Особенности использования Антивируса Касперского для рабочих станций 6.0

Яшутина Ольга
Методист образовательных программ
Olga.Yashutina@kaspersky.com

Антивирус Касперского для Windows Workstations

Обеспечивает блокирование вредоносных программ по каналам:

- Гибкие диски
- Локальные и сетевые ресурсы
- Электронная почта
- Интернет

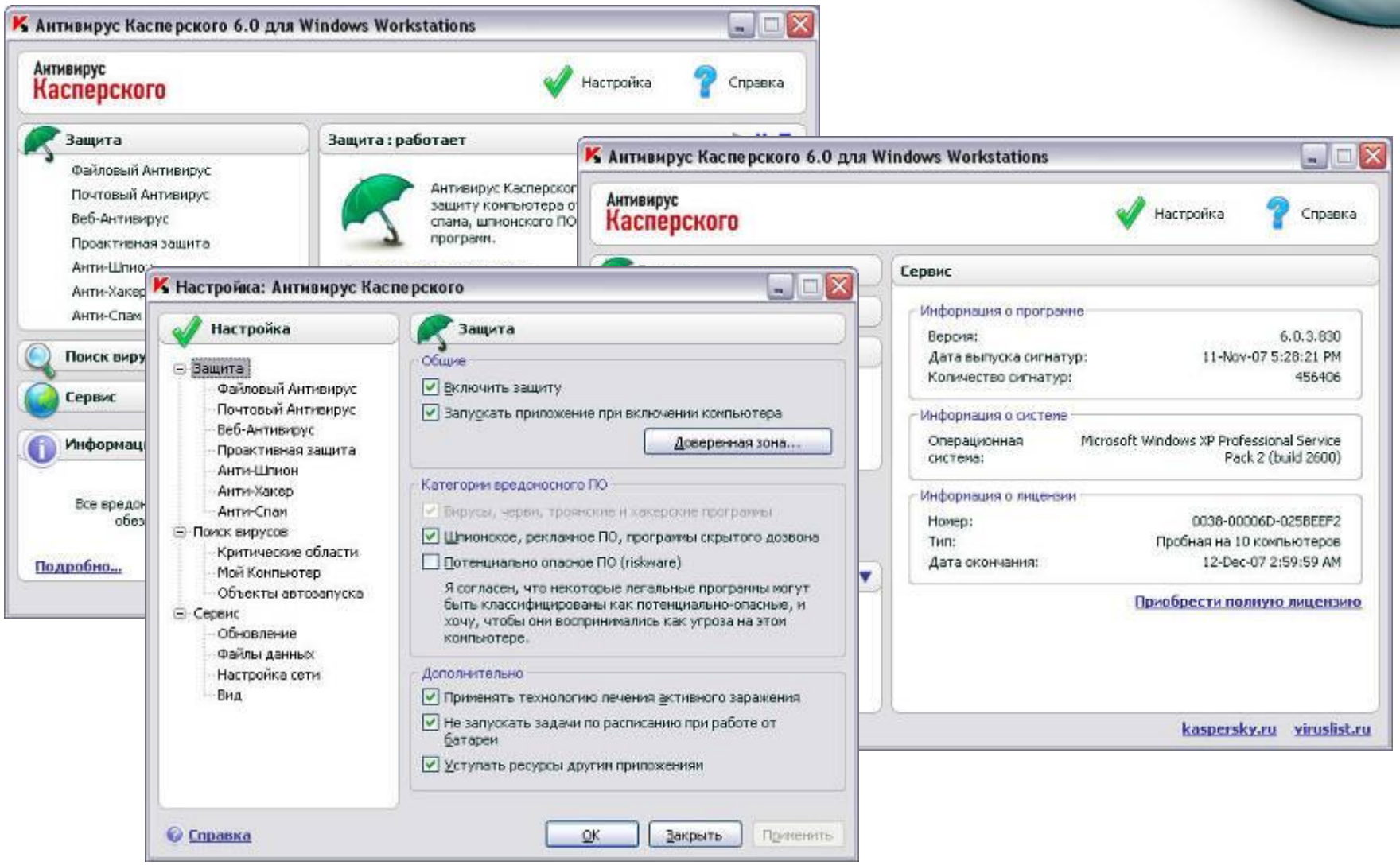
Поддерживаемые платформы

- MS Windows 98 / Me
- MS Windows NT 4.0 Workstation
- MS Windows 2000 Professional
- MS Windows XP Home / XP Professional
- MS Windows Vista

Назначение Антивируса Касперского

- Защита в режиме реального времени
  - файловой системы
  - электронной почты
  - защита при работе в сети Интернет
  - контроль активности приложений
  - контроль сетевых соединений
  - защита от сетевых атак
- Поиск вредоносных программ
- Обновление сигнатур угроз и компонентов приложения
- Аварийная проверка и восстановление системы

Пользовательский интерфейс



Состав Антивируса Касперского

- Компоненты защиты
- Задачи поиска вирусов
- Сервисные функции

Модули приложения

- Базовый модуль
  - антивирусный сканер
  - компонент загрузки обновлений
- Набор опциональных компонентов
  - Файловый Антивирус
  - Почтовый Антивирус
  - Веб-Антивирус
  - Проактивная защита
  - Анти-Шпион
  - Анти-Хакер
  - Анти-Спам

Управление системой защиты

- Настройка и запуск компонентов и задач, получение отчетов
- Создание дисков для аварийной проверки и восстановления системы
- Установка ограничений на доступ к функциям продукта
- Обработка файлов на карантине и в резервном хранилище
- Обращение в службу технической поддержки

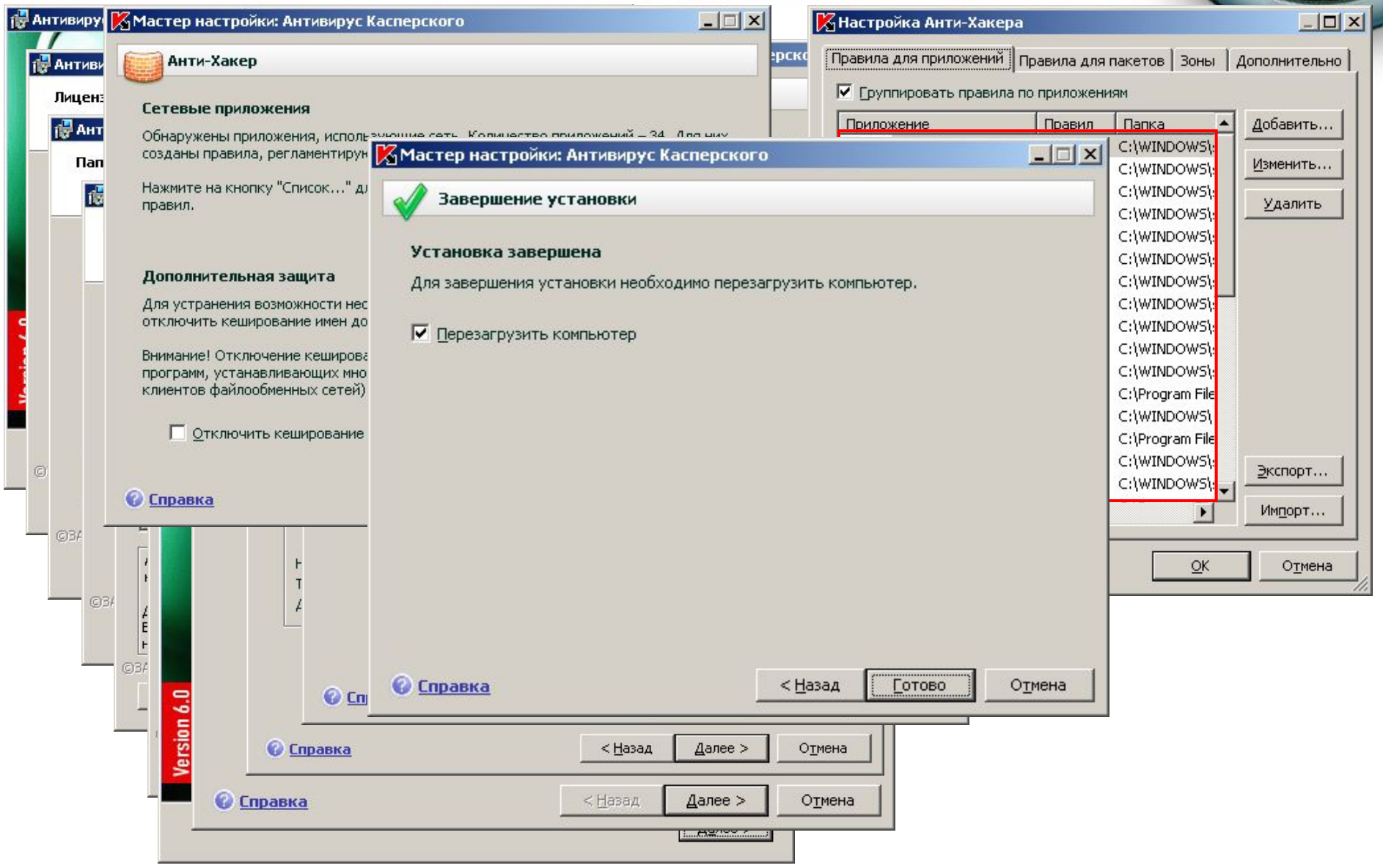
Причины возникновения ошибок при установке :

1. Системные требования
2. Приложения, не совместимые с Антивирусом Касперского 6.0 (http://support.kaspersky.ru/faq/?qid=208635502)
3. Права администратора
4. Размер файла-дистрибутива
5. Вредоносные программы

-проверка на вирусы on-line

-диск аварийного восстановления

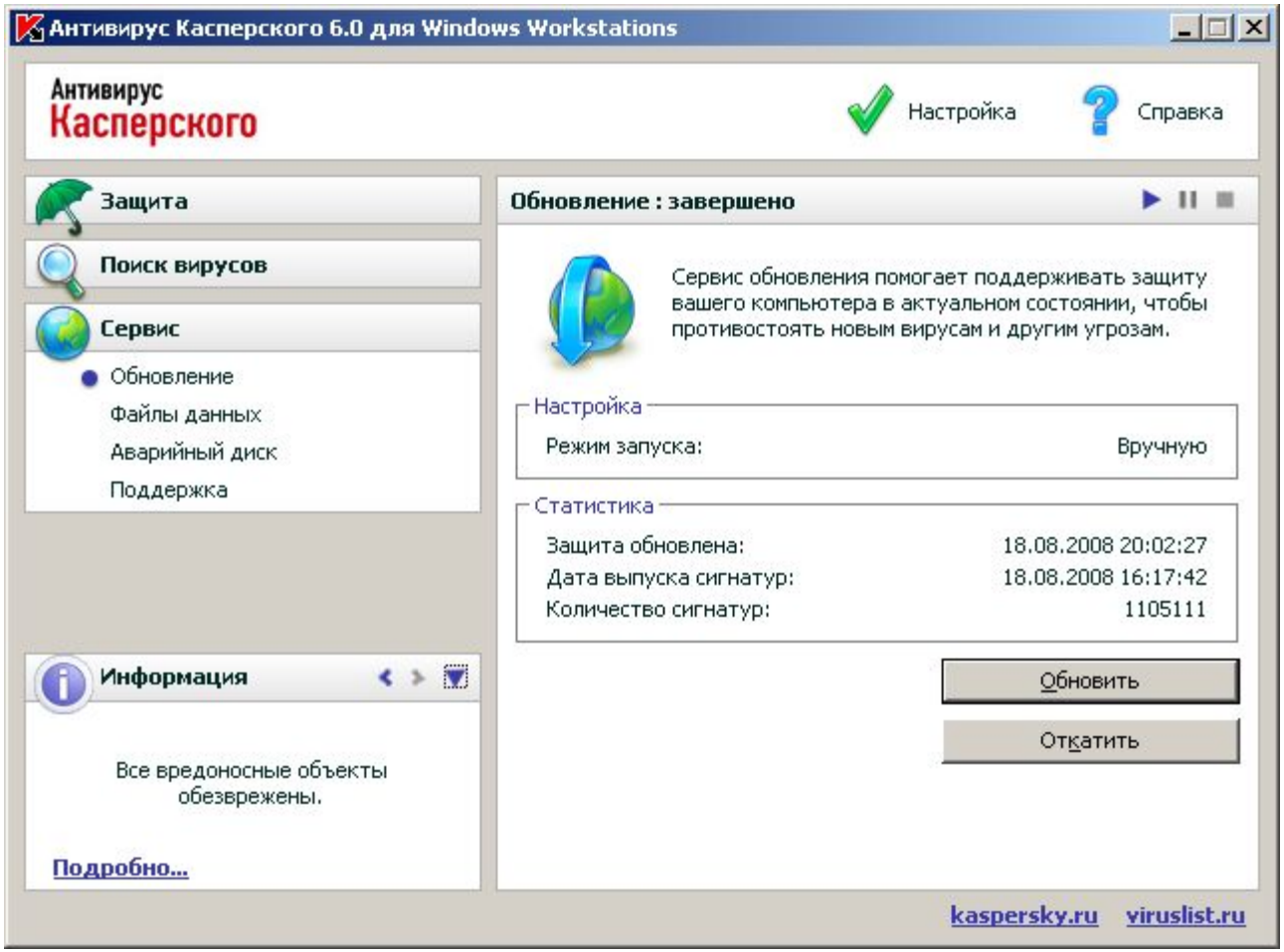
Процесс установки



Значки-индикаторы на системной панели

Значок	Описание
	Хотя бы один компонент защиты запущен
	Проверка файлов на жестких, сменных или сетевых дисках
	Все компоненты защиты выключены
	Проверка файлов при выключенных компонентах защиты
	Проверка почтовых сообщений
	Запущена задача обновления
	Обновление при выключенных компонентах защиты
	Проверка скриптов

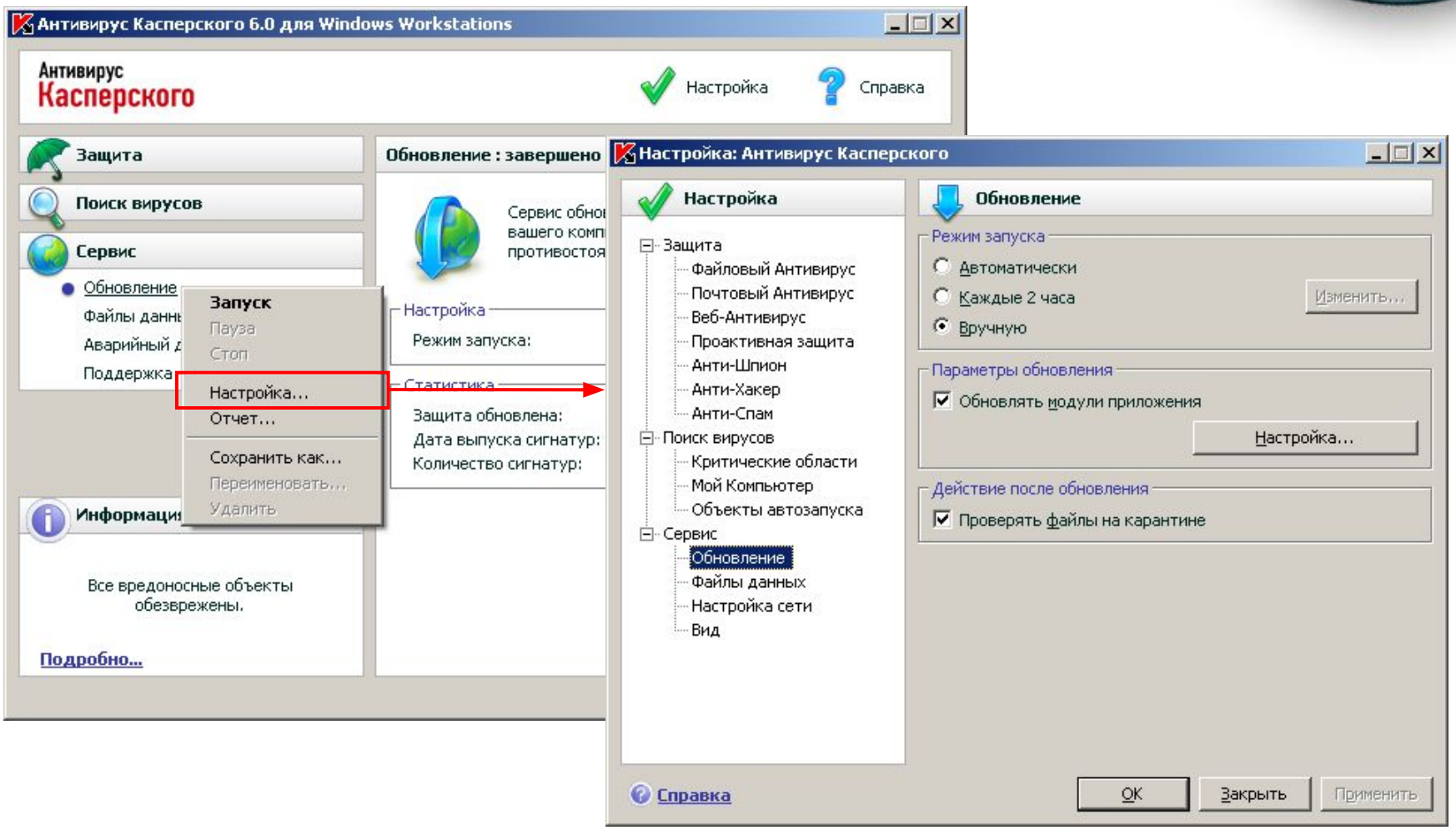
Задача обновления



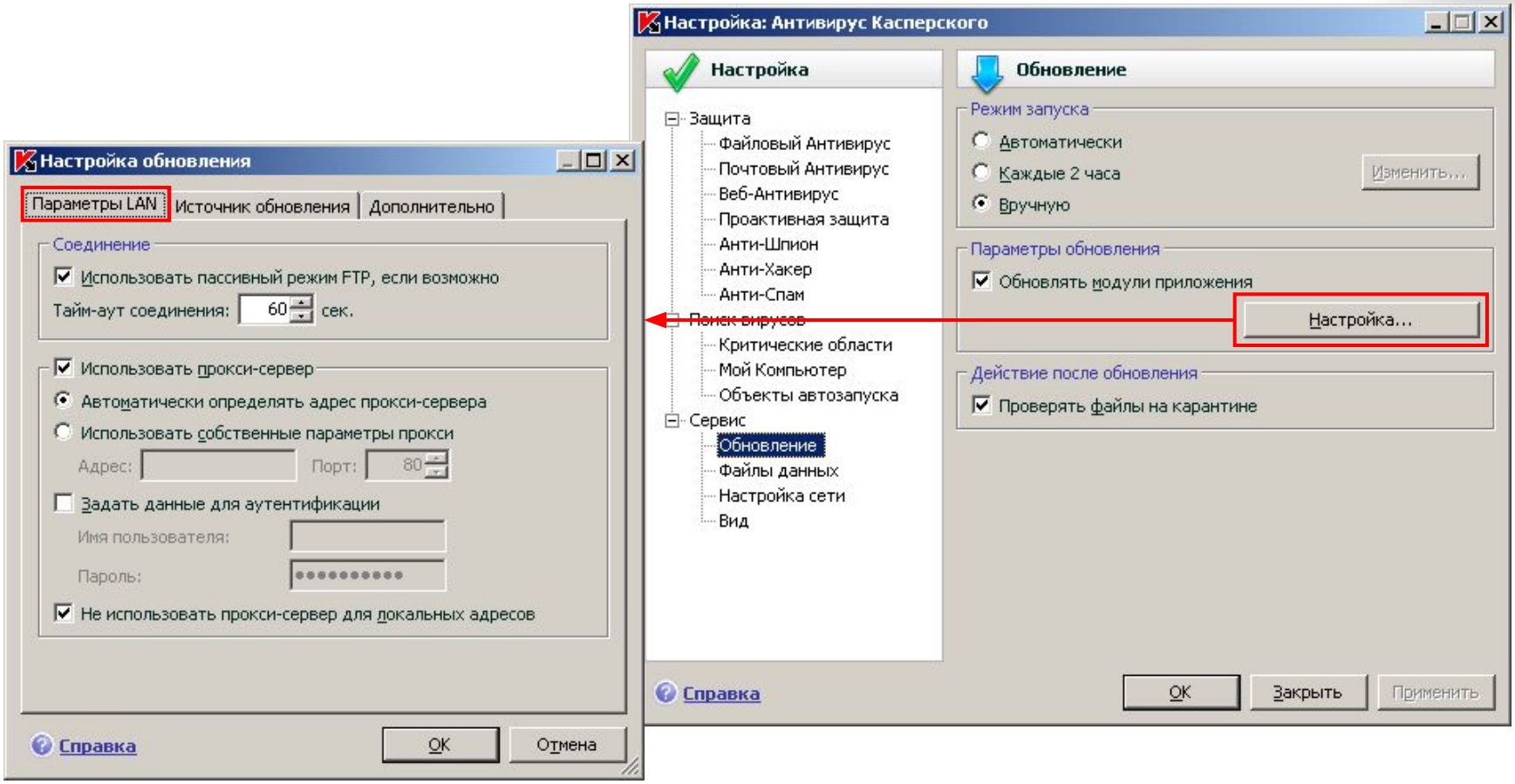
Причины возникновения ошибок при обновлении антивирусных баз

1. Другой антивирус, брандмауэр (сетевой экран)
2. Настройки прокси-сервера
3. Неправильно указан путь к источнику обновлений
4. Установлены ограничения на прокси-сервере на названия расширений или на размер скачиваемых файлов

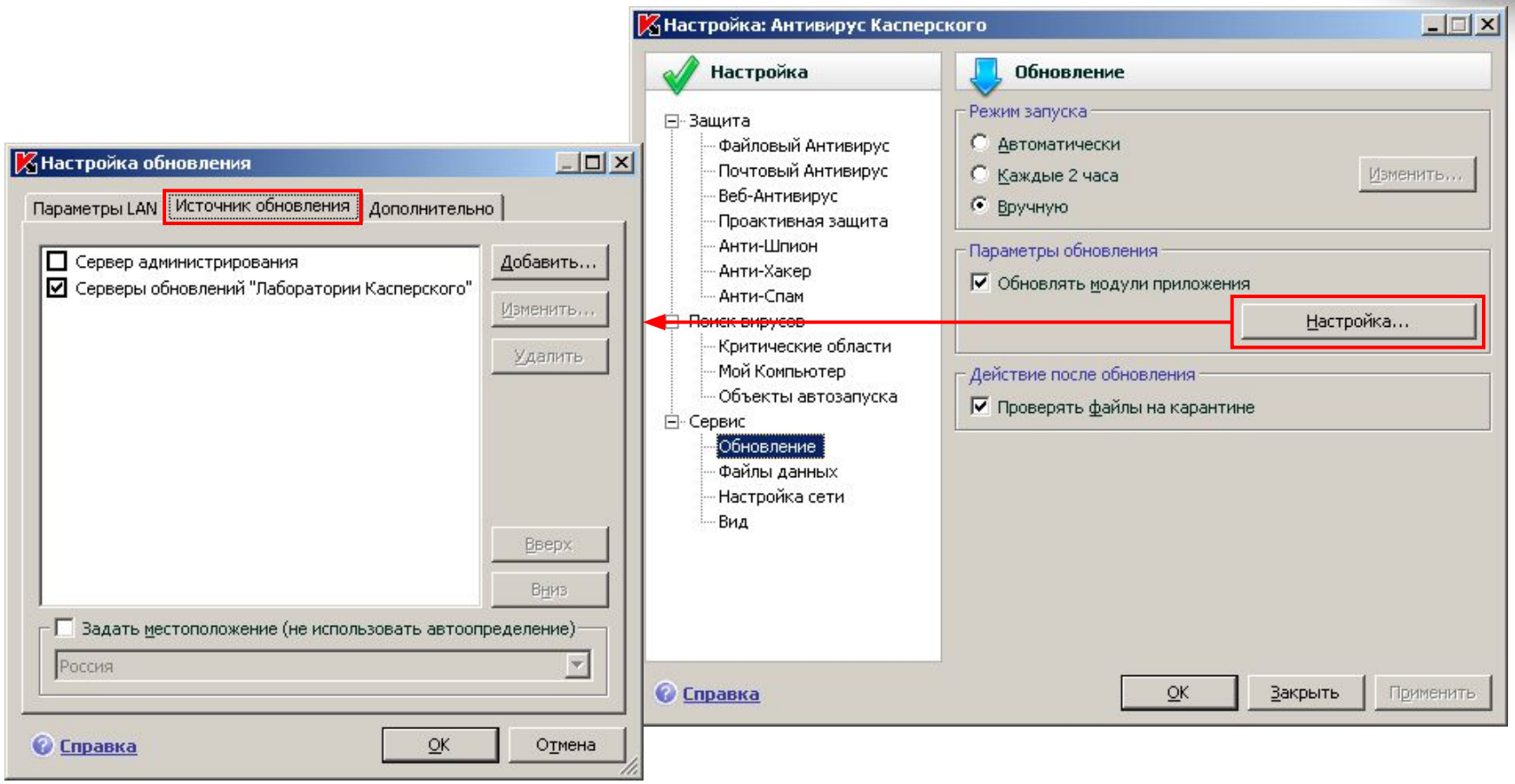
Настройка обновления



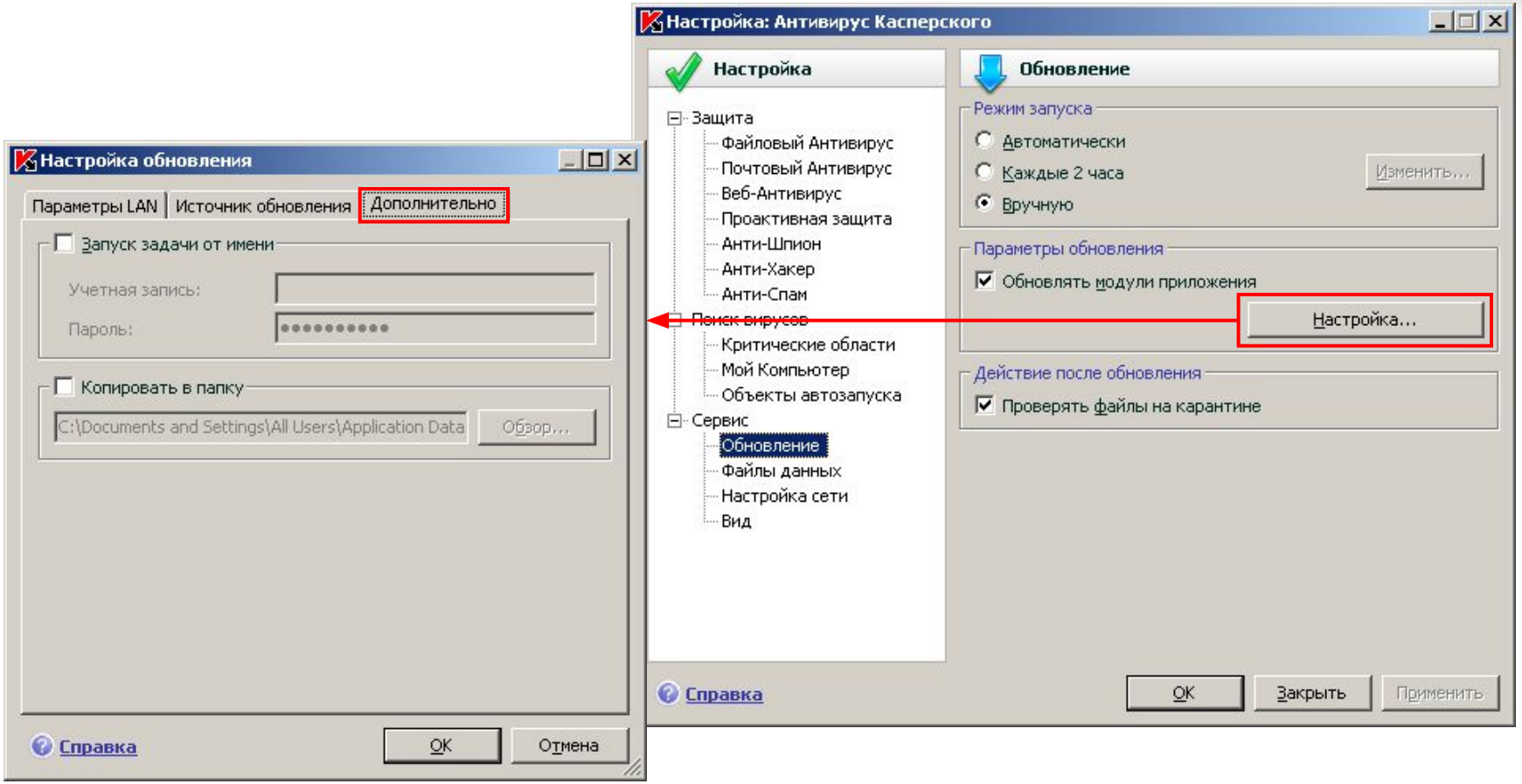
Параметры LAN



Выбор источника обновлений



Дополнительные настройки



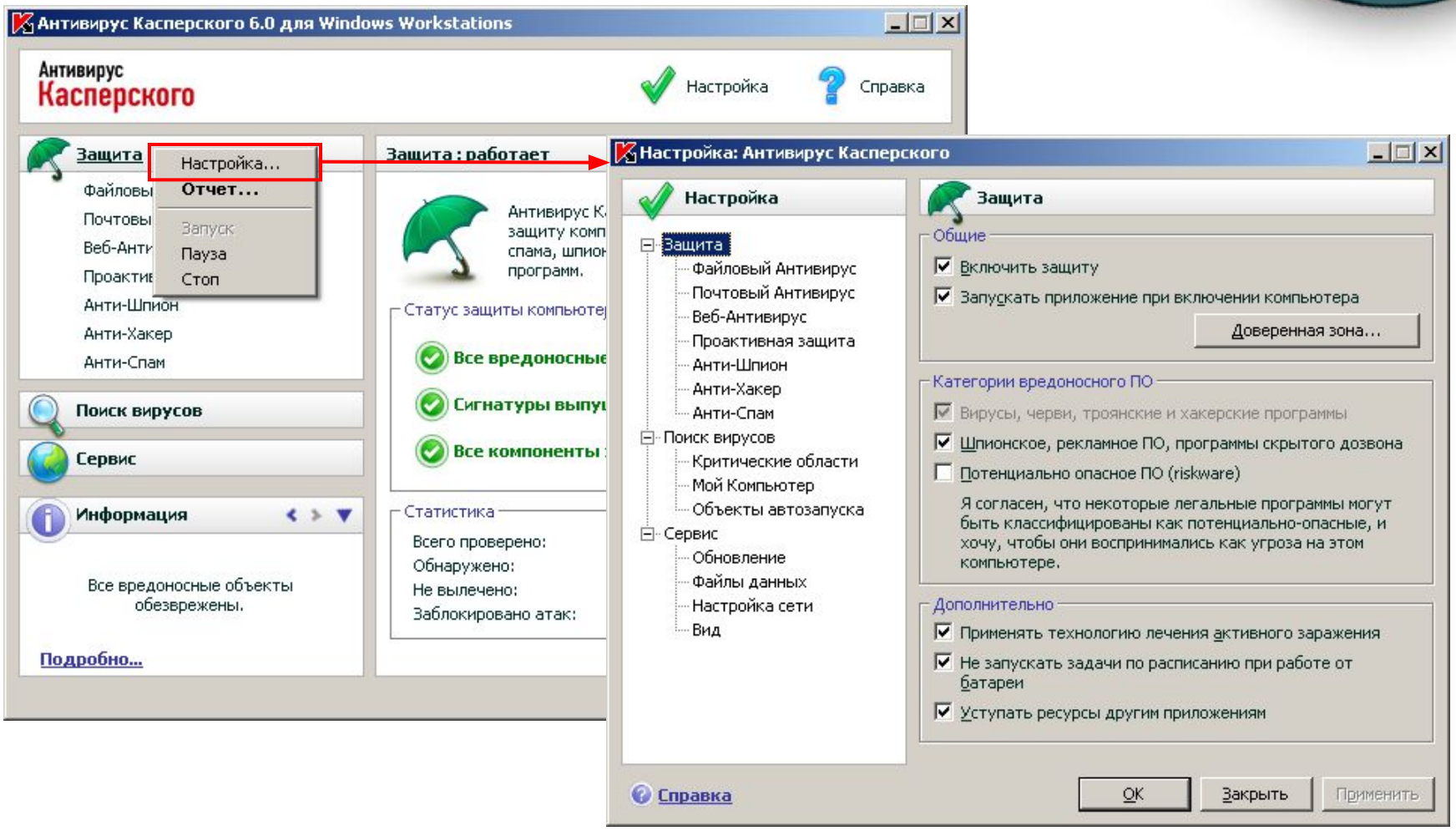
Улучшения в версии 6.0

- Технологии оптимизации и ускорения антивирусной проверки
- Комплекс проактивных технологий
- Установка программы на уже зараженный компьютер и лечение вредоносных программ, активных в оперативной памяти
- Проверка любого трафика, в том числе HTTP
- Защита от шпионского ПО и рекламы
- Технология уменьшения размеров обновлений
- Средства создания аварийного диска
- Возможность отсылки писем по событиям в продукте
- Улучшенная технология самозащиты от вредоносных программ

Время сканирования и нагрузка на систему

- Сканирование только новых и изменённых файлов: оптимизация скорости сканирования без влияния на качество
- Технологии ускорения сканирования (iSwift и iChecker) за счёт интеллектуального кэширования данных предыдущих проверок
- Уменьшение влияния на производительность системы:
  - Приостановка сканирования в случае увеличения пользовательской активности
  - Приостановка сканирования в случае работы от батареи
  - Новый механизм сканирования составных объектов

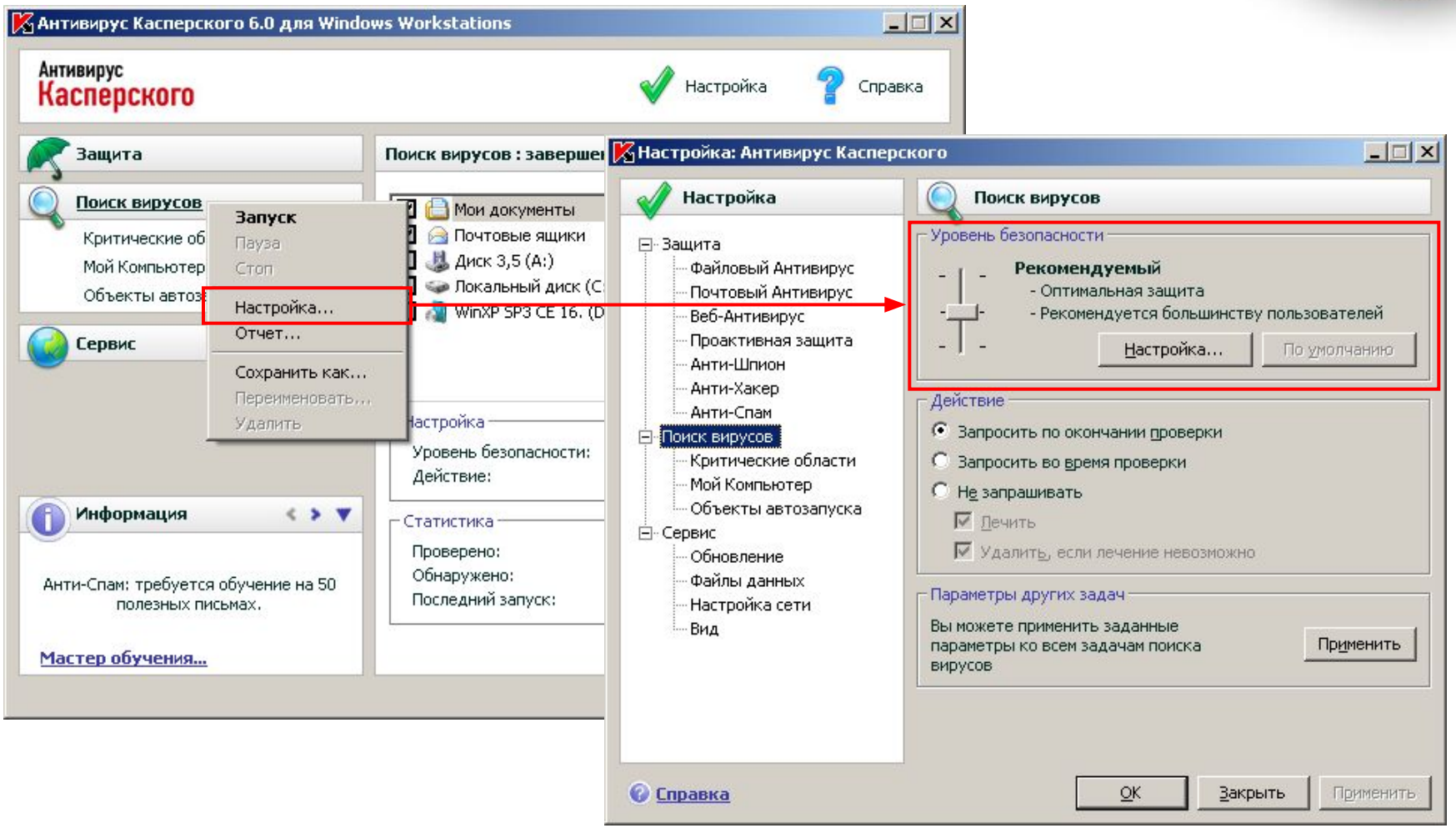
Общие настройки защиты



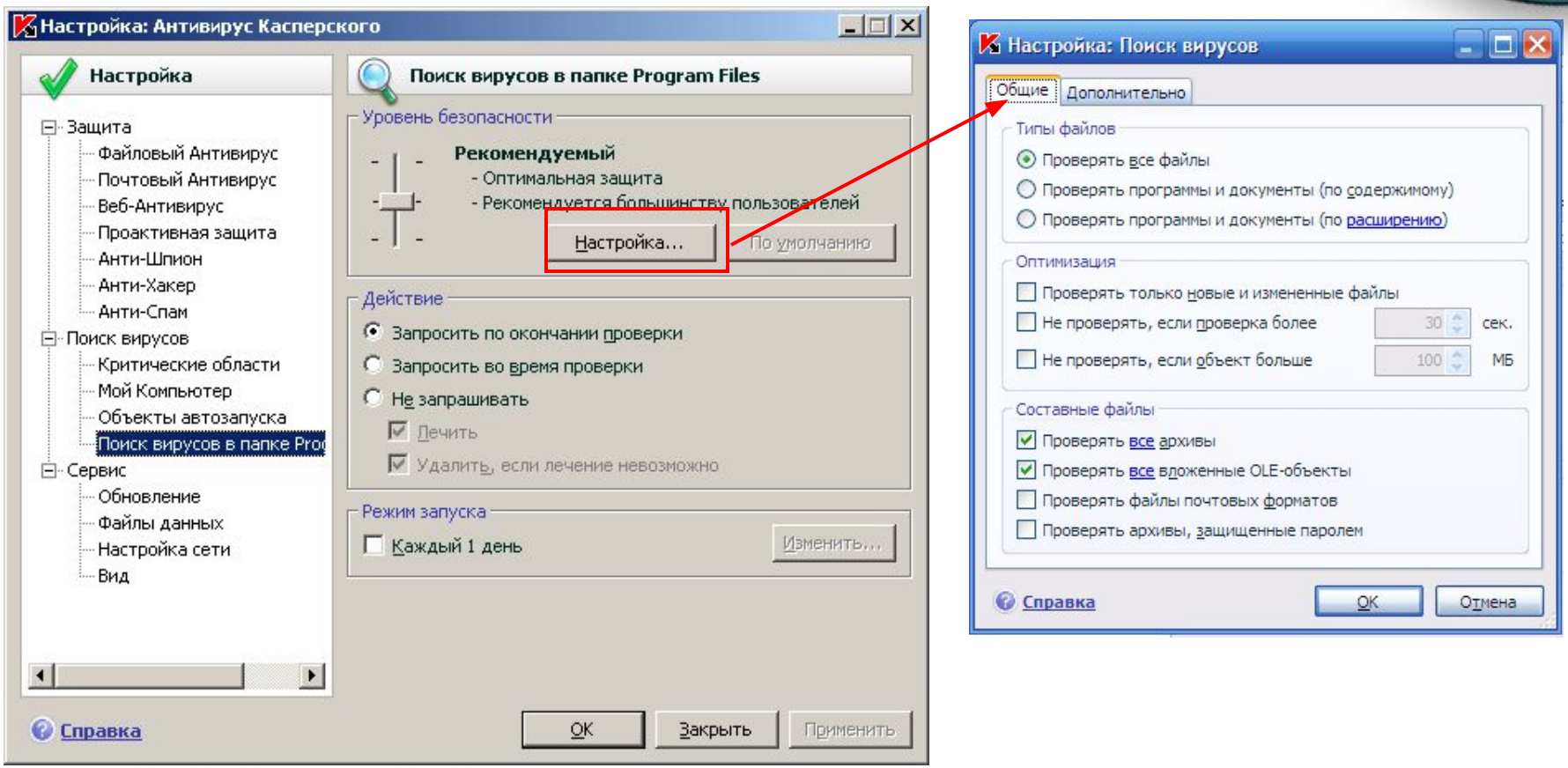
Задачи поиска вредоносных программ

- Системные задачи
  - поиск вирусов
  - проверка критических областей
  - проверка моего компьютера
  - проверка объектов автозапуска
  - проверка карантина
- Пользовательские задачи (до 4-х)

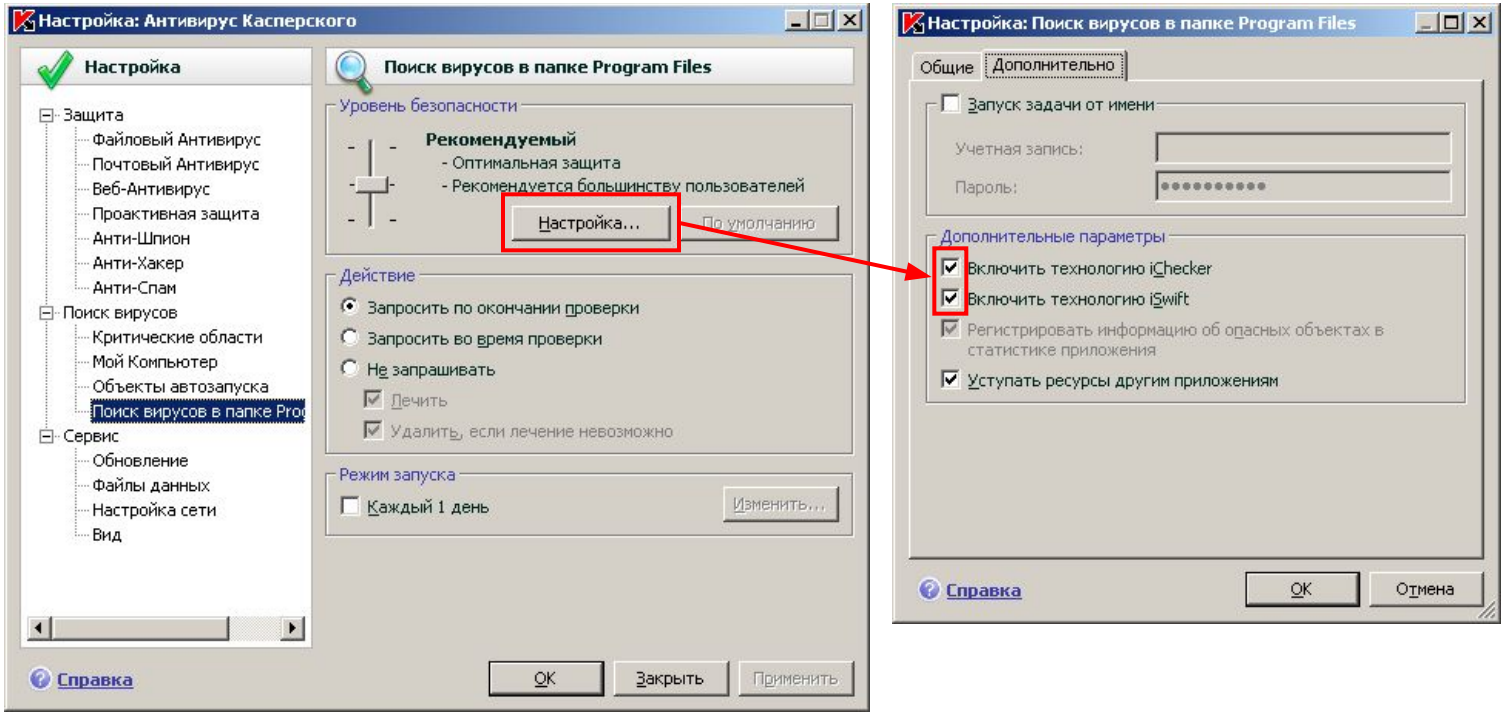
Настройка уровня безопасности



Общие параметры задачи



Дополнительные параметры задачи



Отключение функций автозапуска

Использование параметров групповой политики для отключения всех функций автозапуска в ОС Windows Server 2008 или Windows Vista

1. Нажмите кнопку **Пуск**

, введите **Gpedit.msc** в

При получении запроса
введите пароль или нажмите кн
2. В разделе **Конфигурация ком**
Административные шаблоны
3. В области **Подробности** дважд
4. Щелкните элемент **Включено**,
Отключить автозапуск, чтоб
5. Перезагрузите компьютер.

Перейти к началу страницы

Использование параметров групповой политики для отключения всех функций автозапуска в ОС Windows Server 2003, Windows XP Professional или Windows 2000

1. Выберите в меню **Пуск** пункт **Выполнить**, введите **Gpedit.msc** в поле **Открыть** и нажмите кнопку **ОК**.
2. Последовательно разверните узлы **Конфигурация компьютера**, **Административные шаблоны** и **Система**.
3. В области **Параметры** щелкните правой кнопкой мыши элемент **Отключить автозапуск** и выберите пункт **Свойства**.

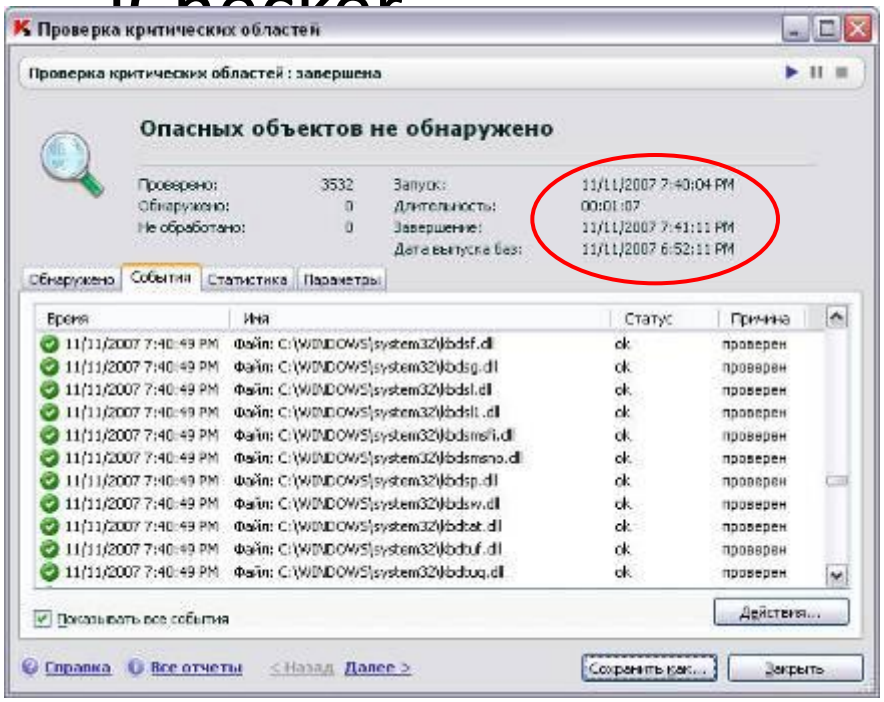
   Примечание. В системе Windows 2000 параметр политики называется **Отключить автозапуск**.
4. Щелкните элемент **Включено**, а затем выберите вариант **Все диски** в окне **Отключить автозапуск**, чтобы отключить автоматический запуск для всех дисков.
5. Нажмите кнопку **ОК**, чтобы закрыть диалоговое окно **Свойства выключения автозапуска**.
6. Перезагрузите компьютер.

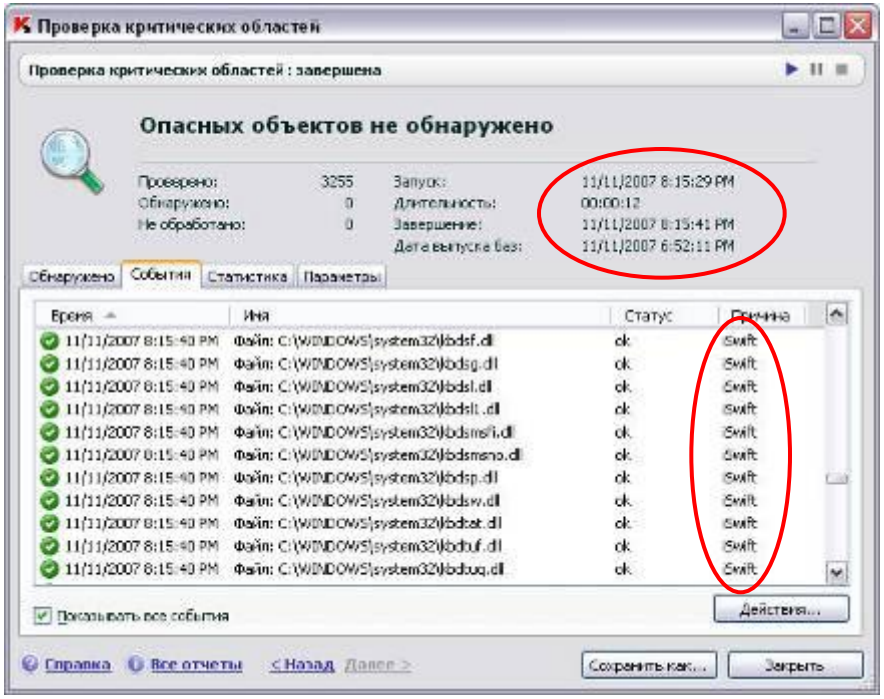
Центр справки и поддержки Microsoft:

http://support.microsoft.com/kb/967715/

Скорость работы

Эффективность технологий iSwift и iChecker

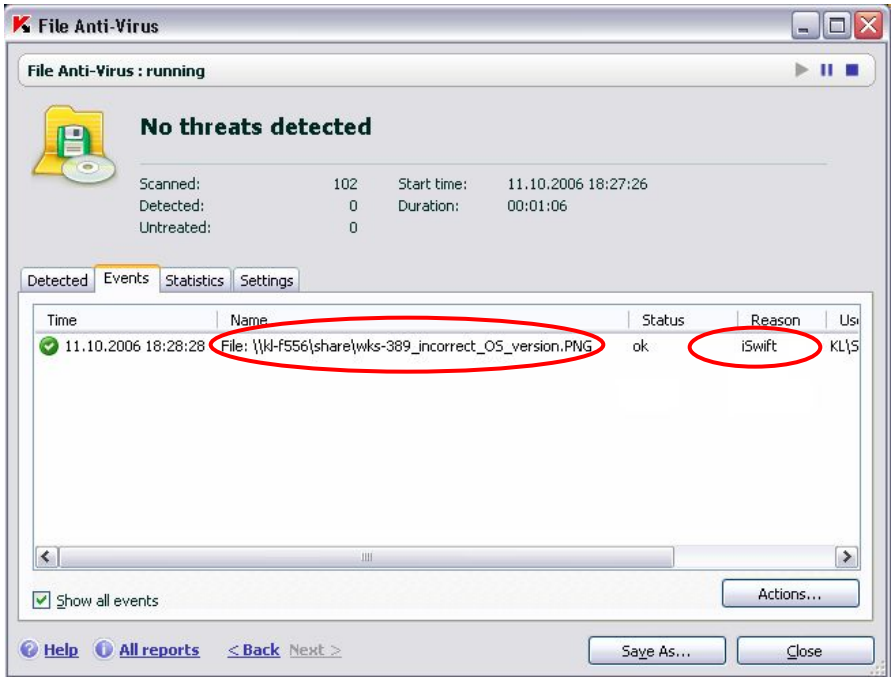


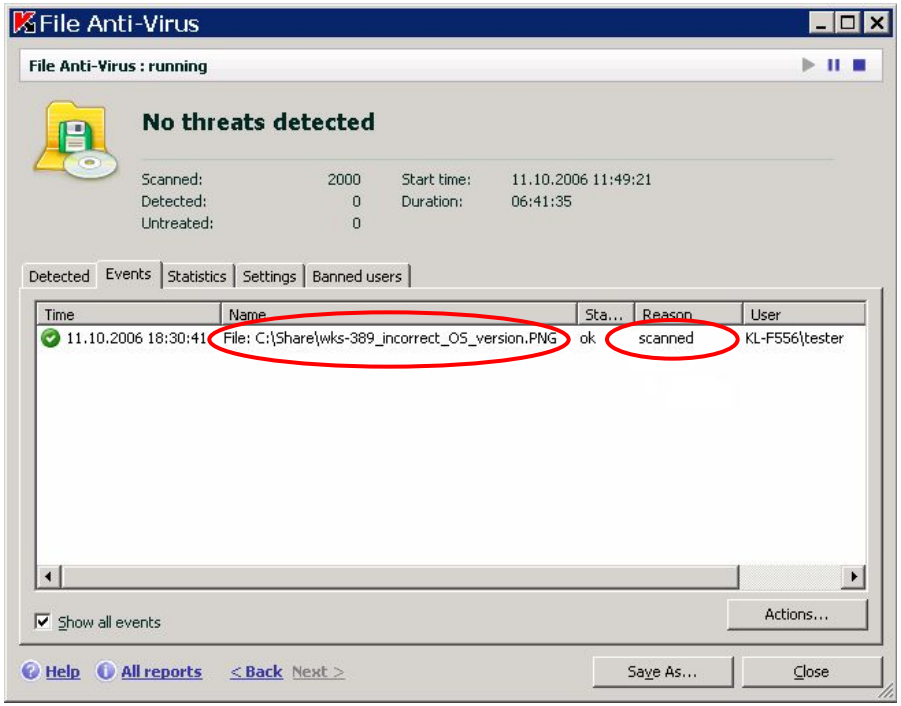


- Существенное ускорение (*12сек* против *1мин 07сек*)

Скорость работы

Сетевой iSwift

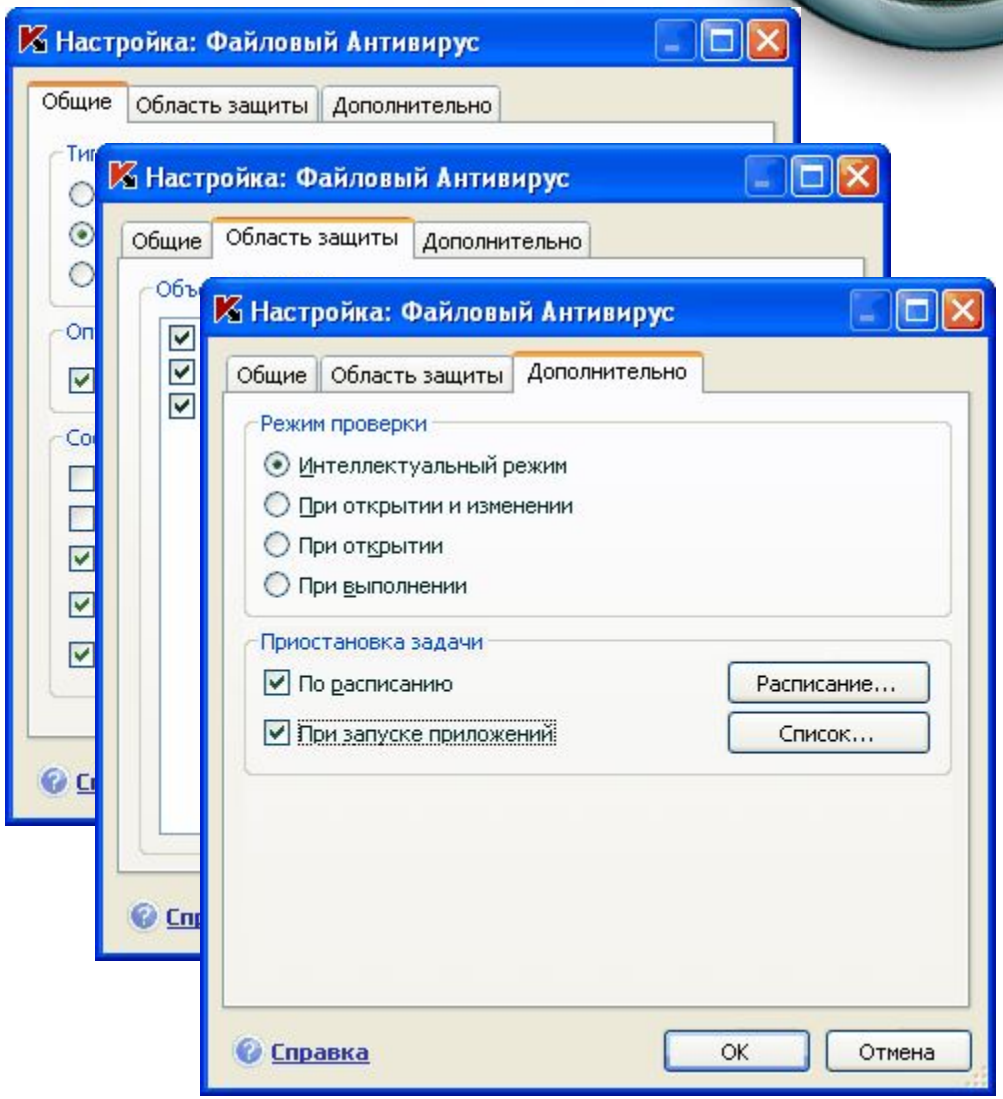




- Разделение iSwift-данных позволяет снизить задержку при передаче файла в 2 раза

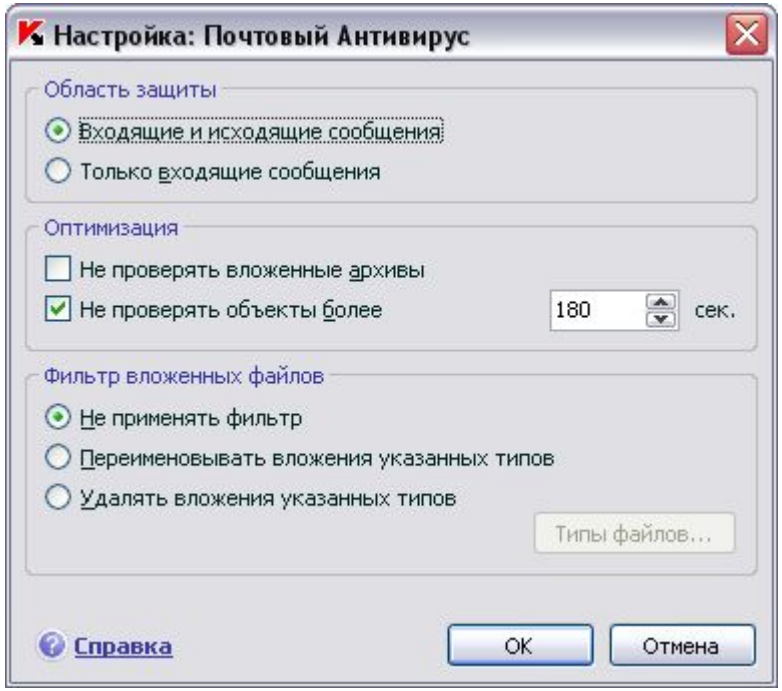
Файловый Антивирус

- Проверка только новых и изменённых файлов (настраиваемая по типам объектов)
- Гибкие возможности антивирусной проверки для составных объектов
- Проверяет файлы на компьютере и на сетевых дисках
- Технология приостановки сканирования при увеличении пользовательской активности



Почтовый Антивирус

- Сканирование SMTP, POP3, IMAP и NNTP трафика (включая SSL)
- Плагины для Microsoft Outlook и TheBat!
- Возможность фильтрации вложений
- Лечение вирусов в почтовых базах Microsoft Outlook, Microsoft Outlook Express
- Технология предотвращение вирусной эпидемии (Anti-Worm)



Веб-Антивирус

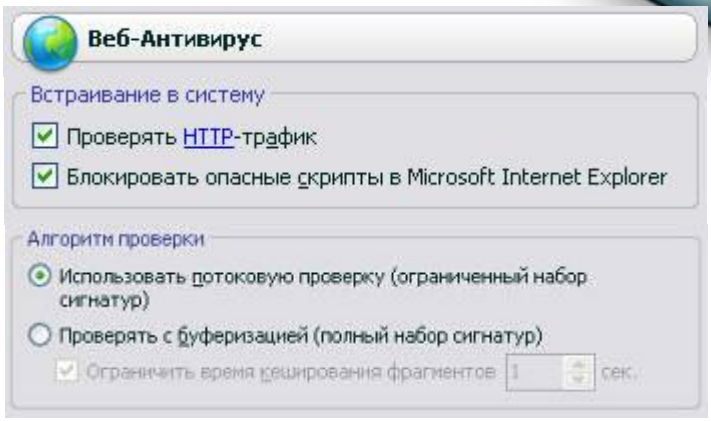
Зачем он нужен?

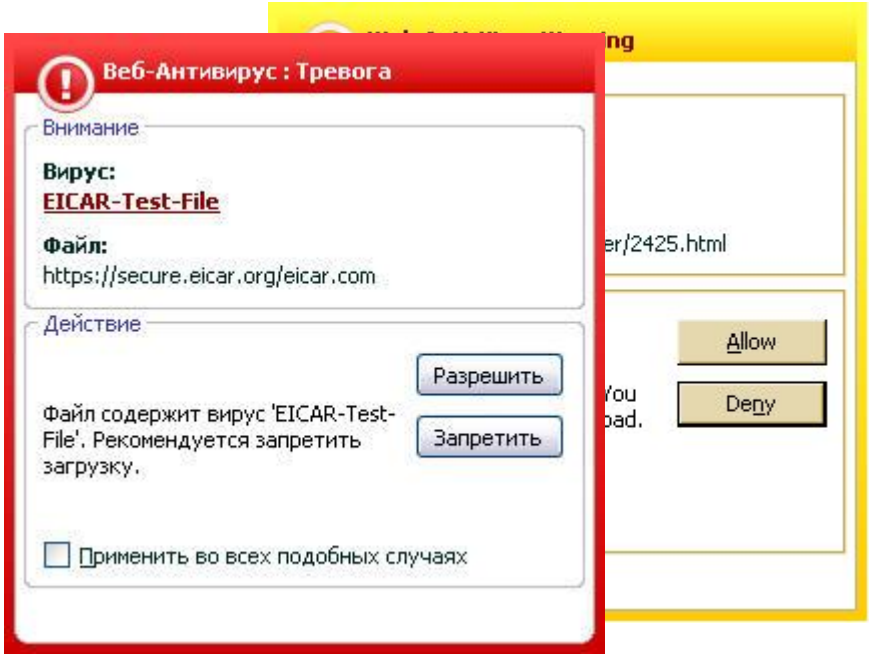
Почему недостаточно Script Checker'а?

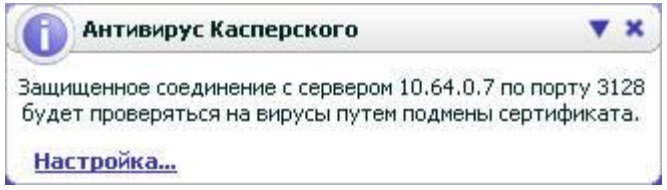
- SC работает только в Internet Explorer
- SC обрабатывает только VB- и Java-скрипты

Технология SafeStream

Проверка защищенных (SSL) соединений







Комплекс проактивных технологий

Проактивно блокирует вредоносные программы классов:

- Trojan.Generic / Trojan.Cryptor
- Worm.Generic / Worm.P2P.Generic
- Скрытые объекты (Rootkits)
- Клавиатурные шпионы (Keyloggers)
- Внедрение в процесс (Invaders)
- Скрытую отправку данных
- Попытку сбора паролей в системе
- Странное поведение приложений

+ Откат вредоносных изменений

Пример работы модуля проактивной защиты

Червь Net-Worm.Win32.Mytob

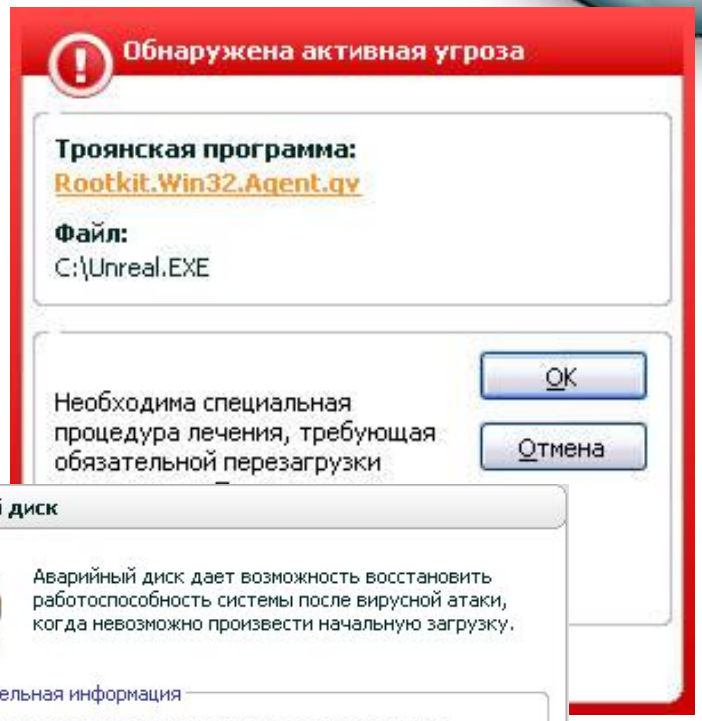
1. Определение

2. Завершение

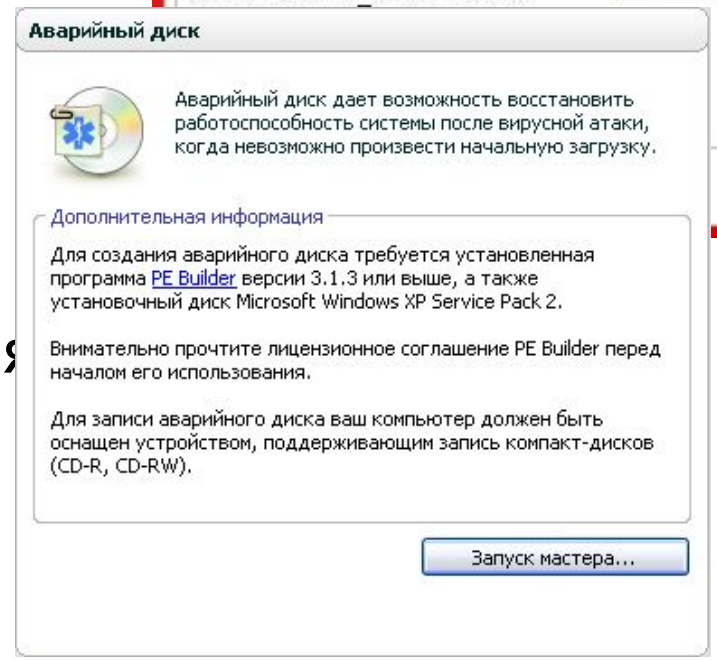
3. Откат изменений

Борьба с активными угрозами

- Лечение активного заражения
  - ✔ Блокировка реестра
  - ✔ Формирование задачи проверки
  - ✔ Попытка завершения процесса и удаление записей о вирусе
  - ✔ Перезагрузка
  - ✔ Удаление исполняемого файла

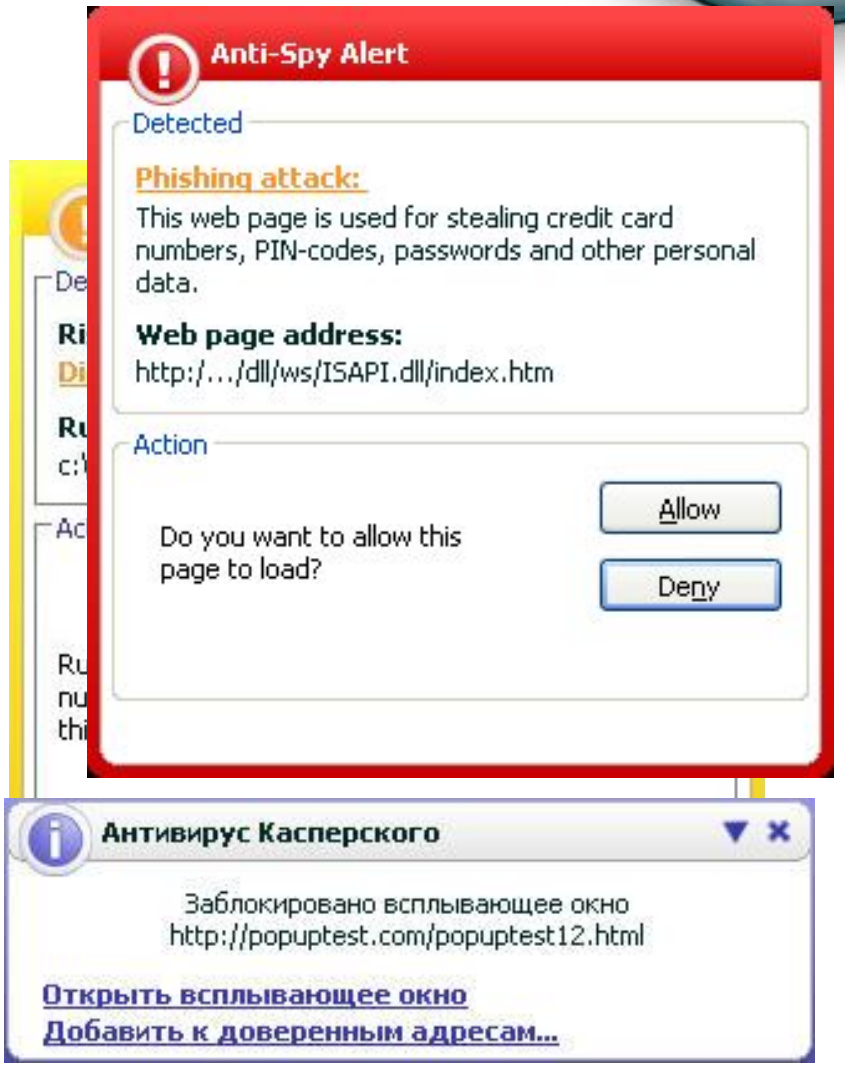


- Мастер создания диска аварийного восстановления



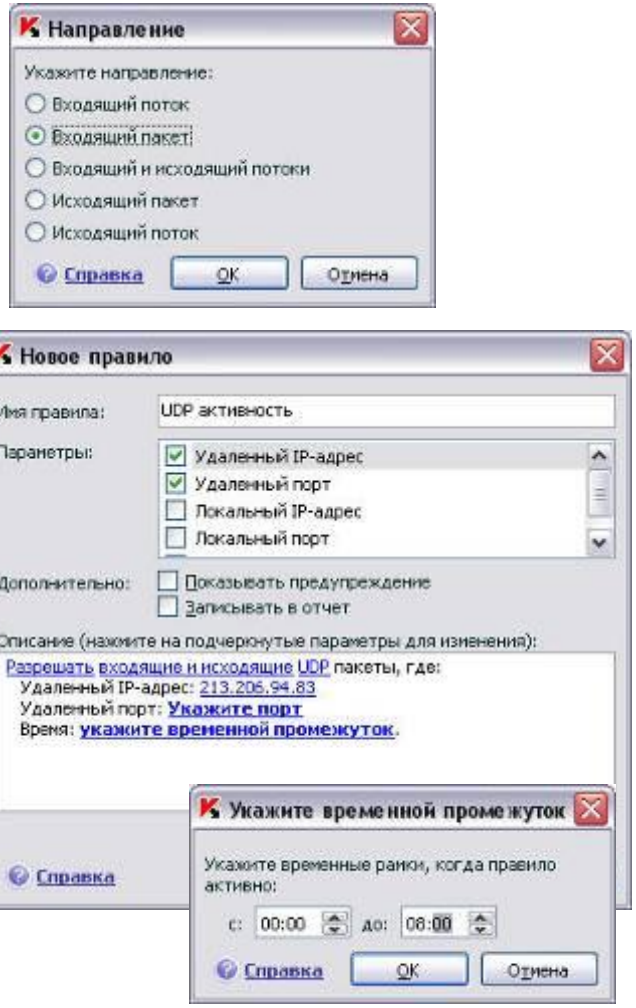
Защита от шпионского ПО и рекламы

- Защита от фишинговых атак
- Блокировка скрытых попыток соединений на платные номера
- Блокировка всплывающих окон и рекламных баннеров

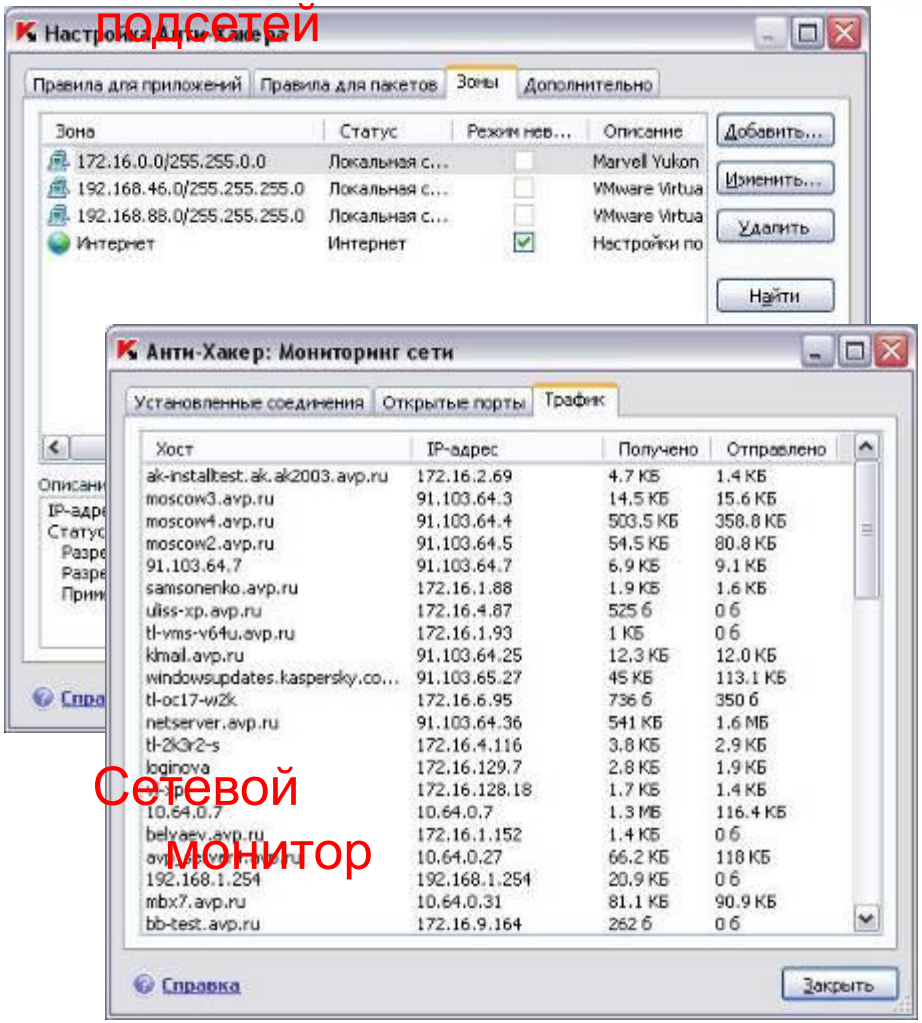


Анти-Хакер: технологии Firewall

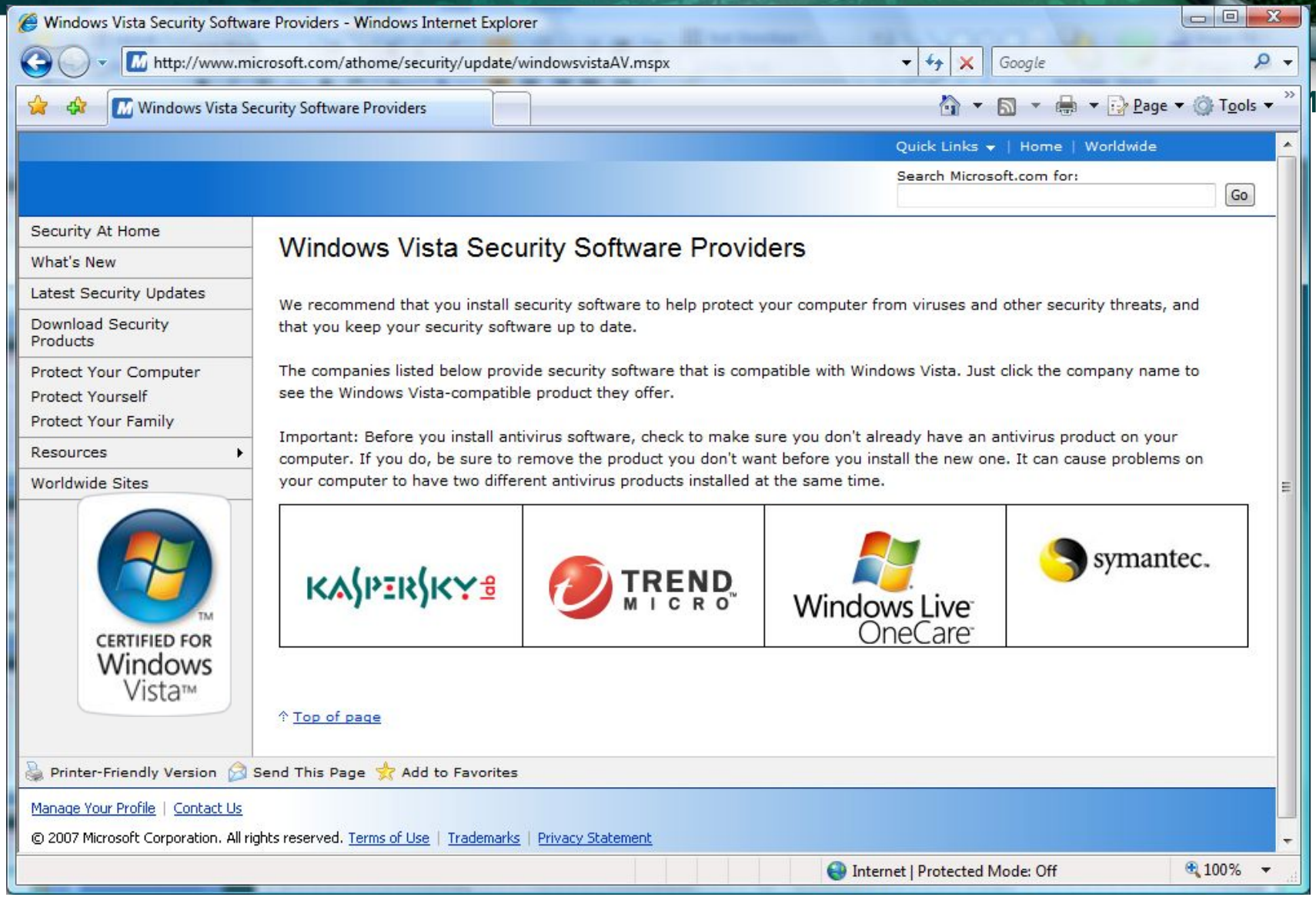
Гибкость создания правил



Настройка уровня доверия подсетей



Сетевой монитор


Windows Vista Security Software Providers - Windows Internet Explorer
http://www.microsoft.com/athome/security/update/windowsvistaAV.mspx
Google
Windows Vista Security Software Providers
Page
Tools
Quick Links | Home | Worldwide
Search Microsoft.com for:
Go
Security At Home
What's New
Latest Security Updates
Download Security Products
Protect Your Computer
Protect Yourself
Protect Your Family
Resources
Worldwide Sites
CERTIFIED FOR Windows Vista™
Windows Vista Security Software Providers
We recommend that you install security software to help protect your computer from viruses and other security threats, and that you keep your security software up to date.
The companies listed below provide security software that is compatible with Windows Vista. Just click the company name to see the Windows Vista-compatible product they offer.
Important: Before you install antivirus software, check to make sure you don't already have an antivirus product on your computer. If you do, be sure to remove the product you don't want before you install the new one. It can cause problems on your computer to have two different antivirus products installed at the same time.
KASPERSKY lab
TREND MICRO
Windows Live OneCare
symantec.
Top of page
Printer-Friendly Version
Send This Page
Add to Favorites
Manage Your Profile | Contact Us
© 2007 Microsoft Corporation. All rights reserved. Terms of Use | Trademarks | Privacy Statement
Internet | Protected Mode: Off
100%

Спасибо за внимание!

Вопросы?