A circular inset on the left side of the slide shows a microscopic view of a cell, with various organelles and structures visible in shades of green and white.

Продукты Лаборатории Касперского для защиты корпоративных сетей

Евгений Лужнов

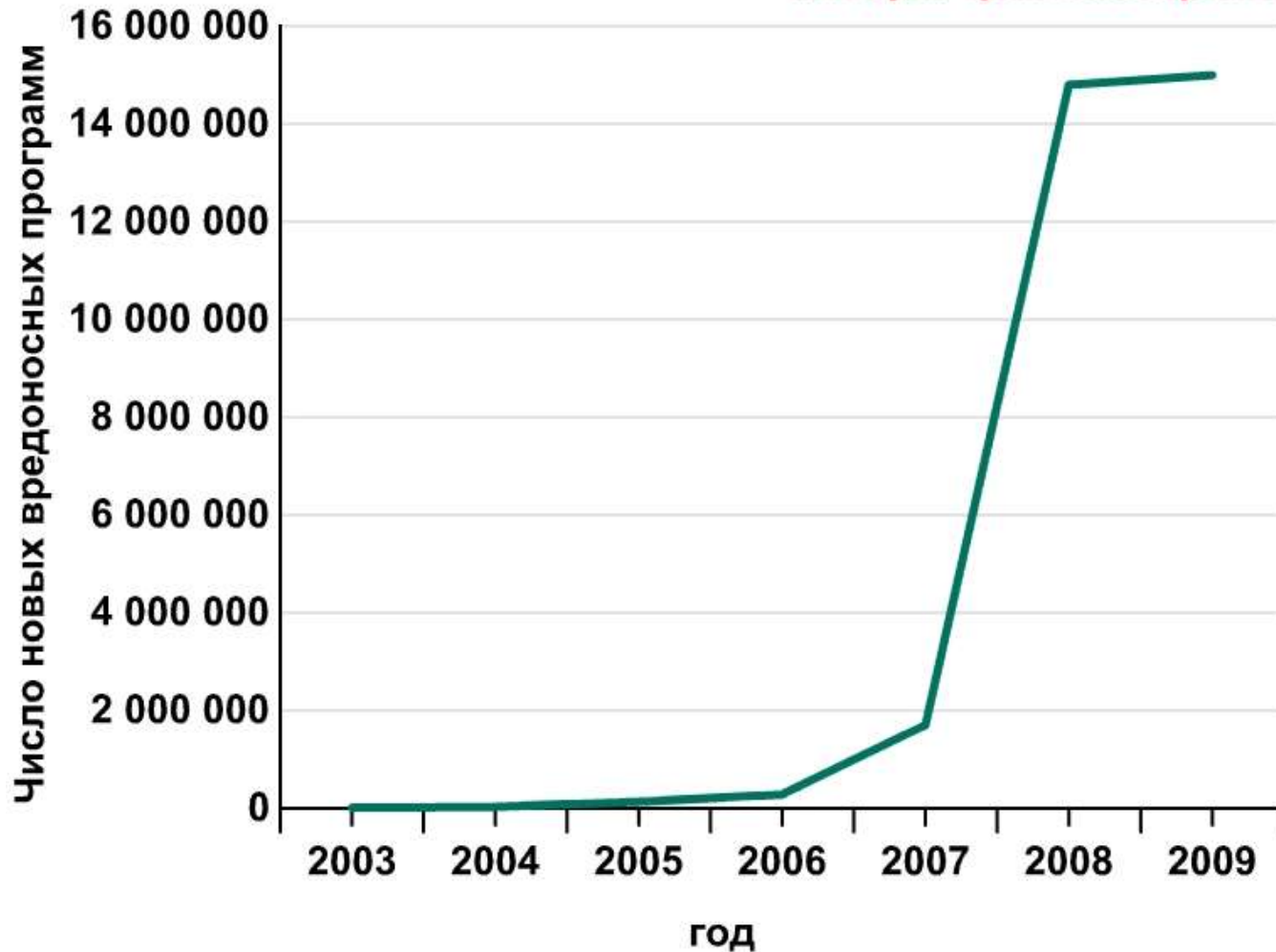
Инженер предпродажной поддержки

Evgeny.Luzhnov@ru.kaspersky.com

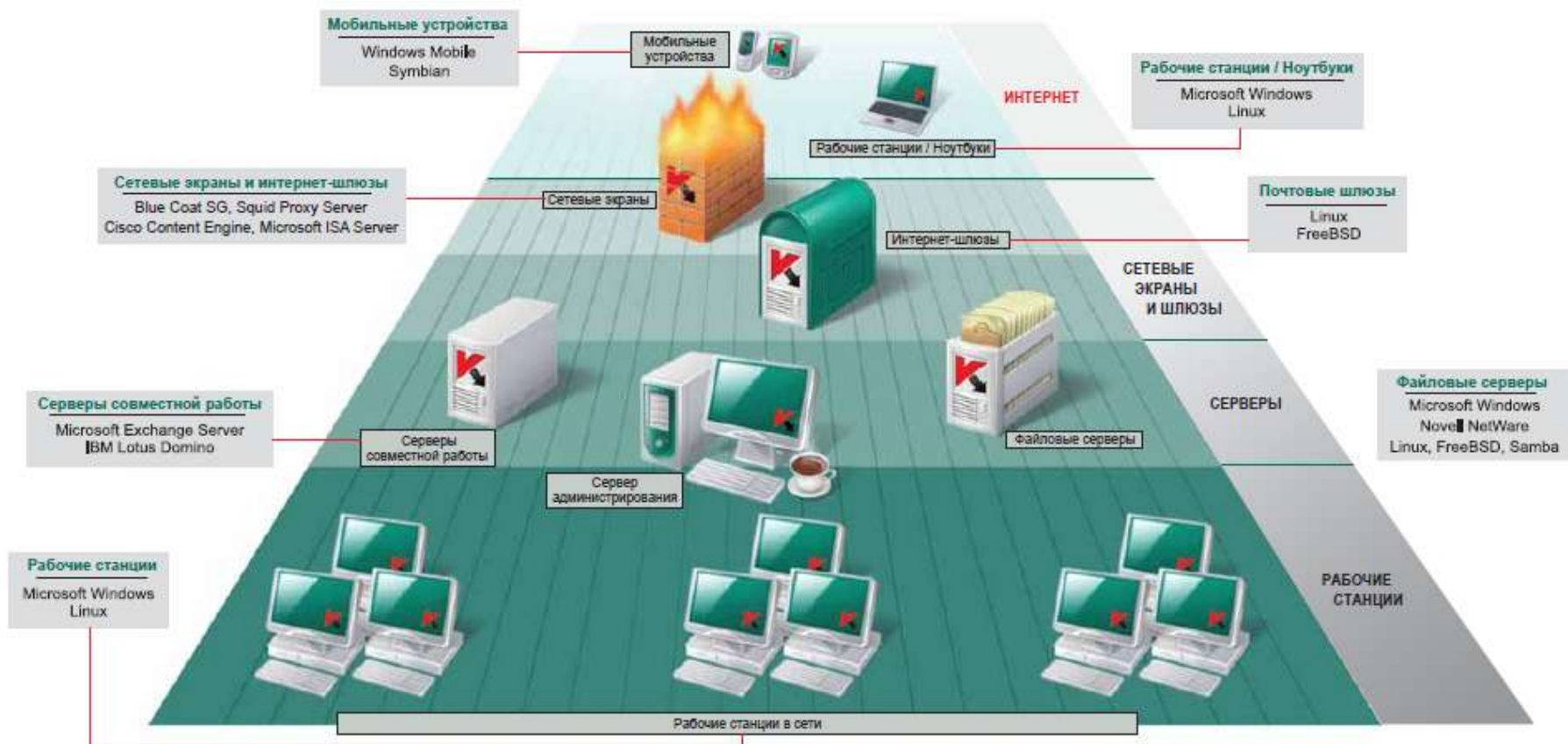
Рост количества вредоносных программ в коллекции



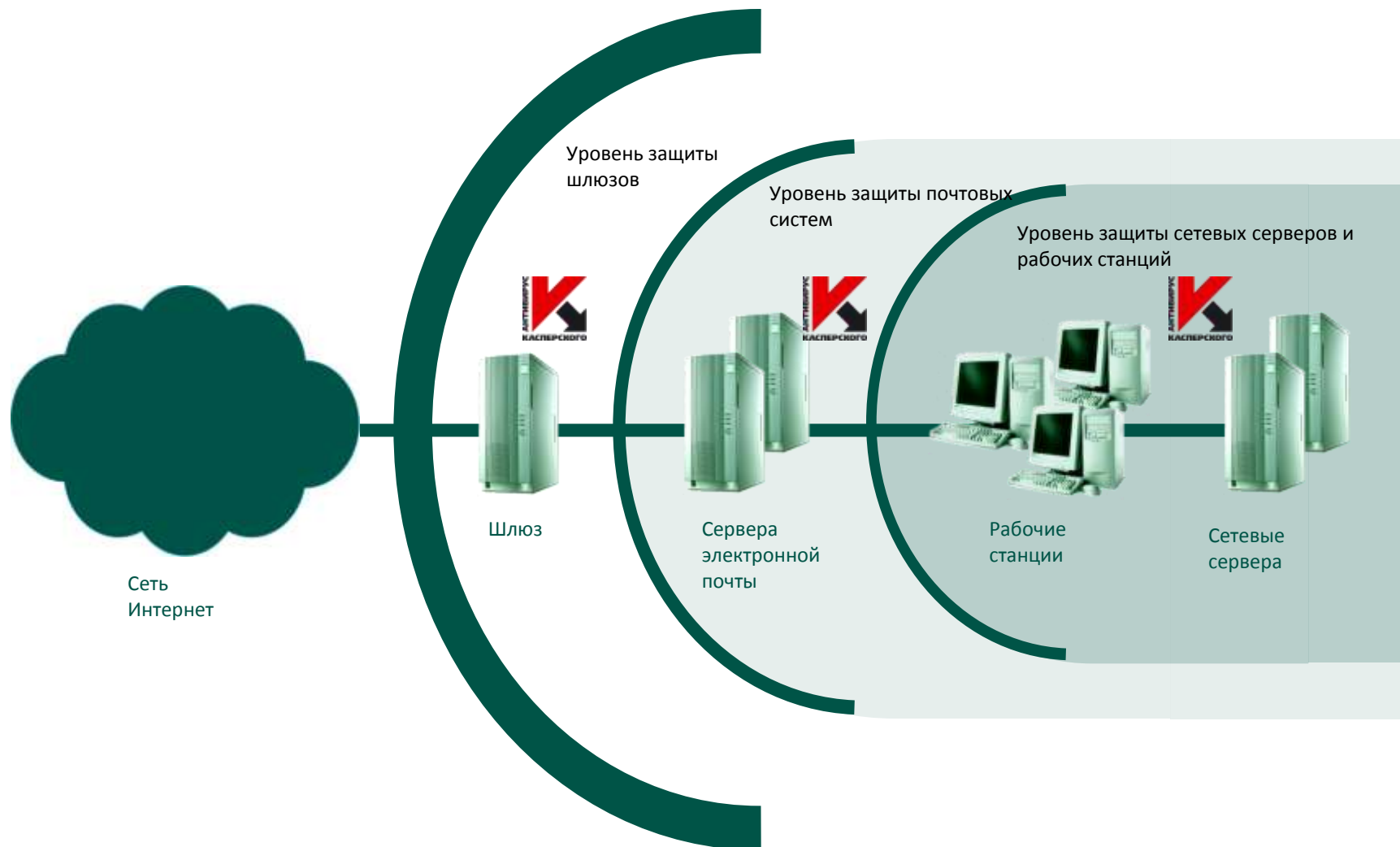
"Лаборатория Касперского"



Современная корпоративная сеть



Многоуровневая защита



- **Поддержка различных платформ**
- **Защита мобильных устройств**
- **Сочетание различных технологий**
- **Централизованное администрирование**
- **Масштабируемость**
- **Самозащита**
- **Эффективное использование сетевых ресурсов**



Антивирус Касперского для Proxy Server

Защита от вирусов, троянских программ и spyware



Антивирус Касперского для Proxy Server – это решение для защиты интернет-трафика (HTTP и FTP), проходящего через прокси-сервер.

- Проверка интернет-трафика в режиме реального времени.
- Выбор параметров фильтрации.
- Проверка архивированных файлов.
- Выявление потенциально опасных программ.
- Удаленное администрирование.
- Групповые политики безопасности.
- Уведомления для пользователей.
- Отчеты и статистика.
- Настройка режима обновления.



Поддерживаются прокси-сервера:

- Squid (с поддержкой протокола ICAP)
- Blue Coat SG Appliance
- NetApp/Blue Coat NetCache
- Cisco ACNS Content Engine

обеспечивает качественную антивирусную защиту данных, проходящих через межсетевой экран Check Point FireWall-1® по протоколам HTTP, FTP и SMTP

- Проверка входящего и исходящего трафика.
- Защита от потенциально опасного ПО.
- Выбор типа проверяемых объектов.
- Ограничение времени сканирования объекта.
- Проверка объектов «на лету».
- Выбор действия для зараженных объектов.
- Резервное копирование.
- Удобное администрирование.
- Масштабируемость решения.
- Автоматическое обновление антивирусных баз.
- Развитая система уведомлений.

Работает на платформе Windows (2000/XP/2003)



- **Антивирусная проверка в режиме реального времени.**
- **Выявление потенциально опасного ПО.**
- **Передовые технологии.**
- **Защита массовых серверов:**
 - Microsoft ISA Server 2006 Enterprise Edition SP1
 - Microsoft ISA Server 2006 Standard Edition SP1
- **Запуск нескольких экземпляров антивируса:**
 - Microsoft ISA Server 2004 Standard Edition
 - Microsoft ISA Server 2004 Enterprise Edition
- **Выбор проверочных технологий:**
 - Microsoft ISA Server 2000 Standard Edition
 - Microsoft ISA Server 2000 Enterprise Edition
- **Настройка групповых политик.**
- **Оптимизация производительности.**
- **Централизованное управление.**
- **Система оповещений и отчетности.**
- **Автоматические обновления.**



- Kaspersky Security для почтовых серверов
 - Антивирус Касперского для MS Exchange 2000/2003
 - Kaspersky Security для MS Exchange Server 2003
 - Kaspersky Security для MS Exchange Server 2007
 - Антивирус Касперского для Lotus Notes/Domino
 - Антивирус Касперского для Linux Mail Server
 - Kaspersky Mail Gateway
- Антивирус Касперского для MIMESweeper
- Kaspersky Anti-Spam



Антивирус Касперского/ Kaspersky Security для MS Exchange 2000/2003/2007



- надежная защита от вредоносных и потенциально опасных программ.
- фильтрация спама (Ksecurity for MS Exchange 2003).
- проверка входящих и исходящих почтовых сообщений и вложений.
- антивирусная проверка всех сообщений, включая общие папки.
- фильтрация сообщений по типам вложений.
- изоляция зараженных и подозрительных объектов.
- удобная система управления.
- предотвращение вирусных эпидемий.
- мониторинг состояния защиты с помощью уведомлений.
- система отчетов о работе приложения.
- масштабируемость.
- автоматическое обновление баз.



- **Комплексная антивирусная проверка.**
- **Уведомления.**
- **Карантин.**
- **Резервные копии.**
- **Проверка файловых систем сервера (iChecker KAVLinMail).**
- **Дополнительная фильтрация сообщений**
- **Удаленное управление.**
- **Настройка режима обновлений.**
- **Фильтрация спама (KMG).**

Sendmail
Qmail
Postfix
Exim



- Антивирус Касперского для файловых серверов
 - Антивирус Касперского для Windows Server **6.0 R2**
 - Антивирус Касперского для Linux File Server
 - Антивирус Касперского для Samba Server
 - Антивирус Касперского для Novell NetWare
 - Kaspersky Administration Kit **8.0**



Интернет

Уровень шлюзов



Шлюз

Уровень почтовых систем



серверы

Обеспечение антивирусной защиты сетевых серверов и рабочих станций

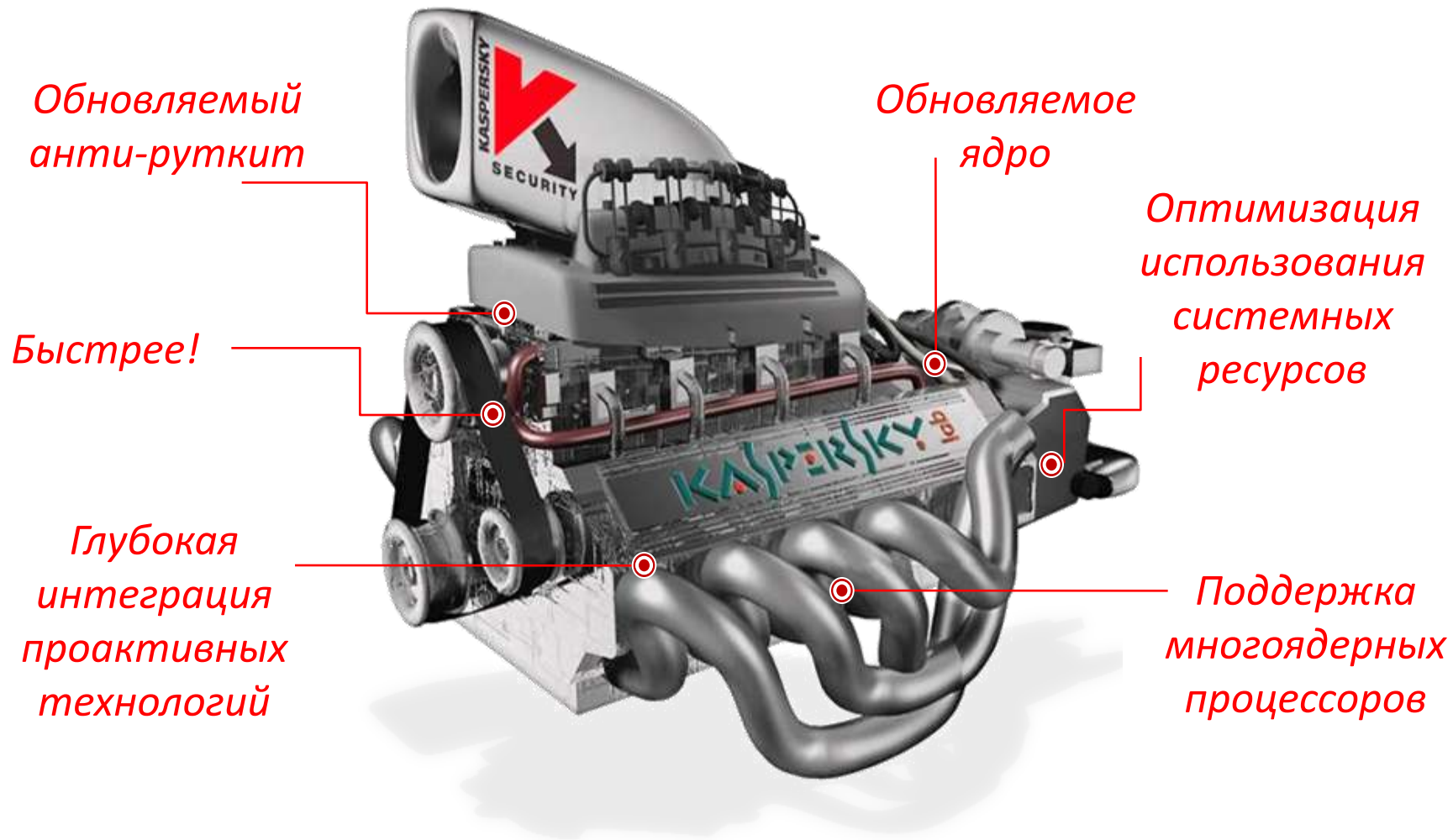
Уровень сетевых серверов и рабочих станций



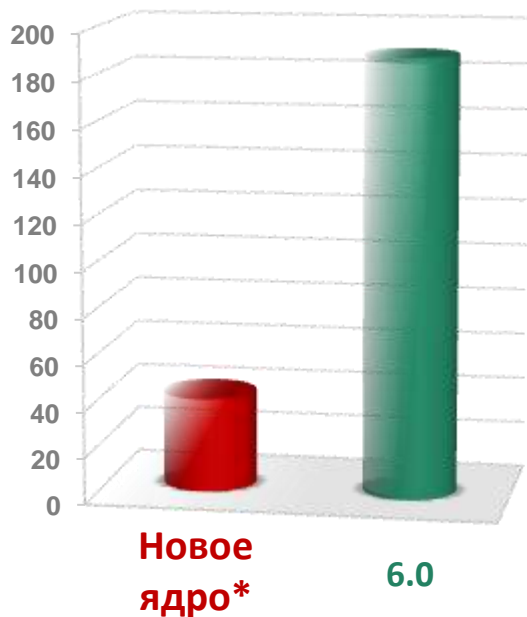
Release 2:

- Антивирус Касперского для **Windows Workstations 6.0 R2**
(защита рабочих станций)
- Антивирус Касперского для **Window Servers 6.0 R2**
(защита серверов)
- Антивирус Касперского **Second Opinion Solution 6.0 R2**
(совместимый сканер по требованию)
- **Kaspersky Administration Kit 8.0**
(средство управления)

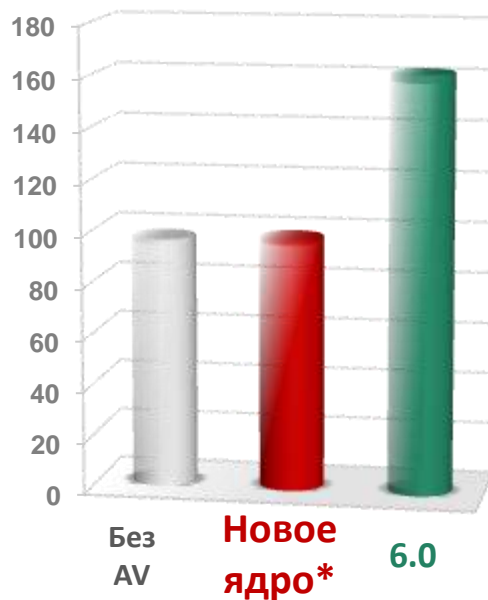
Новый антивирусный движок



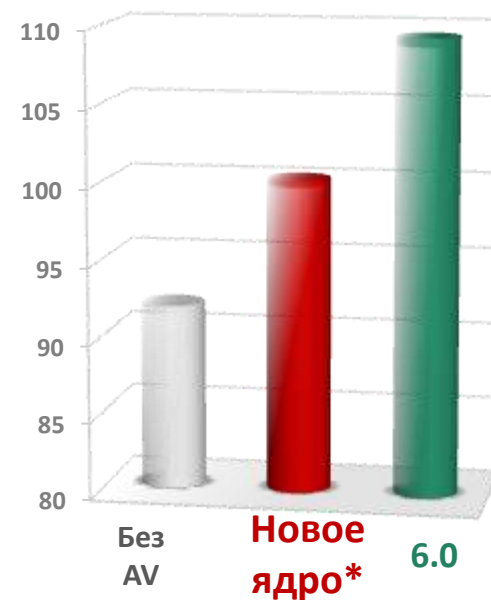
Время сканирования (сек.)



Скорость загрузки системы (сек.)



Время копирования файлов (сек.)



* Данные на примере Kaspersky Internet Security

KAV для Windows Server

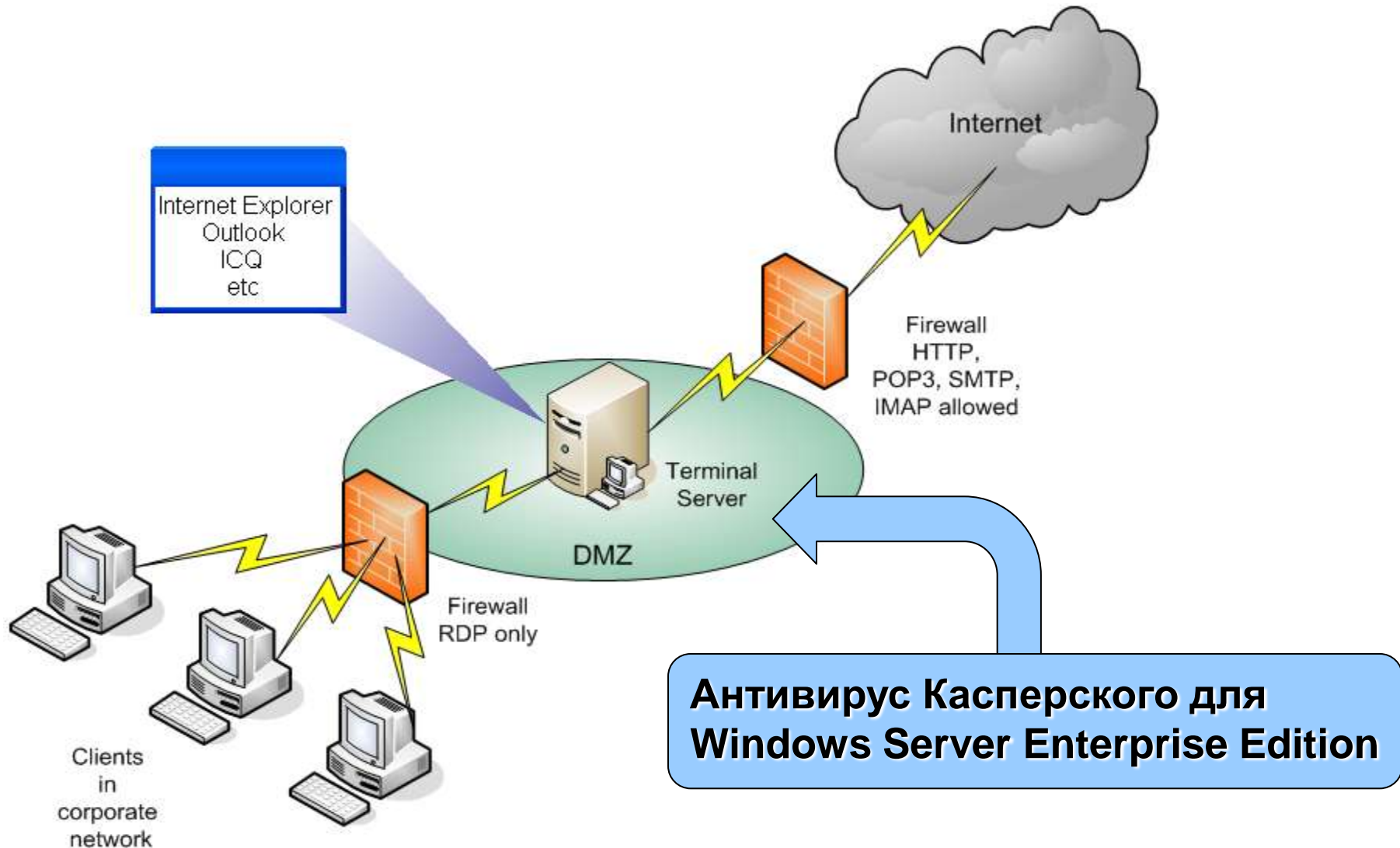
The screenshot displays the Kaspersky Anti-Virus 6.0 for Windows Servers interface. The main window title is "Антивирус Касперского 6.0 для Windows Servers". The interface is divided into several sections:

- Left Sidebar:** Contains navigation options: "Защита" (Protection) with a sub-option "Файловый Антивирус" (File Antivirus), "Поиск вирусов" (Search for viruses), and "Сервис" (Service).
- Top Panel:** Shows "Kaspersky Anti-Virus 6.0" and a green status bar indicating "Компьютер защищен" (Computer is protected). A "Настройка" (Settings) button is visible in the top right.
- Main Content Area:**
 - Защита (Protection):** A green shield icon and text stating "Антивирус Касперского обеспечивает комплексную защиту компьютера от вирусов, шпионского ПО и других вредоносных программ." (Kaspersky Antivirus provides comprehensive protection of the computer from viruses, spyware, and other malicious programs.)
 - Проверка (Check):** Includes options for "Полная проверка" (Full check) and "Быстрая проверка" (Quick check).
 - Обновление (Update):** A globe icon.
 - Лицензия (License):** A document icon.
- Right Panel:**
 - Text: "Защита: работает" (Protection: working).
 - Статистика (Statistics):**

Статистика:	Значение:
Всего проверено	271
Активные угрозы	0
Объекты карантина	0
Объекты хранилища	0
 - Диск аварийного восстановления (Emergency Recovery Disk):** A CD icon with a green cross.
- Bottom Panel:** Includes "Справка | Поддержка" (Help | Support) on the left and "Обнаружено" (Found) and "Отчеты" (Reports) buttons on the right.



- Сетевой iSwift
- Несколько экземпляров **НОВОГО** антивирусного ядра
- Распределение нагрузки на процессоры
- Приостановка сканирования
- Блокирование доступа зараженным компьютерам
- Эвристический анализатор. **Новинка!**
- Анти-руткит. **Новинка!**
- Гибкая настройка времени сканирования
- Настройка уведомлений
- Поддержка Windows 2008 R2. **Новинка!**

Защита терминальных пользователей Enterprise Edition



Разграничение прав администраторов Enterprise Edition

Full control	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Manage task state	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Manage tasks	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Modify settings	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read settings	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Manage Quarantine and Backup	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Manage reports	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read reports	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Connection	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Manage license keys	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Reading the privileges	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Editing privileges	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Антивирус Касперского для Windows Servers	 6.0	 Release 2	
Файловый антивирус	✓	✓ Улучшено	
Эвристик с эмулятором	Повышение уровня защиты		✓
Борьба с руткитами			✓
Windows Server 2008	Поддержка платформ		✓
Windows Server 2008 R2			✓

- Антивирус Касперского для Windows Workstation **6.0 R2**
- Антивирус Касперского для Linux Workstation
- Антивирус Касперского Second Opinion Solution **6.0 R2**



Интернет

Шлюз

Почтовые серверы

Сетевые серверы

Рабочие станции

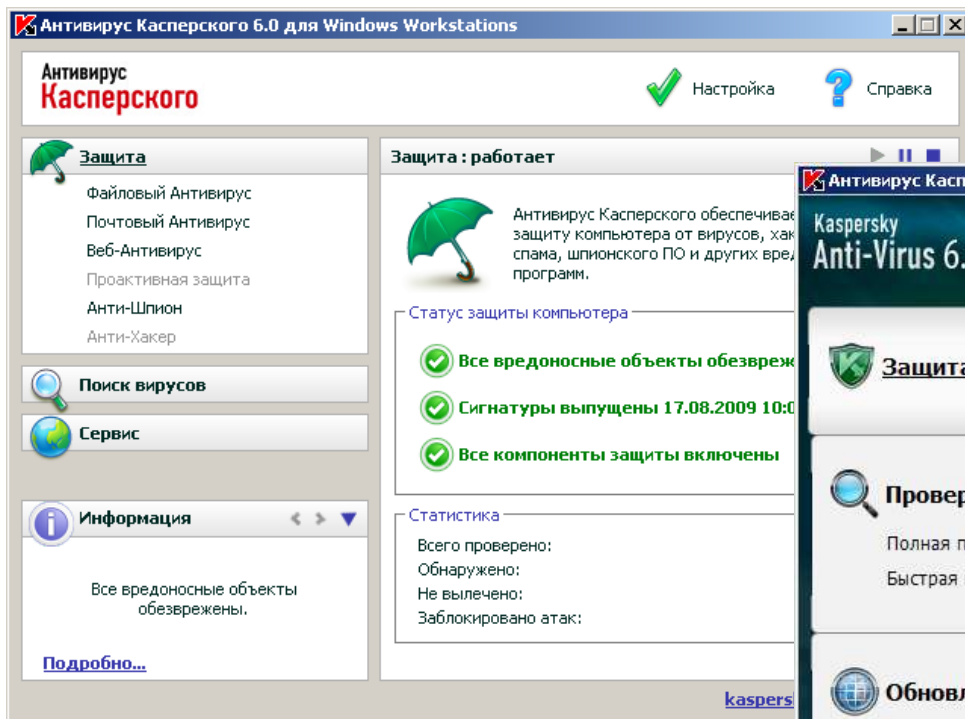
Обеспечение антивирусной защиты сетевых серверов и рабочих станций

Уровень сетевых серверов и рабочих станций

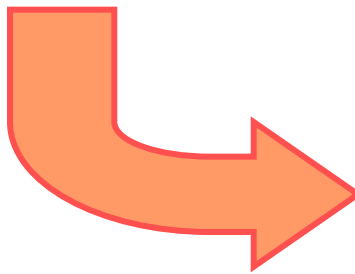


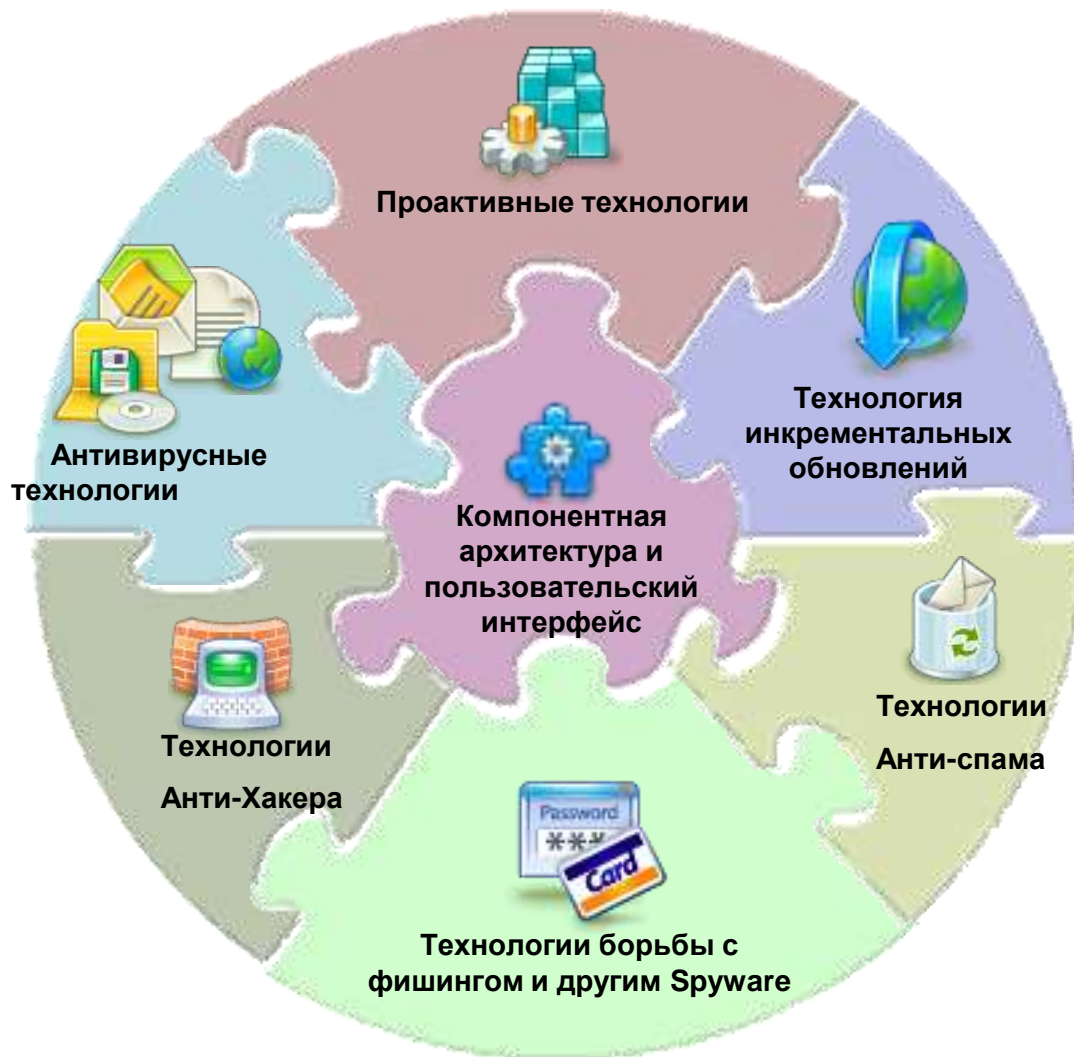
KAV 6.0 R2 для рабочих станций: Новый интерфейс

KAV 6.0 for WKS



KAV 6.0 R2 for WKS







Файловый антивирус (улучшено!)



Веб-антивирус (улучшего!)



Почтовый антивирус (улучшено!)



Проактивная защита (улучшено!)



Анти-хакер (улучшено!)



Анти-спам (улучшено!)

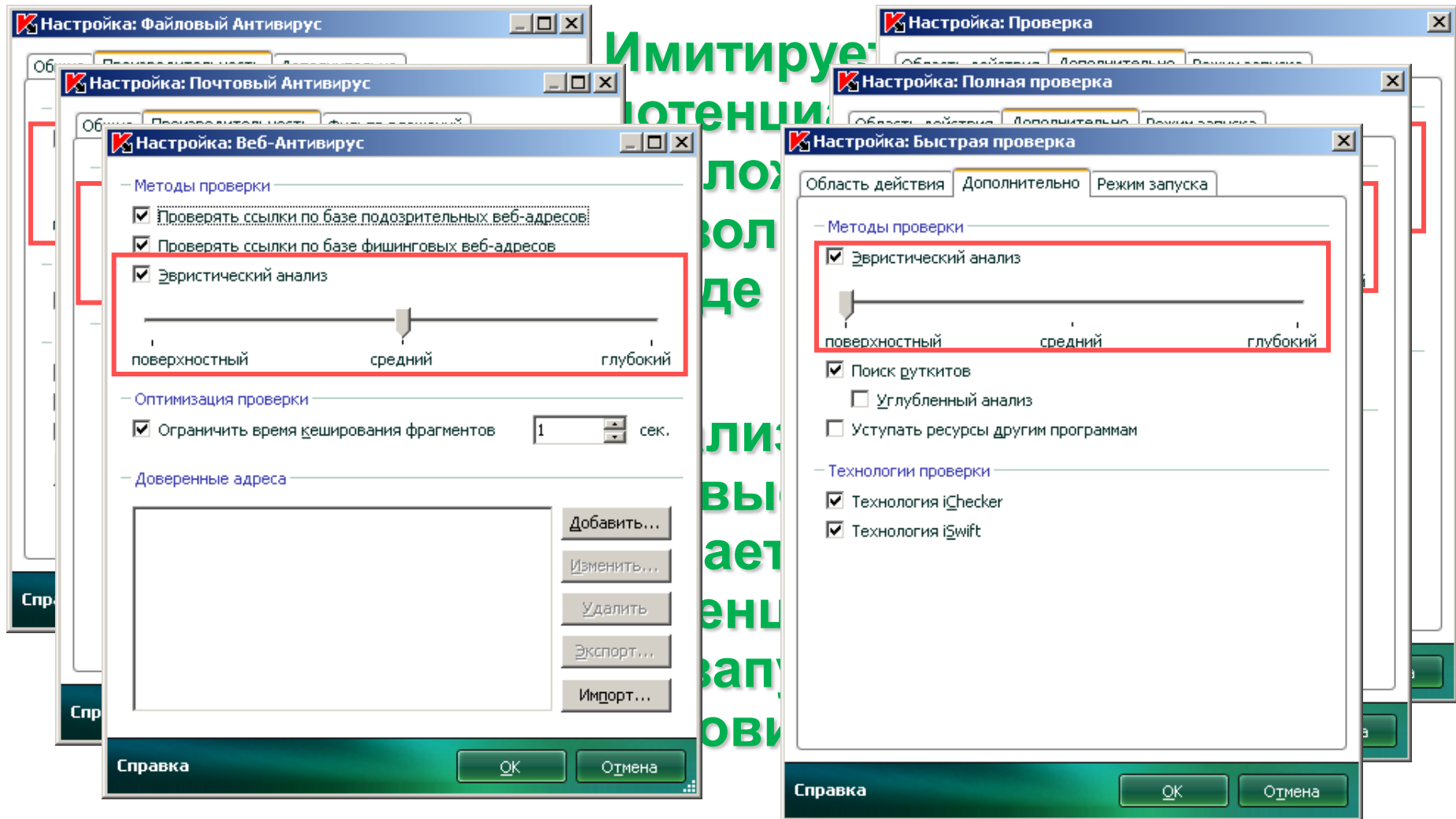


Контроль доступа (новое!)



Анти-шпион

Эвристический анализатор





Оптимизация проверки по требованию

Настройка
Kaspersky
Anti-Virus 6.0 Полная проверка

Защита

- Файловый Антивирус
- Почтовый Антивирус
- Веб-Антивирус
- Проактивная защита
- Анти-Шпион
- Анти-Хакер
- Анти-Спам
- Контроль доступа

Проверка

- Полная проверка**
- Быстрая проверка

Обновление

Параметры

- Отчеты и Хранилища
- Сеть

Справка

Уровень безопасности

Рекомендуемый

- Оптимальная защита
- Рекомендуется большинству пользователей

Настройка...

Действие

- Запросить по окончании проверки
- Запросить во время проверки
- Не запрашивать

- Лечить
- Удалить, если лечение невозможно

Режим запуска

- Каждую неделю по Чт в 21:00
- Приостанавливать проверку по расписанию, если выключен скринсейвер и разблокирован компьютер

OK Отмена

Настройка: Полная проверка

Область действия Дополнительно Режим запуска

Методы проверки

- Эвристический анализ

поверхностный средний глубокий

- Поиск руткитов
- Углубленный анализ
- Уступать ресурсы другим программам

Технологии проверки

- Технология iChecker
- Технология iSwift

Справка OK Отмена

Скорость работы

Файловый антивирус

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\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\bdsli.dll	ok	проверен
11/11/2007 7:40:49 PM	Файл: C:\WINDOWS\system32\bdsmsfi.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\bdsno.dll	ok	проверен
11/11/2007 7:40:49 PM	Файл: C:\WINDOWS\system32\bdsps.dll	ok	проверен
11/11/2007 7:40:49 PM	Файл: C:\WINDOWS\system32\bdsr.dll	ok	проверен
11/11/2007 7:40:49 PM	Файл: C:\WINDOWS\system32\bdtat.dll	ok	проверен
11/11/2007 7:40:49 PM	Файл: C:\WINDOWS\system32\bdtuf.dll	ok	проверен
11/11/2007 7:40:49 PM	Файл: C:\WINDOWS\system32\bdtuq.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\bdsf.dll	ok	Swift
11/11/2007 8:15:40 PM	Файл: C:\WINDOWS\system32\bdsq.dll	ok	Swift
11/11/2007 8:15:40 PM	Файл: C:\WINDOWS\system32\bdsi.dll	ok	Swift
11/11/2007 8:15:40 PM	Файл: C:\WINDOWS\system32\bdsli.dll	ok	Swift
11/11/2007 8:15:40 PM	Файл: C:\WINDOWS\system32\bdsmsfi.dll	ok	Swift
11/11/2007 8:15:40 PM	Файл: C:\WINDOWS\system32\bdsmsno.dll	ok	Swift
11/11/2007 8:15:40 PM	Файл: C:\WINDOWS\system32\bdsno.dll	ok	Swift
11/11/2007 8:15:40 PM	Файл: C:\WINDOWS\system32\bdsps.dll	ok	Swift
11/11/2007 8:15:40 PM	Файл: C:\WINDOWS\system32\bdsr.dll	ok	Swift
11/11/2007 8:15:40 PM	Файл: C:\WINDOWS\system32\bdtat.dll	ok	Swift
11/11/2007 8:15:40 PM	Файл: C:\WINDOWS\system32\bdtuf.dll	ok	Swift
11/11/2007 8:15:40 PM	Файл: C:\WINDOWS\system32\bdtuq.dll	ok	Swift

12 секунд против 1 минуты 07 секунд



Web-антивирус

- **Перехват и проверка HTTP-трафика**
 - В потоковом режиме (Safestream)
 - С буферизацией
- **Блокирование опасных скриптов**
- **Защита соединений SSL**



Проверка ICQ/MSN трафика

Настройка: Почтовый Антивирус

Общие Производительность Фильтр вложений

Область защиты

Входящие и исходящие сообщения

Только входящие сообщения

[414-592-979] - Окно сообщений

Виговский Евгений

Имя: Eugene 38-427-931

Email: Miranda v. 0.5.0.100

Виговский Евгений (17:36:51 13/07/2008)

Зацени

Виговский Евгений (17:36:54 13/07/2008)

Kaspersky Anti-Virus: forbidden incoming black link

Закреть Отправить



Проверка на наличие
фишинга
обнаружение
эксплойтов



Почтовый антивирус

- **Перехват почтового трафика SMTP, POP3, IMAP, NNTP (включая SSL)**
- **Независимо от протокола с помощью плагинов к почтовым клиентам Microsoft Outlook и The Bat!**
- **Возможность фильтрации и обработки вложений**
- **Лечение вирусов в почтовых базах Microsoft Outlook и Microsoft Outlook Express**





Модуль проактивной защиты

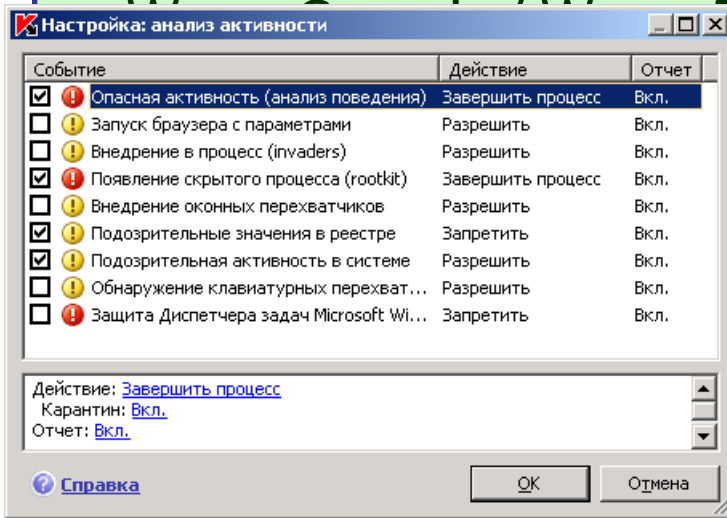


Проактивно блокирует

- Trojan.Generic / Trojan.Cryptor

PDM 6.0

PDM 6.0 R2



Trojan.P2P.Generic

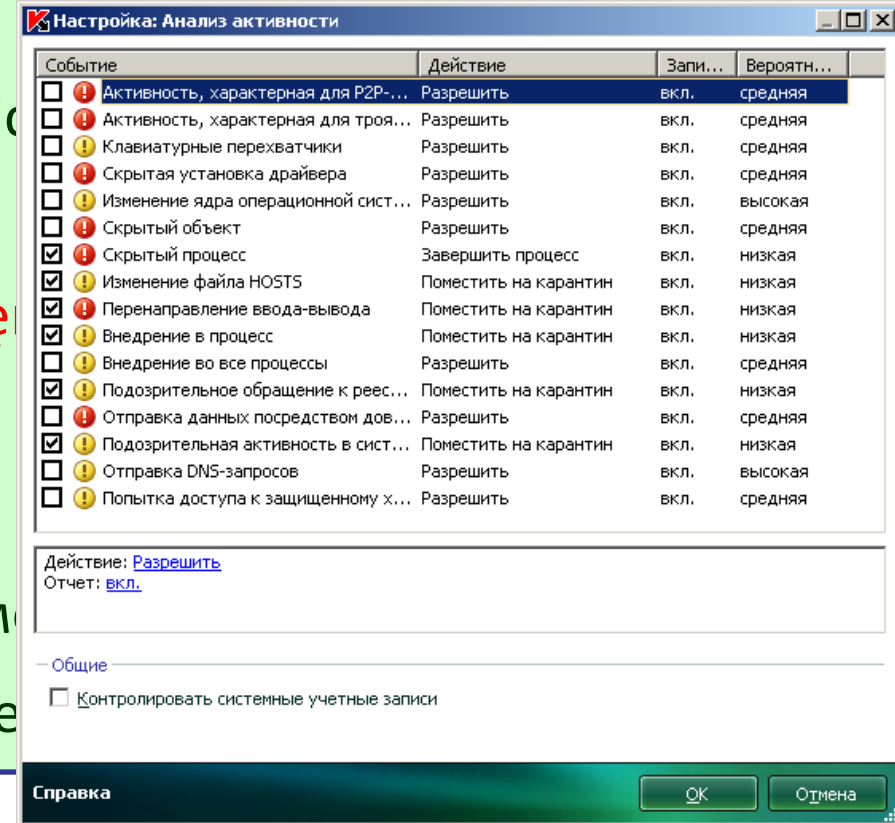
(kits)

(Invaders)

ных

попытку сбора паролей в систем

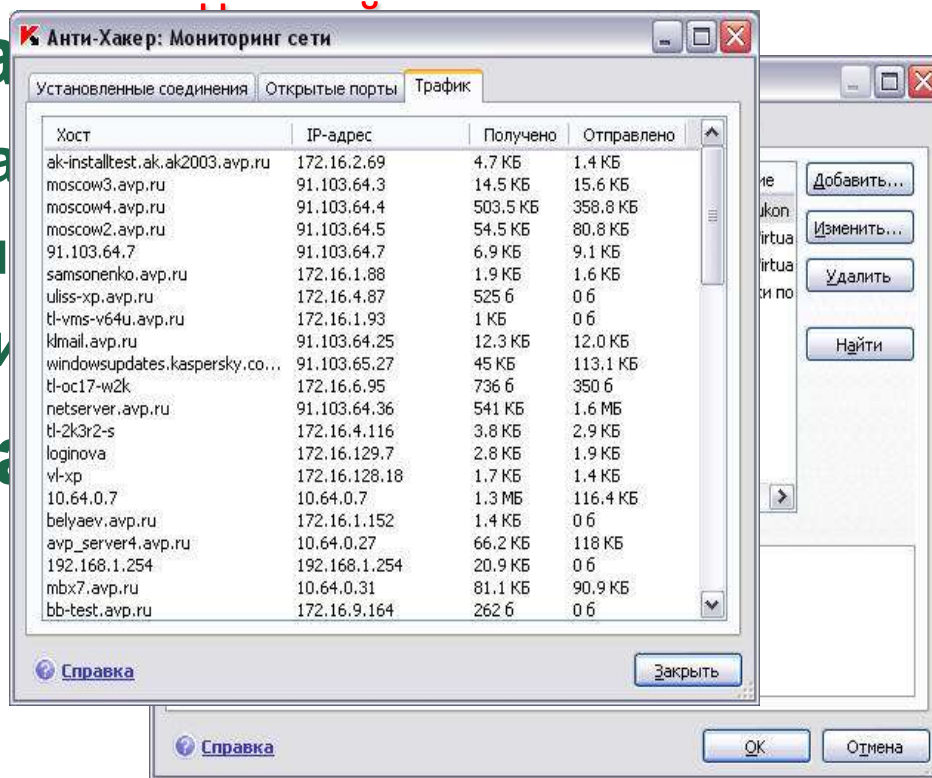
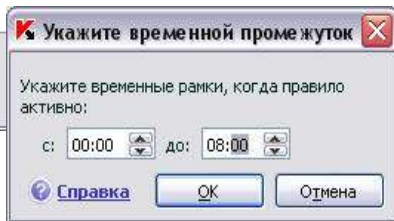
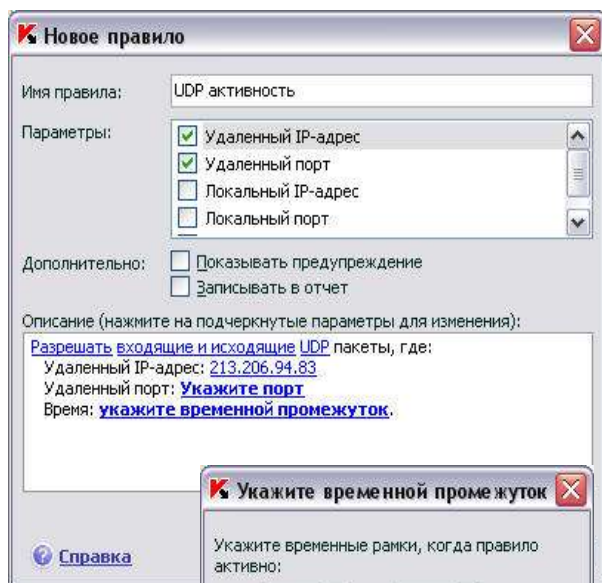
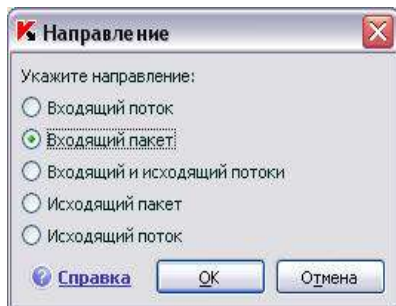
- Аномальное поведение приложе



ИЗМЕНЕНИЯ



Антихакер



● Сетевой монитор



Персональный анти-спам



Настройка: Анти-Спам

Общие | Алгоритмы | "Белый" список | "Черный" список

— Алгоритмы распознавания

- Анализ фраз по базе RecentTerms
 - Использовать расширенную базу
- Анализ заголовков сообщений (PDB)
- Распознавание изображений (GSG)
- Самообучающийся алгоритм анализа текста (iBayes)

— Фактор спама

Добавлять метку [!! SPAM] к теме сообщений со спам-фактором выше

59

— Фактор потенциального спама

Добавлять метку [?? Probable spam] к теме сообщений со спам-фактором выше

50

Дополнительно...

Справка

OK Отмена



Билайн™

Пример защиты почтового трафика

- **Полученные результаты работы системы (сутки):**
 - Количество сообщений ~ **200 000**
 - Количество SPAM-сообщений ~ **140 000**
 - Процент SPAM-сообщений ~ **70%**
 - Количество вирусов в сутки ~ **1500**
 - Объем трафика в сутки ~ **20-22 Гб**
- **Реальная эффективность решения**
 - Время обработки сотрудником одного SPAM-сообщения ~ **10 сек.**
 - Суммарные дневные затраты на SPAM ~ **16,203 чел/дня**
 - Средняя стоимость сотрудника ~ **\$1700**
- **Экономия**
 - В день ~ **\$ 1377**
 - В месяц ~ **\$ 41 318**
 - В год ~ **\$ 495 812**



Настройка: Контроль устройств

— Список блокируемых устройств —

- USB-устройства связи (модемы, телефоны и т.п.)
- USB-принтеры
- USB-устройства хранения данных
- CD/DVD-ROM-устройства
- Дисководы
- Устройства IEEE 1394 (Firewire)
- Модемы
- Устройства PCMCIA
- Устройства COM и LPT
- Стримеры
- Устройства 1284 Dot4
- Принтеры 1284 Dot4
- Устройства вывода
- Инфракрасные устройства
- Устройства Memory Technology Driver
- Многофункциональные устройства
- Устройства чтения смарт-карт
- Устройства Windows CE USB ActiveSync
- Bluetooth-устройства

Внимание! Чтобы изменения вступили в силу, необходимо выполнить повторное подключение устройства или перезагрузить компьютер.

— Автозапуск —

- Запретить автозапуск для всех устройств
- Запретить обработку autorun.inf

Внимание! Чтобы изменения вступили в силу, необходимо перезагрузить компьютер.

Справка ОК Отмена

t 8.0

Антивирус Касперского 6.0 R2 для Windows Workstation





Антишпион

- Антифишинг
- Антиреклама
- Антибаннер
- Антидозвон
- Блокировка всех типов кейлоггеров



Адрес: <http://purevector.com/money.ya.ru/Index.html>

Яндекс

деньги

Почта Лента Деньги Войти...

История платежей Внести

паспорт

Зарегистрироваться

Логин:

Пароль:

не сохранять

Войти

Забыли

В первый раз?
Яндекс.Деньги — это платежная система. Пользоваться ей очень просто.

1 Подключить
[Активировать](#)
[Но у меня уже](#)
[Интернет.Копейки](#)

[Расскажите еще о Яндекс.Деньгах!](#)

Оплата услуг

[Междугородная связь](#) [Мобильная связь](#)

[Skype](#) [МТС](#)

Файловый Антивирус : Тревога

Внимание

Троянская программа:
Trojan-Spy.HTML.Fraud.ay

Файл:
C:\...\Активация Яндекс_Деньги аккаунта[1].eml

Действие

Файл содержит троянскую программу 'Trojan-Spy.HTML.Fraud.ay'. Лечение невозможно

Применить во всех подобных случаях

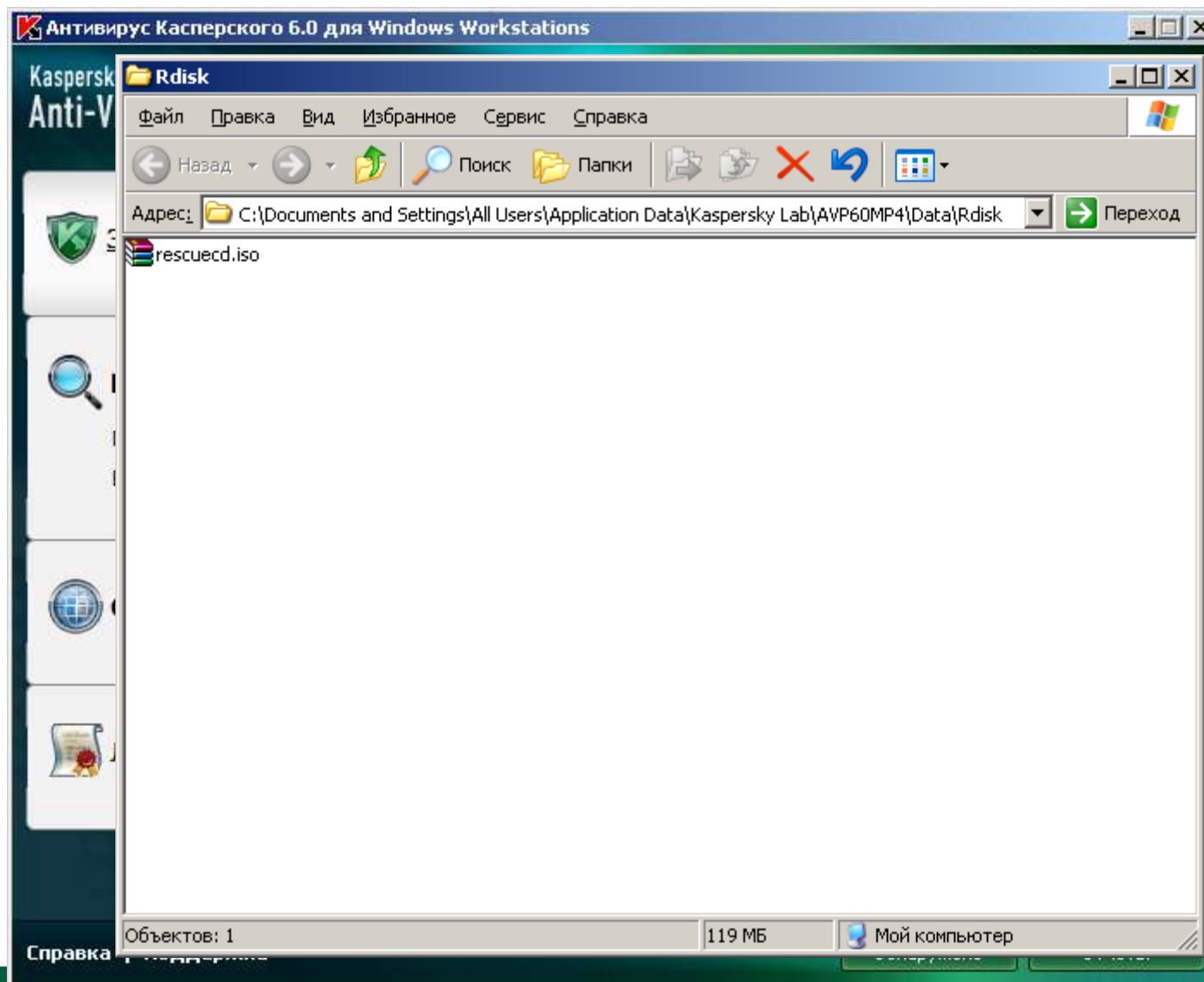


- Инкрементальное обновление
- Улучшенный механизм обновления
- Обновляемое ядро **Новинка!**
- Обновляемый антивирус **Новинка!**
- Обновление программных модулей
- Возможность обновления из локального источника

Компонент	Статус	Начало	Окончание	Размер	
✓ Обновление	завершено	27.05.2007 15:24:29	27.05.2007 15:24:45	12,8 КБ	
✓ Обновление	завершено	27.05.2007 16:24:29	27.05.2007 16:24:42	11,8 КБ	
✓ Обновление	завершено	27.05.2007 17:24:29	27.05.2007 17:24:42	11,8 КБ	
✓ Обновление	завершено	27.05.2007 18:24:40	27.05.2007 18:24:54	11,8 КБ	
✓ Обновление	завершено	27.05.2007 19:24:40	27.05.2007 19:24:55	12,8 КБ	
✓ Обновление	завершено	27.05.2007 20:24:40	27.05.2007 20:24:59	12,8 КБ	
✓ Обновление	завершено	27.05.2007 21:24:40	27.05.2007 21:24:56	11,8 КБ	
✓ Обновление	завершено	27.05.2007 22:24:40	27.05.2007 22:25:04	12,8 КБ	
✓ Обновление	завершено	27.05.2007 23:24:40	27.05.2007 23:25:01	13,9 КБ	
✓ Обновление	завершено	28.05.2007 0:24:40	28.05.2007 0:25:15	13,9 КБ	
✓ Обновление	завершено	28.05.2007 1:24:53	28.05.2007 1:25:12	12,8 КБ	



Диск аварийного восстановления



Что нового? Сравнение версий

Антивирус Касперского для Windows Workstations	 6.0	 Release 2
Файловый антивирус	✓	✓ Улучшено
Почтовый антивирус	✓	✓ Улучшено
Веб-антивирус	✓	✓ Улучшено
Проактивная защита	✓	✓ Улучшено
Анти-шпион	✓	✓
Сетевой экран	✓	✓
Анти-спам	✓	✓
Контроль устройств	Дополнительные возможности	✓
Поддержка IPv6		✓
Эвристик с эмулятором	Повышение уровня защиты	✓
Борьба с руткитами		✓
Проверка ICQ/MSN		✓
Поддержка Windows 7		✓

§ Один пользователь:

- Сам является администратором, другого нет
- Сам настраивает свой компьютер и AV
- Продукт для AV защиты – интерактивен
- У пользователя в распоряжении есть только его компьютер => все элементы защиты могут быть установлены только на нем

§ Корпорации:

- Пользователь не является администратором
- За настройку рабочих мест и AV защиты на них отвечают выделенные администраторы
- Продукт для AV защиты – не интерактивен
- Возможно часть элементов AV защиты вынести за пределы защищаемого компьютера (почта, трафик)

- Рядовые сотрудники не являются специалистами по использованию средств антивирусной защиты

=> Нельзя доверять пользователям настройку AV рабочей станции

- Контроль над антивирусной защитой всей компании лежит на сетевых администраторах, менеджерах по сетевой безопасности и т.д.

=> Администраторы отвечают не только за серверы (почтовые, файловые и др.), но и за большое количество рабочих станций

**Большая сеть без хорошей
системы
администрирования
неуправляема!**

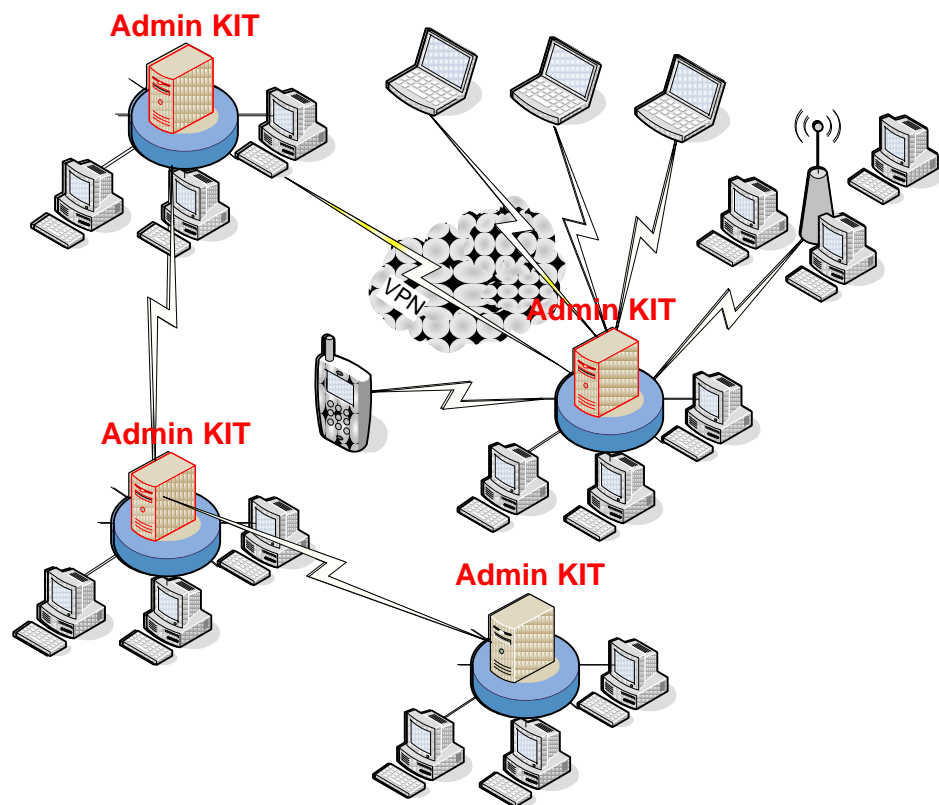
Что важно администратору?

- Быстрое и удобное начальное развертывания системы
- Удобное централизованное управление всей антивирусной защитой из одной точки
- Простота поддержания функционирования всей системы антивирусной защиты
- Мониторинг состояния всей системы
- Построение сводных отчетов
- В случае необходимости - возможность обратиться за помощью и консультацией к специалистам



Производительность - один сервер может поддерживать сеть из тысяч клиентов.

Масштабируемость и поддержка иерархии – несколько серверов существуют в одной сети.

Connectivity – поддержка любых сетевых конфигураций и технологий (VPN, прокси и др.)





Что нового? Сравнение версий

Kaspersky Administration Kit	 6.0	 8.0
Установка из единого дистрибутива (АК + База данных)		✓
Выбор типа установки в зависимости от размера сети		✓
Автоматическое создание инсталляционных пакетов		✓
Автоматическое создание политик		✓
Автоматическое создание задач		✓
Автоматическое добавление новых компьютеров по группам и установка антивирусного ПО на них	✓	✓
Иерархия серверов любой вложенности	✓	✓
Поиск по IP-подсетям/Active Directory/Windows Network	✓	✓
Создание логической сети на основе Active Directory	✓	✓
Управление из одной точки	✓	✓
Централизованное обновление из одной точки	✓	✓
Агенты обновлений	✓	✓
Проверка качества обновлений	✓	✓
Политика для мобильных пользователей	✓	✓
Поддержка Wake-on-LAN	✓	✓
Сбор информации об установленных в сети приложениях		✓
Информационные панели (Dashboards)		✓

Простота установки
и развертывания

Полный контроль

Что нового? Сравнение версий

Kaspersky Administration Kit	 6.0	 8.0
Удаленная установка приложений с помощью RPC/LoginScript/NAgent	✓	✓
Удаленная установка с уже обновленными базами		✓
Количество перезагрузок при удаленной установке	>1	1
Поддержка SNMP		✓
Расширение критериев выборки компьютеров		✓
Аудит действий администраторов	✓	✓
Разграничение полномочий администраторов	✓	✓
Экспорт отчетов в HTML/XML/PDF	Только HTML	✓
Создание и рассылка отчетов по e-mail	✓	✓
Утилита удаленной диагностики		✓
Обнаружение вирусных атак	✓	✓
Копирование объектов из локальных хранилищ на рабочее место администратора		✓
Автоматическое резервное копирование данных сервера администрирования		✓
Интерфейс для утилиты резервного копирования		✓
Поддержка Cisco NAC	✓	✓
Поддержка Microsoft NAP		✓

Выбор конфигурации в зависимости от размера сети

Kaspersky Administration Kit ✕

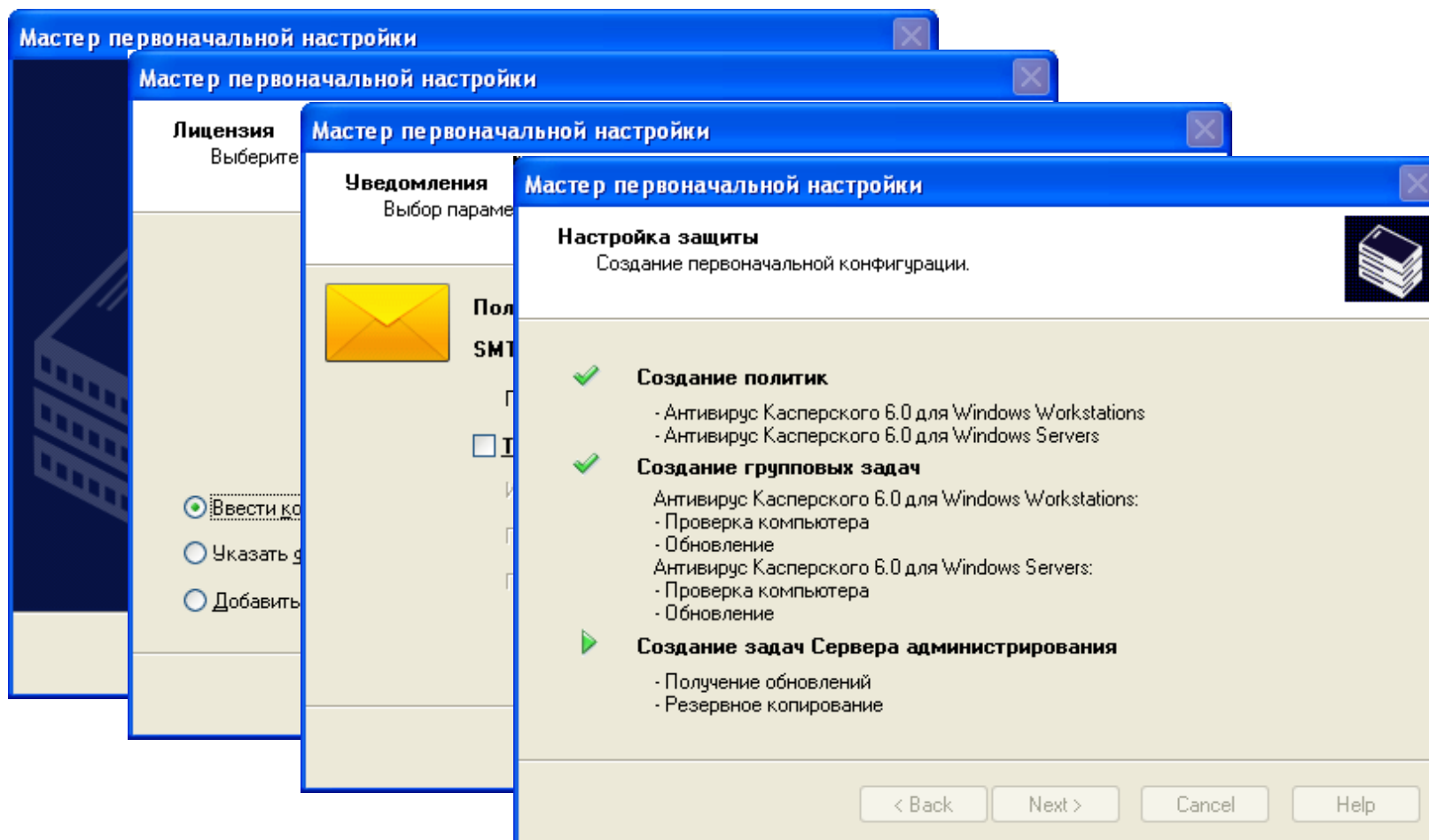
Размер сети
Выбор размера сети

Укажите примерное количество компьютеров, которыми вы планируете управлять. Эта информация будет использована для оптимальной настройки Kaspersky Administration Kit. При необходимости вы сможете изменить параметры позже.

От 1 до 100 компьютеров в сети

От 100 до 1000 компьютеров в сети

Более 1000 компьютеров в сети



Kaspersky Administration Kit

File Action View Help

Кaspersky Administration Kit

- Сервер администрирования - CLI1
- Управляемые компьютеры
- Отчеты и уведомления
- Задачи Kaspersky Administration K
- Задачи для наборов компьютеро
- Выборки событий и компьютеро
- Нераспределенные компьютеры
- Хранилища

Начало работы

Развертывание

Антивирус Касперского установлен на всех управляемых компьютерах

[▶ Установить Антивирус Касперского](#)

Управление компьютерами

Управляемых компьютеров: 1, Обнаружено нераспределенных компьютеров: 0.

[▶ Перейти к управляемым компьютерам](#)

Защита

Защита функционирует нормально

[▶ Настроить защиту рабочих станций](#)
[▶ Настроить защиту серверов](#)

Поиск вирусов

Поиск вирусов проводится по расписанию

[▶ Настроить поиск вирусов для рабочих станций](#)
[▶ Настроить поиск вирусов для серверов](#)

Обновление

Базы в хранилище обновлений устарели.

[▶ Изменить параметры обновления](#)

Настроить обновление

Мониторинг

На Сервере администрирования зарегистрированы критические события.

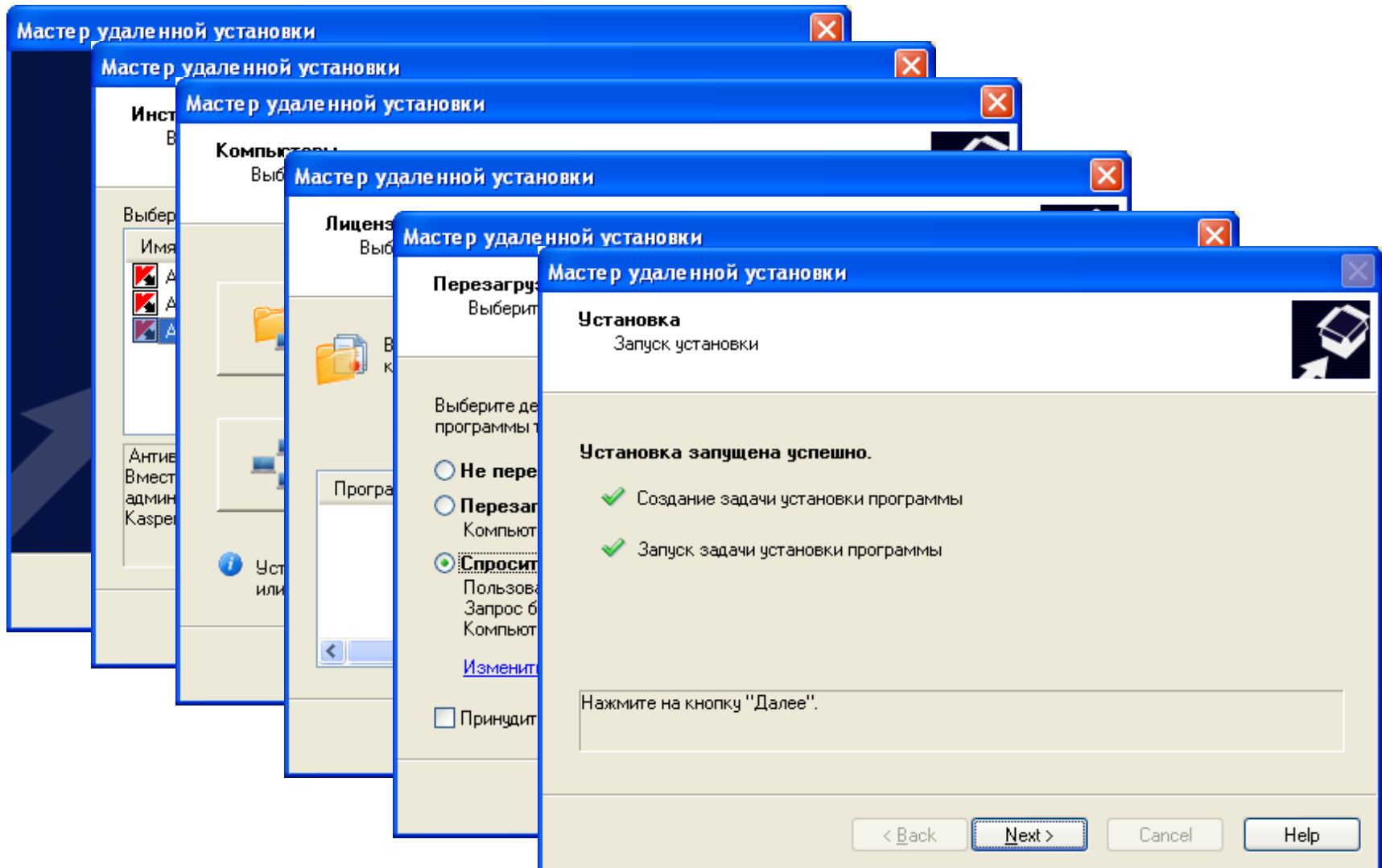
[▶ Посмотреть состояние защиты](#)
[▶ Изменить параметры уведомлений](#)

Просмотреть события

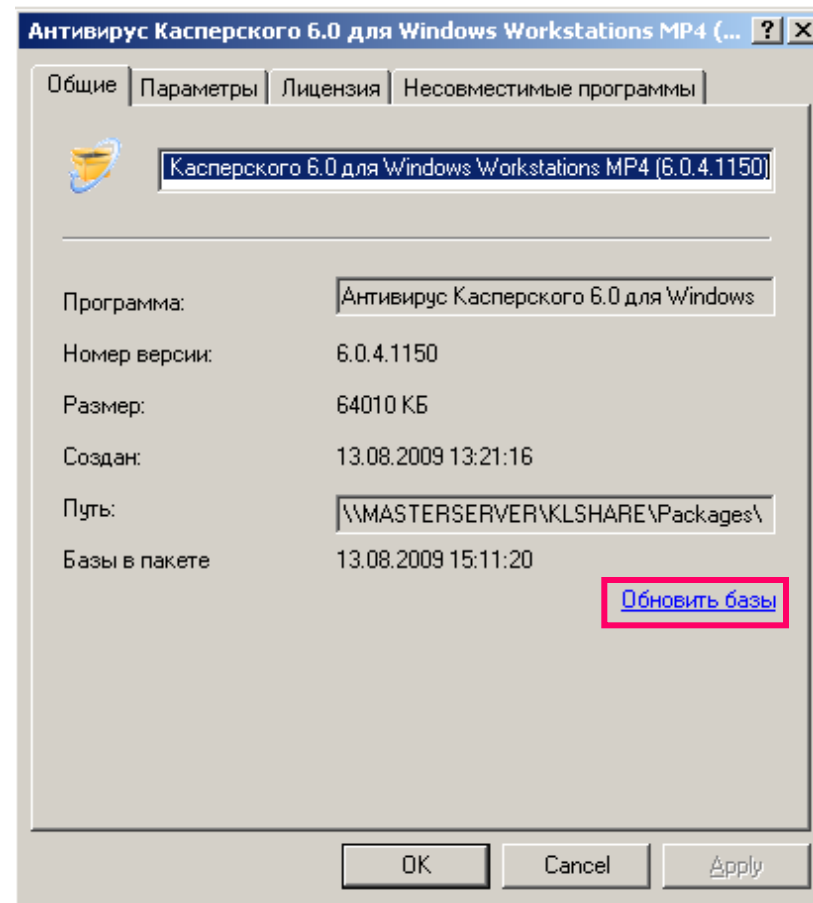
▶ Введение в Kaspersky Administration Kit ▶ Начало работы ▶ Особенности интерфейса управления ▶ Справка

Расширенный / Standard

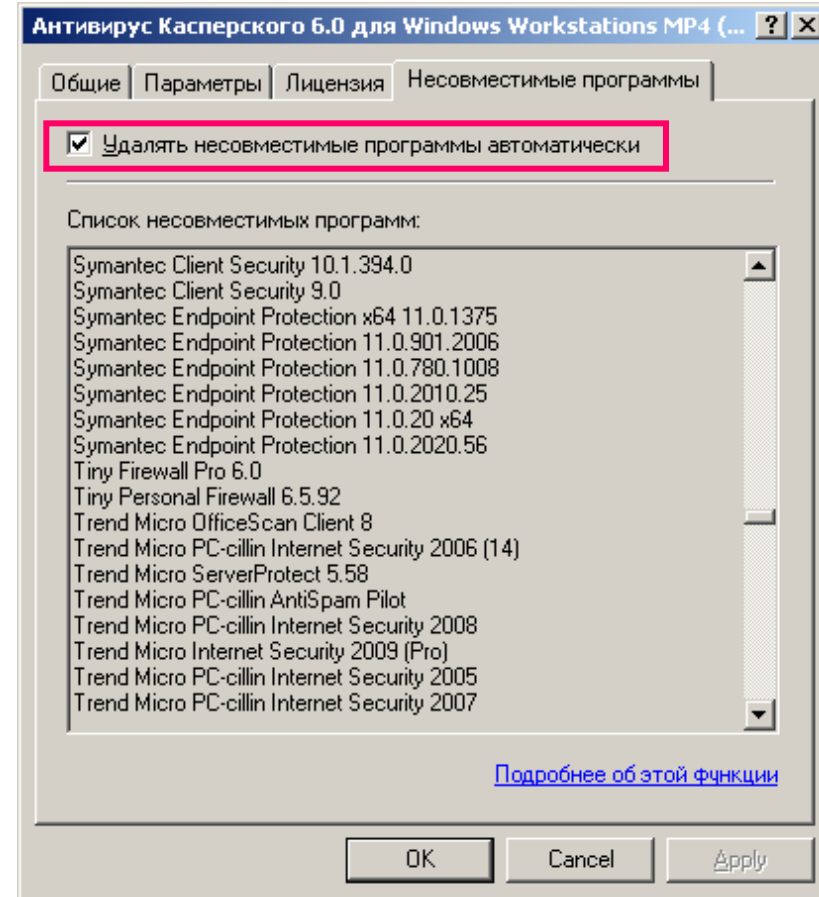
Быстрое развертывание защиты



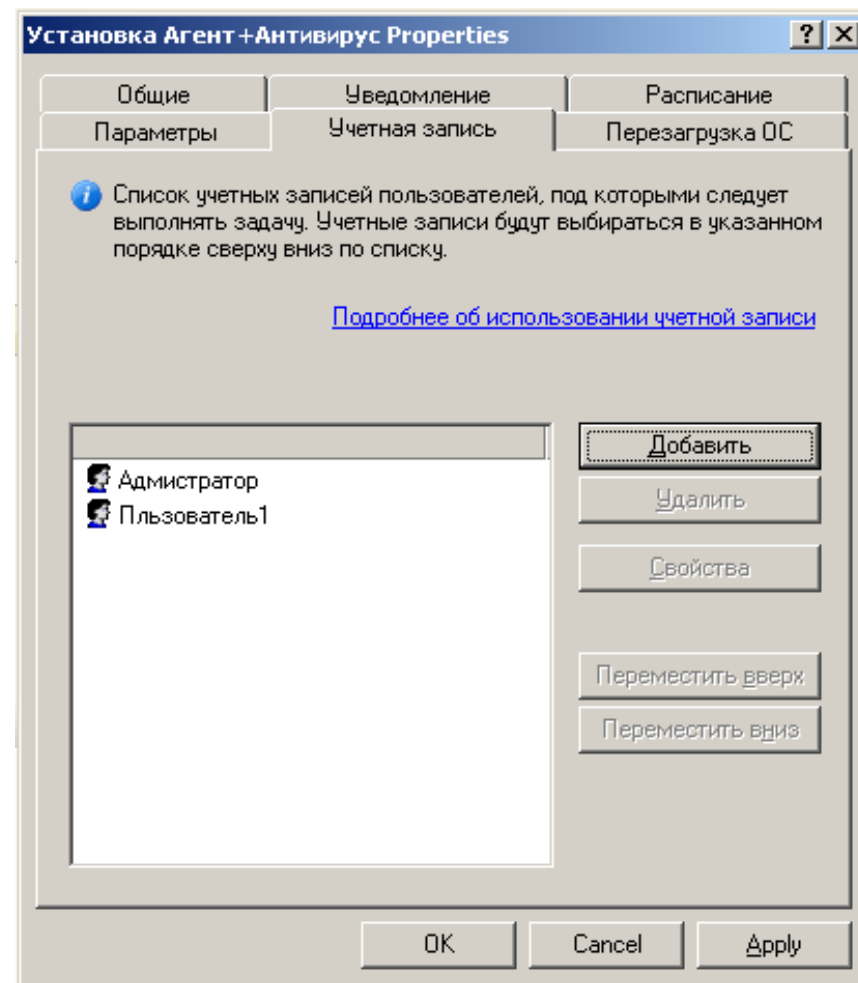
Возможность обновить антивирусные базы в инсталляционном пакете

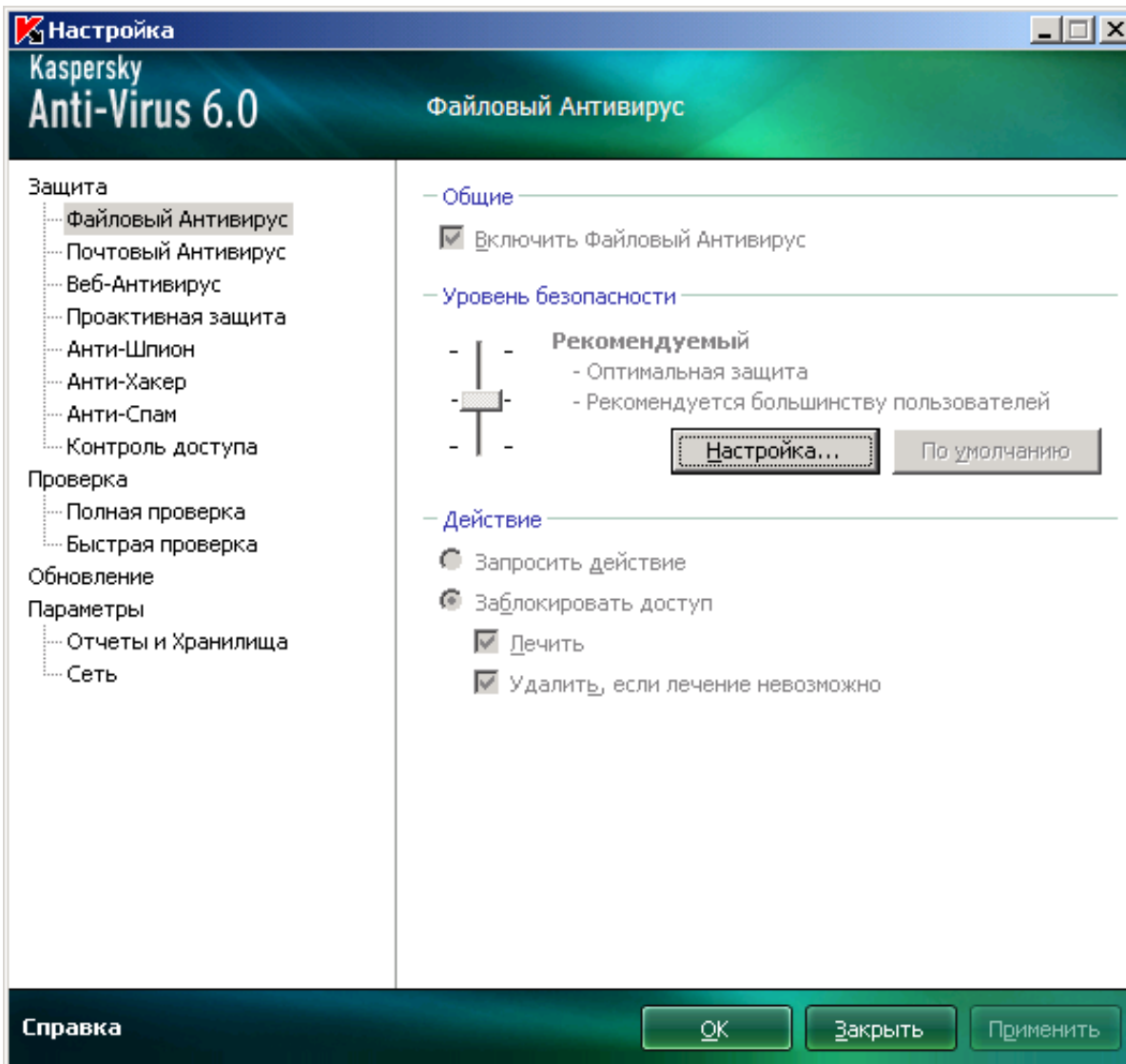


Автоматическое удаление несовместимых приложений перед установкой

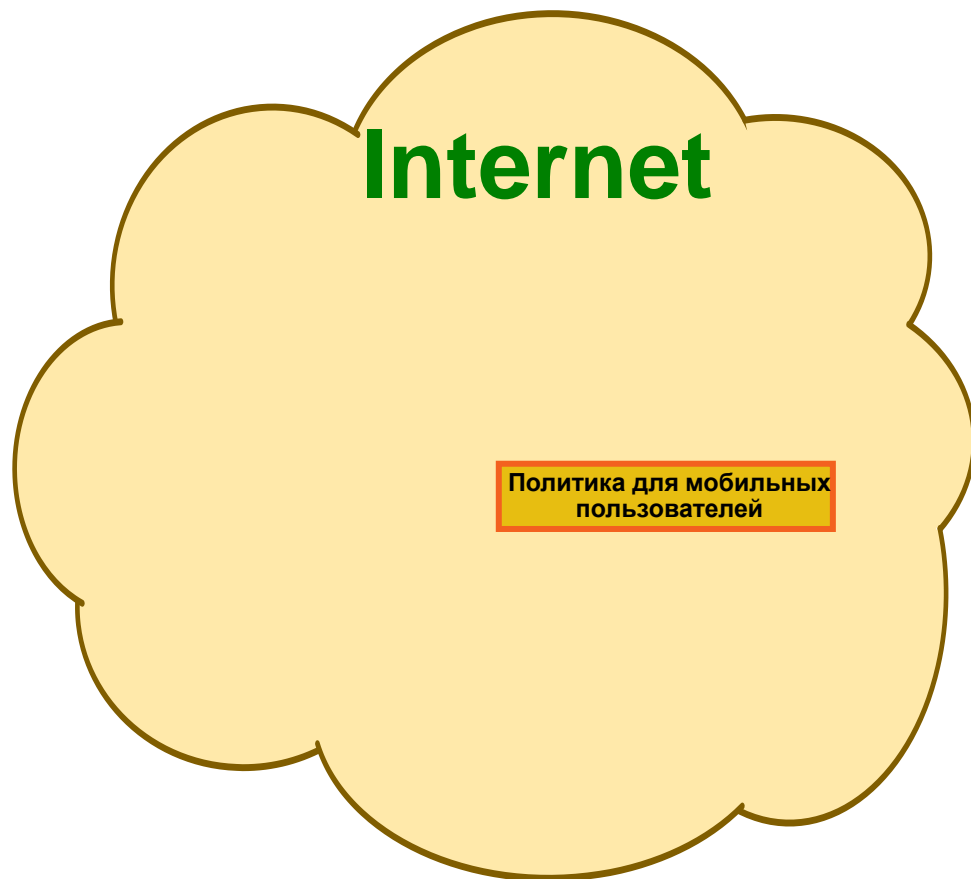


**Возможность задать
несколько учётных записей
для выполнения задачи
удалённой установки**



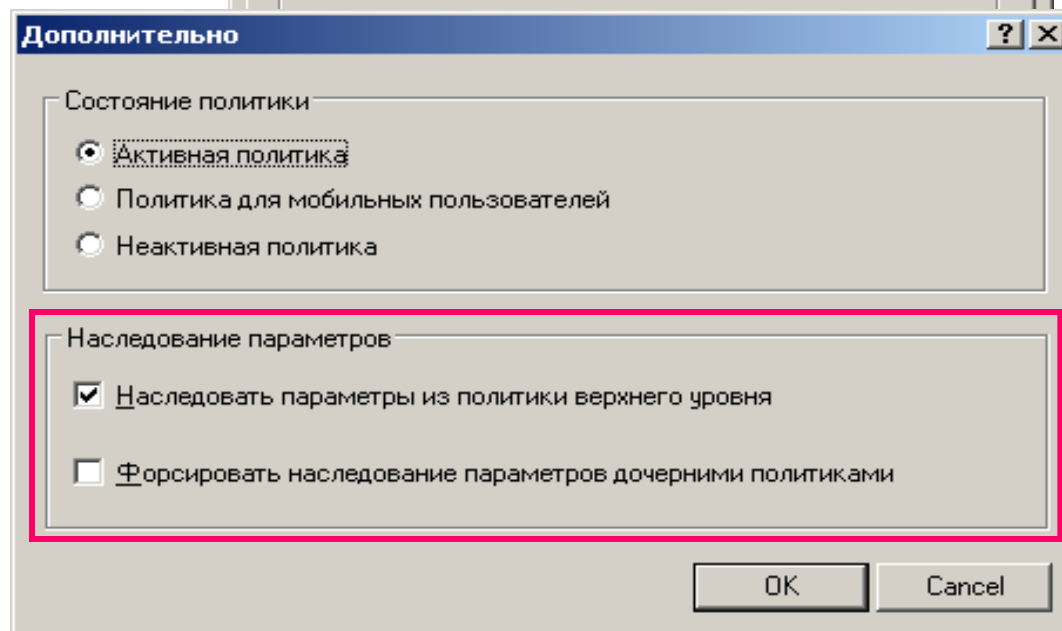
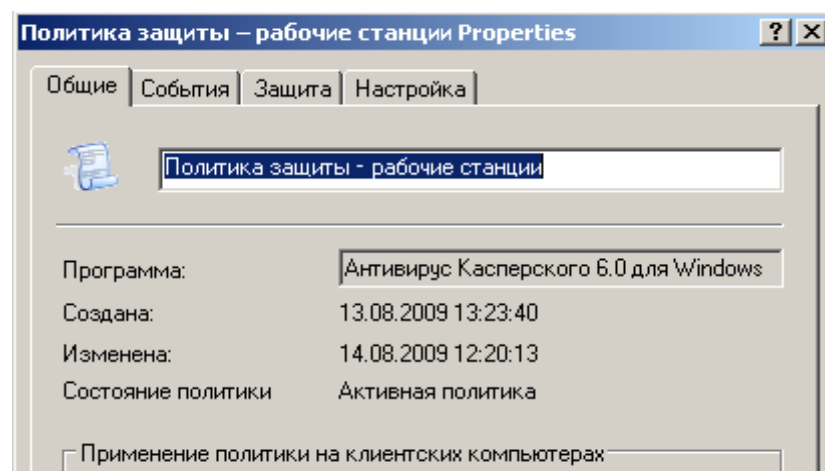


Активирована
полностью

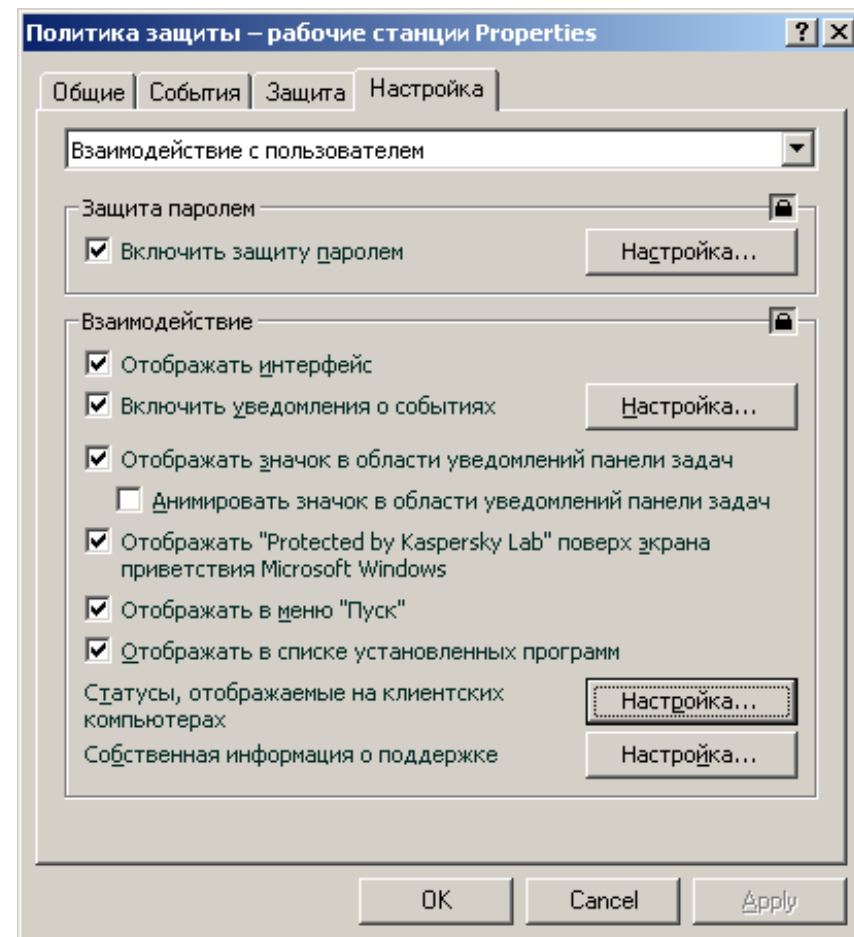




Возможность управления наследованием политик



**Возможность задавать
различные варианты
визуализации приложения
для пользователя**



Информация о состоянии антивирусной защиты и настройка уведомлений

The screenshot displays the Kaspersky Administration Kit (KASP) interface. The main window is titled "Kaspersky Administration Kit" and features a menu bar with "File", "Action", "View", and "Help". On the left, a tree view shows the administrative structure, including "Сервер администрирования - CL11", "Управляемые компьютеры", and "Отчеты и уведомления". The main content area is divided into three tabs: "Статистика", "Отчеты", and "Уведомления". The "Уведомления" tab is active, showing a diagram of the notification process. The diagram includes three main components: "Источники событий" (Sources of events), "Сервер администрирования" (Administration server), and "Доставка уведомлений" (Notification delivery). "Источники событий" is represented by a laptop icon and describes events generated by Kaspersky programs. "Сервер администрирования" is represented by a server tower icon and describes events stored in the database. "Доставка уведомлений" is represented by an envelope icon and lists delivery methods: email, network (NET SEND), file execution, and SNMP. Below the diagram, a "Политики" (Policies) section explains that storage and delivery parameters are defined in policies. At the bottom, the "Управление событиями" (Event management) section provides four actionable links: "Изменить параметры доставки уведомлений", "Изменить параметры событий Антивируса Касперского для Windows Workstations", "Изменить параметры событий Антивируса Касперского для Windows Servers", and "Изменить параметры событий Сервера администрирования". The status bar at the bottom indicates "Отчетов: 11" and "Расширенный / Standard /".

Статистика | **Отчеты** | **Уведомления**

Начало работы » Отчеты и уведомления

Источники событий
События формируются программами "Лаборатории Касперского" и доставляются на Сервер администрирования.

Сервер администрирования
События сохраняются в базе данных и могут инициировать отправку уведомлений.

Доставка уведомлений
Уведомления могут рассылаться:

- по электронной почте;
- по сети (NET SEND);
- запуском исполняемого файла;
- через SNMP.

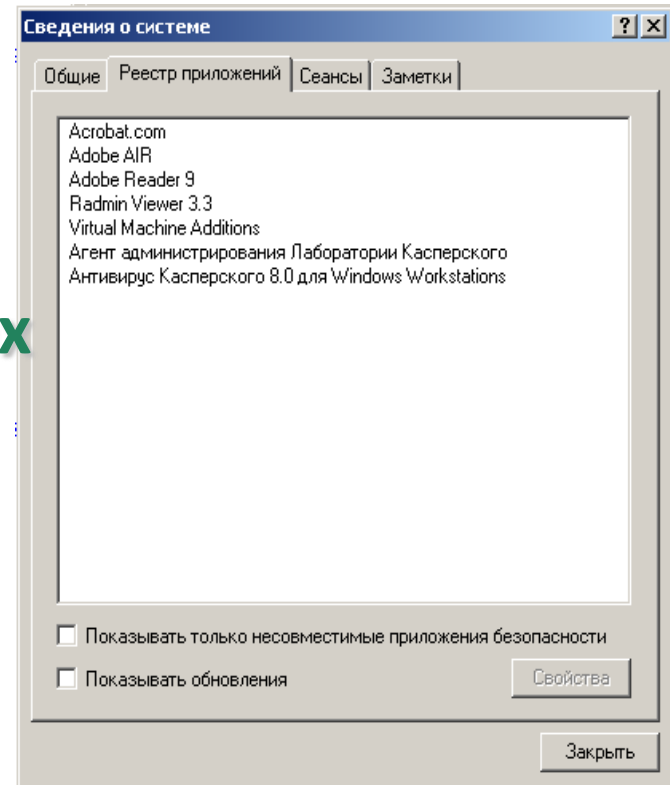
Политики
Параметры хранения событий и отправки уведомлений содержатся в политиках.

Управление событиями

- ▶ Изменить параметры доставки уведомлений
- ▶ Изменить параметры событий Антивируса Касперского для Windows Workstations
- ▶ Изменить параметры событий Антивируса Касперского для Windows Servers
- ▶ Изменить параметры событий Сервера администрирования

Отчетов: 11 | Расширенный / Standard /

Ведение реестра приложений на компьютерах сети



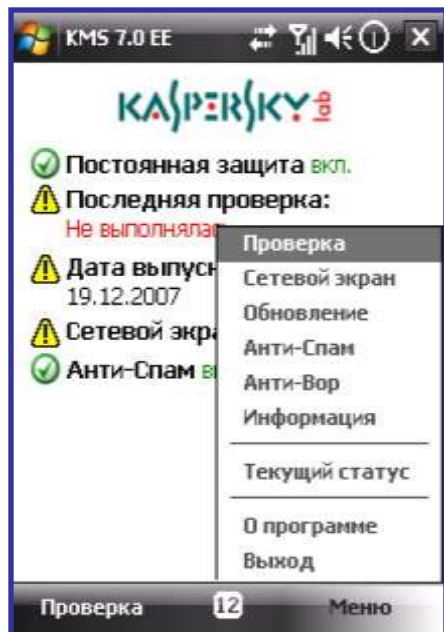


Review of IT Security Suites for Corporate Users, 2009

Installation Wizard	★★★★
User Navigation	★★★★★
Administrator console	★★★★
Default Values	★★★★
MS Active Directory Support	★★★★
Database Support	★★★★★
Remote Installation	★★★★★

- Удобные мастера установки и настройки
- Быстрая установка защиты
- Понятное средство администрирования
- **Не понадобилось «Руководство пользователя»**

Small Networks (0-50 Users)	Medium Networks (50-500 Users)	Large Networks (500-? Users)
★★★★★	★★★★★	★★★★★



Защищает от

- Вирусов
- Спама
- Сетевых атак
- Последствий кражи

Поддерживаемые ОС:

- Windows Mobile 5.0, 6.0, 6.1
- Nokia Symbian OS 9.1, 9.2, 9.3 series 60 3rd



Централизованная установка и управление с помощью
Kaspersky Administration Kit



А дальше?!

Детектирование уязвимостей

Полная проверка

Область действия: **Дополнительно** | Режим запуска

Методы проверки:

- Сигнатурный анализ
- Эвристический анализ

Глубина проверки: поверхностный | **средний** | глубокий

Сигнатурный поиск уязвимостей

Поиск руткитов

Углубленный анализ

Технологии проверки:

- Технология iSwift
- Технология iChecker

Время	Статус
Тип: уязвимость (событий: 3)	
15.03.2009 0:20:31	Обнаружено у
15.03.2009 0:20:31	Обнаружено у
15.03.2009 0:20:32	Обнаружено у

Справка | OK | Отмена

CVE-ID	CVE-2008-2244
Опубликовано	09 июл 2008
Обновлено	12 авг 2008
Опасность	■■■■■
Статус решения	Исправлена патчем от производителя
Уязвимые приложения	Microsoft Office 2003 Professional Edition Microsoft Office 2003 Small Business Edition Microsoft Office 2003 Standard Edition Microsoft Office 2003 Student and Teacher Edition Microsoft Office XP Microsoft Word 2002 Microsoft Word 2003
Источник атаки	Удалённый
Последствия	Доступ к системе Уязвимость позволяет злоумышленникам получить доступ к системе и выполнить произвольный код с привилегиями локального пользователя.
Описание	Более подробное описание уязвимости доступно на английской версии сайта .
Решение	Установить патчи. Microsoft Word 2002 SP3: http://www.microsoft.com/downloads/details.aspx?FamilyId=c7146dfc-e1be-4d13-877b-1d9bcacc4a64 Microsoft Word 2003 SP2: http://www.microsoft.com/downloads/details.aspx?FamilyId=13a37b76-9fec-426f-8176-3c95f934efe0 Microsoft Word 2003 SP3: http://www.microsoft.com/downloads/details.aspx?FamilyId=13a37b76-9fec-426f-8176-3c95f934efe0

Одноклассники.ру - Поиск одноклассников, однокурсников, бывших выпускников и старых друзей - Windows Internet Explorer

http://www.odnoklasniki.ru/ Поиск "Live Search"

Файл Правка Вид Избранное Сервис Справка

Одноклассники.ру - Поиск однокласн...

Страница Сервис

Kaspersky
Anti-Virus 8.0 for Windows Workstations

ACCESS DENIED

The requested URL could not be retrieved

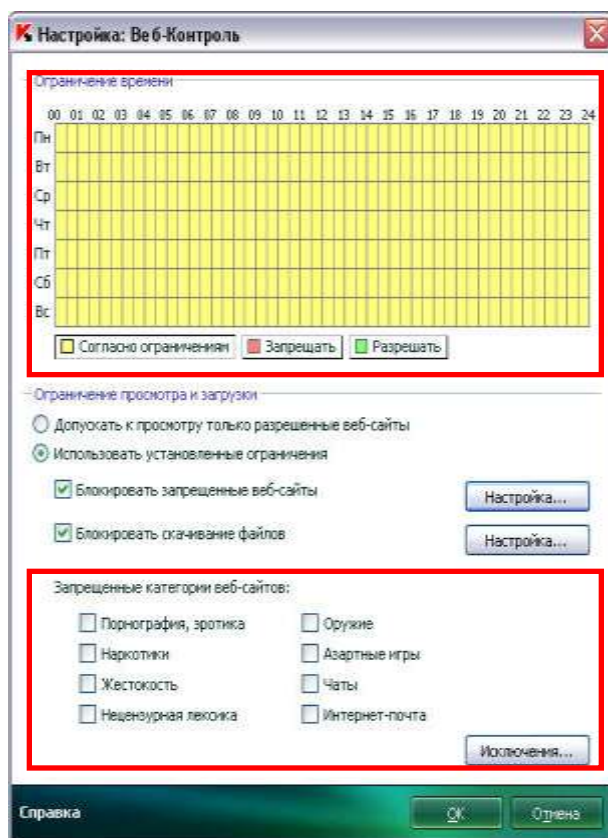
The requested URL:
http://www.odnoklasniki.ru/

Is forbidden by Internet Control

Reason: Black list

Generated:
Fri Oct 31 17:25:02 2008
Kaspersky Anti-Virus 8.0 for Windows Workstations

http://www.odnoklasniki.ru/cdk/st.cmd/main/st.categoryId/1/st.locationId/10412411465/tkn/4995 Интернет 100%



Централизованный контроль доступа к интернету и блокировка загрузки файлов определенного содержания и расширения



И МНОГОЕ ДРУГОЕ

A circular inset on the left side of the slide shows a microscopic view of a cell, with a silver rim and a green-tinted interior containing various organelles.

Благодарю за внимание! Вопросы?

Евгений Лужнов

Инженер предпродажной поддержки

Evgeny.Luzhnov@ru.kaspersky.com