Продукты Лаборатории Касперского для защиты корпоративных сетей

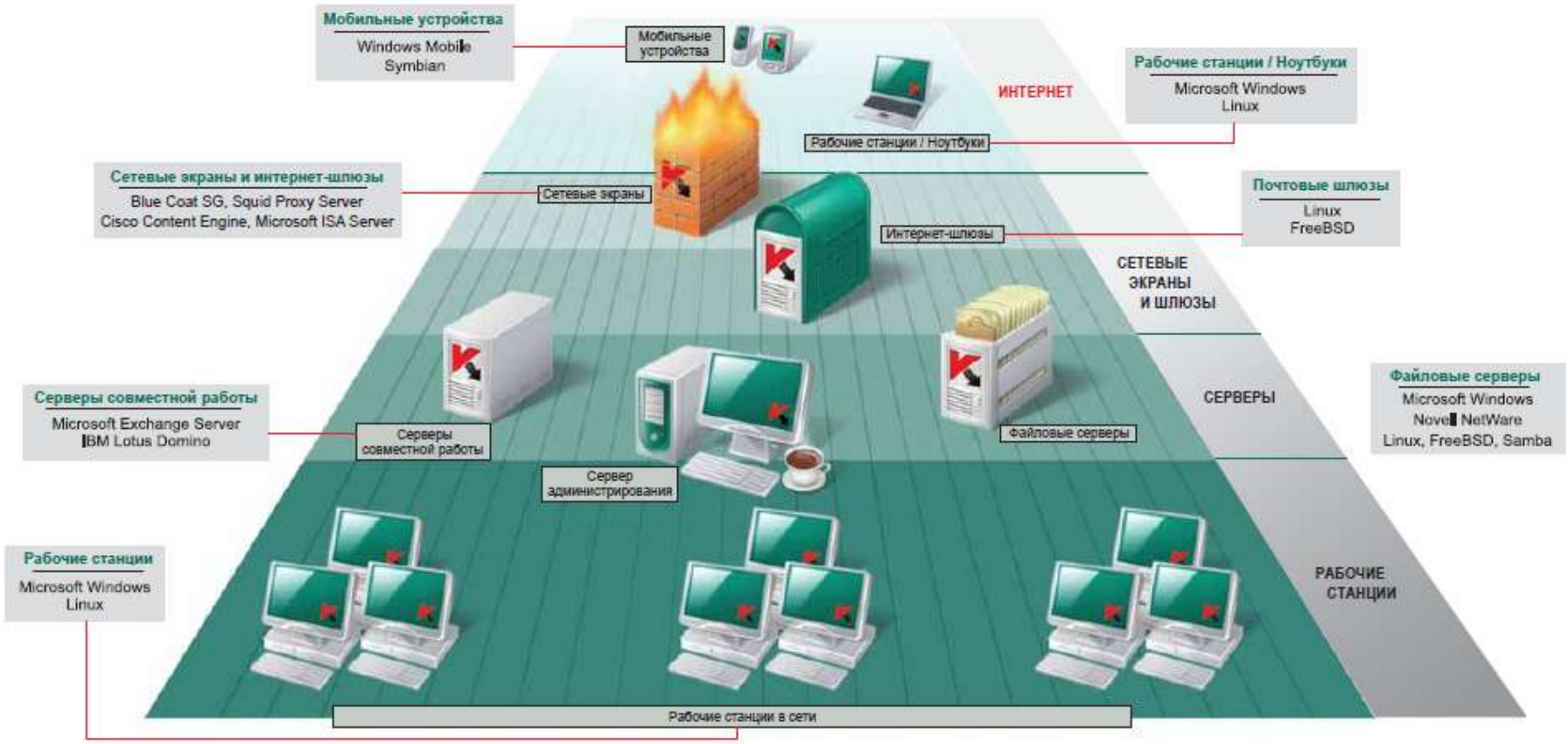
Евгений Лужнов
Инженер предпродажной поддержки
Evgeny.Luzhnov@ru.kaspersky.com

Рост количества вредоносных программ в коллекции

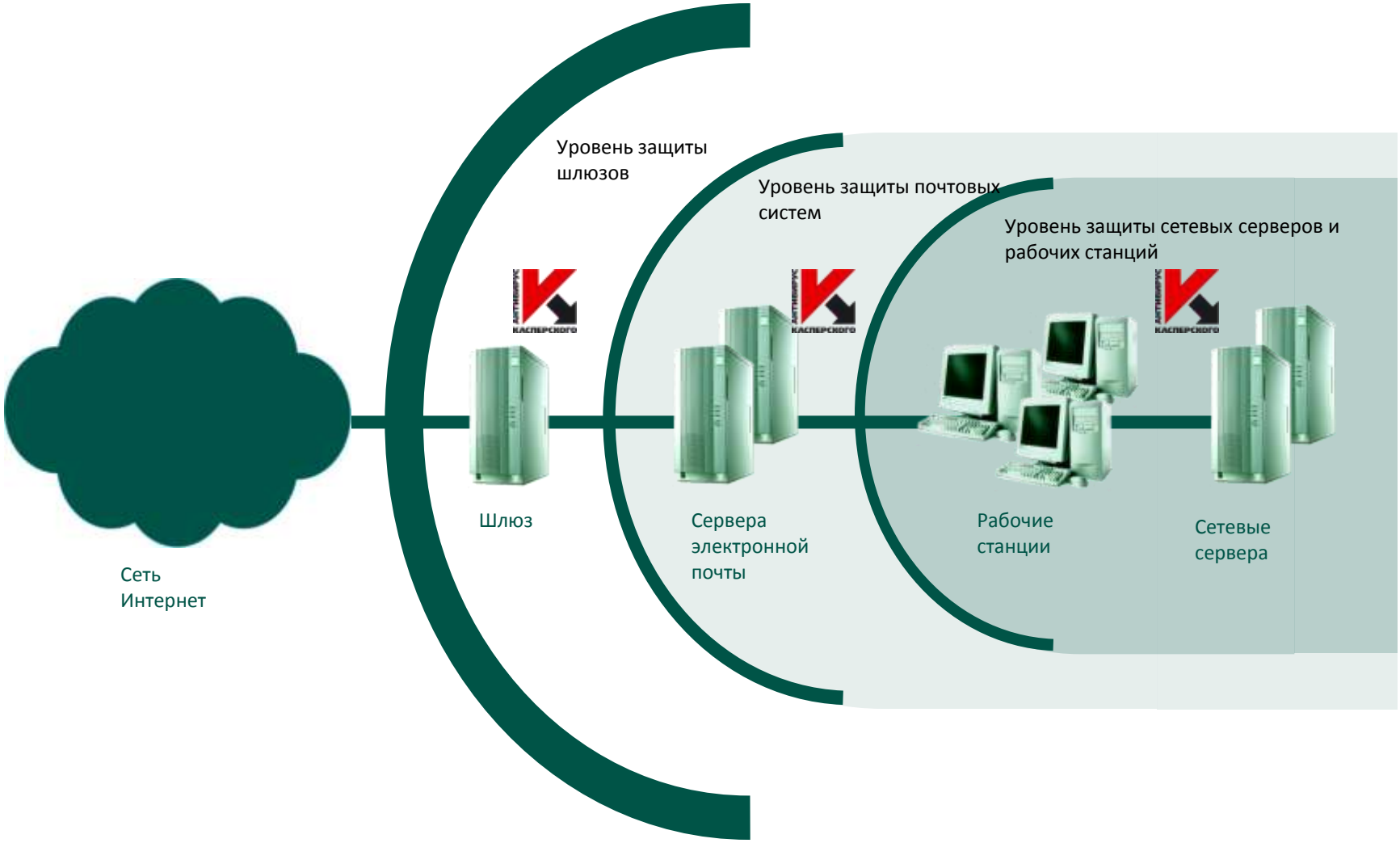
Динамика роста количества угроз

Современная корпоративная сеть

лаборатория Касперского



Многоуровневая защита



Требования к защите корпоративной сети

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

Защита интернет-шлюзов

- Kaspersky Security для интернет-шлюзов
  - Антивирус Касперского для Proxy Server
  - Антивирус Касперского для Check Point FireWall-1
  - Антивирус Касперского для Microsoft ISA Server

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

Антивирус Касперского для Check Point FireWall-1

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)

Антивирус Касперского для Microsoft ISA Server

- **Антивирусная проверка в режиме реального времени.**
- **Выявление потенциально опасного ПО.**
- **Передовые технологии.**
- **Защита масси**
  Enterprise Ed
- **Запуск неско**
- **Выбор прове**
- **Настройка гр**
- **Оптимизация**
- **Централизов**
- **Система оповещений и отчетности.**
- **Автоматические обновления.**

- Microsoft ISA Server 2006 Enterprise Edition SP1
- Microsoft ISA Server 2006 Standard Edition SP1
- Microsoft ISA Server 2004 Standard Edition
- Microsoft ISA Server 2004 Enterprise Edition
- Microsoft ISA Server 2000 Standard Edition
- Microsoft ISA Server 2000 Enterprise Edition

Защита почтовых серверов

- 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.

Антивирус Касперского для Linux Mail Server
Kaspersky Mail Gateway

- **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

Защита сетевых серверов

- 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**

Обновленные приложения

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

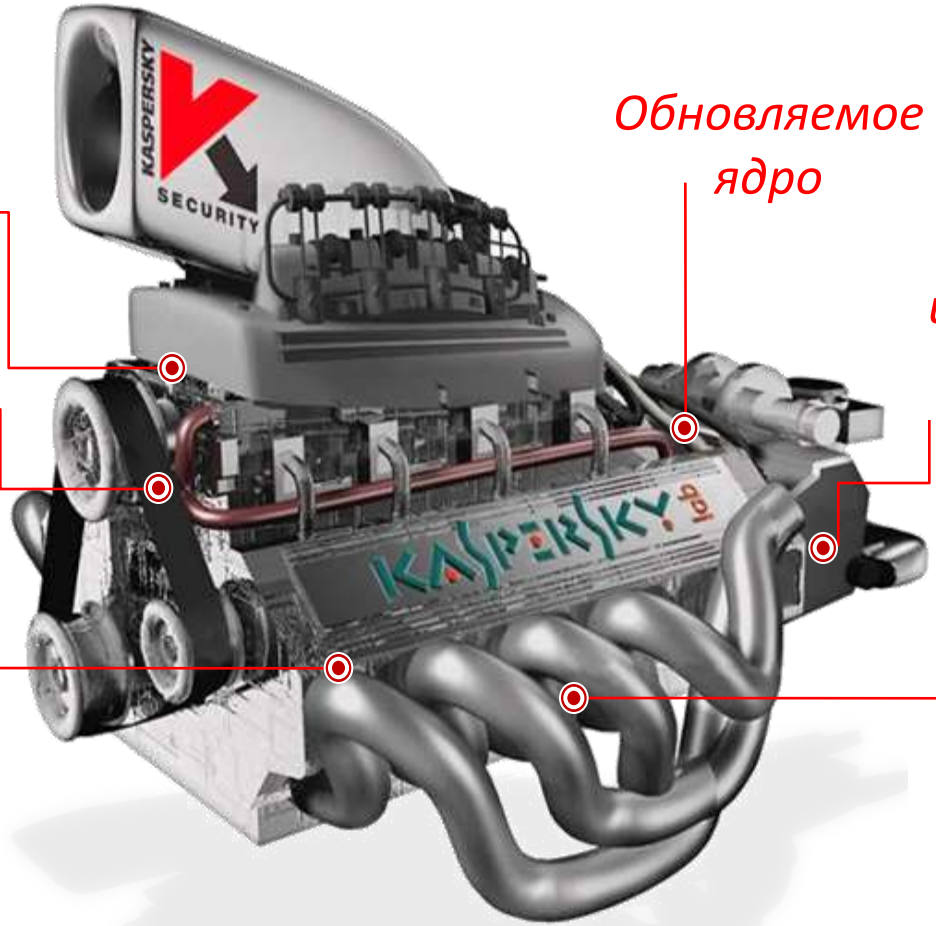
лаборатория КАСПЕРСКОГО

Обновляемый анти-руткит

Обновляемое ядро

Оптимизация использования системных ресурсов

Быстрее!



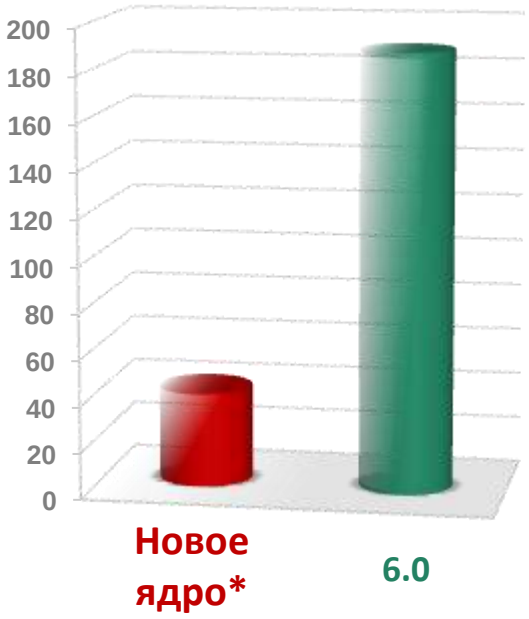
Глубокая интеграция проактивных технологий

Поддержка многоядерных процессоров

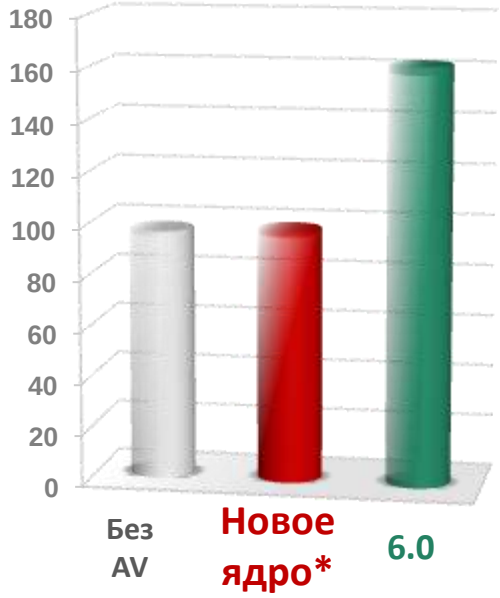
Оценка производительности нового ядра

лаборатория Касперского

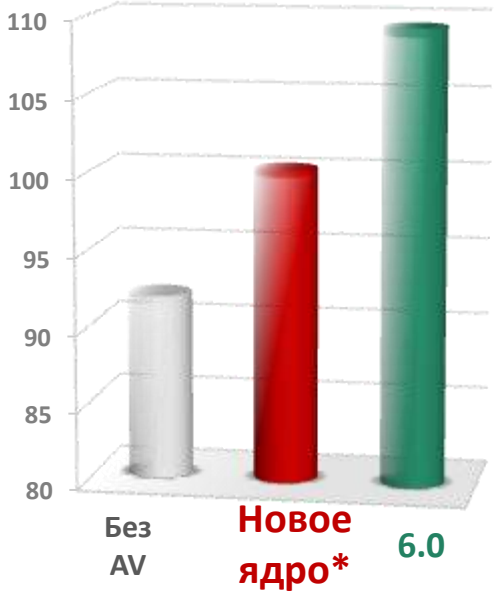
Время сканирования (сек.)



Скорость загрузки системы (сек.)

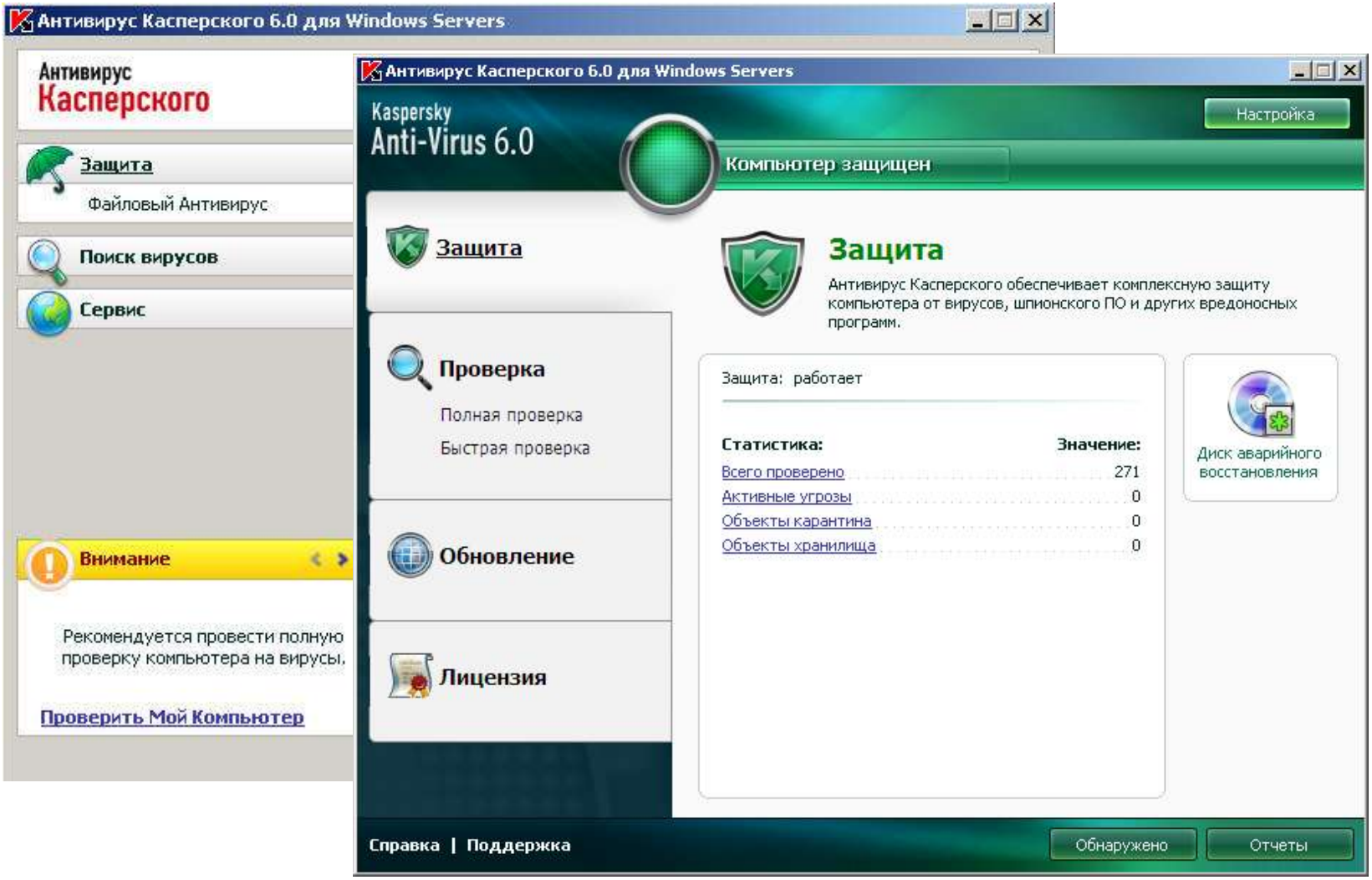


Время копирования файлов (сек.)



* Данные на примере Kaspersky Internet Security

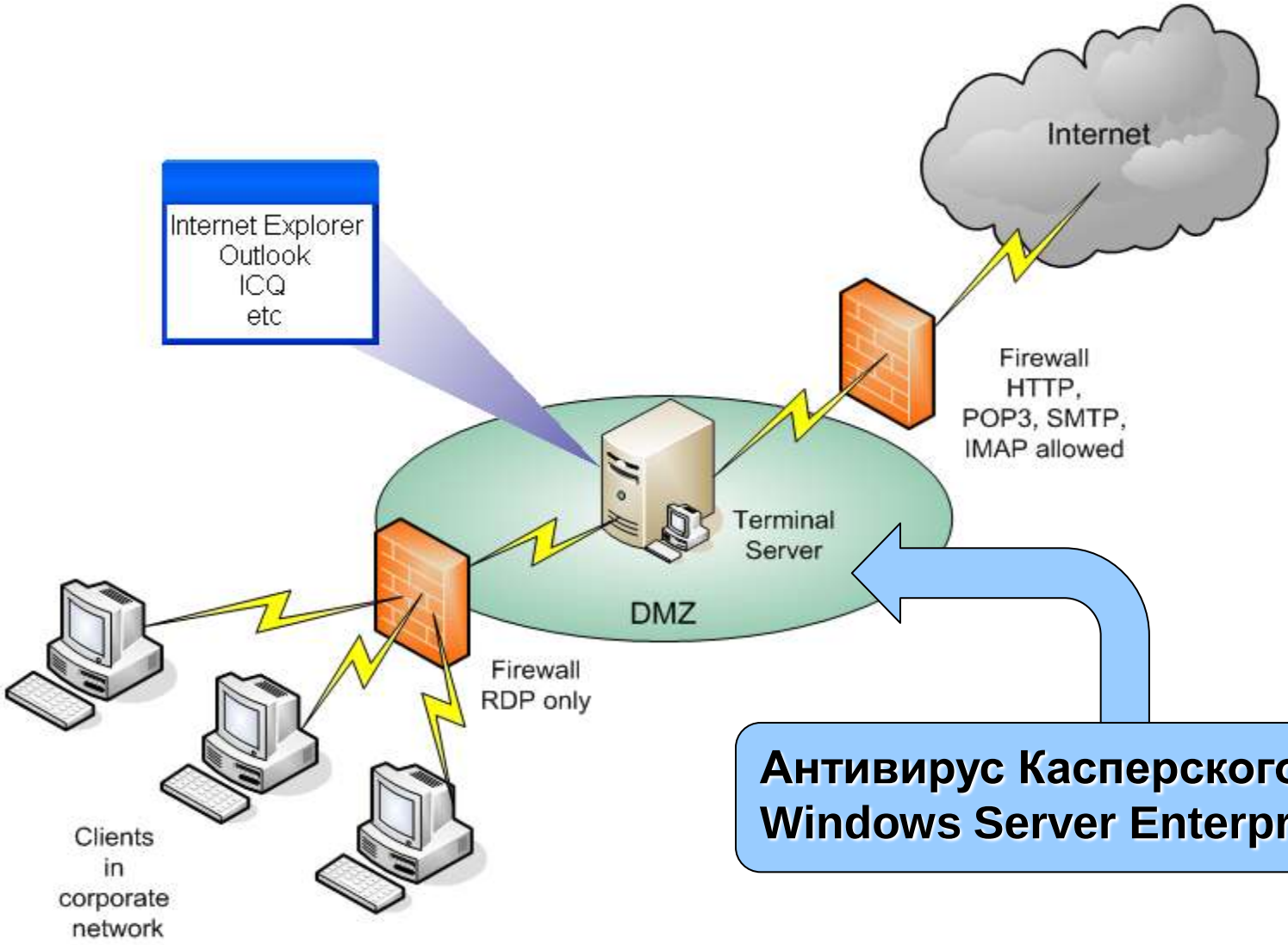
KAV для Windows Server



KAV 6.0 R2 для Windows Server

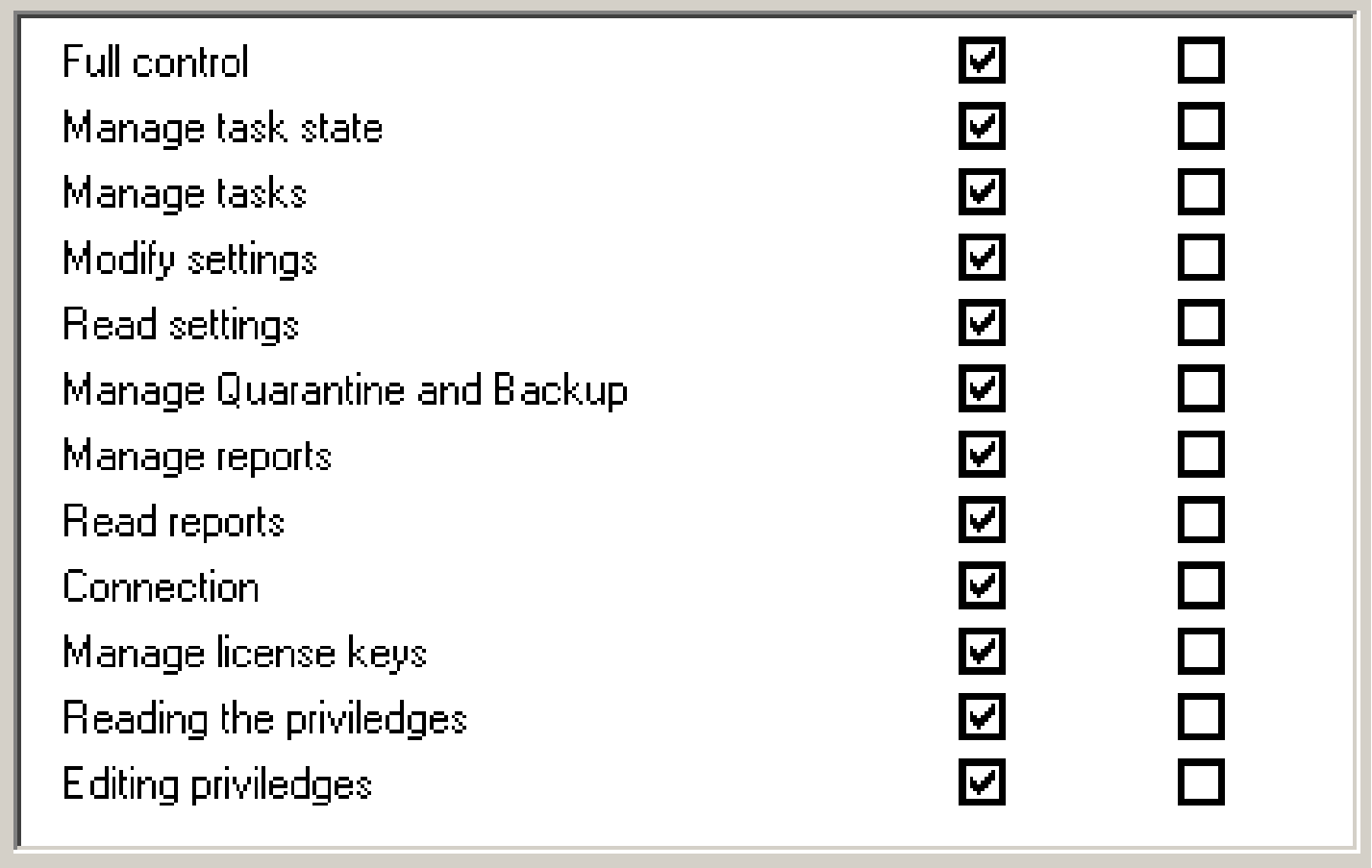
- Сетевой iSwift
- Несколько экземпляров нового антивирусного ядра
- Распределение нагрузки на процессоры
- Приостановка сканирования
- Блокирование доступа зараженным компьютерам
- Эвристический анализатор. Новинка!
- Анти-руткит. Новинка!
- Гибкая настройка времени сканирования
- Настройка уведомлений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

Защита терминальных пользователей Enterprise Edition



Антивирус Касперского для Windows Server Enterprise Edition

Разграничение прав администраторов Enterprise Edition



Сравнение версий

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

Повышение уровня защиты

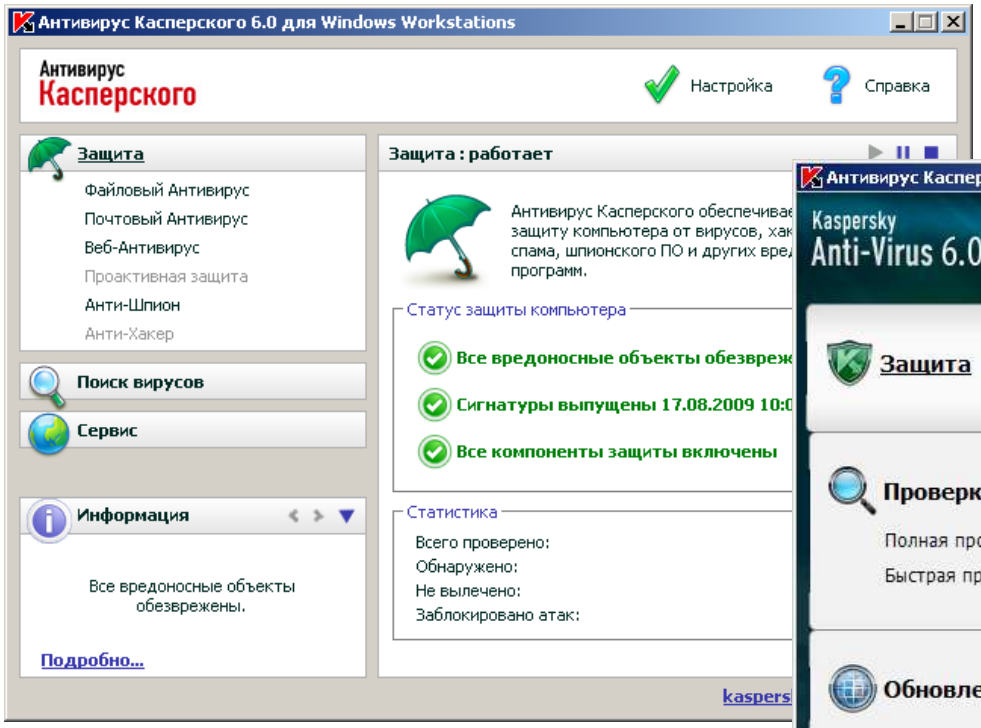
Поддержка платформ

Защита рабочих станций

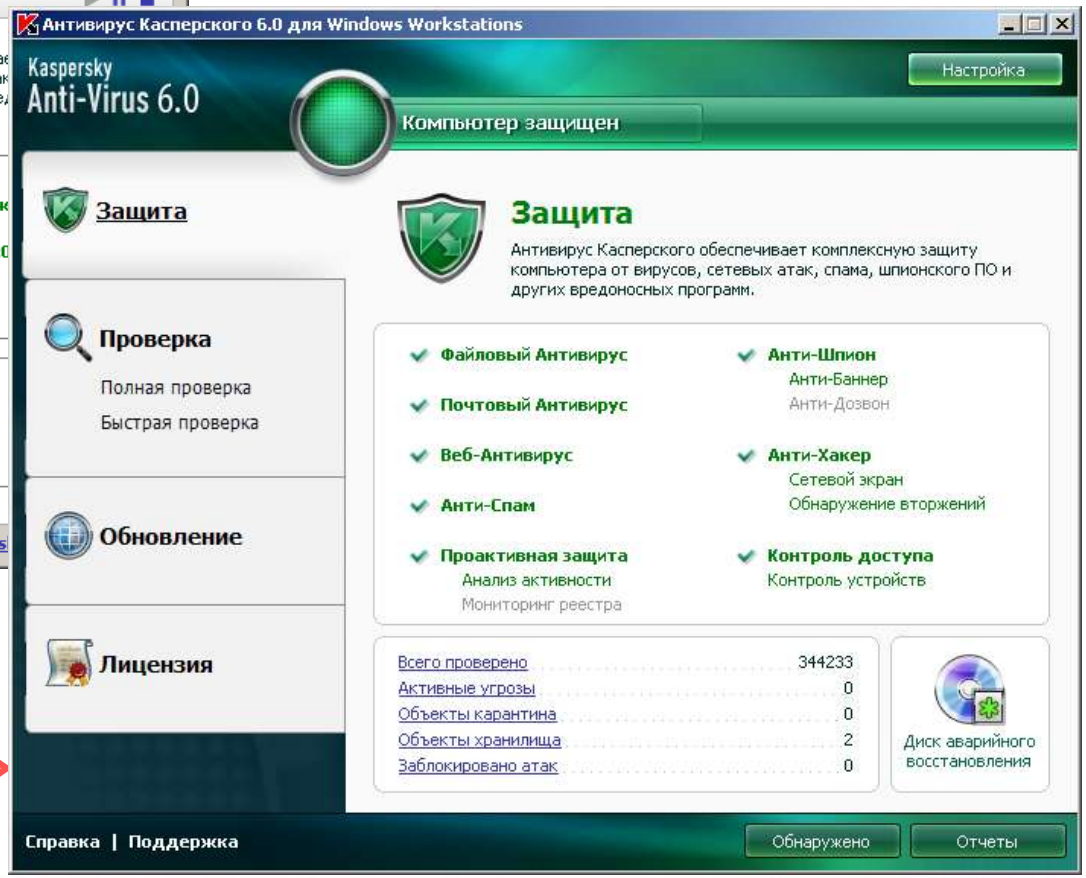
- Антивирус Касперского для Windows Workstation **6.0 R2**
- Антивирус Касперского для Linux Workstation
- Антивирус Касперского Second Opinion Solution **6.0 R2**

KAV 6.0 R2 для рабочих станций: Новый интерфейс

KAV 6.0 for WKS



KAV 6.0 R2 for WKS



Компонентная структура

Компоненты защиты

Файловый антивирус (улучшено!)

Веб-антивирус (улучшего!)

Почтовый антивирус (улучшено!)

Проактивная защита (улучшено!)

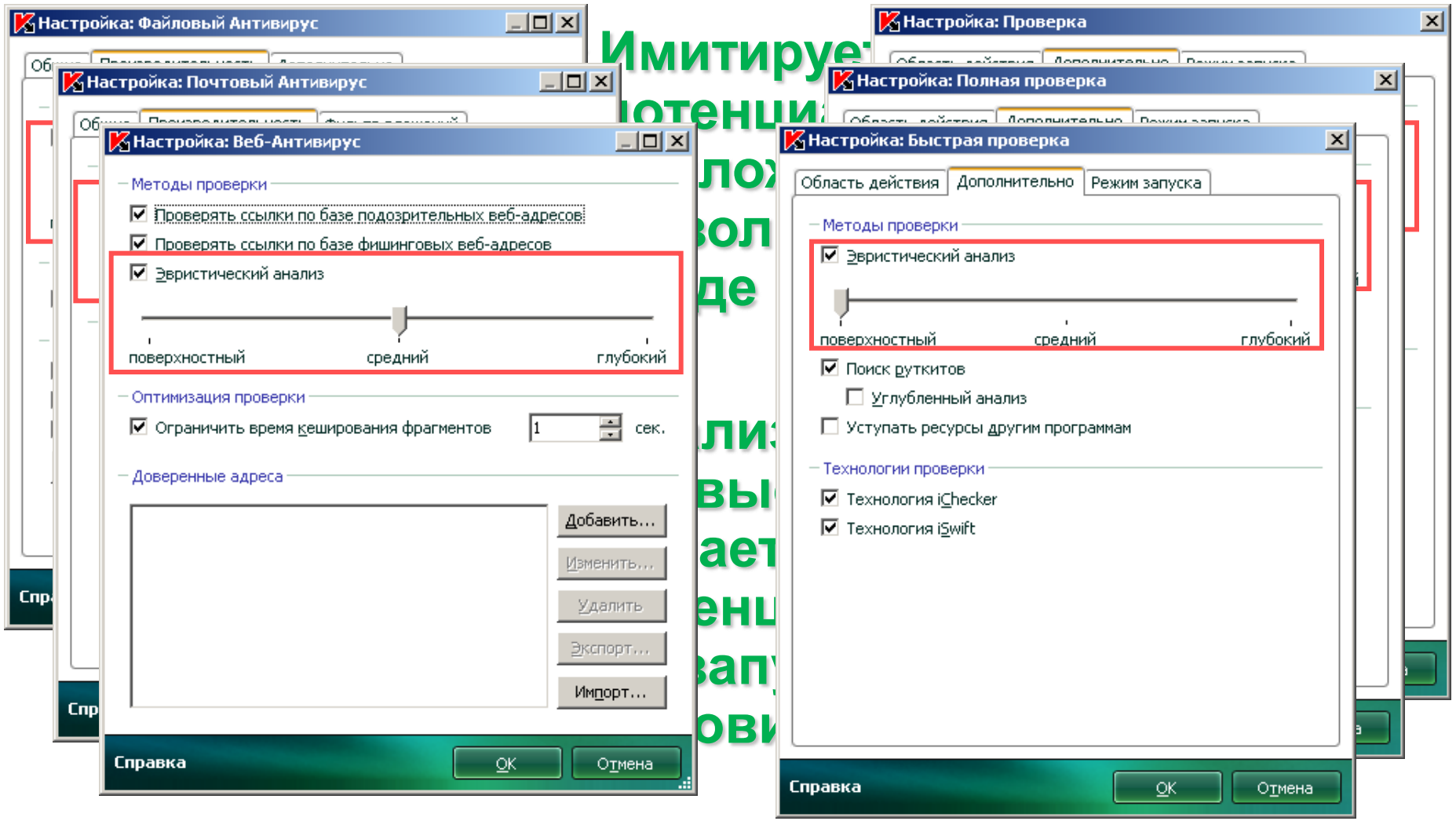
Анти-хакер (улучшено!)

Анти-спам (улучшено!)

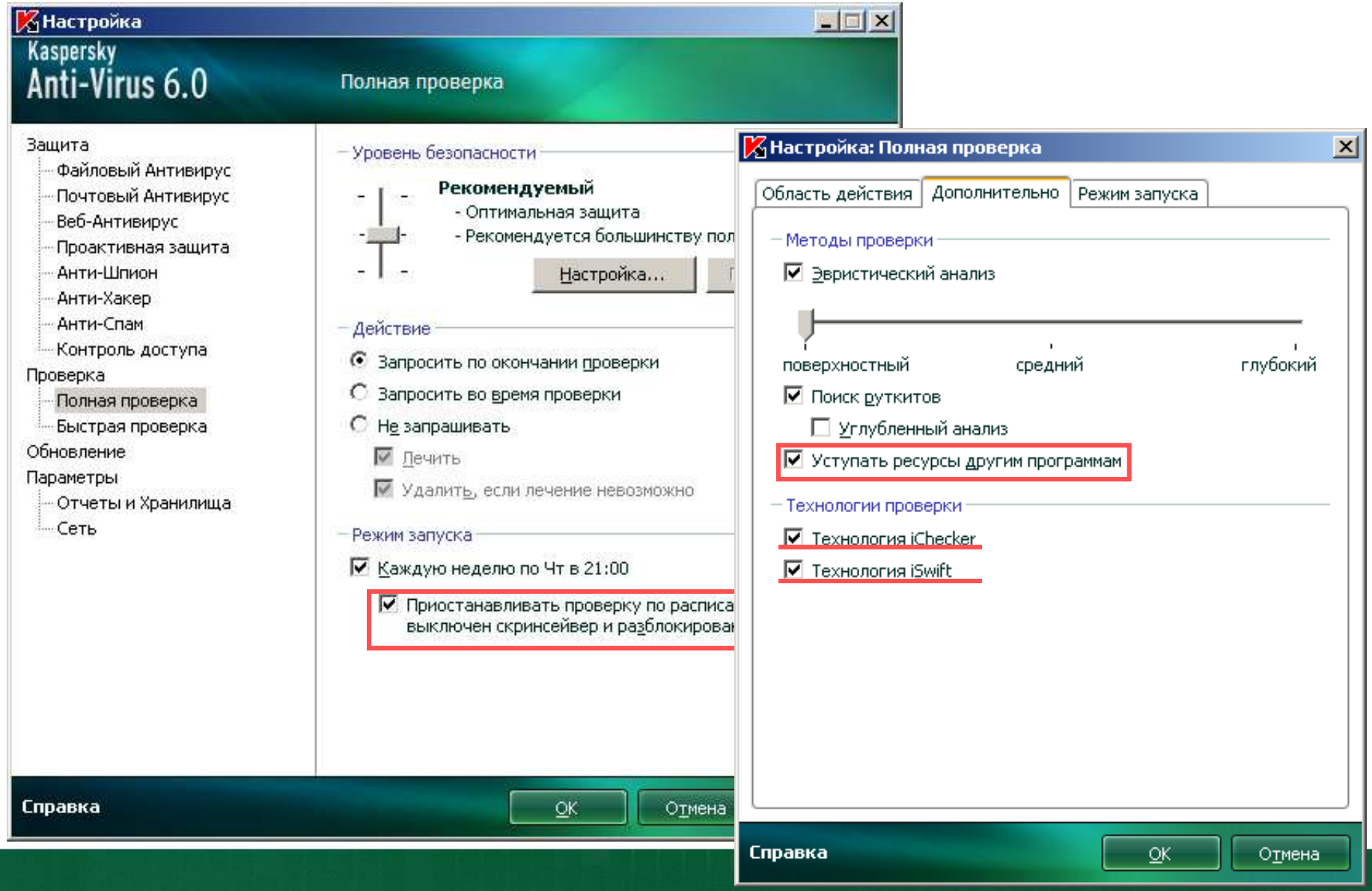
Контроль доступа (новое!)

Анти-шпион

Эвристический анализатор

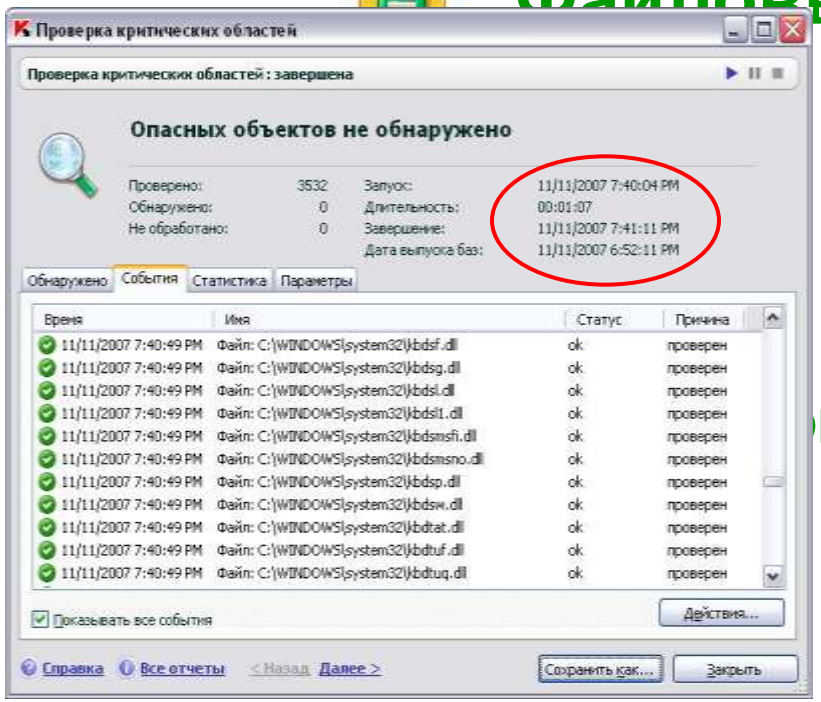


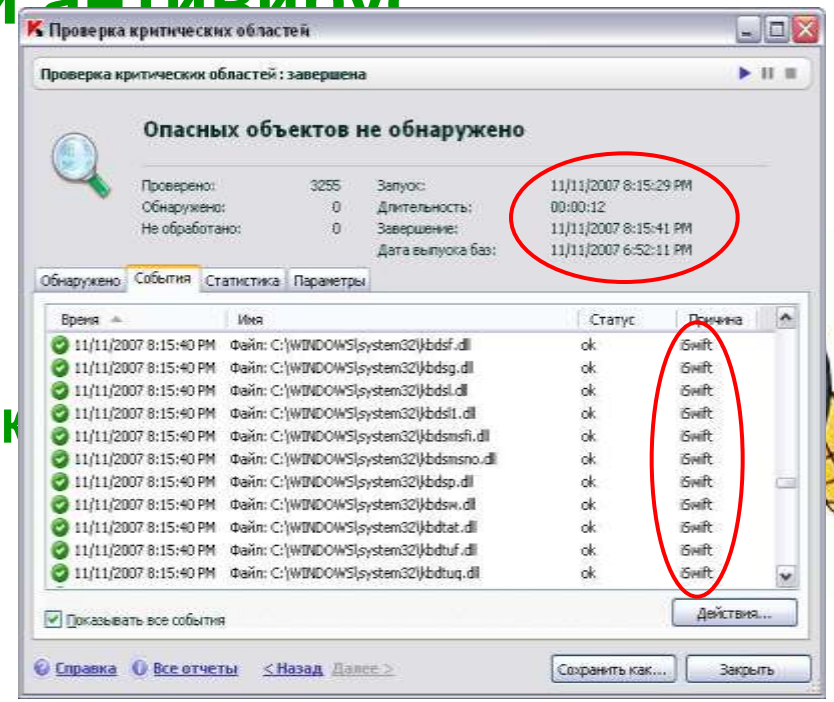
Оптимизация проверки по требованию



Скорость работы

Файловый антивирус





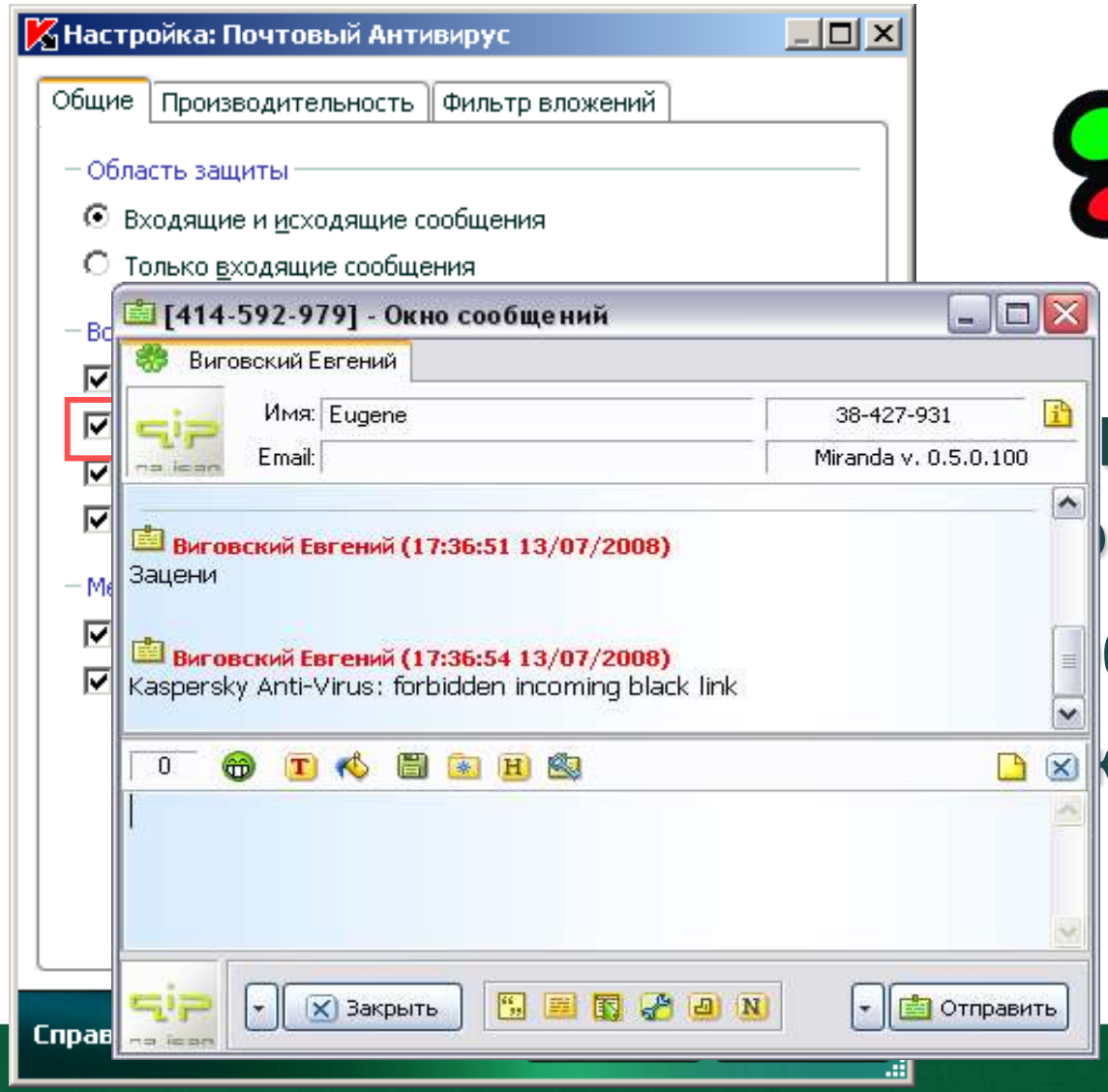
-
-
-

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



роверка на наличие

ишинга

бнаружение

ксплойтов

Почтовый антивирус

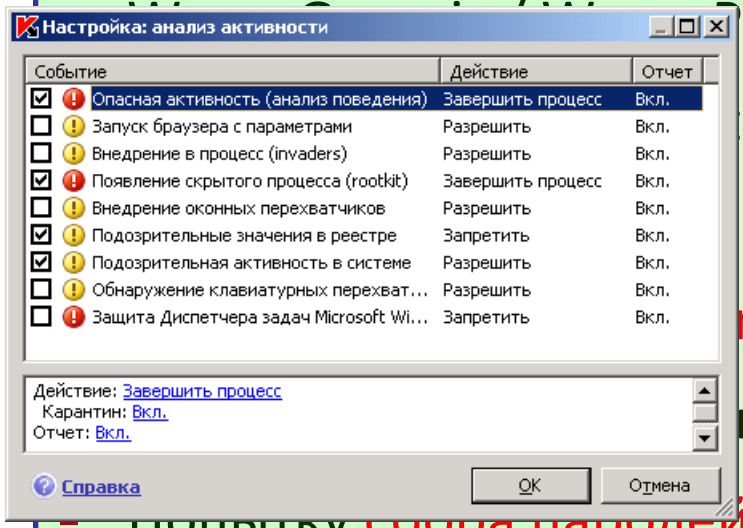
- Перехват почтового трафика SMTP, POP3, IMAP, NNTP (включая SSL)
- Независимо от протокола с помощью плагинов к почтовым клиентам Microsoft Outlook и The Bat!
- Возможность фильтрации и обработки вложений
- Лечение вирусов в почтовых базах Microsoft Outlook и Microsoft Outlook Express

Модуль проактивной защиты

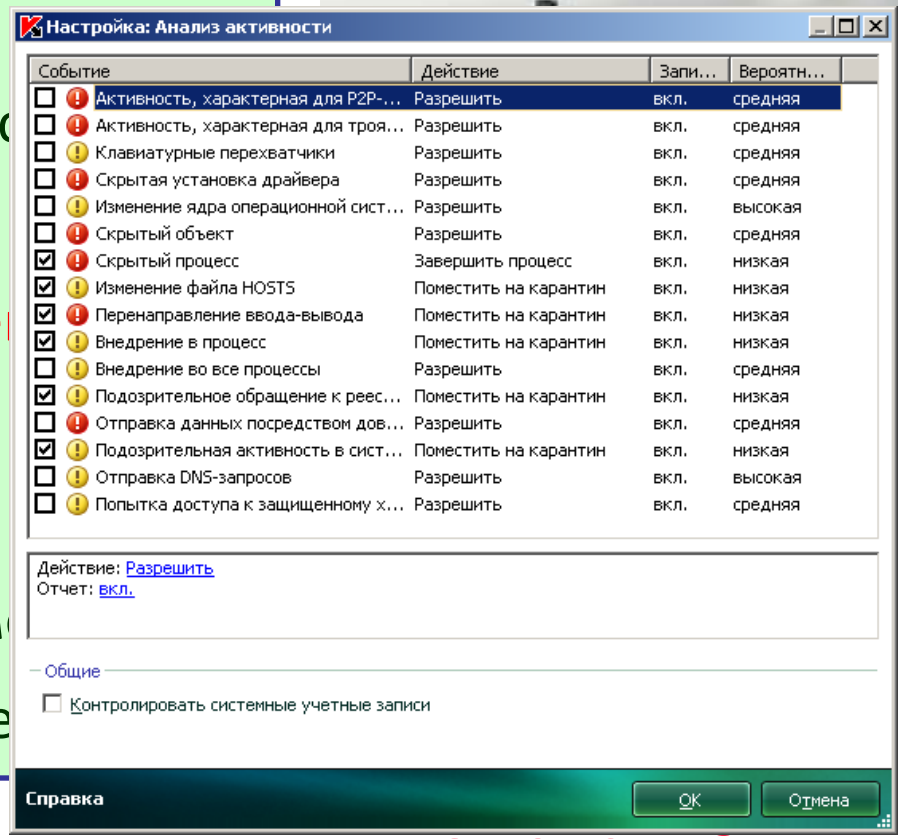
Проактивно блокирует

- Trojan.Generic / Trojan.Cryptor
- 2P.Generic
- kits)
- nvaders)
- ых
- Попытку собра паролей в систем
- Аномальное поведение приложе

PDM 6.0

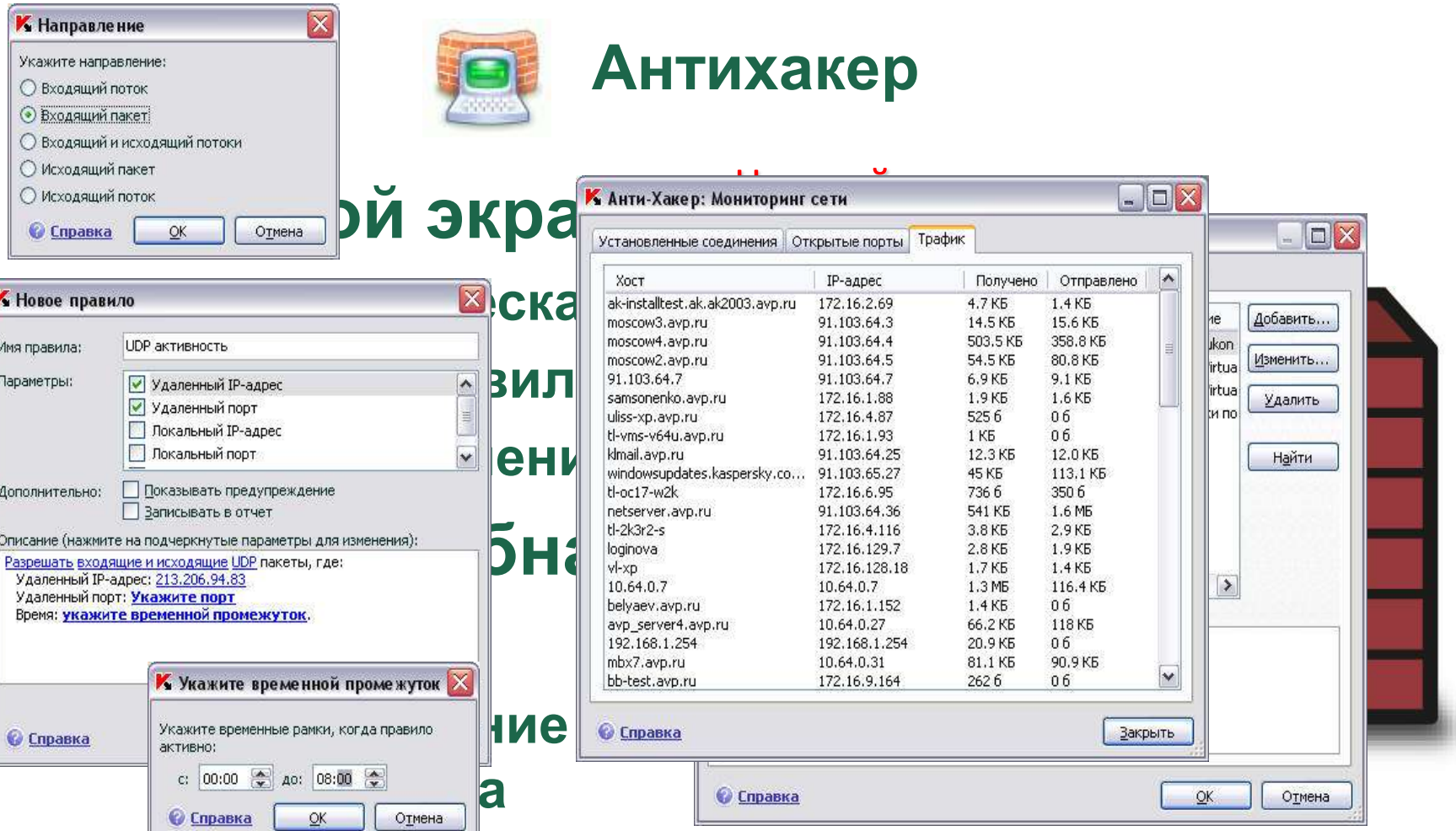


PDM 6.0 R2



изменений

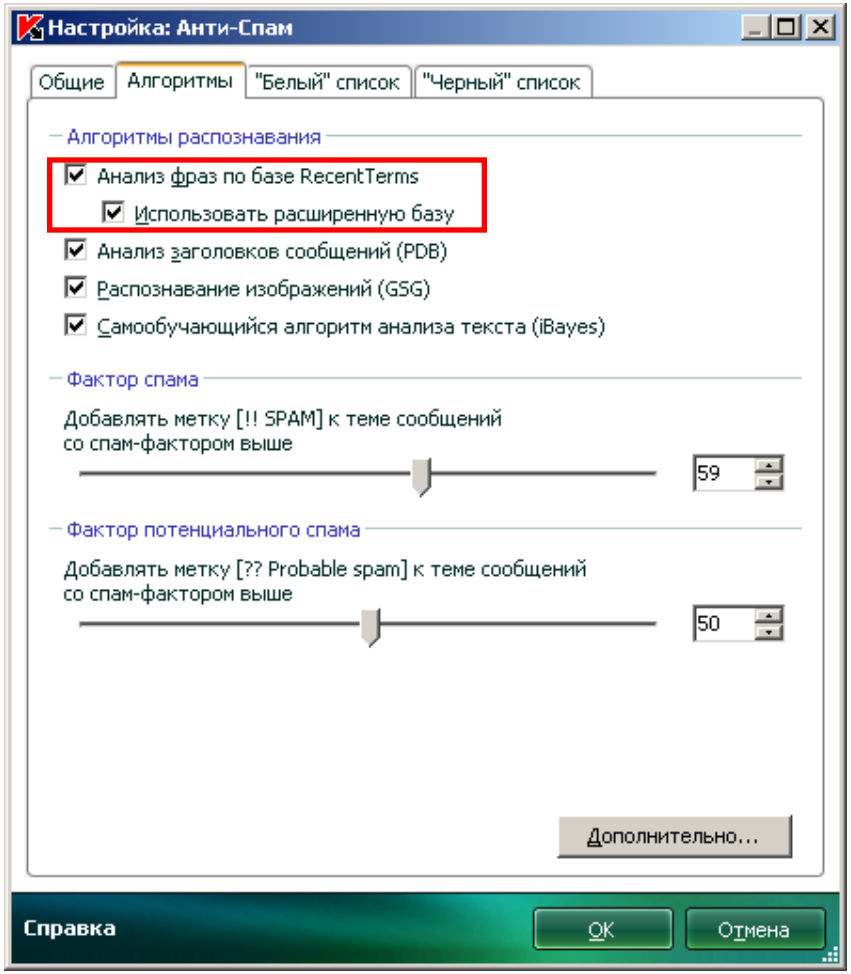
Защита рабочих станций



Антихакер

- Сетевой монитор

Персональный анти-спам



Аргументы и факты

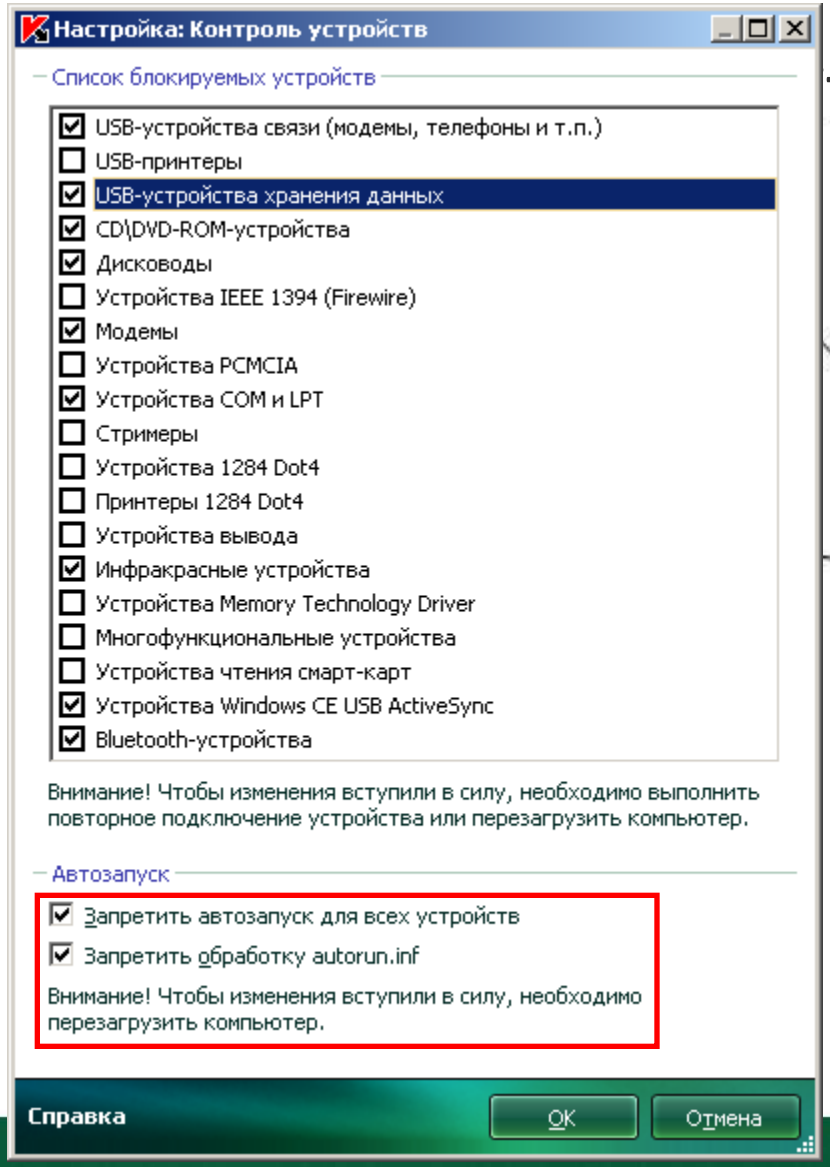
Билайн™

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**

Контроль устройств

t 8.0

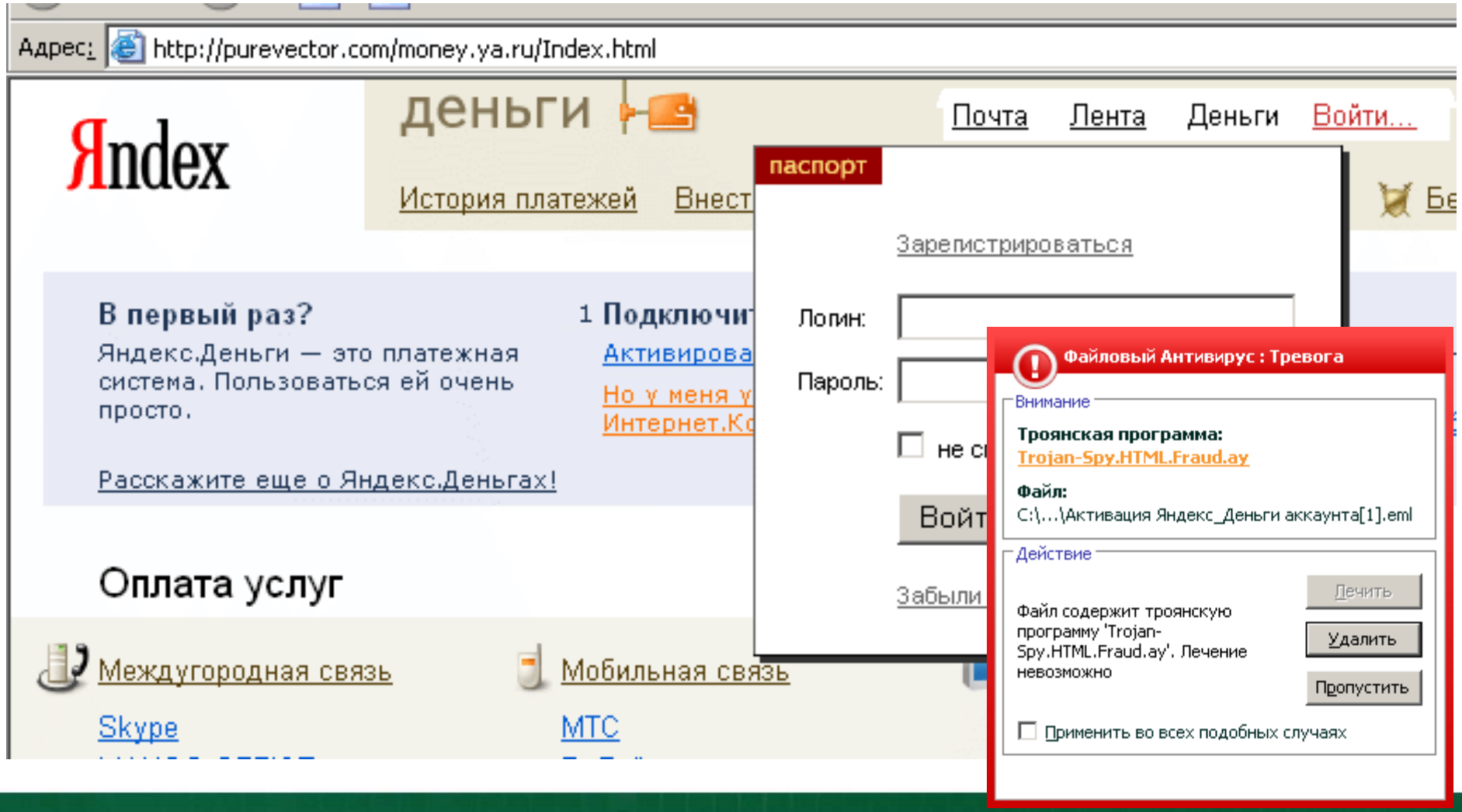


Антивирус Касперского 6.0 R2 для Windows Workstation

Антишпион

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

Фишинг Яндекс-денег

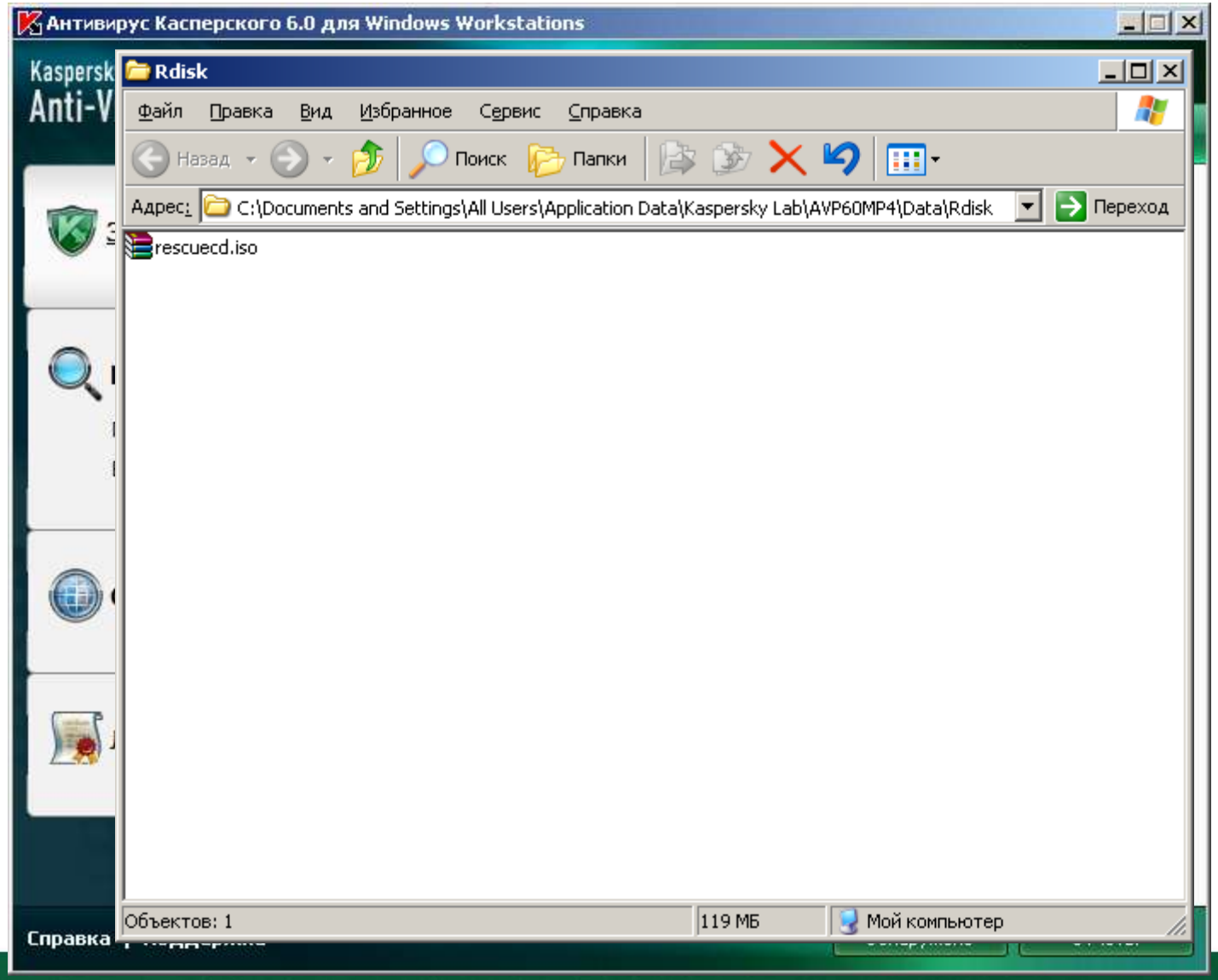


Улучшенный механизм обновления

- Инкрементальное обновление
- Улучшенный механизм обновления
- Обновляемое ядро **Новинка!**
- Обновляемый антируткит **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		✓

Требования к управлению AV защитой

- **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)

Аксиомы и следствия антивирусной безопасности

- 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

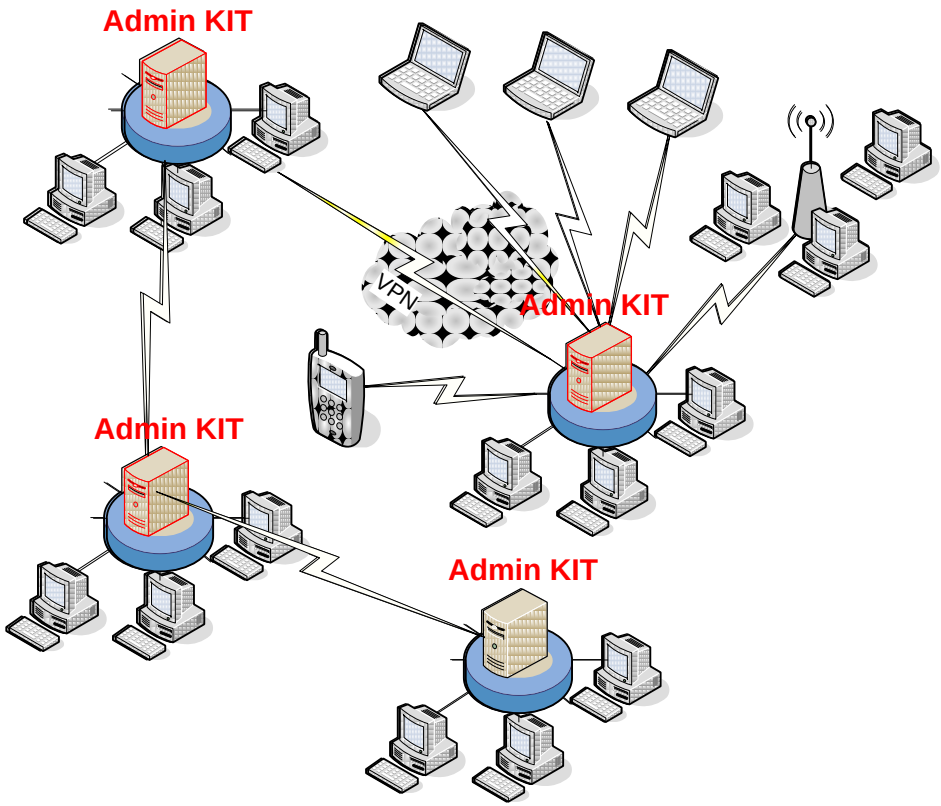
Аксиомы и следствия антивирусной безопасности

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

Kaspersky Administration Kit 8.0



Производительность - один сервер может поддерживать сеть из тысяч клиентов.

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

Connectivity – поддержка любых сетевых конфи-гураций 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	Простота установки и развертывания	✓
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	Полный контроль	✓
Информационные панели (Dashboards)		✓

Что нового? Сравнение версий

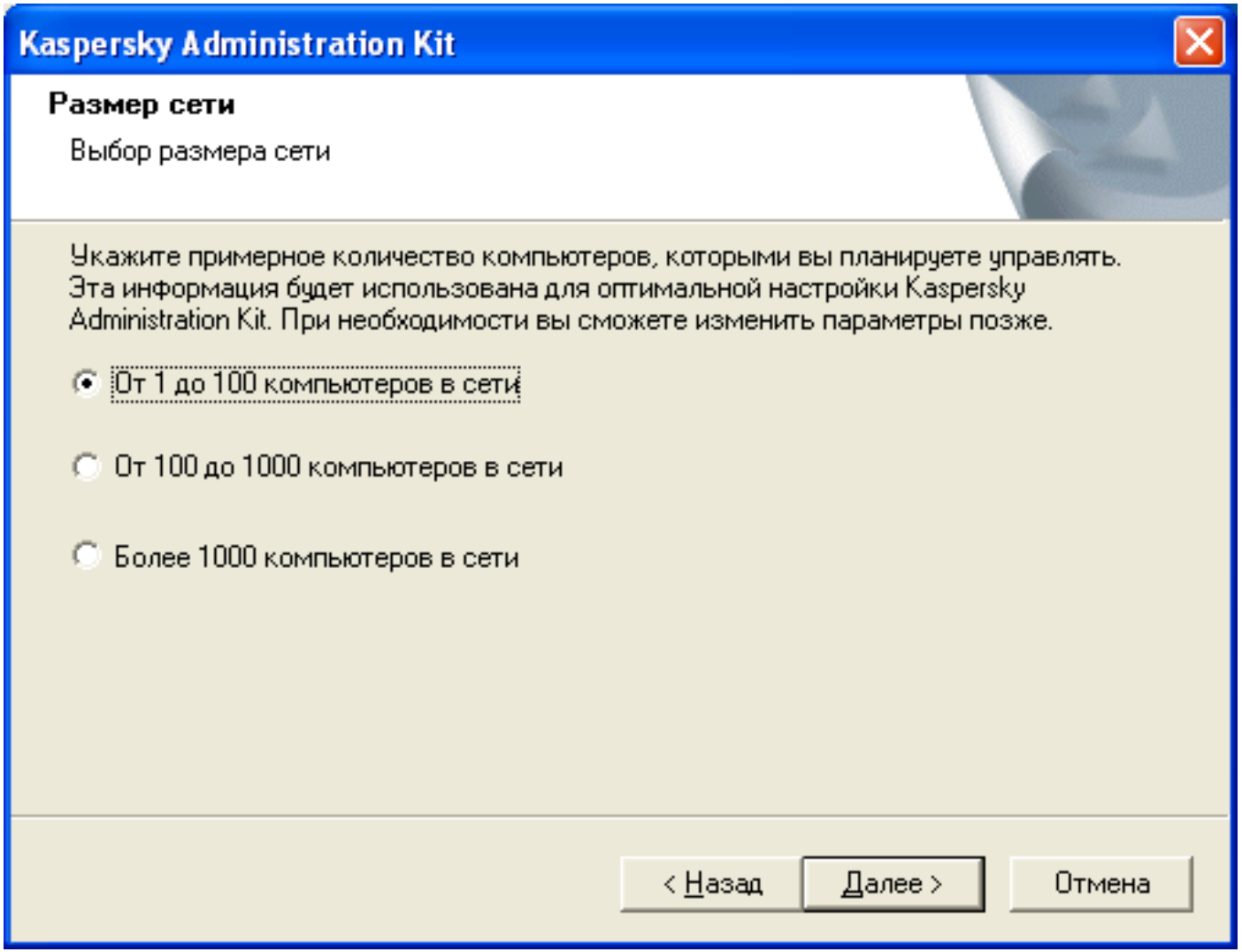
лаборатория Касперского

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		✓

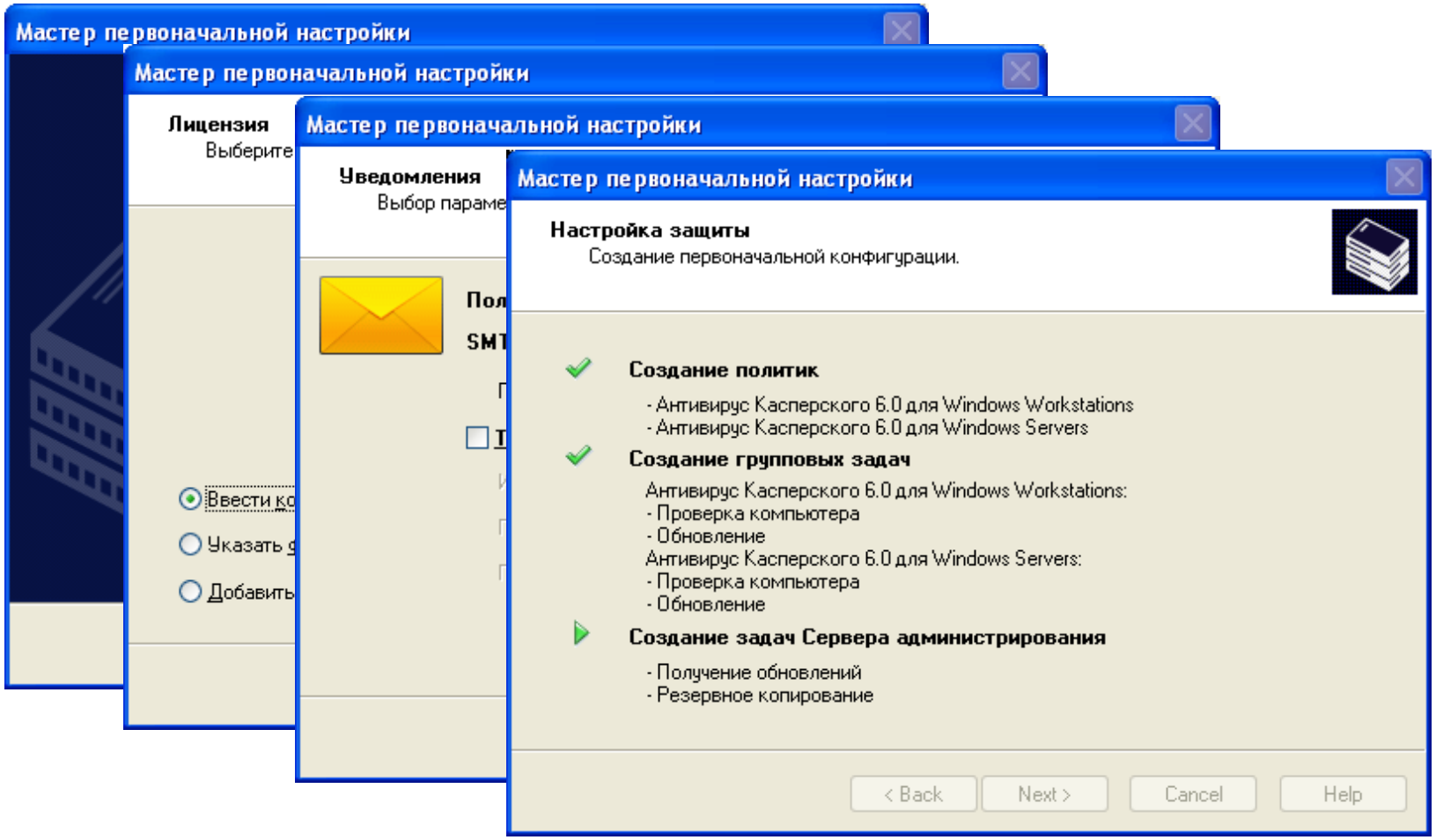
Удобство

Удобство

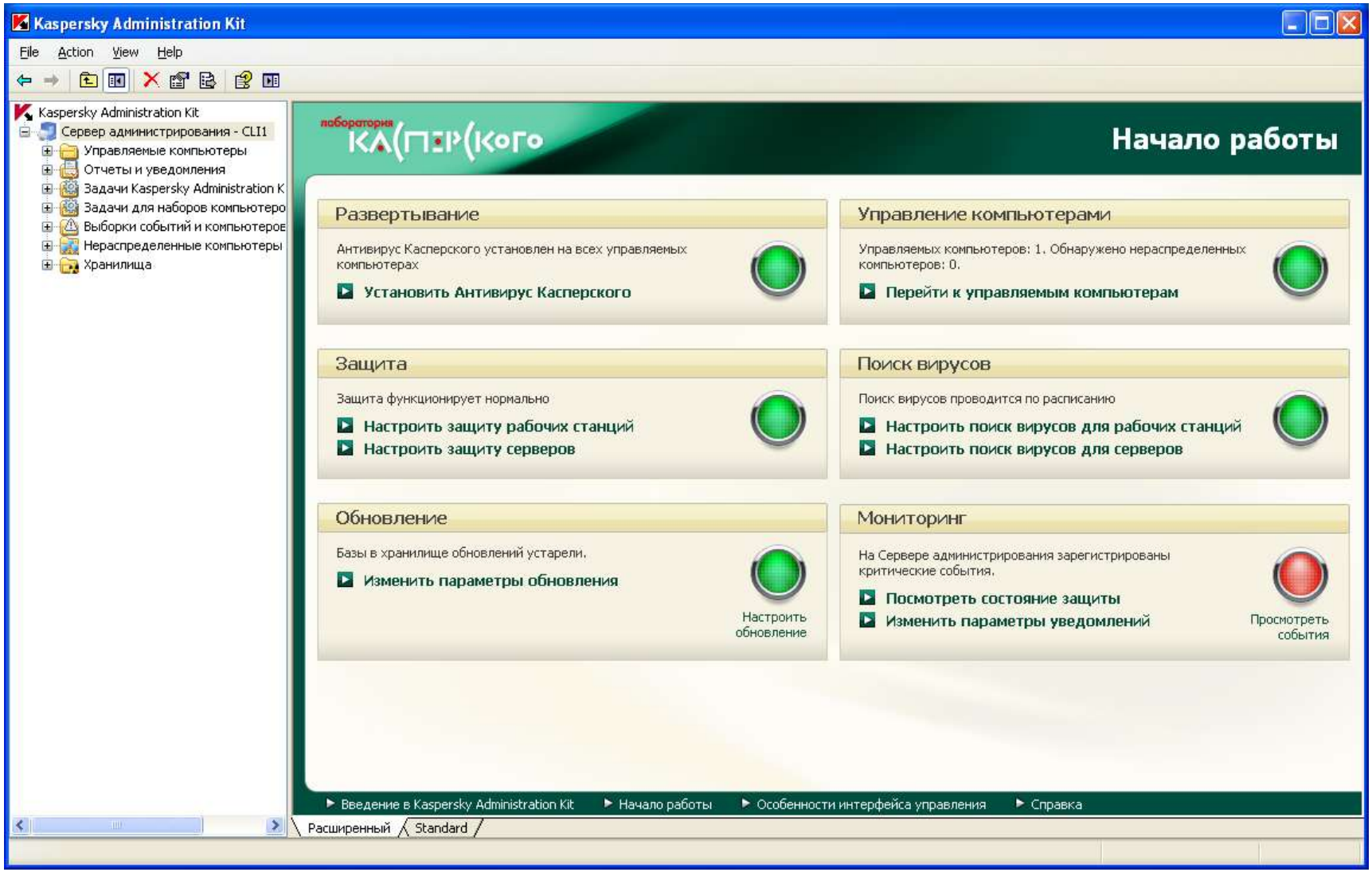
Выбор конфигурации в зависимости от размера сети



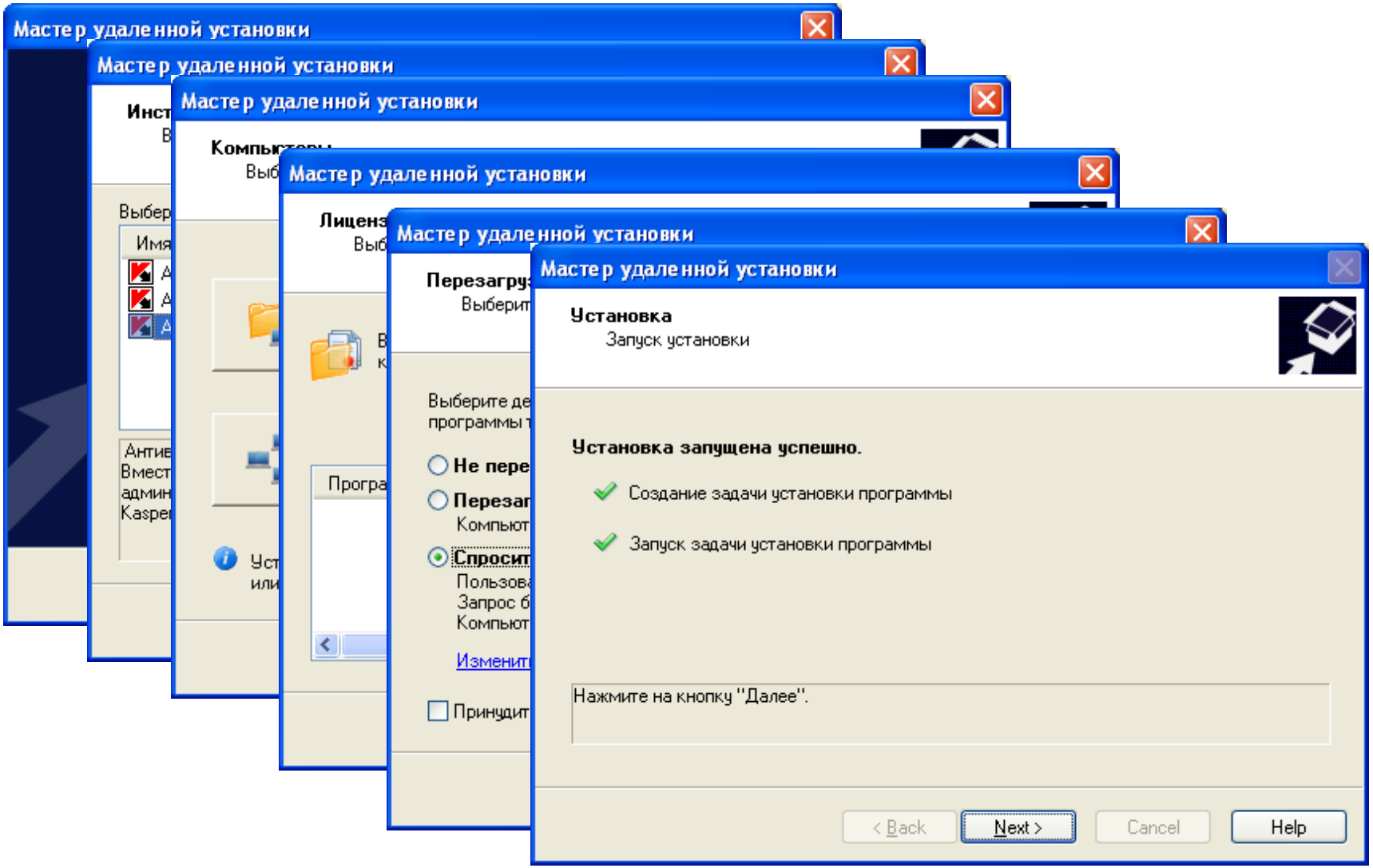
Быстрая установка



Начало работы

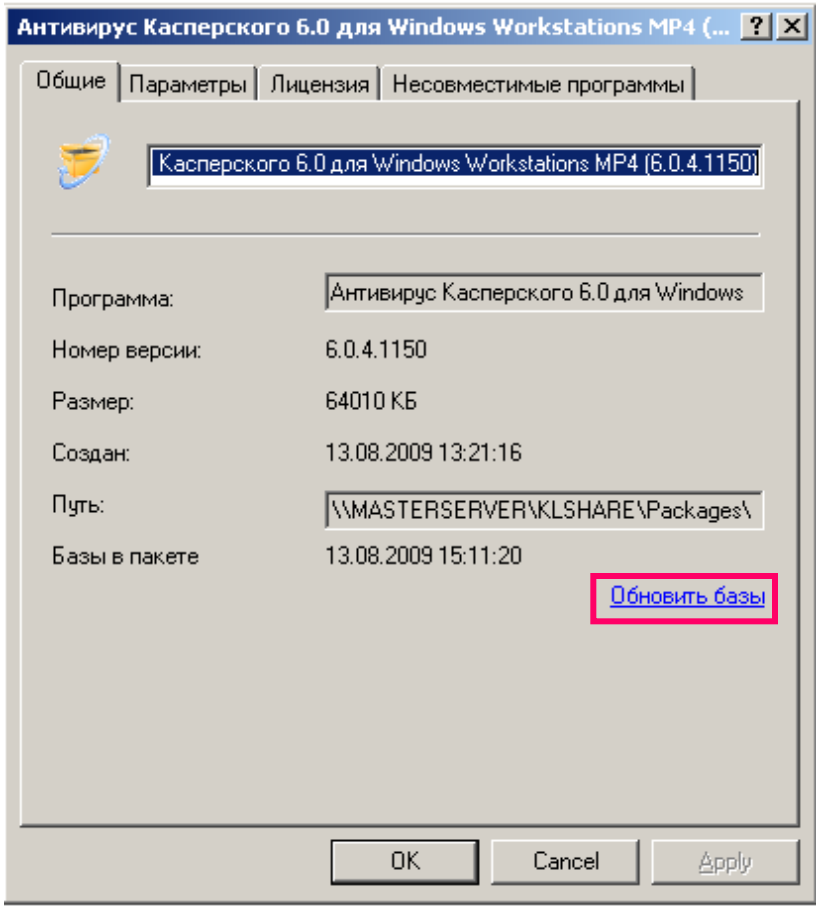


Быстрое развертывание защиты



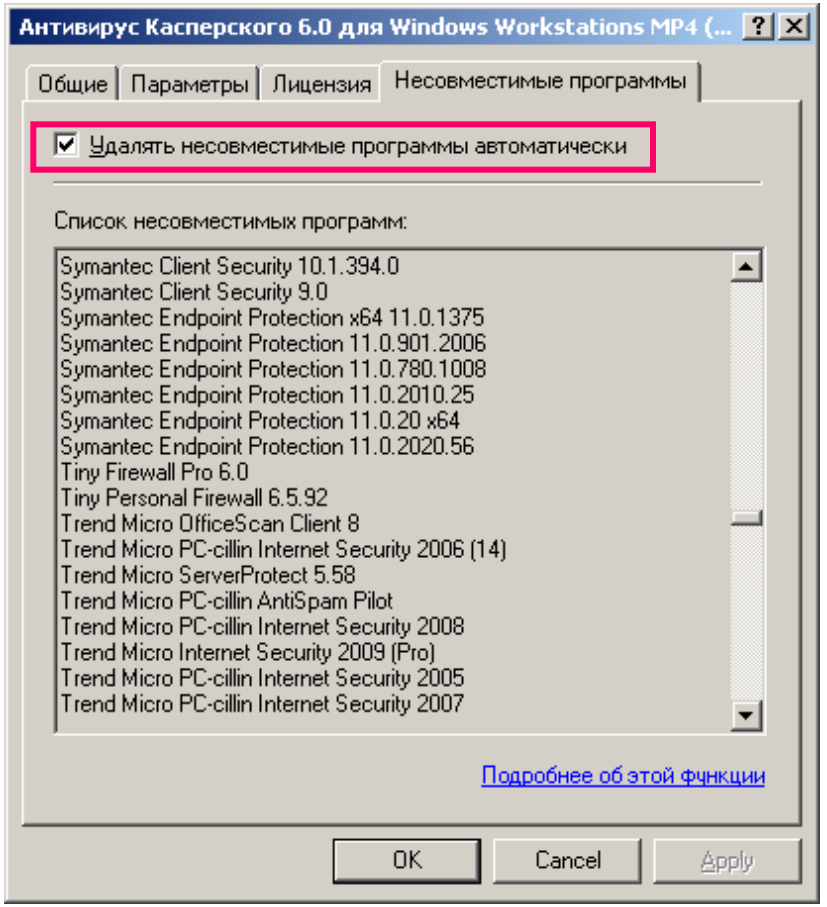
Развёртывание защиты

Возможность обновить антивирусные базы в инсталляционном пакете



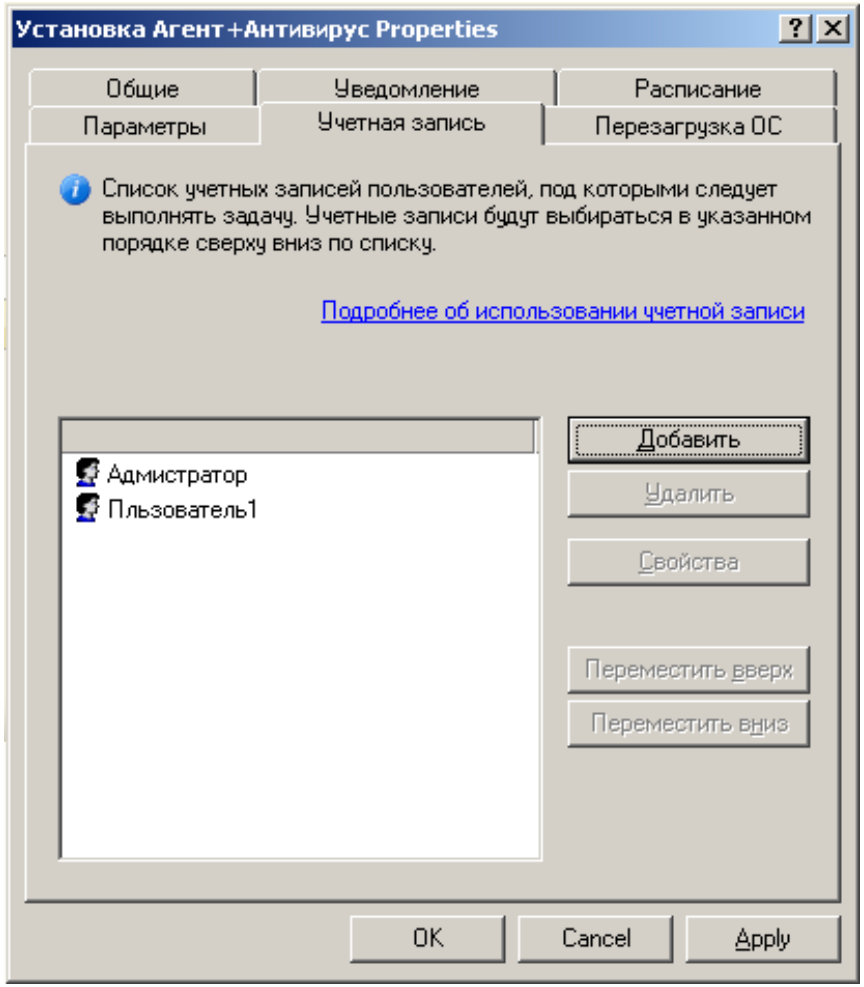
Развёртывание защиты

Автоматическое удаление несовместимых приложений перед установкой

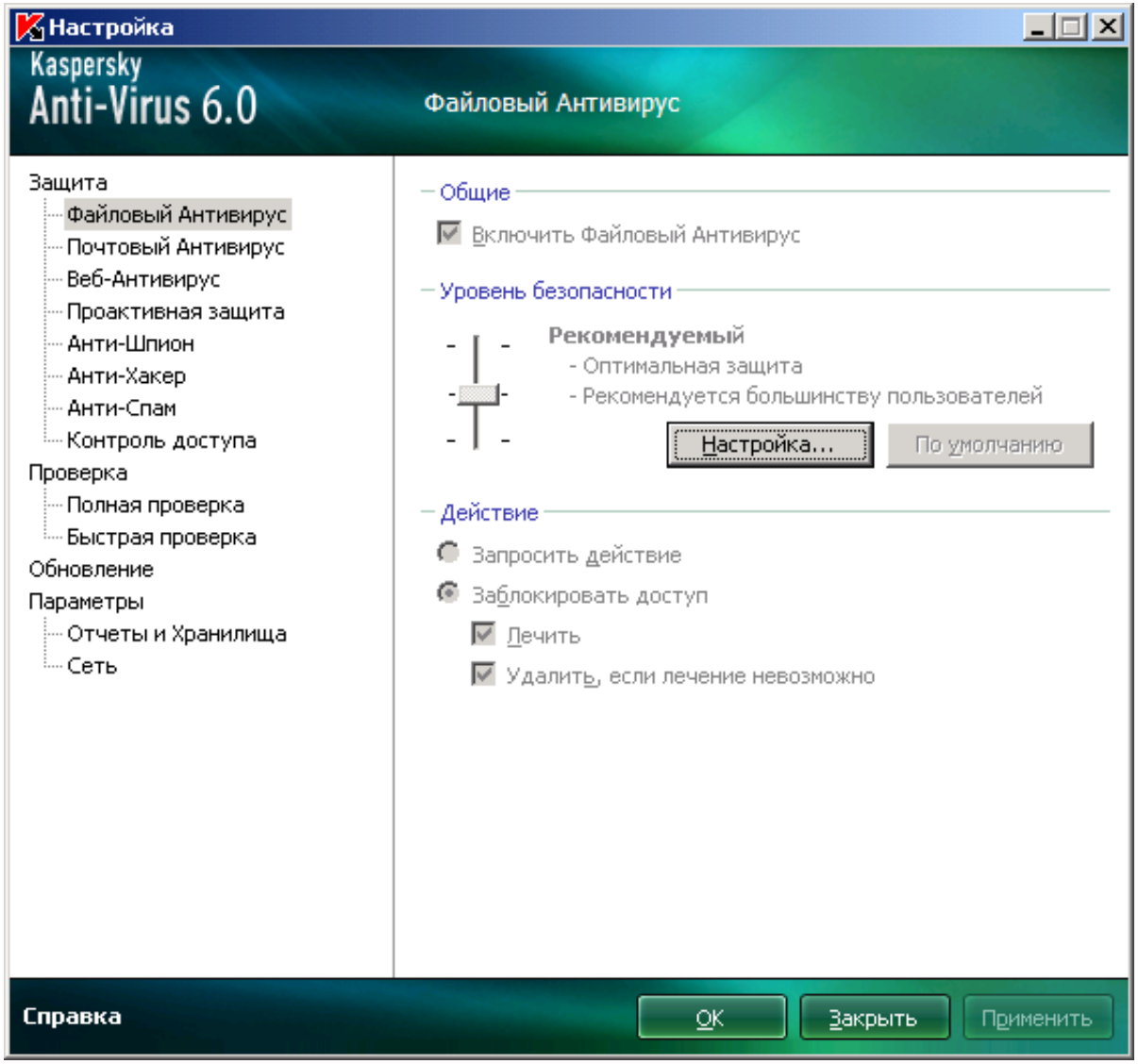


Развёртывание защиты

Возможность задать несколько учётных записей для выполнения задачи удалённой установки

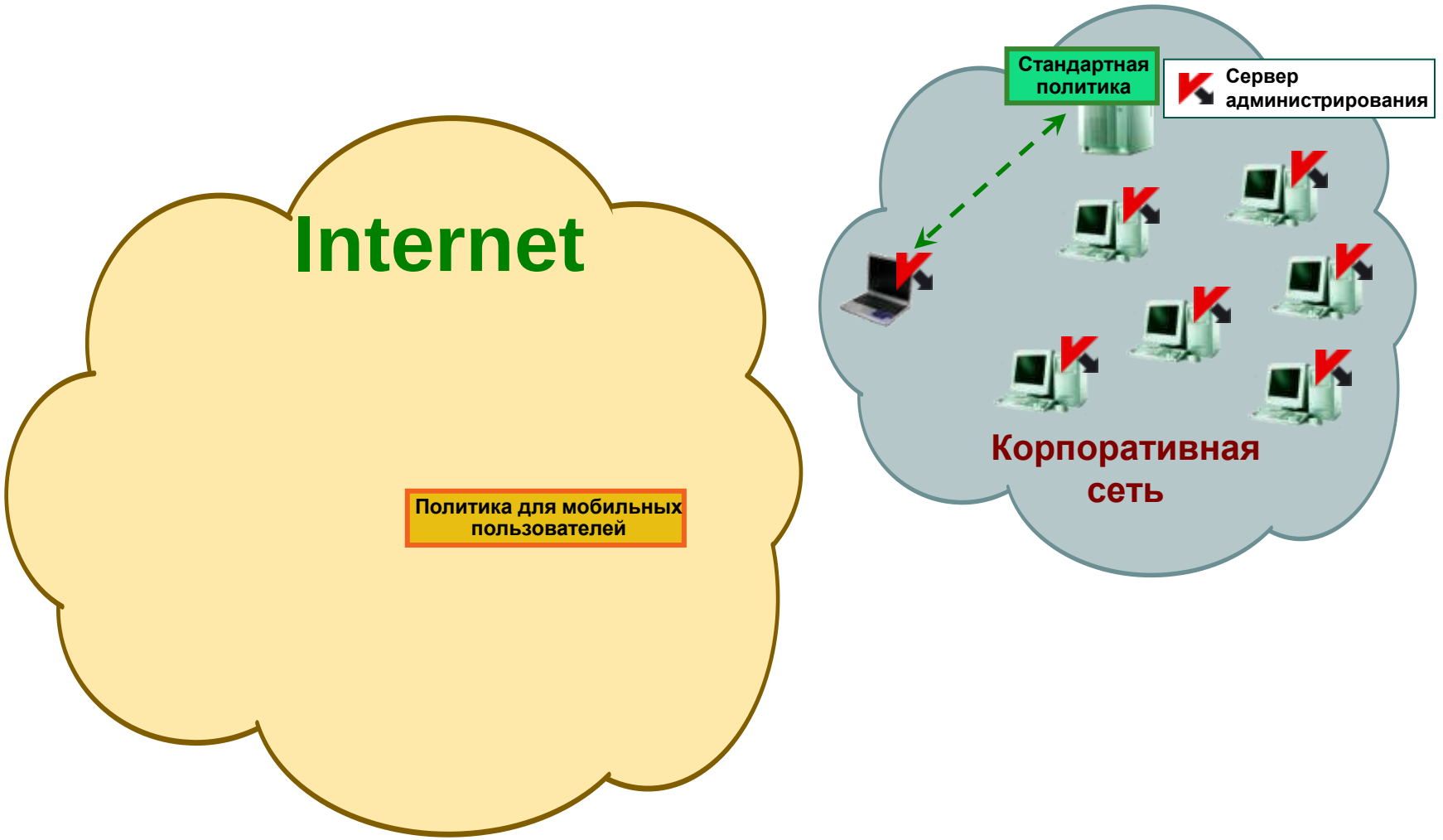


Управление защищаемыми узлами



Активная политика применена

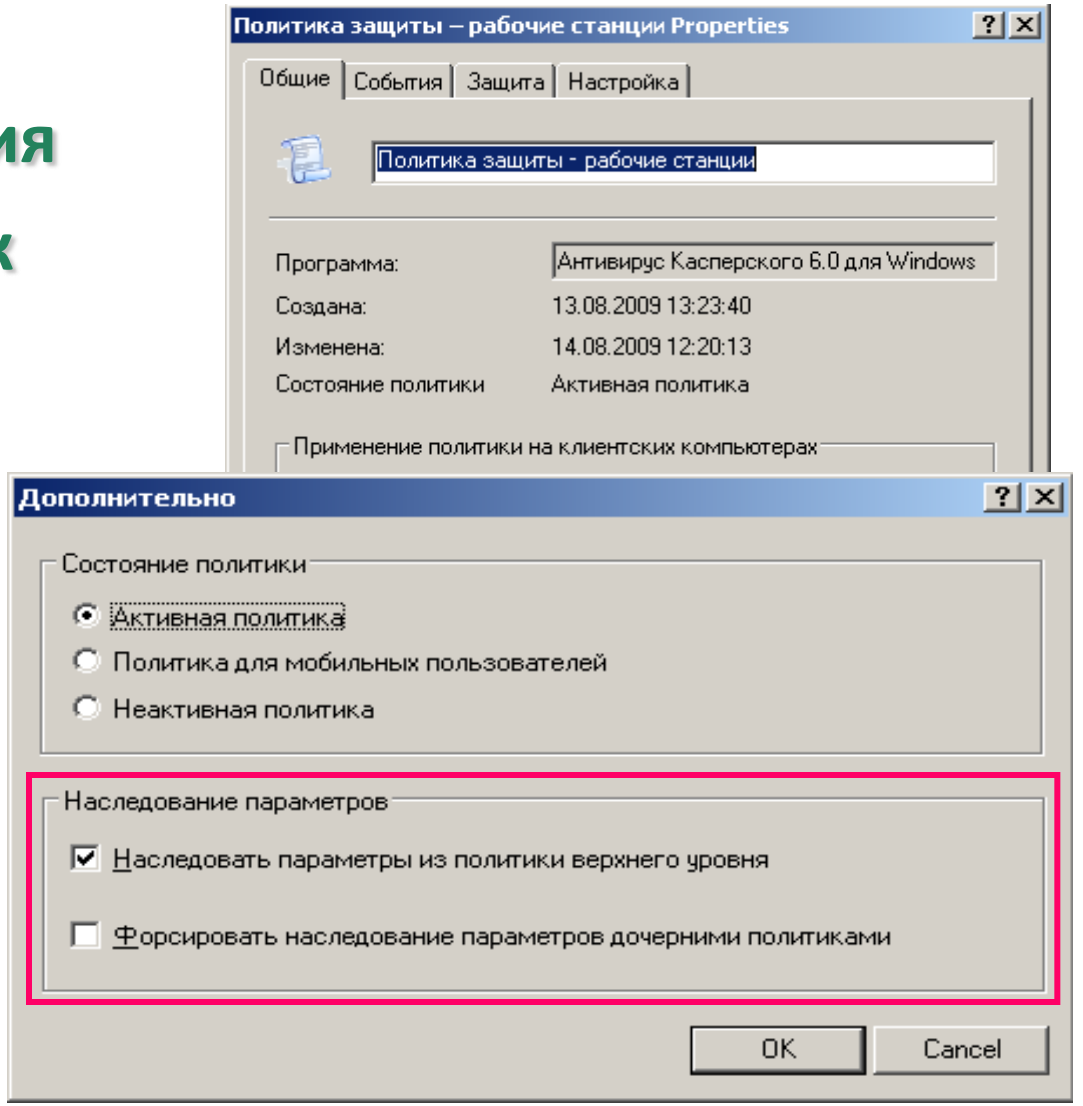
Защита для мобильных сотрудников



Автоматическое принятие мер

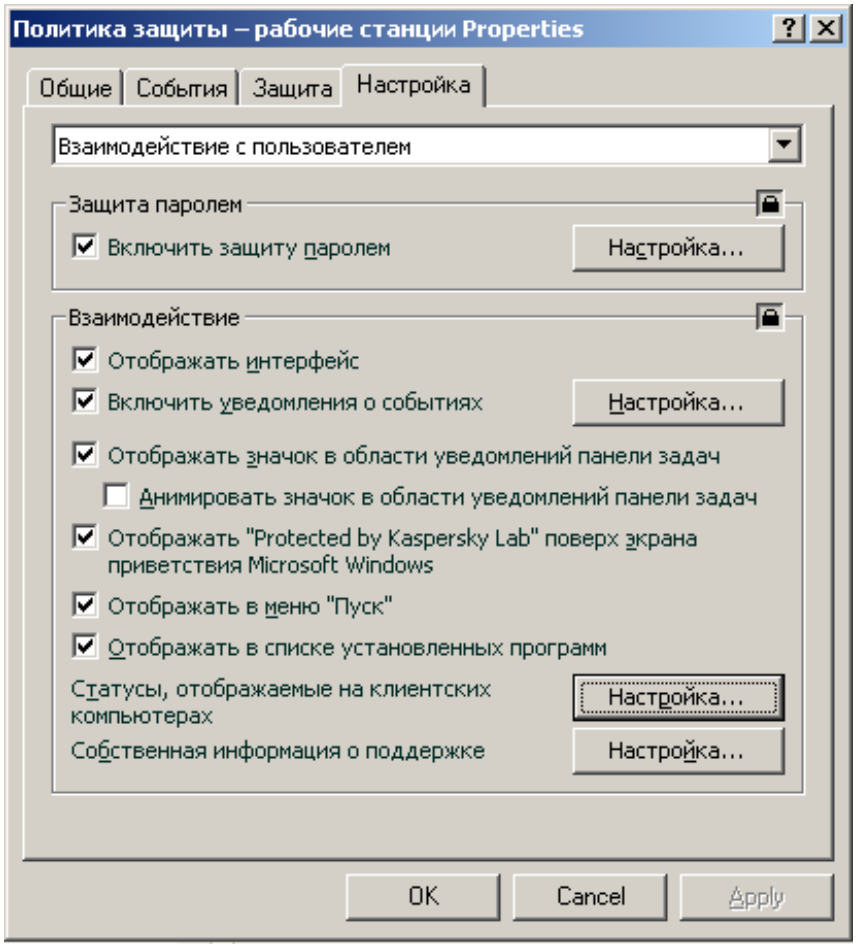
Гибкое управление

Возможность управления наследованием политик

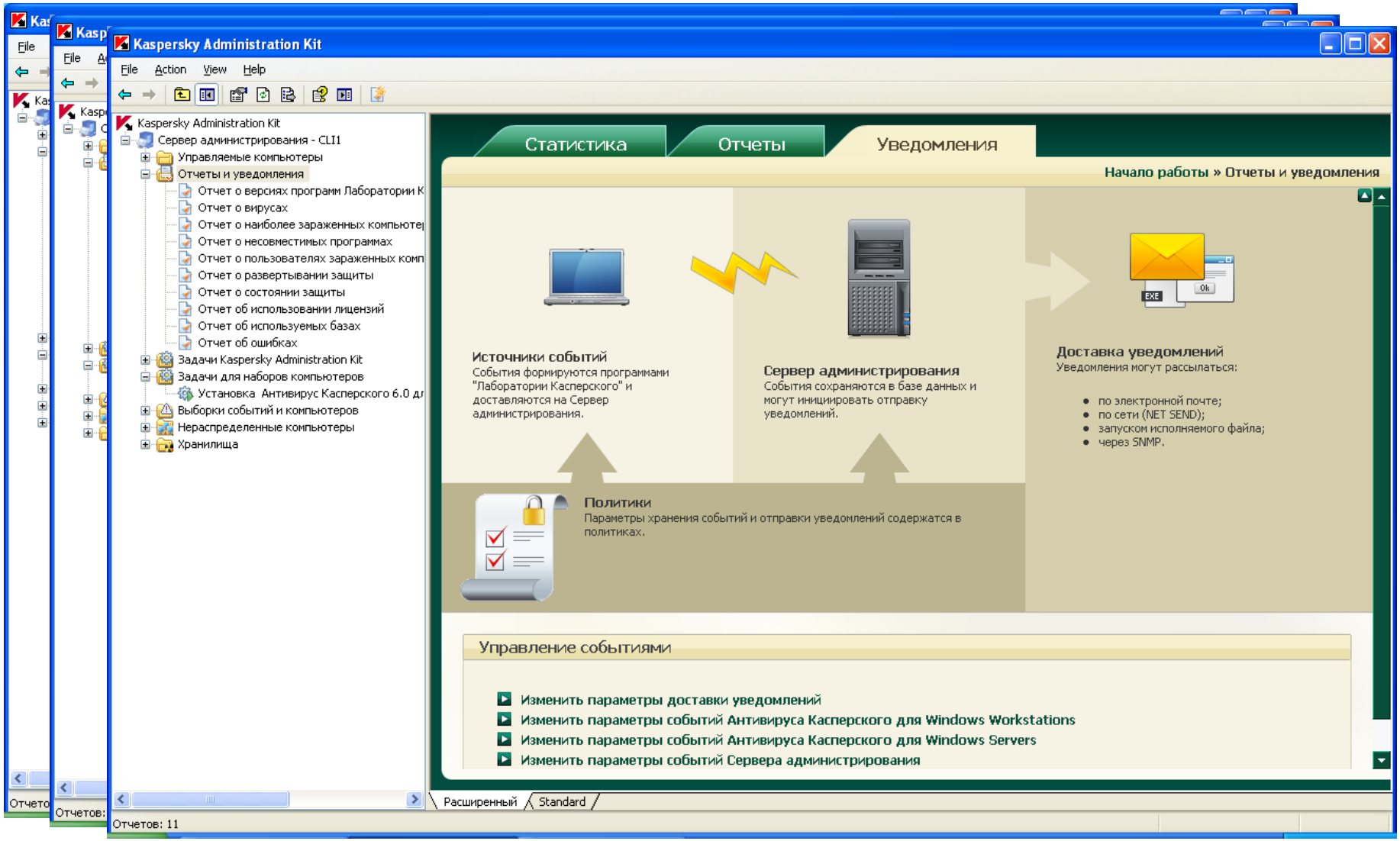


Взаимодействие с пользователем

Возможность задавать различные варианты визуализации приложения для пользователя

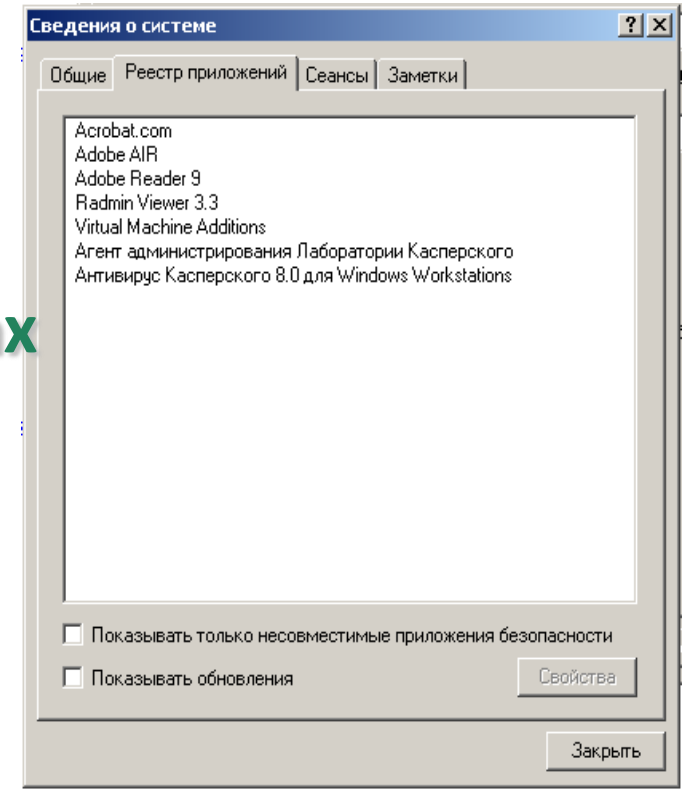


Информация о состоянии антивирусной защиты и настройка уведомлений



Дополнительные возможности

Ведение реестра приложений на компьютерах сети



Результаты независимого тестирования

AV comparatives

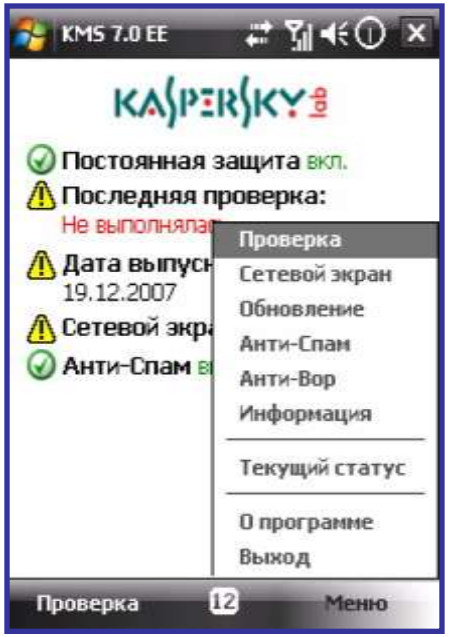
Review of IT Security Suites for Corporate Users, 2009

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

- Удобные мастеры 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)
★★★★★	★★★★★	★★★★★

Kaspersky Mobile Security



Защищает от

- Вирусов
- Спама
- Сетевых атак
- Последствий кражи

Поддерживаемые ОС:

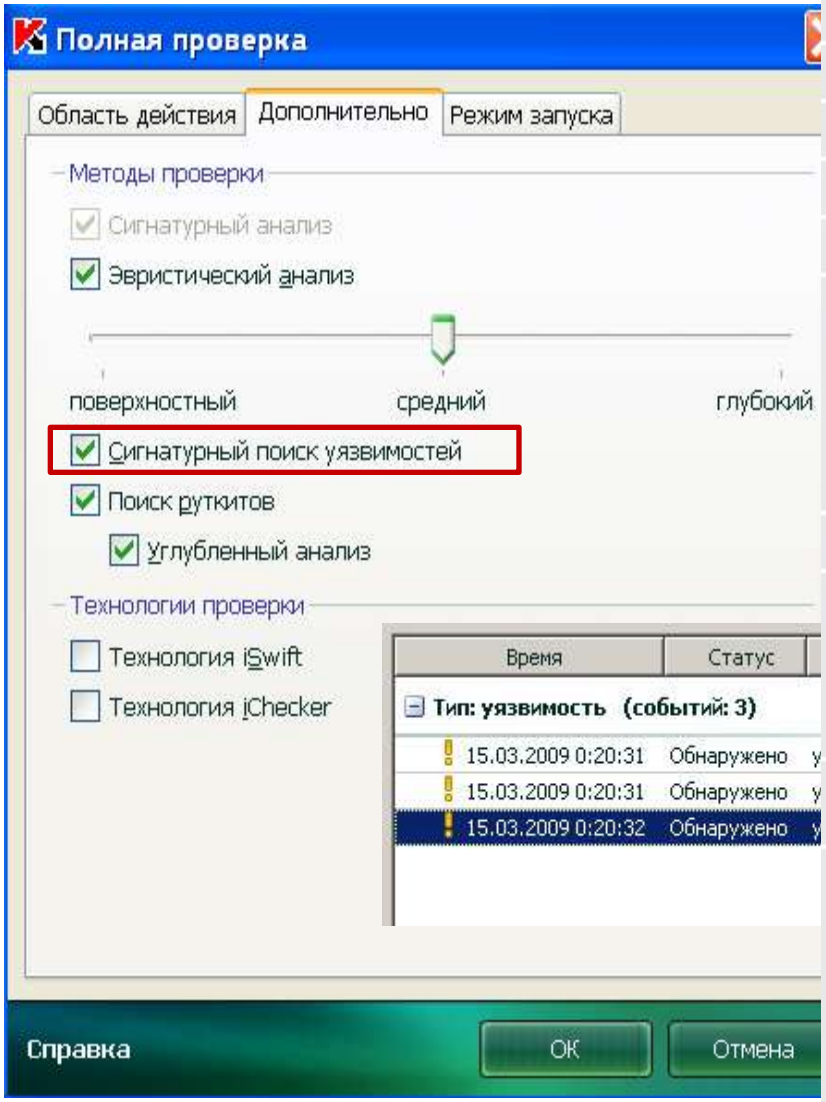
- Widows Mobile 5.0, 6.0, 6.1
- Nokia Symbian OS 9.1, 9.2, 9.3 series 60 3rd

Централизованная установка и управление с помощью Kaspersky Administration Kit

Kaspersky Mobile Security

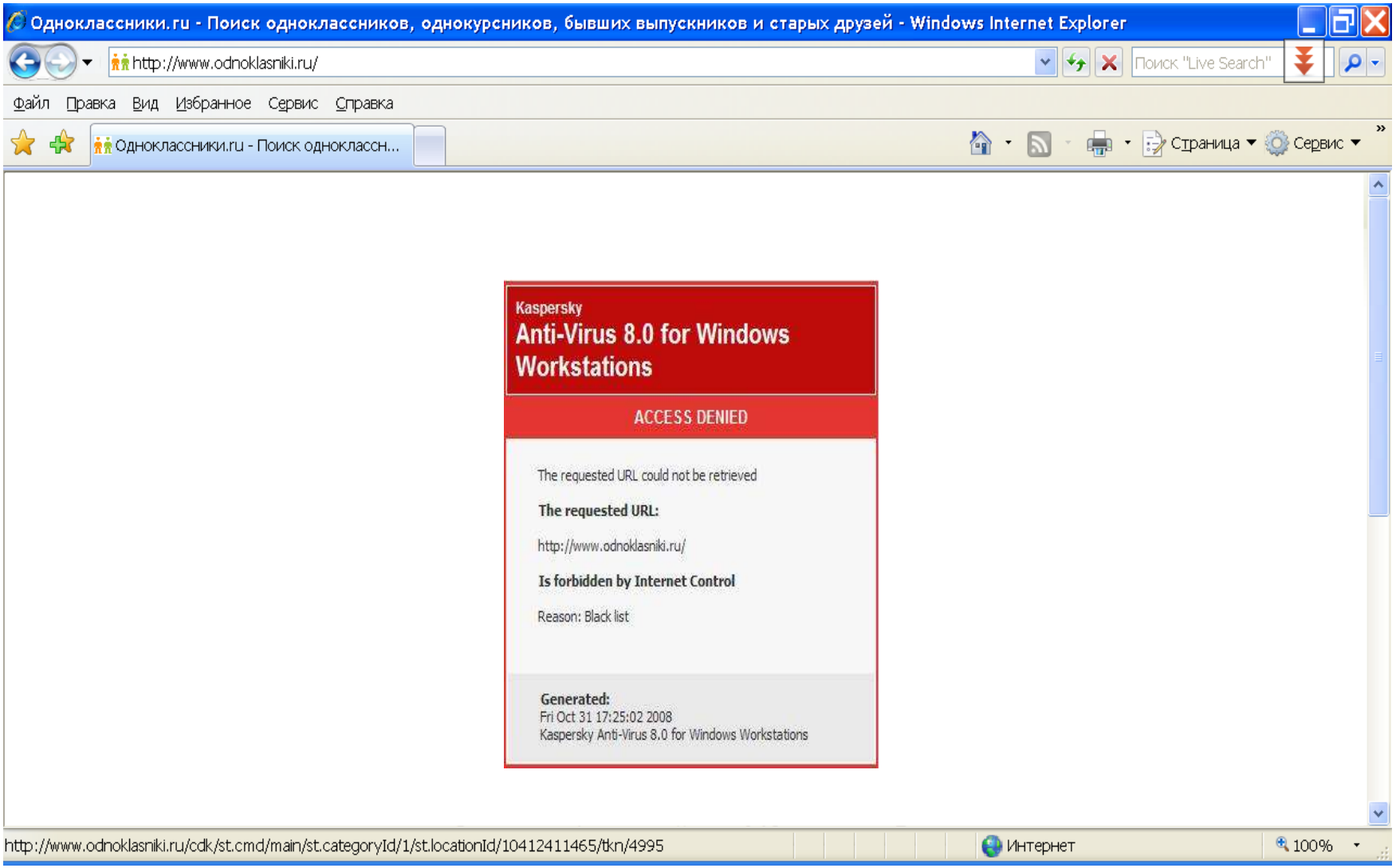
А дальше?!

Детектирование уязвимостей

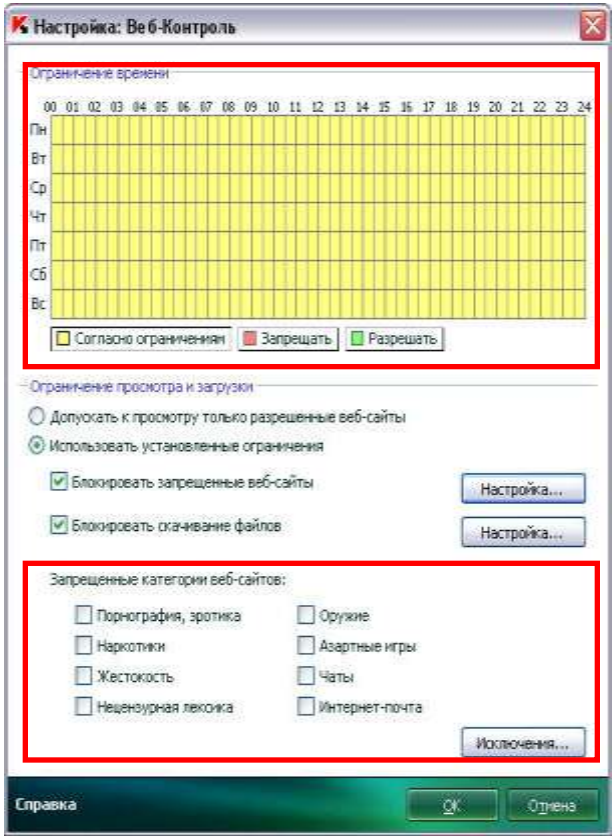


CVE-ID	CVE-2008-2244
Опубликовано	09 июл 2008
Обновлено	12 авг 2008
Опасность	
Статус решения	Исправлена патчем от производителя
Уязвимые приложения	Microsoft Office 2003 Professional Edition Microsoft Office 2003 Small Business Edition Microsoft Office 2003 Standard Edition Microsoft Office 2003 Student 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

Контроль доступа к Интернету



Веб-контроль



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


и многое другое

Благодарю за внимание!
Вопросы?

Евгений Лужнов
Инженер предпродажной поддержки
Evgeny.Luzhnov@ru.kaspersky.com