

# Особенности использования Антивируса Касперского для рабочих станций 6.0

Яшутина Ольга

Методист образовательных программ

*[Olga.Yashutina@kaspersky.com](mailto:Olga.Yashutina@kaspersky.com)*

# Антивирус Касперского для Windows Workstations



## **Обеспечивает блокирование вредоносных программ по каналам:**

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

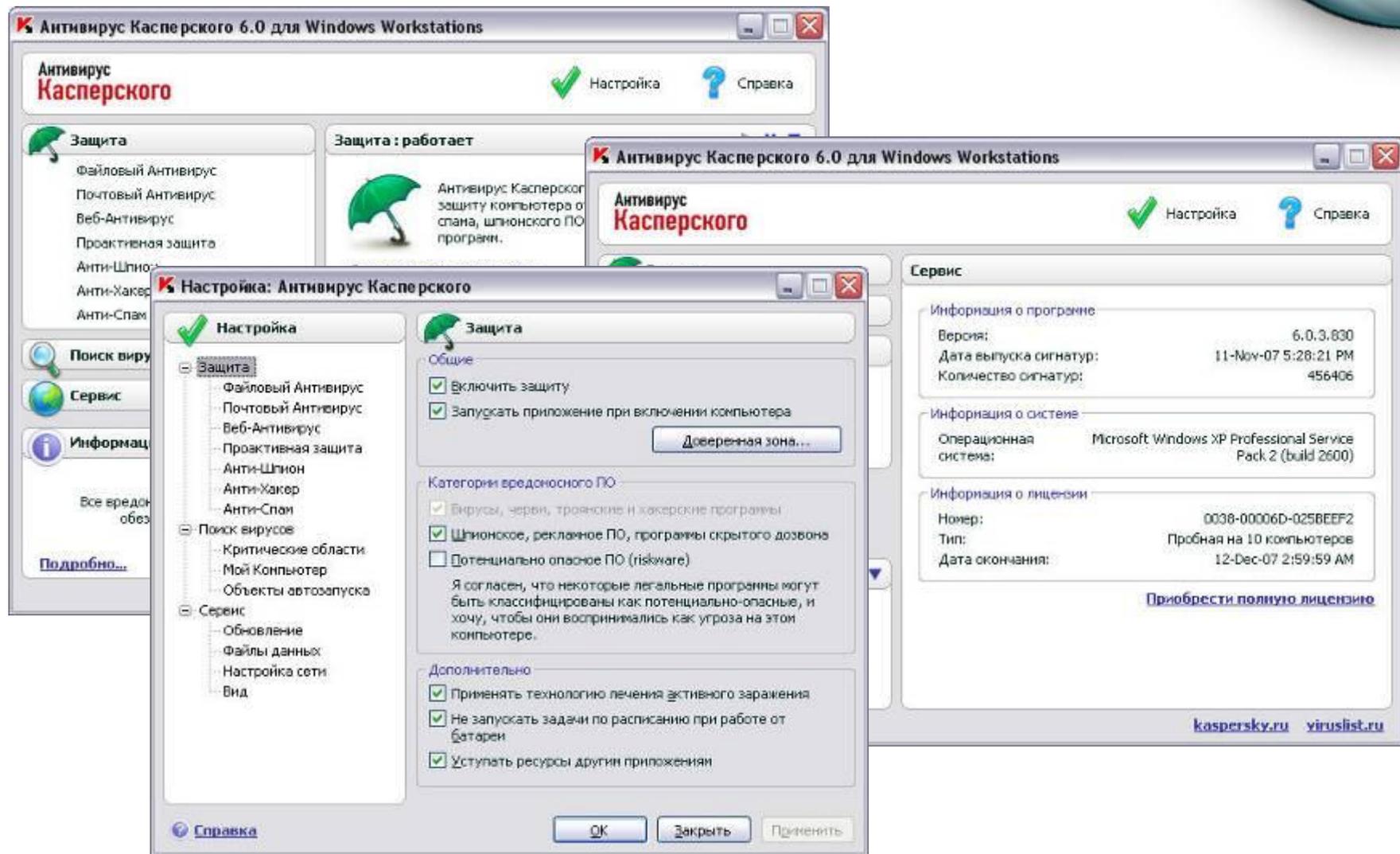
## **Поддерживаемые платформы**

- 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

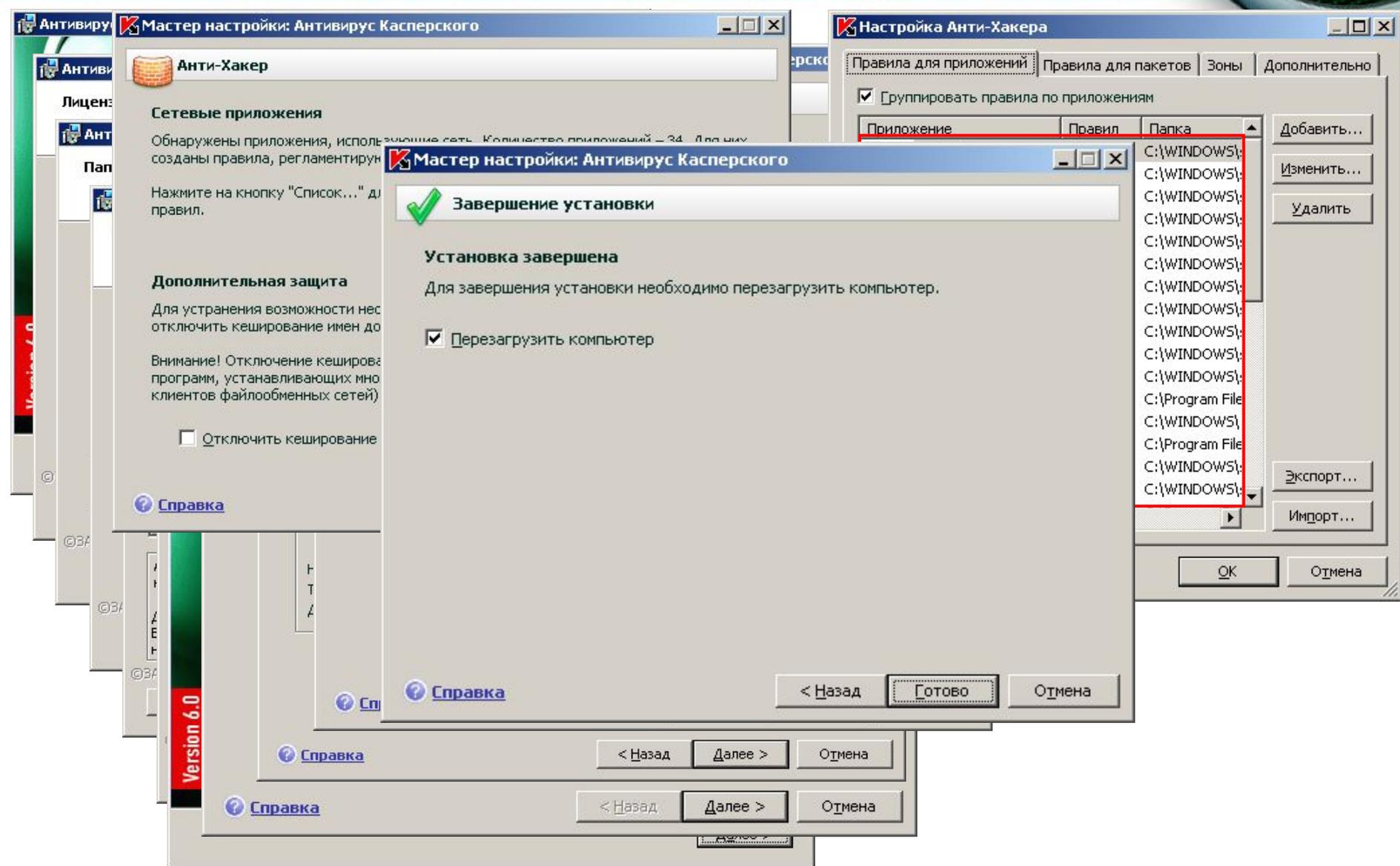
# Управление системой защиты

- 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

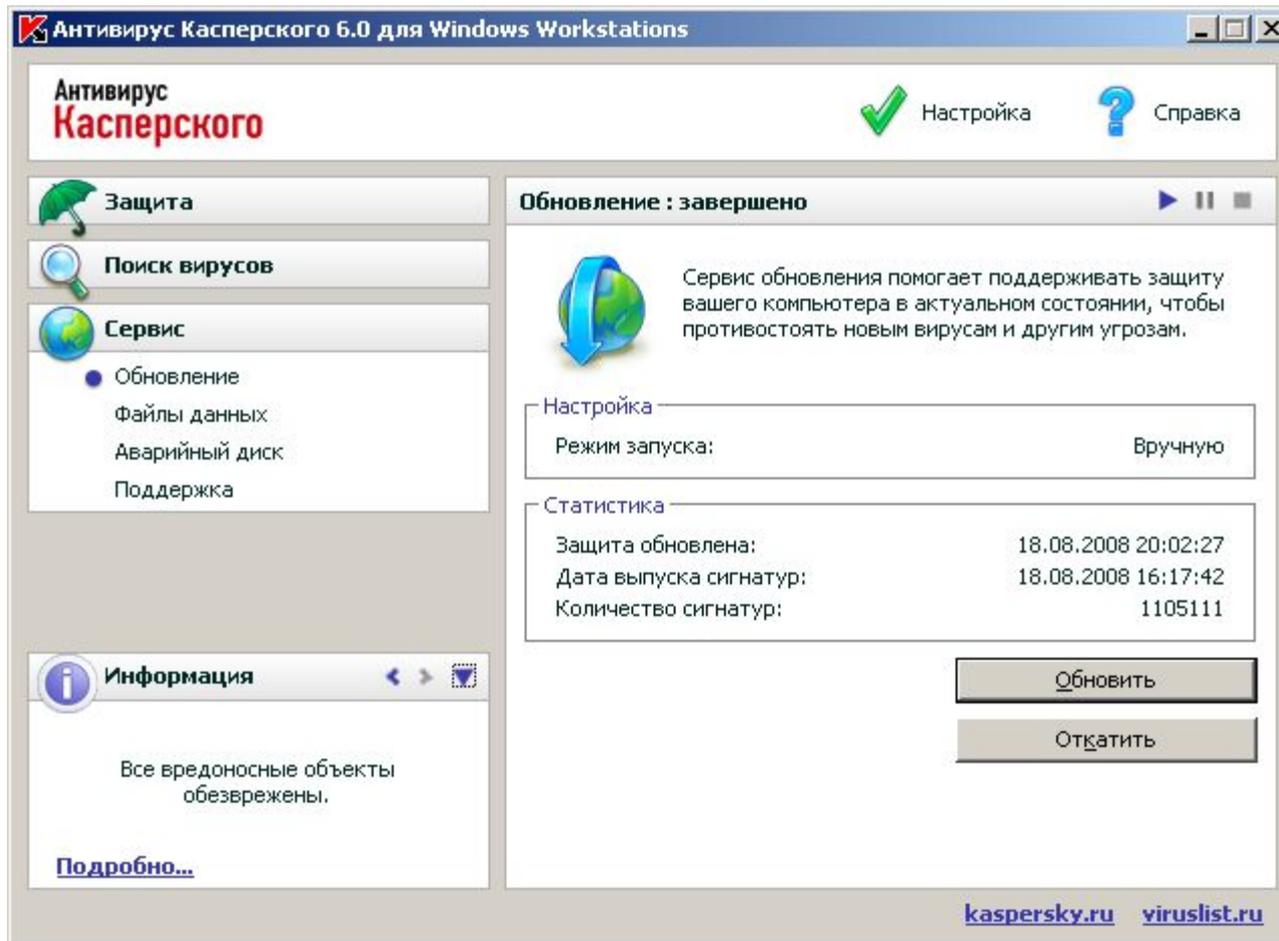
# Процесс установки



# 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



Антивирус Касперского 6.0 для Windows Workstations

Антивирус Касперского

Настройка Справка

**Защита**

Поиск вирусов

Сервис

- Обновление
- Файлы данных
- Аварийный диск
- Поддержка

Информация

Все вредоносные объекты обезврежены.

[Подробнее...](#)

**Обновление : завершено**

Сервис обновления помогает поддерживать защиту вашего компьютера в актуальном состоянии, чтобы противостоять новым вирусам и другим угрозам.

Настройка

Режим запуска: Вручную

Статистика

Защита обновлена:	18.08.2008 20:02:27
Дата выпуска сигнатур:	18.08.2008 16:17:42
Количество сигнатур:	1105111

Обновить

Откатить

[kaspersky.ru](http://kaspersky.ru) [viruslist.ru](http://viruslist.ru)

# 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

The image shows the Kaspersky Anti-Virus 6.0 interface for Windows Workstations. The main window displays the status of the virus protection, with a green checkmark indicating that the update is complete. A context menu is open over the 'Обновление' (Update) option in the left sidebar, with 'Настройка...' (Settings...) highlighted. A red arrow points from this menu item to the 'Настройка: Антивирус Касперского' (Settings: Kaspersky Anti-Virus) window.

The 'Настройка: Антивирус Касперского' window is divided into two main sections: 'Настройка' (Settings) and 'Обновление' (Update). The 'Настройка' section is expanded to show the following categories:

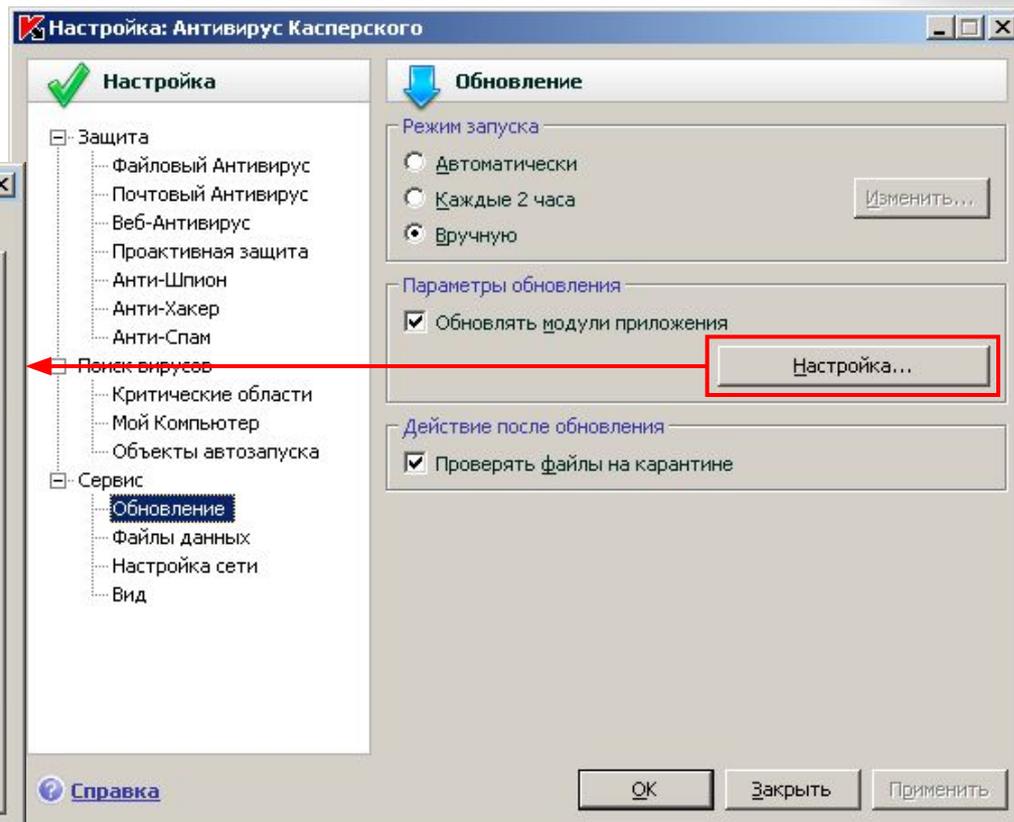
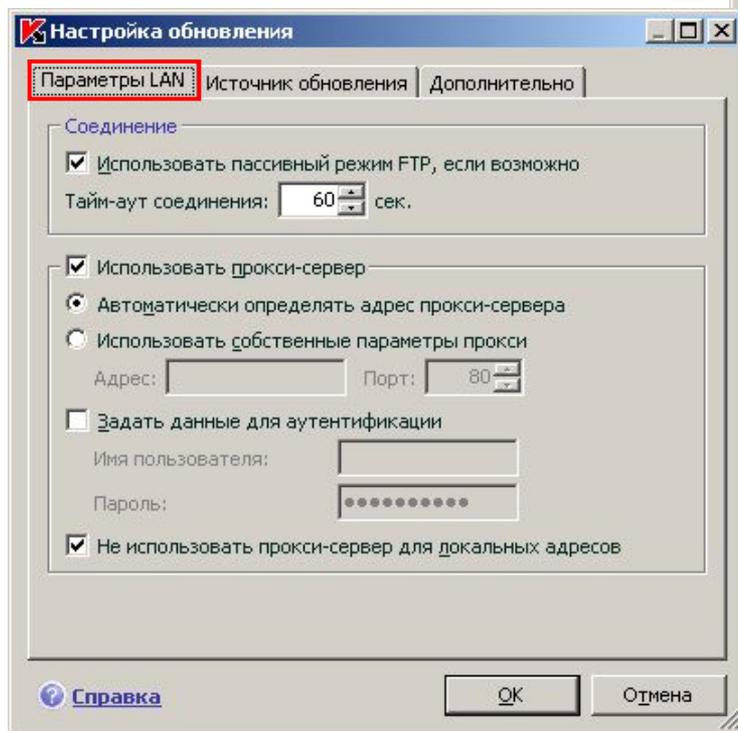
- Защита (Protection)
  - Файловый Антивирус (File Antivirus)
  - Почтовый Антивирус (Mail Antivirus)
  - Веб-Антивирус (Web Antivirus)
  - Проактивная защита (Proactive Protection)
  - Анти-Шпион (Anti-Spyware)
  - Анти-Хакер (Anti-Hacker)
  - Анти-Спам (Anti-Spam)
- Поиск вирусов (Virus Scanning)
  - Критические области (Critical Areas)
  - Мой Компьютер (My Computer)
  - Объекты автозапуска (Startup Objects)
- Сервис (Service)
  - Обновление (Update)
  - Файлы данных (Data Files)
  - Настройка сети (Network Settings)
  - Вид (View)

The 'Обновление' section contains the following settings:

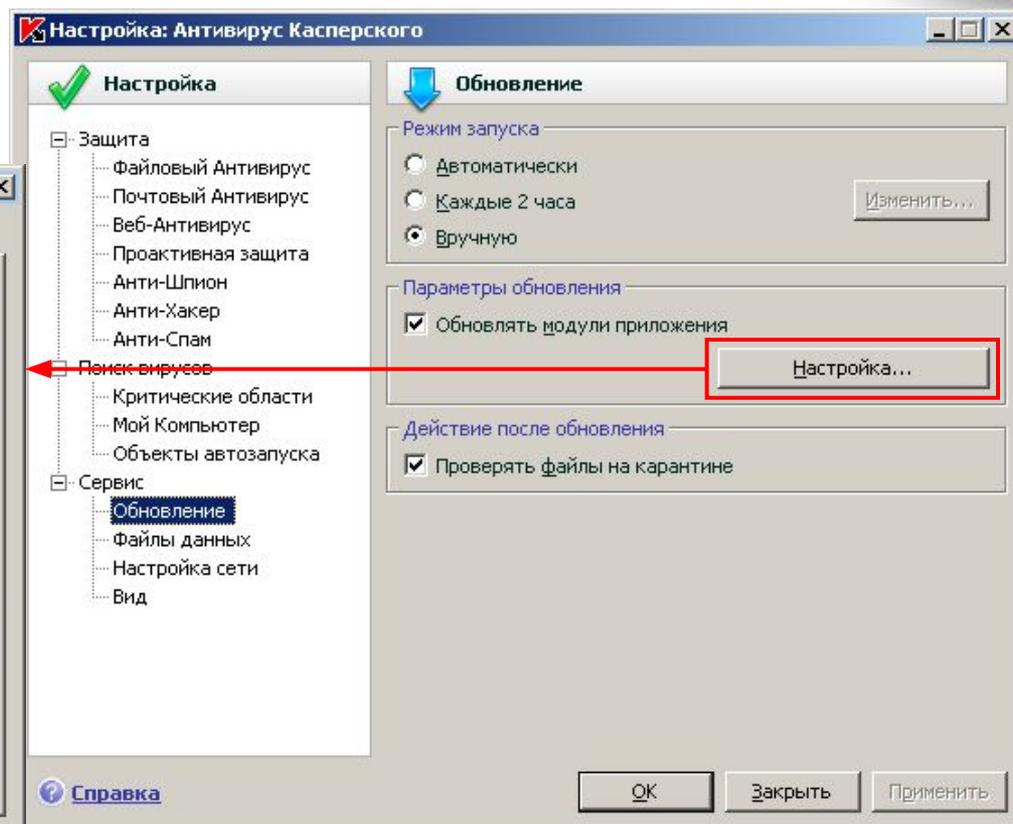
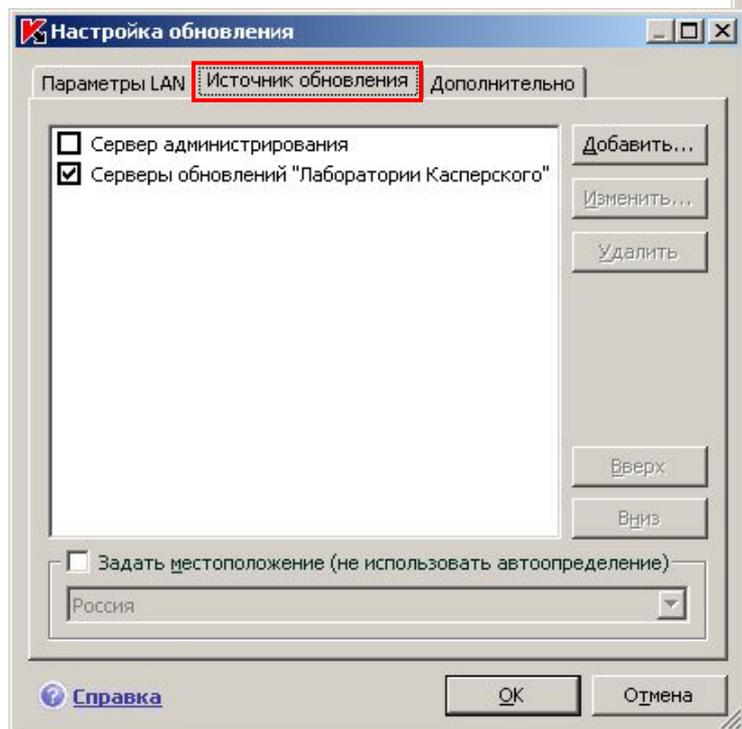
- Режим запуска (Startup Mode):
  - Автоматически (Automatic)
  - Каждые 2 часа (Every 2 hours)
  - Вручную (Manual)
- Параметры обновления (Update Parameters):
  - Обновлять модули приложения (Update application modules)
- Действие после обновления (Action after update):
  - Проверять файлы на карантине (Check files on quarantine)

Buttons at the bottom of the window include 'Справка' (Help), 'ОК', 'Закреть' (Close), and 'Применить' (Apply).

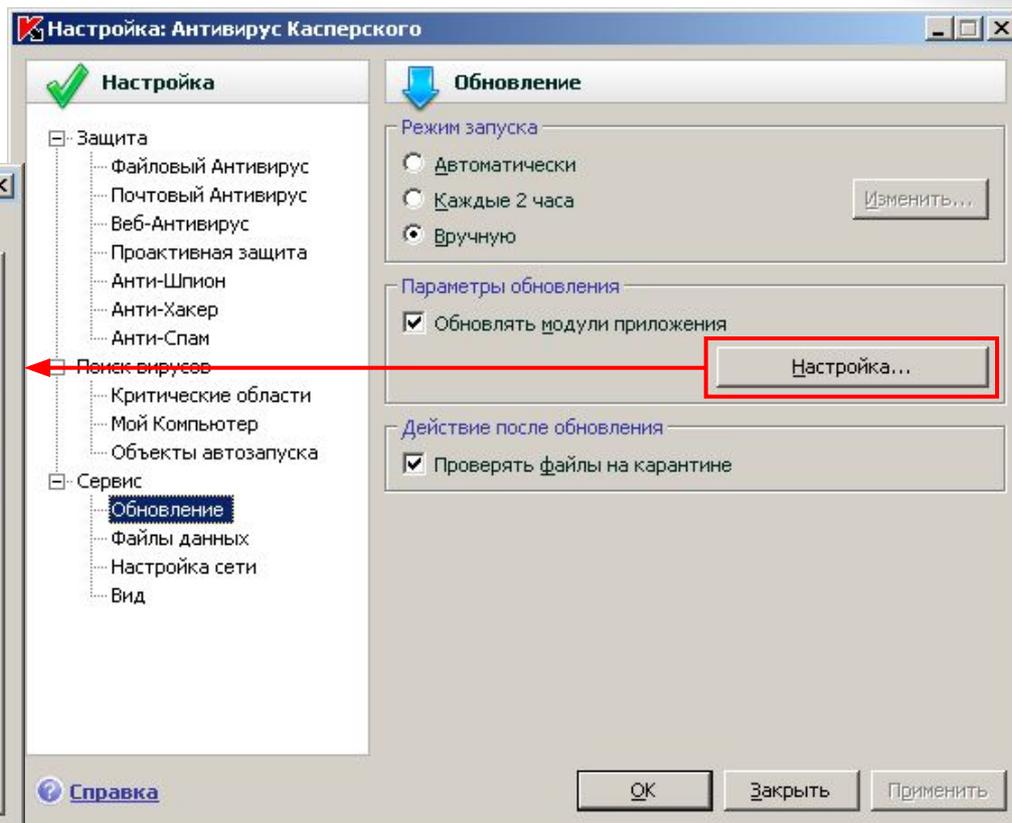
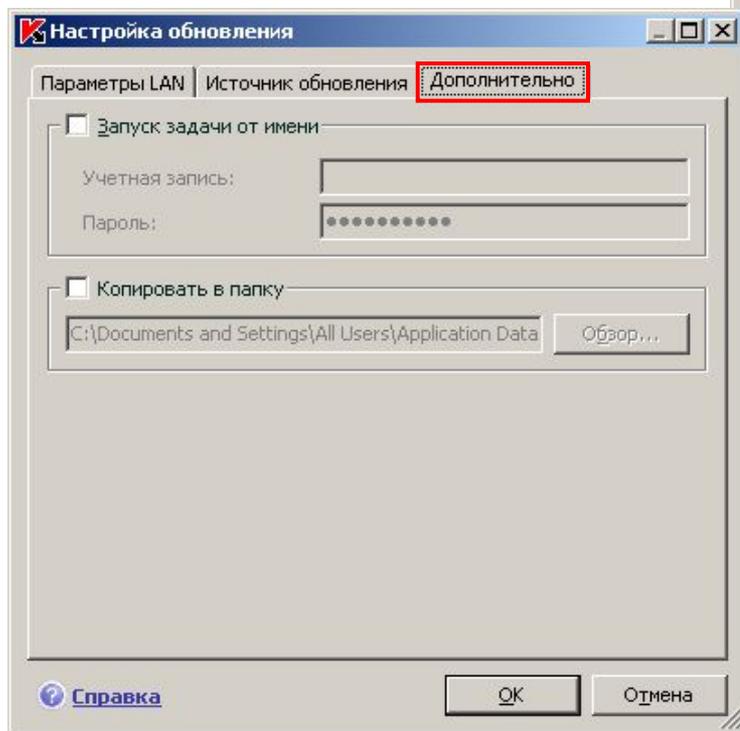
# Параметры LAN



# 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

The image shows the Kaspersky Anti-Virus 6.0 interface for Windows Workstations. The main window is titled "Антивирус Касперского 6.0 для Windows Workstations". It features a sidebar with navigation options: "Защита" (Protection), "Поиск вирусов" (Virus Scan), "Сервис" (Service), and "Информация" (Information). The "Защита" section is active, showing a status of "Защита : работает" (Protection : working) with a green umbrella icon. A red box highlights the "Настройка..." (Settings...) option in the sidebar, with a red arrow pointing to the "Настройка: Антивирус Касперского" (Settings: Kaspersky Anti-Virus) window.

The "Настройка: Антивирус Касперского" window is open, showing the "Настройка" (Settings) tab. The "Защита" (Protection) section is expanded, showing a tree view of protection components:

- Защита
  - Файловый Антивирус
  - Почтовый Антивирус
  - Веб-Антивирус
  - Проактивная защита
  - Анти-Шпион
  - Анти-Хакер
  - Анти-Спам
- Поиск вирусов
  - Критические области
  - Мой Компьютер
  - Объекты автозапуска
- Сервис
  - Обновление
  - Файлы данных
  - Настройка сети
  - Вид

The "Общие" (General) section of the settings window is visible, showing the following options:

- Включить защиту (Enable protection)
- Запускать приложение при включении компьютера (Run application when the computer is turned on)

Below these options is a button labeled "Доверенная зона..." (Trusted zone...). The "Категории вредоносного ПО" (Malware categories) section shows:

- Вирусы, черви, троянские и хакерские программы (Viruses, worms, trojans and hacker programs)
- Шпионское, рекламное ПО, программы скрытого дозвона (Spyware, adware, dialers)
- Потенциально опасное ПО (riskware) (Potentially unwanted software)

A disclaimer text reads: "Я согласен, что некоторые легальные программы могут быть классифицированы как потенциально-опасные, и хочу, чтобы они воспринимались как угроза на этом компьютере." (I agree that some legal programs may be classified as potentially dangerous, and I want them to be perceived as a threat on this computer.)

The "Дополнительно" (Advanced) section shows:

- Применять технологию лечения активного заражения (Apply active infection treatment technology)
- Не запускать задачи по расписанию при работе от батареи (Do not run scheduled tasks when running on battery)
- Уступать ресурсы другим приложениям (Yield resources to other applications)

At the bottom of the settings window are buttons for "Справка" (Help), "ОК", "Закрыть" (Close), and "Применить" (Apply).

# 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

The image shows the Kaspersky Anti-Virus 6.0 interface for Windows Workstations. The main window is titled "Настройка: Антивирус Касперского" (Settings: Kaspersky Anti-Virus). A context menu is open over the "Поиск вирусов" (Scan) button, with "Настройка..." (Settings...) highlighted in red. A red arrow points from this menu item to the "Настройка" (Settings) tab in the main window.

The "Настройка" tab is active, showing a tree view of settings categories: "Защита" (Protection), "Поиск вирусов" (Scan), and "Сервис" (Service). The "Поиск вирусов" category is selected and expanded, showing sub-items like "Критические области" (Critical areas), "Мой компьютер" (My computer), and "Объекты автозапуска" (Autostart objects).

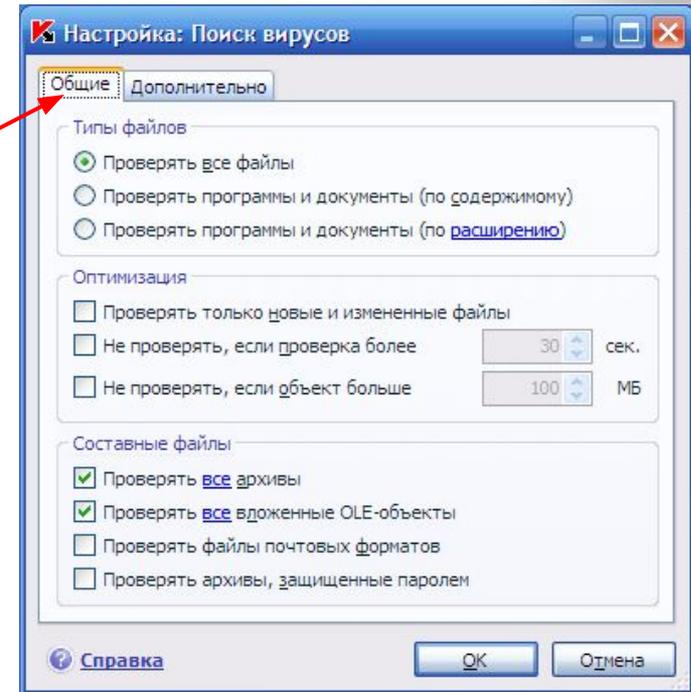
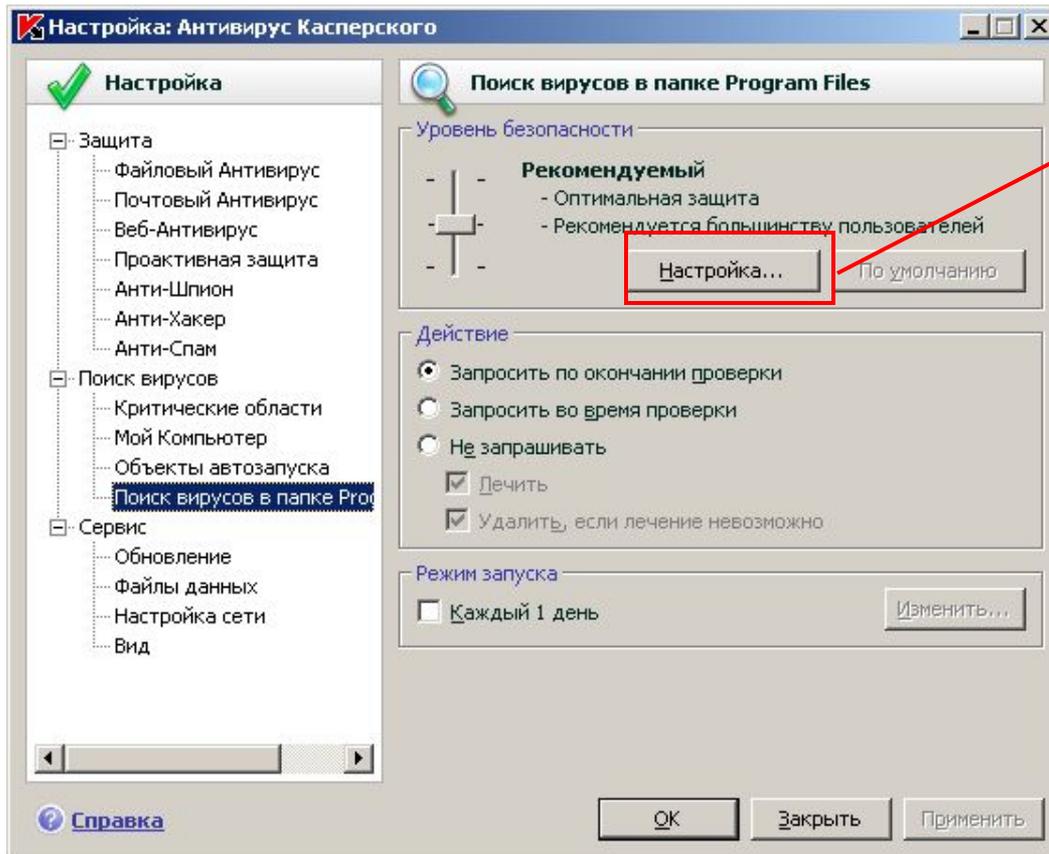
The "Уровень безопасности" (Security level) section is highlighted with a red box. It features a slider set to "Рекомендуемый" (Recommended), which is described as "Оптимальная защита" (Optimal protection) and "Рекомендуется большинству пользователей" (Recommended for most users). Below the slider are buttons for "Настройка..." (Settings...) and "По умолчанию" (Default).

The "Действие" (Action) section has three radio buttons: "Запросить по окончании проверки" (Request after scan) is selected, "Запросить во время проверки" (Request during scan), and "Не запрашивать" (Do not request). There are also checkboxes for "Лечить" (Treat) and "Удалить, если лечение невозможно" (Delete if treatment is impossible).

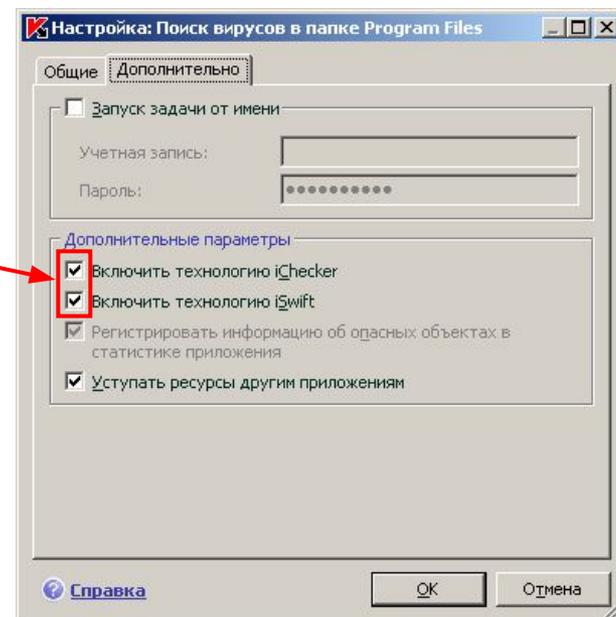
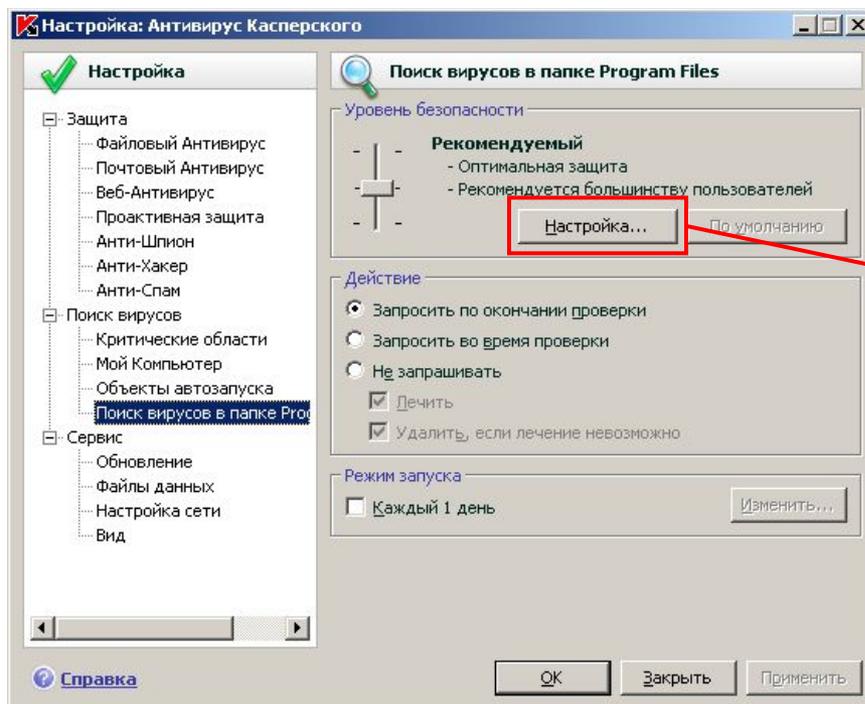
The "Параметры других задач" (Parameters of other tasks) section includes a "Применить" (Apply) button for applying settings to all scan tasks.

At the bottom of the window, there are buttons for "Справка" (Help), "OK", "Закреть" (Close), and "Применить" (Apply).

# 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 поле **Выполнить**



При получении запроса на ввод пароля

2. В разделе **Конфигурация компьютера** выберите **Административные шаблоны**
3. В области **Подробности** дважды щелкните элемент **Включено, Отключить автозапуск**, чтобы отключить автозапуск
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

Проверка критических областей : завершена

Опасных объектов не обнаружено

Проверено: 3532    Запуск: 11/11/2007 7:40:04 PM  
Обнаружено: 0    Длительность: 00:01:07  
Не обработано: 0    Завершение: 11/11/2007 7:41:11 PM  
Дата выпуска бес: 11/11/2007 6:52:11 PM

Время	Имя	Статус	Причина
11/11/2007 7:40:49 PM	Файл: C:\WINDOWS\system32\bdsf.dll	ok	проверен
11/11/2007 7:40:49 PM	Файл: C:\WINDOWS\system32\bdsq.dll	ok	проверен
11/11/2007 7:40:49 PM	Файл: C:\WINDOWS\system32\bdsi.dll	ok	проверен
11/11/2007 7:40:49 PM	Файл: C:\WINDOWS\system32\bdsi_.dll	ok	проверен
11/11/2007 7:40:49 PM	Файл: C:\WINDOWS\system32\bdsmsi.dll	ok	проверен
11/11/2007 7:40:49 PM	Файл: C:\WINDOWS\system32\bdsmsno.dll	ok	проверен
11/11/2007 7:40:49 PM	Файл: C:\WINDOWS\system32\bdspp.dll	ok	проверен
11/11/2007 7:40:49 PM	Файл: C:\WINDOWS\system32\bdsrv.dll	ok	проверен
11/11/2007 7:40:49 PM	Файл: C:\WINDOWS\system32\bdsst.dll	ok	проверен
11/11/2007 7:40:49 PM	Файл: C:\WINDOWS\system32\bdsuf.dll	ok	проверен
11/11/2007 7:40:49 PM	Файл: C:\WINDOWS\system32\bdsuq.dll	ok	проверен

Проверка критических областей : завершена

Опасных объектов не обнаружено

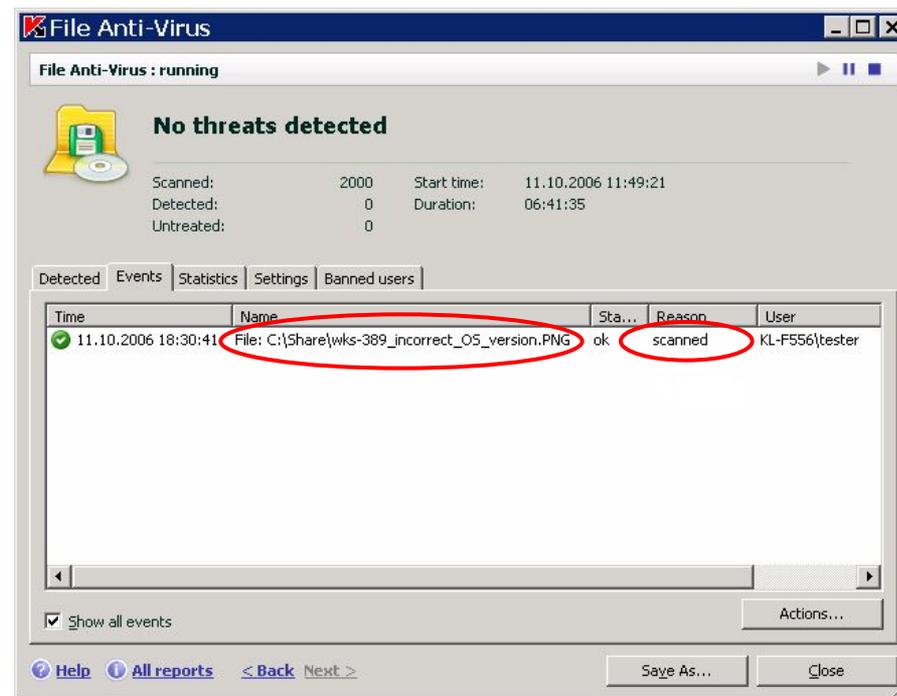
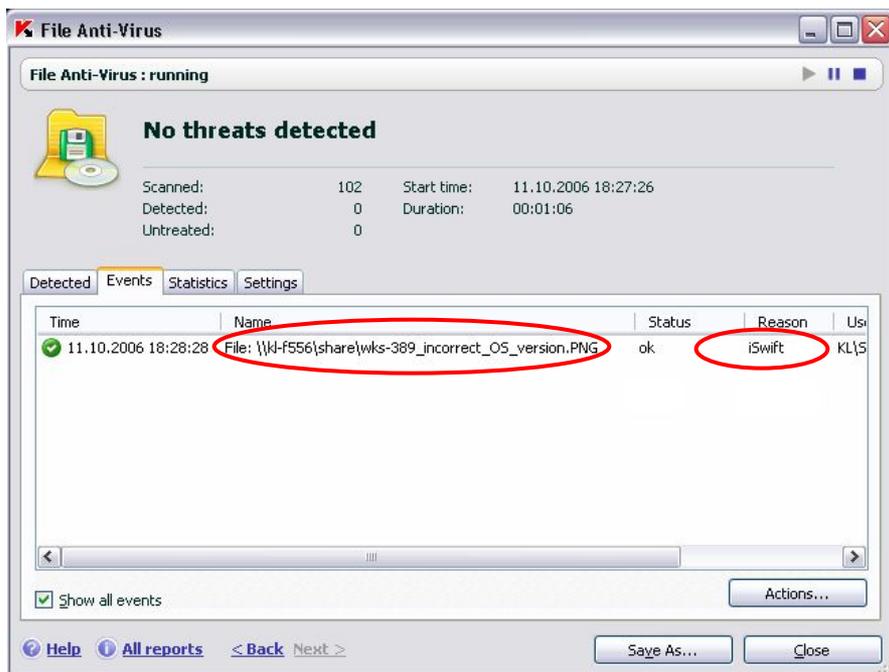
Проверено: 3255    Запуск: 11/11/2007 8:15:29 PM  
Обнаружено: 0    Длительность: 00:00:12  
Не обработано: 0    Завершение: 11/11/2007 8:15:41 PM  
Дата выпуска бес: 11/11/2007 6:52:11 PM

Время	Имя	Статус	Причина
11/11/2007 8:15:40 PM	Файл: C:\WINDOWS\system32\bdsf.dll	ok	iSwift
11/11/2007 8:15:40 PM	Файл: C:\WINDOWS\system32\bdsq.dll	ok	iSwift
11/11/2007 8:15:40 PM	Файл: C:\WINDOWS\system32\bdsi.dll	ok	iSwift
11/11/2007 8:15:40 PM	Файл: C:\WINDOWS\system32\bdsi_.dll	ok	iSwift
11/11/2007 8:15:40 PM	Файл: C:\WINDOWS\system32\bdsmsi.dll	ok	iSwift
11/11/2007 8:15:40 PM	Файл: C:\WINDOWS\system32\bdsmsno.dll	ok	iSwift
11/11/2007 8:15:40 PM	Файл: C:\WINDOWS\system32\bdspp.dll	ok	iSwift
11/11/2007 8:15:40 PM	Файл: C:\WINDOWS\system32\bdsrv.dll	ok	iSwift
11/11/2007 8:15:40 PM	Файл: C:\WINDOWS\system32\bdsst.dll	ok	iSwift
11/11/2007 8:15:40 PM	Файл: C:\WINDOWS\system32\bdsuf.dll	ok	iSwift
11/11/2007 8:15:40 PM	Файл: C:\WINDOWS\system32\bdsuq.dll	ok	iSwift

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

# Скорость работы

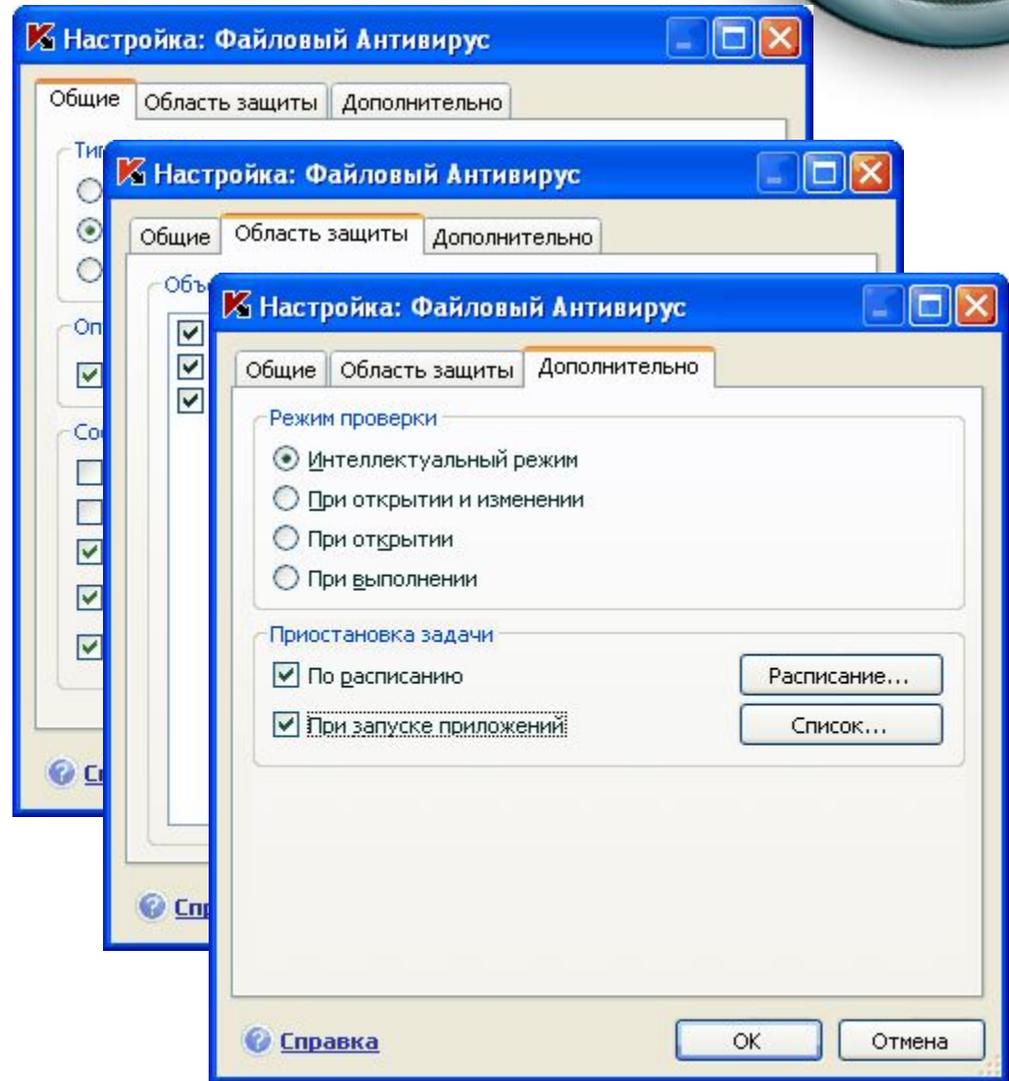
## Сетевой iSwift



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

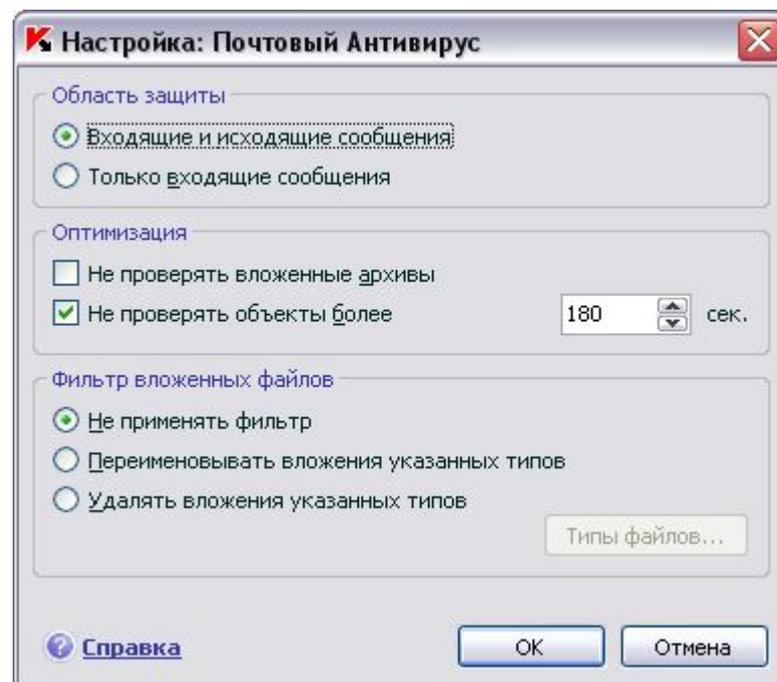
# Файловый Антивирус

- 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 предотвращения вирусной эпидемии (**Anti-Worm**)



# Веб-Антивирус

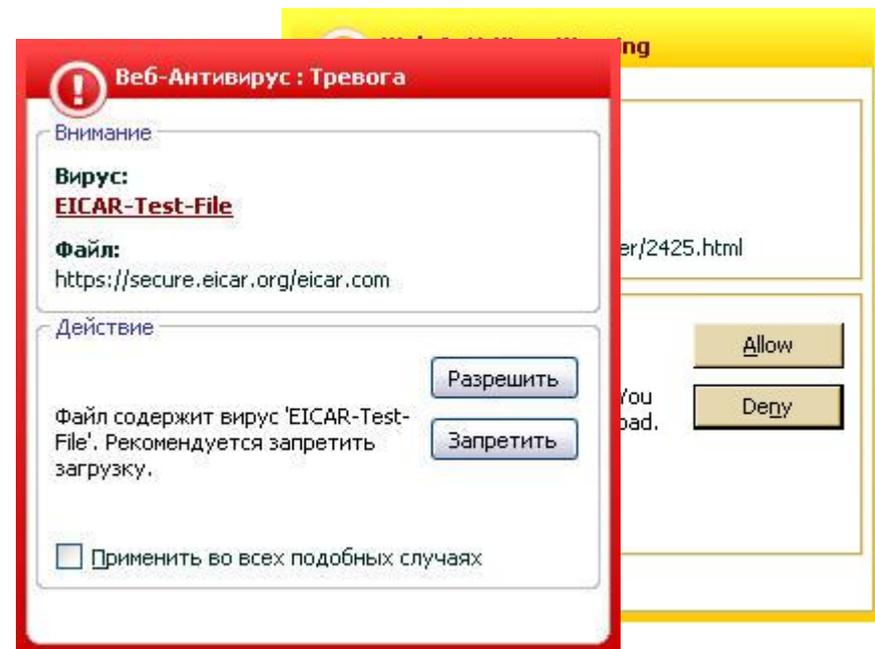
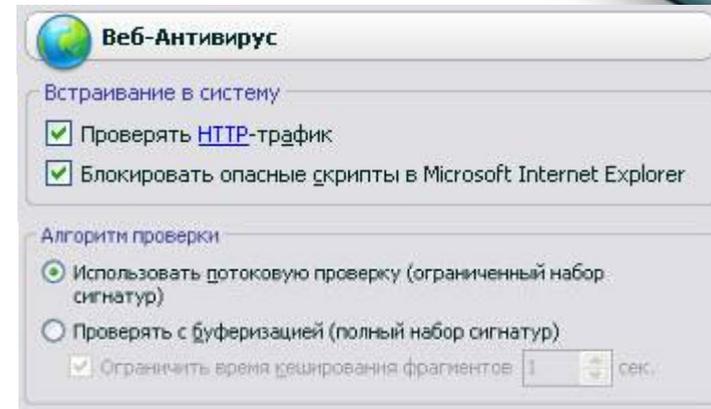
## Зачем он нужен?

### Почему недостаточно Script Checker'a?

- 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



**Proactive Defense Alert**

Detected

**Riskware:**  
**Worm.P2P.generic**

**Running process (PID: 328):**  
C:\WINNT\system32\rnathchk.exe

Action

Quarantine

Process seems to be a P2P worm. Terminate

Skip

Apply to all such cases

[Add to trusted zone...](#)

### 2. Завершение



**Proactive Defense Alert**

Detected

**Riskware:**  
**Worm.P2P.generic**

**Running process (PID: 328):**  
C:\WINNT\system32\rnathchk.exe

Action

Rollback

Process terminated by user. It is recommended to rollback the changes made to the system. Skip

[View history...](#)

[Add to trusted zone...](#)

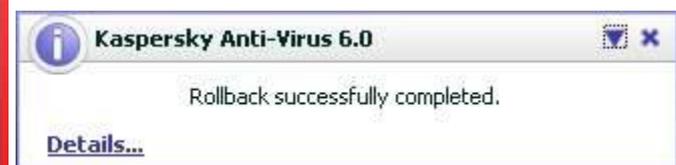
### 3. Откат изменений



**Process changes history**

Type	Object name
CreateFile	C:\my_picture.scr
CreateFile	C:\see_this!.pif
CreateFile	C:\pic.scr

Save Close



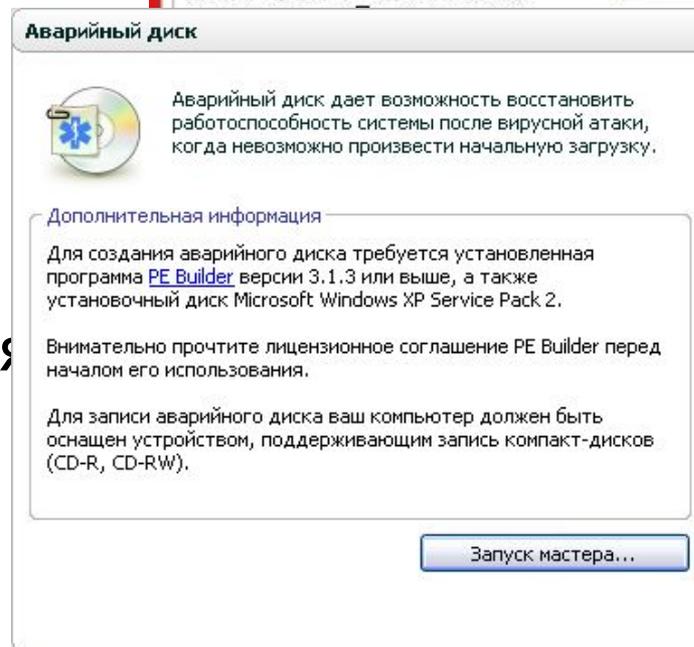
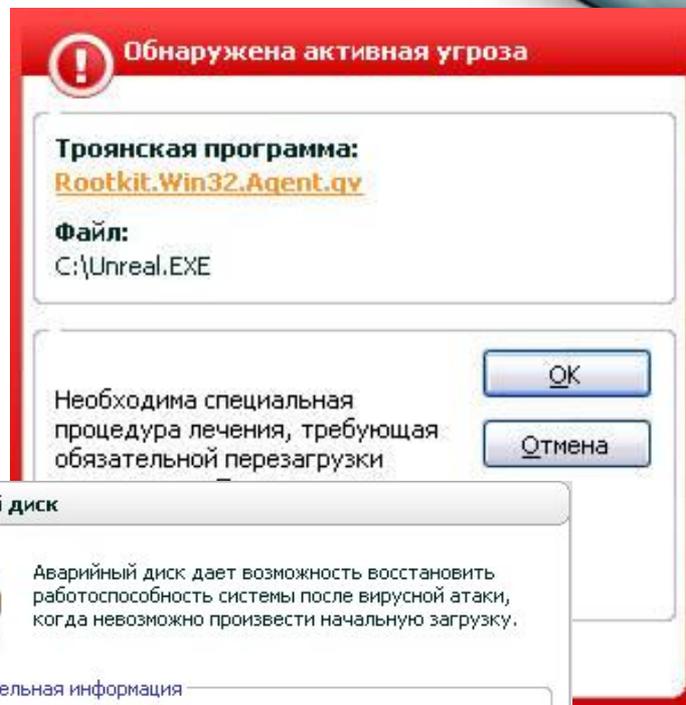
**Kaspersky Anti-Virus 6.0**

Rollback successfully completed.

[Details...](#)

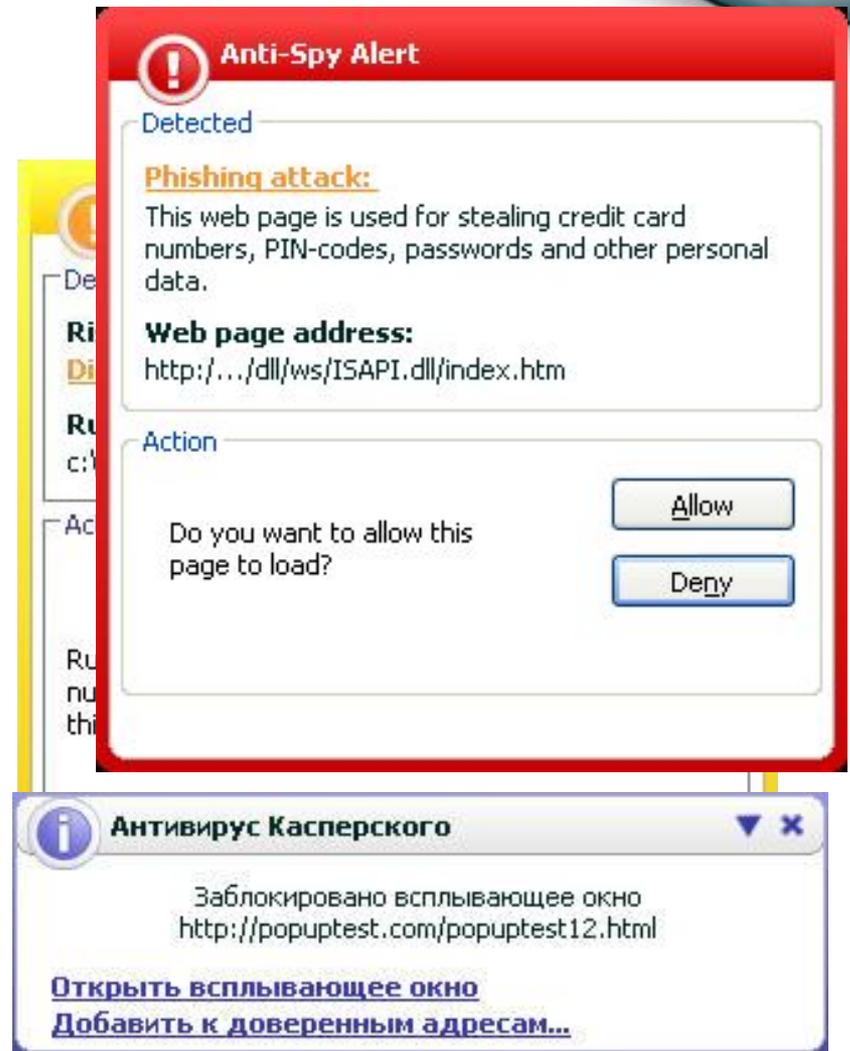
# Борьба с активными угрозами

- 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



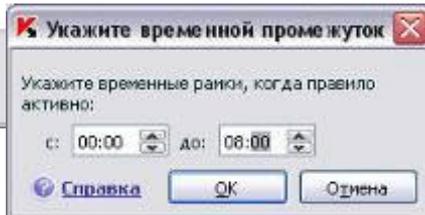
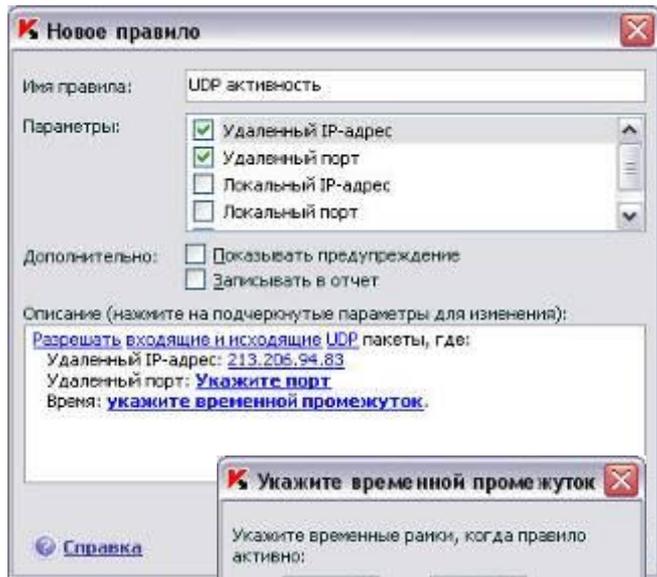
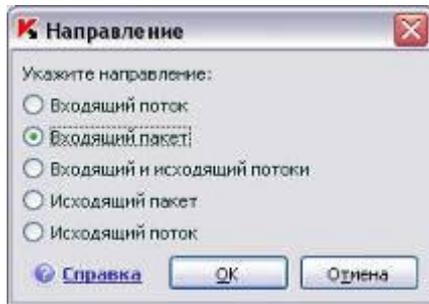
# Защита от шпионского ПО и рекламы

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

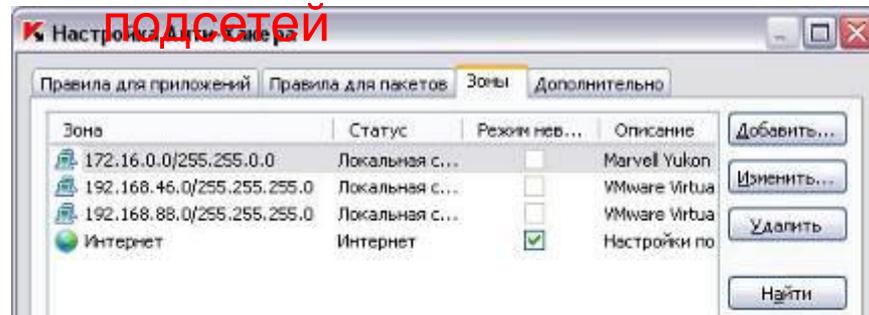


# Анти-Хакер: технологии Firewall

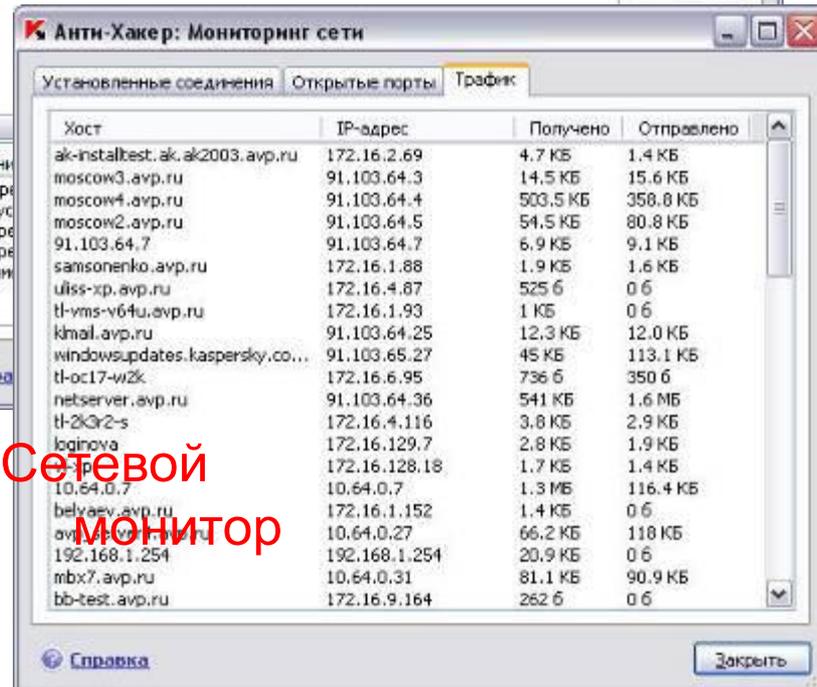
Гибкость создания правил



Настройка уровня доверия



Сетевой монитор



Windows Vista Security Software Providers - Windows Internet Explorer

http://www.microsoft.com/athome/security/update/windowsvistaAV.msp

Windows Vista Security Software Providers

Quick Links | Home | Worldwide

Search Microsoft.com for:

Security At Home

What's New

Latest Security Updates

Download Security Products

Protect Your Computer

Protect Yourself

Protect Your Family

Resources

Worldwide Sites



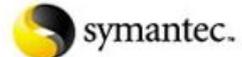
CERTIFIED FOR Windows Vista™

## 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.

			
---	---	--	---

[↑ 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?