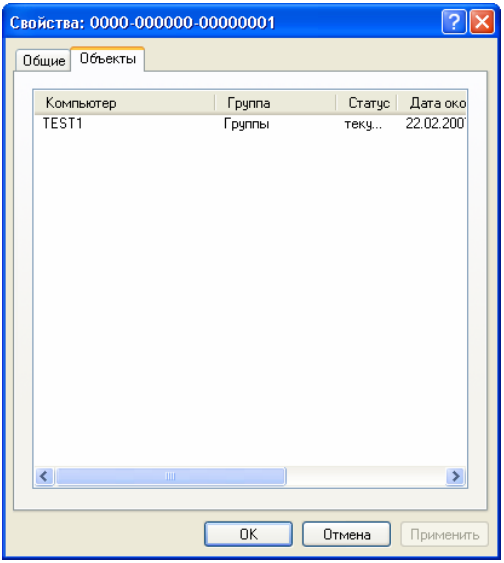

Рисунок 112. Свойства лицензионного ключа.
Закладка **Объекты**

Информацию о том, какие лицензионные ключи установлены для приложения на конкретном клиентском компьютере, можно просмотреть в окне настройки свойств приложения.

5.1.3. Установка лицензионного ключа

Для того чтобы установить лицензионный ключ,

создайте и запустите задачу **установки лицензионного ключа**.

Задача установки лицензионного ключа может быть создана как групповая, глобальная или локальная задача (см. п. 3.2.1 на стр. 111). При ее создании:

- в качестве приложения, для которого формируется задача, выберите приложение, для которого вы устанавливаете лицензионный ключ;
- в качестве типа задачи – **Установка лицензионного ключа**.

На этапе настройки задачи (см. рис. 113) укажите файл лицензионного ключа, который необходимо установить (***.key**). Если данный ключ будет использоваться в качестве текущего ключа для приложения и

заменит предыдущий текущий ключ сразу после установки, установите флажок **Использовать в качестве текущего лицензионного ключа**. Если ключ устанавливается в качестве резервного ключа, флажок устанавливать не следует. Резервный лицензионный ключ становится текущим по окончании срока действия текущего лицензионного ключа. В поле **Информация о лицензионном ключе** приводится более подробная информация о лицензионном ключе.

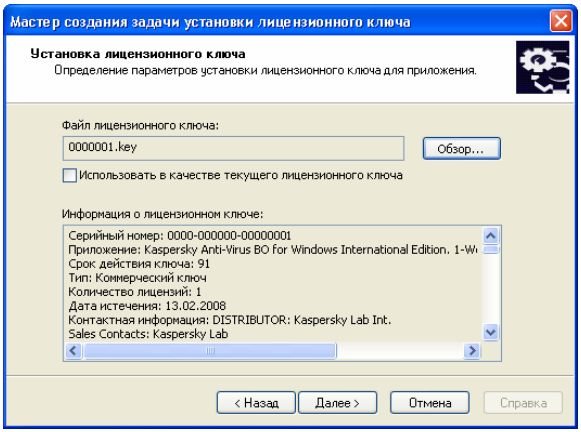

Рисунок 113. Создание задачи продления лицензии. Выбор файла лицензионного ключа

5.1.4. Запуск мастера создания задачи установки лицензионного ключа

Для запуска мастера задачи установки лицензионного ключа:

выберите в дереве консоли узел **Лицензионные ключи** и воспользуйтесь командой **Добавить лицензионный ключ** контекстного меню или аналогичным пунктом в меню **Действие**. В результате запускается мастер создания глобальной задачи, но в нем отсутствует этап выбора типа задачи, он проставляется по умолчанию.

Задачи, сформированные при помощи мастера задач установки лицензионного ключа, являются глобальными и размещаются в узле **Глобальные задачи** дерева консоли.

При редактировании настроек задачи установки лицензионного ключа на закладке **Настройки** (см. рис. 114) вы можете заменить файл лицензионного ключа для установки и установить флажок **Использовать в качестве текущего лицензионного ключа**, чтобы данный ключ

использовался в качестве текущего ключа для приложения. Если флажок не установлен, ключ является резервным. В поле **Информация о лицензионном ключе** приводится более подробная информация о лицензионном ключе.

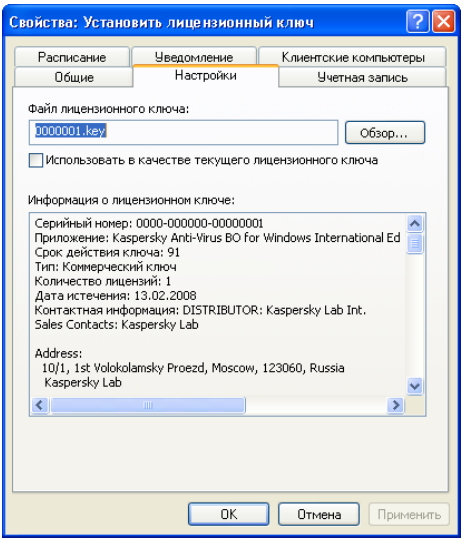

Рисунок 114. Настройка задачи продления лицензии

5.1.5. Создание и просмотр отчета о лицензионных ключах

Для создания отчета о состоянии лицензионных ключей, установленных на клиентские компьютеры логической сети:

воспользуйтесь встроенным шаблоном **Отчет о лицензионных ключах** либо создайте новый шаблон одноименного типа (см. п. 5.4.1 на стр. 169).

В отчете, созданном по шаблону **Отчет о лицензионных ключах**, представлена полная информация обо всех установленных на клиентских компьютерах логической сети лицензионных ключах, как текущих, так и резервных, с указанием компьютеров, на которых они используются, и лицензионных ограничений.

5.2. Карантин и резервное хранилище

5.2.1. Просмотр свойств объекта, помещенного на карантин или в резервное хранилище

Для просмотра свойств объекта, помещенного в хранилище:

выберите в дереве консоли узел **Хранилища**, затем **Карантин** (или **Резервное хранилище**). В панели результатов выберите нужный вам объект и воспользуйтесь командой **Свойства** контекстного меню или аналогичным пунктом в меню **Действие**.

В открывшемся окне (см. рис. 115) представлена следующая информация об объекте:

- имя объекта, под которым он поступил на обработку антивирусному приложению;
- описание объекта;
- действие, которое было выполнено над объектом антивирусным приложением;
- имя компьютера, на котором хранится объект;
- статус, присвоенный объекту антивирусным приложением;
- имя вируса, который содержит или возможно содержит объект;
- дата помещения объекта на карантин или в резервное хранилище;
- размер объекта в байтах;
- путь на клиентском компьютере к каталогу, в котором изначально был расположен объект;
- имя пользователя, поместившего объект на карантин или в резервное хранилище.

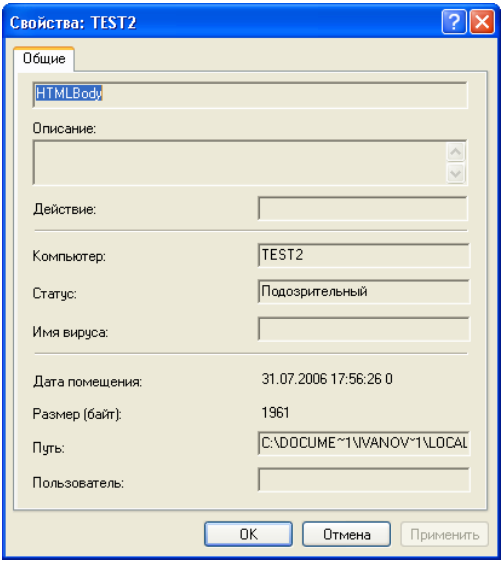

Рисунок 115. Просмотр свойств объекта, помещенного на карантин или в резервное хранилище

5.2.2. Удаление объекта из карантина или резервного хранилища

Для удаления объекта из хранилища:

выберите в дереве консоли узел **Хранилища**, затем **Карантин** (или **Резервное хранилище**). В панели результатов выберите нужный вам объект и воспользуйтесь командой **Удалить** контекстного меню или аналогичным пунктом в меню **Действие**.

В результате антивирусное приложение, поместившее объект в хранилище на клиентском компьютере, удалит объект из карантина или резервного хранилища.

5.2.3. Восстановление объекта из карантина или резервного хранилища

Для восстановления объекта из хранилища:

выберите в дереве консоли узел **Хранилища**, затем **Карантин** (или **Резервное хранилище**). В панели результатов выберите нужный вам объект и воспользуйтесь командой **Восстановить** контекстного меню или аналогичным пунктом в меню **Действие**.

В результате антивирусное приложение, поместившее объект в хранилище на клиентском компьютере, восстановит объект в исходный каталог.

5.2.4. Проверка карантинного каталога на клиентском компьютере

Для проверки карантинного каталога на клиентском компьютере:

выберите в дереве консоли узел **Карантин**, выберите в панели результатов объект, который вы хотите проверить, и воспользуйтесь командой **Проверить объекты на карантине** контекстного меню или аналогичным пунктом в меню **Действие**.

В результате на клиентском компьютере для антивирусного приложения, поместившего объект на карантин, будет запущена задача проверки по требованию карантинного каталога.

5.3. Журналы событий. Выборки событий

5.3.1. Просмотр журнала событий Kaspersky Administration Kit, хранящегося на Сервере администрирования

Для просмотра информации журнала событий Kaspersky Administration Kit, хранящейся на Сервере администрирования,

подключитесь к нужному Серверу администрирования (см. п. 2.1 на стр. 12), раскройте в дереве консоли узел **События** и выберите папку, соответствующую интересующей вас выборке: **Все события**, **Информационные сообщения**, **Критические события**, **Отказы функционирования**, **Предупреждения**, **События аудита**.

После этого в панели результатов будет представлена таблица (см. рис. 116), содержащая полный перечень всех событий выбранного типа, хранящихся на данном Сервере администрирования (для всех групп и всех установленных приложений). В таблице отображается следующая информация:

- **Уровень важности** – уровень важности зарегистрированного события.
- **Клиентский компьютер** – имя клиентского компьютера или Сервера администрирования, на котором произошло событие.
- **Группа** – название группы администрирования, в состав которой входит клиентский компьютер.
- **Приложение** – название приложения, в работе которого зафиксировано событие.
- **Номер версии** – номер версии приложения.
- **Задача** – название задачи, в результате действия которой возникло событие.
- **Событие** – название события.
- **Время** – дата и время регистрации события.
- **Описание** – описание события.

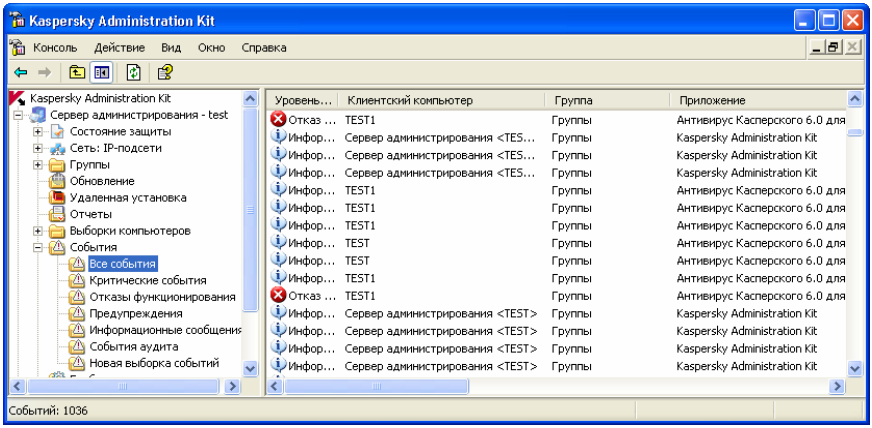

Рисунок 116. Просмотр событий, хранящихся на Сервере администрирования

Вы можете сортировать информацию в таблице по возрастанию или убыванию данных любого из столбцов, а также менять порядок и состав столбцов.

Для упрощения просмотра и поиска необходимой информации предусмотрена возможность создания и настройки пользовательских выборок. Использование выборки позволяет осуществлять поиск, а также отсеивать лишнюю информацию, затрудняющую просмотр, поскольку в таблице событий для каждой выборки отображается только информация, удовлетворяющая ее параметрам. Это является весьма актуальным в связи с большим объемом хранящейся на Сервере информации.

5.3.2. Создание выборки событий

Чтобы создать выборку:

1. Выберите в дереве консоли узел **События**, откройте контекстное меню и воспользуйтесь командой **Создать/ Новая выборка** или аналогичным пунктом в меню **Действие**.
2. В открывшемся окне введите имя выборки (см. рис. 117) и нажмите на кнопку **ОК**.

В результате в дереве консоли будет создана новая папка с именем, заданным для выборки, в ее состав будут включены все события и результаты выполнения задач, хранящиеся на Сервере администрирования. Для поиска нужных событий настройте параметры выборки.

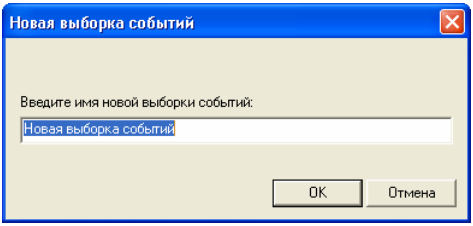

Рисунок 117. Создание выборки событий

5.3.3. Настройка выборки событий

Чтобы настроить выборку:

1. Выберите в дереве консоли или в панели результатов нужную выборку событий, и воспользуйтесь командой **Свойства** контекстного меню или аналогичным пунктом в меню **Действие**.
2. В результате открывается окно настройки выборки (см. рис. 118), состоящее из закладок: **Общие**, **События**, **Компьютеры** и **Время**.

   На закладке **Общие** вы можете изменить имя выборки.

   На закладке **События** (см. рис. 118) определите характеристики событий и результатов выполнения задач, которые должны войти в выборку:

   - Название приложения, работа которого вас интересует.
   - Номер версии приложения.
   - Имя задачи, результаты которой нужно отобразить.
   - Выберите из раскрывающегося списка уровень важности событий.

     Для каждого приложения определены типы событий, которые могут возникать во время его работы. Каждое событие имеет характеристику, отображающую уровень его важности. События одного и того же типа могут иметь различные уровни важности, в зависимости от ситуации, при которой событие произошло.

   - Для того чтобы в выборку вошли только события определенного типа, установите флажок **События** и установите флажки рядом с названиями нужных типов событий. Если тип событий не указан, будут отображаться все типы событий.
   - Для того чтобы в выборку вошли результаты выполнения задач, установите флажок **Результаты выполнения задач** и выберите интересующий статус задачи.

- Установите флажок **Только последние результаты выполнения задачи**, для того чтобы предоставлялась информация только о результатах последнего запуска задачи.
- Для ограничения объема информации, представленной в выборке, установите флажок **Ограничить количество отображаемых событий** и укажите максимальное количество строк таблицы событий.

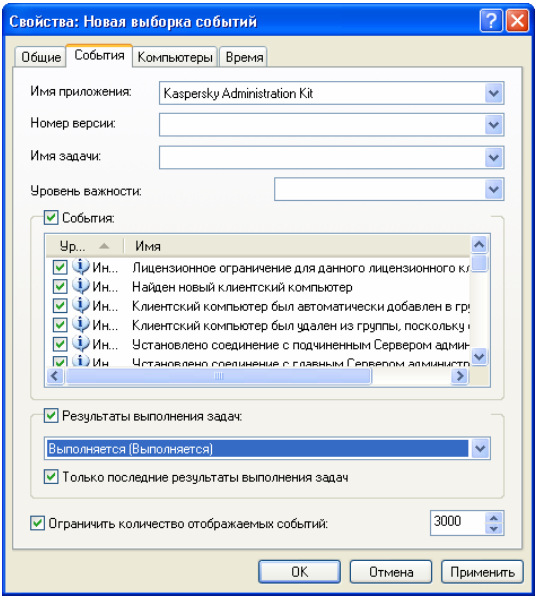

Рисунок 118. Настройка выборки событий. Закладка **События**

На закладке **Компьютеры** (см. рис. 119) определите, на каких компьютерах должны быть зарегистрированы события и результаты выполнения задач, входящие в выборку. Вы можете использовать следующие параметры:

- имя компьютера в логической сети;
- имя компьютера в Windows-сети;
- группу администрирования;
- домен;
- указать диапазон IP-адресов компьютеров, для этого установите флажок **Диапазон IP-адресов** и введите начальный и конечный IP-адрес.

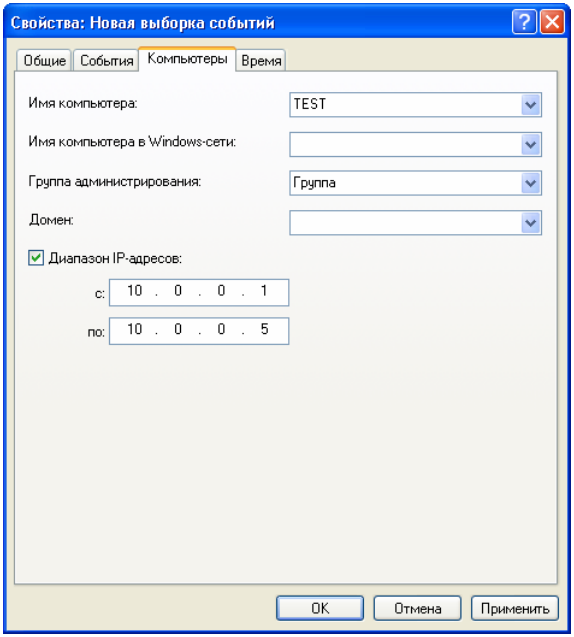

Рисунок 119. Настройка выборки событий.
Закладка **Компьютеры**

На закладке **Время** (см. рис. 120) определите время регистрации событий и результатов выполнения задач, входящих в выборку.

Вы можете выбрать следующие варианты:

- **За период** и определить фиксированные даты начала и конца периода. Для этого в группах полей **С** и **по** соответственно выберите **События на дату** и установите точную дату и время. Если необходима вся зафиксированная информация, выберите **Первое событие** и **Последнее событие**.
- **За последние дни** и указать количество дней.

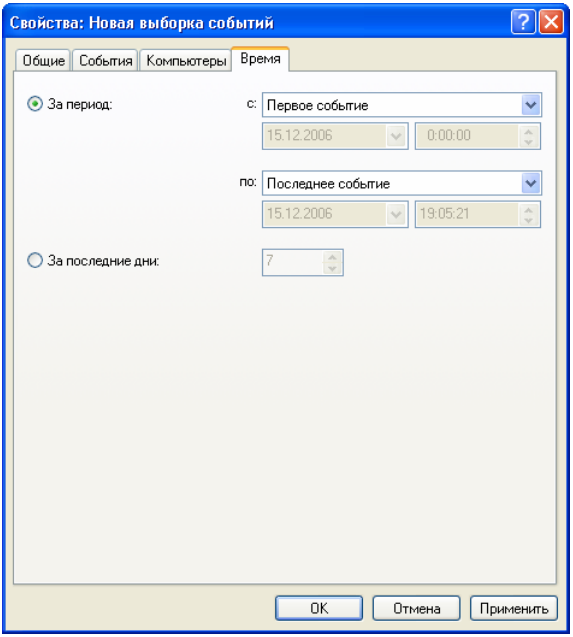

Рисунок 120. Настройка выборки событий.
Закладка **Время**

3. По окончании настройки для применения параметров выборки нажмите на кнопку **Применить** или **OK**. В результате в таблице событий для выборки будет отображаться только информация, удовлетворяющая заданным параметрам.

5.3.4. Сохранение информации о событиях в файле

Для сохранения информации о событиях в файле:

1. Выберите в дереве консоли выборку событий, содержащую нужные вам события и воспользуйтесь командой **Все задачи/ Экспортировать** контекстного меню или аналогичным пунктом в меню **Действие**. В результате запускается мастер.
2. На первом шаге мастера укажите путь к файлу и имя файла, в котором будет сохранена информация. Если вы хотите чтобы в файл были сохранены только выбранные вами в панели

результатов события, установите флажок **Экспортировать только выбранные события**.

3. На втором шаге выберите формат экспорта событий:
   - **Экспортировать как текст, разделенный знаками табуляции –** текстовый файл.
   - **Экспортировать как текст в формате UNICODE, разделенный знаками табуляции** – текстовый файл в формате UNICODE.
4. Для завершения работы мастера нажмите на кнопку **Готово**.

5.3.5. Удаление событий

Для удаления событий, удовлетворяющих определенным условиям,

сформируйте и примените выборку событий с параметрами, соответствующими требуемым условиям. Поле этого удалите все события, представленные в панели результатов, при помощи команды контекстного меню **Очистить**.

В результате из состава узла **События** будут удалены только события, удовлетворяющие параметрам выборки.

5.4. Отчеты

5.4.1. Создание шаблона отчета

Для создания нового шаблона отчета:

1. Выберите в дереве консоли узел **Отчеты** и воспользуйтесь командой **Создать / Шаблон отчета** контекстного меню или аналогичным пунктом в меню **Действие**. В результате запускается мастер. Следуйте его указаниям.
2. Определите имя шаблона. Если вы зададите имя уже существующего, к нему автоматически будет добавлено окончание **_1**.
3. Выберите тип отчета. Дальнейшие шаги мастера зависят от сделанного вами выбора.
4. Установите временной интервал, за который будет составляться отчет (см. рис. 121). Вы можете определить фиксированные даты начала и конца интервала либо

установить интервал с открытой датой окончания. При выборе второго варианта в качестве даты окончания будет использоваться текущая системная дата. Вы также можете выбрать вариант **за последние дни** и указать необходимое количество дней в поле справа.

Этот шаг отсутствует для отчетов, отображающих состояние, соответствующее дате их составления, например, для шаблонов отчетов об уровне антивирусной защиты.

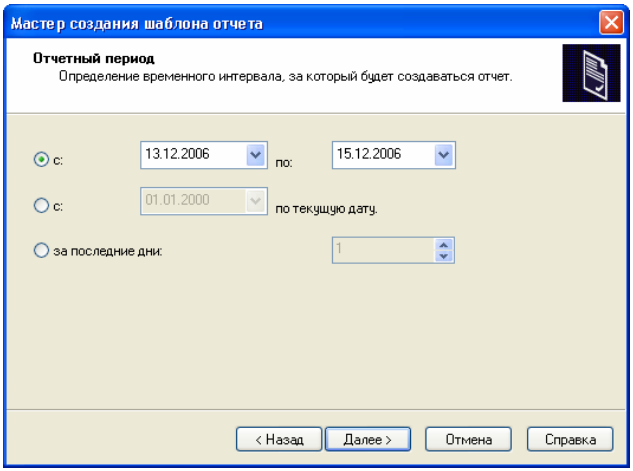

Рисунок 121. Создание шаблона отчета. Определение отчетного периода

5. Далее укажите, для каких объектов будет создаваться отчет (см. рис. 122):

   - **Отчет для группы** – для клиентских компьютеров, входящих в состав группы администрирования.
   - **Отчет для набора клиентских компьютеров** – для набора клиентских компьютеров из состава логической сети.

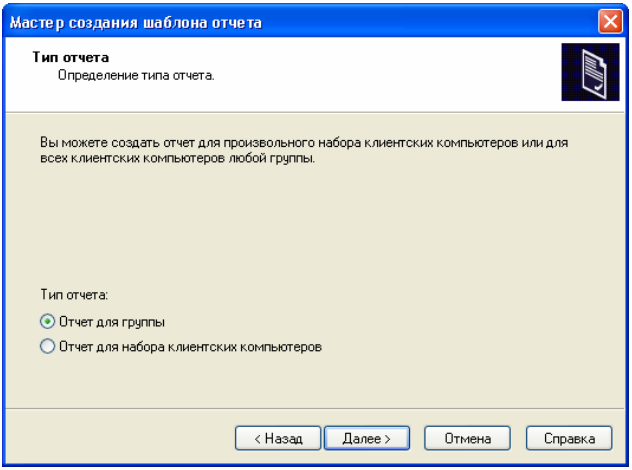

Рисунок 122. Создание шаблона отчета.
Выбор объектов для составления отчета

Если отчет может быть создан только для всей системы антивирусной защиты в целом, например, **Отчет о лицензионных ключах**, данный и следующий этапы отсутствуют.

6. После этого укажите группу либо выберите клиентские компьютеры, информация о которых должна входить в отчет (см. рис. 123), и завершите работу мастера.

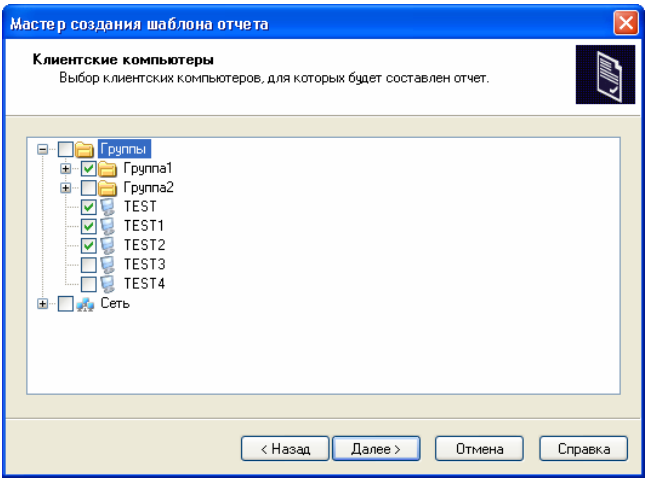

Рисунок 123. Создание шаблона отчета, выбор клиентских компьютеров

По окончании работы мастера сформированный шаблон отчета будет добавлен в состав узла **Отчеты** дерева консоли и представлен в панели результатов. Он может быть использован для создания и просмотра отчетов.

5.4.2. Просмотр и редактирование параметров шаблона отчета

Для просмотра параметров шаблона отчета и/или его изменения:

подключитесь к Серверу администрирования (см. п. 2.1 на стр. 12) и выберите в дереве консоли узел **Отчеты**. После этого в панели результатов будет представлен перечень сформированных шаблонов отчетов. Выберите нужный шаблон и воспользуйтесь командой **Свойства** контекстного меню или аналогичным пунктом в меню **Действие**.

В результате открывается окно настройки шаблона отчета **Свойства: <Имя шаблона отчета>** (см. рис. 124), состав закладок которого зависит от типа отчета.

На закладке **Общие** отображаются общие сведения о шаблоне. Вы можете:

- изменить название шаблона отчета;
- просмотреть название типа шаблона, его описание, дату и время создания и последнего изменения настроек;
- добавить в отчет данные с подчиненных Серверов администрирования (см. п. 5.4.4 на стр. 178);
- ограничить число отображаемых в отчете записей (см. п. 5.4.5 на стр. 179);
- установить флажок **Версия для печати**, чтобы сформированный отчет отображался в удобном для печати виде;
- включить использование данных с подчиненных Серверов администрирования с помощью гиперссылки **Настроить параметры для иерархии Серверов администрирования** (см. п. 5.4.4 на стр. 178).
- сформировать отчет по шаблону, нажав на кнопку **Создать отчет**.

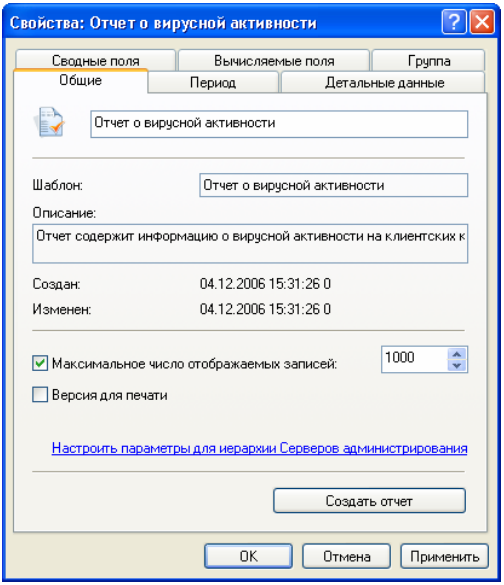

Рисунок 124. Окно настройки шаблона отчета.
Закладка **Общие**

На закладке **Период** задается временной интервал, за который составляется отчет. Ее параметры аналогичны параметрам в окне **Отчетный период** (см. рис. 121) в мастере создания шаблона отчета.

На закладке **Детальные данные** (см. рис. 125) определяются поля, составляющие таблицу детальных данных, включенных в отчет, порядок сортировки записей в них и настраиваются параметры фильтрации. Для формирования списка полей используйте кнопки **Добавить** и **Удалить**. Изменить очередность полей можно с помощью кнопок **Вверх** и **Вниз**. Чтобы изменить порядок сортировки в поле и задать фильтрацию, нажмите на кнопку **Изменить**. В открывшемся окне (см. рис. 126) произведите следующие настройки:

- чтобы задать порядок сортировки записей выбранного поля, установите флажок **Сортировать значения поля отчета** и выберите **По возрастанию** или **По убыванию**;
- для использования в поле фильтрации записей, установите флажок **Фильтровать значения поля** и в полях ниже задайте необходимые условия. Каждому полю отчета соответствует свой набор условий фильтрации.

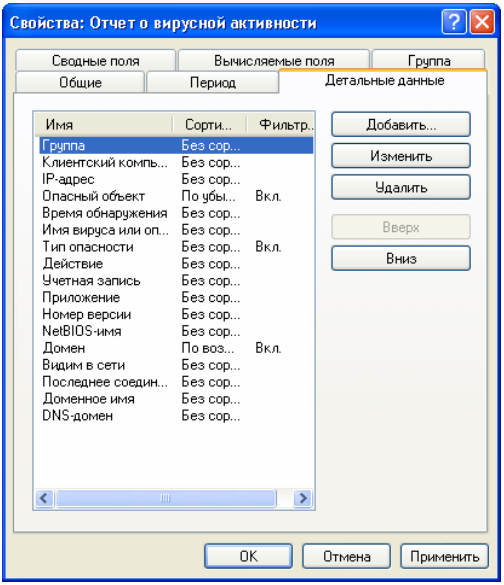

Рисунок 125. Окно настройки шаблона отчета.
Закладка **Детальные данные**

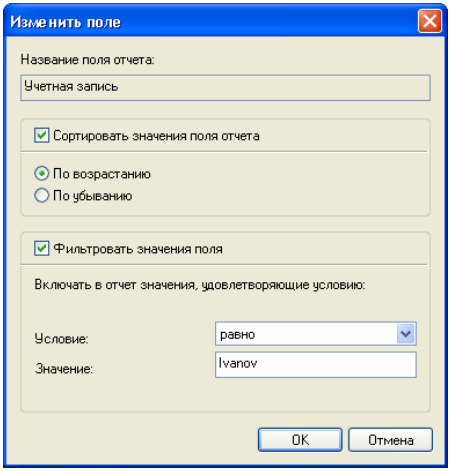

Рисунок 126. Выбор порядка сортировки поля отчета

На закладке **Сводные поля** (см. рис. 127) определяются поля, составляющие таблицу сводных данных, включаемых в отчет и порядок сортировки записей в них. Настройки этой закладки (за исключе-

нием фильтрации) аналогичны настройкам на закладке **Детальные данные** (см. рис. 125).

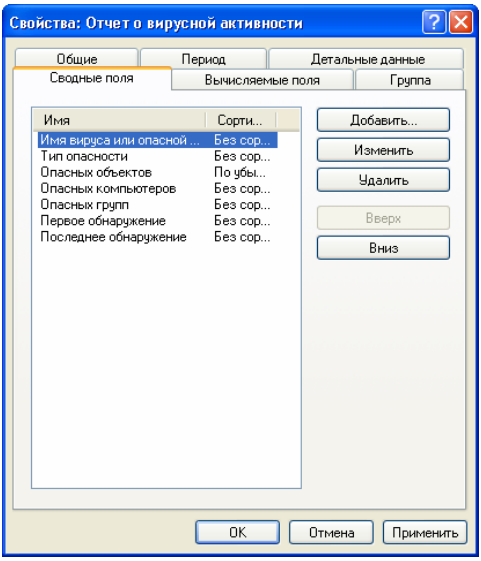

Рисунок 127. Окно настройки шаблона отчета.
Закладка **Сводные поля**

На закладке **Вычисляемые поля** (см. рис. 128) задаются вычисляемые (суммируемые) поля отчета. Чтобы удалить поле из шаблона отчета, выберите его в списке **Поля отчета** и нажмите на кнопку **Удалить**. Чтобы добавить поле в шаблон отчета, выберите его в списке **Доступные поля** и нажмите на кнопку **Добавить**.

На закладке **Группа / Клиентский компьютер** указываются группа или набор клиентских компьютеров, информация о которых включается в отчет. Ее параметры аналогичны параметрам соответствующего окна (см. рис. 123) в мастере создания шаблона отчета.

Для применения настроек следует нажать на кнопку **Применить** или **OK**.

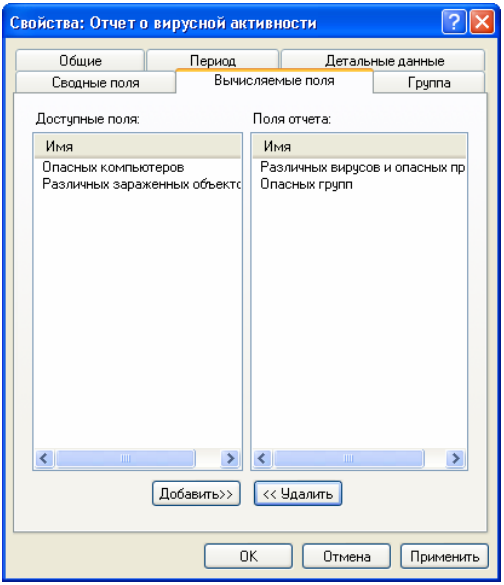

Рисунок 128. Окно настройки шаблона отчета.
Закладка **Вычисляемые поля**

5.4.3. Создание и просмотр отчета

Для создания отчета по шаблону:

подключитесь к Серверу администрирования (см. п. 2.1 на стр. 12) и выберите в дереве консоли узел **Отчеты**. После этого в панели результатов будет представлен перечень сформированных шаблонов отчетов. Выберите нужный шаблон и воспользуйтесь командой **Создать** контекстного меню или аналогичным пунктом в меню **Действие**. В результате откроется браузер, в главном окне которого будет отображен сформированный отчет. Его вид соответствует выбранному шаблону (см. рис. 129) и включает в себя:

- тип и название отчета, его краткое описание и отчетный период, а также информацию том, для какой группы компьютеров создан отчет;
- общие агрегированные показатели отчета (вычисляемые, суммируемые поля отчета);
- графическую диаграмму, наглядно отображающую наиболее характерные данные отчета;

- сводную таблицу данных, отображающих агрегированные показатели отчета;
- таблицу детальных данных отчета.

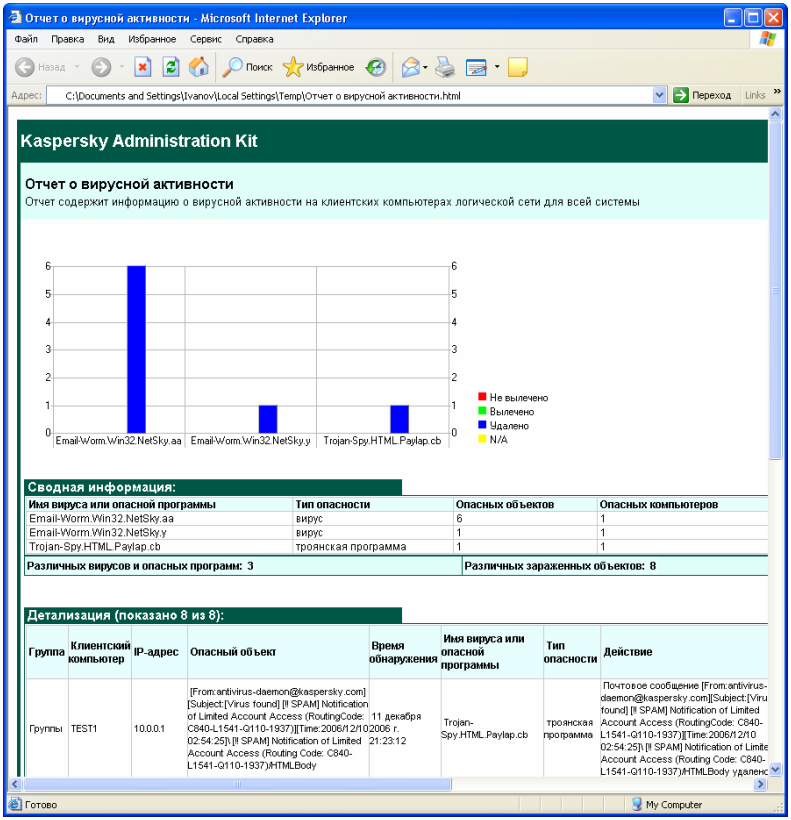

Рисунок 129. Просмотр отчета об уровне антивирусной защиты

5.4.4. Создание общих отчетов для подчиненных Серверов администрирования

Для того чтобы создать общий отчет, включающий в себя информацию с подчиненных Серверов:

1. Выберите необходимый шаблон отчета в узле **Отчеты** главного Сервера администрирования.
2. В контекстном меню выберите команду **Свойства** и перейдите на закладку **Общие** (см. рис. 124).
3. Щелкните по гиперссылке **Настроить параметры для иерархии Серверов администрирования** и в открывшемся окне (см. рис. 130):
   - установите флажок **Использовать данные с подчиненных Серверов администрирования**;
   - задайте глубину вложенности Серверов администрирования в соответствии с их иерархией в поле **Уровень вложенности**;
   - укажите нужное значение в поле **Время ожидания данных (минут)**. Если по истечении этого времени информация с подчиненного Сервера не получена, он считается недоступным (информация об этом будет содержаться в отчете).

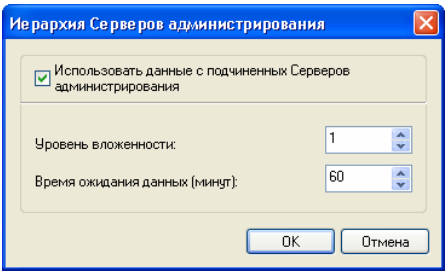

Рисунок 130. Окно **Иерархия Серверов администрирования**

4. Нажмите на кнопку **Создать отчет**.

В результате сформированный отчет отобразится в окне браузера.

5.4.5. Ограничение количества отображаемых в отчете записей

Для того чтобы задать максимальное количество отображаемых в отчете записей:

выберите необходимый шаблон отчета в узле **Отчеты** главного Сервера администрирования. В контекстном меню выберите команду **Свойства** и на закладке **Общие** (см. рис. 124) установите флажок **Максимальное число отображаемых записей**. В поле справа введите необходимое значение.

Для применения настроек нажмите на кнопку **Применить** или **OK**.

5.5. Отслеживание состояния антивирусной защиты с помощью информации в системном реестре

Для просмотра состояния антивирусной защиты на клиентском компьютере с помощью информации, записанной в системный реестр Агентом администрирования:

1. Откройте системный реестр клиентского компьютера (например, локально с помощью команды **regedit** в меню **Пуск / Выполнить**).
2. Перейдите в раздел:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\
   Components\34\1103\1.0.0.0\Statistics\AVState
   ```

Состояние антивирусной защиты соответствует значению ключей, описанных в таблице 1.

Таблица 1

Ключ (Тип данных)	Значение	Описание
Protection_AvInstalled (REG_DWORD)	отлично от 0	На компьютере установлено антивирусное приложение[4].
Protection_AvRunning (REG_DWORD)	отлично от 0	Постоянная защита компьютера включена.
Protection_HasRtp (REG_DWORD)	отлично от 0	Установлен компонент постоянной защиты.
Protection_RtpState (REG_DWORD)		Состояние постоянной защиты:
	0	• неизвестно;
	1	• не включена;
	2	• приостановлена;
	3	• запускается;
	4	• включена[5];
	5	• включена, высокий уровень (максимальная защита);
	6	• включена, низкий уровень (максимальная скорость);
	7	• включена, рекомендуемые настройки;
	8	• включена, настройки пользователя;
	9	• сбой в работе.

[4] Антивирусным считается приложение, содержащие антивирусные базы (или базы сигнатур угроз).

[5] Для приложений, не поддерживающих подробные состояния антивирусной защиты (значения 5–8).

Ключ (Тип данных)	Значение	Описание
Protection_LastFscan (REG_SZ)	ДД-ММ-ГГГГ ЧЧ-ММ-СС	Дата и время (в формате UTC) последней полной проверки.
Protection_BasesDate (REG_SZ)	ДД-ММ-ГГГГ ЧЧ-ММ-СС	Дата и время (в формате UTC) выпуска антивирусных баз (баз сигнатур угроз)[6].
Protection_LastConnected (REG_SZ)	ДД-ММ-ГГГГ ЧЧ-ММ-СС	Дата и время (в формате UTC) последнего соединения с Сервером администрирования.

5.6. Поиск компьютеров

5.6.1. Поиск компьютеров

Для того чтобы найти компьютер или группу компьютеров, соответствующих заданным критериям,

в контекстном меню узла Сервер администрирования, папки **Сеть** или группы администрирования выберите пункт **Найти компьютер**. В открывшемся окне вы можете задать критерии поиска на следующих закладках: **Сеть**, **Приложение**, **Статус компьютера**, **Антивирусная защита** и **Стороннее приложение**.

На закладке **Сеть** (см. рис. 131) вы можете указать следующие критерии поиска:

- **Имя компьютера** в логической сети.
- **Имя компьютера в Windows-сети**.
- **Домен**. Укажите домен, к которому принадлежит клиентский компьютер.
- **Диапазон IP-адресов**. Укажите начальный и конечный IP-адреса.
- **Время последнего соединения с Сервером администрирования**. Укажите временной интервал последнего соединения клиентского компьютера с Сервером администрирования.

[6] Если установлено несколько антивирусных приложений, то указываются дата и время самых новых антивирусных баз или баз сигнатур угроз.

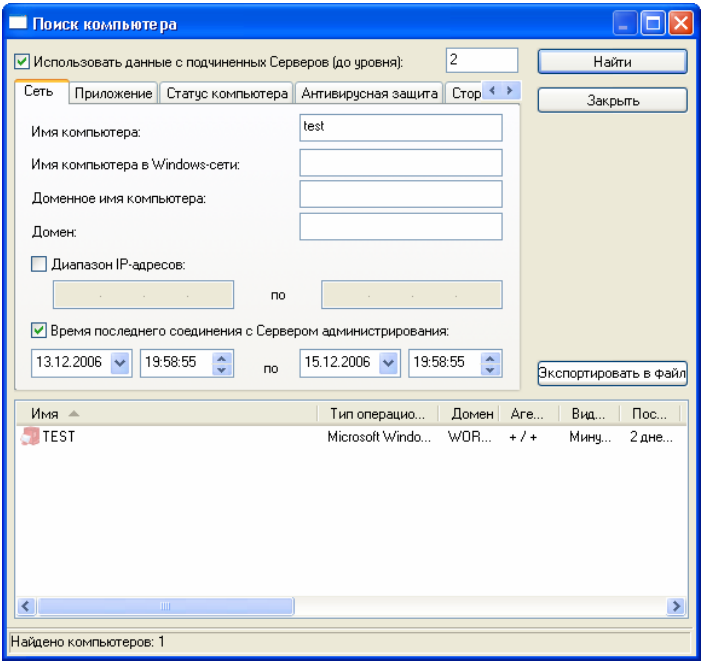

Рисунок 131. Поиск компьютера. Закладка **Сеть**

На закладке **Приложение** (см. рис. 132) вы можете указать следующие критерии поиска:

- **Имя приложения**. Укажите название приложения, установленного на клиентском компьютере. Для этого выберите из раскрывающегося списка нужное значение. В списке представлены названия только тех приложений, для которых на рабочее место администратора установлены плагины управления.
- **Версия приложения**. Укажите версию приложения, установленного на клиентском компьютере.
- **Время последнего обновления**. Укажите временной интервал последнего обновления антивирусных баз и модулей приложений, установленных на клиентском компьютере.
- **Версия операционной системы**. Укажите версию установленной на компьютере версию операционной системы.

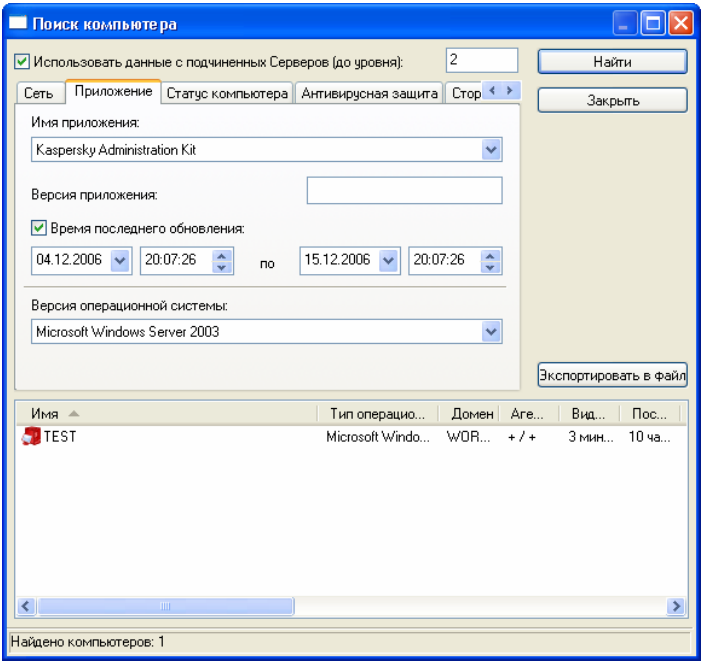

Рисунок 132. Поиск компьютера. Закладка **Приложение**

На закладке **Статус компьютера** (см. рис. 133) вы можете указать следующие критерии поиска:

- **Статус компьютера**. Выберите текущий статус компьютера: **OK**, **Критический** или **Предупреждение**.
- **Описание статуса компьютера**. Установите флажки рядом с условиями, на основании которых клиентскому компьютеру присвоен выбранный статус.
- **Статус постоянной защиты**. Выберите из списка текущий статус постоянной антивирусной защиты клиентского компьютера.

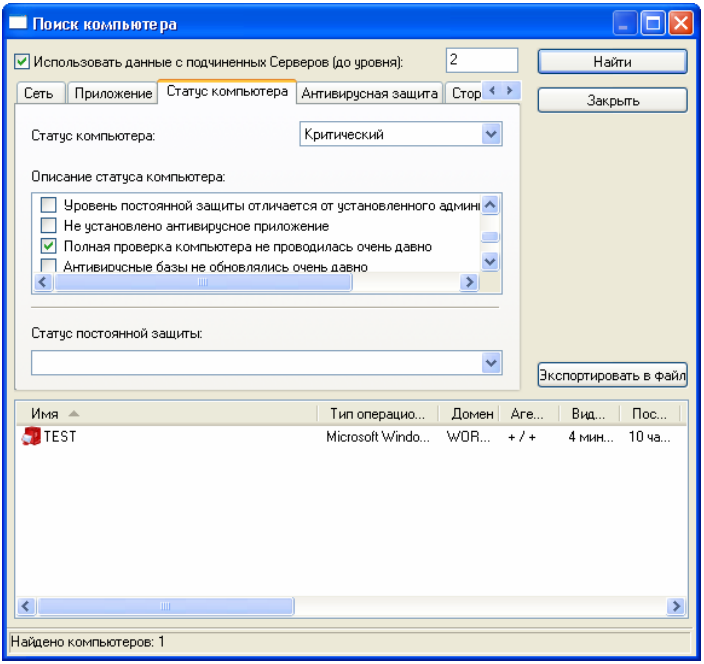

Рисунок 133. Поиск компьютера. Закладка **Статус компьютера**

На закладке **Антивирусная защита** (см. рис. 134) вы можете указать следующие критерии поиска:

- **Дата антивирусных баз**. Укажите дату выпуска антивирусных баз.
- **Количество записей в антивирусных базах**.
- **Время последней полной проверки**. Укажите временной интервал, в течение которого последний раз проводилась полная проверка клиентского компьютера.
- **Количество найденных вирусов**.

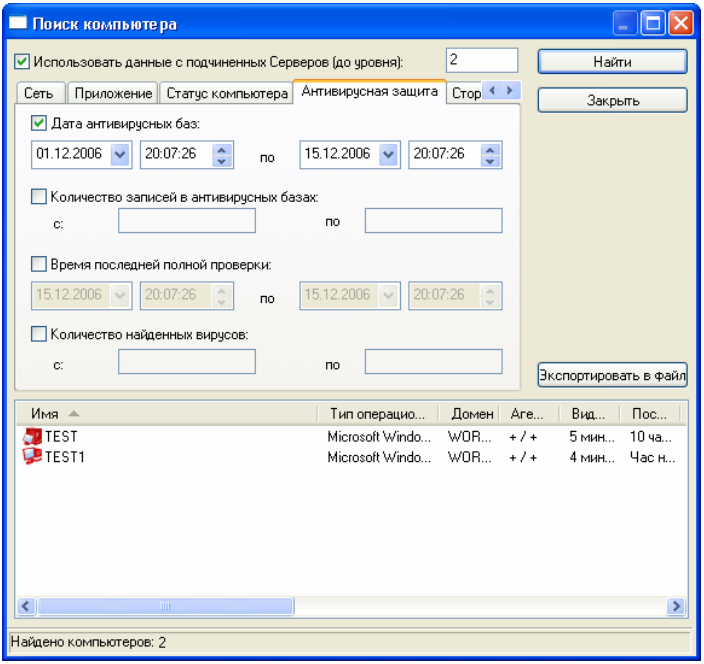

Рисунок 134. Поиск компьютера. Закладка **Антивирусная защита**

На закладке **Стороннее приложение** (см. рис. 135) выберите в списке название одного из обнаруженных в сети сторонних приложений.

Для того, что бы при поиске учитывались информация о компьютерах, хранящаяся на подчиненных Серверах администрирования, установите флажок **Использовать данные с подчиненных серверов (до уровня)**. После этого укажите уровень вложенности, включая который будет осуществляться поиск.

Задав критерии поиска, нажмите на кнопку **Найти**, и в нижней части окна отобразится список компьютеров, соответствующих указанным критериям. В этом списке будет также приведена общая информация о найденных компьютерах.

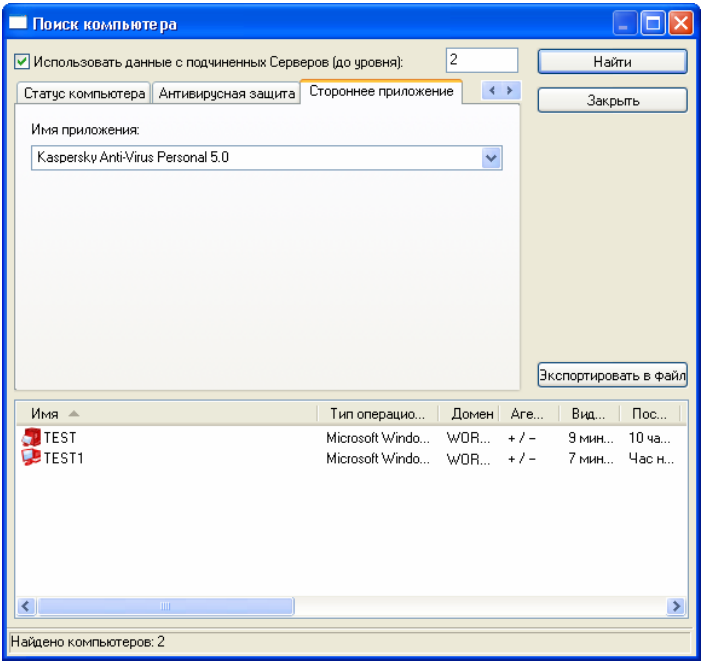

Рисунок 135. Поиск компьютера. Закладка **Стороннее приложение**

5.6.2. Сохранение результатов поиска компьютеров в текстовом файле

Для того чтобы сохранить результаты поиска в текстовом файле,

нажмите на кнопку **Экспортировать в файл** в окне **Поиск компьютера** (см. рис. 134) и в открывшемся окне укажите файл для сохранения.

5.7. Выборки компьютеров

5.7.1. Создание выборки компьютеров

Чтобы создать выборку компьютеров:

1. Выберите в дереве консоли узел **Выборки компьютеров**, откройте контекстное меню и воспользуйтесь командой **Создать/ Новая выборка** или аналогичным пунктом в меню **Действие**.
2. В открывшемся окне введите имя выборки (см. рис. 136) и нажмите на кнопку **ОК**.

В результате в дереве консоли в узле **Выборки компьютеров** будет создана новая папка с именем, заданным для выборки. Для того чтобы в состав выборки были добавлены компьютеры, настройте параметры выборки.

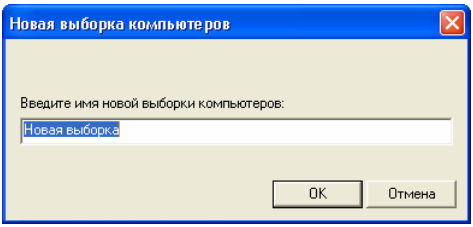

Рисунок 136. Создание выборки компьютеров

5.7.2. Настройка выборки компьютеров

Чтобы настроить выборку компьютеров:

1. Выберите в дереве консоли или в панели результатов нужную выборку компьютеров и воспользуйтесь командой **Свойства** контекстного меню или аналогичным пунктом в меню **Действие**.
2. В результате открывается окно настройки выборки компьютеров (см. рис. 137), состоящее из закладок: **Общие**, **Сеть**, **Приложение**, **Статус компьютера**, **Антивирусная защита** и **Стороннее приложение**.

На закладке **Общие** (см. рис. 137) вы можете изменить имя выборки и определить область поиска компьютеров, выбрав один из вариантов:

- **Поиск в группах и в сети** – поиск будет осуществляться среди всех компьютеров сети, как входящих в состав логической сети, так и не включенных в нее.
- **Поиск в группах** – поиск только среди клиентских компьютеров логической сети.
- **Поиск в сети** – поиск среди компьютеров, не входящих в логическую сеть.

Для того, что бы при поиске учитывались информация о компьютерах, хранящаяся на подчиненных Серверах администрирования, установите флажок **Использовать данные с подчиненных серверов (до уровня)**. После этого укажите уровень вложенности, включая который будет осуществляться поиск.

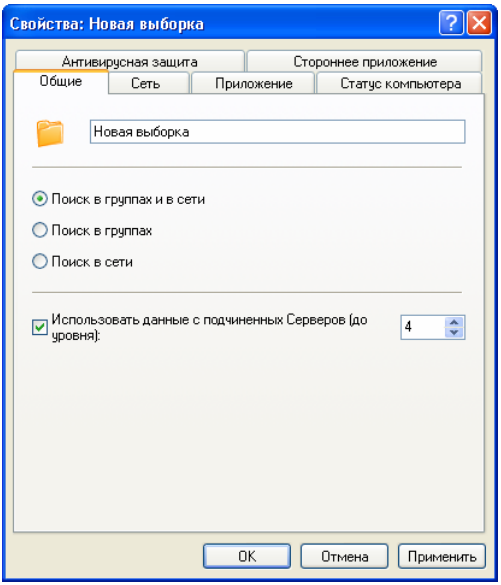

Рисунок 137. Настройка выборки компьютеров. Закладка **Общие**

На закладке **Сеть** (см. рис. 138) определите атрибуты компьютеров, которые должны войти в выборку. Вы можете использовать следующие параметры:

- имя компьютера в логической сети;
- имя компьютера в Windows-сети;
- домен, в состав которого должны входить компьютеры;
- диапазон IP-адресов компьютеров; для этого установите флажок **Диапазон IP-адресов** и введите начальный и конечный IP-адреса;
- время последнего соединения клиентского компьютера с Сервером администрирования; для этого установите флажок **Время последнего соединения с Сервером администрирования** и укажите начальную и конечную дату и время интервала в полях **с** и **по**.
- время появления новых компьютеров в сети; для этого установите флажок **Новые обнаруженные при опросе сети компьютеры** и укажите период в днях в поле **Период обнаружения (дни)**.

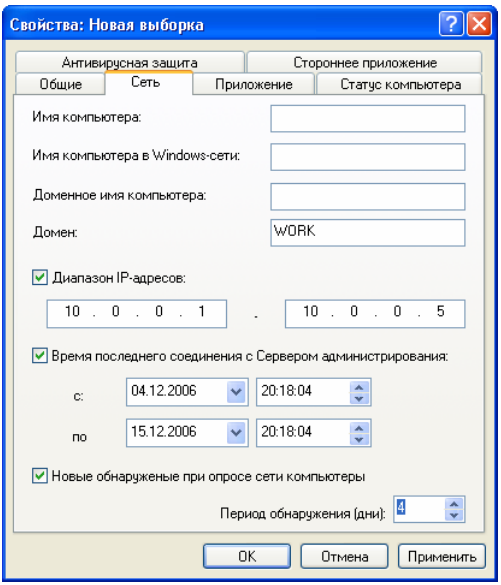

Рисунок 138. Настройка выборки компьютеров. Закладка **Сеть**

На закладке **Приложение** (см. рис. 139) укажите, какое приложение «Лаборатории Касперского» должно быть установлено на компьютерах. Вы можете использовать следующие параметры:

- название приложения; выберите из раскрывающегося списка нужное значение. В списке представлены названия только тех приложений, для которых на рабочее место администратора установлены плагины управления.
- номер версии приложения;
- время последнего обновления приложения; для этого установите флажок **Время последнего обновления** и укажите начальную и конечную дату и время интервала в полях **с** и **по**;
- версия операционной системы, установленной на компьютере.

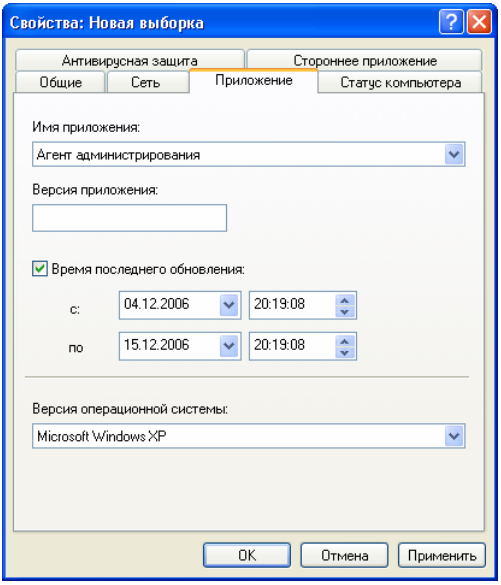

Рисунок 139. Настройка выборки компьютеров. Закладка **Приложения**

На закладке **Антивирусная защита** (см. рис. 140) определите критерии оценки состояния антивирусной защиты на компьютерах, которые должны войти в выборку. Вы можете указать:

- дату создания используемых приложениями антивирусных баз; для этого установите флажок **Дата антивирусных баз** и укажите временной интервал, соответствующий дате выпуска антивирусных баз;
- количество записей в используемых приложениями антивирусных базах; для этого установите флажок **Количество записей в антивирусных базах** и укажите нижнее и верхнее значения требуемой величины;
- время последней полной проверки компьютера одним из антивирусных приложений «Лаборатории Касперского»; для этого установите флажок **Время последней полной проверки** и укажите временной интервал, в течение которого была выполнена проверка;
- количество обнаруженных на компьютере вирусов; для этого установите флажок **Количество найденных вирусов** и укажите нижнее и верхнее значения требуемой величины.

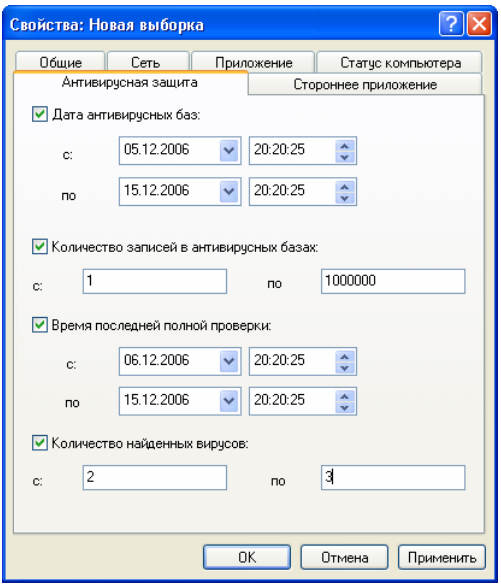

Рисунок 140. Настройка выборки компьютеров. Закладка **Антивирусная защита**

На закладке **Статус компьютера** (см. рис. 141) определите параметры, характеризующие статус компьютеров, и статус задачи постоянной защиты на компьютерах. Для этого:

- из раскрывающегося списка **Статус компьютера** выберите нужное значение: **OK**, **Критический** или **Предупреждение**;
- в списке **Описание статуса компьютера** выберите условия, на основании которых компьютеру был присвоен статус;
- в списке **Статус постоянной защиты** выберите значение статуса постоянной защиты, выполняющейся на компьютерах, входящих в выборку.

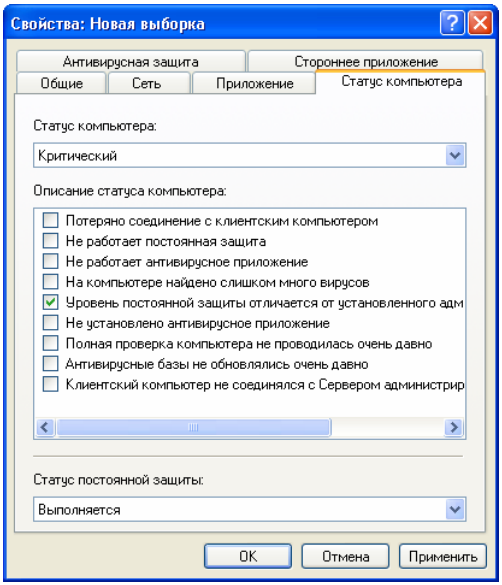

Рисунок 141. Настройка выборки компьютеров. Закладка **Статус компьютера**

На закладке **Стороннее приложение** (см. рис. 141) укажите стороннее приложение, установлено е на компьютере.

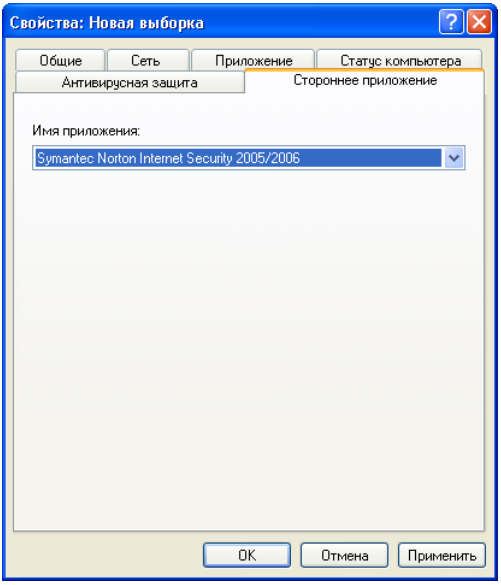

Рисунок 142. Настройка выборки компьютеров.
Закладка **Стороннее приложение**

3. По окончании настройки для применения параметров выборки нажмите на кнопку **Применить** или **OK**.

5.8. Отслеживание вирусных эпидемий

5.8.1. Включение механизма распознавания вирусной атаки

*Для того чтобы в логической сети фиксировалось событие **Вирусная атака** и выполнялось уведомление о нем:*

1. Выберите в дереве консоли узел, соответствующий нужному Серверу администрирования, откройте контекстное меню и воспользуйтесь командой **Свойства** или аналогичным пунктом в меню **Действие**. В результате открывается диалоговое окно **Свойства: <Имя Сервера администрирования>**.

2. На закладке **Вирусная атака** (см. рис. 70) установите флажки рядом с названиями нужных типов антивирусных приложений и укажите для них значения параметров, определяющих порог вирусной активности. Превышение этого порога будет считаться повышением вирусной активности и возникновением события **Вирусная атака**.

3. На закладке **События** (см. рис. 66) при настройке событий с уровнем важности **Критическое событие** выберите тип событий **Вирусная атака** и укажите значения параметров оповещения.

4. В политиках для всех антивирусных приложений на закладке **События** (см. рис. 41) при настройке событий с уровнем важности **Критическое событие** выберите тип событий **Найден вирус** или **Обнаружение вирусов, червей, троянских и хакерских программ** и на закладке **Регистрация** (см. рис. 47) в окне свойств этого события установите флажок **На Сервере администрирования в течение (дней)**.

При подсчете событий **Найден вирус** и **Обнаружение вирусов, червей, троянских и хакерских программ** учитывается только информация с клиентских компьютеров главного Сервера администрирования. Для каждого подчиненного Сервера событие **Вирусная атака** настраивается индивидуально.

5.8.2. Смена политики для приложения при регистрации события Вирусная атака

*Для того чтобы при возникновении события **Вирусная атака** выполнялась смена текущей политики для приложения:*

в окне настройки политики для приложения на закладке **Общие** (см. рис. 37) должен быть установлен флажок **Активировать политику по событию** и выбрано событие **Вирусная атака**.

5.9. Резервное копирование и восстановление данных Сервера администрирования

5.9.1. Создание резервной копии данных Сервера администрирования

Для создания резервной копии данных Сервера администрирования:

- через Консоль администрирования создайте и запустите глобальную задачу **резервного копирования данных** (см. п. 5.9.3 на стр. 196)

  либо

- на компьютере, где установлен Сервер администрирования, запустите утилиту **klbackup** с необходимым набором ключей из командной строки (см. п. 5.9.4 на стр. 199). Данная утилита входит в состав дистрибутива Kaspersky Administration Kit и после установки компонента Сервер администрирования располагается в корне каталога установки.

5.9.2. Восстановление данных Сервера администрирования из резервной копии

Для восстановления данных Сервера администрирования:

на компьютере, где установлен новый Сервер администрирования, запустите утилиту **klbackup** с необходимым набором ключей из командной строки (см. п. 5.9.4 на стр. 199).

Название баз данных старого и нового SQL-серверов должны совпадать.

5.9.3. Задача резервного копирования данных

5.9.3.1. Создание задачи резервного копирования данных Сервера администрирования

Для создания задачи резервного копирования данных Сервера администрирования:

1. 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 (см. п. 3.2.1 на стр. 111).
2. Создайте глобальную задачу (см. п. 3.2.2 на стр. 121). При ее создании укажите следующие значения параметров:
   - В качестве приложения, для которого формируется задача (см. рис. 143), выберите **Kaspersky Administration Kit**; в качестве типа задачи – **Резервное копирование Сервера администрирования**.

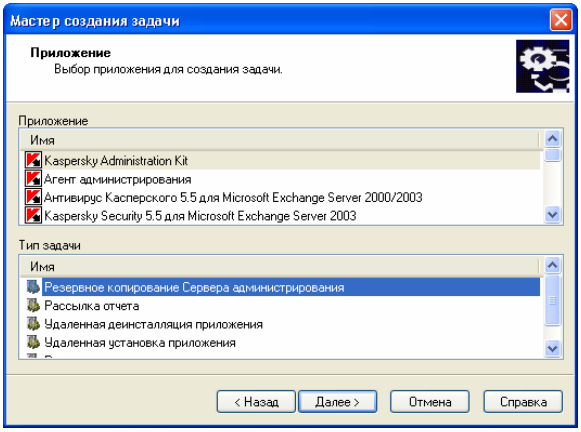

Рисунок 143. Создание задачи резервного копирования. Выбор приложения и типа задачи

- На этапе настройки параметров задачи (см. рис. 144) укажите:
  - каталог для сохранения резервной копии данных – резервное хранилище; он должен быть доступен для записи, как для Сервера администрирования, так и для SQL-сервера, на котором размещается база данных Сервера администрирования;
  - пароль, который будет использоваться для шифрования/ расшифровки сертификата Сервера администрирования; в поле ниже повторите пароль.

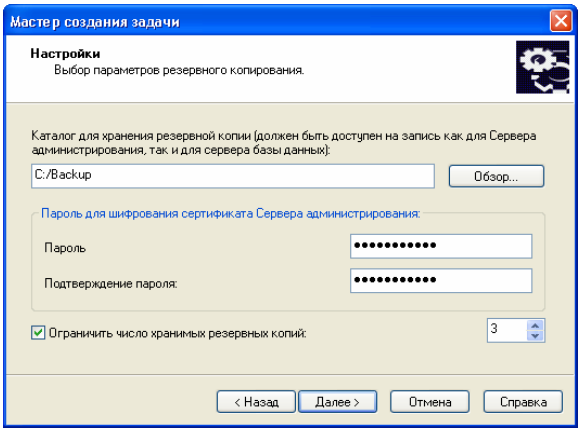

Рисунок 144. Создание задачи резервного копирования. Настройка параметров

Резервная копия данных создается в указанном каталоге в виде подкаталога с именем, отображающим текущую дату и время операции в формате **klbackup ГГГГ-ММ-ДД # ЧЧ-ММ-СС** (где **ГГГГ** – год, **ММ** – месяц, **ДД** – день, **ЧЧ** – час, **ММ** – минуты, **СС** – секунды). В нем сохраняются:

- информационная база Сервера администрирования (политики, задачи, настройки приложения, сохраненные на Сервере администрирования события);
- конфигурационная информация о структуре логической сети и клиентских компьютерах;
- хранилище дистрибутивов программ для удаленной установки (содержимое папки Packages);
- сертификат Сервера администрирования.

- По необходимости ограничьте количество хранящихся резервных копий – максимальное количество подкаталогов, которые могут одновременно размещаться в резервном хранилище. Для этого установите флажок **Ограничить число хранимых резервных копий** и укажите нужное значение. Если достигнуто наложенное ограничение, при создании очередной резервной копии будет удалена предыдущая, наиболее старая копия, размещенная в резервном хранилище.

5.9.3.2. Настройка задачи резервного копирования данных Сервера администрирования

Для настройки задачи резервного копирования данных Сервера администрирования:

1. Выберите в панели результатов для узла **Глобальные задачи** нужную задачу, откройте контекстное меню и выберите команду **Свойства** или воспользуйтесь аналогичным пунктом в меню **Действие**.
2. В открывшемся окне выберите закладку **Настройки** (см. рис. 145). На ней представлены те же параметры, что определялись при создании задачи:
   - каталог для сохранения резервной копии данных;
   - пароль, который будет использоваться для шифрования/ расшифровки сертификата Сервера администрирования; в поле ниже повторите пароль;
   - ограничение на количество резервных копий.

   Установите нужные значения параметров.
3. После окончания настройки нажмите на кнопку **Применить** или **ОК**.

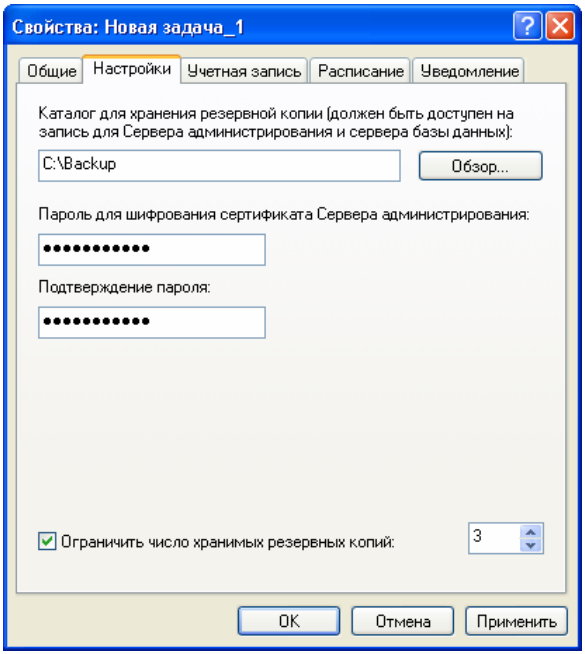

Рисунок 145. Настройка параметров задачи резервного копирования

5.9.4. Утилита резервного копирования данных

5.9.4.1. Создание резервной копии данных Сервера администрирования вручную. Утилита *klbackup*

Для создания резервной копии данных Сервера администрирования вручную:

на компьютере, где установлен Сервер администрирования, запустите утилиту **klbackup** с необходимым набором ключей из командной строки.

Синтаксис утилиты:

- **klbackup [-logfile LOGFILE][7] -path BACKUP_PATH [-use_ts]|[-restore] -savecert PASSWORD**

Описание ключей:

- **-logfile LOGFILE** – сохранить отчет о выполнении копирования/ восстановления данных Сервера администрирования.
- **-path BACKUP_PATH** – сохранить информацию в каталоге **BACKUP_PATH**/ для восстановления использовать данные из каталога **BACKUP_PATH** (обязательный параметр).

  Учетная запись сервера базы данных и утилита **klbackup** должны обладать правами на модификацию каталога **BACKUP_PATH**.

- **-use_ts** – при сохранении данных копировать информацию во вложенной в каталог **BACKUP_PATH** папку с именем, отображающим текущую дату и время операции в формате **klbackup YYYY-MM-DD # HH-MM-SS**. Если ключ не задан, информация сохраняется в корне каталога **BACKUP_PATH**.

  При попытке сохранения информации в каталог, в котором уже есть резервная копия, появится сообщение об ошибке, и обновления информации не произойдет.

  Наличие ключа **-use_ts** позволяет вести архив данных Сервера администрирования. Например, если ключом **-path** был задан каталог **C:\KLBackups**, то в папке **klbackup 2006-06-19 # 11-30-18** была сохранена информация о состоянии Сервера администрирования на дату 19 июня 2006 года 11 часов, 30 минут, 18 секунд.

- **-restore** – выполнить восстановление данных Сервера администрирования. Восстановление данных осуществляется на основании информации, представленной в каталоге **BACKUP_PATH**. Если ключ отсутствует, производится резервное копирование данных в каталог **BACKUP_PATH**.
- **-savecert PASSWORD** – сохранить / восстановить сертификат Сервера администрирования; для шифрования/ расшифровки сертификата использовать пароль, заданный параметром **PASSWORD**.

[7] В квадратных скобках приводятся необязательные ключи.

Полное восстановление данных системы администрирования требует обязательного сохранения сертификата Сервера администрирования. Параметр **PASSWORD** обязательно должен быть определен.

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

Если при восстановлении данных Сервера администрирования изменился путь к папке общего доступа, следует проверить корректность работы задач, в которых она используется (задачи обновления, удаленной установки), и, в случае необходимости, внести изменения в их настройки.

5.9.4.2. Перенос Сервера администрирования на другой компьютер

Для переноса Сервера администрирования на другой компьютер:

1. Создайте резервную копию данных Сервера администрирования.
2. Установите новый Сервер администрирования.

   Для упрощения переноса логической сети желательно чтобы адрес нового Сервера совпадал с адресом старого. Адрес (*имя компьютера в Windows-сети* или *IP-адрес*) указывается в настройках Агента администрирования в параметрах подключения к Серверу.

3. На новом Сервере администрирования выполните восстановление данных старого Сервера из резервной копии.
4. Если адрес (имя компьютера в Windows-сети или IP-адрес) нового и старого Серверов не совпадают, для подключения клиентских компьютеров к новому Серверу, на старом Сервере создайте задачу **смены Сервера администрирования** для группы **Группы**.

   Если адреса совпадают, задачу смены Сервера создавать не нужно, подключение будет выполнено по указанному в параметрах адресу Сервера без каких-либо проблем.
5. Удалите старый Сервер администрирования.

5.9.4.3. Перенос базы Сервера администрирования на другой компьютер

Для переноса Сервера администрирования на другой компьютер и смены базы данных Сервера администрирования:

1. Создайте резервную копию данных Сервера администрирования.
2. Установите новый SQL-сервер.

Для корректного переноса информации база данных на новом SQL-сервере должна иметь те же схемы сопоставления (collation), что и на предыдущем SQL-сервере.

3. Установите новый Сервер администрирования. Название баз данных старого и нового SQL-серверов должны совпадать.

Для упрощения переноса логической сети желательно чтобы адрес нового Сервера совпадал с адресом старого. Адрес (*имя компьютера в Windows-сети* или *IP-адрес*) указывается в настройках Агента администрирования в параметрах подключения к Серверу.

4. На новом Сервере администрирования выполните восстановление данных старого Сервера из резервной копии.
5. Если адрес (имя компьютера в Windows-сети или IP-адрес) нового и старого Серверов не совпадают, для подключения клиентских компьютеров к новому Серверу, на старом сервере создайте задачу **смены Сервера администрирования** для группы **Группы**.

   Если адреса совпадают, задачу смены Сервера создавать не нужно, подключение будет выполнено без каких-либо проблем.
6. Удалите старый Сервер администрирования.

5.10. Настройка совместной работы с Cisco Network Admission Control (NAC)

Для того чтобы настроить соответствие между статусами Cisco NAC и условиями антивирусной защиты:

1. В дереве консоли выберите узел, соответствующий нужному Серверу администрирования, откройте контекстное меню и воспользуйтесь командой **Свойства** или аналогичным пунктом в меню **Действие**. В результате откроется диалоговое окно **Свойства: <Имя Сервера администрирования>**.
2. Перейдите на закладку **Cisco NAC** (см. рис. 72).
3. В верхнем поле выберите один из статусов компьютера Cisco NAC: **Healthy**, **Checkup**, **Quarantine** или **Infected**.
4. Установите флажки рядом с соответствующими этому статусу условиями антивирусной защиты. При необходимости измените пороговые значения условий (подробнее см. п. 3.1.2.2 на стр. 94).
5. В поле **Номер PVS-порта** укажите номер порта Postrure Validation Server, через который идет обмен данными с сервером Cisco.
6. После окончания настройки нажмите на кнопку **Применить** или **ОК**.

ПРИЛОЖЕНИЕ А. КАК ОБРАТИТЬСЯ В СЛУЖБУ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

В случае возникновения сбоев в работе приложения вы можете обратиться в Службу технической поддержки «Лаборатории Касперского».

Прежде всего, убедитесь, не описан ли метод решения вашей проблемы в документации или в разделе **Сервис/ Сайт технической поддержки** на сайте «Лаборатории Касперского» (www.kaspersky.ru).

Если вы не нашли решения вашей проблемы в документации и Базе знаний на веб-сайте, рекомендуем вам обратиться в Службу технической поддержки «Лаборатории Касперского».

Для решения срочных проблем позвоните по телефонам, указанным в разделе С.2 на стр. 225. Поддержка пользователей по телефону осуществляется в круглосуточном режиме на русском, английском, французском и немецком языках. Обратите внимание, что для получения помощи вы должны иметь статус зарегистрированного пользователя и сообщить сотруднику Службы технической поддержки ваш регистрационный номер (при покупке коробочного варианта продукта) либо информацию по вашему заказу (при покупке продукта через интернет).

Для того чтобы отправить письмо о сбоях в работе программы в Службу технической поддержки,

откройте веб-сайт «Лаборатории Касперского» (www.kaspersky.ru) и перейдите в раздел **Сервис/ Сайт технической поддержки / Запрос в службу технической поддержки**.

На открывшейся странице заполните форму запроса в Службу технической поддержки. В первом окне формы вам нужно указать информацию о возникшей проблеме и лицензионные данные:

- В поле **Тип запроса** укажите в раскрывающемся списке именно ту проблему, которая вас беспокоит в работе приложения.
- Выберите **Kaspersky Administration Kit** в качестве имени продукта «Лаборатории Касперского» и детально опишите возникающую проблему в поле **Детальное содержание вашего запроса**.

- Выберите тип регистрации программы, работающей под управлением Kaspersky Administration Kit (например, Антивирус Касперского 5.0 для Windows Workstations). Для этого укажите **лицензионный ключ**, если вы приобретали продукт в коробке и устанавливали лицензионный ключ с дискеты, или **онлайн-заказ**, если вы покупали программу в интернет-магазине.
- В поле **Серийный номер лицензии или онлайн-заказа** введите серийный номер лицензии программы, работающей под управлением Kaspersky Administration Kit. Номер лицензии можно посмотреть в свойствах лицензионного ключа в узле **Лицензионные ключи**.
- Введите адрес вашей электронной почты в поле **Ваш электронный адрес**.
- Нажмите на кнопку **Далее**.

В следующем окне формы укажите следующую информацию:

- Укажите ваши координаты в разделе **Контактная информация**, чтобы мы могли с вами связаться и как можно быстрее помочь разрешить возникшую проблему.
- Введите специальный числовой код, отображаемый в разделе **Защита от автоматической регистрации**, в поле, расположенное рядом с ним.

По окончании нажмите на кнопку **Отправить запрос**.

ПРИЛОЖЕНИЕ В. 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.

A

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.

B

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.

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

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.

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

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.

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.

K

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 С. ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

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

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

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

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

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

С.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 дозвона 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 потребуется их восстановление;
- *изоляция подозрительных объектов* в специальном хранилище;
- *оповещения о событиях* в работе программного продукта администратора системы;
- *ведение детальных отчетов*;
- *автоматическое обновление баз* программного продукта.

Kaspersky Open Space Security

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

Программный продукт включает в себя четыре продукта:

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

Рассмотрим подробнее каждый продукт.

Kaspersky WorkSpace Security – это 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.

С.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