Kaspersky Administration Kit 8.0

Руководство администратора

ВЕРСИЯ ПРОГРАММЫ: 8.0 КРИТИЧЕСКОЕ ИСПРАВЛЕНИЕ 2

Уважаемый пользователь!

Спасибо за то, что выбрали наш продукт. Мы надеемся, что этот документ поможет вам в работе и ответит на большинство возникающих вопросов.

Документ может быть изменен без предварительного уведомления. Последнюю версию документа вы можете найти на сайте «Лаборатории Касперского» по адресу http://www.kaspersky.ru/docs.

Дата редакции документа: 15.10.2010

http://www.kaspersky.ru
http://support.kaspersky.ru

Лицензионное соглашение ЗАО «Лаборатория Касперского» с конечным пользователем о предоставлении неисключительного права на использование программного обеспечения.

Исключительные права на Kaspersky Administration Kit (далее Программное Обеспечение) принадлежат ЗАО «Лаборатория Касперского».

Нажатие Вами кнопки подтверждения согласия в окне с текстом Лицензионного соглашения при установке Программного Обеспечения означает Ваше безоговорочное согласие с условиями настоящего Лицензионного соглашения. Если Вы не согласны с условиями настоящего Лицензионного соглашения, Вы должны прервать установку Программного Обеспечения.

Использовать Программное Обеспечение, распространяемое без выплаты вознаграждения, для осуществления управления корпоративными программными продуктами ЗАО «Лаборатория Касперского», описанными в документе «Руководство по внедрению», в том числе для их удаленной установки, управления лицензиями, настройки и мониторинга антивирусной защиты имеют право только пользователи корпоративных программных продуктов ЗАО «Лаборатория Касперского», согласившиеся с условиями Лицензионного соглашения, сопровождающего корпоративные программные продукты ЗАО «Лаборатория Касперского».

Пользователи корпоративных программных продуктов ЗАО «Лаборатория Касперского», согласившиеся с условиями Лицензионного соглашения, сопровождающего корпоративные программные продукты, также имеют право на техническую поддержку Программного Обеспечения по телефону и/или через интернет.

Служба технической поддержки: http://support.kaspersky.com

Запрещается декомпилировать, дизассемблировать, модифицировать Программное Обеспечение или выполнять производные работы, основанные на Программном Обеспечении, целиком или частично, за исключением случаев, предусмотренных применимым законодательством.

ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПОСТАВЛЯЕТСЯ «КАК ЕСТЬ». ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО» НЕ ДАЕТ НИКАКИХ ГАРАНТИЙ НА ЕГО ИСПОЛЬЗОВАНИЕ ИЛИ ПРОИЗВОДИТЕЛЬНОСТЬ, ЗА ИСКЛЮЧЕНИЕМ ГАРАНТИЙ, УСЛОВИЙ, ПРЕДСТАВЛЕНИЙ ИЛИ ПОЛОЖЕНИЙ, СТЕПЕНЬ КОТОРЫХ НЕ МОЖЕТ БЫТЬ ИСКЛЮЧЕНА ИЛИ ОГРАНИЧЕНА ПРИМЕНЯЕМЫМ ЗАКОНОДАТЕЛЬСТВОМ. ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО» И ПАРТНЕРЫ НЕ ДАЮТ НИКАКИХ ГАРАНТИЙ, УСЛОВИЙ, ПРЕДСТАВЛЕНИЙ ИЛИ ПОЛОЖЕНИЙ (ВЫРАЖАЕМЫХ В ЯВНОЙ ИЛИ В ПОДРАЗУМЕВАЕМОЙ ФОРМЕ) НА ВСЕ, ВКЛЮЧАЯ БЕЗ ОГРАНИЧЕНИЙ НЕНАРУШЕНИЕ ПРАВ ТРЕТЬИХ ЛИЦ, КОММЕРЧЕСКОЕ КАЧЕСТВО, ИНТЕГРАЦИЮ ИЛИ ПРИГОДНОСТЬ ДЛЯ ОПРЕДЕЛЕННЫХ ЦЕЛЕЙ. ВЫ СОГЛАШАЕТЕСЬ С ТЕМ, ЧТО ВЫ НЕСЕТЕ ОТВЕТСТВЕННОСТЬ ЗА ВЫБОР ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ДОСТИЖЕНИЯ НУЖНЫХ РЕЗУЛЬТАТОВ, ЗА УСТАНОВКУ И ИСПОЛЬЗОВАНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, А ТАКЖЕ ЗА РЕЗУЛЬТАТЫ, ПОЛУЧЕННЫЕ С ЕГО ПОМОЩЬЮ.

СОДЕРЖАНИЕ

ОБ ЭТОМ РУКОВОДСТВЕ

Данный документ содержит описание основных понятий и функций программы Kaspersky Administration Kit, а также общие схемы работы с ним. Пошаговое описание действий приводится в Справочном руководстве к Kaspersky Administration Kit. Функции, описываемые в Справочном руководстве, выделены в тексте подчеркиванием.

В ЭТОМ РАЗДЕЛЕ

В ЭТОМ ДОКУМЕНТЕ

В этом документе представлены следующие разделы:

- Дополнительные источники информации (см. стр. 8). В разделе представлена информация о том, где можно получить сведения о программе, помимо набора документов, входящих в комплект поставки.
- Kaspersky Administration Kit (см. стр. 11). Раздел содержит информацию о назначении, ключевых возможностях и составе программы Kaspersky Administration Kit.
- Интерфейс программы (см. стр. 16). В разделе описаны основные особенности интерфейса программы Kaspersky Administration Kit.
- Запуск и остановка программы (см. стр. 26). В разделе описан способ запуска программы Kaspersky Administration Kit.
- Основные понятия (см. стр. 27). Раздел содержит развернутые определения основных понятий, относящихся к программе Kaspersky Administration Kit.
- Концепция работы Kaspersky Administration Kit (см. стр. 33). В разделе описаны основные принципы работы программы и способы решения отдельных задач.
- Управление компьютерами сети (см. стр. 40). В разделе описаны особенности работы с Kaspersky Administration Kit в рамках управления компьютерами сети.
- Удаленное управление программами (см. стр. 53). В разделе описаны способы управления программами с помощью Kaspersky Administration Kit.
- Обновление баз и программных модулей (см. стр. 64). Раздел содержит информацию о том, как с помощью Kaspersky Administration Kit обновлять базы программ, используемые при проверке зараженных объектов, устанавливать критические обновления программных модулей, а также обновлять версии программ.
- Обслуживание (см. стр. 71). В разделе рассмотрены мероприятия по обслуживанию сети, которые рекомендуется проводить регулярно. Кроме того, здесь описан ряд функций, облегчающих обслуживание сети.
- Обращение в службу технической поддержки (см. стр. 92). В разделе описаны правила обращения в Службу технической поддержки.
- Глоссарий терминов. В разделе перечислены термины, используемые в этом документе.

- ЗАО «Лаборатория Касперского» (см. стр. 98). В разделе приводится информация о ЗАО «Лаборатория Касперского».
- Информация об использовании стороннего кода. В разделе приводится информация о стороннем коде, используемом в программе.
- Предметный указатель. С помощью этого раздела вы можете быстро найти необходимые сведения в документе.

Условные обозначения

В документе используются условные обозначения, описанные в таблице ниже.

Таблица 1. Условные обозначения

Пример текста	Описание условного обозначения
Обратите внимание на то, что...	Предупреждения выделяются красным цветом и заключаются в рамку. В предупреждениях содержится важная информация, например, связанная с критическими для безопасности компьютера действиями.
Рекомендуется использовать...	Примечания заключаются в рамку. В примечаниях содержится вспомогательная и справочная информация.
Пример: ...	Примеры приводятся в блоке на желтом фоне под заголовком «Пример».
Обновление – это...	Новые термины выделяются курсивом.
ALT+F4	Названия клавиш клавиатуры выделяются полужирным шрифтом и прописными буквами. Названия клавиш, соединенные знаком «плюс», означают комбинацию клавиш.
Включить	Названия элементов интерфейса, например, полей ввода, команд меню, кнопок, выделяются полужирным шрифтом.
➡ *Чтобы настроить расписание задачи, выполните следующие действия:*	Вводные фразы инструкций выделяются курсивом.
`help`	Тексты командной строки или тексты сообщений, выводимых программой на экран, выделяются специальным шрифтом.
<IP-адрес вашего компьютера>	Переменные заключаются в угловые скобки. Вместо переменной в каждом случае требуется подставить соответствующее ей значение, угловые скобки при этом опускаются.

ДОПОЛНИТЕЛЬНЫЕ ИСТОЧНИКИ ИНФОРМАЦИИ

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

«Лаборатория Касперского» предоставляет различные источники информации о программе. Среди них вы можете выбрать наиболее удобный для вас в зависимости от важности и срочности вопроса.

В ЭТОМ РАЗДЕЛЕ

Источники информации для самостоятельного поиска

Вы можете обратиться к следующим источникам информации о программе:

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

Страница на веб-сайте «Лаборатории Касперского»

http://www.kaspersky.ru/administration_kit

На этой странице вы получите общую информацию о программе, ее возможностях и особенностях.

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

http://support.kaspersky.ru/remote_adm

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

Эти статьи содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы, связанные с приобретением, установкой и использованием Kaspersky Administration Kit. Они сгруппированы по темам, например, «Работа с ключевыми файлами», «Обновление баз» или «Устранение сбоев в работе». Статьи могут отвечать на вопросы, относящиеся не только к Kaspersky Administration Kit, но и к другим продуктам «Лаборатории Касперского», а также содержать новости Службы технической поддержки в целом.

Электронная справочная система

В комплект поставки программы входит файл полной справки.

Полная справка содержит пошаговое описание предоставляемых программой функций.

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

Если у вас возникнет вопрос, связанный с отдельным окном программы, вы можете обратиться к контекстной справке.

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

Документация

Комплект документации к программе содержит большую часть информации, необходимой для работы с ней. В его состав входят следующие документы:

- **Руководство администратора** – содержит назначение, основные понятия, функции и общие схемы работы с программой Kaspersky Administration Kit.
- **Руководство по внедрению** – содержит описание установки компонентов Kaspersky Administration Kit, а также удаленной установки программ в компьютерной сети простой конфигурации.
- **Начало работы** – содержит описание шагов, с помощью которых администратор антивирусной безопасности предприятия может быстро начать работу с программой Kaspersky Administration Kit и развернуть в своей сети антивирусную защиту на базе программ «Лаборатории Касперского».
- **Справочное руководство** – содержит назначение программы Kaspersky Administration Kit и пошаговое описание предоставляемых ею функций.

Файлы с этими документами в формате PDF входят в комплект поставки Kaspersky Administration Kit.

Загрузить файлы документов можно со страницы программы на веб-сайте «Лаборатории Касперского».

Информация о программном интерфейсе управления (API) Kaspersky Administration Kit отображена в файле klakaut.chm, который расположен в папке установки программы.

Обсуждение программ «Лаборатории Касперского» на веб-форуме

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

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

Обращение в Группу подготовки пользовательской документации

Если у вас возникли вопросы, связанные с документацией, или вы обнаружили в ней ошибку, или хотите оставить отзыв о наших документах, вы можете обратиться к сотрудникам Группы разработки технической документации.

Перейдя по ссылке **Написать отзыв**, расположенной в правом верхнем углу окна справки, вы можете открыть окно почтового клиента, который используется на вашем компьютере по умолчанию. В открывшемся окне будет указан адрес группы разработки документации – docfeedback@kaspersky.com, а в теме письма – «Kaspersky Help Feedback: Kaspersky Administration Kit». Не изменяя тему письма, напишите ваш отзыв и отправьте письмо.

KASPERSKY ADMINISTRATION KIT

Программный продукт бесплатно поставляется со всеми программами «Лаборатории Касперского», входящими в состав Kaspersky Open Space Security (коробочный вариант). Кроме того, он доступен для загрузки с веб-сайта «Лаборатории Касперского» (http://www.kaspersky.ru).

Программа **Kaspersky Administration Kit** предназначена для централизованного решения основных административных задач по управлению системой антивирусной безопасности компьютерной сети предприятия, построенной на основе программ, входящих в состав продуктов Kaspersky Open Space Security. Kaspersky Administration Kit поддерживает работу во всех сетевых конфигурациях, использующих протокол TCP/IP.

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

При помощи данной программы администратор может:

- Формировать структуру групп администрирования, обеспечивающую антивирусную защиту предприятия. Группы администрирования позволяют управлять набором компьютеров как единым целым.
- Проводить удаленную установку и деинсталляцию программ антивирусной защиты предприятия.
- Осуществлять удаленное централизованное управление программами антивирусной защиты.
- Централизованно получать и распространять на компьютеры сети обновления баз и программных модулей антивирусных программ.
- Получать уведомления о критических событиях в работе программ антивирусной защиты.
- Получать статистику и отчеты о работе программ антивирусной защиты.
- Управлять лицензиями всех установленных антивирусных программ.
- Централизованно работать с объектами, помещенными антивирусными программами на карантин или в резервное хранилище, а также с объектами, обработка которых отложена.
- Централизованно работать с программами сторонних производителей в сети.

Программа Kaspersky Administration Kit состоит из следующих основных компонентов:

- **Сервер администрирования** – осуществляет функции централизованного хранения информации об установленных в сети предприятия программах «Лаборатории Касперского» и управления ими.
- **Агент администрирования** – осуществляет взаимодействие между Сервером администрирования и программами «Лаборатории Касперского», установленными на конкретном сетевом узле (рабочей станции или сервере). Данный компонент является единым для всех Windows-программ из состава продуктов компании Kaspersky Open Space Security. Для Novell- и Unix-программ «Лаборатории Касперского» существуют отдельные версии Агента администрирования.
- **Консоль администрирования** – предоставляет пользовательский интерфейс к административным службам Сервера и Агента. Консоль администрирования выполнена в виде компонента расширения к Microsoft Management Console (MMC).

В ЭТОМ РАЗДЕЛЕ

Что нового

Изменения, внесенные в программу Kaspersky Administration Kit 8.0 по сравнению с версией Kaspersky Administration Kit 6.0:

- Введен режим упрощенной установки программы.
- В задаче удаленной установки можно задавать несколько учетных записей.
- В состав программы включен дистрибутив Microsoft SQL Express 2005: его установка происходит автоматически при выборе стандартной установки.
- Добавлена возможность SNMP-мониторинга за основными параметрами антивирусной защиты корпоративной сети.
- Добавлена возможность создания автономного пакета установки для программ «Лаборатории Касперского».
- Значительно переработан пользовательский интерфейс программы: панель результатов, вид отчетов, информационные панели (см. раздел «Главное окно программы» на стр. 17).
- Добавлен механизм сбора информации об установленных на клиентских компьютерах программах (реестр программ).
- Переработана и расширена система прав доступа.
- Добавлена поддержка технологии Microsoft NAP.
- Добавлена возможность переключения мобильных клиентов между Серверами администрирования.
- Расширены критерии переключения клиентов между мобильной и обычной политиками.
- Расширены возможности автоматического перемещения компьютеров в группы администрирования.
- Добавлена возможность создания групп администрирования на основе структуры Active Directory.
- Добавлены новые отчеты, появилась возможность добавлять собственные системы отчетности, расширена отображаемая в отчетах информация.
- Добавлена возможность экспорта отчетов в файлы форматов PDF и XML (Microsoft Excel).
- Добавлена возможность сбора детализированных данных при построении общих отчетов.
- Реализован механизм кеширования информации для построения общих отчетов, включающих данные с подчиненных Серверов администрирования.
- Добавлена поддержка двух наборов граф в Консоли администрирования, а также расширен набор граф (см. стр. 23).
- Добавлены новые графы для списка компьютеров: «Перезагрузка», «Описание статуса», «Версия Агента администрирования», «Версия защиты», «Версия баз», «Время включения».
- Добавлены новые критерии, по которым формируются статусы компьютеров.
- Добавлены новые выборки компьютеров, сформированные по умолчанию, добавлена возможность создания выборок компьютеров с учетом данных подчиненных Серверов администрирования.
- Добавлена возможность ведения списка примечаний администратора.

- Добавлена возможность просмотра имеющихся на компьютере пользовательских сессий и контактной информации пользователей.
- Добавлен графический интерфейс для утилиты резервного копирования и восстановления данных.
- Файлы политик и групповых задач распространяются при помощи многоадресной IP-рассылки.
- Параметр Wake On Lan доступен для клиентских компьютеров, расположенных в подсетях, отличающихся от подсети Сервера администрирования, и в случае запуска задачи вручную.
- Параметры перезагрузки для клиентских компьютеров можно установить в свойствах задачи удаленной установки.
- Изменен механизм ограничения количества отправляемых в единицу времени уведомлений – теперь ограничения считаются независимо для каждого типа событий.
- Добавлена возможность поиска групп и подчиненных Серверов администрирования по иерархии Серверов.
- Расширена статистика агентов обновлений.
- Задача удаления сторонних программ теперь позволяет удалять сразу несколько программ.
- Разработана утилита подготовки компьютеров к удаленной установке.
- Реализован механизм получения необходимых для программы обновлений непосредственно после создания ее инсталляционного пакета.
- При получении обновлений учитываются программы, уже подключенные к подчиненным Серверам администрирования.
- Введена классификация возможных ошибок подсистемы удаленной установки программ и даны рекомендации по решению типичных проблем.
- Добавлен механизм автоматического применения обновлений модулей для компонентов системы администрирования.

Аппаратные и программные требования

Сервер администрирования

- Программные требования:
  - Microsoft Data Access Components (MDAC) версии 2.8 и выше или Windows DAC 6.0.
  - Система управления базами данных: Microsoft SQL Express 2005, Microsoft SQL Express 2008, Microsoft SQL Express 2008 R2, Microsoft SQL Server 2005, Microsoft SQL Server 2008, Microsoft SQL Server 2008 R2 или MySQL Enterprise.
  - Microsoft Windows Server 2003 и выше; Microsoft Windows Server 2003 x64 и выше; Microsoft Windows Server 2008; Microsoft Windows Server 2008, развернутая в режиме Server Core; Microsoft Windows Server 2008 x64 с установленным Пакетом обновлений 1 и всеми текущими обновлениями (для Microsoft Windows Server 2008 x64 должен быть установлен Microsoft Windows Installer 4.5); Microsoft Windows Server 2008 R2; Microsoft Windows Server 2008 R2, развернутая в режиме Server Core; Microsoft Windows XP Professional с установленным Пакетом обновлений 2 и выше; Microsoft Windows XP Professional x64 и выше; Microsoft Windows Vista с установленным Пакетом обновлений 1 и выше, Microsoft Windows Vista x64 с установленным Пакетом обновлений 1 и всеми текущими обновлениями (для Microsoft Windows Vista x64 должен быть установлен Microsoft Windows Installer 4.5); Microsoft Windows 7.

- Аппаратные требования:
  - процессор с частотой 1 ГГц или выше;
  - объем оперативной памяти 512 МБ;
  - объем свободного места на диске 1 ГБ.

Консоль администрирования

- Программные требования:
  - Операционная система Windows.

    Версия поддерживаемой операционной системы определяется требованиями Сервера администрирования.
  - Microsoft Management Console версии 2.0 и выше.
  - При работе с Microsoft Windows XP, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2 или Windows Vista: наличие установленного браузера Microsoft Internet Explorer 7.0 и выше.
  - При работе с Microsoft Windows 7: наличие установленного браузера Microsoft Internet Explorer 8.0 и выше.
- Аппаратные требования:
  - При работе с 32-разрядной операционной системой:
    - процессор с частотой 1 ГГц или выше;
    - объем оперативной памяти 512 МБ;
    - объем свободного места на диске 1 ГБ.
  - При работе с 64-разрядной операционной системой:
    - процессор с частотой 1,4 ГГц или выше;
    - объем оперативной памяти 512 МБ;
    - объем свободного места на диске 1 ГБ.

Агент администрирования и агент обновлений

- Программные требования:
  - Операционная система:
    - Windows.

      Версия поддерживаемой операционной системы определяется требованиями Сервера администрирования.
    - Linux.
    - Mac OS.
- Аппаратные требования:

- При работе с 32-разрядной операционной системой:
  - процессор с частотой 1 ГГц или выше;
  - объем оперативной памяти 512 МБ;
  - объем свободного места на диске: 32 МБ для Агента администрирования, 500 МБ для агента обновлений.
- При работе с 64-разрядной операционной системой:
  - процессор с частотой 1,4 ГГц или выше;
  - объем оперативной памяти 512 МБ;
  - объем свободного места на диске: 32 МБ для Агента администрирования, 500 МБ для агента обновлений.

ИНТЕРФЕЙС ПРОГРАММЫ

Просмотр, создание, изменение и настройка групп администрирования, централизованное управление работой всех установленных на клиентских компьютерах программ «Лаборатории Касперского» осуществляется с рабочего места администратора. Интерфейс управления обеспечивает компонент Консоль администрирования. Он представляет собой специализированную автономную оснастку, интегрированную в Microsoft Management Console (MMC), поэтому интерфейс Kaspersky Administration Kit является стандартным для MMC.

Консоль администрирования позволяет подключаться к удаленному Серверу администрирования через интернет.

Для локальной работы с клиентскими компьютерами программа предусматривает возможность установки удаленного соединения с компьютером через Консоль администрирования с помощью стандартной программы Microsoft Windows **Подключение к удаленному рабочему столу**.

Чтобы использовать эту возможность, на клиентском компьютере необходимо разрешить удаленное подключение к рабочему столу.

В ЭТОМ РАЗДЕЛЕ

НАСТРОЙКА ИНТЕРФЕЙСА

Kaspersky Administration Kit позволяет администратору настроить интерфейс Консоли администрирования.

Чтобы изменить уже установленные параметры интерфейса, выполните следующие действия:

1. В дереве консоли перейдите в узел Сервера администрирования.
2. Пройдите в меню **Вид** → **Настройка интерфейса**. В результате откроется одноименное окно (см. рис. ниже).

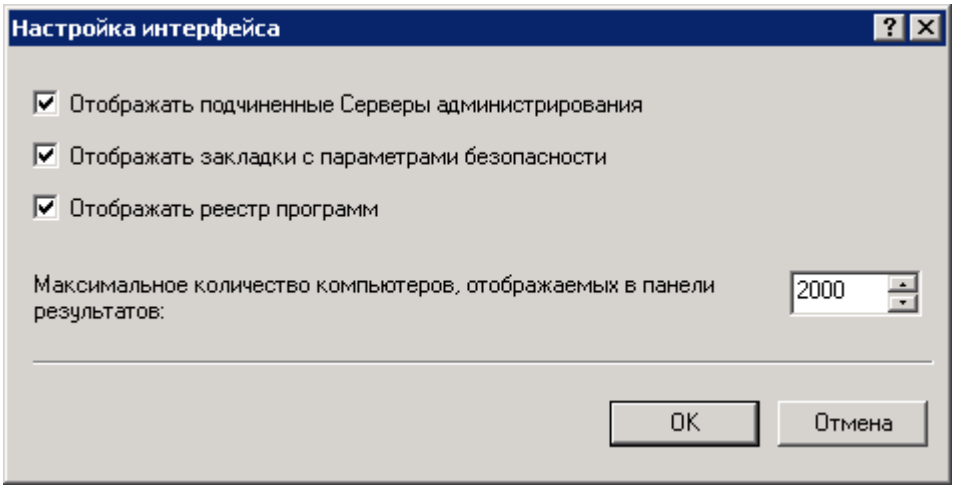

*Рисунок 1. Просмотр свойств группы. Окно **Настройка интерфейса***

3. В открывшемся окне можно задать следующие параметры:

   - **Отображать подчиненные Серверы администрирования**.
   - **Отображать закладки с параметрами безопасности**.
   - **Отображать реестр программ**.
   - **Максимальное количество компьютеров, отображаемых в панели результатов**. Данный параметр определяет количество компьютеров, отображаемых в панели результатов Консоли администрирования. По умолчанию значение параметра составляет 2000.

     Если количество компьютеров в группе превышает установленное значение, на экран выводится соответствующее предупреждение. Чтобы просмотреть список всех компьютеров, следует увеличить значение параметра.

Установленное в параметрах какой-либо группы (или домена) значение максимального количества отображаемых компьютеров вступает в силу для всех групп всех уровней иерархии, а так же для всех доменов.

Главное окно программы

Главное окно программы (см. рис. ниже) содержит меню, панель инструментов, панель обзора и информационную область, которая может быть представлена панелью задач или панелью результатов.

Меню обеспечивает управление окнами и предоставляет доступ к справочной системе. Пункт меню **Действие** дублирует команды контекстного меню для текущего объекта дерева консоли.

Набор кнопок панели инструментов обеспечивает прямой доступ к некоторым пунктам главного меню. Состав панели инструментов изменяется в зависимости от текущего узла или папки дерева консоли.

Панель обзора отображает пространство имен **Kaspersky Administration Kit** в виде дерева консоли (см. раздел «Дерево консоли» на стр. 18).

Информационная область главного окна может быть представлена панелью задач, панелью результатов или их комбинацией. Для ряда папок дерева консоли информационная область имеет два вида представления: расширенный и стандартный. Переход между ними доступен по одноименным закладкам.

Панель задач (см. стр. 20) содержит одну или несколько закладок со ссылками быстрого доступа к основным операциям, предусмотренным для выбранного в дереве консоли объекта.

Панель результатов (см. стр. 23) представляет собой список элементов выбранного в дереве консоли объекта или набор информационных панелей. Это может быть, например, список компьютеров в группах, перечень отчетов, выборок событий или компьютеров.

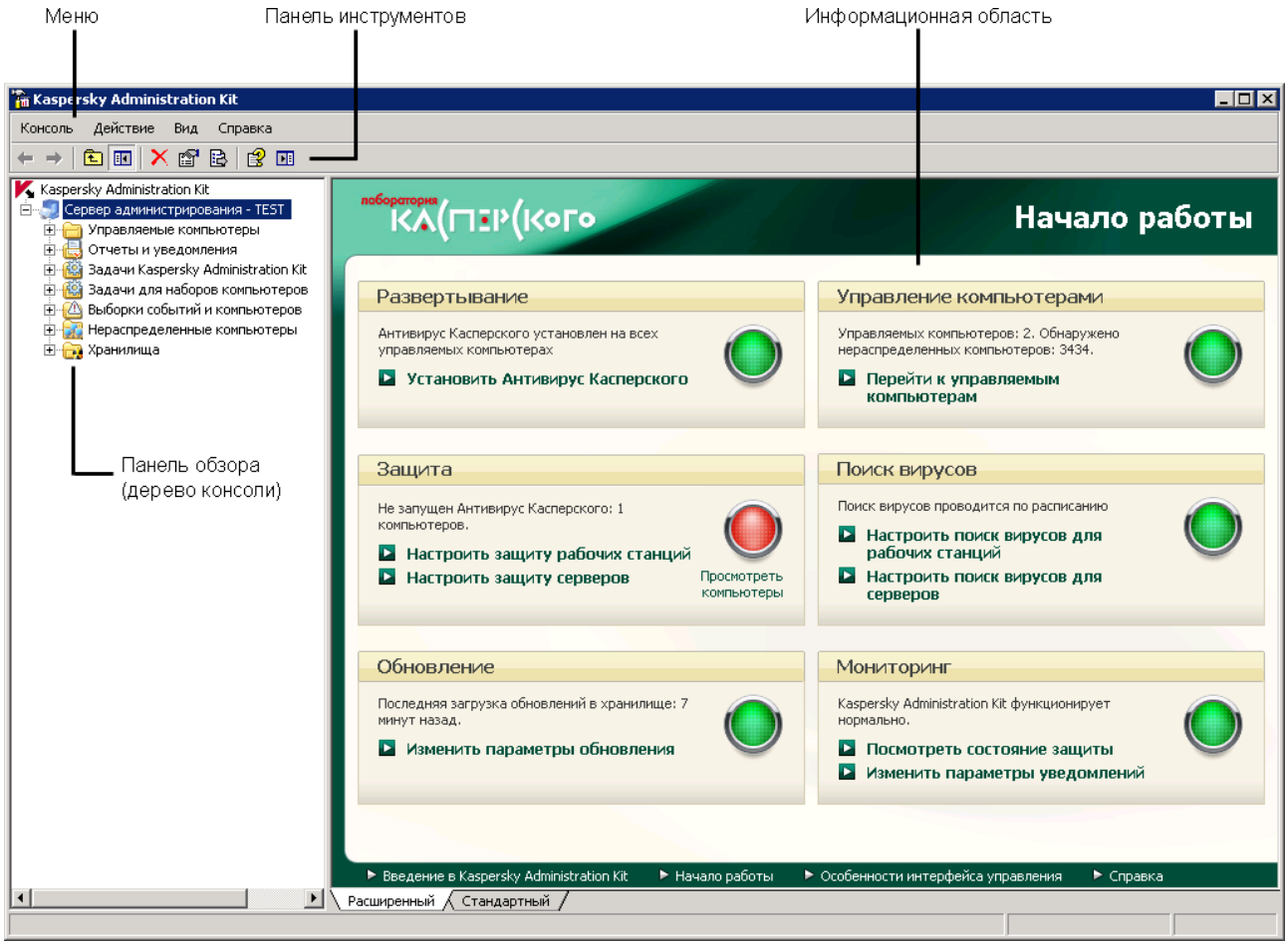

Рисунок 2. Главное окно программы Kaspersky Administration Kit

Дерево консоли

Дерево консоли (см. рис. ниже) предназначено для отображения сформированной в сети предприятия иерархии Серверов администрирования, структуры их групп администрирования, а также других объектов программы, таких как хранилища, выборки и т. д.

Пространство имен **Kaspersky Administration Kit** может содержать несколько узлов с именами серверов, соответствующих установленным и включенным в структуру Серверам администрирования.

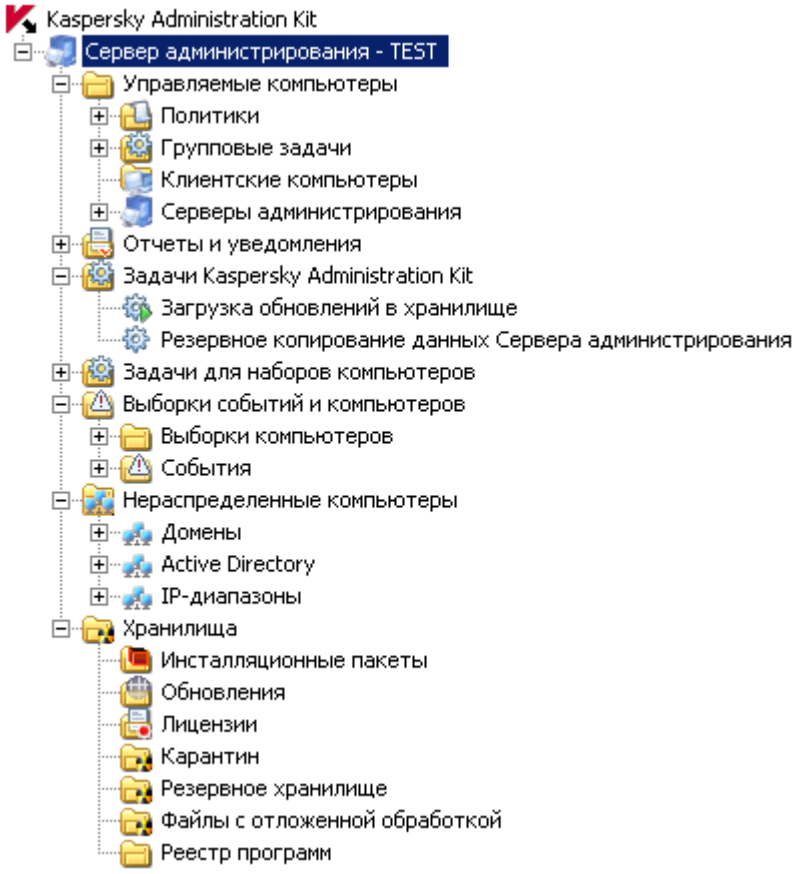

Рисунок 3. Дерево консоли

Узел **Сервер администрирования – <Имя компьютера>** является контейнером и отображает структурную организацию указанного Сервера администрирования. В состав контейнера **Сервер администрирования – <Имя компьютера>** входят следующие папки:

- **Управляемые компьютеры**.
- **Отчеты и уведомления**.
- **Задачи Kaspersky Administration Kit**.
- **Задачи для наборов компьютеров**.
- **Выборки событий и компьютеров**.
- **Нераспределенные компьютеры**.
- **Хранилища**.

Папка **Управляемые компьютеры** предназначена для хранения, отображения, настройки и изменения структуры групп администрирования, групповых политик и групповых задач. Она включает в себя вложенные папки **Политики**, **Групповые задачи**, **Клиентские компьютеры** и **Серверы администрирования**. Для каждой отдельной группы администрирования в дереве консоли создается точно такая же структура папок.

Папка **Задачи Kaspersky Administration Kit** содержит набор задач, определенных для Сервера администрирования. Существует три типа задач Сервера администрирования: рассылка отчетов, резервное копирование и получение обновления Сервером администрирования.

Папка **Задачи для наборов компьютеров** содержит задачи, определенные для наборов компьютеров в составе групп администрирования или папки **Нераспределенные компьютеры**. Такие задачи удобны для небольших групп клиентских компьютеров, которые не могут быть объединены в отдельную группу администрирования.

Папка **Отчеты и уведомления** дерева консоли содержит набор шаблонов для формирования отчетов о состоянии системы антивирусной защиты на клиентских компьютерах групп администрирования. Шаблоны доступны на закладке **Статистика** панели задач данной папки. На закладке **Уведомления** доступна настройка параметров уведомлений о работе системы. При выборе в дереве консоли какого-либо шаблона сформированный отчет отображается в панели результатов.

Папка **Выборки событий и компьютеров** содержит следующие вложенные папки:

- **Выборки компьютеров** – предназначена для поиска клиентских компьютеров по заданным критериям.
- **События** – содержит выборки событий, в которых представлена информация о событиях, зарегистрированных в работе программ, и результатах выполнения задач.

Папка **Нераспределенные компьютеры** предназначена для отображения компьютерной сети, в которой установлен Сервер администрирования. Информацию о структуре сети и входящих в ее состав компьютерах Сервер администрирования получает в ходе регулярных опросов Windows-сети, IP-диапазонов и Active Directory, сформированных в компьютерной сети предприятия. Результаты опросов отображаются в панели результатов соответствующих папок: **Домены**, **IP-диапазоны** и **Active Directory**.

Папка **Хранилища** предназначена для работы с объектами, которые используются для мониторинга состояния клиентских компьютеров и их обслуживания. В ее состав входят следующие папки:

- **Инсталляционные пакеты** – содержит список инсталляционных пакетов, которые могут использоваться для удаленной установки программ на клиентские компьютеры.
- **Обновления** – содержит список полученных Сервером администрирования обновлений, которые могут быть распространены на клиентские компьютеры.
- **Лицензии** – содержит список лицензий, установленных на клиентских компьютерах.
- **Карантин** – содержит список объектов, помещенных антивирусными программами в карантинные папки на клиентских компьютерах.
- **Резервное хранилище** – содержит список резервных копий объектов, помещенных в хранилище.
- **Файлы с отложенной обработкой** – содержит список файлов, для которых антивирусные программы определили необходимость отложенного лечения.
- **Реестр программ** – содержит список программ, установленных на клиентских компьютерах, на которых установлен Агент администрирования.

Панель задач

Панель задач представляет собой область окна, содержащую набор ссылок для управления объектами Сервера администрирования, а также непосредственно самим Сервером администрирования.

Условно различают два вида панелей задач – стандартный и расширенный.

Расширенная панель задач (см. рис. ниже) доступна для большинства узлов и папок дерева консоли и представляет собой HTML-страницу, содержащую ссылки для выполнения различных операций, перехода к другим объектам Сервера администрирования и краткую информацию о текущем объекте.

Для одного узла или папки может быть предусмотрено несколько панелей задач, представленных в виде закладок с заголовками в верхней части информационной области.

Для удобства перехода между объектами Сервера администрирования в верхней части панели задач предусмотрена навигационная цепочка вида **Начало работы** → **<Название узла>** → **...** → **<Название**

папки> → **<Название элемента>**. Группы ссылок могут объединяться в блоки для более удобного размещения в панели.

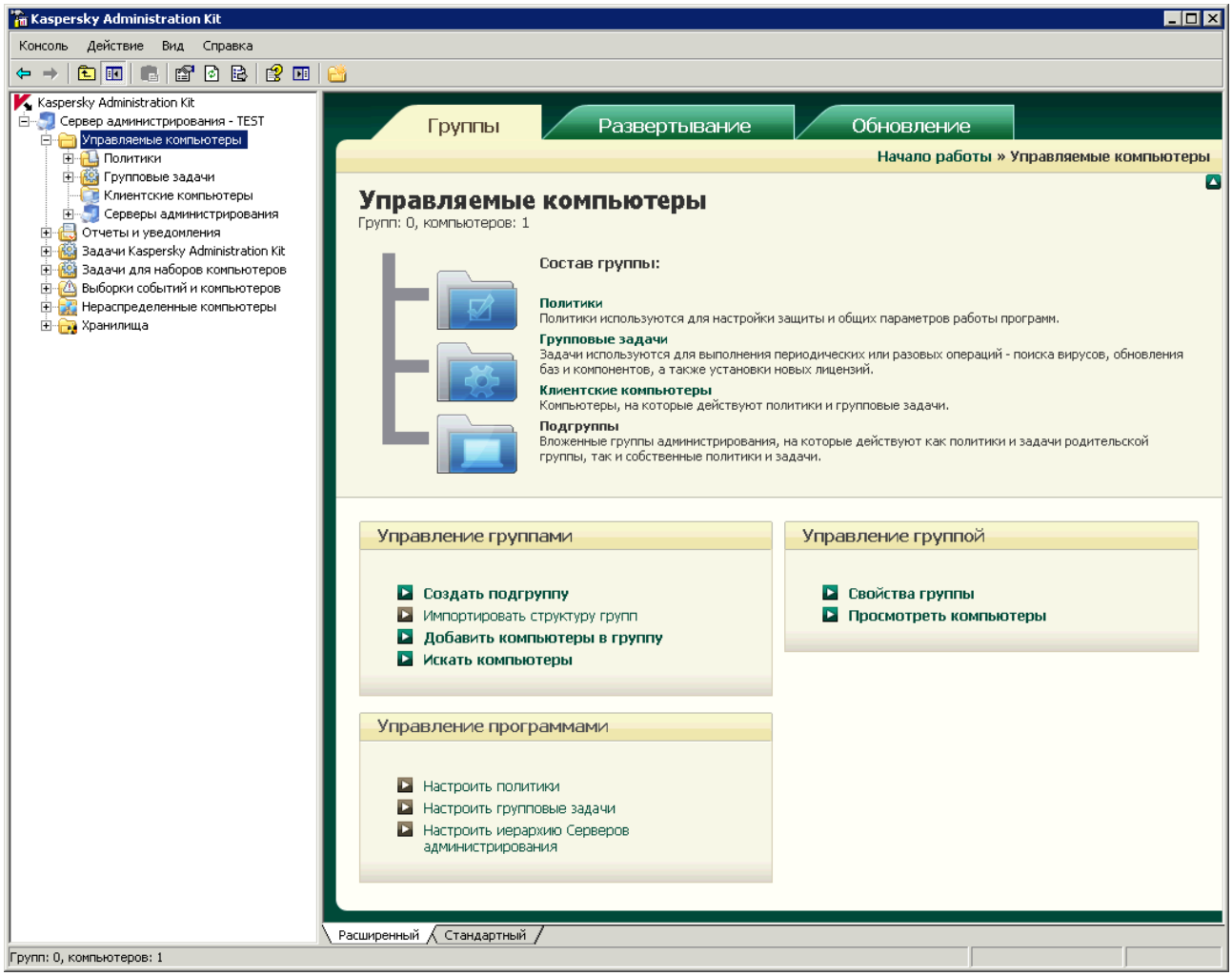

Рисунок 4. Панель задач

Для некоторых объектов дерева консоли в панели задач может приводиться сводная информация об объекте, например, данные статистики при выборе папки Отчеты и уведомления (см. рис. ниже). В таком случае панель задач выполняет также функцию панели результатов (см. стр. 23).

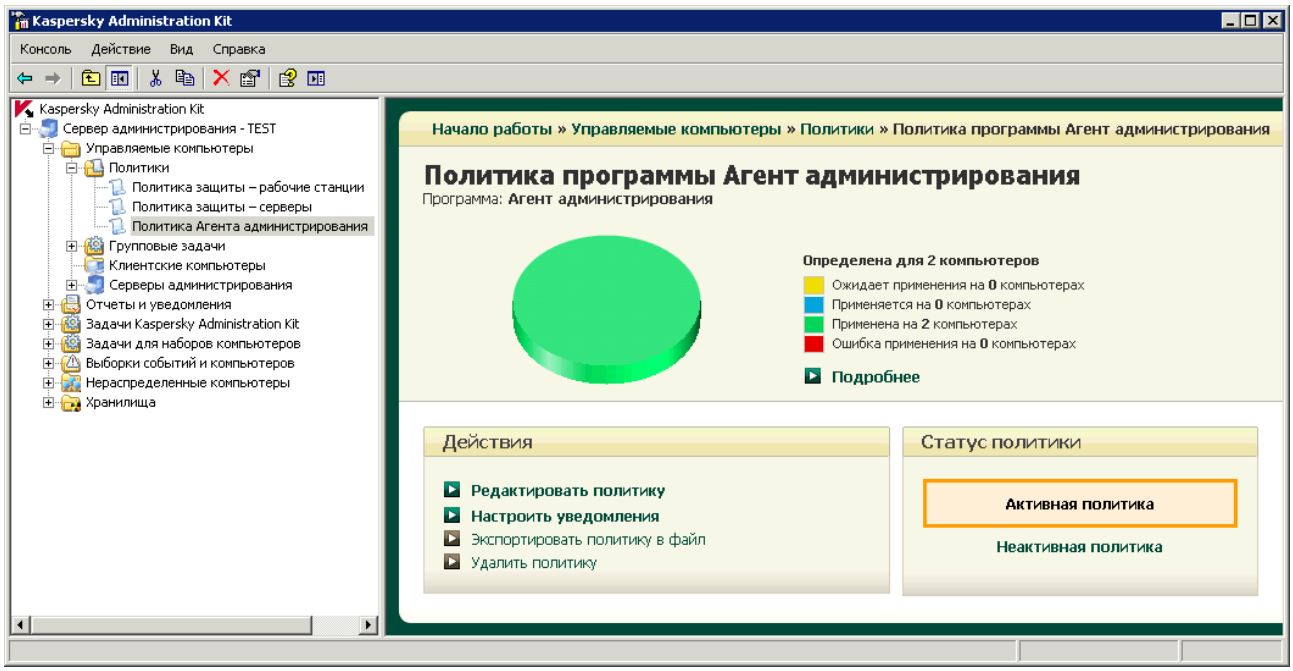

Рисунок 5. Панель задач, выполняющая функцию панели результатов

Для некоторых папок, не имеющих расширенной панели задач, предусмотрена стандартная панель задач, представленная двумя закладками в нижней части панели: закладкой **<Имя папки>** и закладкой **Стандартный**. В случае выбора закладки **<Имя папки>** в левой части панели представлен набор ссылок (см. рис. ниже). Ссылки стандартной панели задач, так же как и расширенной, служат для перехода к выполнению операций, просмотру или редактированию свойств папки.

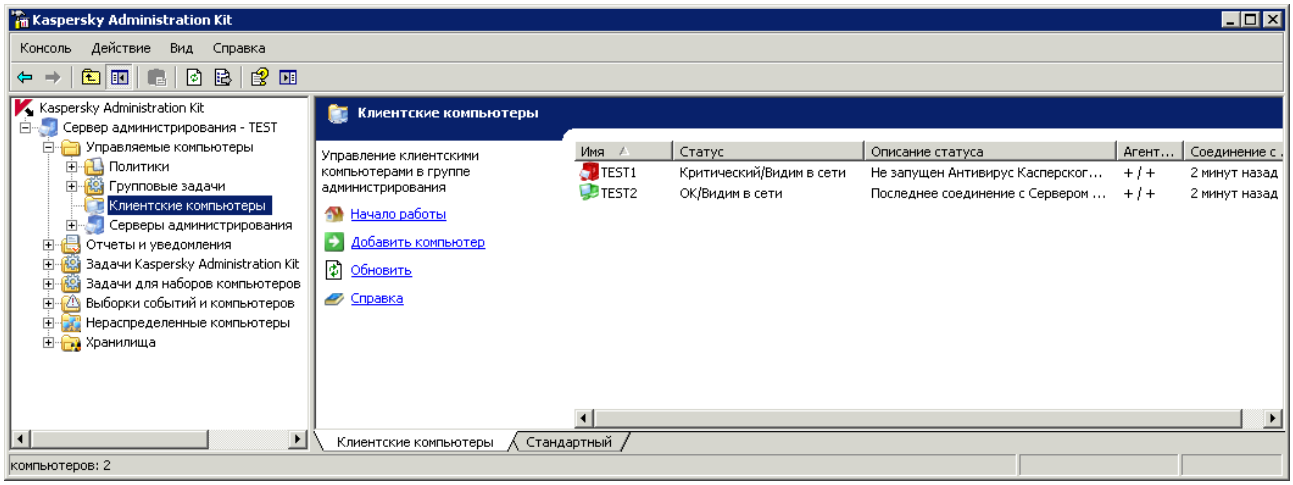

*Рисунок 6. Стандартная панель задач для папки **Клиентские компьютеры***

В рамках документации к программе Kaspersky Administration Kit под термином «панель задач» подразумевается панель задач расширенного вида. При ссылке на панель задач стандартного вида ее элементы описываются как элементы панели результатов.

Панель результатов

Панель результатов представляет собой область окна, отображающую различного рода информацию, например: список компьютеров, политик или задач, сформированные по заданным шаблонам отчеты.

Условно различают два вида панелей результатов: стандартные и расширенные. Они доступны по одноименным закладкам.

Для сформированных отчетов предусмотрена расширенная панель результатов. Она содержит диаграммы, а также сводную и подробную информацию, представленную в виде таблиц (см. рис. ниже).

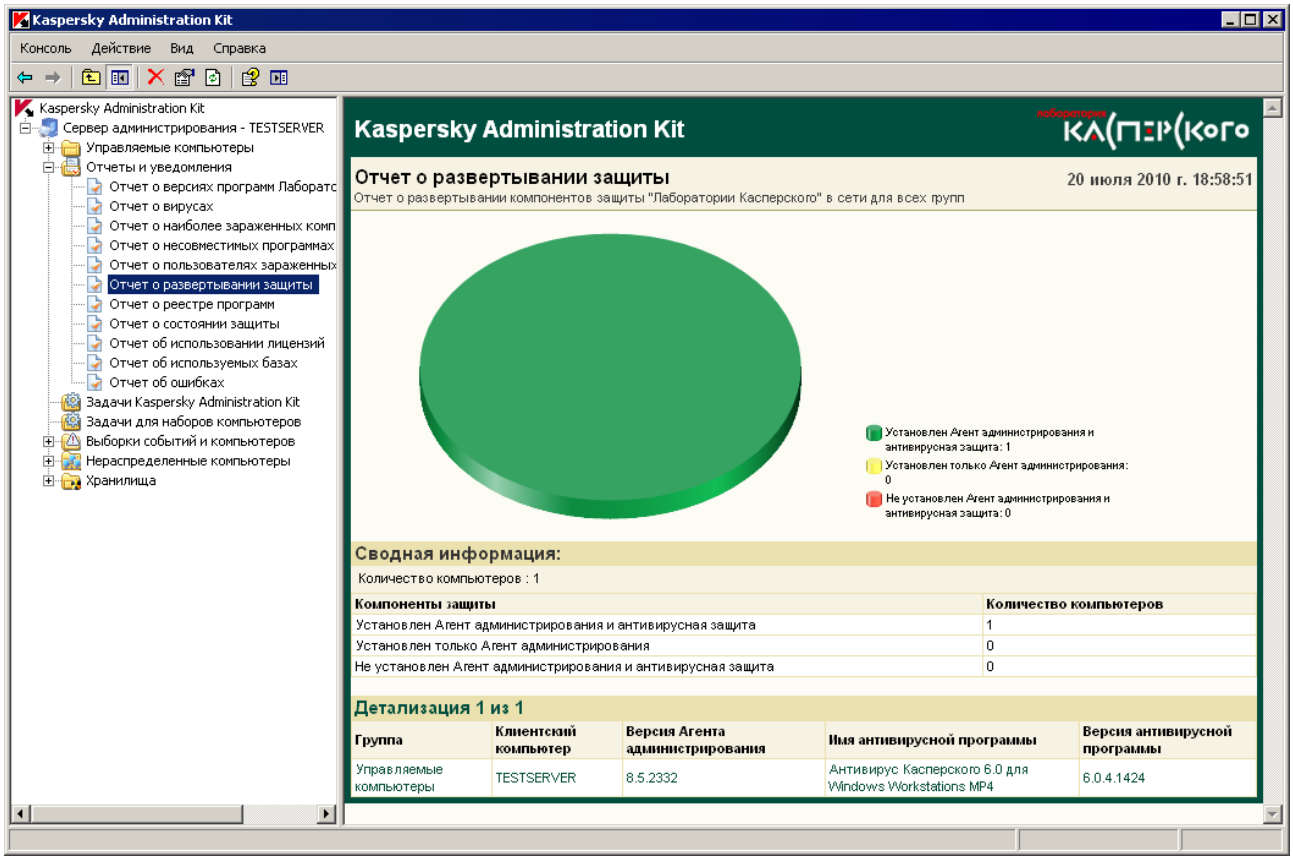

Рисунок 7. Панель результатов. Отчет о развертывании

Расширенная панель результатов может состоять из нескольких страниц (см. рис. ниже), каждая из которых содержит набор информационных панелей.

Данные в информационных панелях могут отображаться в виде таблицы или диаграммы (круговой или столбчатой). Набор страниц и информационных панелей, а также состав и способ отображения данных могут быть изменены администратором:

- Список страниц закладки можно изменить, нажав на кнопку  , расположенную в правом верхнем углу данной закладки.
- Состав страницы можно настроить, нажав на кнопку  , расположенную рядом с именем страницы, и указав в открывшемся окне нужные параметры.
- Параметры отображения отдельной информационной панели можно выбрать, нажав на кнопку  , расположенную рядом с именем панели.

- Свернуть и развернуть панели можно с помощью кнопок и .

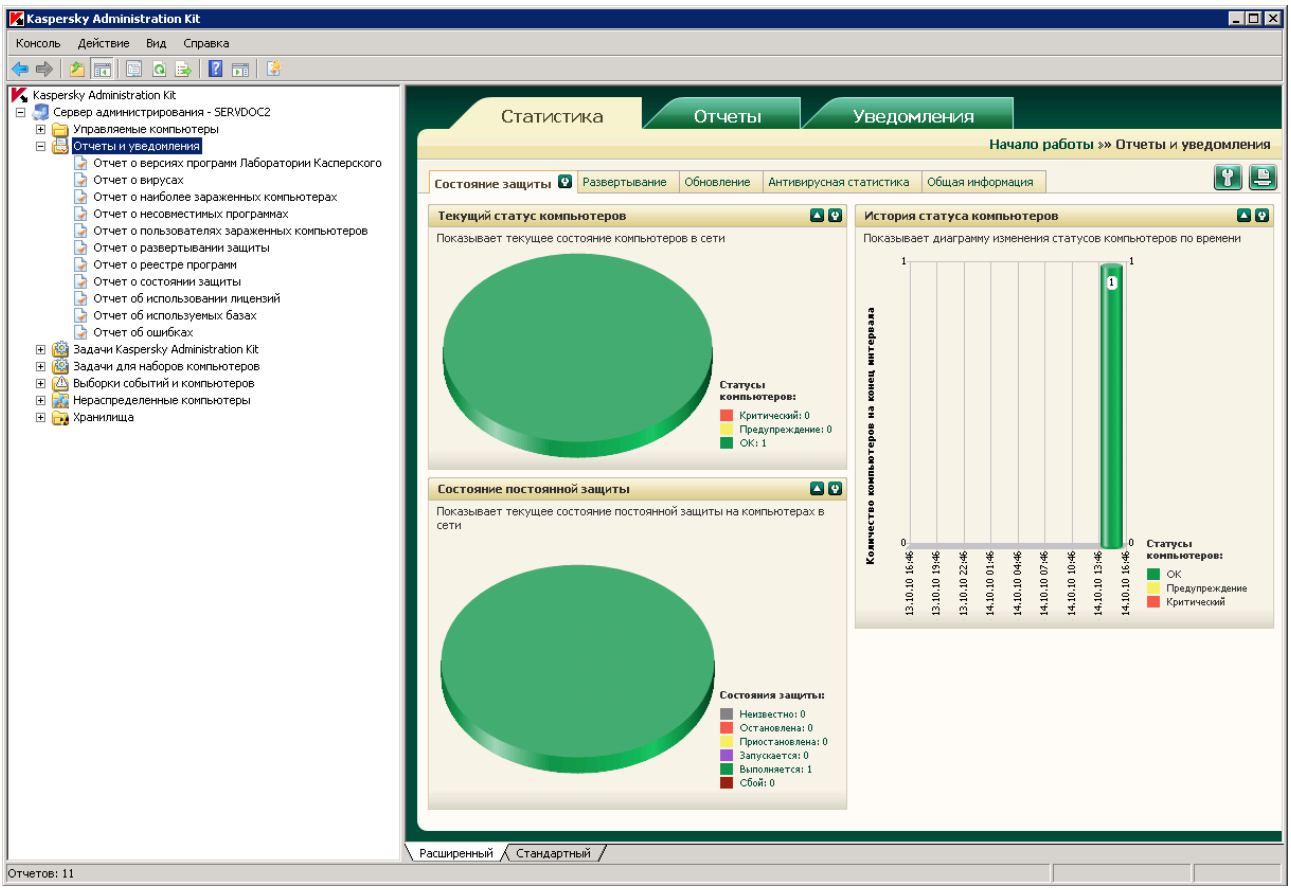

Рисунок 8. Панель результатов, содержащая информационные панели

В стандартной панели результатов данные представлены в виде таблицы (см. рис. ниже). Перечень граф для различных объектов дерева консоли приведен в Справочном руководстве.

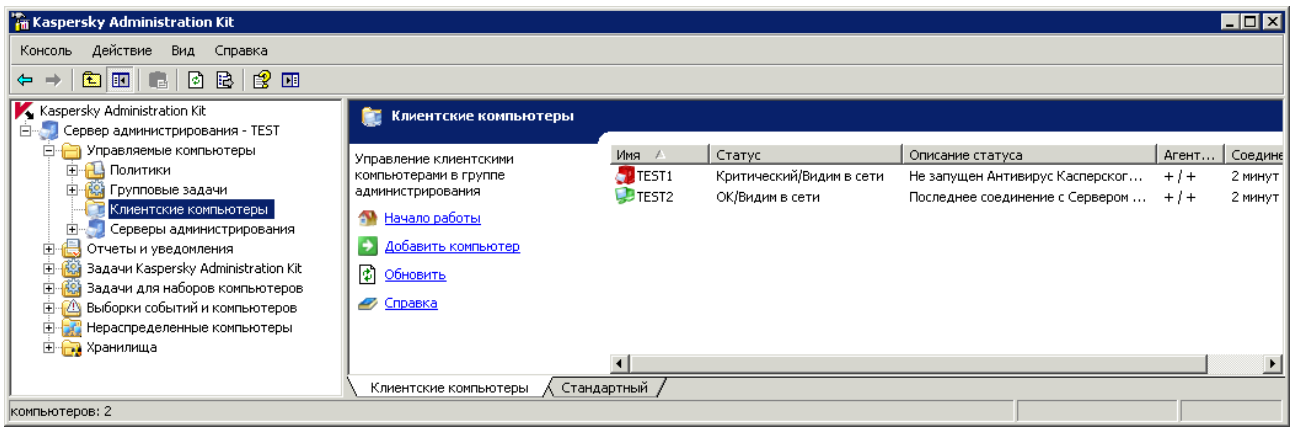

Рисунок 9. Панель результатов стандартного вида

В Kaspersky Administration Kit информация в панели результатов (например: статусы компьютеров, статистика, отчеты) автоматически не обновляется. Обновить данные в панели результатов вы можете тремя способами: нажав на клавишу **F5**, выбрав в контекстном меню объекта пункт **Обновить** или нажав на кнопку , расположенную в панели инструментов.

Контекстное меню

В дереве консоли каждая категория объектов пространства имен **Kaspersky Administration Kit** имеет свое контекстное меню. В нем к стандартным командам контекстного меню MMC добавлены команды, при помощи которых осуществляется работа с данным объектом. Перечень объектов и соответствующий им дополнительный набор возможных команд контекстного меню приводится в Справочном руководстве.

В панели результатов каждый элемент выбранного в дереве объекта также имеет контекстное меню, при помощи команд которого осуществляется работа с данным элементом. Основные типы элементов и соответствующие им дополнительные наборы возможных команд приводятся в Справочном руководстве.

ЗАПУСК И ОСТАНОВКА ПРОГРАММЫ

Kaspersky Administration Kit запускается автоматически при запуске Сервера администрирования.

Запуск программы Kaspersky Administration Kit производится путем выбора пункта **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.

Для доступа к функциональности программы Kaspersky Administration Kit необходимо, чтобы был запущен Сервер администрирования Kaspersky Administration Kit.

ОСНОВНЫЕ ПОНЯТИЯ

Раздел содержит развернутые определения основных понятий, относящихся к программе Kaspersky Administration Kit. Определения этих понятий, а также некоторых терминов представлены в разделе **Глоссарий терминов**.

В ЭТОМ РАЗДЕЛЕ

СЕРВЕР АДМИНИСТРИРОВАНИЯ. ГРУППЫ АДМИНИСТРИРОВАНИЯ

Компоненты Kaspersky Administration Kit позволяют осуществлять удаленное управление программами «Лаборатории Касперского» в рамках сети предприятия.

Компьютеры, на которых установлен компонент Сервер администрирования, будем называть Серверами администрирования.

Множество компьютеров сети предприятия может быть разбито на группы, организующие некую иерархическую структуру. Такие группы будем называть группами администрирования. Структура групп администрирования отображается в дереве консоли в узле Сервера администрирования.

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

- под именем Kaspersky Administration Server;
- с автоматическим типом запуска при старте операционной системы;
- с учетной записью **Локальная система** либо учетной записью пользователя в соответствии с выбором, сделанным при установке компонента.

В число функций Сервера администрирования, а именно установленного на нем компонента Сервер администрирования, входят следующие:

- хранение структуры групп администрирования;
- хранение копии конфигурационной информации клиентских компьютеров;
- организация хранилищ дистрибутивов программ «Лаборатории Касперского»;

- удаленная установка программ на компьютеры и их деинсталляция;
- обновление баз и модулей программ;
- управление политиками и задачами на клиентских компьютерах;
- хранение информации о событиях;
- формирование отчетов о работе программ;
- распространение лицензий на клиентские компьютеры, хранение информации о лицензиях;
- отправка уведомлений о ходе выполнения задач. Такие уведомления могут сообщать, например, об обнаружении на компьютере вирусов.

Иерархия Серверов администрирования

Серверы администрирования могут образовывать иерархию вида «главный сервер – подчиненный сервер». Каждый Сервер администрирования может иметь несколько подчиненных Серверов как на одном, так и на вложенных уровнях иерархии. Уровень вложенности подчиненных серверов не ограничен. При этом в состав групп администрирования главного Сервера будут входить клиентские компьютеры всех подчиненных Серверов. Таким образом, независимые участки компьютерной сети могут управляться различными Серверами администрирования, которые, в свою очередь, управляются главным Сервером.

Возможность построения иерархии Серверов может быть использована для следующих целей:

- Ограничение нагрузки на Сервер администрирования (по сравнению с одним установленным в сети Сервером).
- Сокращение трафика внутри сети и упрощение работы с удаленными офисами. Нет необходимости устанавливать соединение между главным Сервером и всеми компьютерами сети, которые могут находиться, например, в других регионах. Достаточно установить в каждом сегменте сети подчиненный Сервер администрирования, распределить компьютеры в группах администрирования подчиненных Серверов и обеспечить подчиненным Серверам соединение с главным Сервером по быстрым каналам связи.
- Более четкое разделение ответственности между администраторами антивирусной безопасности. При этом сохраняются все возможности централизованного управления и мониторинга состояния антивирусной безопасности сети организации.

Каждый компьютер, включенный в структуру групп администрирования, может быть подключен только к одному Серверу администрирования. Администратор должен самостоятельно контролировать корректность подключения компьютеров к Серверам администрирования, используя функцию поиска компьютеров по сетевым атрибутам в группах администрирования различных Серверов.

Клиентский компьютер. Группа

Взаимодействие между Сервером администрирования и компьютерами осуществляет Агент администрирования. Под таким взаимодействием подразумевается:

- доставка информации о текущем состоянии программ;
- отправка и получение команд управления;
- синхронизация конфигурационной информации;
- отправка на Сервер информации о событиях в работе программ;

- функционирование *агента обновлений*.

Агент администрирования должен быть установлен на все компьютеры, где управление работой программ «Лаборатории Касперского» выполняется с помощью Kaspersky Administration Kit.

Данный компонент устанавливается на компьютере в качестве службы со следующим набором атрибутов:

- под именем Kaspersky Network Agent;
- с автоматическим типом запуска, при старте операционной системы;
- с учетной записью **Локальная система**.

Совместно с Агентом администрирования на компьютер устанавливается плагин для работы с Cisco NAC. Этот плагин работает в том случае, когда на компьютере установлена программа Cisco Trust Agent. Параметры совместной работы с Cisco NAC указываются в свойствах Сервера администрирования.

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

Компьютер, сервер или рабочая станция, на которых установлен Агент администрирования и управляемые программы «Лаборатории Касперского», будем называть *клиентом Сервера администрирования* (или просто *клиентским компьютером*).

В соответствии с организационной или территориальной структурой предприятия, выполняемыми функциями и устанавливаемым на них набором программ «Лаборатории Касперского» клиентские компьютеры могут быть организованы в группы администрирования. Это делается для удобства управления компьютерами группы как единым целым. При объединении клиентских компьютеров может использоваться любое сочетание указанных принципов, а также другие признаки по выбору администратора. Например, верхний уровень могут составлять группы, соответствующие отделам. На следующем уровне внутри каждого отдела компьютеры объединяются в зависимости от выполняемых ими функций: одна группа компьютеров может включать в себя все рабочие станции, другая – все файловые серверы и т. п.

Группа администрирования (далее также *группа*) – это набор клиентских компьютеров, объединенных по какому-либо признаку, с целью управления компьютерами группы как единым целым. Для всех клиентских компьютеров в группе устанавливаются:

- единые параметры работы программ – с помощью *групповых политик*;
- единый режим работы программ – путем создания групповых задач (функций программы) с заданным набором параметров (например, создание и установка единого *инсталляционного пакета*, обновление баз и модулей программ, проверка компьютера по требованию и постоянная защита).

Клиентский компьютер может входить в состав только одной группы администрирования.

Администратор может создавать иерархию Серверов и групп любой глубины вложенности, если это облегчает ему выполнение задач по управлению программами. На одном уровне иерархии могут располагаться подчиненные Серверы администрирования, группы и клиентские компьютеры.

Рабочее место администратора

Компьютеры, на которых установлен компонент Консоль администрирования, будем называть **рабочими местами администраторов**. С этих компьютеров администраторы могут осуществлять удаленное централизованное управление конфигурацией всех программ «Лаборатории Касперского», установленных на клиентских компьютерах.

После установки Консоли администрирования на компьютере в меню **Пуск → Программы → Kaspersky Administration Kit** появляется значок для ее запуска.

Рабочее место администратора не является объектом группы администрирования, однако также может быть включено в ее состав в качестве клиентского компьютера. Количество рабочих мест администратора ничем не ограничивается. Рабочие места администраторов для разных Серверов администрирования могут совпадать: с каждого из них может осуществляться управление группами администрирования любого Сервера администрирования в структуре сети предприятия.

В пределах групп администрирования любого Сервера один и тот же компьютер может быть и клиентом Сервера администрирования, и Сервером администрирования, и рабочим местом администратора.

Плагин управления программой

Интерфейс для управления работой конкретной программы через Консоль администрирования предоставляет специализированный компонент – *плагин управления программой*. Он входит в состав всех программ «Лаборатории Касперского», управление которыми может осуществляться при помощи Kaspersky Administration Kit. Плагин управления для каждой программы свой. Он устанавливается на рабочее место администратора и представляет собой набор диалоговых окон (интерфейс) для создания и редактирования:

- политик программы;
- параметров программы;
- параметров задач, реализуемых программой.

Плагин управления обеспечивает:

- предоставление информации о задачах, реализуемых программой;
- предоставление информации о событиях, генерируемых программой;
- предоставление Консоли администрирования функций отображения информации о событиях и статистике работы программы, получаемой с клиентских компьютеров.

Политики, параметры программы и задачи

Именованное действие, выполняемое программой «Лаборатории Касперского», называется *задачей*. В соответствии с выполняемыми функциями задачи разделяют по *типам*.

Каждой задаче соответствует набор параметров работы программы при ее выполнении. Набор параметров работы программы, общий для всех типов его задач, составляет *параметры программы*. Параметры работы программы, специфичные для каждого типа задач, образуют *параметры задачи*. Параметры программы и параметры задач не пересекаются.

Подробное описание типов задач для каждой программы «Лаборатории Касперского» приводится в Руководствах к ним.

Параметры программы, которые определяются для отдельного клиентского компьютера через локальный интерфейс или удаленно через Консоль администрирования, будем называть *локальными параметрами программы*.

Централизованная настройка параметров работы программ, установленных на клиентских компьютерах, осуществляется через определение политик.

Политика – это набор параметров работы программы в группе. Политика определяет не все параметры программы.

Параметры программы определяются параметрами политик и задач.

Каждый параметр, представленный в политике, имеет атрибут – «замок», который показывает, наложен ли запрет на изменение параметра в политиках вложенного уровня иерархии (для вложенных групп и подчиненных Серверов администрирования), в параметрах задач и локальных параметрах программы. Если в политике для параметра установлен «замок», переопределить значение будет невозможно (см. раздел «Взаимосвязь политики и локальных параметров программы» на стр. 32). Снятый флажок **Наследовать параметры из политики верхнего уровня** отменяет действие «замка» для унаследованных политик.

В группе для каждой программы определяется своя собственная политика. Для одной программы может быть определено несколько политик с различными значениями параметров, но действующая политика для программы может быть только одна.

Предусмотрена возможность активировать политику, не являющуюся действующей, при наступлении события, что позволяет, например, устанавливать более жесткие параметры антивирусной защиты в периоды вирусных эпидемий.

Также можно сформировать политику для мобильных пользователей. Она будет вступать в силу при отключении компьютера от сети предприятия.

Для разных групп параметры работы программы могут быть различными. В каждой группе может быть создана собственная политика для программы.

Вложенные группы и подчиненные Серверы администрирования наследуют политики группы более высокого уровня иерархии.

Создание и настройка задач для объектов, находящихся под управлением одного Сервера администрирования, осуществляется централизованно. Могут быть определены задачи следующих типов:

- *групповая задача* – задача, определяющая параметры работы программ, установленных на компьютерах, включенных в группу администрирования;
- *локальная задача* – задача для отдельного компьютера;
- *задача для набора компьютеров* – задача для произвольного набора компьютеров, как входящих, так и не входящих в группы администрирования;
- *задача Kaspersky Administration Kit* – задача, определяемая непосредственно для Сервера администрирования.

Для группы может быть определена групповая задача, даже если программа «Лаборатории Касперского» установлена не на все клиентские компьютеры группы. В этом случае групповая задача выполняется только для тех компьютеров, на которых данная программа установлена.

Вложенные группы и подчиненные Серверы администрирования наследуют задачи групп более высоких уровней иерархии. Задача, определенная для группы, будет выполняться не только на клиентских компьютерах, включенных в состав данной группы, но и на клиентских компьютерах, включенных в состав вложенных в нее групп и подчиненных Серверов, на всех последующих уровнях иерархии.

Задачи, созданные для клиентского компьютера локально, будут выполняться только для данного компьютера. При синхронизации клиента с Сервером администрирования локальные задачи будут добавлены в перечень сформированных задач для клиентского компьютера.

Поскольку параметры работы программы определяются политикой, в параметрах задачи могут быть переопределены те из них, на которые в политике не наложен запрет на изменение, а также параметры, которые могут быть установлены только для конкретного экземпляра задачи. Например, для задачи проверки диска это имя диска, маски проверяемых файлов и т. п.

Задача может запускаться автоматически (по расписанию) или вручную. Результаты выполнения задач сохраняются на Сервере администрирования и локально. Администратор может получать уведомления о том, как выполнена та или иная задача, а также просматривать подробные отчеты.

Информация о политиках, параметрах программы, параметрах задач для наборов компьютеров и о групповых задачах сохраняется на Сервере и распространяется на клиентские компьютеры в ходе синхронизации. При этом в данные Сервера администрирования, в свою очередь, вносятся локальные изменения, проведенные на

клиентских компьютерах и разрешенные политикой. Кроме того, обновляется список программ, функционирующих на клиентском компьютере, их статус и перечень сформированных задач.

Взаимосвязь политики и локальных параметров программы

При помощи политик могут быть установлены одинаковые значения параметров работы программы для всех компьютеров, входящих в состав группы.

Переопределить значения параметров, заданные политикой, для отдельных компьютеров в группе можно при помощи локальных параметров программы. При этом можно установить значения только тех параметров, изменение которых не запрещено политикой (параметр не закрыт «замком»).

Значение, которое использует программа на клиентском компьютере (см. рис. ниже), определяется наличием «замка» у параметра в политике:

- Если на изменение параметра наложен запрет, на всех клиентских компьютерах используется одно и то же значение – заданное политикой.

- Если запрет не наложен, то на каждом клиентском компьютере программа использует локальное значение параметра, а не то, которое указано в политике. При этом значение параметра может изменяться через локальные параметры программы.

Рисунок 10. Политика и локальные параметры программы

Таким образом, при выполнении задачи на клиентском компьютере программа использует параметры, заданные двумя разными способами:

- параметрами задачи и локальными параметрами программы, если в политике не был установлен запрет на изменение параметра;

- политикой группы, если в политике был установлен запрет на изменение параметра.

Локальные параметры программы изменяются после первого применения политики в соответствии с параметрами политики.

КОНЦЕПЦИЯ РАБОТЫ KASPERSKY ADMINISTRATION KIT

В этом разделе описываются основные принципы работы программы, способы решения отдельных задач, а также дается краткий обзор пользовательского интерфейса и приемов работы с ним.

В ЭТОМ РАЗДЕЛЕ

РАЗВЕРТЫВАНИЕ СИСТЕМЫ АНТИВИРУСНОЙ ЗАЩИТЫ

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

- Посредством удаленной централизованной установки программ на клиентские компьютеры. При этом установка программ и подключение к системе централизованного удаленного управления происходит автоматически, не требует какого-либо вмешательства со стороны администратора и позволяет устанавливать антивирусное программное обеспечение на любое количество клиентских компьютеров.

- Путем локальной установки программ на каждый клиентский компьютер. В этом случае установка необходимых компонентов на клиентские компьютеры и рабочее место администратора производится вручную, параметры подключения клиентов к Серверу задаются при установке Агента администрирования. Этот вариант развертывания используется в том случае, когда невозможно провести удаленную централизованную установку.

Удаленная установка может быть использована для инсталляции любых программ по выбору пользователя. Однако следует помнить, что Kaspersky Administration Kit поддерживает управление только программами «Лаборатории Касперского», в дистрибутив которых входит специализированный компонент – плагин управления программой.

СОВМЕСТИМОСТЬ С CISCO NETWORK ADMISSION CONTROL (NAC)

Kaspersky Administration Kit предоставляет возможность задать соответствие между условиями антивирусной защиты компьютера и статусами безопасности Cisco Network Admission Control (NAC).

Для этого необходимо сформировать условия, при которых клиентскому компьютеру будут присваиваться статусы безопасности Cisco Network Admission Control (NAC): *Healthy*, *Checkup*, *Quarantine* или *Infected*. Если клиентский компьютер не подпадает ни под одно из условий, ему будет присвоен статус *Unknown*. Статус *Healthy* присваивается только при выполнении всех условий, статусы *Checkup*, *Quarantine* или *Infected* – при выполнении хотя бы одного из них.

СОВМЕСТИМОСТЬ С MICROSOFT NETWORK ACCESS PROTECTION (NAP)

Kaspersky Administration Kit предоставляет возможность интеграции в платформу Microsoft Network Access Protection (NAP). Microsoft NAP позволяет регулировать доступ клиентских компьютеров в сеть. Microsoft NAP предполагает, что в сети выделен сервер с установленной операционной системой Microsoft Windows Server 2008, на который установлена служба PVS (Posture Validation Server), а на клиентских компьютерах установлены NAP-совместимые операционные системы: Microsoft Windows Vista, Microsoft Windows XP с установленным Пакетом обновлений 3, Microsoft Windows 7.

- *Для интеграции Kaspersky Administration Kit нужно выполнить следующие действия:*

1. Развернуть Kaspersky Administration Kit в сети обычным образом.

2. Установить на PVS Kaspersky Lab System Health Validator (SHV). Для этого при установке Kaspersky Administration Kit на этапе выбора компонентов программы установите флажок напротив средства проверки работоспособности системы Kaspersky Lab System Health Validator (SHV).

   При этом на клиентские компьютеры будет установлен Агент администрирования, который в Microsoft NAP играет роль агента работоспособности системы Kaspersky Lab System Health Agent (SHA), передавая Microsoft NAP-агенту информацию о параметрах антивирусной защиты и их изменениях на клиентском компьютере.

   В результате Kaspersky Lab System Health Validator (SHV) появится в списке доступных SHV в консоли PVS, где можно будет настроить правила проверки данных клиентских компьютеров, собираемых Агентом администрирования.

СОЗДАНИЕ СИСТЕМЫ ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ АНТИВИРУСНОЙ ЗАЩИТОЙ

Первый этап построения системы централизованного управления антивирусной защитой сети предприятия при помощи программного комплекса Kaspersky Administration Kit – проектирование структуры групп администрирования. На данном этапе необходимо решить следующие задачи:

1. Выделить в сети изолированные участки и определить, какое количество Серверов администрирования потребуется установить.

2. Определить, какие компьютеры в составе сети предприятия будут выполнять функции главного Сервера администрирования и подчиненных Серверов, какие – рабочих мест администратора и клиентских компьютеров. Клиентскими должны стать все компьютеры, на которые предполагается установить программы «Лаборатории Касперского».

3. Решить, по какому признаку будет осуществляться объединение клиентских компьютеров в группы, и определить иерархию групп.

4. Выбрать, какой вид развертывания системы антивирусной защиты будет использоваться: удаленная или локальная установка.

На следующем этапе администратор должен создать структуру папок Сервера администрирования путем установки соответствующих программных компонентов Kaspersky Administration Kit на компьютеры сети предприятия, а именно:

1. Установить Сервер администрирования на компьютеры, входящие в состав сети предприятия.

2. Установить Консоль администрирования на компьютеры, с которых будет осуществляться управление.

3. Принять решение о назначении администраторов Kaspersky Administration Kit, определить, какие еще категории пользователей будут работать с системой, и закрепить за каждой категорией перечень выполняемых функций.

   Система допускает одновременную работу администраторов с одними и теми же ресурсами. Действительными будут последние по времени применения параметры. В этом случае все действия, осуществляемые администраторами, должны быть согласованы.

4. Сформировать группы пользователей и предоставить каждой из них права доступа, необходимые для выполнения функций, возложенных на ее пользователей.

После этого необходимо создать иерархию Серверов администрирования, для каждого Сервера построить иерархию групп администрирования и провести распределение компьютеров в соответствующие группы.

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

Не все программы «Лаборатории Касперского», управление которыми доступно через Kaspersky Administration Kit, могут быть установлены на клиентские компьютеры удаленно. Подробную информацию об этом см. в Руководствах к соответствующим программам.

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

На заключительном этапе производится настройка установленных программ посредством определения и применения групповых политик (см. раздел «Управление политиками» на стр. 53) и создание необходимых задач (см. раздел «Локальные параметры программы» на стр. 57).

Программа предоставляет возможность создать систему централизованного управления антивирусной защитой с минимальными параметрами с помощью мастера первоначальной настройки (см. раздел «Мастер первоначальной настройки» на стр. 44). При этом организуется структура групп администрирования, идентичная доменной структуре Windows-сети, и формируется система антивирусной защиты с использованием Антивируса Касперского для Windows Workstations версии 6.0 MP4.

После создания структуры папок Сервера администрирования, установки и настройки антивирусной защиты администраторам рекомендуется регулярно выполнять мероприятия по обслуживанию сети (см. раздел «Обслуживание» на стр. 71).

Подключение клиентских компьютеров к Серверу администрирования

Взаимодействие между клиентскими компьютерами и Сервером администрирования осуществляется в процессе подключения клиентов к Серверу. Эту функциональность обеспечивает Агент администрирования, установленный на клиентских компьютерах.

Подключение производится для выполнения следующих операций:

- синхронизации списка программ, установленных на клиентском компьютере;

- синхронизации политик, параметров программы, задач и параметров задач;
- получения Сервером текущей информации о состоянии программ и выполнении задач;
- доставки на Сервер информации о событиях, которые он должен обработать.

Основной способ подключения клиентских компьютеров к Серверу состоит в том, что клиент соединяется с Сервером. Данный вид соединения выполняется при автоматической синхронизации данных клиента и Сервера, а также доставке на Сервер информации о событиях в работе программ.

Автоматическая синхронизация производится периодически, в соответствии с параметрами Агента администрирования (например, раз в 15 минут). Интервал между соединениями задается администратором.

Информация о событии доставляется на Сервер сразу после того, как оно произошло.

Для клиентского компьютера предусмотрен параметр **Не разрывать соединение с Сервером администрирования**, который определяет, будет ли завершаться соединение клиента с Сервером по окончании перечисленных выше операций. Непрерывное соединение необходимо в том случае, если требуется постоянный контроль состояния программ, а Сервер по тем или иным причинам не может устанавливать соединение с клиентом (соединение защищено межсетевым экраном, запрещено открывать порты на клиентском компьютере, неизвестен IP-адрес клиента, и т. д.).

Процесс синхронизации может быть также произведен администратором вручную при помощи команды **Синхронизировать** контекстного меню (см. раздел «Контекстное меню» на стр. 25) клиентского компьютера. В этом случае используется вспомогательный способ подключения, при котором соединение инициирует Сервер. Для этого на клиентском компьютере открывается UDP-порт. Сервер посылает на UDP-порт запрос на соединение. В ответ на него производится проверка прав Сервера на подключение к клиенту (на основании цифровой подписи Сервера администрирования), и, если они наличествуют, осуществляется соединение.

Второй способ соединения используется также при обращении к данным клиента на Сервере: для получения текущей информации о состоянии программ, задач и статистики работы программ.

Защищенное подключение к Серверу администрирования

Обмен информацией между клиентскими компьютерами и Сервером администрирования, а также подключение Консоли к Серверу администрирования может производиться с использованием протокола SSL (Secure Socket Layer). Он позволяет идентифицировать взаимодействующие стороны, осуществлять шифрование передаваемых данных и обеспечивать их защиту от изменения при передаче. В основе используемого при защищенном соединении SSL-протокола лежит аутентификация взаимодействующих сторон и шифрование данных по методу открытых ключей.

В этом разделе

Сертификат Сервера администрирования

Аутентификация Сервера администрирования при подключении к нему Консоли администрирования и обмене информацией с клиентскими компьютерами осуществляется на основании *сертификата Сервера администрирования*. Сертификат используется также для аутентификации между главными и подчиненными Серверами администрирования.

Сертификат Сервера администрирования создается при установке компонента Сервер администрирования и хранится на Сервере администрирования в папке установки программы во вложенной папке Cert.

Сертификат Сервера администрирования создается только один раз, при установке. Его рекомендуется сохранять средствами мастера установки. В случае если сертификат Сервера администрирования утерян, для его восстановления необходимо провести переустановку компонента Сервер администрирования и восстановление данных (см. раздел «Резервное копирование и восстановление данных Сервера администрирования» на стр. 90).

Аутентификация Сервера при подключении клиентского компьютера

При первом подключении клиентского компьютера к Серверу Агент администрирования получает сертификат Сервера администрирования и сохраняет его локально.

Если установка Агента администрирования проводится локально, сертификат Сервера администрирования может быть выбран администратором вручную.

На основании полученной копии сертификата осуществляется проверка прав и полномочий Сервера администрирования при следующих соединениях.

В дальнейшем, при каждом подключении клиентского компьютера к Серверу Агент администрирования запрашивает сертификат Сервера администрирования и сравнивает его с локальной копией. Если они не совпадают, доступ Сервера администрирования к клиентскому компьютеру не разрешается.

Если соединение инициирует Сервер администрирования, аналогичным образом сначала проверяется поступивший с Сервера администрирования запрос на соединение через UDP-порт.

Аутентификация Сервера при подключении Консоли

При первом после установки подключении к Серверу Консоль администрирования запрашивает сертификат Сервера администрирования и сохраняет его локально на рабочем месте администратора. На основании полученной копии сертификата при последующих подключениях к Серверу администрирования с данным именем будет осуществляться идентификация Сервера.

Если сертификат Сервера администрирования не совпадает с копией сертификата, хранящейся на рабочем месте администратора, выводится запрос на подтверждение подключения к Серверу с заданным именем и получение нового сертификата. При удачном подключении Консоль администрирования сохраняет копию нового сертификата Сервера администрирования, она будет использоваться для идентификации Сервера в дальнейшем.

Идентификация клиентских компьютеров на Сервере администрирования

Идентификация клиентских компьютеров осуществляется на основании имен клиентских компьютеров. Имя клиентского компьютера является уникальным среди всех имен компьютеров, подключенных к Серверу администрирования.

Имя клиентского компьютера передается на Сервер администрирования либо при опросе Windows-сети и обнаружении в ней нового компьютера, либо при первом подключении установленного на клиентский компьютер Агента администрирования. По умолчанию имя совпадает с именем компьютера в Windows-сети (NetBIOS-имя). Если на Сервере администрирования клиентский компьютер с таким именем уже зарегистрирован, то к имени нового клиентского компьютера будет добавлено окончание с порядковым номером, например: **<Имя>-1**, **<Имя>-2** и т. д. Под этим именем клиентский компьютер включается в состав группы администрирования.

Права доступа к Серверу администрирования и его объектам

В Kaspersky Administration Kit предусмотрены следующие типы разрешений на доступ к функциональности программы:

- **Все** – включает в себя все разрешения (см. ниже).
- **Чтение** – просмотр параметров объектов Kaspersky Administration Kit без права выполнения операций, создания новых объектов и изменения существующих.
- **Запись** – изменение параметров объектов Kaspersky Administration Kit, а также создание новых объектов без права выполнения операций над объектами.
- **Выполнение** – выполнение операций над объектами Kaspersky Administration Kit без права создания новых объектов и изменения существующих.
- **Изменение прав доступа** – предоставление пользователям и группам пользователей прав доступа к функциональности Kaspersky Administration Kit.
- **Изменение параметров регистрации событий**.
- **Изменение параметров отправки уведомлений**.
- **Удаленная установка программ «Лаборатории Касперского»**.
- **Удаленная установка сторонних программ** – подготовка инсталляционных пакетов и удаленная установка на клиентские компьютеры программ сторонних производителей, а также программ «Лаборатории Касперского».
- **Изменение параметров иерархии Серверов администрирования**.
- **Сохранение содержимого сетевых списков** – копирование файлов из резервного хранилища, карантина и файлов с отложенным лечением с клиентских компьютеров на компьютер, где установлена Консоль администрирования.
- **Создание туннелей** – создание туннелированного соединения между компьютером, на котором установлена Консоль администрирования, и клиентским компьютером.

После установки Сервера администрирования права на подключение к Серверу и работе с его объектами по умолчанию предоставляются пользователям, входящим в группы **KLAdmins** и **KLOperators**.

Данные группы формируются при установке компонента Сервер администрирования. В зависимости от того, какая учетная запись была выбрана для запуска службы Сервера администрирования, они создаются:

- в домене, в который входит Сервер администрирования, и на компьютере Сервера администрирования, если Сервер администрирования запускается под учетной записью пользователя, входящего в домен;
- только на компьютере Сервера администрирования, если Сервер запускается под учетной записью системы.

Группе **KLAdmins** предоставлены все права, группе **KLOperators** – права на **Чтение** и **Выполнение**. Изменить набор прав, предоставленных группе **KLAdmins**, невозможно.

Пользователей, входящих в группу **KLAdmins**, будем называть **администраторами Kaspersky Administration Kit**, пользователей из группы **KLOperators** – **операторами Kaspersky Administration Kit**.

Просмотр групп **KLAdmins** и **KLOperators** и внесение необходимых изменений осуществляется при помощи стандартных средств администрирования Windows – **Управление** → **Локальные пользователи и группы**.

Помимо пользователей, входящих в группу **KLAdmins**, права администратора предоставляются:

- администраторам домена, компьютеры которого входят в состав этой группы администрирования данного Сервера;
- локальным администраторам компьютеров, на которых установлен Сервер администрирования.

Локальные администраторы могут быть исключены из списка пользователей, имеющих права на администрирование Сервера.

Все операции, инициированные администраторами Kaspersky Administration Kit, будут выполняться с правами учетной записи Сервера администрирования. Для каждого Сервера администрирования может быть сформирована своя группа **KLAdmins**, обладающая правами только в рамках работы с этим Сервером.

Если компьютеры, относящиеся к одному домену, образуют группы администрирования разных Серверов, то администратор домена является администратором Kaspersky Administration Kit в рамках всех групп. При этом группа **KLAdmins** для этих групп администрирования едина и создается при установке первого Сервера администрирования. Ее пополнение может быть проведено средствами администрирования операционной системы. Операции, инициированные администраторами Kaspersky Administration Kit, будут выполняться с правами соответствующего Сервера администрирования.

Права пользователей (см. раздел «Предоставление прав» на стр. 41) в программе Kaspersky Administration Kit устанавливаются на основании Windows-аутентификации пользователей в сети.

После установки программы администратор Kaspersky Administration Kit может:

- изменить права, предоставляемые группам **KLOperators**;
- предоставить права доступа к функциональности программы Kaspersky Administration Kit другим группам пользователей и отдельным пользователям, зарегистрированным на компьютере, где установлена Консоль администрирования;
- предоставить различные права доступа для работы в каждой группе администрирования.

УПРАВЛЕНИЕ КОМПЬЮТЕРАМИ СЕТИ

В рамках мероприятий по управлению компьютерами сети предприятия определяются:

- Серверы администрирования (см. раздел «Подключение к Серверу администрирования» на стр. 40) и их иерархия (см. раздел «Подчиненные Серверы администрирования» на стр. 50);
- права доступа к Серверу администрирования (см. раздел «Предоставление прав» на стр. 41);
- состав и иерархия групп администрирования (см. раздел «Создание, просмотр и изменение структуры групп администрирования» на стр. 44).

В ЭТОМ РАЗДЕЛЕ

Подключение к Серверу администрирования

Консоль администрирования можно использовать для подключения удаленных клиентских компьютеров к Серверу администрирования через интернет.

После запуска Kaspersky Administration Kit главное окно программы содержит дерево консоли, в котором отображается верхний уровень иерархии пространства имен **Kaspersky Administration Kit**. Чтобы в главном окне загрузилось отображение структуры папок Сервера администрирования, следует добавить в дерево консоли узел – Сервер и подключиться к нужному Серверу администрирования (см. рис. ниже).

Подключить удаленные клиентские компьютеры к Серверу администрирования можно с помощью Консоли администрирования через интернет.

Программа получает информацию о структуре папок с Сервера администрирования и отображает ее в дереве консоли.

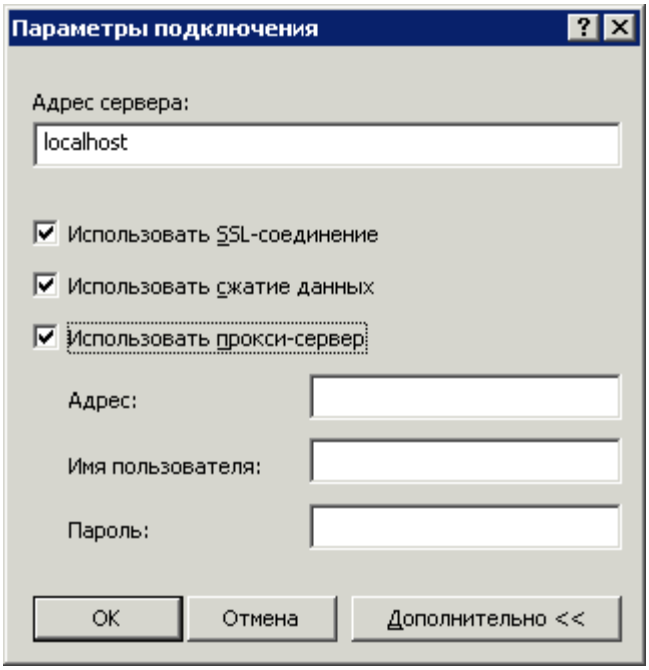

Рисунок 11. Установка соединения с Сервером администрирования

Пользователям, не обладающим правами на подключение, будет отказано в доступе к Серверу администрирования. Проверка прав осуществляется на основании Windows-аутентификации пользователя в сети.

Если в структуре сети предприятия установлено несколько Серверов администрирования, вы можете работать с каждым из них с единого рабочего места администратора. Для **перехода** к группам администрирования другого Сервера можно подключиться к нужному Серверу, либо добавить в дерево консоли несколько Серверов и подключиться к каждому из них.

Вы можете параллельно работать с несколькими Серверами администрирования только в том случае, если являетесь оператором или администратором Kaspersky Administration Kit для каждого Сервера либо обладаете необходимыми правами на всех Серверах.

Предоставление прав

После установки Сервера администрирования права на подключение к Серверу и работу с ним предоставляются пользователям, входящим в группы (см. раздел «Права доступа к Серверу администрирования и его объектам» на стр. 38) **KLAdmins** и **KLOperators**.

Вы можете изменить права доступа для группы **KLOperators**, предоставить права на работу с Сервером другим группам пользователей и отдельным пользователям, зарегистрированным на компьютере, где установлена Консоль администрирования.

Предоставление прав доступа ко всем объектам Сервера администрирования выполняется в окне свойств Сервера администрирования на закладке **Безопасность** (см. рис. ниже).

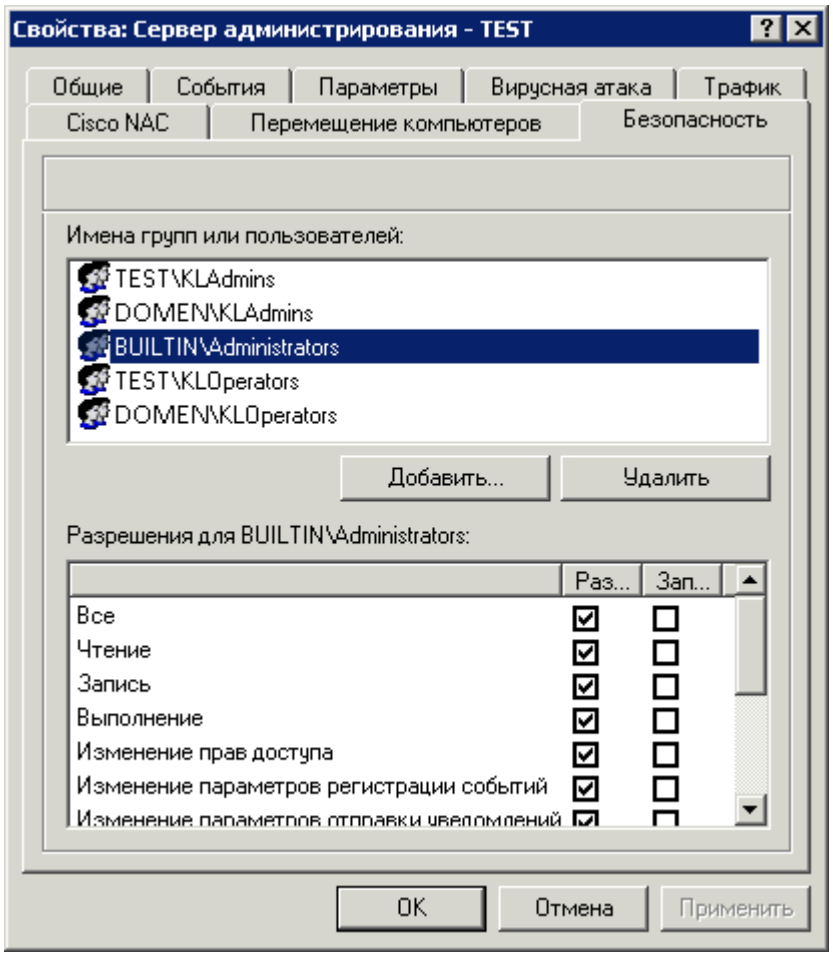

Рисунок 12. Предоставление прав доступа к Серверу администрирования

Предусмотрена возможность отдельно назначить права доступа к каждой группе администрирования или к другим объектам Сервера администрирования, например, задачам Сервера администрирования. Эта настройка выполняется в окне свойств объекта на закладке **Безопасность**.

Отследить действия пользователя администратор может с помощью событий в работе Сервера администрирования, фиксируемых в журналах событий. Эти события имеют уровень важности **Информационное сообщение**; типы событий начинаются со слова **Аудит**. В дереве консоли в папке **События** они отображаются во вложенной папке **События аудита**.

Просмотр информации о компьютерной сети. Домены, IP-диапазоны и группы Active Directory

Информация о структуре компьютерной сети и входящих в ее состав компьютерах представлена в папке Нераспределенные компьютеры дерева консоли.

Папка **Нераспределенные компьютеры** содержит три вложенные папки:

- **Домены**.
- **Active Directory**.

- **IP-диапазоны**.

Папка **Домены** 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 групп администрирования. При включении компьютера в какую-либо группу информация о нем сразу же удаляется из папки. При исключении компьютера из состава группы администрирования, информация о нем вновь появляется в соответствующей папке.

Отображение компьютеров в папке **Active Directory** строится на основании структуры Active Directory.

Отображение компьютеров в папке **IP-диапазоны** строится на основании структуры сформированных в сети IP-диапазонов. Структуру папки **IP-диапазоны** администратор может формировать путем создания IP-диапазонов и изменения параметров существующих.

По умолчанию в виде IP-диапазонов отображаются только те диапазоны, в состав которых входит Сервер администрирования.

Панель задач папки **Нераспределенные компьютеры** содержит ссылки перехода к настройке параметров и просмотру содержимого вложенных папок.

Содержимое каждой из папок **Домены**, **Active Directory** или **IP-диапазоны** отображается в панели результатов в виде таблицы. Полный перечень граф панели результатов для каждого объекта Консоли администрирования приведен в Справочном руководстве. Если структура многоуровневая, то в ней имеются вложенные объекты, и она отображается в дереве консоли. Конечные элементы иерархии (клиентские компьютеры) в дереве консоли не отображаются.

Создание группы **Нераспределенные компьютеры** и ее поддержка в актуальном состоянии осуществляется Сервером администрирования. В соответствии с установленными параметрами Сервер администрирования регулярно проводит опрос сети предприятия на предмет появления в ней новых компьютеров и отключения компьютеров от сети.

Сервер администрирования может проводить следующие виды опросов сети:

- *Опрос Windows-сети*. Различают два вида опроса: быстрый и полный. В процессе быстрого опроса собирается только информация о списке NetBIOS-имен компьютеров всех доменов и рабочих групп сети. В ходе полного опроса запрашивается дополнительная информация о компьютерах: операционная система, IP-адрес, DNS-имя и т. п.

  Для просмотра и изменения параметров опроса Windows-сети воспользуйтесь ссылкой **Изменить параметры опроса**, расположенной в блоке **Опрос сети Microsoft** в панели задач папки **Нераспределенные компьютеры**.

- *Опрос групп Active Directory*. При этом в базу данных Сервера администрирования записывается информация о структуре организационных единиц Active Directory, а также информация о DNS-именах компьютеров.

  Для просмотра и изменения опроса групп Active Directory воспользуйтесь ссылкой **Изменить параметры опроса**, расположенной в блоке **Опрос Active Directory** в панели задач папки **Нераспределенные компьютеры**.

- *Опрос IP-диапазонов*. При этом Сервер администрирования опрашивает сформированные IP-диапазоны с помощью ICMP-пакетов и собирает полную информацию о компьютерах, входящих в диапазон.

  Для просмотра и изменения параметров опроса IP-диапазонов воспользуйтесь ссылкой **Изменить параметры опроса**, расположенной в блоке **Опрос IP-диапазонов** в панели задач папки **Нераспределенные компьютеры**.

На основании полученной информации и данных о структуре компьютерной сети Сервер администрирования обновляет содержимое папки **Нераспределенные компьютеры**. При этом обнаруженные в сети компьютеры могут автоматически включаться в состав определенных групп администрирования. Предусмотрена возможность отключения опроса компьютеров, отображаемых в папке **Нераспределенные компьютеры**.

В папке **Нераспределенные компьютеры** главного Сервера администрирования, в числе прочих, отображаются и компьютеры, входящие в состав компьютерных сетей, к которым принадлежат подчиненные Серверы администрирования.

МАСТЕР ПЕРВОНАЧАЛЬНОЙ НАСТРОЙКИ

Программа Kaspersky Administration Kit предоставляет возможность провести настройку минимального набора параметров, необходимых для построения системы централизованного управления антивирусной защитой с помощью мастера первоначальной настройки. В результате работы мастера будут:

- добавлены лицензии, которые можно автоматически распространять на компьютеры в группах администрирования, установив флажок в одноименном поле;
- сформированы параметры рассылки оповещений по электронной почте и средствами NET SEND о событиях, регистрируемых в работе Сервера администрирования, а также всех остальных программ «Лаборатории Касперского». (Чтобы уведомление прошло успешно, на Сервере администрирования и всех компьютерах-получателях должна быть запущена служба сообщений Messenger);
- сформированы политики и задачи самого верхнего уровня иерархии для Антивируса Касперского для Windows Workstations и Windows Servers 6.0 MP4, а также задачи Сервера администрирования: получения обновлений и резервного копирования данных.

Политики для Антивируса Касперского для Windows Workstations версий 6.0 MP4 не создаются, если в папке **Управляемые компьютеры** политики для данных программ уже существуют. Если групповые задачи для группы **Управляемые компьютеры** и задачи обновления и резервного копирования данных Сервера администрирования с такими именами уже сформированы, они также не будут создаваться.

Предложение запустить мастер первоначальной настройки выводится при первом после установки Сервера администрирования подключении к нему. По завершении работы мастера предлагается запустить мастер удаленной установки.

СОЗДАНИЕ, ПРОСМОТР И ИЗМЕНЕНИЕ СТРУКТУРЫ ГРУПП АДМИНИСТРИРОВАНИЯ

Структура групп администрирования, то есть иерархия подчиненных Серверов администрирования, а также перечень и состав групп администрирования определяются на этапе проектирования. Группы администрирования формируются в главном окне программы Kaspersky Administration Kit в папке **Управляемые компьютеры** (см. рис. ниже) путем создания иерархии групп и добавления в них клиентских компьютеров и подчиненных Серверов администрирования.

Сразу после установки Kaspersky Administration Kit папка **Управляемые компьютеры** содержит только пустые папки **Серверы администрирования**, **Политики**, **Групповые задачи** и **Клиентские компьютеры**. При создании администратором структуры групп администрирования в состав папки **Управляемые компьютеры** могут быть включены клиентские компьютеры и добавлены вложенные группы.

Группы администрирования отображаются в виде папок. Структура каждой из них аналогична структуре папки **Управляемые компьютеры**:

- При создании каждой группы автоматически создаются вложенные папки **Серверы администрирования**, **Политики**, **Групповые задачи** и **Клиентские компьютеры** для хранения информации и работы с подчиненными Серверами администрирования, политиками и задачами данной группы.

При включении в группу клиентских компьютеров информация о них отображается в виде таблицы в панели результатов вложенной папки **Клиентские компьютеры**.

При выборе папки в дереве консоли в панели результатов отображается ее содержимое. Полный перечень закладок и граф панели результатов для каждого объекта Консоли администрирования приведен в Справочном руководстве.

Работа с объектами папки **Управляемые компьютеры** осуществляется при помощи команд контекстного меню (см. раздел «Контекстное меню» на стр. 25) и ссылок в панели задач.

Для групп администрирования со структурой, идентичной структуре доменов и рабочих групп Windows-сети, вы можете воспользоваться мастером первоначальной настройки (см. раздел «Мастер первоначальной настройки» на стр. 44).

Чтобы сформировать спроектированную структуру вручную, выполните следующие действия:

1. Подключитесь к нужному Серверу администрирования.
2. Сформируйте иерархию групп путем последовательного создания вложенных групп.
3. Добавьте в состав групп клиентские компьютеры.
4. Добавьте подчиненные Серверы администрирования.

Структура групп администрирования отображается в папке **Управляемые компьютеры**. Вы можете получить информацию о каждом из ее объектов: подчиненных Серверах, группах и клиентских компьютерах. Предоставляются данные о том, когда был создан объект, когда последний раз редактировались его параметры (см. рис. ниже). Вы также можете посмотреть и изменить параметры взаимодействия объекта (подчиненного Сервера, клиентского компьютера или всех клиентских компьютеров в составе группы) и Сервера администрирования.

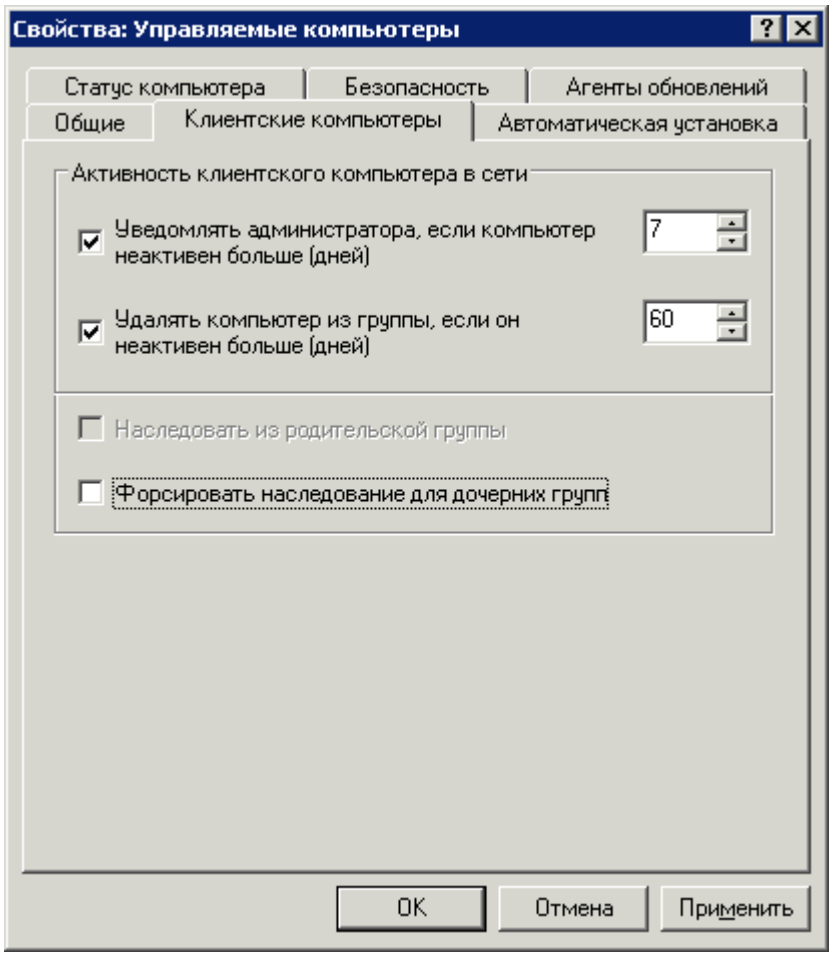

Рисунок 13. Просмотр свойств группы

Чтобы получить информацию о конкретных клиентских компьютерах, воспользуйтесь функцией поиска компьютера (см. раздел «Поиск компьютеров» на стр. 82) в сети предприятия на основании заданных критериев. При поиске может использоваться информация о подчиненных Серверах администрирования. Для поиска, сохранения и отображения информации о компьютерах в отдельной папке дерева консоли воспользуйтесь функцией создания выборок (см. раздел «Выборки компьютеров» на стр. 84).

При изменении конфигурации компьютерной сети предприятия необходимо своевременно вносить соответствующие изменения в структуру групп администрирования. Вы можете:

- добавлять в состав какой-либо группы администрирования произвольное количество групп любых уровней (в группу могут быть добавлены подчиненные Серверы администрирования и вложенные группы, образующие следующий уровень иерархии);
- определять, какие программы «Лаборатории Касперского» будут автоматически устанавливаться на все вновь включенные в состав группы клиентские компьютеры;
- добавлять в состав групп клиентские компьютеры;
- изменять иерархию объектов групп администрирования путем перемещения отдельных клиентских компьютеров и целых групп в другие группы;
- удалять из состава групп вложенные группы и клиентские компьютеры;
- добавлять подчиненные Серверы администрирования с целью уменьшения нагрузки на главный Сервер, сокращения внутреннего трафика и повышения надежности системы удаленного управления;
- переносить клиентские компьютеры из состава групп администрирования одного Сервера в группы другого.

В этом разделе

Группы

Kaspersky Administration Kit предоставляет возможность создавать собственные группы. Для добавления новой группы воспользуйтесь ссылкой **Создать подгруппу**, расположенной в панели результатов. В дереве консоли в папке **Управляемые компьютеры** (см. рис. ниже) в составе указанной вами группы появится новая папка с заданным именем. В папке автоматически создаются вложенные папки:

- **Политики**.
- **Групповые задачи**.
- **Клиентские компьютеры**.
- **Серверы администрирования**.

Наличие или отсутствие этой папки в дереве консоли определяется параметрами пользовательского интерфейса. Чтобы настроить отображение данной папки, пройдите в меню **Вид** → **Настройка интерфейса** и установите флажок в строке **Отображать подчиненные Серверы администрирования**.

Наполнение папки осуществляется на этапе определения политик группы, создания групповых задач и подчиненных Серверов.

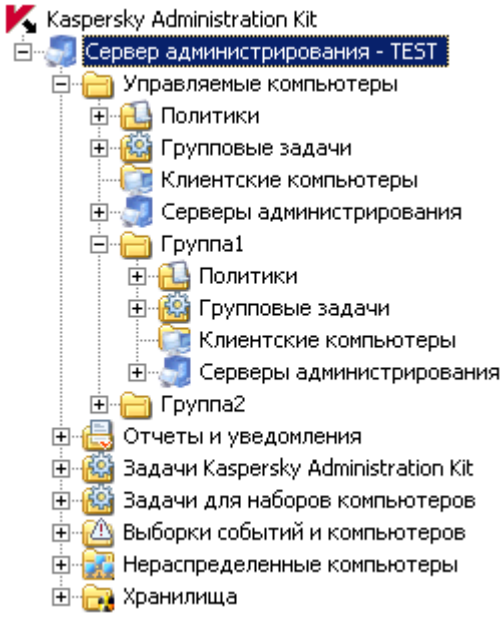

Рисунок 14. Просмотр структуры папок Сервера администрирования

В состав группы могут быть включены клиентские компьютеры и добавлены вложенные группы, образующие следующий уровень иерархии. Можно настроить отображение унаследованных политик и групповых задач во вложенных группах.

Вы также можете определить, какие программы «Лаборатории Касперского» будут автоматически устанавливаться на все вновь включенные в состав группы клиентские компьютеры.

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

Группа перемещается вместе со всеми вложенными группами, подчиненными Серверами администрирования, клиентскими компьютерами, групповыми политиками и задачами. К ней будут применены все параметры, соответствующие ее новому положению в иерархии групп администрирования.

Перемещение группы осуществляется путем стандартных команд контекстного меню **Вырезать** и **Вставить** или аналогичных пунктов в меню **Действие**, а также при помощи мыши.

При перемещении групп необходимо соблюдать правило уникальности имени группы в пределах одного уровня иерархии. Для разрешения конфликта имен перед перемещением следует изменить название. В случае несоблюдения правила уникальности к названию будет добавлено окончание **_1**, **_2** и т. д.

Невозможно изменить название группы **Управляемые компьютеры**, поскольку она является встроенным элементом Консоли администрирования.

Группа может быть удалена из состава папок Сервера администрирования, если она не содержит подчиненных Серверов администрирования, вложенных групп и клиентских компьютеров, и если для нее нет сформированных для группы задач и политик. Удаление выбранной группы осуществляется при помощи команды **Удалить** контекстного меню или аналогичного пункта в меню **Действие**.

Клиентские компьютеры

Добавление клиентского компьютера в группу позволяет применять к нему политики и задачи, созданные в группе. Для добавления клиентских компьютеров в группу воспользуйтесь ссылкой **Добавить компьютер**, расположенной в панели задач группы, в которую добавляется компьютер. В результате запускается мастер. В случае успешного завершения его работы компьютеры включаются в состав группы и отображаются в панели

результатов папки **Клиентские компьютеры** под именами, установленными для них Сервером администрирования (см. рис. ниже). Если по какой-либо причине Сервер администрирования не обнаружил клиентский компьютер, необходимо установить на него Агент администрирования и подключиться к Серверу администрирования. Сервер администрирования поместит данный компьютер в папку **Нераспределенные компьютеры**, откуда вы сможете переместить его в нужную вам группу.

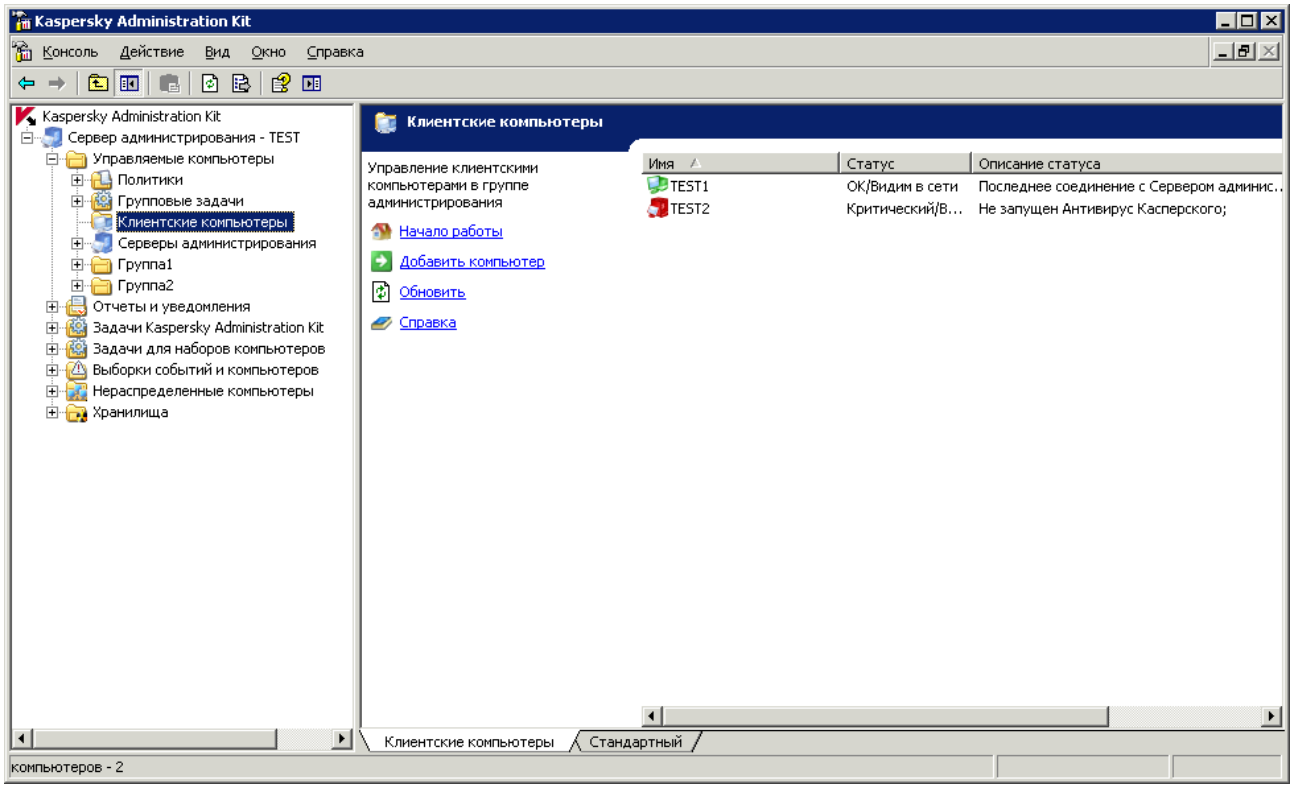

Рисунок 15. Клиентские компьютеры в группе

Рядом с именами клиентских компьютеров в панели результатов отображаются значки, характеризующие их статус. Перечень значков и соответствующих им статусов приведен в приложении к Справочному руководству.

Добавление клиентских компьютеров в состав групп администрирования может быть настроено таким образом, чтобы Сервер администрирования самостоятельно включал все вновь обнаруженные в сети компьютеры в состав определенной административной группы. Для этого в свойствах Сервера администрирования должны быть установлены соответствующие параметры (см. рис. ниже).

Добавить компьютер можно также в главном окне программы Kaspersky Administration Kit путем перемещения компьютера из папки **Нераспределенные компьютеры** в папку нужной группы администрирования при помощи мыши.

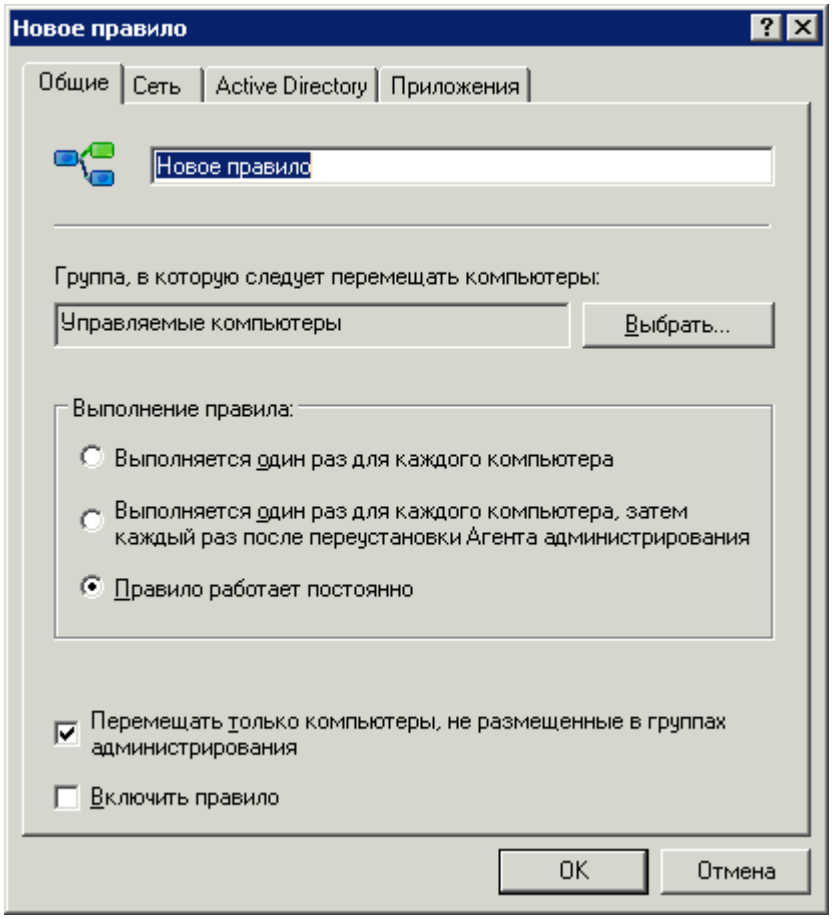

Рисунок 16. Настройка автоматического переноса новых компьютеров в группу

Вы можете переносить клиентские компьютеры из одной группы в другую, исключать из состава групп администрирования при помощи стандартных команд контекстного меню **Вырезать**, **Вставить** и **Удалить** или аналогичных пунктов в меню **Действие**. Удаленные из состава групп администрирования компьютеры перемещаются в папку **Нераспределенные компьютеры**. Операция перемещения может быть также осуществлена при помощи мыши.

Предусмотрена возможность перемещения клиентских компьютеров из групп администрирования одного Сервера в группы другого Сервера. Например, при добавлении подчиненного Сервера администрирования вы можете перенести клиентские компьютеры из групп администрирования главного Сервера в группы подчиненного Сервера. Для этого следует подключить клиентские компьютеры к новому Серверу администрирования.

Подключить клиентский компьютер к другому Серверу администрирования можно локально с клиентского компьютера. Эта операция выполняется при помощи утилиты klmover.exe, входящей в состав дистрибутива Агента администрирования. После установки Агента администрирования данная утилита располагается в корне папки установки компонента.

Подключение клиентского компьютера к другому Серверу администрирования осуществляется путем создания и запуска задачи смены Сервера администрирования. Возможен перенос как отдельных компьютеров путем создания задачи для наборов компьютеров, так и всех клиентских компьютеров из определенной группы администрирования при помощи групповой задачи. В результате выполнения задачи смены Сервера клиентские компьютеры, для которых она была сформирована и успешно завершена, отключаются от одного Сервера администрирования и появляются в папке **Нераспределенные компьютеры** другого Сервера. Перенос

клиентских компьютеров из групп администрирования одного Сервера в группы администрирования другого Сервера осуществляется вручную через Консоль администрирования.

Подчиненные Серверы администрирования

С помощью иерархии серверов для всех подчиненных Серверов администрирования и подключенных к ним клиентских компьютеров с главного Сервера могут быть выполнены следующие операции:

- создание и распространение политик для программ;
- формирование и распространение групповых задач (включая задачи удаленной установки);
- распространение полученных главным Сервером обновлений и инсталляционных пакетов;
- создание отчетов, объединяющих информацию по всем подчиненным Серверам администрирования.

Политики и задачи, полученные с главного Сервера администрирования, на подчиненном Сервере недоступны для изменения.

Для добавления подчиненного Сервера

воспользуйтесь пунктом **Создать** → **Сервер администрирования** для узла **Серверы администрирования** в нужной вам группе.

При этом запускается мастер добавления подчиненного Сервера. В результате его работы будут выполнены следующие действия:

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

Этапы подключения и настройки можно пропустить. В этом случае следует выполнить их вручную: подключиться через Консоль администрирования к Серверу, который будет подчиненным Сервером, и указать параметры его подключения к главному Серверу (см. рис. ниже).

После успешного добавления подчиненного Сервера администрирования значок и имя Сервера отображаются в папке **Серверы администрирования** в соответствующей группе.

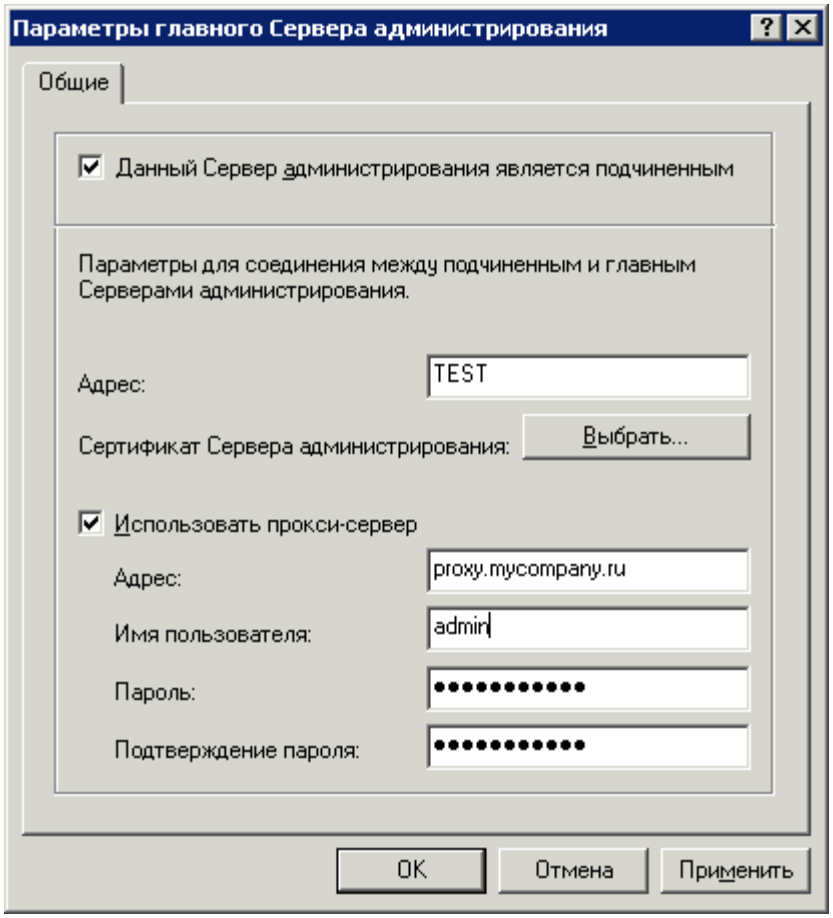

Рисунок 17. Настройка параметров подключения к главному Серверу администрирования

Работать с группами администрирования подчиненного Сервера администрирования вы можете как через узел **Серверы администрирования** главного Сервера, так и напрямую, добавив Сервер в дерево консоли в качестве нового Сервера администрирования.

Подчиненный Сервер является полноценным Сервером администрирования и выполняет все функции Сервера администрирования в рамках собственных групп администрирования.

При этом подчиненный Сервер администрирования наследует от 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 (Обычный значок политики –).
- Значения параметров унаследованной политики недоступны для изменения на подчиненном Сервере.
- Параметры, запрещенные к изменению в унаследованной политике, недоступны для изменения (значок) во всех политиках программы на подчиненном Сервере и используют значения, заданные в унаследованной политике.
- Значения параметров, не запрещенных к изменению в унаследованной политике, можно изменять (см. раздел «Взаимосвязь политики и локальных параметров программы» на стр. 32) в политиках подчиненного Сервера (значок). Если параметр не был закрыт «замком» в политике подчиненного Сервера, его также можно будет изменить (см. раздел «Взаимосвязь политики и локальных параметров программы» на стр. 32) в параметрах программы и параметрах задачи.

- Рядом с именем групповой задачи, полученной с главного Сервера администрирования, отображается значок  (обычный значок задачи – ).

Задачи удаленной установки для набора компьютеров на подчиненные Серверы не передаются. Передача групповых задач настраивается в свойствах задачи.

Обновление клиентских компьютеров подчиненного Сервера администрирования (см. раздел «Получение обновлений подчиненными Серверами и их клиентскими компьютерами» на стр. 68) может быть настроено таким образом, чтобы после получения обновлений главным Сервером автоматически запускалась задача получения обновлений подчиненным Сервером. После ее успешного завершения запускаются задачи обновления программ на клиентских компьютерах подчиненного Сервера.

УДАЛЕННОЕ УПРАВЛЕНИЕ ПРОГРАММАМИ

Kaspersky Administration Kit поддерживает управление только теми программами компании, в состав дистрибутива которых входит специализированный компонент – плагин управления программой.

Управление программами осуществляется двумя способами:

- управлением параметрами программ посредством определения политик (см. раздел «Управление политиками» на стр. 53) и редактирования локальных параметров программ (см. раздел «Локальные параметры программы» на стр. 57);
- путем создания и запуска задач (см. раздел «Управление работой программы» на стр. 57).

В ЭТОМ РАЗДЕЛЕ

Управление политиками

Создание политики для программы возможно только в случае, если на рабочее место администратора установлен плагин управления данной программой.

Для создания политики воспользуйтесь ссылкой **Создать политику**, расположенной в панели задач группы, для которой вы создаете политику. На этапе создания политики производится настройка минимального набора параметров, без которых программа не будет работать. Остальные значения устанавливаются по умолчанию и соответствуют значениям по умолчанию при локальной установке программы. Для быстрого создания политик для определенных программ воспользуйтесь ссылками **Создать политику Антивируса Касперского для Windows Workstations** и **Создать политику Антивируса Касперского для Windows Servers**, расположенными в панели задач.

Политики группы, сформированные для программ, отображаются в дереве консоли в соответствующей папке. Рядом с именами политик отображаются значки, характеризующие их статус. Перечень значков и соответствующих им статусов приведен в Справочном руководстве.

В дальнейшем вы сможете менять значения параметров, накладывать запрет на их изменение в политиках вложенных групп и в параметрах программы (см. рис. ниже).

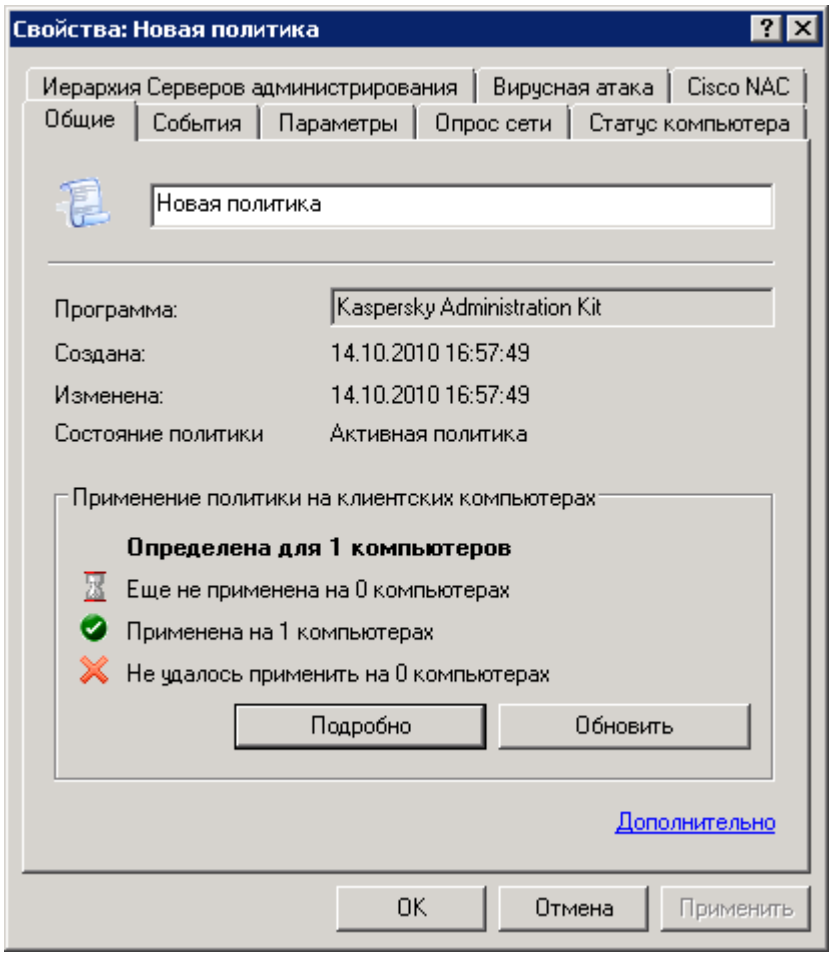

Рисунок 18. Окно свойств политики

Параметры политики, изменение которых может быть запрещено, сопровождаются значком . Для наложения запрета нажмите на него левой кнопкой мыши – значок изменится на . Такие параметры будут недоступны для изменения в параметрах программы, параметрах задач и политиках вложенных групп и подчиненных Серверов администрирования. Предусмотрена возможность снятия запрета на изменение параметров для унаследованных политик.

Политика имеет приоритет над локальными параметрами только в случае запрета на изменение параметров (установки «замка»).

После создания политики она добавляется в папку **Политики** (см. рис. ниже) соответствующей группы, отображается в дереве консоли и в качестве унаследованной политики распространяется на все вложенные группы и подчиненные Серверы администрирования, входящие в состав группы.

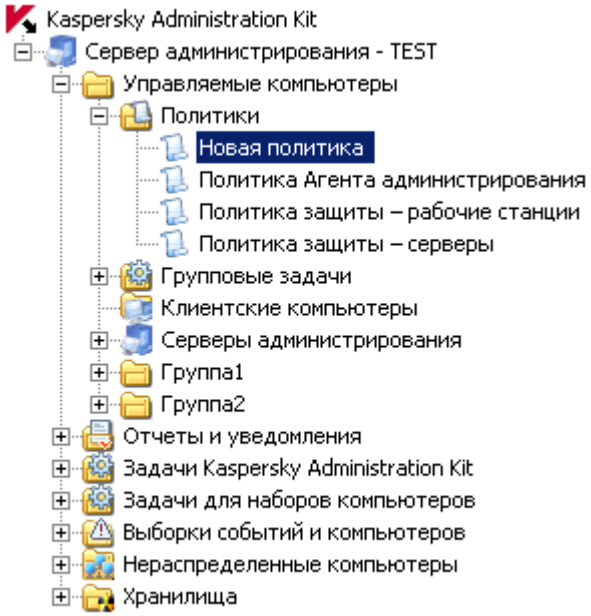

Рисунок 19. Просмотр списка политик

Сформированные политики вы можете удалять, копировать, экспортировать и импортировать из одной группы в другую при помощи команд контекстного меню выбранной в панели результатов политики. Чтобы импортировать политику из внешнего файла, воспользуйтесь ссылкой **Импортировать политику из файла**, расположенной в панели задач папки **Политики**. В открывшемся окне укажите путь к файлу с расширением .klp, содержащему параметры политики.

Для каждой программы может быть сформировано несколько групповых политик, однако действующая политика может быть только одна. В параметрах такой политики должен быть выбран параметр **Активная политика**.

Активирование политики может выполняться при наступлении события **Вирусная атака**. При этом возврат к предыдущей политике выполняется вручную.

Также можно сформировать политику для мобильных пользователей, которая будет вступать в силу сразу после отключения компьютера от Сервера администрирования. Вы можете настроить критерии активации политики для мобильных пользователей при помощи профилей Агента администрирования.

Компьютер по умолчанию считается отключенным от Сервера администрирования после трех неудачных попыток соединения. Временной интервал между попытками задается в параметрах Агента администрирования в поле **Период синхронизации (мин.)** и по умолчанию равен 15 минутам.

Результаты применения политики можно просмотреть в окне свойств политики.

Изменение локальных параметров производится автоматически в соответствии с параметрами политики при первом применении политики на клиентском компьютере, то есть:

- при добавлении клиентского компьютера в область действия политики;
- при активации политики;
- при установке на клиентский компьютер антивирусной программы, для которой сформирована политика.

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

Применение политики производится следующим образом. Если на клиентском компьютере выполняются резидентные задачи (задачи постоянной защиты), они продолжат свое выполнение с новыми значениями параметров, не прерываясь. Запущенные периодические задачи (проверка по требованию, обновление баз

программ) продолжат выполнение со старыми значениями, новый запуск будет произведен с измененными значениями параметров. Значения параметров работы программы, установленные после применения политики, вы можете посмотреть через Консоль администрирования в окне свойств конкретного клиентского компьютера.

В случае иерархической структуры Серверов администрирования подчиненные Серверы получают политики с главного Сервера администрирования и распространяют их на клиентские компьютеры. При включенном механизме наследования параметры политики можно изменять на главном Сервере администрирования. После этого подчиненные Серверы администрирования соответственно модифицируют свои политики и распространяют их на подключенные клиентские компьютеры.

При разрыве соединения между главным и подчиненным Серверами администрирования политика на подчиненном Сервере продолжает действовать с прежними параметрами. Параметры политики, измененные на главном Сервере администрирования, распространятся на подчиненный Сервер после восстановления соединения.

При отключенном механизме наследования параметры политики можно изменять на подчиненном Сервере, независимо от главного Сервера.

Если происходит разрыв соединения между Сервером администрирования и клиентским компьютером, на клиентском компьютере вступает в силу политика для мобильного пользователя (если она определена), или политика продолжает действовать с прежними параметрами до восстановления соединения.

Результаты распространения политики на подчиненные Серверы администрирования отображаются в окне свойств политики на главном Сервере администрирования.

Аналогичным образом можно просмотреть результаты распространения политики на клиентских компьютерах в окне свойств политики подчиненного Сервера администрирования, предварительно подключившись к нему.

Подробное описание настройки политик для программ «Лаборатории Касперского» приводится в Руководствах к каждой из них. Настройка политики для Агента администрирования и Сервера администрирования описана в Справочном руководстве к Kaspersky Administration Kit.

Локальные параметры программы

Система администрирования Kaspersky Administration Kit предоставляет возможность удаленно управлять локальными параметрами программ на клиентских компьютерах через Консоль администрирования (см. рис. ниже). Вы можете установить индивидуальные значения параметров работы программы для каждого клиентского компьютера в группе. Изменять можно значения только тех параметров, модификация которых не запрещена групповой политикой для данной программы: параметр не закрыт «замком» в политике.

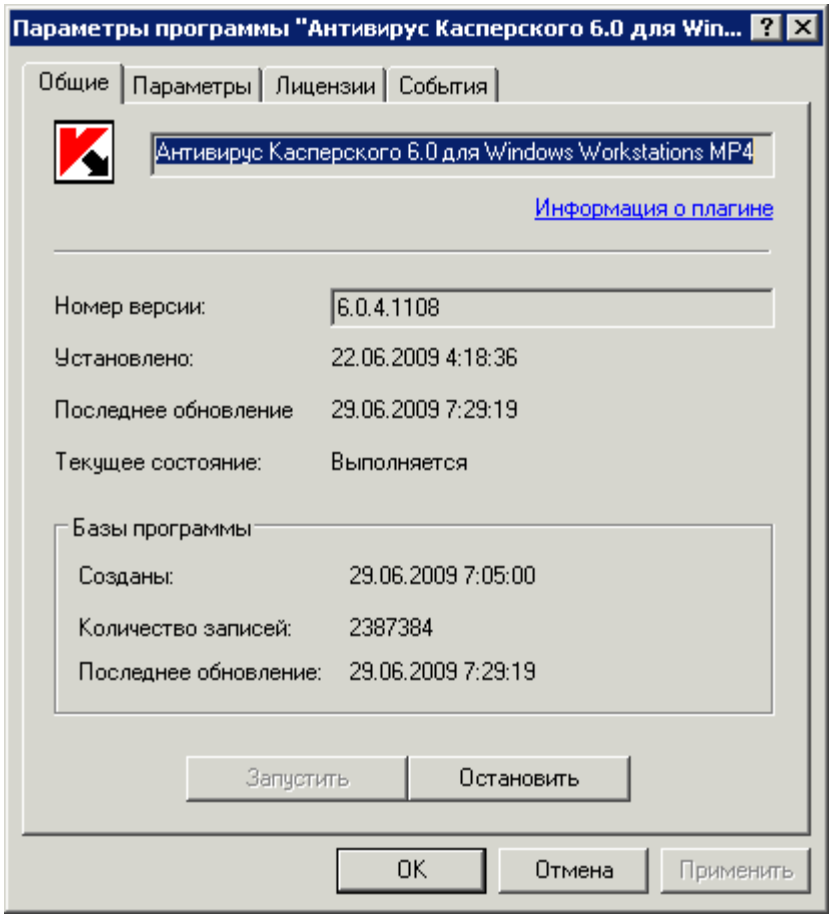

*Рисунок 20. Просмотр свойств клиентского компьютера. Закладка **Общие***

Настройка локальных параметров проводится для каждого клиентского компьютера отдельно в окне **Параметры программы «<Название программы>»**. Данное окно можно вызвать на закладке **Программы** окна **Свойства: <Имя компьютера>**, которое открывается с помощью контекстного меню выбранного клиентского компьютера.

Для каждой программы «Лаборатории Касперского» набор локальных параметров свой. Их подробное описание приводится в Руководствах к каждой из программ.

Подробное описание параметров Агента администрирования и Сервера администрирования приводится в Справочном руководстве к Kaspersky Administration Kit.

Управление работой программы

Управление работой программ, установленных на клиентских компьютерах, осуществляется путем создания и запуска задач, реализующих все основные функции: установку программ, установку лицензий, проверку файлов, обновление баз и модулей программ и др.

Сформированные задачи отображаются в дереве консоли в соответствующей папке. Рядом с именами задач отображаются значки, характеризующие их статус. Перечень значков и соответствующих им статусов приведен в Справочном руководстве.

Kaspersky Administration Kit поддерживает работу со всеми типами задач, предусмотренными при локальной работе с программой. Кроме того, программа предоставляет возможность удаленного запуска и остановки программ с помощью соответствующих задач управления для Агента администрирования. Подробное описание типов задач для каждой программы компании приводится в руководстве к ней.

Через Консоль администрирования осуществляется удаленный запуск и остановка программы с помощью соответствующих задач.

Создание задач для программы возможно только в случае, если на рабочее место администратора установлен плагин управления данной программой.

Для обеспечения защиты сети администратор может создавать любое количество различных задач (кроме задач, создаваемых в одном экземпляре) для всех программ, управление которыми может осуществляться при помощи Kaspersky Administration Kit.

Например, чтобы проверить клиентские компьютеры, являющиеся рабочими станциями, на наличие вредоносного программного обеспечения, следует создать задачу проверки по требованию для Антивируса Касперского для Windows Workstations.

Функции управления программами и общие сервисные операции реализуют задачи компонентов Kaspersky Administration Kit: Сервера администрирования и Агента администрирования. Для этих компонентов определены следующие типы задач:

- **Смена Сервера администрирования**.
- **Запуск и остановка программы**.
- **Удаленная установка программы**.
- **Удаленная деинсталляция программы**.
- **Управление клиентским компьютером**.
- **Сообщение для пользователя**.
- **Проверка обновлений**.
- **Распространение инсталляционного пакета**.
- **Рассылка отчета**.
- **Резервное копирование данных Сервера администрирования**.
- **Загрузка обновлений в хранилище**.

Создание и запуск задач перечисленных типов имеют ряд особенностей. Подробное описание работы с такими задачами приводится в Справочном руководстве к Kaspersky Administration Kit.

При работе с данными типами задач вы можете создавать групповые и локальные задачи, задачи для наборов компьютеров и задачи Kaspersky Administration Kit.

Для задачи удаленной установки возможно создание групповых задач и задач для наборов компьютеров. Для задач получения обновлений, создания резервной копии и рассылки отчетов возможно создание только задач Сервера администрирования.

Задачи получения обновлений и создания резервной копии данных Сервера администрирования могут быть созданы только в единственном экземпляре. Они создаются и выполняются только для одного компьютера – компьютера Сервера администрирования.

Групповые задачи размещаются во вложенных папках **Групповые задачи** соответствующих групп (см. рис. ниже). Для создания групповой задачи откройте в дереве консоли папку **Групповые задачи** группы, для которой вы создаете задачу, и воспользуйтесь ссылкой **Создать задачу**, расположенной в панели задач.

Задачи для наборов компьютеров размещаются в папке дерева консоли **Задачи для наборов компьютеров**. Для создания такой задачи выберите данную папку в дереве консоли и воспользуйтесь ссылкой **Создать задачу**, расположенной в панели задач.

Задачи Сервера администрирования размещаются в папке дерева консоли **Задачи Kaspersky Administration Kit**. Для создания новой задачи Сервера администрирования откройте в дереве консоли контекстное меню папки **Задачи Kaspersky Administration Kit** и воспользуйтесь командой **Создать** → **Задачу**.

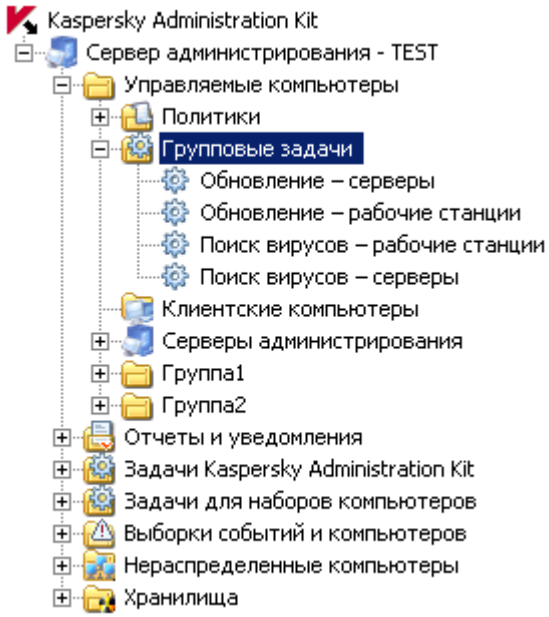

Рисунок 21. Групповые задачи

Со списком локальных задач клиентского компьютера можно ознакомиться в окне просмотра его свойств.

Для просмотра списка локальных задач выполните следующие действия:

1. Откройте в дереве консоли папку **Клиентские компьютеры** группы, содержащей нужный компьютер.

2. Выберите компьютер в списке, представленном в панели результатов.

3. Откройте окно свойств компьютера на закладке **Задачи**, которая содержит список локальных задач для выбранного компьютера. Для этого воспользуйтесь ссылкой **Просмотреть свойства клиентского компьютера**, расположенной слева от списка компьютеров в панели результатов, или пунктом **Свойства** контекстного меню выбранного компьютера.

Обмен информацией о задачах между локальной программой и информационной базой Kaspersky Administration Kit происходит в момент соединения Агента администрирования с Сервером. При этом информация о задачах, созданных локально, попадает в базу Сервера администрирования.

Вы можете вносить изменения в параметры задач, наблюдать за их выполнением, копировать, экспортировать и импортировать задачи из одной группы в другую, а также удалять при помощи команд контекстного меню и ссылок в панели задач.

Параметры работы программы при выполнении задач на каждом клиентском компьютере устанавливаются в соответствии с политикой группы (см. раздел «Взаимосвязь политики и локальных параметров программы» на стр. 32), параметрами задачи и параметрами данной программы на клиентском компьютере.

Большая часть параметров определяется политикой программы, которая выполняет эту задачу. Если изменение этих параметров в политике заблокировано, они не могут быть изменены в параметрах задачи (см. рис. ниже).

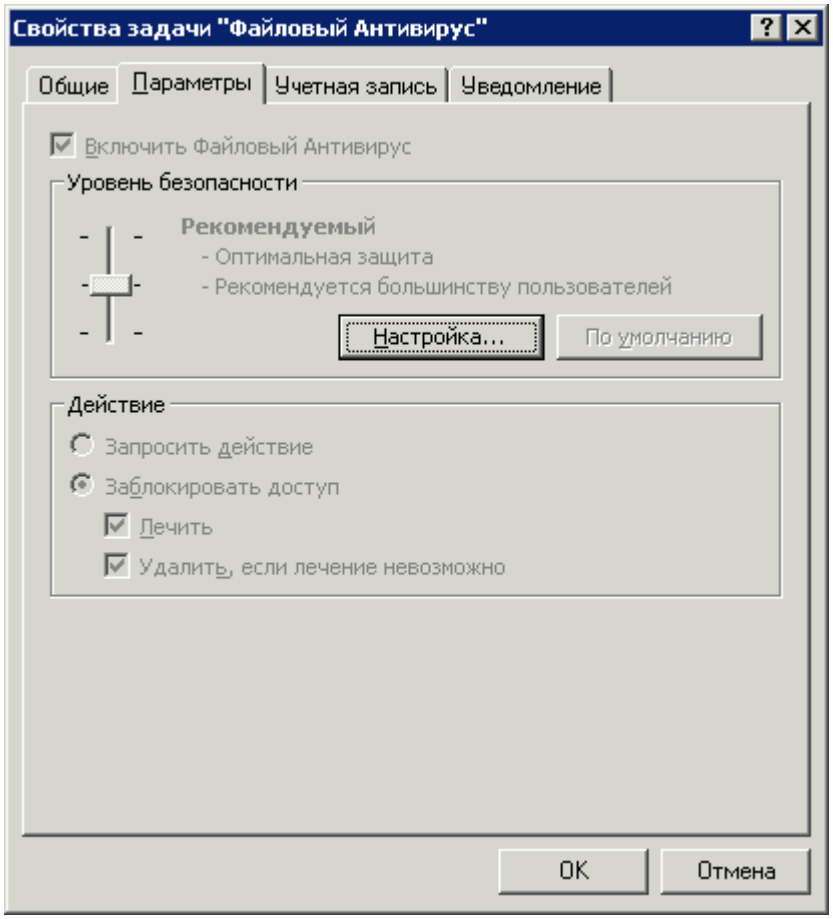

Рисунок 22. Параметры задачи, запрещенные к изменению в политике

Однако часть параметров индивидуальна для конкретной задачи, например, расписание запуска задачи, учетная запись, под которой запускается задача, область проверки для задач проверки по требованию. Значения этих параметров устанавливаются для каждой задачи и могут быть изменены после создания задачи (см. рис. ниже).

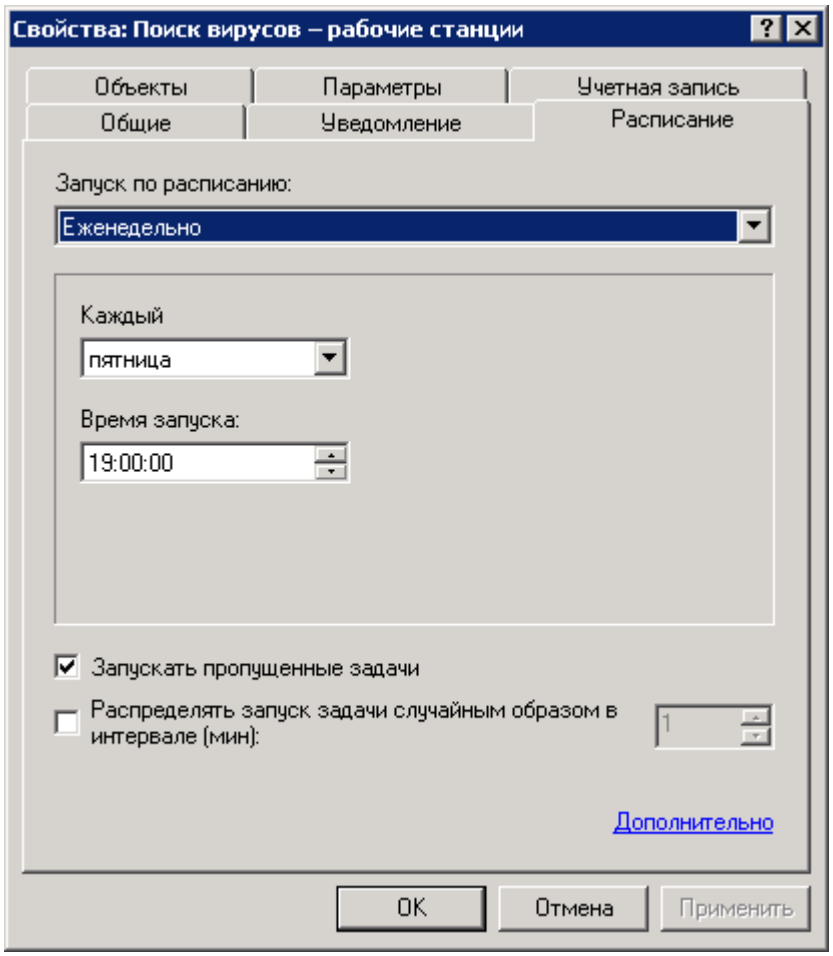

*Рисунок 23. Редактирование свойств задачи. Закладка **Расписание***

Задачи запускаются на выполнение в соответствии со своим расписанием. На компьютерах, выключенных в установленное в расписании время запуска, может автоматически загружаться операционная система при помощи функции Wake On Lan. Для этого в окне, открывающемся по кнопке **Дополнительно** на закладке **Расписание** (см. рис. выше), должен быть установлен соответствующий флажок (см. рис. ниже).

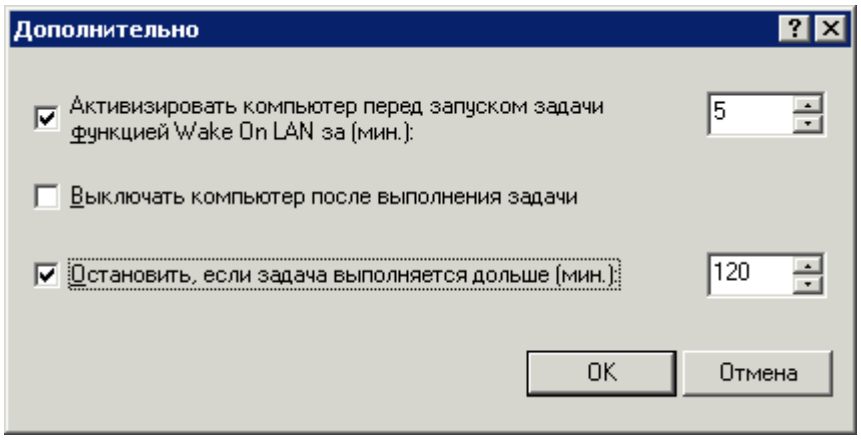

Рисунок 24. Включение автоматической загрузки операционной системы

Можно задать автоматическое выключение компьютера после выполнения задачи по расписанию.

Время выполнения задачи может быть ограничено, в этом случае она будет остановлена по истечении заданного в параметрах времени. Предусмотрена возможность отключать запуск задач по расписанию. При этом задачи не удаляются, но их запуск не будет производиться.

Вы можете запустить задачу, прервать, приостановить или возобновить ее выполнение вручную при помощи команд контекстного меню и из окна просмотра параметров задачи (см. рис. ниже). С помощью ссылок в блоке **Управление задачей** панели задач вы также можете запустить или остановить задачу.

Запуск задач на клиентском компьютере выполняется только в том случае, если запущена соответствующая программа. При остановке программы выполнение всех запущенных задач прекращается.

Наблюдать за выполнением задачи и просматривать результаты выполнения вы можете в окне свойств задачи (см. рис. ниже) или в верхней части панели задач в блоке с именем, соответствующим имени задачи.

Результаты выполнения задач фиксируются и сохраняются в соответствии с заданными параметрами в журналах событий Windows и Kaspersky Administration Kit как централизованно на Сервере администрирования, так и локально на каждом клиентском компьютере. При этом может производиться уведомление администратора и других пользователей о результатах, форма и способ оповещения также определяются параметрами задачи.

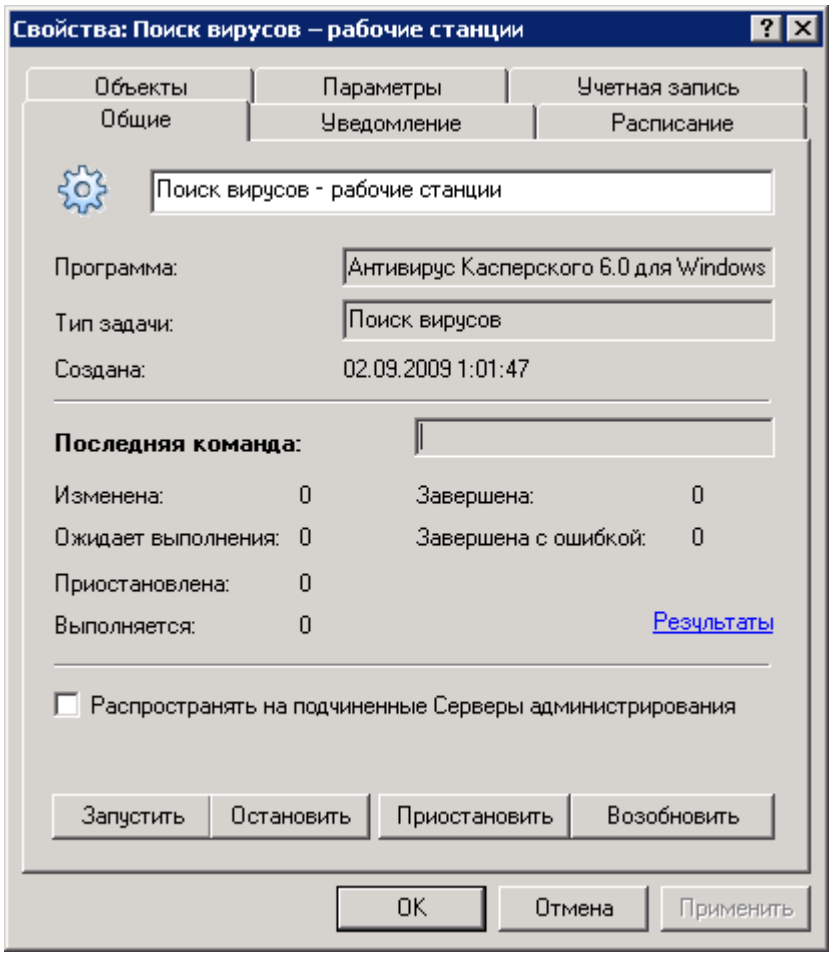

*Рисунок 25. Редактирование параметров задачи. Закладка **Общие***

Вы можете просмотреть результаты выполнения задач, зафиксированные в журнале событий Kaspersky Administration Kit, через папку **События** дерева консоли. С результатами выполнения задачи для каждого клиентского компьютера можно ознакомиться в окне просмотра его свойств.

При иерархической структуре Серверов администрирования, если в параметрах задачи установлен флажок **Распространять на подчиненные Серверы администрирования** (см. рис. выше), подчиненные Серверы получают групповые задачи с главного Сервера администрирования и распространяют их на клиентские компьютеры. Параметры групповой задачи можно изменить на главном Сервере администрирования. После

этого подчиненные Серверы администрирования соответственно модифицируют свои групповые задачи и распространяют их на подключенные клиентские компьютеры.

Результаты распространения групповой задачи на подчиненные Серверы администрирования отображаются в окне **Результаты выполнения задачи**. Данное окно можно вызвать по ссылке **Результаты** на закладке **Общие** окна свойств групповой задачи Сервера администрирования.

Аналогичным образом можно просмотреть результаты распространения групповой задачи на клиентские компьютеры в окне свойств групповой задачи подчиненного Сервера администрирования, предварительно подключившись к нему.

ОБНОВЛЕНИЕ БАЗ И ПРОГРАММНЫХ МОДУЛЕЙ

Важные факторы, влияющие на надежность системы антивирусной защиты – своевременное обновление баз программ, используемых при проверке зараженных объектов, установка критических обновлений программных модулей программ, а также регулярное обновление их версий.

Обновление баз программ, размещаемых на серверах обновлений «Лаборатории Касперского», производится каждый час. Мы рекомендуем вам проводить обновление баз с той же периодичностью и незамедлительно устанавливать все критические обновления программных модулей.

Для обновления баз и программных модулей программ, управляемых при помощи Kaspersky Administration Kit, следует создать задачу загрузки обновлений в хранилище. В результате ее выполнения с источника получения обновлений скачиваются базы и обновления программных модулей в соответствии с параметрами задачи. Полученные данные размещаются на Сервере администрирования в папке Updates папки общего доступа и могут быть распространены на клиентские компьютеры и подчиненные Серверы администрирования автоматически сразу после завершения обновления. Папка общего доступа создается при установке Сервера администрирования. По умолчанию папкой общего доступа является папка KLSHARE, расположенная в папке назначения, выбранной при установке компонента Сервер администрирования (<Диск>:\Program Files\Kaspersky Lab\Kaspersky Administration Kit).

На клиентские компьютеры обновления распространяются с помощью задач обновления для программ. Обновление подчиненных Серверов выполняется с помощью задачи загрузки обновлений Сервером администрирования. Эти задачи могут запускаться автоматически сразу после получения обновлений главным Сервером, независимо от расписания, установленного в параметрах задач.

Перед распространением на клиентские компьютеры обновления могут быть проверены на корректность. Для этого в программе предусмотрена функция проверки обновлений. Проверка обновлений предполагает распространение обновлений сначала на набор тестовых компьютеров, а затем, при отсутствии ошибок, на остальные клиентские компьютеры.

В ЭТОМ РАЗДЕЛЕ

Загрузка обновлений в хранилище Сервера администрирования

Задача получения обновлений Сервером администрирования является глобальной и может быть создана в единственном экземпляре. Данная задача создается и запускается только для одного компьютера, того, на котором установлен компонент Сервер администрирования.

Если вы использовали мастер первоначальной настройки, задача **Загрузка обновлений в хранилище** уже сформирована и расположена в дереве консоли в папке **Задачи Kaspersky Administration Kit**.

Для создания задачи получения обновлений Сервером администрирования запустите мастер создания задачи для папки **Задачи Kaspersky Administration Kit** и в качестве типа задачи выберите **Загрузка обновлений в хранилище** (см. рис. ниже).

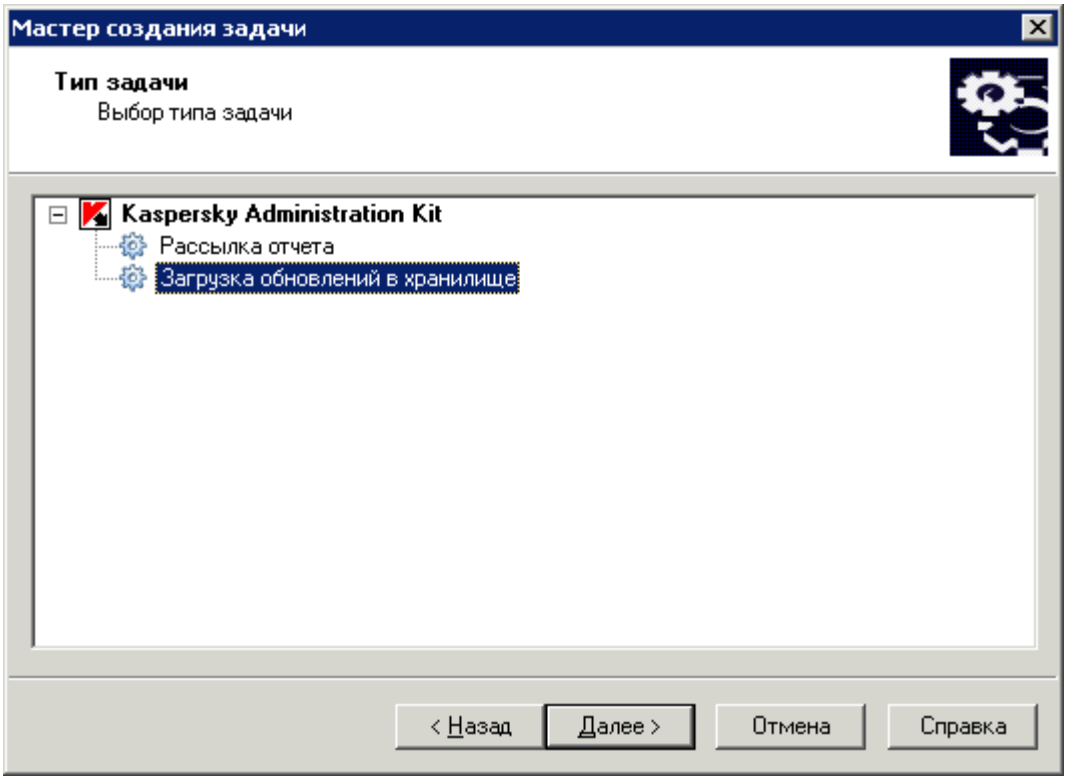

Рисунок 26. Создание задачи загрузки обновлений в хранилище

Если в компьютерной сети сформирована (или планируется) иерархия Серверов администрирования, в параметрах задачи на главном Сервере для автоматического распространения обновлений на подчиненные Серверы должен быть установлен флажок **Форсировать обновление подчиненных Серверов** (см. рис ниже). В этом случае сразу после обновления главного Сервера будут запускаться задачи обновления подчиненных Серверов (если они созданы).

При установке флажка **Форсировать обновление подчиненных Серверов** на подчиненных Серверах администрирования не происходит автоматическое создание задач получения обновлений. Их следует создать вручную для каждого подчиненного Сервера отдельно.

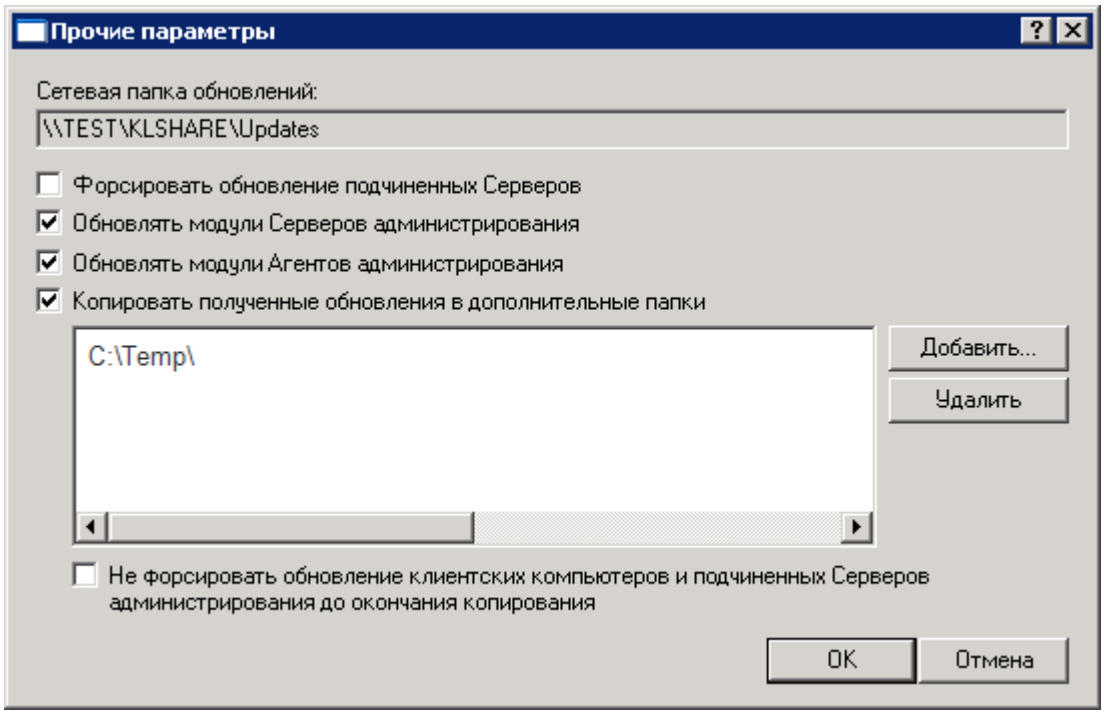

Рисунок 27. Настройка прочих параметров задачи

В результате выполнения задачи **Загрузка обновлений в хранилище** обновления баз и программных модулей копируются с источника обновлений и размещаются в папке общего доступа.

Из папки общего доступа обновления распространяются на клиентские компьютеры (см. раздел «Распространение обновлений на клиентские компьютеры» на стр. 67) и подчиненные Серверы администрирования (см. раздел «Получение обновлений подчиненными Серверами и их клиентскими компьютерами» на стр. 68).

В качестве источника обновлений для Сервера администрирования могут быть использованы следующие ресурсы:

- серверы обновлений «Лаборатории Касперского»;
- главный Сервер администрирования;
- FTP- / HTTP-сервер или сетевая папка обновлений.

Выбор ресурса зависит от параметров задачи.

В случае обновления с FTP- / HTTP-сервера или из сетевой папки для корректного обновления Сервера на эти ресурсы должна быть скопирована правильная структура папок с обновлениями, совпадающая со структурой, формируемой при копировании обновлений программными средствами «Лаборатории Касперского».

Просмотреть информацию о полученных обновлениях можно в дереве консоли в папке **Хранилища** → **Обновления**. Перечень обновлений представлен в панели результатов (см. рис. ниже).

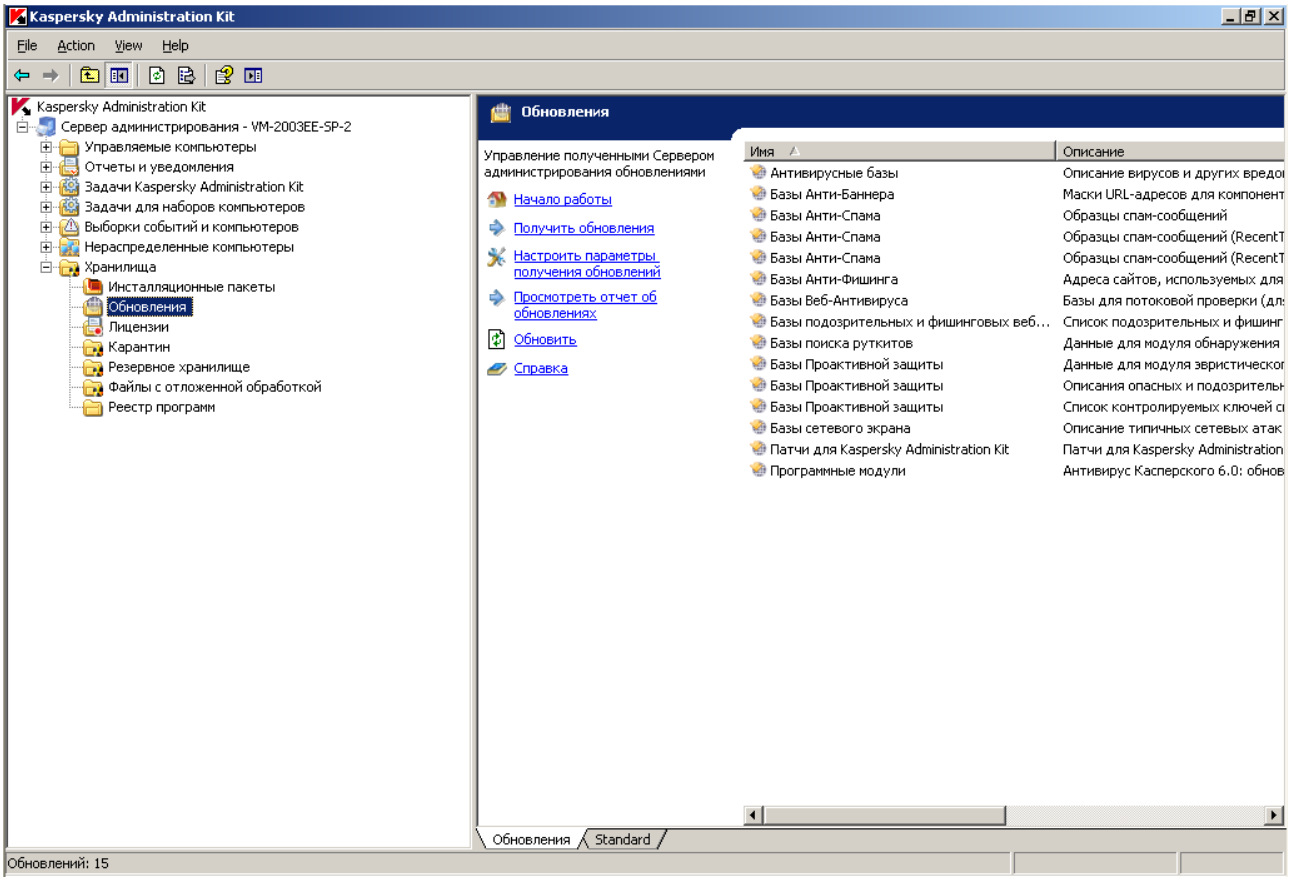

Рисунок 28. Просмотр полученных обновлений

Распространение обновлений на клиентские компьютеры

Для повышения надежности антивирусной защиты следует сформировать групповые задачи получения обновлений для всех антивирусных программ, входящих в систему антивирусной защиты клиентских компьютеров.

Чтобы на клиентских компьютерах были установлены одинаковые версии баз и обновления программных модулей, в параметрах задач получения обновлений программами следует выбрать в качестве источника обновлений Сервер администрирования.

Если в задаче обновления программы в качестве источника обновлений выбран Сервер администрирования, то при иерархической структуре Серверов клиентские компьютеры будут обновляться с того Сервера, к которому подключены, то есть с подчиненного, а не главного.

Формирование задач обновления для программ подробно описывается в Руководствах к этим программам.

Для задач обновления на закладке **Расписание** (см. рис. ниже) можно выбрать вариант запуска **При загрузке обновлений в хранилище**. Это позволит сократить трафик и количество обращений клиентских компьютеров к Серверу администрирования, а также избежать возможных неточностей и ошибок при формировании задач обновления для групп администрирования, содержащих большое количество клиентских компьютеров.

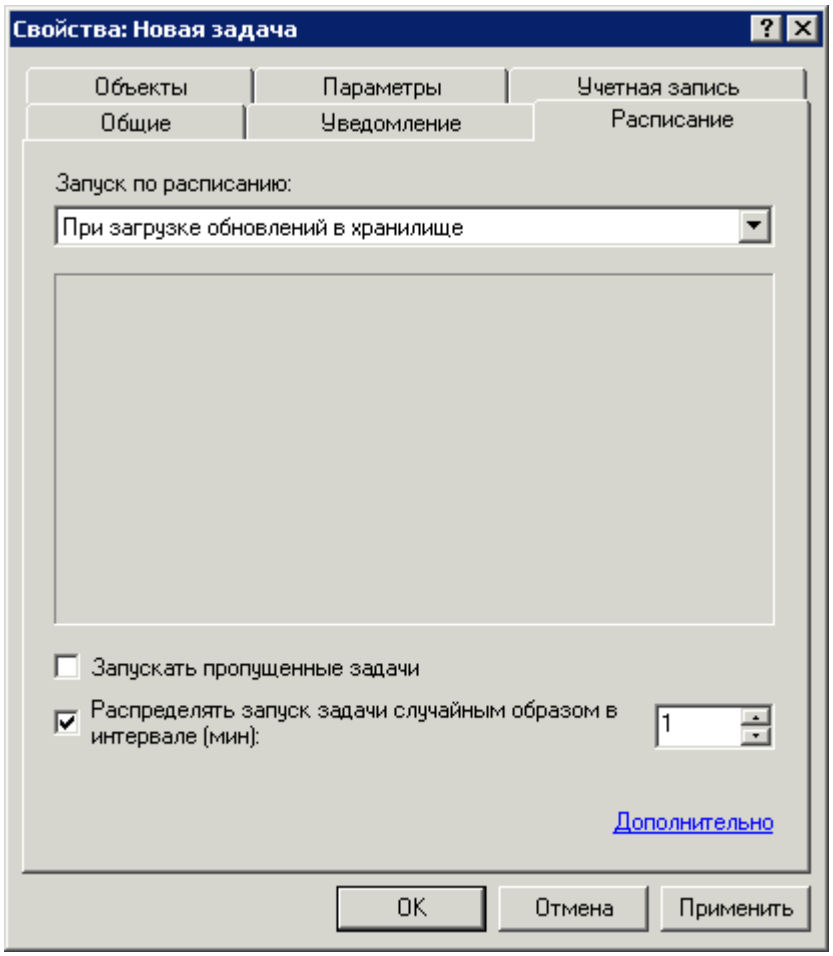

Рисунок 29. Расписание задачи обновления

Для сокращения нагрузки на Серверы администрирования рекомендуется использовать агенты обновлений (см. раздел «Распространение обновлений с помощью агентов обновлений» на стр. 69), позволяющие распространять обновления в пределах группы администрирования. При включенной многоадресной IP-рассылке Агенты обновлений также распространяют параметры политик и задач.

Получение обновлений подчиненными Серверами и их клиентскими компьютерами

Получение обновлений программами производится с того Сервера администрирования, к которому подключен клиентский компьютер, то есть с подчиненного, а не главного Сервера.

Если в компьютерной сети организована иерархическая структура Серверов администрирования, то для получения обновлений подчиненными Серверами и распространения обновлений на подключенные к ним клиентские компьютеры нужно выполнить следующие действия:

1. Создать задачу получения обновлений для каждого подчиненного Сервера администрирования.

2. В параметрах задачи получения обновлений для подчиненных Серверов в качестве источника обновлений выбрать **Главный Сервер администрирования** (см. рис. ниже).

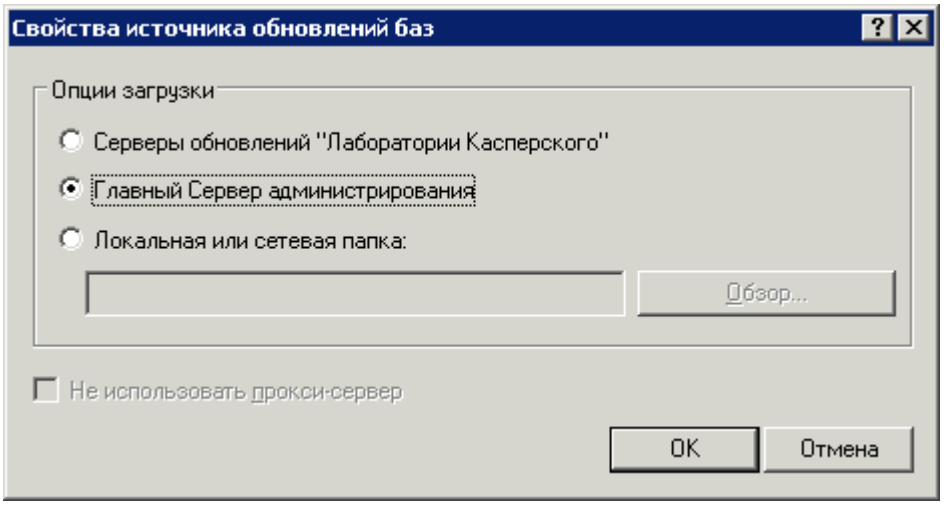

Рисунок 30. Обновление с главного Сервера администрирования

3. В параметрах задачи получения обновлений главным Сервером администрирования включить режим автоматического распространения обновлений на подчиненные Серверы, установив для этого флажок **Форсировать обновление подчиненных Серверов** (см. рис ниже).

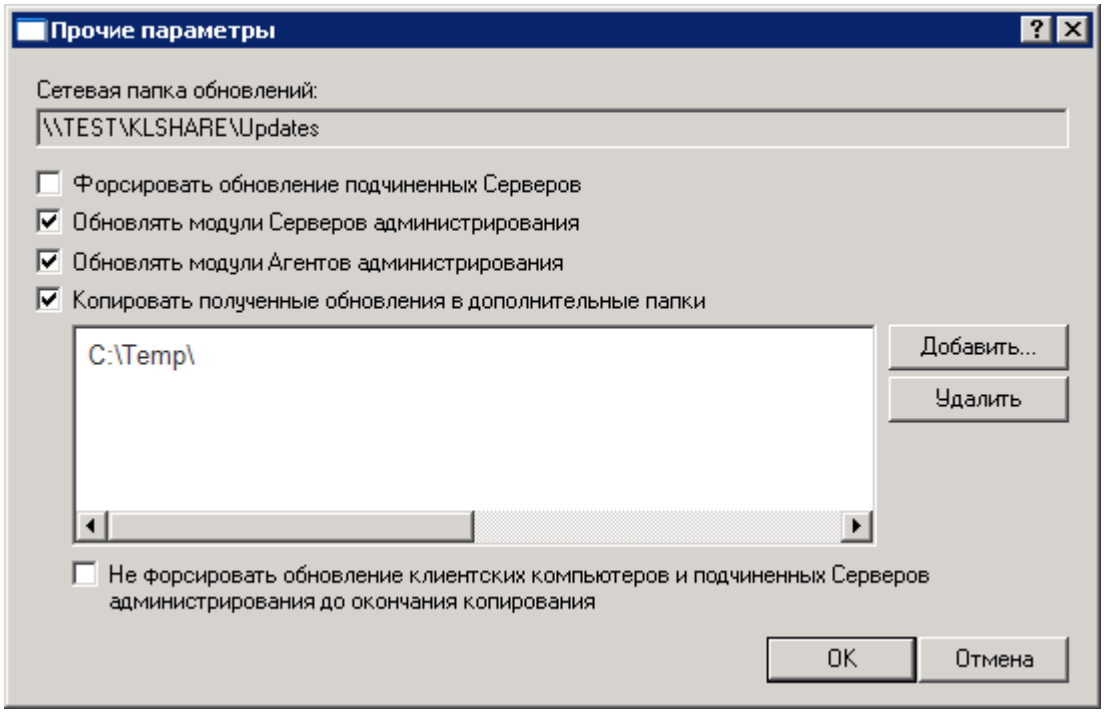

Рисунок 31. Настройка прочих параметров задачи

4. При необходимости указать агенты обновлений (см. раздел «Распространение обновлений с помощью агентов обновлений» на стр. 69) в пределах групп администрирования.

Распространение обновлений с помощью агентов обновлений

Для распространения обновлений на клиентские компьютеры группы можно использовать агенты обновлений – компьютеры, представляющие собой промежуточные центры распространения обновлений и инсталляционных

пакетов в пределах группы администрирования. Они получают обновления с Сервера администрирования и размещают их в папке назначения, указанной при установке программы. Папку назначения можно изменить в свойствах агента обновлений. При этом копируются только те обновления, которые нужны в пределах группы. В дальнейшем клиентские компьютеры группы обращаются за обновлениями к агентам.

Формирование списка агентов обновлений и их настройка происходят в окне свойств группы на закладке **Агенты обновлений** (см. рис. ниже). Помимо пакетов обновлений, агенты распространяют на клиентские компьютеры параметры групповых политик и задач.

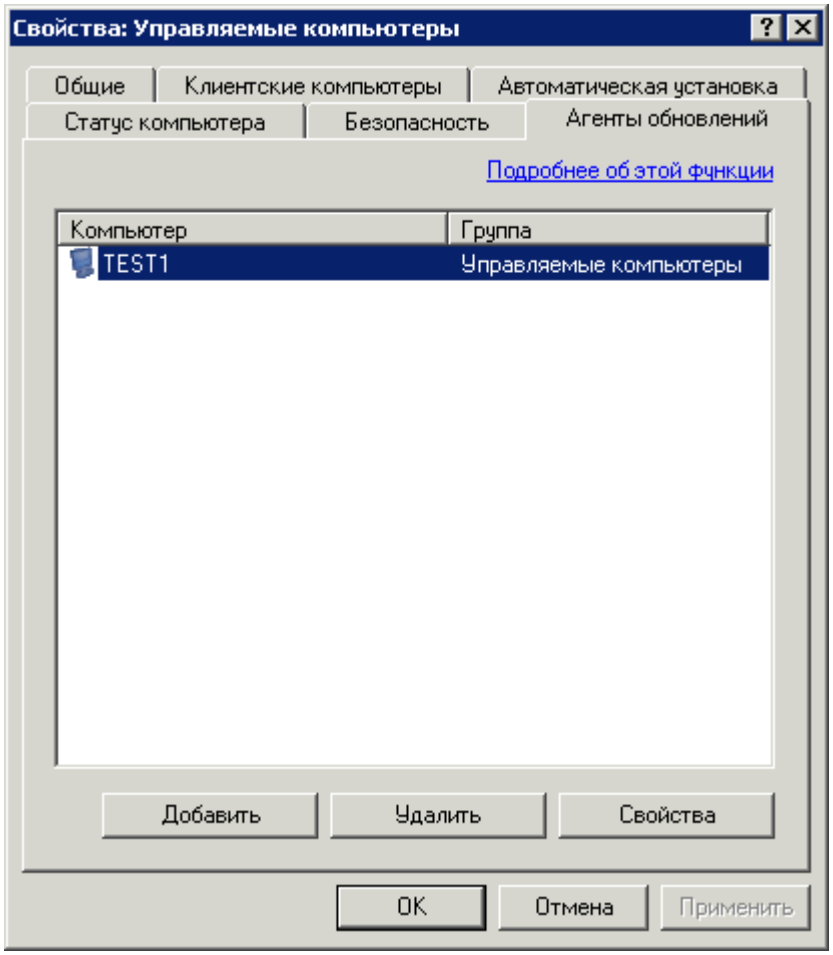

Рисунок 32. Формирование списка агентов обновлений

ОБСЛУЖИВАНИЕ

В рамках обслуживания групп администрирования рекомендуется регулярно проводить ряд мероприятий:

- Периодически формировать и просматривать отчеты о работе программ на клиентских компьютерах (см. раздел «Отчеты» на стр. 79).
- Читать уведомления, отправленные с клиентских компьютеров и Сервера администрирования.

  Полный список уведомлений, посылаемых программами из состава продуктов «Лаборатории Касперского», приведен в прилагающихся к ним документах.

- Своевременно обновлять (см. раздел «Обновление баз и программных модулей» на стр. 64) на клиентских компьютерах базы и программные модули установленных на клиентских компьютерах программ.
- Следить за размерами базы данных для размещения информации о работе программ, поступающей с клиентских компьютеров, а также за наличием необходимого для ее размещения объема свободного дискового пространства на Сервере администрирования.
- Своевременно добавлять в группы администрирования вновь установленные в сети предприятия компьютеры и устанавливать на них необходимые антивирусные программы.
- Регулярно выполнять резервное копирование данных системы администрирования (см. раздел «Резервное копирование и восстановление данных Сервера администрирования» на стр. 90).
- Следить за состоянием лицензий установленных в сети программ и по мере надобности продлевать их (см. раздел «Продление срока действия лицензии» на стр. 72).
- Просматривать информацию о событиях Сервера администрирования и программ, находящихся под его управлением (см. раздел «Журналы событий. Выборки событий» на стр. 75).
- Отслеживать состояние карантинного хранилища (см. раздел «Карантин и резервное хранилище» на стр. 73) и информацию о файлах с отложенной проверкой (см. раздел «Файлы с отложенной обработкой» на стр. 90).
- При необходимости с рабочего места администратора выполнять действия с объектами на клиентских компьютерах. Например, проводить лечение зараженных файлов на компьютере.

В Kaspersky Administration Kit предусмотрен ряд функций, значительно облегчающих обслуживание сети:

- поиск компьютеров, групп администрирования и подчиненных Серверов по заданным параметрам (см. раздел «Поиск компьютеров» на стр. 82);
- ведение реестра программ (см. раздел «Реестр программ» на стр. 86);
- контроль возникновения вирусных эпидемий (см. стр. 87).

В этом разделе

Продление срока действия лицензии

Право использования программного обеспечения «Лаборатории Касперского» предоставляется на основании заключаемого при его покупке лицензионного соглашения.

В течение срока действия лицензии вам предоставляются следующие возможности:

- использование антивирусной функциональности программы;
- обновление баз программ;
- обновление версий данной программы;
- консультации по вопросам, связанным с установкой, настройкой и эксплуатацией данной программы, оказываемые по телефону и посредством веб-формы запроса в Службу технической поддержки, расположенной на веб-сайте «Лаборатории Касперского»;
- возможность пересылать обнаруженные зараженные и подозрительные объекты в «Лабораторию Касперского» для анализа.

Для работы программы Kaspersky Administration Kit не требуется лицензия! При обращении в Службу технической поддержки используйте информацию о лицензии любой приобретенной вами программы «Лаборатории Касперского», управление которой осуществляется через Kaspersky Administration Kit.

Программа Kaspersky Administration Kit устанавливает наличие лицензии, которая является неотъемлемой частью любого продукта «Лаборатории Касперского», и определяет срок ее действия. У программы может быть только одна активная лицензия. В ней содержатся ограничения на использование программного обеспечения, которые могут быть проверены специальными механизмами.

По истечении срока действия лицензии перечисленные выше возможности ограничиваются. Продление срока действия лицензии заключается в покупке и установке новой лицензии.

В программе Kaspersky Administration Kit реализованы возможности централизованного наблюдения за состоянием лицензий, установленных на клиентских компьютерах, и продления срока их действия.

При установке лицензии с помощью служб Kaspersky Administration Kit все данные о ней сохраняются на Сервере администрирования. На основании этой информации составляются отчеты о состоянии установленных лицензий, а также производится уведомление об истечении срока действия и превышении заложенного в лицензии максимального количества использующих ее программ. Параметры оповещений о состоянии лицензий редактируются в параметрах Сервера администрирования.

Для создания отчета о состоянии лицензий, установленных на клиентские компьютеры, вы можете воспользоваться встроенным шаблоном **Отчет об использовании лицензий** либо создать шаблон одноименного типа.

В отчете, созданном по шаблону **Отчет об использовании лицензий**, представлена полная информация обо всех установленных на клиентские компьютеры лицензиях, как активных, так и дополнительных, с указанием компьютеров, на которых они используются, и их ограничений.

Полный перечень лицензий, установленных на клиентские компьютеры, представлен в папке **Хранилища** → **Лицензии** (см. рис. ниже). Подробная информация о каждой из них приводится в панели результатов. Полный перечень граф панели результатов для папки **Лицензии** приведен в Справочном руководстве.

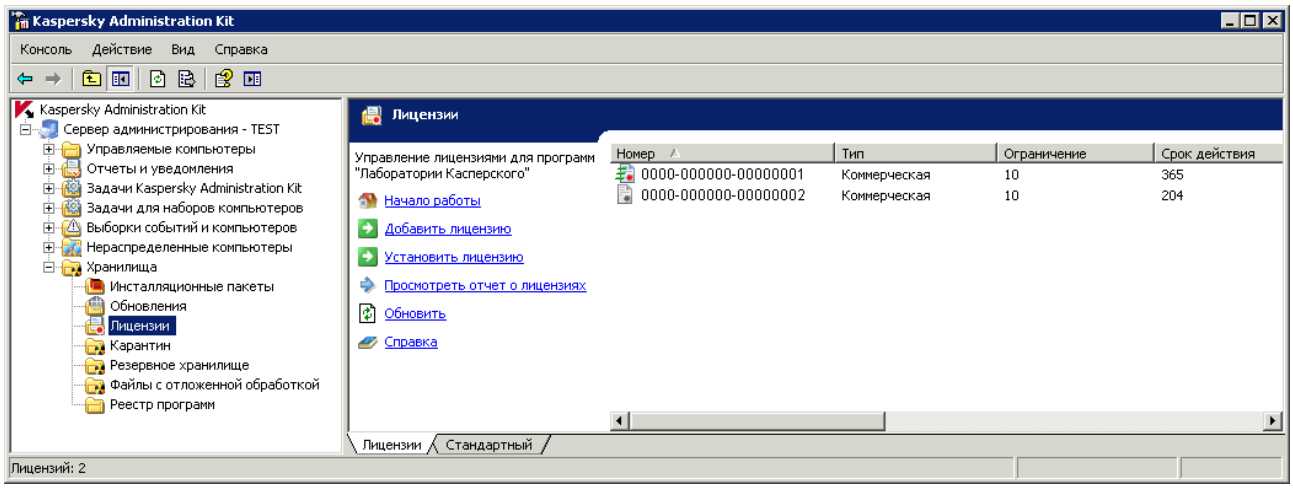

Рисунок 33. Лицензии

Информацию о том, какие лицензии установлены для программы на конкретном клиентском компьютере, можно просмотреть в окне свойств программы.

Чтобы установить лицензию, необходимо создать и запустить задачу установки лицензии.

Задача установки лицензии может быть создана как групповая или локальная, а также как задача для набора компьютеров. Задачу установки лицензии можно создать с помощью мастера.

Для замены уже установленной лицензии или установки ее в качестве активной можно использовать ранее созданную задачу, предварительно изменив ее параметры.

Карантин и резервное хранилище

Работа с карантином и резервным хранилищем доступна для Антивируса Касперского для Windows Workstations и Антивируса Касперского для Windows Servers версий 6.0 и выше.

Антивирусные программы предоставляют функциональность для хранения объектов в специализированных хранилищах. Для каждого компьютера существуют индивидуальные папки карантина и резервного хранилища, расположенные локально на данном компьютере. В хранилище карантина помещаются подозрительные объекты, а в резервное хранилище – резервные копии зараженных объектов перед лечением или удалением.

В программе Kaspersky Administration Kit предусмотрена возможность вести централизованный список объектов, помещаемых программами «Лаборатории Касперского» в хранилища. Данная информация передается с клиентских компьютеров Агентами администрирования и хранится в информационной базе Сервера администрирования. При этом предоставляется возможность через Консоль администрирования просматривать свойства объектов, находящихся в хранилищах на локальных компьютерах, запускать антивирусную проверку хранилищ и удалять из них объекты.

Чтобы активировать функцию удаленного управления объектами локальных хранилищ,

в политике программы следует установить флажки в блоке **Информировать Сервер администрирования** (см. рис. ниже):

- **Об объектах на карантине**.
- **Об объектах резервного хранилища**.
- **Об объектах с отложенной обработкой**.

Настройка параметров хранилищ выполняется для каждой программы индивидуально: в политике или в параметрах программы.

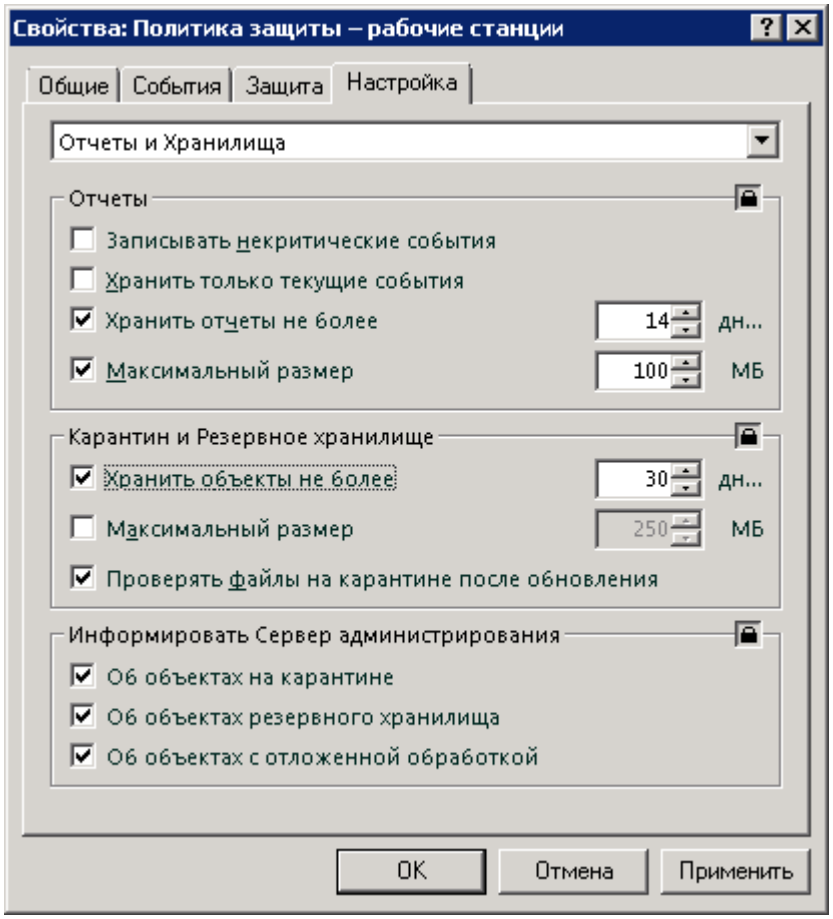

Рисунок 34. Настройка удаленных хранилищ

Просмотр объектов, размещенных в хранилищах клиентских компьютеров групп администрирования, и работа с объектами осуществляется в папке **Хранилища** (см. рис. ниже).

Kaspersky Administration Kit не копирует объекты на Сервер администрирования. Все объекты размещаются в локальных хранилищах на клиентских компьютерах. Восстановление объектов выполняется на компьютер, где установлена антивирусная программа, поместившая объект в хранилище, в папку, заданную администратором.

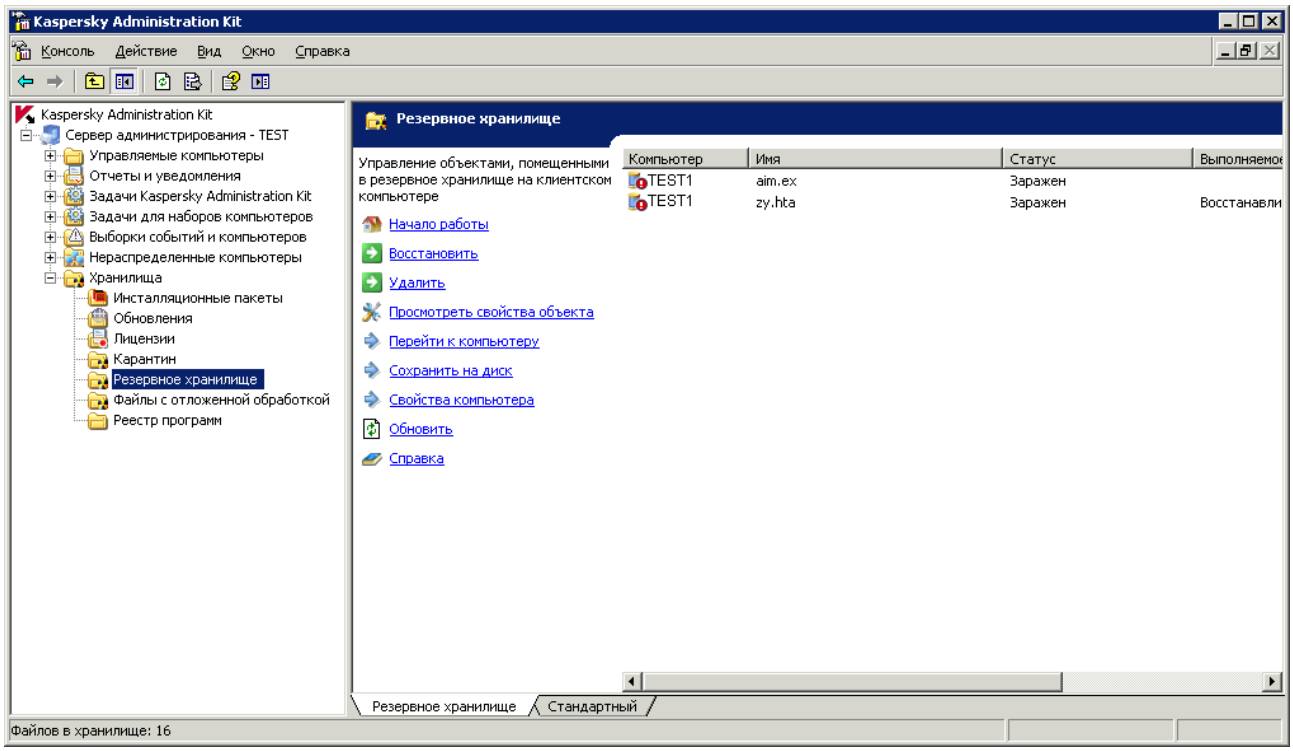

Рисунок 35. Просмотр содержимого хранилища

Журналы событий. Выборки событий

Программа Kaspersky Administration Kit предоставляет широкие возможности по наблюдению за работой системы антивирусной защиты.

Предусмотрена возможность ведения журналов событий в работе Сервера администрирования и всех программ, управляемых при помощи Kaspersky Administration Kit. Данные могут сохраняться как в системном журнале Microsoft Windows, так и в журнале событий Kaspersky Administration Kit.

В журналах фиксируются события, зарегистрированные в работе программ, и результаты выполнения задач.

Вы можете указать перечень регистрируемых событий в работе каждой программы, а также порядок оповещения о них администратора и других пользователей для каждой группы администрирования. Данные параметры определяются групповой политикой для программы. Их установка осуществляется в окне свойств групповой политики на закладке **События** (см. рис. ниже).

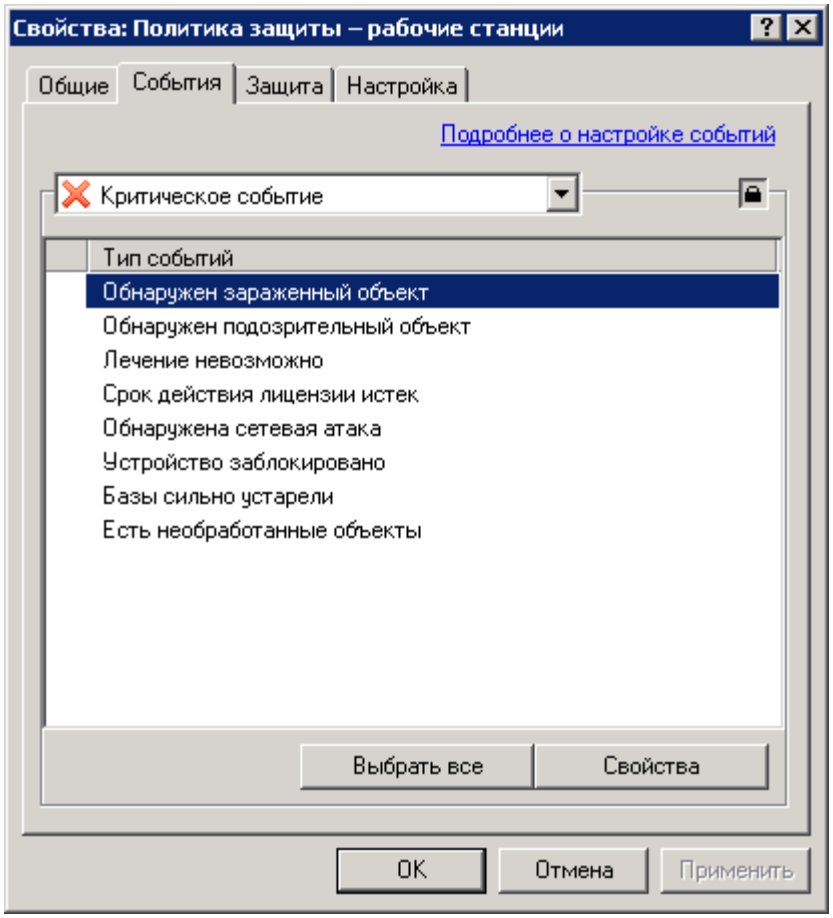

*Рисунок 36. Редактирование политики. Закладка **События***

Порядок сохранения результатов выполнения задач, форма и способ оповещения о них определяются в параметрах задачи.

Оповещение может производиться путем рассылки сообщений по электронной почте или по сети, а также с помощью запуска определенной программы или скрипта.

Информация о зарегистрированных событиях и результатах выполнения задач может храниться централизованно на Сервере администрирования, а также для каждого клиентского компьютера локально на этом компьютере.

Просматривать информацию, сохраненную в журнале событий Microsoft Windows, можно при помощи стандартной MMC-оснастки **Просмотр событий**. Просмотр информации журнала событий Kaspersky Administration Kit, сохраненной на Сервере администрирования, осуществляется через папку **Выборки событий и компьютеров** → **События** дерева консоли (см. рис. ниже).

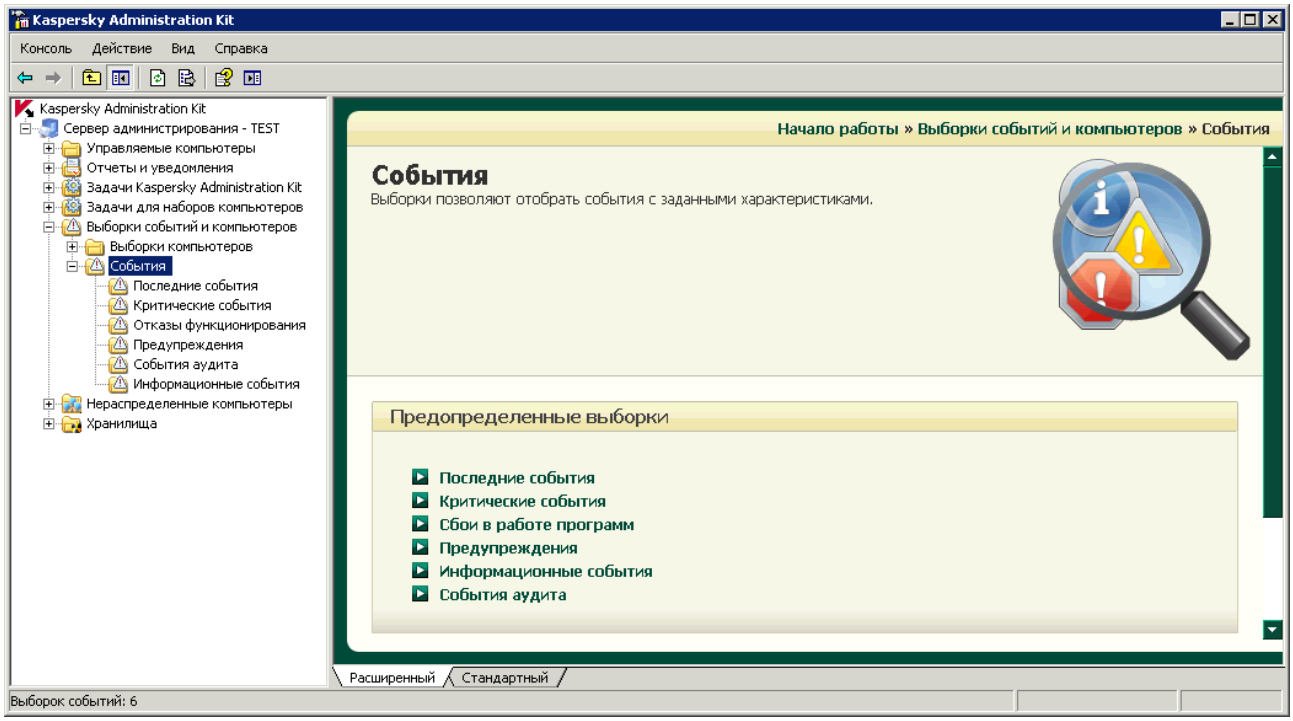

Рисунок 37. Просмотр информации журнала событий Kaspersky Administration Kit

Для упрощения просмотра и поиска информация в папке **События** распределена по выборкам. По умолчанию доступны следующие выборки событий: **Последние события**, **Критические события**, **Отказы функционирования**, **Предупреждения**, **События аудита**, **Информационные события**. Выборка позволяет искать и структурировать информацию о зарегистрированных событиях, поскольку после ее применения доступной становится только информация, удовлетворяющая заданным параметрам. Это весьма актуально в связи с большим объемом хранящейся на Сервере информации. Предусмотрена возможность создания дополнительных выборок, изменения набора отображаемых граф и сохранения выборки событий в виде файла формата txt.

Для создания выборки воспользуйтесь ссылкой в панели результатов **Создать выборку** или командой контекстного меню **Создать** → **Новая выборка** папки **События**. В результате в дереве консоли в папке **События** будет создана новая папка с именем, заданным для выборки. В нее будут включены все события и результаты выполнения задач. Чтобы изменить состав информации, настройте параметры выборки (см. рис. ниже).

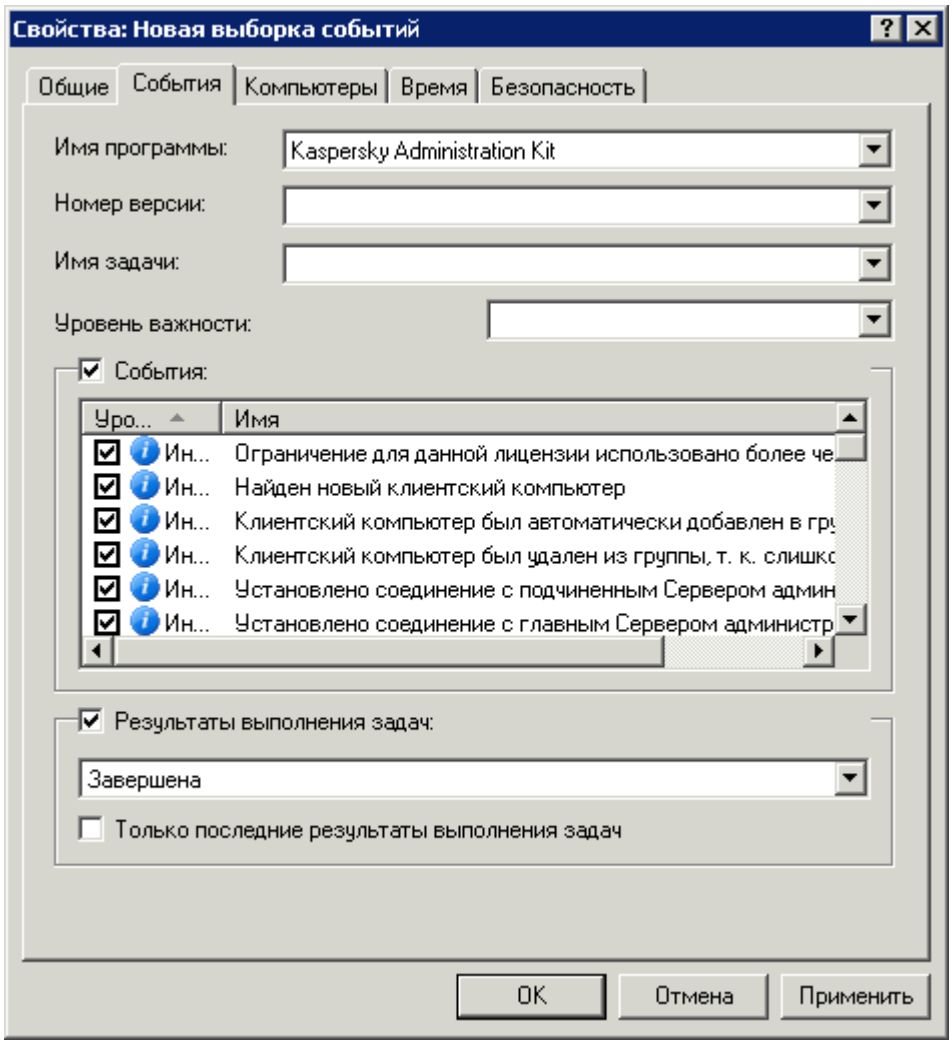

*Рисунок 38. Настройка выборки событий. Закладка **События***

Удаление зарегистрированных событий происходит автоматически по истечении заданного политикой срока хранения либо вручную при помощи команды контекстного меню **Удалить**. Вы можете удалять отдельное, выбранное в панели результатов событие, все события, либо события, удовлетворяющие определенным условиям.

Со списком событий, зарегистрированных в работе программы, для каждого клиентского компьютера вы можете ознакомиться в окне **События** (см. рис. ниже), которое открывается с помощью команды контекстного меню **События**. Предоставляется информация журнала событий Kaspersky Administration Kit, хранящаяся на Сервере администрирования. Для поиска информации воспользуйтесь фильтром событий.

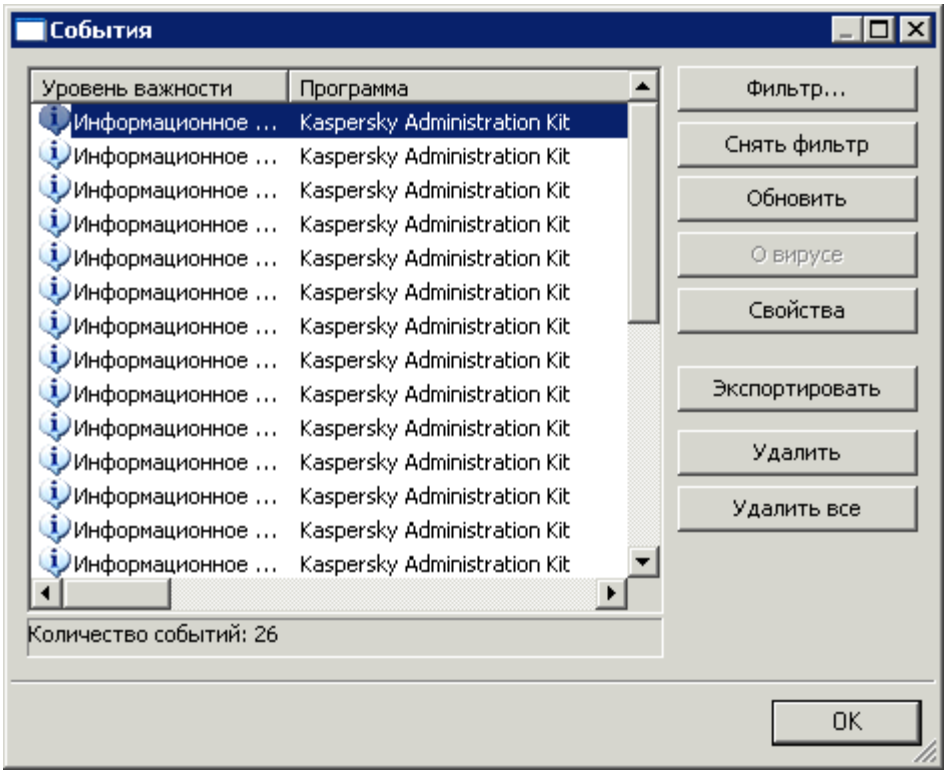

Рисунок 39. Просмотр событий, хранящихся на Сервере администрирования

Отчеты

Вы можете получать отчеты о состоянии системы антивирусной защиты на основании информации, хранящейся на Сервере администрирования.

Отслеживать состояние антивирусной защиты можно также на клиентском компьютере с помощью информации, записываемой Агентом администрирования в системный реестр.

Отчеты могут создаваться для следующих объектов:

- системы антивирусной защиты в целом;
- компьютеров, входящих в определенную группу администрирования;
- набора клиентских компьютеров из различных групп администрирования;
- системы антивирусной защиты подчиненных Серверов администрирования.

Предусмотрено получение отчетов следующих типов:

- **Состояние защиты**:
  - **Отчет о состоянии защиты** содержит информацию о клиентских компьютерах, обладающих недостаточным уровнем антивирусной безопасности.
  - **Отчет об ошибках** содержит информацию об ошибках (отказах функционирования), зафиксированных в работе программ, установленных на клиентских компьютерах.

- **Отчет о событиях** содержит перечень событий программ для выбранной группы. В список заносятся только события, которые были указаны при создании отчета.

- **Отчет о работе агентов обновлений** содержит статистику работы агентов обновлений в рамках выбранных групп администрирования.

- **Отчет о подчиненных Серверах администрирования** содержит информацию о подчиненных Серверах администрирования, входящих в выбранные группы администрирования.

- **Развертывание**:

  - **Отчет об использовании лицензий** содержит информацию о состоянии лицензий, используемых программами, и соблюдении установленных ими ограничений.

  - **Отчет о версиях программ Лаборатории Касперского** включает информацию о версиях установленных на клиентских компьютерах антивирусных программ «Лаборатории Касперского».

  - **Отчет о несовместимых программах** содержит информацию об установленных на клиентских компьютерах антивирусных программах сторонних производителей или программах «Лаборатории Касперского», которые не поддерживают управление через Kaspersky Administration Kit.

  - **Отчет о развертывании защиты** содержит перечень компьютеров в сети и информацию об установленных на них антивирусных программах.

- **Обновление**:

  - **Отчет об используемых базах** содержит информацию о версиях баз, используемых программами.

  - **Отчет о версиях обновлений программных модулей программ Лаборатории Касперского** содержит сводную информацию о версиях установленных обновлений программных модулей, количестве установленных обновлений, а также количестве компьютеров и групп, куда производилась установка.

- **Антивирусная статистика**:

  - **Отчет о вирусах** предоставляет информацию о результатах антивирусной проверки клиентских компьютеров.

  - **Отчет о наиболее зараженных компьютерах** включает информацию о клиентских компьютерах, в ходе проверки которых обнаружено наибольшее количество подозрительных объектов.

  - **Отчет о сетевых атаках** предоставляет информацию о сетевых атаках, зарегистрированных на клиентских компьютерах.

  - **Сводный отчет о программах для защиты рабочих станций и файловых серверов** содержит подробную информацию об установленных антивирусных программах для защиты рабочих станций и файловых серверов, а также сведения о зараженных объектах, обнаруженных программами этого типа, и связанных с ними действиях.

  - **Сводный отчет о программах для защиты почтовых систем** содержит подробную информацию об установленных антивирусных программах для защиты почтовых систем, а также сведения о зараженных объектах, обнаруженных программами этого типа, и связанных с ними действиях.

  - **Сводный отчет о программах для защиты периметра** содержит подробную информацию об установленных антивирусных программах защиты периметра, а также сведения о зараженных объектах, обнаруженных программами этого типа, и связанных с ними действиях.

  - **Сводный отчет о типах программ** содержит информацию о типах установленных на клиентских компьютерах антивирусных программ, а также информацию о зараженных объектах, обнаруженных этими программами, и связанных с ними действиях.

  - **Отчет о пользователях зараженных компьютеров** содержит информацию о пользователях сети, на компьютерах которых обнаружено наибольшее количество подозрительных объектов.

- **Прочее**:
  - **Отчет о реестре программ** содержит информацию обо всех программах, установленных на клиентские компьютеры в группах администрирования.
  - **Отчет о заметках администратора** отображает перечень заметок администратора, сохраненных в группе за указанный промежуток времени.

Вы можете формировать отчеты по заранее созданным шаблонам. Большая часть сформированных по умолчанию шаблонов отчетов размещается в дереве консоли в папке **Отчеты и уведомления** (см. рис. ниже). В мастере формирования отчетов также можно выбрать некоторые дополнительные шаблоны.

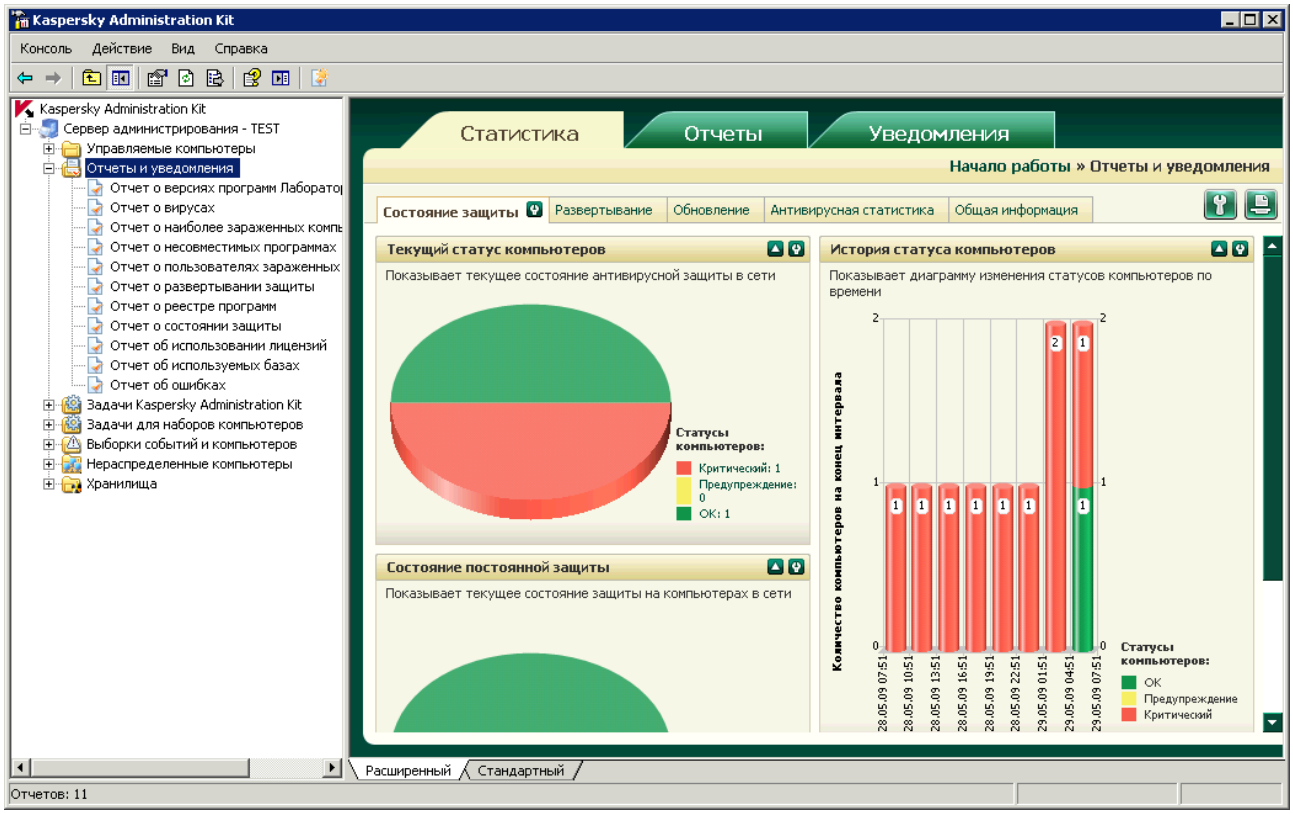

Рисунок 40. Просмотр списка отчетов

Предусмотрен ряд стандартных шаблонов, соответствующих типам отчетов о состоянии системы антивирусной защиты.

Вы можете создавать новые шаблоны, удалять существующие, просматривать и редактировать их параметры.

Для просмотра отчетов используется панель результатов элемента дерева консоли, соответствующего шаблону для формирования отчета, или браузер, установленный в системе по умолчанию.

При использовании иерархической структуры Серверов администрирования можно создавать общие отчеты, включающие в себя информацию с подчиненных Серверов администрирования.

Если некоторые Серверы администрирования недоступны, информация об этом будет содержаться в отчете.

Чтобы сохранить отчет, выберите его в дереве консоли, откройте контекстное меню отчета и выберите **Сохранить**. В запустившемся мастере укажите папку хранения файлов отчета и выберите в раскрывающемся списке формат, в котором будет сохранен отчет. Нажмите на кнопку **Готово**.

Поиск компьютеров

Чтобы получить информацию о конкретном компьютере или группе компьютеров, вы можете воспользоваться функцией поиска компьютера на основании заданных критериев. При поиске может использоваться информация подчиненных Серверов администрирования. Результаты поиска могут быть сохранены в текстовом файле.

Функция поиска позволяет находить:

- клиентские компьютеры, входящие в состав групп администрирования Сервера администрирования и его подчиненных Серверов;
- компьютеры, не включенные в группы администрирования, но входящие в состав компьютерных сетей, где установлен Сервер администрирования и его подчиненные Серверы;
- все компьютеры в сетях, где установлен Сервер администрирования и его подчиненные Серверы, независимо от того, входит компьютер в состав групп администрирования или нет.

Для поиска компьютеров следует воспользоваться командой **Поиск** контекстного меню для выбранного в дереве консоли узла **Сервер администрирования**, папки **Нераспределенные компьютеры**, папки **Управляемые компьютеры** или папок вложенных групп администрирования (см. рис. ниже). Для этой цели вы также можете воспользоваться ссылками в панели задач: **Искать нераспределенные компьютеры** для папки **Нераспределенные компьютеры** и **Искать компьютеры** для папки **Управляемые компьютеры**.

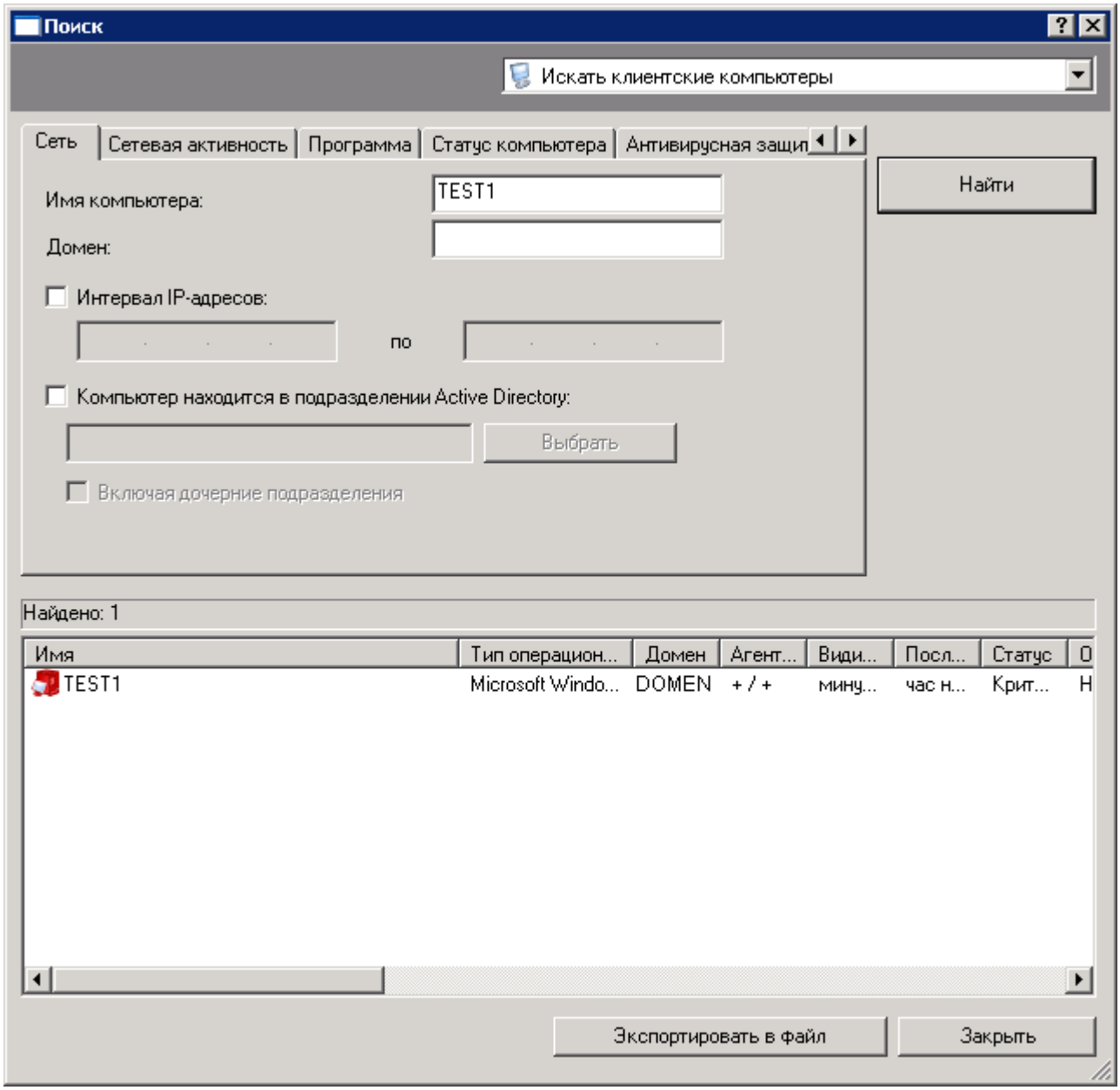

*Рисунок 41. Поиск компьютеров. Закладка **Сеть***

В зависимости от того, для какого узла или папки организуется поиск, его результаты будут следующими:

- **Управляемые компьютеры** или любая вложенная папка – поиск клиентских компьютеров, подключенных к Серверу администрирования, управляющему выбранной группой.

  Поиск выполняется на основании информации о структуре папок Сервера администрирования и его подчиненных Серверов (если в параметрах поиска установлен флажок **Включая данные с подчиненных Серверов до уровня**).

- **Нераспределенные компьютеры** – поиск не включенных в состав групп администрирования компьютеров в сети, где установлен Сервер администрирования.

  Поиск выполняется на основании данных, полученных в ходе опроса компьютерной сети Сервером администрирования и подчиненными Серверами (если в параметрах поиска установлен флажок **Включая данные с подчиненных Серверов до уровня**).

Результатами поиска будут компьютеры, входящие в выбранную для поиска папку **Нераспределенные компьютеры** и в папки **Нераспределенные компьютеры** всех подчиненных Серверов (если в параметрах поиска установлен флажок **Включая данные с подчиненных Серверов до уровня**).

- **Сервер администрирования <Имя сервера>** – полный поиск компьютеров.

  Поиск выполняется на основании информации о структуре групп администрирования и данных, полученных в ходе опроса компьютерной сети выбранным Сервером администрирования и подчиненными Серверами администрирования (если в параметрах поиска установлен флажок **Включая данные с подчиненных Серверов до уровня**).

  Результатами поиска будут:

  - клиентские компьютеры, входящие в состав групп администрирования выбранного Сервера администрирования и всех его подчиненных Серверов (если в параметрах поиска установлен флажок **Включая данные с подчиненных Серверов до уровня**).

  - компьютеры, входящие в группу **Нераспределенные компьютеры** выбранного Сервера администрирования и в группы **Нераспределенные компьютеры** всех его подчиненных Серверов (если в параметрах поиска установлен флажок **Включая данные с подчиненных Серверов до уровня**).

Для поиска, сохранения и отображения информации о компьютерах в отдельной папке дерева консоли воспользуйтесь функцией создания выборок.

Выборки компьютеров

Для более гибкого контроля над состоянием клиентских компьютеров информация о них на основе различных критериев представлена в отдельной папке дерева консоли **Выборки событий и компьютеров** → **Выборки компьютеров** (см. рис. ниже).

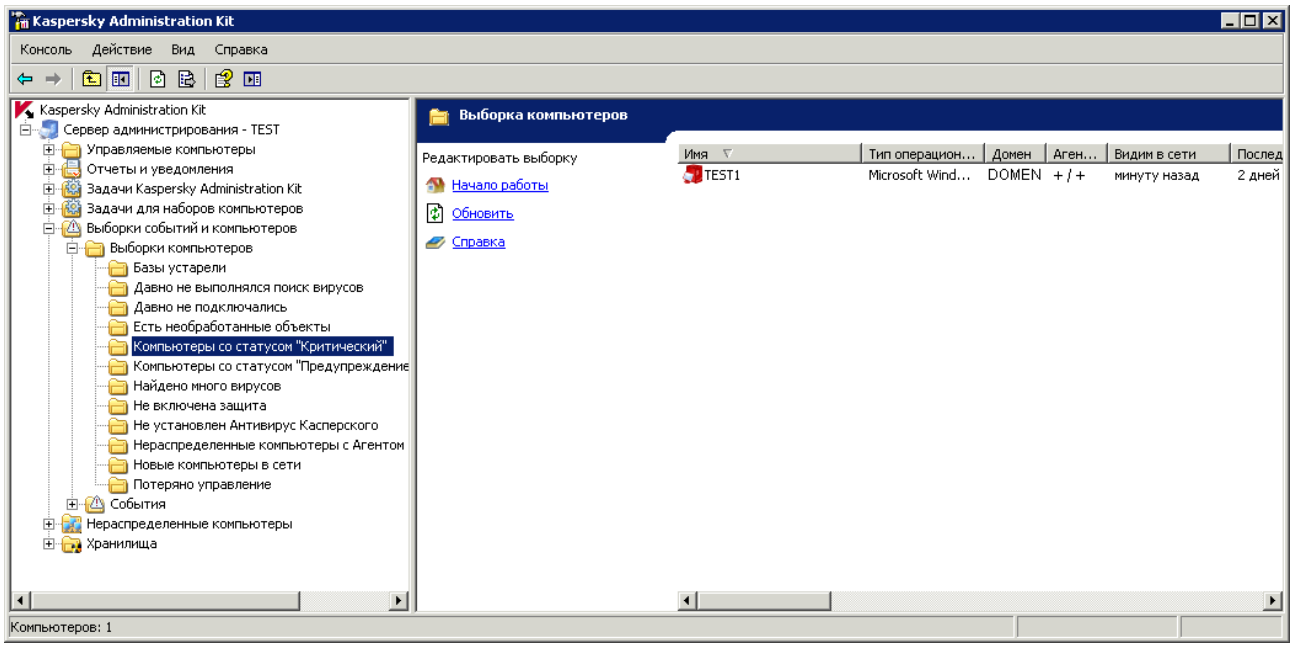

Рисунок 42. Выборки компьютеров

Диагностика состояния клиентских компьютеров выполняется на основании информации о статусе антивирусной защиты на компьютере и данных о его активности в сети. Настройка параметров диагностики производится для каждой группы администрирования отдельно на закладке **Статус компьютера** (см. рис. ниже).

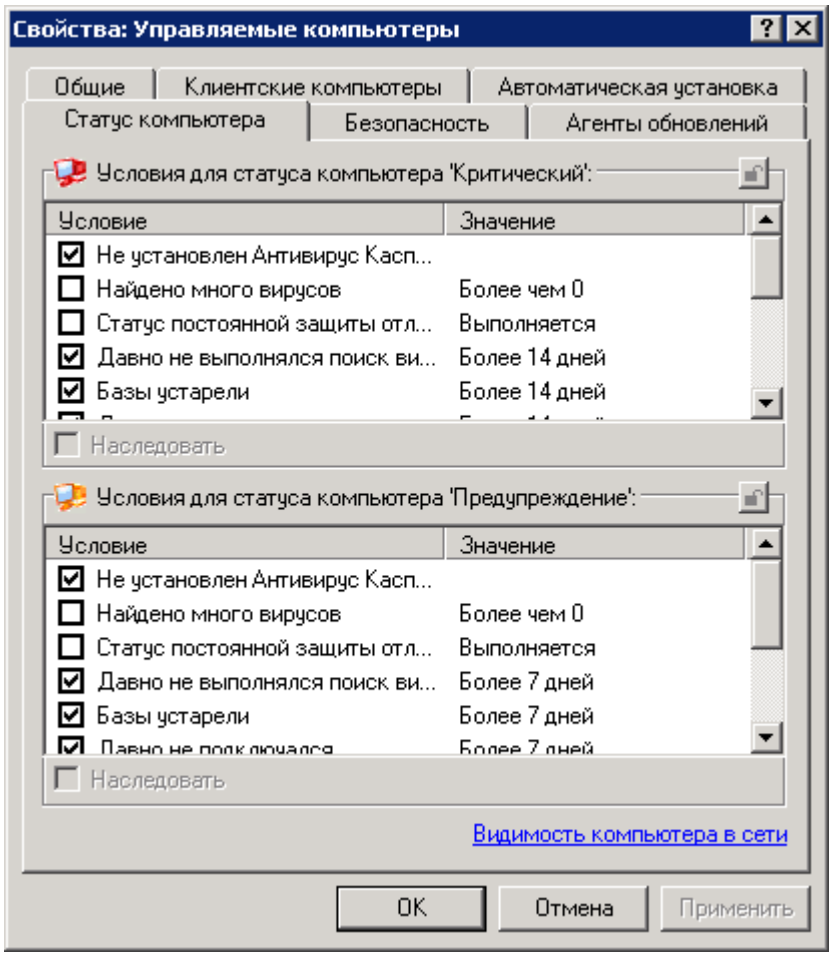

Рисунок 43. Настройка диагностики статуса клиентского компьютера

Информация о новых компьютерах предоставляется по результатам опроса Сервером администрирования компьютерной сети.

Предусмотрена возможность создания дополнительных выборок, изменения набора отображаемых граф и сохранения выборки компьютеров в виде файла формата txt. Чтобы в состав выборки были добавлены компьютеры, настройте параметры выборки (см. рис. ниже). Выборка может быть использована для поиска и дальнейшего перемещения обнаруженных компьютеров в группы администрирования. Перемещение осуществляется при помощи мыши.

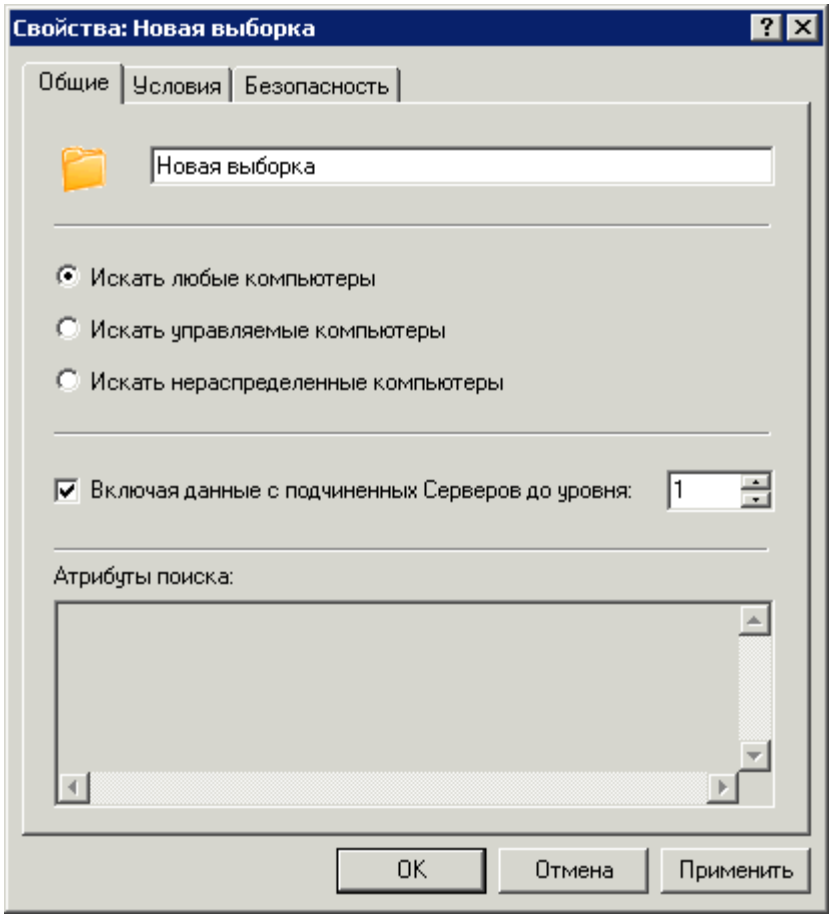

Рисунок 44. Настройка выборки компьютеров

Реестр программ

Наличие или отсутствие этой папки в дереве консоли определяется параметрами пользовательского интерфейса. Чтобы настроить отображение данной папки, пройдите в меню **Вид** → **Настройка интерфейса** и установите флажок в строке **Отображать реестр программ**.

Для просмотра реестра программ, установленных на компьютеры сети,

откройте папку **Хранилища** → **Реестр программ**.

Информация о программах составляется на основе данных системного реестра клиентских компьютеров локальной сети и представлена в таблице, содержащей следующие поля:

- **Имя** – название программы;
- **Версия** – номер версии программы;
- **Производитель** – наименование компании-производителя;
- **Число компьютеров** – количество компьютеров в сети, на которых установлена программа;
- **Комментарии** – краткое описание программы;
- **Служба технической поддержки** – адрес веб-сайта службы технической поддержки;

- **Телефон Службы технической поддержки** – телефон технической поддержки.

Поля **Комментарии**, **Служба технической поддержки** и **Телефон Службы технической поддержки** могут быть пустыми, если производителем программы не предусмотрена возможность занести соответствующие данные в системный реестр при установке программы.

Для просмотра данных о программах, удовлетворяющих определенным критериям, можно воспользоваться фильтром. Для программ списка предусмотрена возможность просмотра списка компьютеров, на которые установлена программа.

Контроль возникновения вирусных эпидемий

Kaspersky Administration Kit предоставляет возможность контролировать вирусную активность на клиентских компьютерах при помощи события **Вирусная атака**, которое регистрируется в работе компонента Сервер администрирования.

Эта функция имеет большое значение в периоды вирусных эпидемий и позволяет своевременно реагировать на возникающие угрозы вирусных атак.

Критерии, на основании которых фиксируется событие **Вирусная атака**, устанавливаются в окне свойств Сервера администрирования на закладке **Вирусная атака** (см. рис. ниже).

Событие может фиксироваться для нескольких типов программ.

Чтобы включить механизм распознавания вирусной атаки,

установите флажки рядом с нужными типами программ:

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

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

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

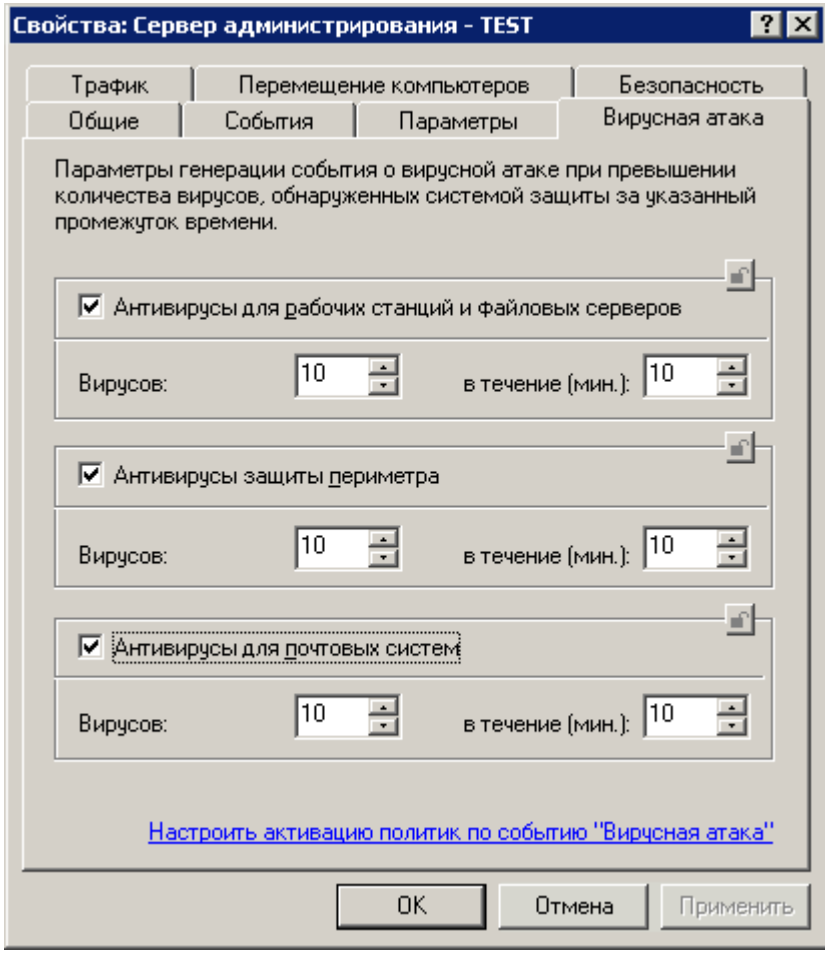

*Рисунок 45. Просмотр свойств Сервера администрирования. Закладка **Вирусная атака***

Событие **Вирусная атака** формируется на основании события **Обнаружен зараженный объект** в работе антивирусных программ. Поэтому для успешного распознавания вирусной эпидемии вся информация об этих событиях должна сохраняться на Сервере администрирования. Для этого нужно установить соответствующие параметры в политиках для всех антивирусных программ. В окне свойств события **Обнаружен зараженный объект** должен быть установлен флажок **На Сервере администрирования в течение (дней)**.

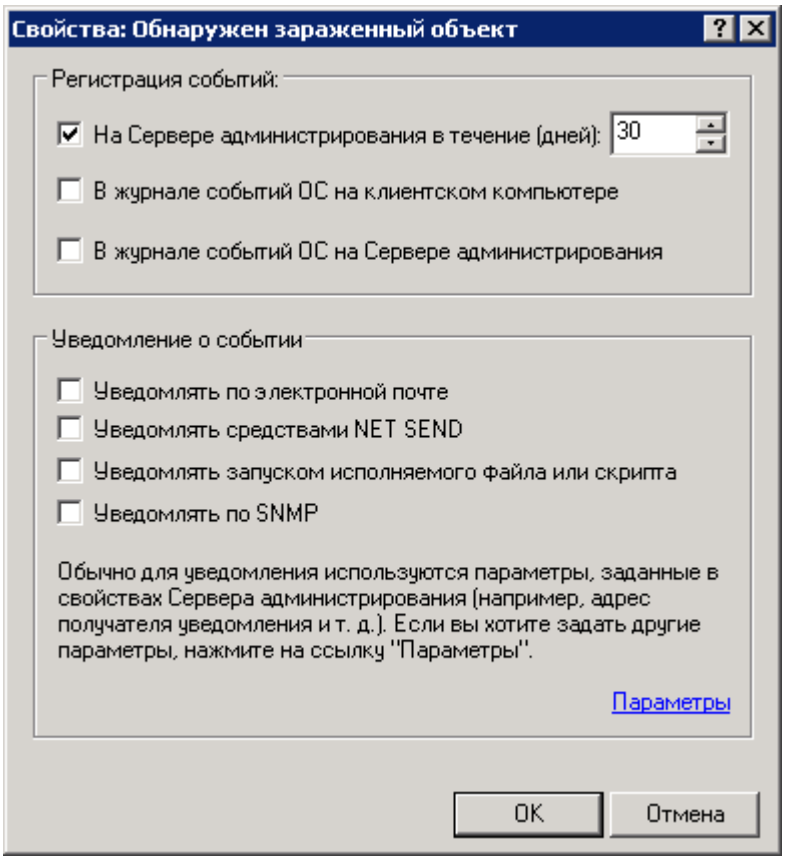

Рисунок 46. Настройка регистрации события

Порядок оповещения о событии **Вирусная атака** определяется на Сервере администрирования в окне свойств события в блоке **Уведомление о событии** (см. рис. ниже).

В качестве реакции на возникновение вирусной эпидемии может быть также задана автоматическая смена текущей политики для программ. Набор политик для каждого типа вирусной атаки определяется в окне **Активация политик**, которое открывается по ссылке **Настроить активацию политик по событию «Вирусная атака»**, расположенной в окне свойств Сервера администрирования на закладке **Вирусная атака**.

При подсчете событий **Обнаружен зараженный объект** учитывается только информация с клиентских компьютеров главного Сервера администрирования. Для каждого подчиненного Сервера событие **Вирусная атака** настраивается индивидуально.

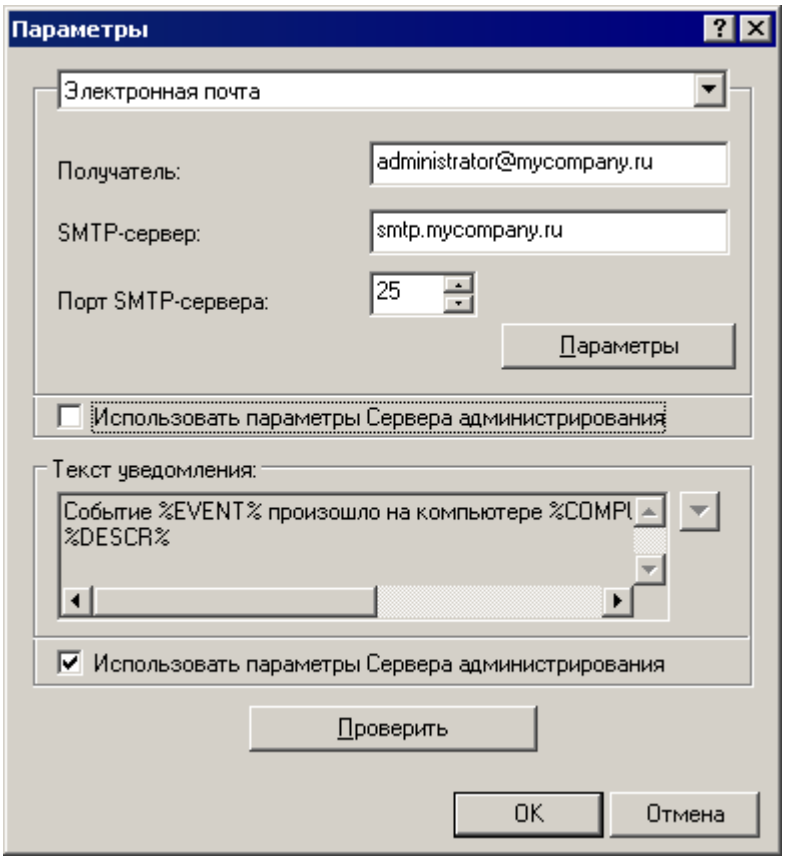

Рисунок 47. Редактирование параметров уведомления по электронной почте

Файлы с отложенной обработкой

Информация о файлах, очередная проверка и лечение которых отложены, содержится в папке **Хранилища** → **Файлы с отложенной обработкой**. В папке собирается информация обо всех таких файлах на Серверах администрирования и клиентских компьютерах.

Отложенные обработка и лечение осуществляются по требованию или после наступления определенного события. Предусмотрена возможность настройки параметров для отложенного лечения набора файлов.

Резервное копирование и восстановление данных Сервера администрирования

Резервное копирование позволяет переносить Сервер администрирования с одного компьютера на другой без каких-либо потерь информации, а также восстанавливать данные при переносе информационной базы Сервера администрирования на другой компьютер или при переходе на более новую версию программы Kaspersky Administration Kit.

При удалении Сервера администрирования с компьютера Kaspersky Administration Kit всегда предлагает создать резервную копию.

При резервном копировании сохранению или восстановлению подлежат:

- информационная база Сервера администрирования (политики, задачи, настройки программы и события, сохраненные на Сервере администрирования);

- конфигурационная информация о структуре групп администрирования и клиентских компьютерах;
- хранилище дистрибутивов программ для удаленной установки (содержимое папок Packages, Uninstall, Updates);
- сертификат Сервера администрирования.

Восстановление данных при переходе на более позднюю версию программы поддерживается, начиная с Kaspersky Administration Kit версии 5.0 Maintenance Pack 3.

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 параметры.

Копирование данных Сервера администрирования для резервного хранения и последующего восстановления может выполняться задачей резервного копирования данных либо вручную с помощью утилиты *klbackup*, входящей в состав дистрибутива Kaspersky Administration Kit. Восстановление данных производится только с помощью утилиты *klbackup*.

После установки Сервера администрирования утилита *klbackup* сохраняется в папке назначения, указанной при установке компонента, и при запуске из командной строки в зависимости от используемых ключей осуществляет копирование или восстановление данных.

Задача резервного копирования создается вручную и размещается в папке **Задачи Kaspersky Administration Kit**. Для выполнения резервного копирования данных следует настроить параметры данной задачи. Вы можете также создать задачу резервного копирования данных вручную: в качестве программы, для которой формируется задача, выберите **Kaspersky Administration Kit**; в качестве типа задачи – **Резервное копирование данных Сервера администрирования**.

ОБРАЩЕНИЕ В СЛУЖБУ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

Вы можете получить информацию о программе от специалистов Службы технической поддержки по телефону или через интернет. При обращении в Службу технической поддержки указывайте информацию о лицензии продукта «Лаборатории Касперского», совместно с которым используется программа.

Специалисты Службы технической поддержки ответят на ваши вопросы об установке и использовании программы, не отраженные в справке. Если ваш компьютер был заражен, они помогут преодолеть последствия работы вредоносных программ.

Прежде чем обращаться в Службу технической поддержки, пожалуйста, ознакомьтесь с правилами ее предоставления (http://support.kaspersky.ru/support/rules).

Электронный запрос в Службу технической поддержки

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

Запрос можно отправить на русском, английском, немецком, французском или испанском языках.

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

Если вы еще не являетесь зарегистрированным пользователем программ «Лаборатории Касперского», заполните регистрационную форму (https://support.kaspersky.com/ru/personalcabinet/registration/form/). При регистрации укажите *код активации* программы или *файл ключа*.

Вы получите ответ на свой запрос от специалиста Службы технической поддержки в своем Персональном кабинете (https://support.kaspersky.com/ru/PersonalCabinet) и по электронному адресу, который вы указали в запросе.

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

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

Техническая поддержка по телефону

Если возникла неотложная проблема, вы всегда можете позвонить в Службу технической поддержки в вашем городе. Перед обращением к специалистам русскоязычной (http://support.kaspersky.ru/support/support_local) или интернациональной (http://support.kaspersky.ru/support/international) технической поддержки, пожалуйста, соберите информацию (http://support.kaspersky.ru/support/details) о своем компьютере. Это поможет нашим специалистам быстрее помочь вам.

ГЛОССАРИЙ ТЕРМИНОВ

А

Агент администрирования

Компонент программы Kaspersky Administration Kit, осуществляющий взаимодействие между Сервером администрирования и программами «Лаборатории Касперского», установленными на конкретном сетевом узле (рабочей станции или сервере). Данный компонент является единым для всех Windows-программ из состава продуктов компании. Для Novell-, Unix- и Mac-программ «Лаборатории Касперского» существуют отдельные версии Агента администрирования.

Агент обновления

Компьютер, представляющий собой промежуточный центр распространения обновлений и инсталляционных пакетов в пределах группы администрирования.

Администратор Kaspersky Administration Kit

Лицо, управляющее работой программы через систему удаленного централизованного администрирования Kaspersky Administration Kit.

Активная лицензия

Лицензия, используемая в данный временной период для работы программы «Лаборатории Касперского». Лицензия определяет срок действия полной функциональности и лицензионную политику в отношении программы. В программе не может быть больше одной лицензии со статусом «активная».

Б

Базы

Базы данных, формируемые специалистами «Лаборатории Касперского» и содержащие подробное описание всех существующих на текущий момент угроз компьютерной безопасности, способов их обнаружения и обезвреживания. Базы постоянно обновляются в «Лаборатории Касперского» по мере появления новых угроз.

В

Восстановление

Перемещение оригинального объекта из карантина или резервного хранилища в папку его исходного расположения, где объект хранился до его помещения на карантин, лечения или удаления, либо другую папку, указанную пользователем.

Восстановление данных Сервера администрирования

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, параметры программы, сохраненные на Сервере администрирования события);
- конфигурационную информацию о структуре групп администрирования 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 программ «Лаборатории Касперского». Компьютеры группируются для удобства управления ими как единым целым. В состав группы могут входить другие группы. Для каждой из установленных в группе программ могут быть созданы групповые политики и сформированы групповые задачи.

Групповая задача

Задача, определенная для группы администрирования и выполняемая на всех входящих в ее состав клиентских компьютерах.

Д

Дополнительная лицензия

Лицензия, добавленная для работы программы «Лаборатории Касперского», но не активированная. Дополнительная лицензия начинает действовать по окончании срока действия активной лицензии.

Доступное обновление

Пакет обновлений модулей программы «Лаборатории Касперского», в состав которого включены набор срочных обновлений, собранных за некоторый период, и изменения в архитектуре программы.

З

Задача

Функции, выполняемые программой «Лаборатории Касперского», реализованы в виде задач, например: **Постоянная защита файлов**, **Полная проверка компьютера**, **Обновление баз**.

Задача для набора компьютеров

Задача, определенная для набора клиентских компьютеров из произвольных групп администрирования и выполняемая на них.

И

Инсталляционный пакет

Набор файлов, формируемый для удаленной установки программы «Лаборатории Касперского» при помощи системы удаленного управления Kaspersky Administration Kit. Инсталляционный пакет создается на основании специальных файлов с расширениями .kpd и .kud, входящих в состав дистрибутива программы, и содержит набор параметров, необходимых для установки программы и обеспечения ее работоспособности сразу после установки. Значения параметров соответствуют значениям параметров программы по умолчанию.

К

Клиент Сервера администрирования (Клиентский компьютер)

Компьютер, сервер или рабочая станция, на котором установлены Агент администрирования и управляемые программы «Лаборатории Касперского».

Консоль администрирования

Компонент программы Kaspersky Administration Kit, предоставляющий пользовательский интерфейс к административным сервисам Сервера администрирования и Агента администрирования.

Л

Локальная задача

Задача, определенная и выполняющаяся на отдельном клиентском компьютере.

Н

Непосредственное управление программой

Управление программой через локальный интерфейс.

Несовместимая программа

Антивирусная программа стороннего производителя или программа «Лаборатории Касперского», не поддерживающая управление через Kaspersky Administration Kit.

О

Обновление

Процедура замены / добавления новых файлов (баз или программных модулей), получаемых с серверов обновлений «Лаборатории Касперского».

Оператор Kaspersky Administration Kit

Пользователь, который ведет наблюдение за состоянием и работой системы защиты, управляемой при помощи Kaspersky Administration Kit.

П

Параметры задачи

Параметры работы программы, специфичные для каждого типа задач.

Параметры программы

Параметры работы программы, общие для всех типов ее задач и отвечающие за работу программы в целом, например, параметры производительности программы, параметры ведения отчетов, параметры резервного хранилища.

Плагин управления программой

Специализированный компонент, предоставляющий интерфейс для управления работой программы через Консоль администрирования. Для каждой программы существует свой плагин управления. Он входит в состав всех программ «Лаборатории Касперского», управление которыми может осуществляться при помощи Kaspersky Administration Kit.

Политика

Набор параметров работы программы в группе администрирования при управлении через Kaspersky Administration Kit. Для разных групп параметры работы программы могут быть различны. Для каждой программы определяется своя собственная политика. Политика включает в себя параметры полной настройки всей функциональности программы.

Порог вирусной активности

Максимально допустимое количество событий заданного типа в течение ограниченного времени, превышение которого будет считаться повышением вирусной активности и возникновением угрозы вирусной атаки. Данная характеристика имеет большое значение в периоды вирусных эпидемий и позволяет администратору своевременно реагировать на возникающие угрозы вирусных атак.

Р

Рабочее место администратора

Компьютер, на котором установлен компонент, предоставляющий интерфейс управления программой. Для Антивирусных продуктов это - Консоль Антивируса, для программы Kaspersky Administration Kit - Консоль администрирования.

С рабочего места администратора выполняются настройка серверной части программы и управление ею, а для Kaspersky Administration Kit – построение системы централизованной антивирусной защиты сети предприятия, сформированной на базе программ «Лаборатории Касперского», и управление ею.

Резервное копирование

Создание резервной копии файла перед его лечением или удалением и размещение этой копии в резервном хранилище с возможностью последующего восстановления файла, например, для его проверки с помощью обновленных баз.

Резервное копирование данных Сервера администрирования

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, параметры программы, сохраненные на Сервере администрирования события);
- конфигурационную информацию о структуре групп администрирования и клиентских компьютерах;
- хранилище дистрибутивов программ для удаленной установки (содержимое папок Packages, Uninstall, Updates);
- сертификат Сервера администрирования.

Резервное хранилище

Специальное хранилище, предназначенное для сохранения резервных копий объектов, создаваемых перед их первым лечением или удалением.

С

Сервер администрирования

Компонент программы Kaspersky Administration Kit, осуществляющий функции централизованного хранения информации об установленных в сети предприятия программах «Лаборатории Касперского» и управления ими.

Серверы обновлений «Лаборатории Касперского»

Список HTTP- и FTP-серверов «Лаборатории Касперского», с которых программа копирует базы и обновления модулей 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 во вложенной папке **Cert** папки установки программы.

Состояние защиты

Текущее состояние защиты, характеризующее степень защищенности компьютера.

Срок действия лицензии

Период, в течение которого вам предоставляется возможность использовать полную функциональность программы «Лаборатории Касперского». Срок действия лицензии, как правило, составляет календарный год со дня ее установки. После окончания срока действия лицензии функциональность программы сокращается: вы не сможете обновлять базы программы.

У

Удаленная установка

Установка программ «Лаборатории Касперского» при помощи сервисов, предоставляемых программой Kaspersky Administration Kit.

Уровень важности события

Характеристика события, зафиксированного в работе программы «Лаборатории Касперского». Существуют четыре уровня важности:

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

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

Установка с помощью сценария входа

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

Ф

Файл ключа

Файл с расширением *.key, который является вашим личным «ключом», необходимым для работы с программой «Лаборатории Касперского». Файл ключа входит в комплект поставки продукта, если вы приобрели его у дистрибьюторов «Лаборатории Касперского», или присылается вам по почте, если продукт был приобретен в интернет-магазине.

Форсированная установка

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

Х

Хранилище резервных копий

Специальная папка для сохранения копий данных Сервера администрирования, создаваемых при помощи утилиты резервного копирования.

Ц

Централизованное управление программой

Удаленное управление программой при помощи сервисов администрирования, предоставляемых Kaspersky Administration Kit.

ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

«Лаборатория Касперского» была основана в 1997 году. 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 тысячи 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 мировые разработчики используют в своих продуктах программное ядро Антивируса Касперского, например, такие как: Nokia ICG (США), Aladdin (Израиль), Sybari (США), G Data (Германия), Deerfield (США), Alt-N (США), Microworld (Индия), BorderWare (Канада).

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

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

Веб-сайт «Лаборатории Касперского»:	http://www.kaspersky.ru
Вирусная энциклопедия:	http://www.securelist.com/ru/
Антивирусная лаборатория:	newvirus@kaspersky.com (только для отправки подозрительных объектов в архивированном виде) http://support.kaspersky.ru/virlab/helpdesk.html (для запросов вирусным аналитикам)

ИНФОРМАЦИЯ О СТОРОННЕМ КОДЕ

Для создания программы использовался код сторонних производителей.

В ЭТОМ РАЗДЕЛЕ

Программный код

Для создания программы использовался программный код сторонних производителей.

В ЭТОМ РАЗДЕЛЕ

BOOST 1.34.1

Copyright (C) 2000-2003, Beman Dawes

GSOAP 2.7.0D

The gSOAP public license is derived from the Mozilla Public License (MPL1.1). The sections that were deleted from the original MPL1.1 text are 1.0.1, 2.1.(c),(d), 2.2.(c),(d), 8.2.(b), 10, and 11. Section 3.8 was added. The modified sections are 2.1.(b), 2.2.(b), 3.2 (simplified), 3.5 (deleted the last sentence), and 3.6 (simplified).

1 DEFINITIONS.

1.0.1.

1.1. «Contributor» means each entity that creates or contributes to the creation of Modifications.

1.2. «Contributor Version» means the combination of the Original Code, prior Modifications used by a Contributor, and the Modifications made by that particular Contributor.

1.3. «Covered Code» means the Original Code, or Modifications or the combination of the Original Code, and Modifications, in each case including portions thereof.

1.4. «Electronic Distribution Mechanism» means a mechanism generally accepted in the software development community for the electronic transfer of data.

1.5. «Executable» means Covered Code in any form other than Source Code.

1.6. «Initial Developer» means the individual or entity identified as the Initial Developer in the Source Code notice required by Exhibit A.

1.7. «Larger Work» means a work which combines Covered Code or portions thereof with code not governed by the

terms of this License.

1.8. «License» means this document.

1.8.1. «Licensable» means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.

1.9. «Modifications» means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications. When Covered Code is released as a series of files, a Modification is:

A. Any addition to or deletion from the contents of a file containing Original Code or previous Modifications.

B. Any new file that contains any part of the Original Code, or previous Modifications.

1.10. «Original Code» means Source Code of computer software code which is described in the Source Code notice required by Exhibit A as Original Code, and which, at the time of its release under this License is not already Covered Code governed by this License.

1.10.1. «Patent Claims» means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.

1.11. «Source Code» means the preferred form of the Covered Code for making modifications to it, including all modules it contains, plus any associated interface definition files, scripts used to control compilation and installation of an Executable, or source code differential comparisons against either the Original Code or another well known, available Covered Code of the Contributor’s choice. The Source Code can be in a compressed or archival form, provided the appropriate decompression or de-archiving software is widely available for no charge.

1.12. «You» (or «Your») means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License or a future version of this License issued under Section 6.1. For legal entities, «You» includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, «control» means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2 SOURCE CODE LICENSE.

2.1. The Initial Developer Grant.

The Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims:

(a) under intellectual property rights (other than patent or trademark) Licensable by Initial Developer to use, reproduce, modify, display, perform, sublicense and distribute the Original Code (or portions thereof) with or without Modifications, and/or as part of a Larger Work; and

(b) under patents now or hereafter owned or controlled by Initial Developer, to make, have made, use and sell («offer to sell and import») the Original Code, Modifications, or portions thereof, but solely to the extent that any such patent is reasonably necessary to enable You to utilize, alone or in combination with other software, the Original Code, Modifications, or any combination or portions thereof.

(c)

(d)

2.2. Contributor Grant.

Subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royaltyfree, non-exclusive license

(a) under intellectual property rights (other than patent or trademark) Licensable by Contributor, to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof) either on an unmodified basis, with other Modifications, as Covered Code and/or as part of a Larger Work; and

(b) under patents now or hereafter owned or controlled by Contributor, to make, have made, use and sell («offer to sell and import») the Contributor Version (or portions thereof), but solely to the extent that any such patent is reasonably necessary to enable You to utilize, alone or in combination with other software, the Contributor Version (or portions thereof).

(c)

(d)

3 DISTRIBUTION OBLIGATIONS.

3.1. Application of License.

The Modifications which You create or to which You contribute are governed by the terms of this License

including without limitation Section 2.2. The Source Code version of Covered Code may be distributed only under the terms of this License or a future version of this License released under Section 6.1, and You must include a copy of this License with every copy of the Source Code You distribute. You may not offer or impose any terms on any Source Code version that alters or restricts the applicable version of this License or the recipients' rights hereunder. However, You may include an additional document offering the additional rights described in Section 3.5.

3.2. Availability of Source Code.

Any Modification created by You will be provided to the Initial Developer in Source Code form and are subject to the terms of the License.

3.3. Description of Modifications.

You must cause all Covered Code to which You contribute to contain a file documenting the changes You made to create that Covered Code and the date of any change. You must include a prominent statement that the Modification is derived, directly or indirectly, from Original Code provided by the Initial Developer and including the name of the Initial Developer in (a) the Source Code, and (b) in any notice in an Executable version or related documentation in which You describe the origin or ownership of the Covered Code.

3.4. Intellectual Property Matters.

(a) Third Party Claims. If Contributor has knowledge that a license under a third party's intellectual property rights is required to exercise the rights granted by such Contributor under Sections 2.1 or 2.2, Contributor must include a text file with the Source Code distribution titled «LEGAL» which describes the claim and the party making the claim in sufficient detail that a recipient will know whom to contact. If Contributor obtains such knowledge after the Modification is made available as described in Section 3.2, Contributor shall promptly modify the LEGAL file in all copies Contributor makes available thereafter and shall take other steps (such as notifying appropriate mailing lists or newsgroups) reasonably calculated to inform those who received the Covered Code that new knowledge has been obtained.

(b) Contributor APIs. If Contributor's Modifications include an application programming interface and Contributor has knowledge of patent licenses which are reasonably necessary to implement that API, Contributor must also include this information in the LEGAL file.

(c) Representations. Contributor represents that, except as disclosed pursuant to Section 3.4(a) above, Contributor believes that Contributor's Modifications are Contributor's original creation(s) and/or Contributor has sufficient rights to grant the rights conveyed by this License.

3.5. Required Notices.

You must duplicate the notice in Exhibit A in each file of the Source Code. If it is not possible to put such notice in a particular Source Code file due to its structure, then You must include such notice in a location (such as a relevant directory) where a user would be likely to look for such a notice. If You created one or more Modification(s) You may add your name as a Contributor to the notice described in Exhibit A. You must also duplicate this License in any documentation for the Source Code where You describe recipients' rights or ownership rights relating to Covered Code. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Code. However, You may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor.

3.6. Distribution of Executable Versions.

You may distribute Covered Code in Executable form only if the requirements of Section 3.1-3.5 have been met for that Covered Code. You may distribute the Executable version of Covered Code or ownership rights under a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable version does not attempt to limit or alter the recipient's rights in the Source Code version from the rights set forth in this License. If You distribute the Executable version under a different license You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or any Contributor. If you distribute executable versions containing Covered Code as part of a product, you must reproduce the notice in Exhibit B in the documentation and/or other materials provided with the product.

3.7. Larger Works.

You may create a Larger Work by combining Covered Code with other code not governed by the terms of this License and distribute the LargerWork as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Code.

3.8. Restrictions.

You may not remove any product identification, copyright, proprietary notices or labels from gSOAP.

4 INABILITY TO COMPLY DUE TO STATUTE OR REGULATION.

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Code due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum

extent possible; and (b) describe the limitations and the code they affect. Such description must be included in the LEGAL file described in Section 3.4 and must be included with all distributions of the Source Code. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5 APPLICATION OF THIS LICENSE.

This License applies to code to which the Initial Developer has attached the notice in Exhibit A and to related Covered Code.

6 VERSIONS OF THE LICENSE.

6.1. New Versions.

Grantor may publish revised and/or new versions of the License from time to time. Each version will be given a distinguishing version number.

6.2. Effect of New Versions.

Once Covered Code has been published under a particular version of the License, You may always continue to use it under the terms of that version. You may also choose to use such Covered Code under the terms of any subsequent version of the License.

6.3. Derivative Works.

If You create or use a modified version of this License (which you may only do in order to apply it to code which is not already Covered Code governed by this License), You must (a) rename Your license so that the phrase «gSOAP» or any confusingly similar phrase do not appear in your license (except to note that your license differs from this License) and (b) otherwise make it clear that Your version of the license contains terms which differ from the gSOAP Public License. (Filling in the name of the Initial Developer, Original Code or Contributor in the notice described in Exhibit A shall not of themselves be deemed to be modifications of this License.)

7 DISCLAIMER OF WARRANTY.

COVERED CODE IS PROVIDED UNDER THIS LICENSE ON AN «AS IS» BASIS, WITHOUT WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, WITHOUT LIMITATION, THE IMPLIEDWARRANTIES OF MERCHANTABILITY, OF FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS, AND ANY WARRANTY THAT MAY ARISE BY REASON OF TRADE USAGE, CUSTOM, OR COURSE OF DEALING. WITHOUT LIMITING THE FOREGOING, YOU ACKNOWLEDGE THAT THE SOFTWARE IS PROVIDED «AS IS» AND THAT THE AUTHORS DO NOTWARRANT THE SOFTWAREWILL RUN UNINTERRUPTED OR ERROR FREE. LIMITED

LIABILITY THE ENTIRE RISK AS TO RESULTS AND PERFORMANCE OF THE SOFTWARE IS ASSUMED BY YOU. UNDER NO CIRCUMSTANCES WILL THE AUTHORS BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES OF ANY KIND OR NATURE WHATSOEVER, WHETHER BASED ON CONTRACT, WARRANTY, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, ARISING OUT OF OR IN ANY WAY RELATED TO THE SOFTWARE, EVEN IF THE AUTHORS HAVE BEEN ADVISED ON THE POSSIBILITY OF SUCH DAMAGE OR IF SUCH DAMAGE COULD HAVE BEEN REASONABLY FORESEEN, AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY EXCLUSIVE REMEDY PROVIDED. SUCH LIMITATION ON DAMAGES INCLUDES, BUT IS NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOST PROFITS, LOSS OF DATA OR SOFTWARE, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION OR IMPAIRMENT OF OTHER GOODS. IN NO EVENTWILL THE AUTHORS BE LIABLE FOR THE COSTS OF PROCUREMENT OF SUBSTITUTE SOFTWARE OR SERVICES. YOU ACKNOWLEDGE THAT THIS SOFTWARE IS NOT DESIGNED FOR USE IN ON-LINE EQUIPMENT IN HAZARDOUS ENVIRONMENTS SUCH AS OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR CONTROL, OR LIFE-CRITICAL APPLICATIONS. THE AUTHORS EXPRESSLY DISCLAIM ANY LIABILITY RESULTING FROM USE OF THE SOFTWARE IN ANY SUCH ON-LINE EQUIPMENT IN HAZARDOUS ENVIRONMENTS AND ACCEPTS NO LIABILITY IN RESPECT OF ANY ACTIONS OR CLAIMS BASED ON THE USE OF THE SOFTWARE IN ANY SUCH ONLINE EQUIPMENT IN HAZARDOUS ENVIRONMENTS BY YOU. FOR PURPOSES OF THIS PARAGRAPH, THE TERM «LIFE-CRITICAL

APPLICATION» MEANS AN APPLICATION IN WHICH THE FUNCTIONING OR MALFUNCTIONING OF THE SOFTWARE MAY RESULT DIRECTLY OR INDIRECTLY IN PHYSICAL INJURY OR LOSS OF HUMAN LIFE. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY COVERED CODE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

8 TERMINATION.

8.1. This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. All sublicenses to the Covered Code which are properly granted shall survive any termination of this License. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

8.2.

8.3. If You assert a patent infringement claim against Participant alleging that such Participant's Contributor Version directly or indirectly infringes any patent where such claim is resolved (such as by license or settlement) prior to the initiation of patent infringement litigation, then the reasonable value of the licenses granted by such Participant under Sections 2.1 or 2.2 shall be taken into account in determining the amount or value of any payment or license.

8.4. In the event of termination under Sections 8.1 or 8.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or any distributor hereunder prior to termination shall survive termination.

9 LIMITATION OF LIABILITY.

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL YOU, THE INITIAL DEVELOPER, ANY OTHER CONTRIBUTOR, OR ANY DISTRIBUTOR OF COVERED CODE, OR ANY SUPPLIER OF ANY OF SUCH PARTIES, BE LIABLE TO ANY PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM SUCH PARTY'S NEGLIGENCE TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

10 U.S. GOVERNMENT END USERS.

11 MISCELLANEOUS.

12 RESPONSIBILITY FOR CLAIMS.

As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.

EXHIBIT A.

«The contents of this file are subject to the gSOAP Public License Version 1.3 (the “License”); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.cs.fsu.edu/~engelen/soaplicense.html

Software distributed under the License is distributed on an “AS IS” basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License. The Original Code of the gSOAP Software is: stdsoap.h, stdsoap2.h, stdsoap.c, stdsoap2.c, stdsoap.cpp, stdsoap2.cpp, soapcpp2.h, soapcpp2.c, soapcpp2 lex.l, soapcpp2 yacc.y, error2.h, error2.c, symbol2.c, init2.c, soapdoc2.html, and soapdoc2.pdf, httpget.h, httpget.c, stl.h, stldeque.h, stllist.h, stlvector.h, stlset.h.

The Initial Developer of the Original Code is Robert A. van Engelen. Portions created by Robert A. van Engelen are Copyright (C) 2001–2004 Robert A. van Engelen, Genivia inc. All Rights Reserved.

Contributor(s):

“___”

[Note: The text of this Exhibit A may differ slightly form the text of the notices in the Source Code files of the Original code. You should use the text of this Exhibit A rather than the text found in the Original Code Source Code for Your Modifications.]

EXHIBIT B.

“Part of the software embedded in this product is gSOAP software.

Portions created by gSOAP are Copyright (C) 2001–2004 Robert A. van Engelen, Genivia inc. All Rights Reserved.

THE SOFTWARE IN THIS PRODUCT WAS IN PART PROVIDED BY GENIVIA INC AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANYWAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.”

LIBMSPACK 2004-03-08

Copyright (C) 2003-2004, Stuart Caie

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do

these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original

author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that

any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary

General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the

entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the “Lesser” General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a “work based on the library” and a “work that uses the library”. The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called “this License”). Each licensee is addressed as “you”.

A “library” means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The “Library”, below, refers to any such software library or work which has been distributed under these terms. A “work based on the Library” means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a

portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term “modification”.)

“Source code” for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for

writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you

distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a

medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not

compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a “work that uses the Library”. Such a work, in isolation, is not a derivative work of the Library, and

therefore falls outside the scope of this License.

However, linking a “work that uses the Library” with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a “work that uses the library”. The executable is therefore covered by this License.

Section 6 states terms for distribution of such executables.

When a “work that uses the Library” uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be

linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative

work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a “work that uses the Library” with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit

modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable “work that uses the Library”, as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the “work that uses the Library” must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is

normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein.

You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues),conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by

all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus

excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our

decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO

WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN

WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA. Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a “copyright disclaimer” for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990

Ty Coon, President of Vice

That's all there is to it!

In addition to the provisions of the LGPL, you are permitted to use the library directly as part of your build process provided you meet all of the following conditions:

Any modifications to the existing libmspack source code are ALL published and distributed under the LGPL license.

You MUST NOT use function calls, structures or definitions unless they are defined in the public library interface, “mspack.h”.

MICROSOFT .NET FRAMEWORK VERSION 2.0 REDISTRIBUTABLE PACKAGE (X86)

Copyright (C) 2008, Microsoft Corporation

MICROSOFT CORE XML SERVICES (MSXML) 6.0

Copyright (C) 2008, Microsoft Corporation

MICROSOFT DATA ACCESS COMPONENTS (MDAC) 2.8

Copyright (C) 2008, Microsoft Corporation

MICROSOFT SQL SERVER 2005 EXPRESS EDITION SERVICE PACK 3

Copyright (C) 2007, Microsoft Corporation

MYSQL C API

Copyright (C) 1995-2008, MySQL AB

OPENSSL 0.9.8L

Copyright (C) 1998-2008, The OpenSSL Project

Copyright (C) 1995-1998, Eric A. Young (eay@cryptsoft.com), Tim J. Hudson (tjh@cryptsoft.com)

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)”

The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.

Redistributions of any form whatsoever must retain the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

All advertising materials mentioning features or use of this software must display the following acknowledgement: “This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”

The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, TRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

STLPORT 4.6.2

Copyright (C) 1994, Hewlett-Packard Company

Copyright (C) 1996-1999, Silicon Graphics Computer Systems, Inc.

Copyright (C) 1997, Moscow Center for SPARC Technology

Copyright (C) 1999, 2000, 2001, 2002, Boris Fomitchev

This software is being distributed under the following terms :

This material is provided “as is”, with absolutely no warranty expressed or implied. Any use is at your own risk.

Permission to use or copy this software for any purpose is hereby granted without fee, provided the above notices are retained on all copies.

Permission to modify the code and to distribute modified code is granted, provided the above notices are retained, and a notice that the code was modified is included with the above copyright notice.

UNZIP 5.52

Copyright (C) 1990-2005, Info-ZIP

For the purposes of this copyright and license, “Info-ZIP” is defined as

the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White.

This software is provided “as is,” without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

Redistributions of source code must retain the above copyright notice, definition, disclaimer, and this list of conditions.

Redistributions in binary form (compiled executables) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, and dynamic, shared, or static library versions--must be plainly marked as such and must not be misrepresented as being the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names “Info-ZIP” (or any variation thereof, including, but not limited to, different capitalizations), “Pocket UnZip,” “WiZ” or “MacZip” without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or of the Info-ZIP URL(s).

Info-ZIP retains the right to use the names “Info-ZIP,” “Zip,” “UnZip,” “UnZipSFX,” “WiZ,” “Pocket UnZip,” “Pocket Zip,” and “MacZip” for its own source and binary releases.

VISUAL STUDIO 6.0 SERVICE PACK 6 WINDOWS INSTALLER MERGE MODULES

Copyright (C) 2004, Microsoft Corporation

WINDOWS INSTALLER 3.1 REDISTRIBUTABLE (V2)

ZLIB 1.2.3

Другая информация

Для проверки электронной цифровой подписи используется программная библиотека защиты информации (ПБЗИ) “Агава-С”, разработанная ООО “Р-Альфа”.

Данный продукт содержит или может содержать программы, которые лицензируются (или сублицензируются) пользователю в соответствии с общедоступной лицензией GNU или иными аналогичными лицензиями Open Source, которые помимо прочих прав разрешают пользователю копировать, модифицировать, перераспределять определенные программы или их части и получать доступ к исходному коду (“ПО с открытым исходным кодом”). Если такая лицензия предусматривает предоставление исходного кода пользователям, которым предоставляется ПО в формате исполняемого двоичного кода, исходный код делается доступным при осуществлении запроса на адрес source@kaspersky.com или сопровождается с продуктом.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

Р

С

У

Х