



Антивирус Касперского для Windows Workstation 6.0

Антивирус Касперского для Windows Workstations

Обеспечивает блокирование вирусов по таким 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

Пользовательский интерфейс

The image displays the user interface of Kaspersky 6.0 for Windows Workstations, consisting of several overlapping windows:

- Main Dashboard:** Shows the status of protection. A green checkmark indicates that protection is active. A sidebar on the left lists protection components: File Antivirus, Mail Antivirus, Web Antivirus, Proactive Protection, Anti-Spyware, Anti-Hacker, and Anti-Spam. A status bar at the bottom indicates "Защита : работает" (Protection: working).
- Настройка: Антивирус Касперского (Settings):** A dialog box with a tree view on the left and configuration options on the right.
 - Настройка (Settings):** A tree view with categories: Защита (Protection), Поиск вирусов (Virus scanning), and Сервис (Service).
 - Защита (Protection):** Includes a "Общие" (General) section with checked options for "Включить защиту" (Enable protection) and "Запускать приложение при включении компьютера" (Start application when computer is turned on). It also features a "Категории вредоносного ПО" (Malware categories) section with checked options for "Вирусы, черви, троянские и хакерские программы" (Viruses, worms, trojans, and hacker programs) and "Шпионское, рекламное ПО, программы скрытого дозвона" (Spyware, adware, and dialers). A note explains that some legal programs may be classified as potentially dangerous. The "Дополнительно" (Advanced) section has checked options for "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 on battery), and "Уступать ресурсы другим приложениям" (Yield resources to other applications).
- Сервис (Service):** A window displaying program and system information.
 - Информация о программе (Program information):** Version: 6.0.3.830; Date of signature release: 11-Nov-07 5:28:21 PM; Number of signatures: 456406.
 - Информация о системе (System information):** Operating system: Microsoft Windows XP Professional Service Pack 2 (build 2600).
 - Информация о лицензии (License information):** Number: 0038-00006D-025BEEF2; Type: Пробная на 10 компьютеров (Trial for 10 computers); Date of completion: 12-Dec-07 2:59:59 AM.

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**

Скорость работы

Эффективность технологий iSwift и

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 баз: 11/11/2007 6:52:11 PM

Время	Имя	Статус	Причина
11/11/2007 7:40:49 PM	Файл: C:\WINDOWS\system32\kbsdf.dll	ok	проверен
11/11/2007 7:40:49 PM	Файл: C:\WINDOWS\system32\kbsdsg.dll	ok	проверен
11/11/2007 7:40:49 PM	Файл: C:\WINDOWS\system32\kbsdl.dll	ok	проверен
11/11/2007 7:40:49 PM	Файл: C:\WINDOWS\system32\kbsdl1.dll	ok	проверен
11/11/2007 7:40:49 PM	Файл: C:\WINDOWS\system32\kbsdmsfi.dll	ok	проверен
11/11/2007 7:40:49 PM	Файл: C:\WINDOWS\system32\kbsdmsno.dll	ok	проверен
11/11/2007 7:40:49 PM	Файл: C:\WINDOWS\system32\kbsdsp.dll	ok	проверен
11/11/2007 7:40:49 PM	Файл: C:\WINDOWS\system32\kbsdw.dll	ok	проверен
11/11/2007 7:40:49 PM	Файл: C:\WINDOWS\system32\kbsdtat.dll	ok	проверен
11/11/2007 7:40:49 PM	Файл: C:\WINDOWS\system32\kbsdtuf.dll	ok	проверен
11/11/2007 7:40:49 PM	Файл: C:\WINDOWS\system32\kbsdtuq.dll	ok	проверен

Проверка критических областей : завершена

Опасных объектов не обнаружено

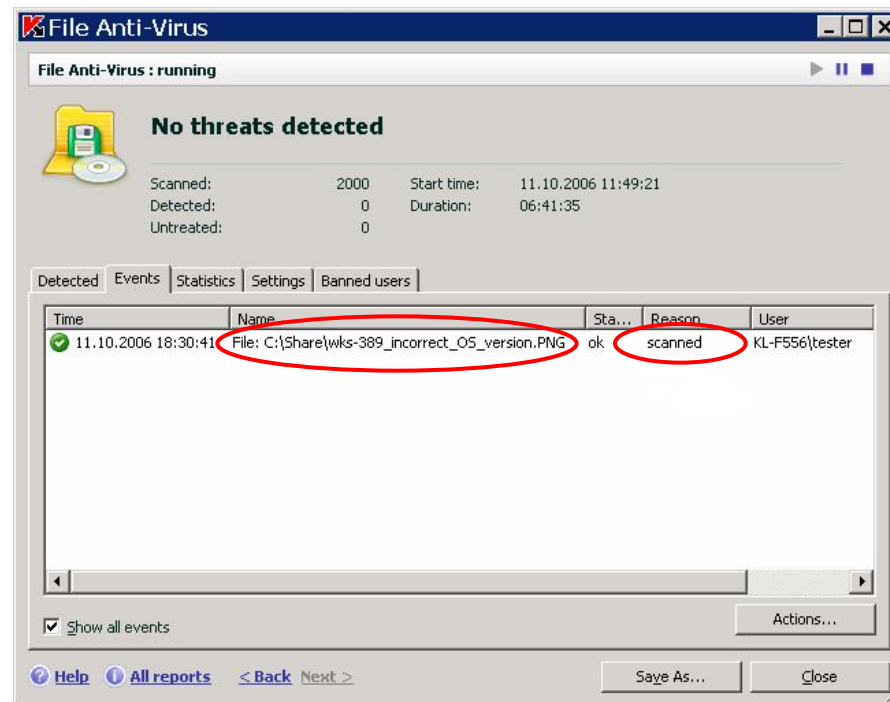
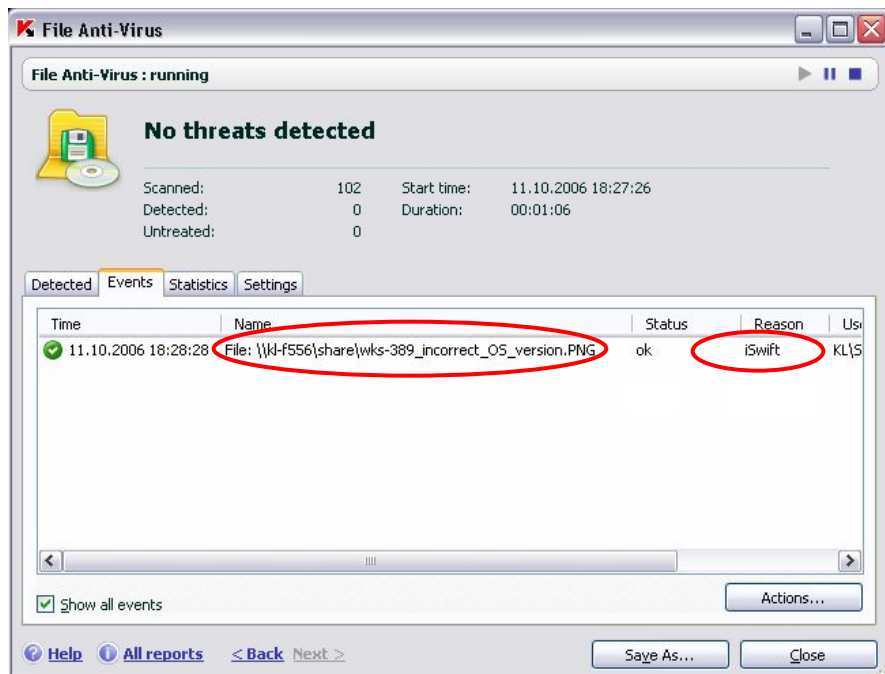
Проверено: 3255 Запуск: 11/11/2007 8:15:29 PM
Обнаружено: 0 Длительность: 00:00:12
Не обработано: 0 Завершение: 11/11/2007 8:15:41 PM
Дата выпуска баз: 11/11/2007 6:52:11 PM

Время	Имя	Статус	Причина
11/11/2007 8:15:40 PM	Файл: C:\WINDOWS\system32\kbsdf.dll	ok	iSwift
11/11/2007 8:15:40 PM	Файл: C:\WINDOWS\system32\kbsdsg.dll	ok	iSwift
11/11/2007 8:15:40 PM	Файл: C:\WINDOWS\system32\kbsdl.dll	ok	iSwift
11/11/2007 8:15:40 PM	Файл: C:\WINDOWS\system32\kbsdl1.dll	ok	iSwift
11/11/2007 8:15:40 PM	Файл: C:\WINDOWS\system32\kbsdmsfi.dll	ok	iSwift
11/11/2007 8:15:40 PM	Файл: C:\WINDOWS\system32\kbsdmsno.dll	ok	iSwift
11/11/2007 8:15:40 PM	Файл: C:\WINDOWS\system32\kbsdsp.dll	ok	iSwift
11/11/2007 8:15:40 PM	Файл: C:\WINDOWS\system32\kbsdw.dll	ok	iSwift
11/11/2007 8:15:40 PM	Файл: C:\WINDOWS\system32\kbsdtat.dll	ok	iSwift
11/11/2007 8:15:40 PM	Файл: C:\WINDOWS\system32\kbsdtuf.dll	ok	iSwift
11/11/2007 8:15:40 PM	Файл: C:\WINDOWS\system32\kbsdtuq.dll	ok	iSwift

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

Скорость работы

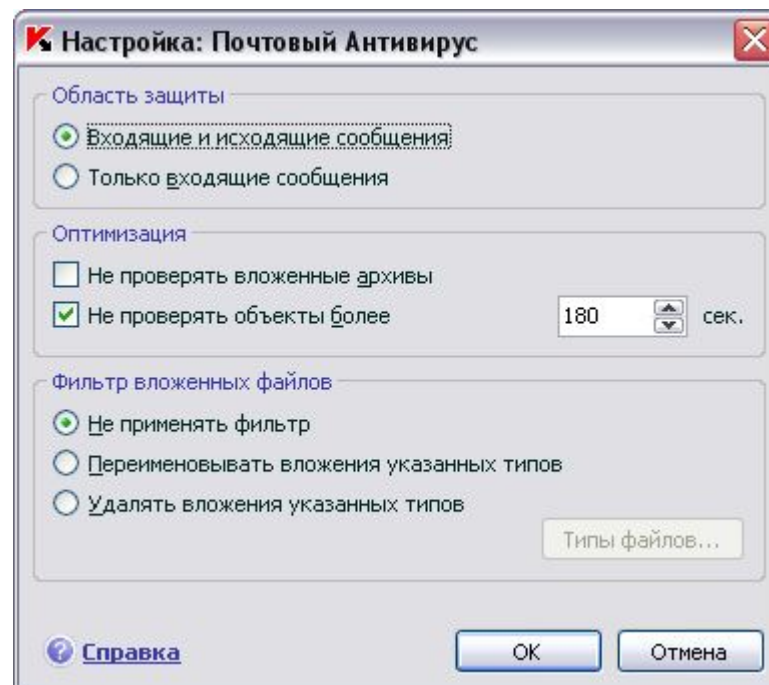
Сетевой iSwift



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

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

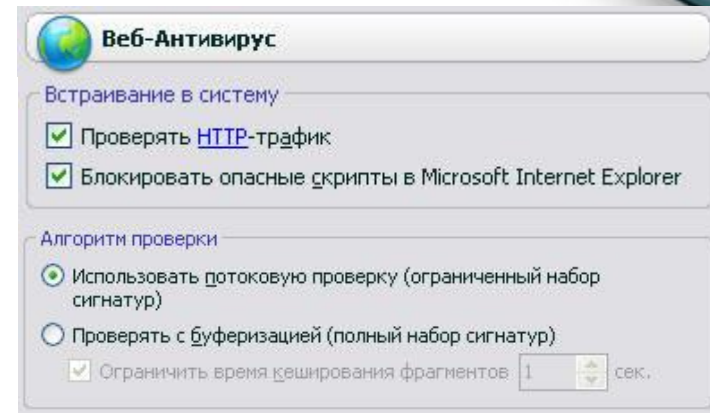
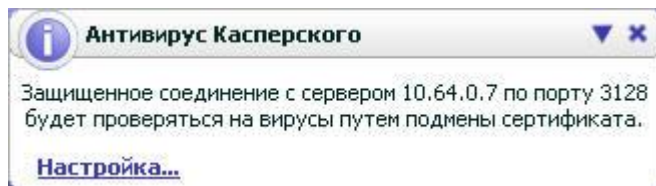
Зачем он нужен?

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

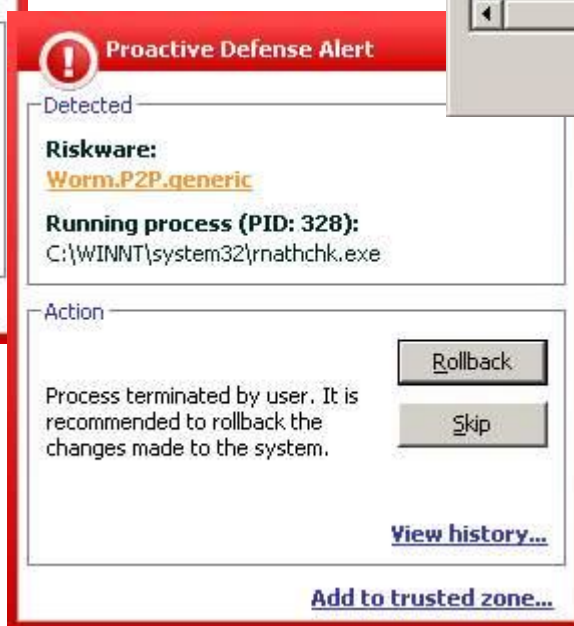
Process seems to be a P2P worm. Terminate

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

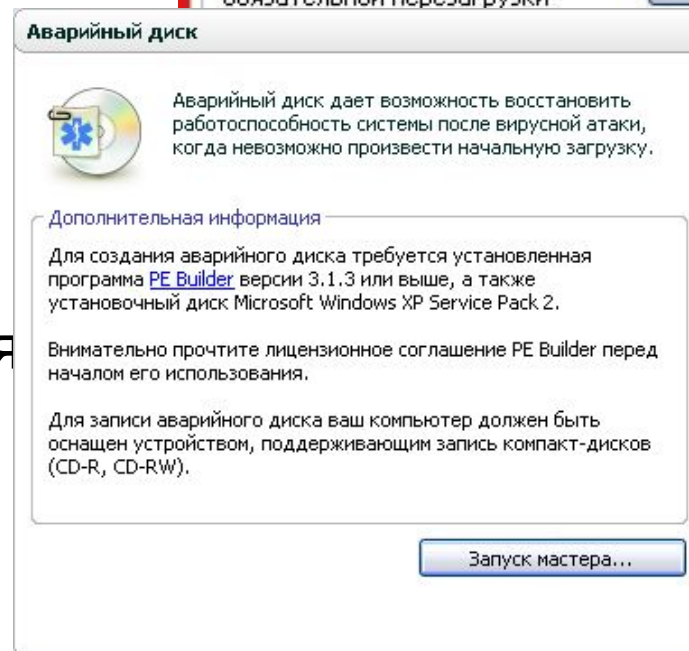
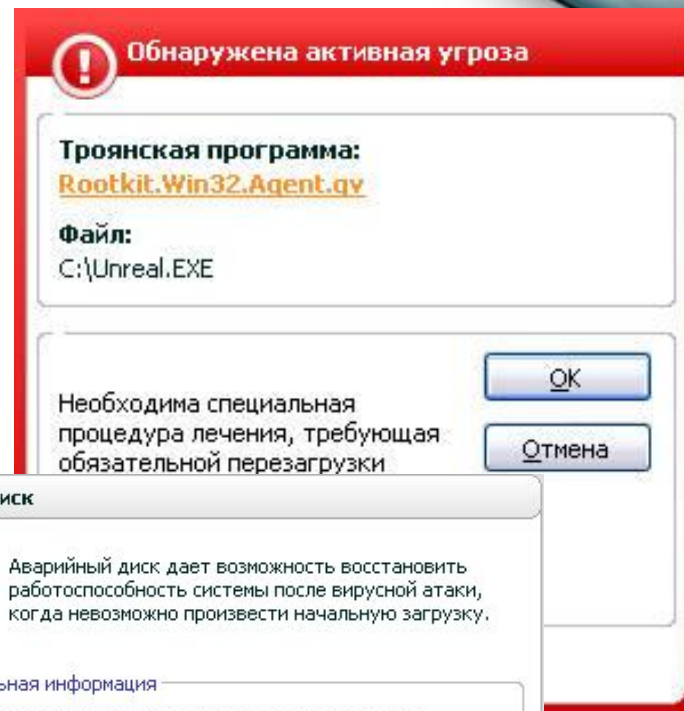
Rollback successfully completed.

[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

Направление

Укажите направление:

- Входящий поток
- Входящий пакет
- Входящий и исходящий потоки
- Исходящий пакет
- Исходящий поток

[Справка](#)

Новое правило

Имя правила: UDP активность

Параметры:

- Удаленный IP-адрес
- Удаленный порт
- Локальный IP-адрес
- Локальный порт

Дополнительно:

- Показывать предупреждение
- Записывать в отчет

Описание (нажмите на подчеркнутые параметры для изменения):
Разрешать входящие и исходящие UDP пакеты, где:
Удаленный IP-адрес: 213.206.94.83
Удаленный порт: Укажите порт
Время: укажите временной промежуток.

[Справка](#)

Укажите временной промежуток

Укажите временные рамки, когда правило активно:

с: 00:00 до: 08:00

[Справка](#)

Настройка уровня доверия

Настройка Анти-Хакера

Правила для приложений | Правила для пакетов | **Зоны** | Дополнительно

Зона	Статус	Режим нев...	Описание
172.16.0.0/255.255.0.0	Локальная с...	<input type="checkbox"/>	Marvell Yukon
192.168.46.0/255.255.255.0	Локальная с...	<input type="checkbox"/>	VMware Virtua
192.168.88.0/255.255.255.0	Локальная с...	<input type="checkbox"/>	VMware Virtua
Интернет	Интернет	<input checked="" type="checkbox"/>	Настройки по

Сетевой
монитор

Анти-Хакер: Мониторинг сети

Установленные соединения | Открытые порты | **Трафик**

Хост	IP-адрес	Получено	Отправлено
ak-installtest.ak.ak2003.avp.ru	172.16.2.69	4.7 КБ	1.4 КБ
moscow3.avp.ru	91.103.64.3	14.5 КБ	15.6 КБ
moscow4.avp.ru	91.103.64.4	503.5 КБ	358.8 КБ
moscow2.avp.ru	91.103.64.5	54.5 КБ	80.8 КБ
91.103.64.7	91.103.64.7	6.9 КБ	9.1 КБ
samsonenko.avp.ru	172.16.1.88	1.9 КБ	1.6 КБ
uliss-xp.avp.ru	172.16.4.87	525 Б	0 Б
tl-vms-v64u.avp.ru	172.16.1.93	1 КБ	0 Б
kmail.avp.ru	91.103.64.25	12.3 КБ	12.0 КБ
windowsupdates.kaspersky.co...	91.103.65.27	45 КБ	113.1 КБ
tl-oc17-w2k	172.16.6.95	736 Б	350 Б
netserver.avp.ru	91.103.64.36	541 КБ	1.6 МБ
tl-2k3r2-s	172.16.4.116	3.8 КБ	2.9 КБ
loginova	172.16.129.7	2.8 КБ	1.9 КБ
172.16.128.18	172.16.128.18	1.7 КБ	1.4 КБ
10.64.0.7	10.64.0.7	1.3 МБ	116.4 КБ
belyaev.avp.ru	172.16.1.152	1.4 КБ	0 Б
avp-avp-avp.ru	10.64.0.27	66.2 КБ	118 КБ
192.168.1.254	192.168.1.254	20.9 КБ	0 Б
mbx7.avp.ru	10.64.0.31	81.1 КБ	90.9 КБ
bb-test.avp.ru	172.16.9.164	262 Б	0 Б

[Справка](#)

Спасибо за внимание!

