КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Компьютер как средство

- производства,
- хранения,
- распространения и
- использования информации

Хранение: информация как ценность

- **Личные данные,**
- **финансовая информация,**
- **базы данных различных ведомств.**

Производство и использование информации

- Техническое состояние компьютерной системы

Распространение информации

- Данный компьютер может применяться для распространения нелигитимной информации без ведома владельца

Политика информационной безопасности

- Ее задачей является уменьшение степени риска утраты или утечки важной информации.
- Политика информационной безопасности является планом высокого уровня, в котором описываются цели и задачи мероприятий в сфере безопасности.
- Политика не представляет собой ни директиву, ни норматив, ни инструкции, ни средства управления.
- Политика описывает безопасность в обобщенных терминах без специфических деталей.

Направления безопасности

- Конфиденциальность данных
- Достоверность и надежность программ
- Защита от вирусов
- Защита от проникновения по сети (Интернет)

Конфиденциальность

- **законодательство**
- Ограничение доступа (политика безопасности)
- Шифрование
- Протоколирование доступа
- Достоверное стирание старых программ и данных

Ограничение доступа

1. *Физическое ограничение доступа* (отдельные помещения)
2. *Парольная защита*: (пароль должен быть достаточно сложным)

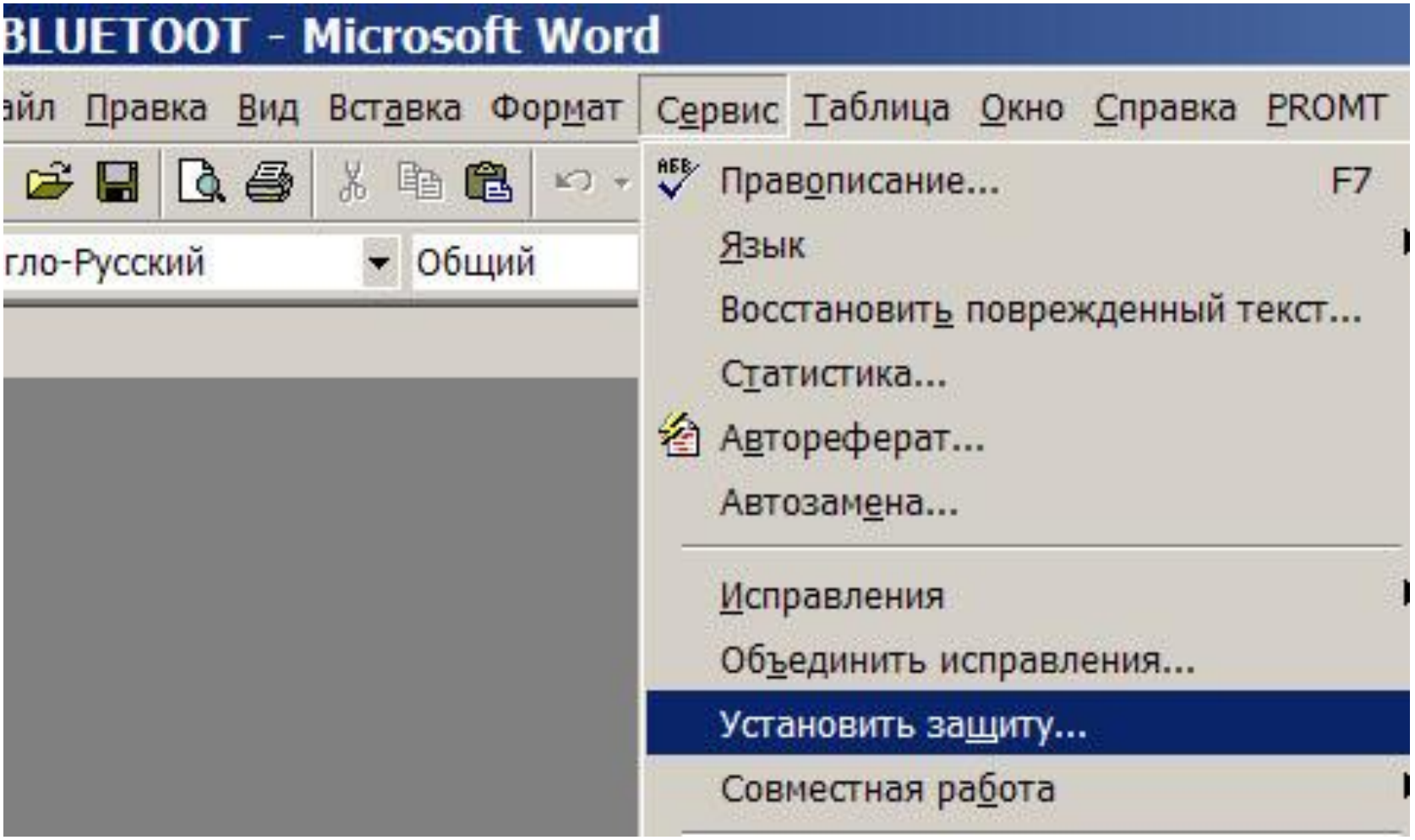
- при включении компьютера (в SETUP)
- при входе в операционную систему
- при доступе к файлам
- С помощью стандартных или специальных программ

(но есть *клавиатурные шпионы,* программы *восстановления паролей*)

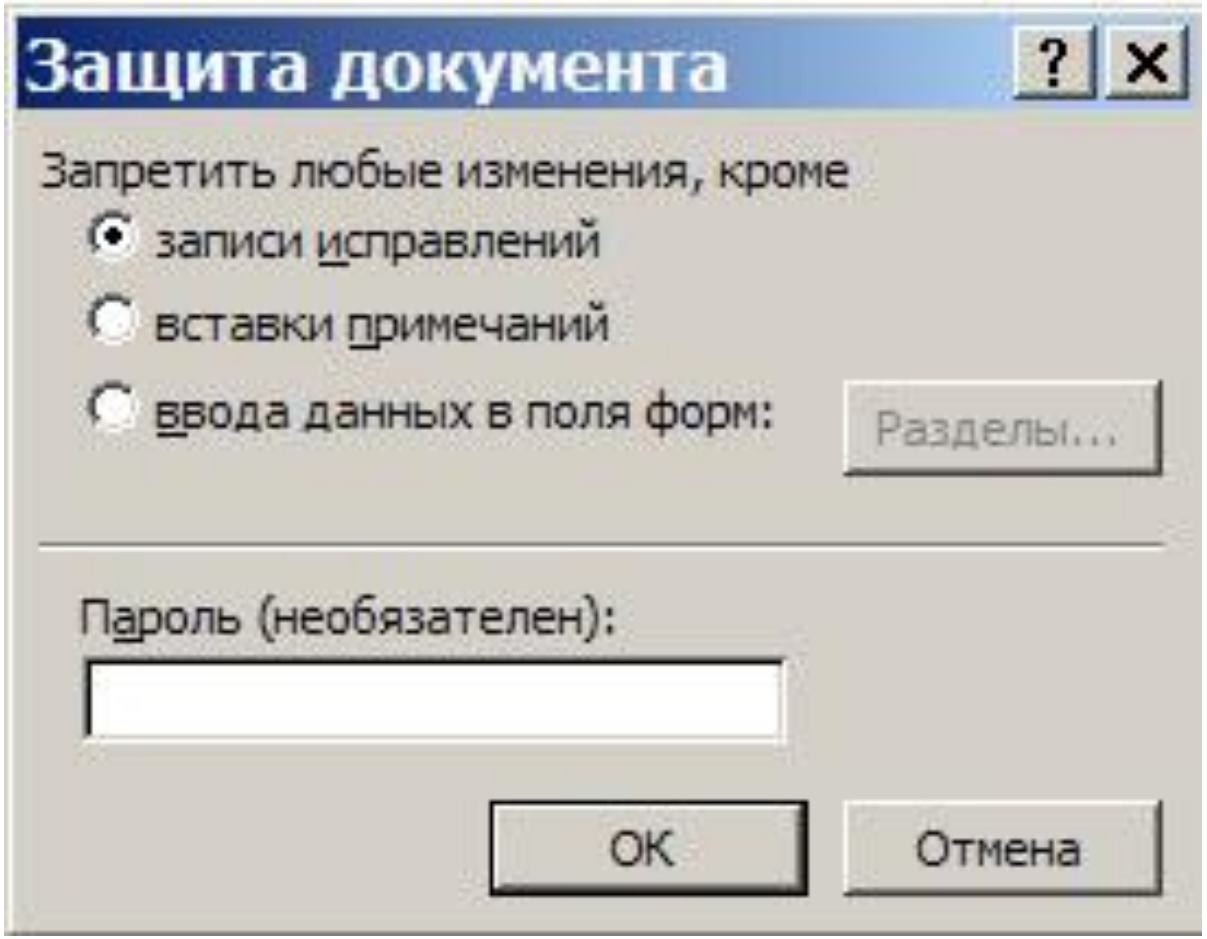
Ограничение доступа

3. *Протоколирование доступа*
4. Различные *права доступа* и действий к файлам для каждого пользователя (NTFS, особые программы)
5. Защита с помощью *электронных ключей*

Защита паролем файла Word



Защита документа



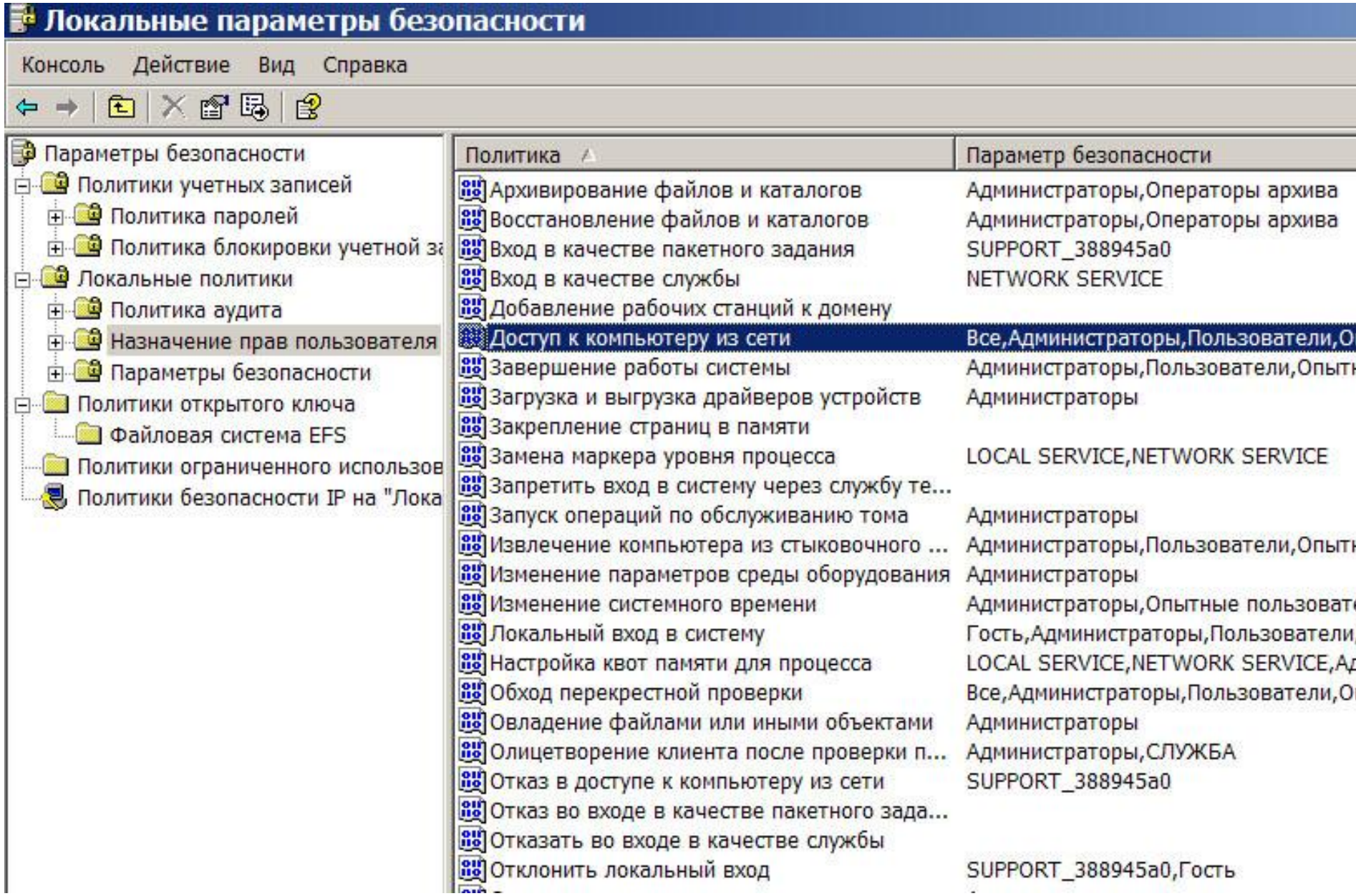
Права доступа

Групповые

- Пользователь относится к одной из групп: *администраторы, опытные пользователи, пользователи, гости*
- Права задаются для групп

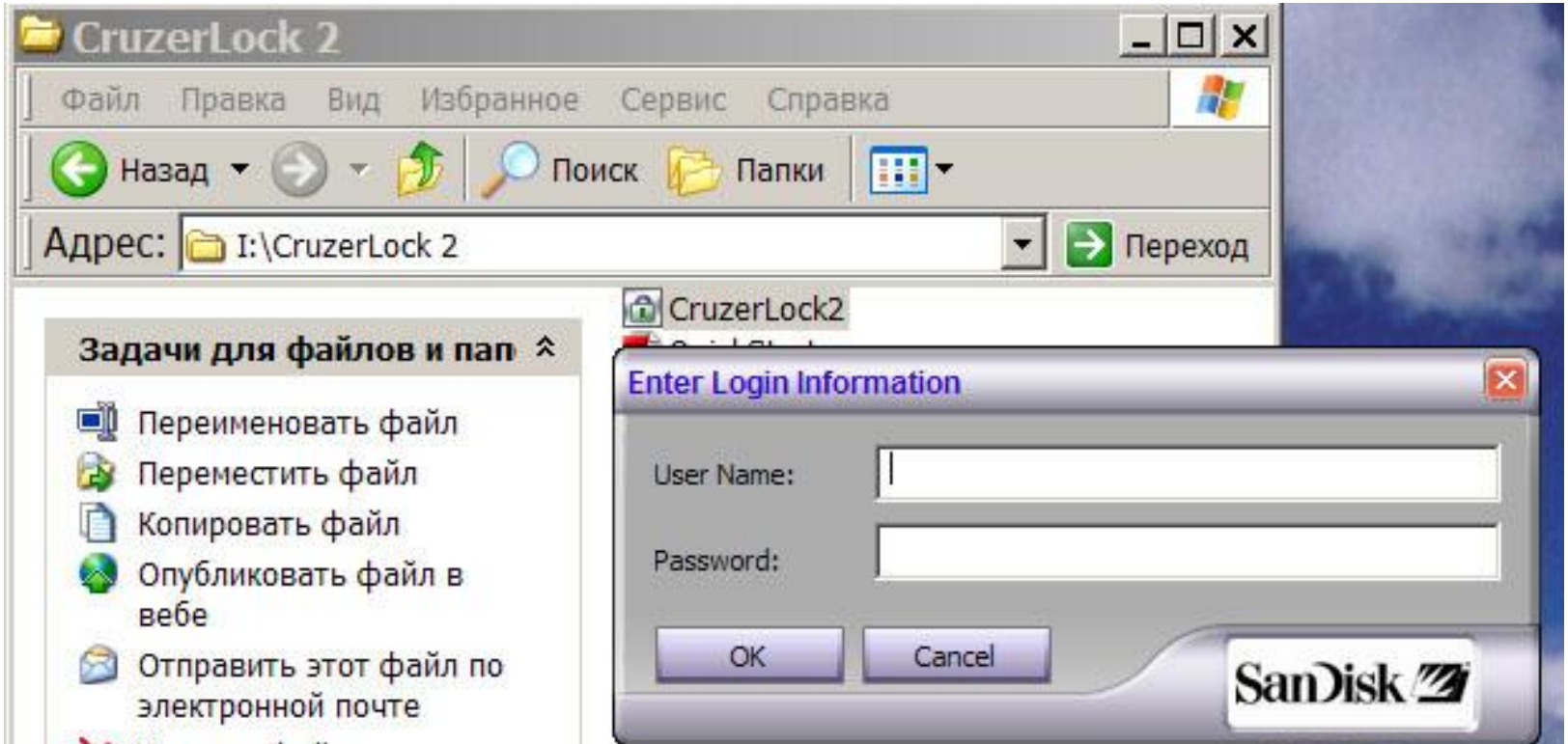
Индивидуальные

- Права задаются для конкретного пользователя

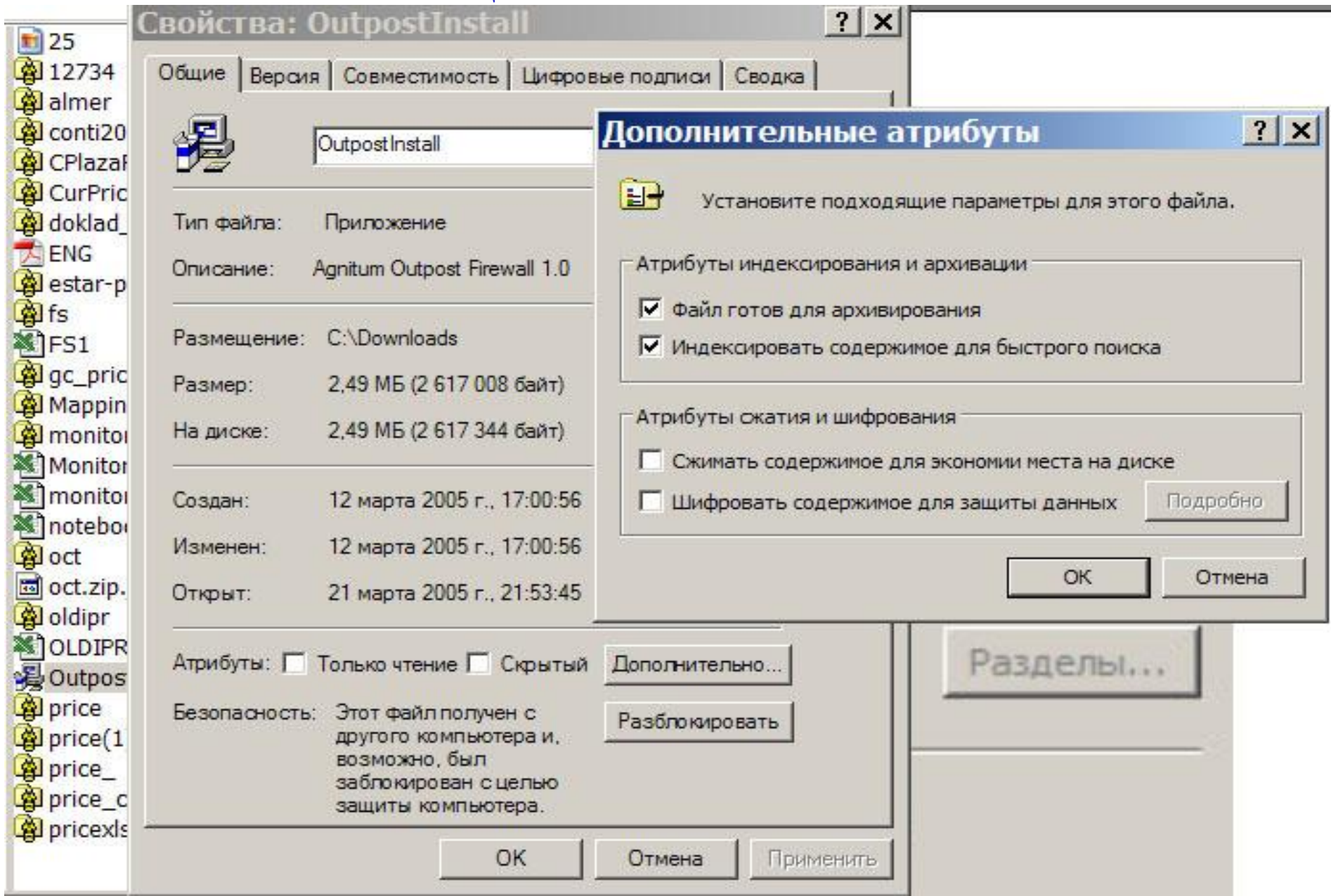

Локальные параметры безопасности
Консоль Действие Вид Справка
Параметры безопасности
Политики учетных записей
Политика паролей
Политика блокировки учетной за
Локальные политики
Политика аудита
Назначение прав пользователя
Параметры безопасности
Политики открытого ключа
Файловая система EFS
Политики ограниченного использов
Политики безопасности IP на "Лока
Политика
Параметр безопасности
Архивирование файлов и каталогов
Администраторы,Операторы архива
Восстановление файлов и каталогов
Администраторы,Операторы архива
Вход в качестве пакетного задания
SUPPORT_388945a0
Вход в качестве службы
NETWORK SERVICE
Добавление рабочих станций к домену
Доступ к компьютеру из сети
Все,Администраторы,Пользователи,О
Завершение работы системы
Администраторы,Пользователи,Опыт
Загрузка и выгрузка драйверов устройств
Администраторы
Закрепление страниц в памяти
Замена маркера уровня процесса
LOCAL SERVICE,NETWORK SERVICE
Запретить вход в систему через службу те...
Запуск операций по обслуживанию тома
Администраторы
Извлечение компьютера из стыковочного ...
Администраторы,Пользователи,Опыт
Изменение параметров среды оборудования
Администраторы
Изменение системного времени
Администраторы,Опытные пользовате
Локальный вход в систему
Гость,Администраторы,Пользователи,
Настройка квот памяти для процесса
LOCAL SERVICE,NETWORK SERVICE,Ад
Обход перекрестной проверки
Все,Администраторы,Пользователи,О
Овладение файлами или иными объектами
Администраторы
Олицетворение клиента после проверки п...
Администраторы,СЛУЖБА
Отказ в доступе к компьютеру из сети
SUPPORT_388945a0
Отказ во входе в качестве пакетного зада...
Отказать во входе в качестве службы
Отклонить локальный вход
SUPPORT_388945a0,Гость

Шифрование

- Дисков, папок, файлов, писем
- Особые программы:
  CryptKEY, SecretFolders
- Защита информации на флешке



Защита в NTFS



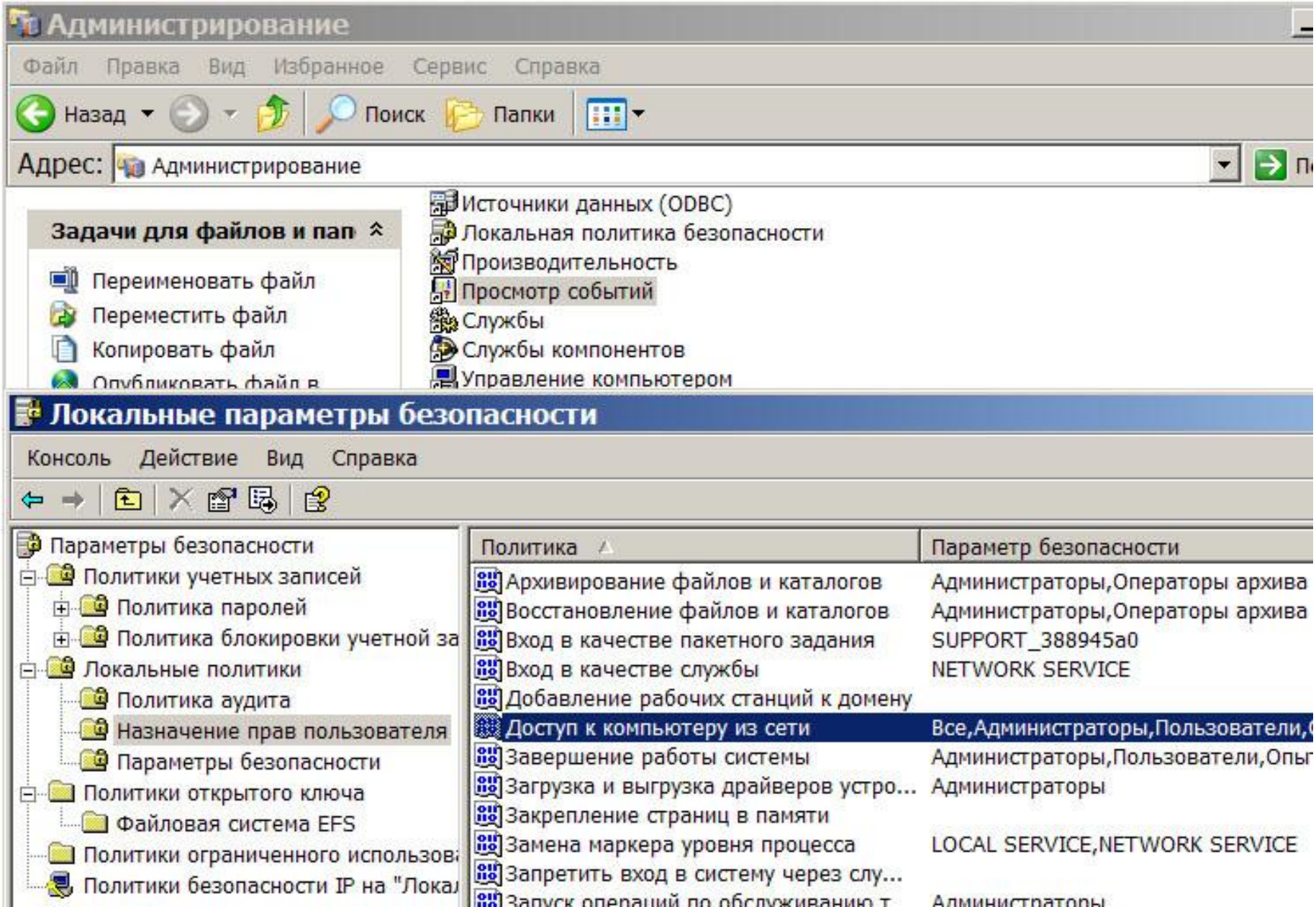
Достоверное стирание старых программ и данных

- При удалении файла он остается на носителе, изменяется лишь первая буква в названии, он *объявляется* стертым.
- Даже форматирование диска не приводит к стиранию.
- Восстановление возможно почти всегда, но требует больших технических, временных и трудовых затрат.

Достоверное стирание

- Многократная запись поверх файла (Ontrack DiskWipper)
- Особые программы (утилиты) восстановления затертых файлов (Ontrack EasyRecovery, MAPILab File Recovery for Office – документы Office, даже после форматирования диска)

Политика безопасности



Достоверность и надежность программ

- **Сертификат**: подлинности и безопасности
- Гарантирует достоверность (подлинность)
- Гарантирует правильную работу, совместимость с другими программами

Защита с помощью *электронных ключей*

- Механические устройства для LPT, COM, USB
- Могут иметь таймер для ограничения во времени работы программы

Защита от вредоносных действий

Виды вредоносных и нежелательных действий

- Повреждение программного обеспечения
- Кража личных данных (паролей и т.п.)
- Использование вашего компьютера для противоправных или нежелательных действий

Виды вредоносного и нежелательного содержания

- Virus Ware - вирусы
- Trojan Ware - трояны
- SpyWare – программы-шпионы
- AdWare – добавочные модули
- MalWare – остальные вредоносные программы

Каналы распространения

- Дискеты
- Флешки
- Электронная почта
- ICQ (ссылки)
- Веб-страницы (активное содержание, cookie)
- Интернет и локальные сети

Malware

- **Вредоносная программа** (буквальный перевод англоязычного термина **Malware**, **mal***icious* — злонамеренный и *soft***ware** — программное обеспечение, жаргонное название — «малварь») — злонамеренная программа, то есть программа, созданная со злым умыслом и/или злыми намерениями.

- Если в 2007 году было зарегистрировано чуть более 624 тысяч различных вредоносных программ,
- то в 2008 году их оказалось уже больше полутора миллионов.

Компьютерные вирусы

Компьютерный вирус *- это специально написанная, небольшая по размерам программа, которая может "приписывать" себя к другим программам ("заражать" их), создавать свои копии и внедрять их в файлы, системные области компьютера и т.д., а также выполнять различные нежелательные действия на компьютере.*

Признаки наличия вирусов

- Неправильная работа
- Медленная работа
- Исчезновение файлов и директорий
- Изменение даты и времени модификации файлов
- Изменение размеров файлов
- Увеличение количества файлов
- Появление неожиданных сообщений и действий

Классификация

- По среде обитания
- По способу заражения
- По деструктивным возможностям
- По особенностям алгоритма вируса

Среда обитания

- сетевые
- файловые
- загрузочные
- резидентные
- нерезидентные
- Макровирусы

- распространяются по компьютерной сети
- внедряются в выполняемые файлы
- внедряются в загрузочный сектор диска (Boot-сектор)
- находятся в памяти, активны до выключения компьютера
- не заражают память, являются активными ограниченное время
- Заражают файлы распространенных прикладных программ (Word, Excell, Outlook)

Защита в интернете

- Защита при обращении к сайтам
- Защита от проникновения в компьютер извне по сети

Защита при обращении к сайтам

- **Активные сценарии**, приложения *Java*

  Улучшают вид веб-страницы, но производят действия на компьютере
- **Cookie -** остаются после посещения некоторых сайтов. Содержат сведения о предпочтениях пользователя
- **Трояны** – программы, собирающие сведения о компьютере и предающие их на определенный адрес

  (SpyWare – шпионские программы)

Троя́нская программа

(также — **троя́н**, **троя́нец**, **троя́нский конь**, **тро́й**) — программа, используемая злоумышленником для сбора информации, её разрушения или модификации, нарушения работоспособности компьютера или использования его ресурсов в неблаговидных целях. Действие троянской программы может и не быть в действительности вредоносным.

По принципу распространения и действия троян не является вирусом, так как не способен распространяться саморазмножением.

SpyWare

- несанкционированно применяемые мониторинговые программные продукты (англ. ***Tracking Software)*** ;
- несанкционированно применяемые программные продукты, предназначенные для контроля нажатий клавиш на клавиатуре компьютера.(англ. ***Keyloggers)***;
- несанкционированно применяемые программные продукты, предназначенные для контроля скриншотов экрана монитора компьютера.(англ. ***Screen Scraper***);
- **Rootkit** (*рутки́т*, от англ. *root kit*, то есть «набор root'а») — программа или набор программ для скрытия следов присутствия злоумышленника или вредоносной программы в системе.

нежелательное проникновение по сети

проект ***Honeynet***

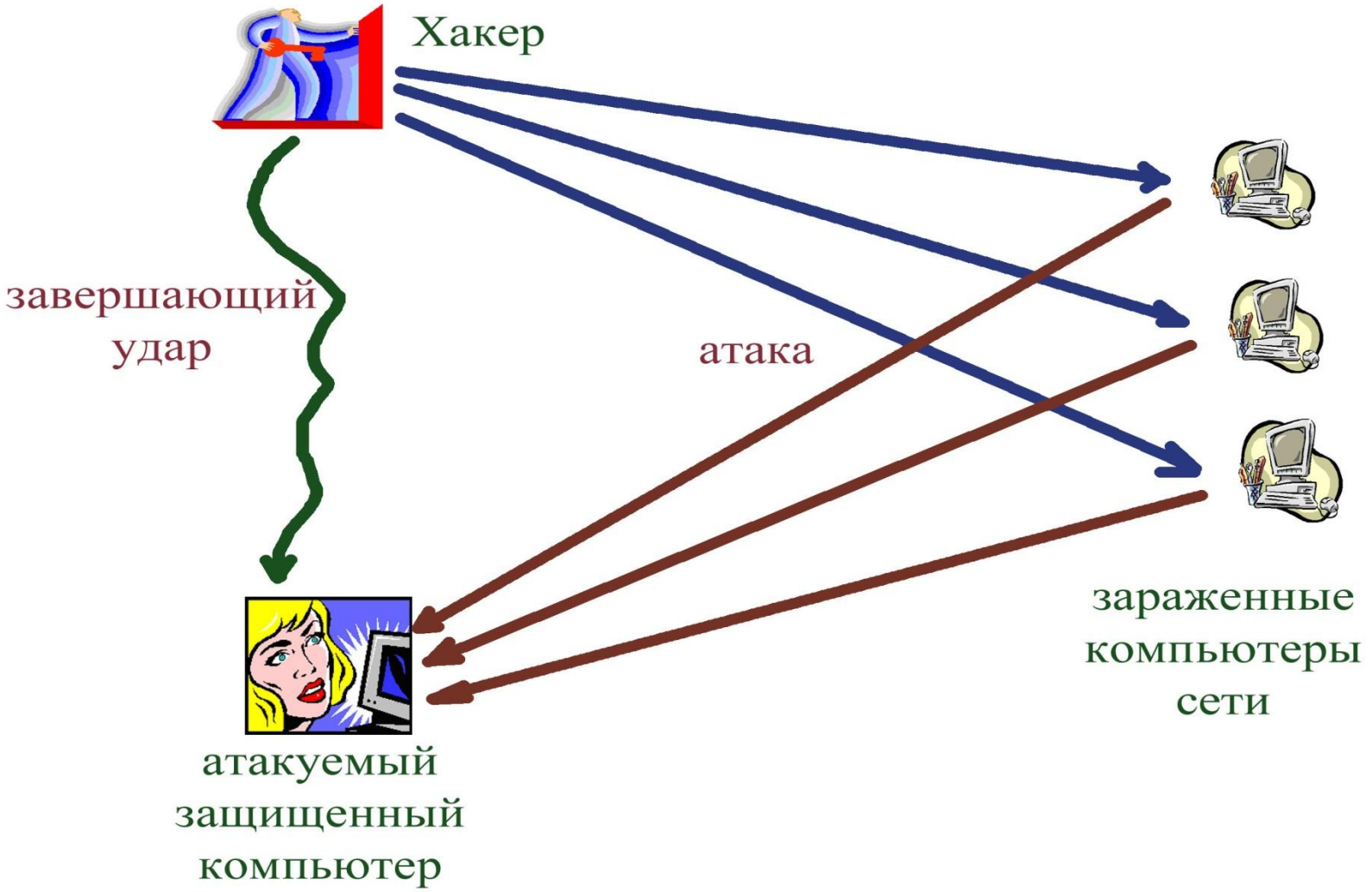
Длительное исследование сети с помощью подставных компьютеров 2005г.

- Каждые 10-100 сек. попытка проникновения в компьютер
- Для заражения используется широкий спектр уязвимостей, имеющихся в операционной системе Windows
- Особенно вожделенным «призом» для хакеров являются домашние ПК, имеющие широкополосный доступ в Сеть и никогда не отключающиеся.
- Зараженные компьютеры связываются по каналам чатов с IRC- серверами и ждут поступления команд от хакеров.

Применяются:

- для рассылки и маршрутизации **спама**
- в качестве платформ для распространения **вирусов**. (**Черви** – интернет-вирусы, которые проникают без участия пользователей)
- в качестве платформ для **атак** на различные цели
- для **атак** на своих конкурентов (других групп хакеров)

Схема взлома защищенных компьютеров путем DOS-атаки (Denial of Service - отказ в обслуживании). Используются ошибки в программном обеспечении или протоколах



Веб-приложения становятся все уязвимее

- Из всех зарегистрированных уязвимостей за период с 1 июля по 31 декабря 2004 г. 48% приходятся на веб-приложения.
- среднем на каждый день приходилось 13,6 атак хакеров. (в первом полугодии 2004 года - 10,6 атак).
- самый большой процент «ботов», зомбированных компьютеров, в Великобритании («bot» —от «robot» — программа, скрытно установленная на компьютере, с помощью которой злоумышленник может дистанционно управлять зараженным устройством).
- Ежедневно отслеживается более 30 тыс. зараженных компьютеров, которые составляют целые сети.
- создание таких сетей увеличит число атак с использованием аудио- и видеоприложений, ожидается рост атак на устройства мобильной связи

Заражение сайта

В последнее время излюбленные ранее вирусописателями "сайты для взрослых" не пользуются прежней популярностью.

Теперь **гораздо легче подвергнуться атаке вируса, зайдя на солидный сайт серьезной компании**, работающей, например, в сфере услуг.

На вашем компьютере может быть удаленно установлен почтовый сервер.

По данным антивирусной компании Sophos на апрель 2008 г. ежедневно в Интернете спамеры создают более 23 тысяч сайтов, каждые 3 секунды появляется их новый сайт.

За первые 3 месяца 2008 года на каждые 100 электронных писем 92,3 письма – это спам.

примером современного вируса может служить "пасхальный троянец" – вирус Banker.LSL, проникающий на компьютеры пользователей во время проигрывания видеороликов из сети.

Вредоносная программа считывает информацию с клавиатуры и мышки, а также запоминает данные, которые пользователи вводят при заполнении различных веб-форм, например, при авторизации или веб-банкинге.

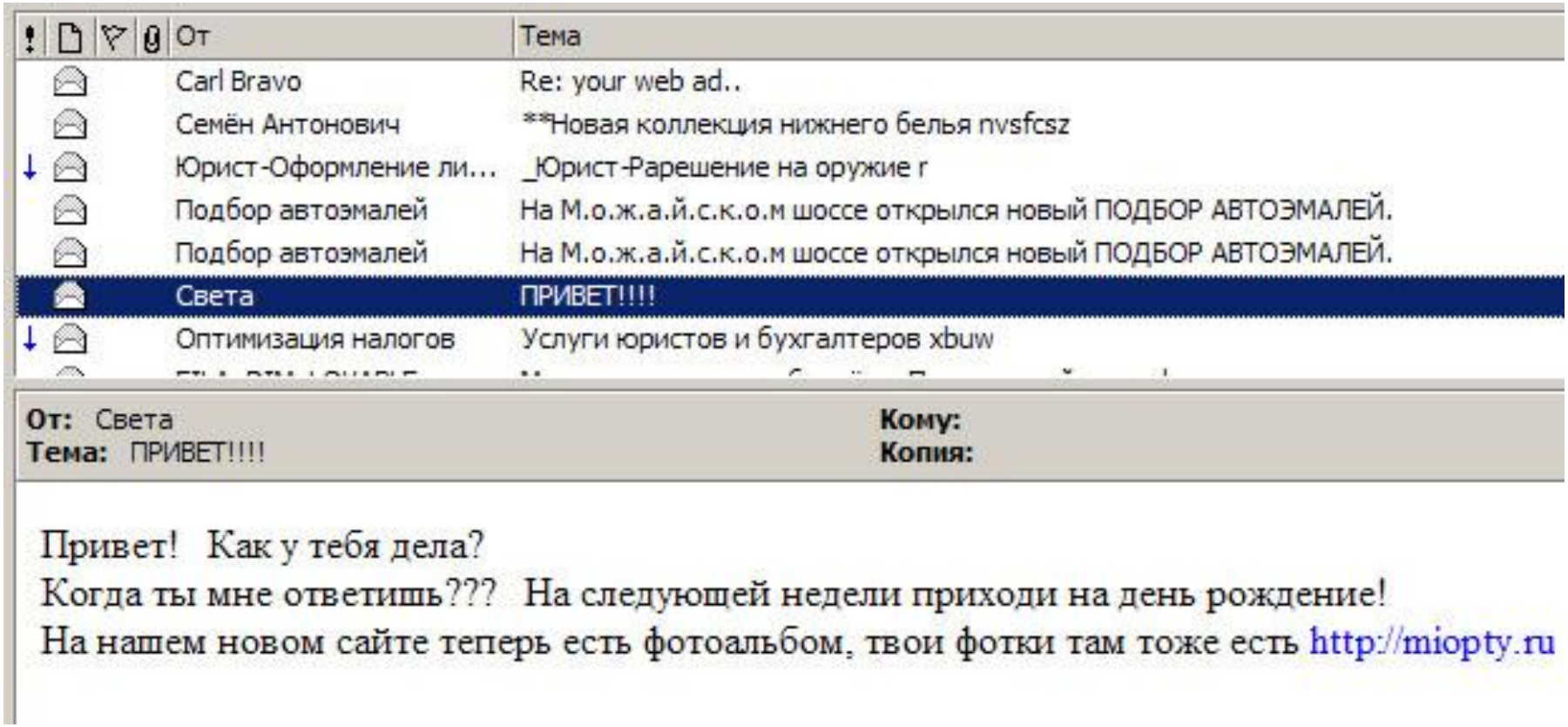
Угрозы в электронной почте

- Вирусы
- Спам
- Фишинг

СПАМ

- **спам — это анонимная массовая незапрошенная рассылка**
- В марте 2006г. доля спама в почтовом траффике составила 75%
- «Хороший провайдер» (mail.ru)
- «Черные списки» отправителей
- Никогда не отвечать на непонятные письма

Спам



От	Тема
Carl Bravo	Re: your web ad..
Семён Антонович	**Новая коллекция нижнего белья nvsfcsz
Юрист-Оформление ли...	_Юрист-Рарешение на оружие r
Подбор автоэмалей	На М.о.ж.а.й.с.к.о.м шоссе открылся новый ПОДБОР АВТОЭМАЛЕЙ.
Подбор автоэмалей	На М.о.ж.а.й.с.к.о.м шоссе открылся новый ПОДБОР АВТОЭМАЛЕЙ.
Света	ПРИВЕТ!!!!
Оптимизация налогов	Услуги юристов и бухгалтеров xbuw

От: Света
Тема: ПРИВЕТ!!!!
Кому:
Копия:

Привет! Как у тебя дела?
Когда ты мне ответишь??? На следующей недели приходи на день рождение!
На нашем новом сайте теперь есть фотоальбом, твои фотки там тоже есть http://miopty.ru

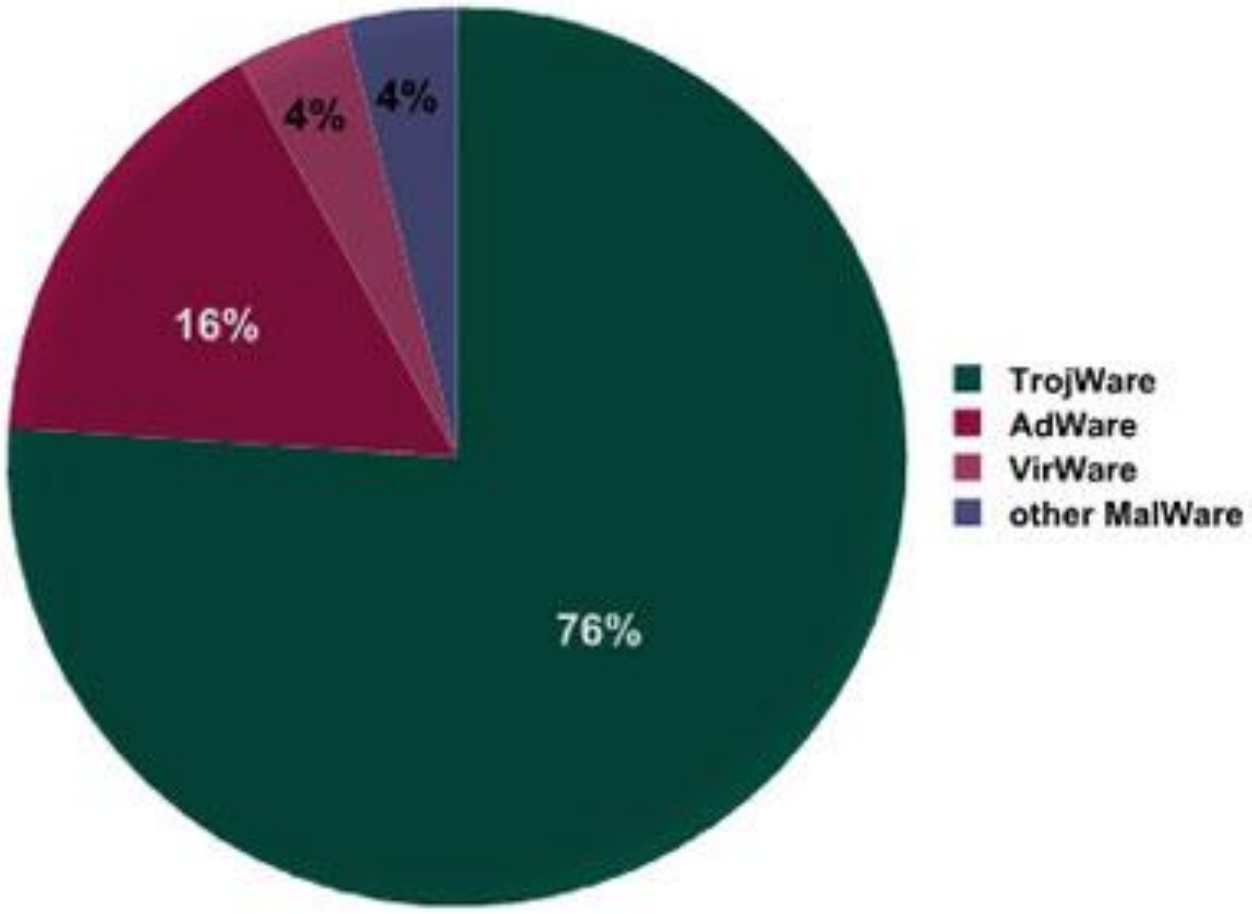
ФИШИНГ

Фи́шинг (англ. *phishing*, от *password* — пароль и *fishing* — рыбная ловля, выуживание) — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям.

Мошенниками (фишерами) часто используются адреса с опечатками, поддельные веб-сайты, внешне не отличимый от настоящего. (**yndex.ru**)

Письма, которые якобы отправлены из банка. В письме часто содержится прямая ссылка на сайт, где надо ввести пароль

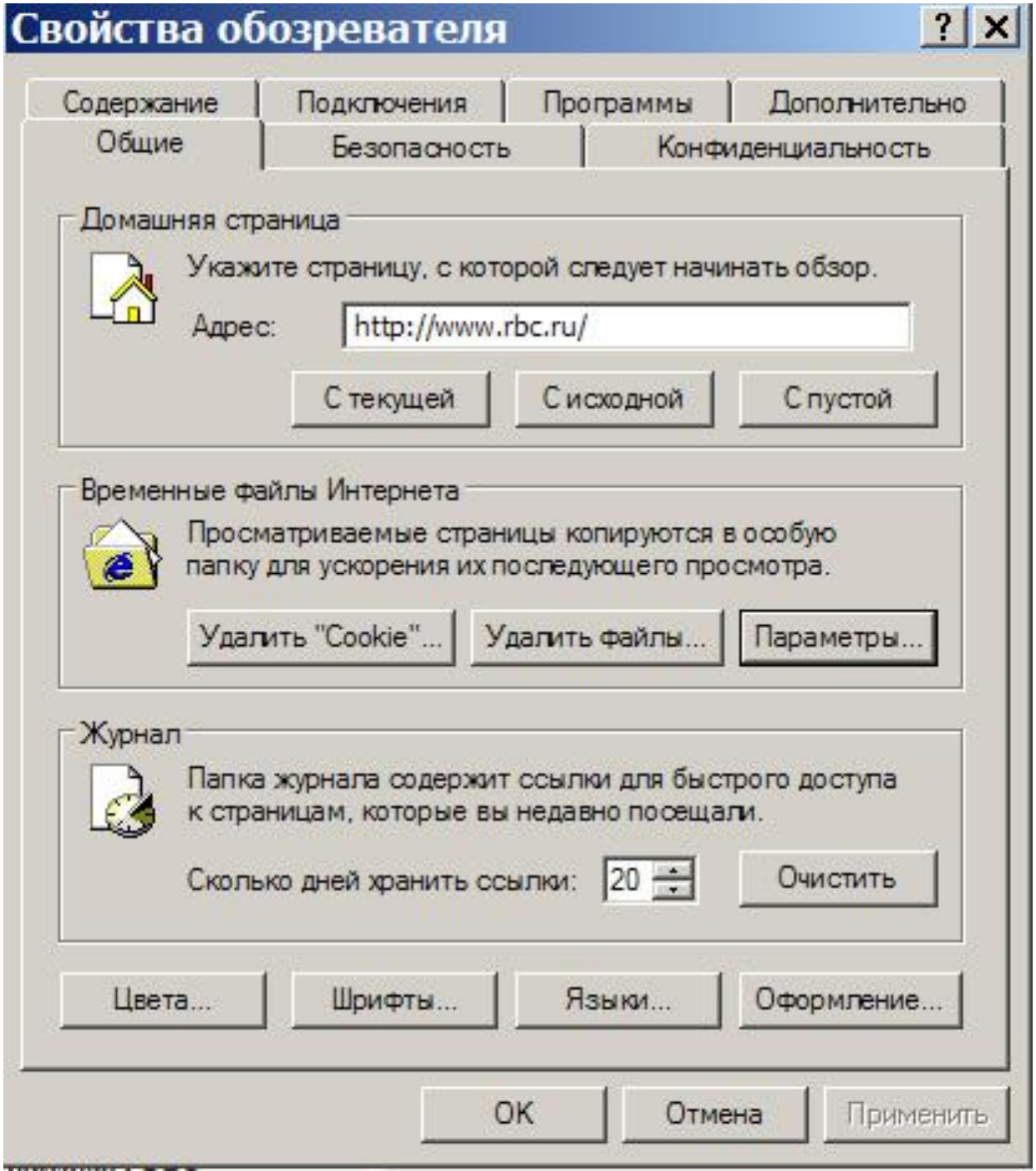
Распределение вредоносных программ по классам, июль 2008

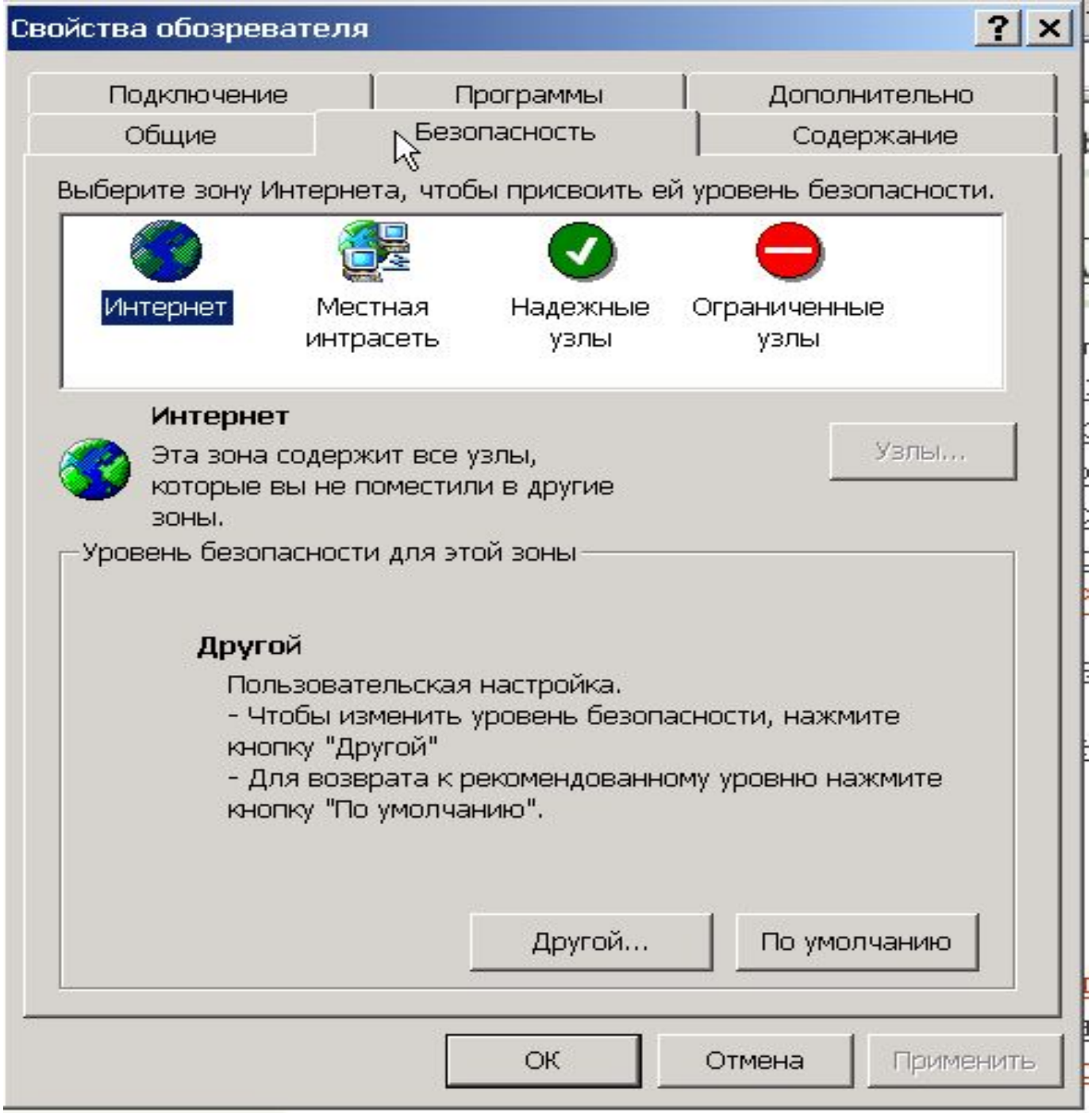


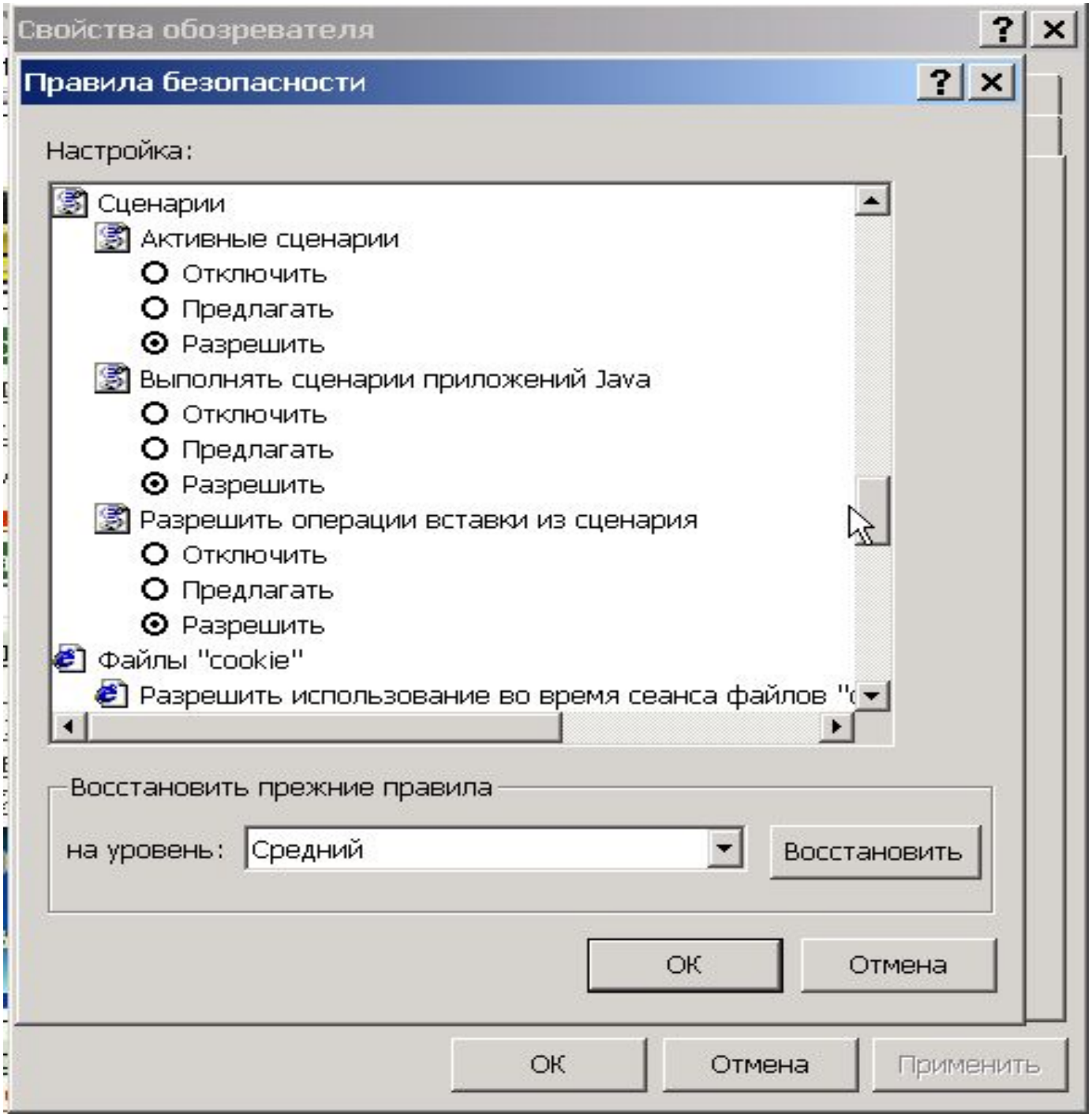
Методы защиты

- общие
- профилактические меры
- специализированные программы

- Ограничение доступа
- Дублирование, резервное копирование
- Пакеты антивирусных программ


Свойства обозревателя
Содержание
Подключения
Программы
Дополнительно
Общие
Безопасность
Конфиденциальность
Домашняя страница
Укажите страницу, с которой следует начинать обзор.
Адрес:
http://www.rbc.ru/
С текущей
С исходной
С пустой
Временные файлы Интернета
Просматриваемые страницы копируются в особую папку для ускорения их последующего просмотра.
Удалить "Cookie"...
Удалить файлы...
Параметры...
Журнал
Папка журнала содержит ссылки для быстрого доступа к страницам, которые вы недавно посещали.
Сколько дней хранить ссылки:
20
Очистить
Цвета...
Шрифты...
Языки...
Оформление...
OK
Отмена
Применить


Свойства обозревателя
Подключение
Программы
Дополнительно
Общие
Безопасность
Содержание
Выберите зону Интернета, чтобы присвоить ей уровень безопасности.
Интернет
Местная интрасеть
Надежные узлы
Ограниченные узлы
Интернет
Эта зона содержит все узлы, которые вы не поместили в другие зоны.
Узлы...
Уровень безопасности для этой зоны
Другой
Пользовательская настройка.
- Чтобы изменить уровень безопасности, нажмите кнопку "Другой"
- Для возврата к рекомендованному уровню нажмите кнопку "По умолчанию".
Другой...
По умолчанию
ОК
Отмена
Применить


Свойства обозревателя
Правила безопасности
Настройка:
Сценарии
Активные сценарии
Отключить
Предлагать
Разрешить
Выполнять сценарии приложений Java
Отключить
Предлагать
Разрешить
Разрешить операции вставки из сценария
Отключить
Предлагать
Разрешить
Файлы "cookie"
Разрешить использование во время сеанса файлов "
Восстановить прежние правила
на уровень:
Средний
Восстановить
ОК
Отмена
ОК
Отмена
Применить

Защита от вирусов по почте

- Не открывать вложения от незнакомцев
- «Хороший провайдер» (mail.ru)
- Антивирусные программы, проверяющие почту

Антивирусные системы

- **антивирус – это не просто программа, а сложная система, предоставляющая целый комплекс услуг**

Методы защиты

- ***Защита от «известных» программных продуктов - использование*** **сигнатурной базы**
- ***Защита от «неизвестных» программных продуктов - использование*** **так называемых эвристических (поведенческих) анализаторов, не требующих наличия сигнатурной базы.**

По прогнозам в 2009 году в мире появится более 20 млн новых вредоносных программ, поэтому несмотря на то, что **сигнатурный** подход по-прежнему будет использоваться и развиваться, будущее - в превентивной и проактивной защите компьютера пользователя.

Антивирусные системы

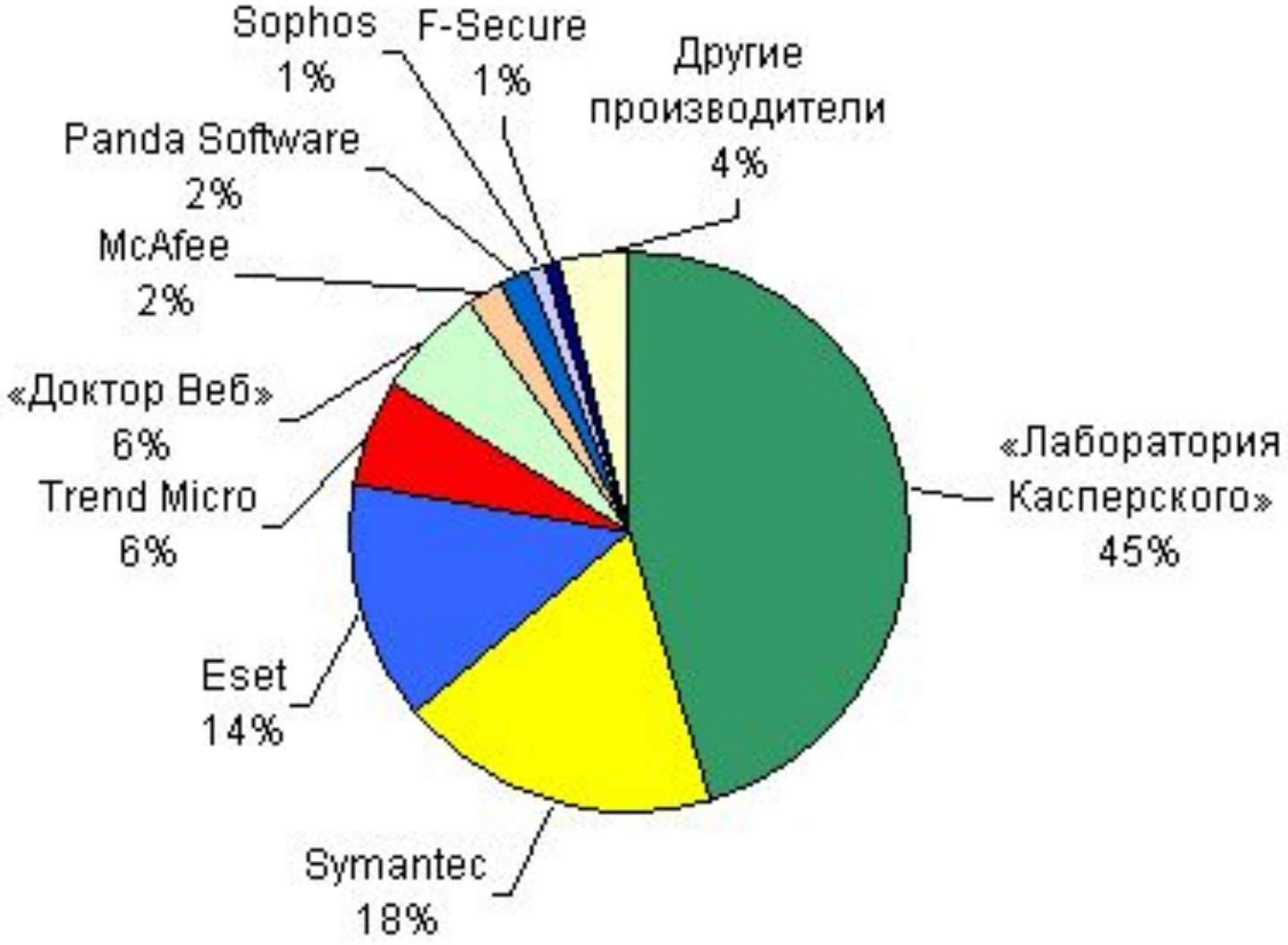
- Panda Antivirus
- Avira Antivir Premium
- Sophos Anti-Virus.
- Касперский Antivirus (AVP, KAV) вер.
- Symantec Norton Antivirus
- Eset Nod32
- McAfee Antivirus
- DrWeb
- Dr Solomons Antivirus

Будьте внимательны!

- Agtinum Outpost Antivirus Pro
- Pc-Cillins
- Adinf
- CleanCIH
- Avast! Home edition (бесплатный)
- ClamWin AntiVirus (бесплатный)
- AVG Antivirus (бесплатный)

- ***Не устанавливайте две антивирусных программы!***

Доли основных систем антивирусной защиты в России в 2008 году



Определены самые быстрые антивирусы (сент. 2008)

Портал Anti-Malware.ru подвел итоги первого теста антивирусных продуктов на быстродействие и потребление системных ресурсов. Самыми быстрыми антивирусами (Platinum Award) были признаны Panda Antivirus 2008, Avira Antivir Premium 8.1.00.331 и Sophos Anti-Virus 7.3.3.

Среди других победителей тестирования (Gold Award от Anti-Malware.ru) российскому пользователю известны Symantec Norton (номинация «Самые быстрые антивирусные сканеры по требованию, on-demand сканеры») и продукт Eset Nod32, получивший награды во всех четырех номинациях. Продукты от «Лаборатории Касперского», Agnitum, Dr.Web получили, в основном, «серебро».

Типовой состав систем

Основные программы:

- монитор
- сканер
- *защита почты*
- *защита офисных программ*
- *защита в интернете*
- *Удаление троянов, руткитов и т.п.*

Антивирусные базы

- базы должны постоянно обновляться

компоненты антивирусных систем

- **Фильтр** (сторож, монитор) – всегда включен, может замедлять работу компьютера
  (***Проверка в режиме реального времени***)

- **Сканер** – просмотр содержания всех потенциально опасных файлов, работает не постоянно
  (***Проверка по требованию***)

- **Ревизор** – просмотр информации о файлах, выявление незарегистрированных изменений, работает не постоянно


Norton AntiVirus
LiveUpdate
Options
Help & Support
Norton AntiVirus
Status
Scan for Viruses
Reports
System Status: OK
Security Scanning Features
Auto-Protect On
Internet Worm Protection On
Email Scanning On
Full System Scan 02.03.2007
Subscription Service
Virus Definitions 02.03.2007
Renewal Date 23.02.2008
Automatic LiveUpdate On
Auto-Protect
Provides continuous protection from viruses and other malicious threats.
More Info
symantec.
Norton AntiVirus 2005

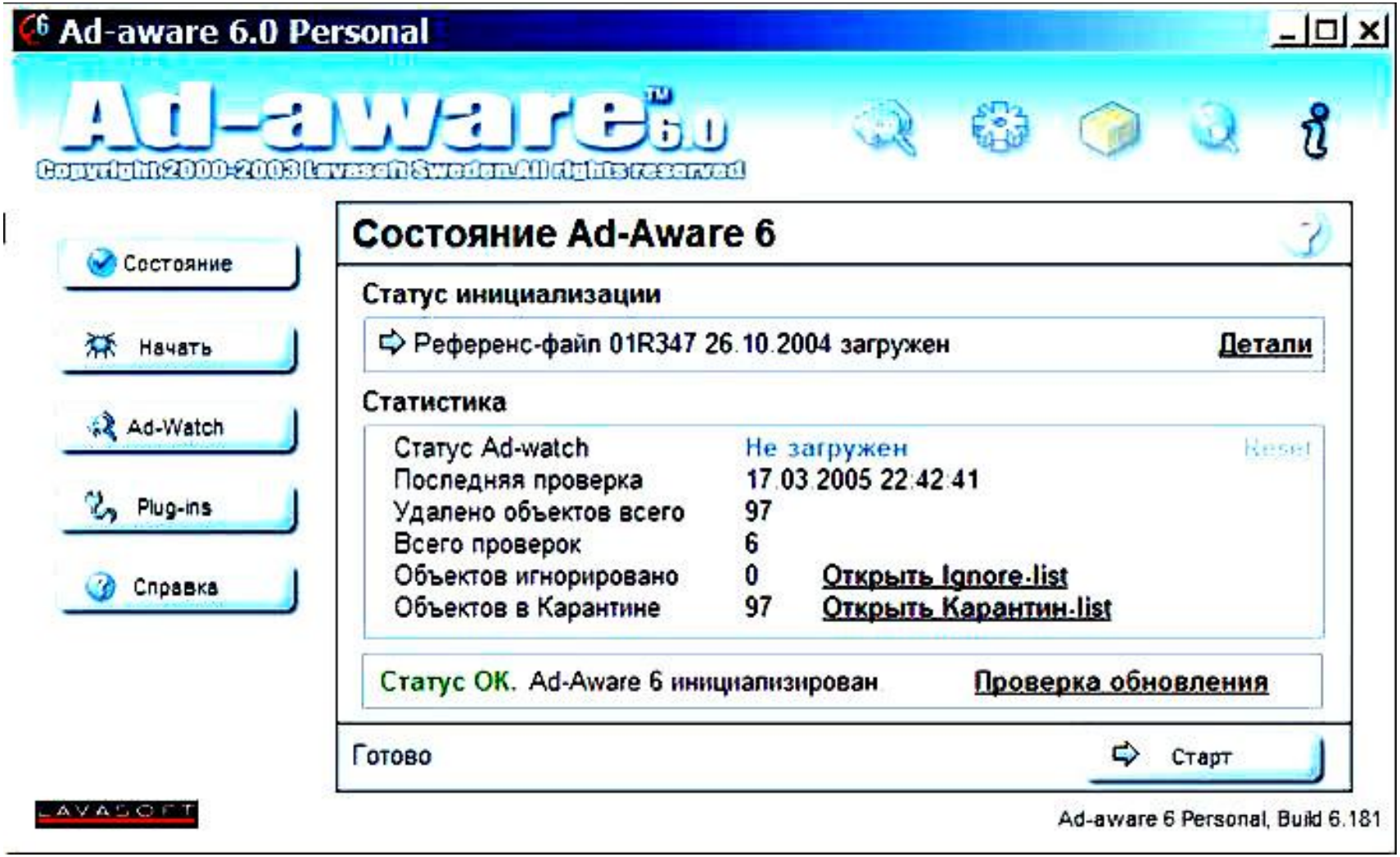
Борьба с троянами и активным содержанием

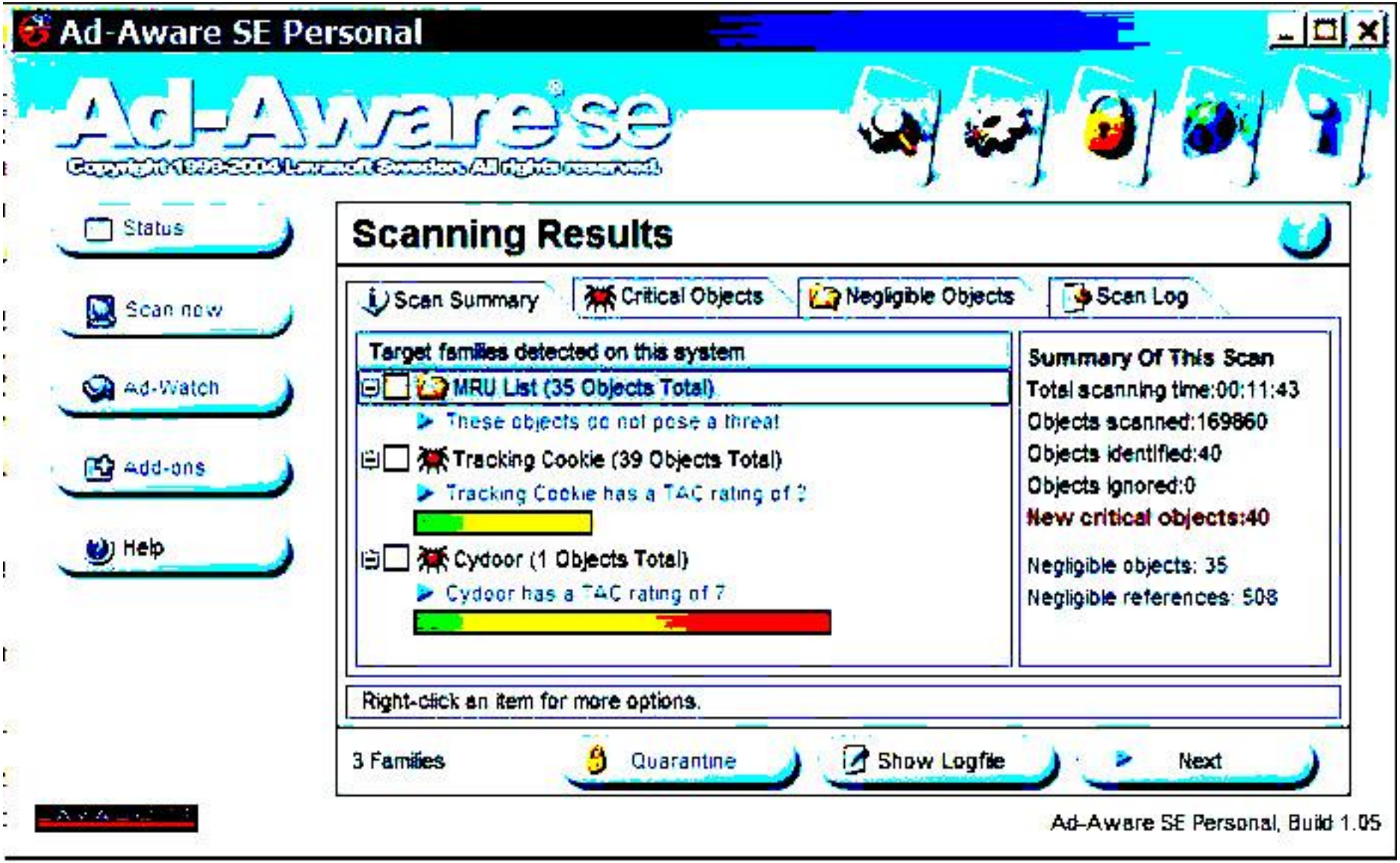
Специальные программы:

Ad-aware, SpyBot:

- уничтожают известные трояны,
- клавиатурные регистраторы,
- активные программы,
- ссылки на нежелательные сайты,
- агрессивную рекламу,
- нежелательные «усовершенствования» ***Internet Explorer***

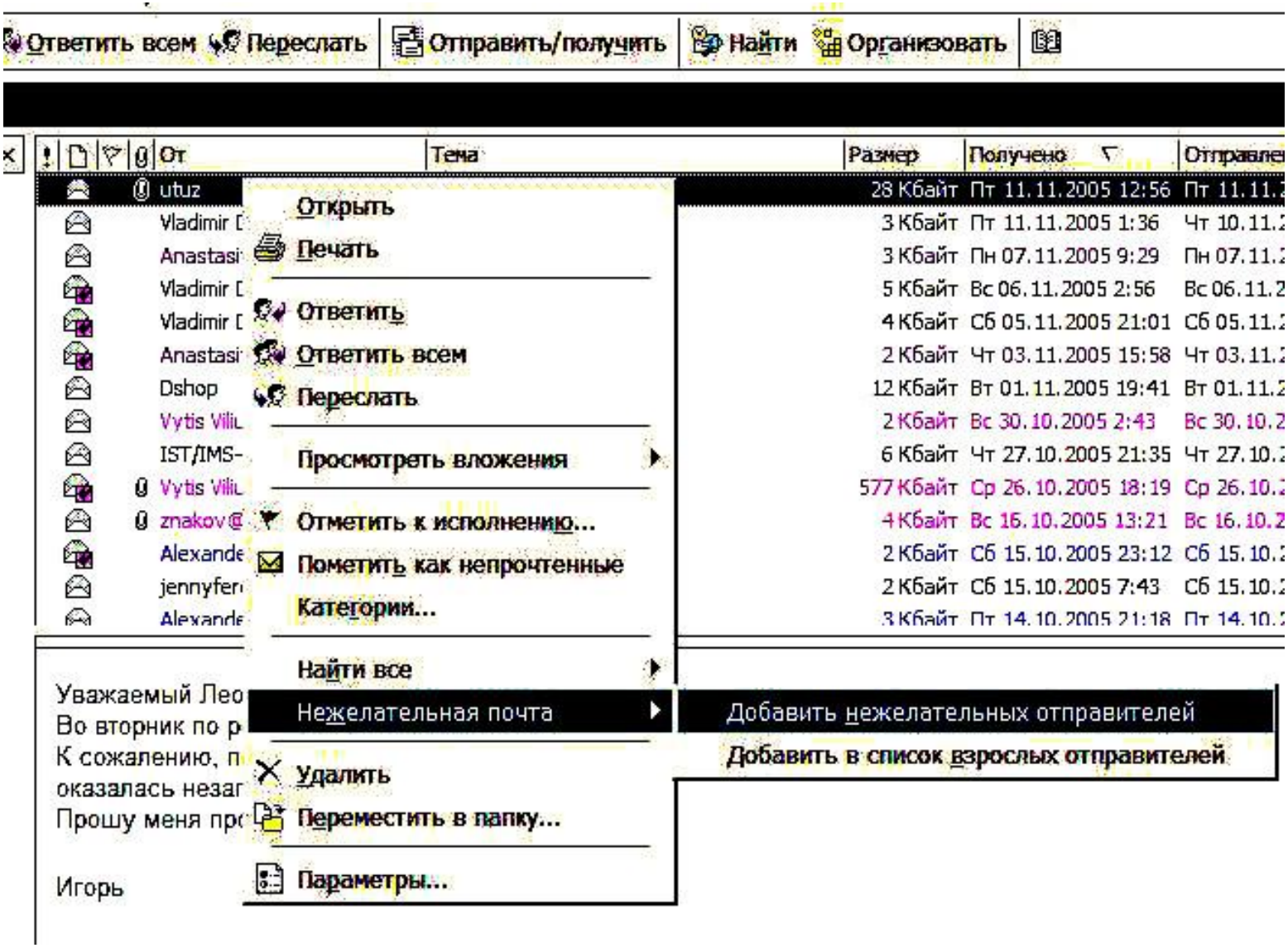
сайт разработчика
www.lavasoft.com

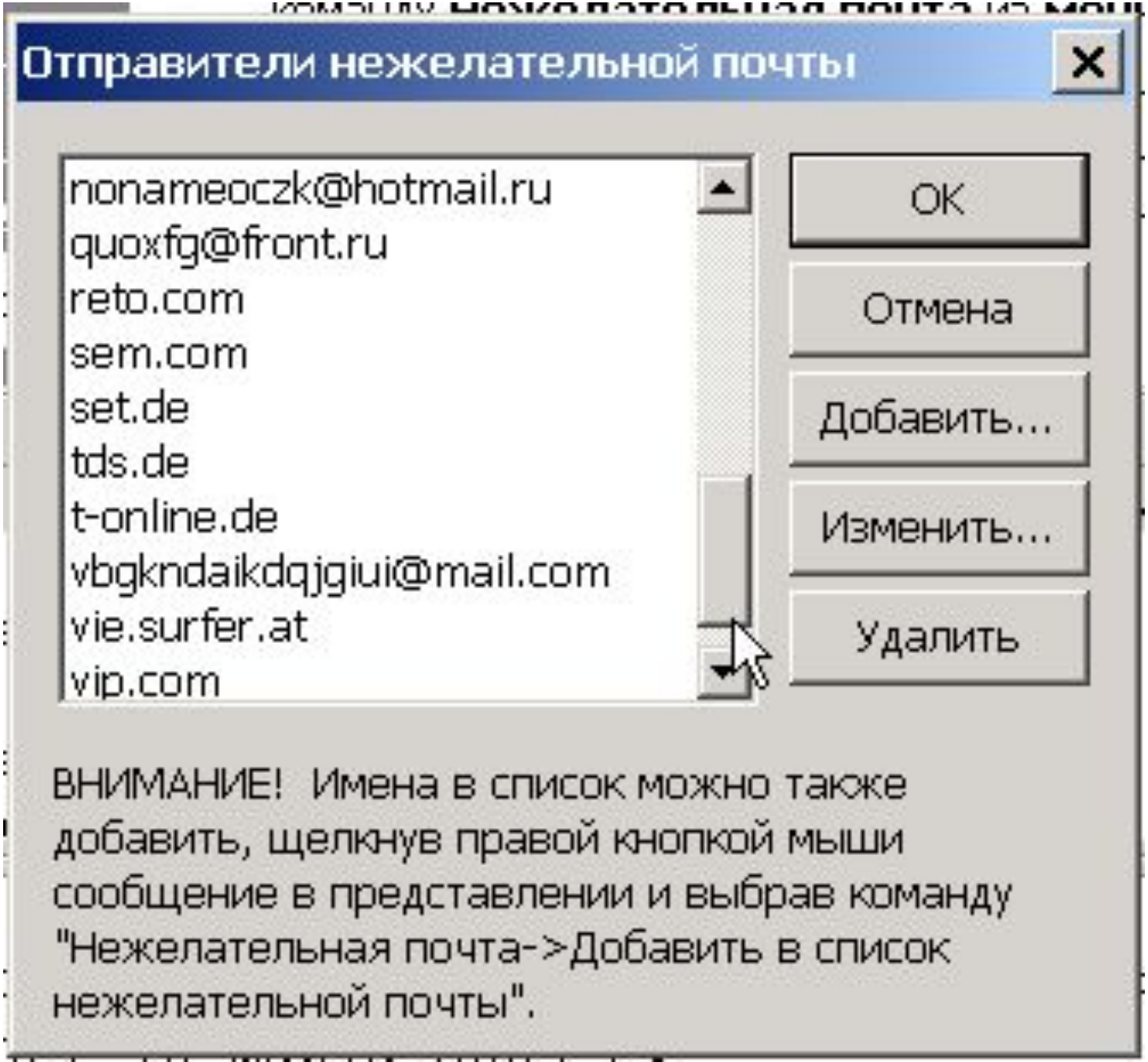



Ad-Aware SE Personal
Ad-Aware se
Copyright © 1999-2004 Lavasoft Sweden. All rights reserved.
Status
Scan now
Ad-Watch
Add-ons
Help
Scanning Results
Scan Summary
Critical Objects
Negligible Objects
Scan Log
Target families detected on this system
MRU List (35 Objects Total)
These objects do not pose a threat
Tracking Cookie (39 Objects Total)
Tracking Cookie has a TAC rating of 2
Cydoor (1 Objects Total)
Cydoor has a TAC rating of 7
Summary Of This Scan
Total scanning time:00:11:43
Objects scanned:169860
Objects identified:40
Objects ignored:0
New critical objects:40
Negligible objects: 35
Negligible references: 508
Right-click an item for more options.
3 Families
Quarantine
Show Logfile
Next
Ad-Aware SE Personal, Build 1.05


Ad-Aware SE Personal
Ad-Aware se
Copyright 1999-2004 Lavasoft Sweden. All rights reserved.
Status
Scan now
Ad-Watch
Add-ons
Help
Scanning Results
Scan Summary
Critical Objects
Negligible Objects
Scan Log
Target families detected on this system
MRU List (35 Objects Total)
These objects do not pose a threat.
Tracking Cookie (39 Objects Total)
Tracking Cookie has a TAC rating of 3
Cydoor (1 Objects Total)
Summary Of This Scan
Total scanning time:00:11:43
Objects scanned:169860
Objects identified:40
Objects ignored:0
New critical objects:40
Negligible objects: 35
Negligible references: 508
Next
Ad-Aware SE Personal, Build 1.05
Ad-Aware SE
75 objects will be removed. Continue?
OK
Cancel

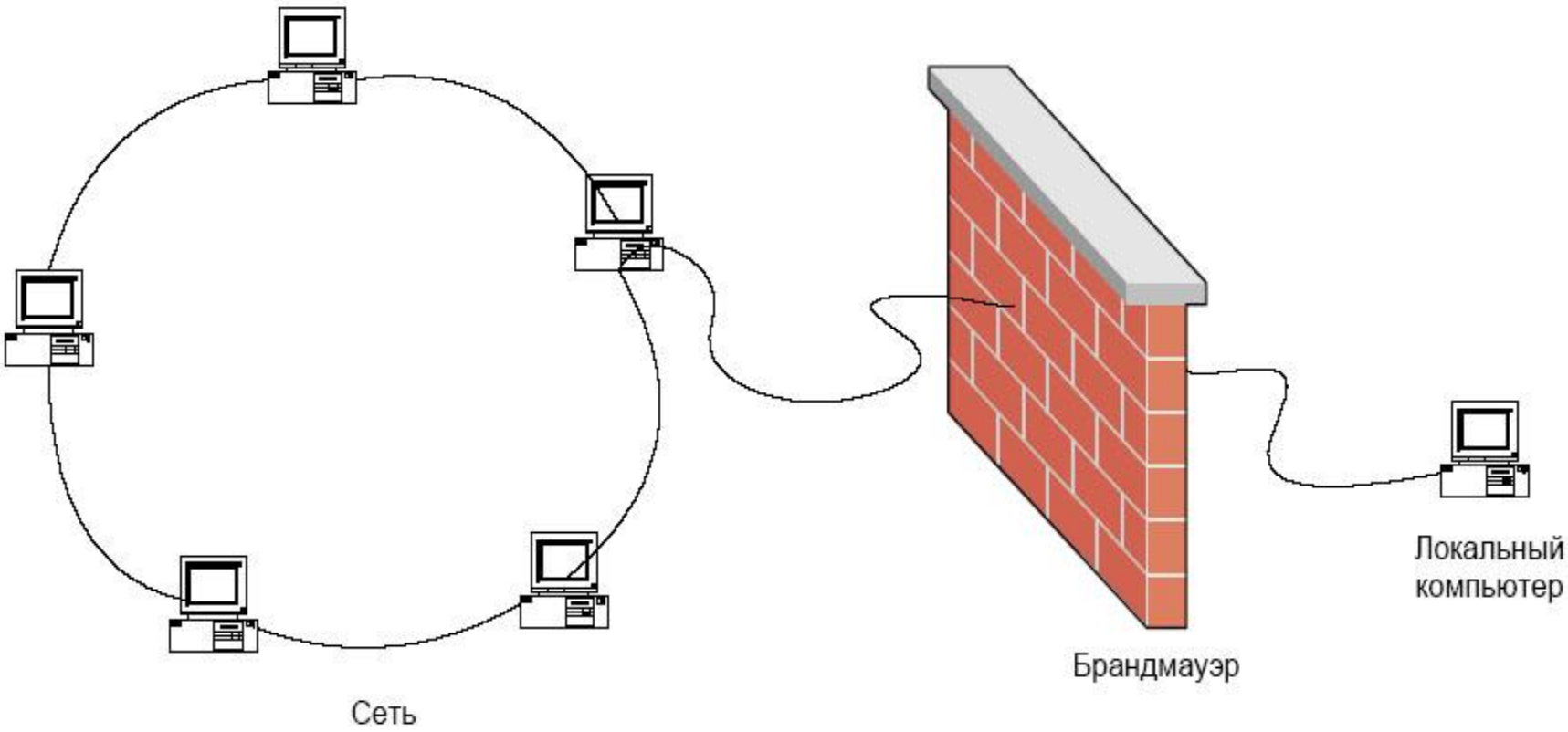
Нежелательная почта




Отправители нежелательной почты
nonameoczk@hotmail.ru
quoxfg@front.ru
reto.com
sem.com
set.de
tds.de
t-online.de
vbgkndaikdqjgiui@mail.com
vie.surfer.at
vip.com
OK
Отмена
Добавить...
Изменить...
Удалить
ВНИМАНИЕ! Имена в список можно также добавить, щелкнув правой кнопкой мыши сообщение в представлении и выбрав команду "Нежелательная почта->Добавить в список нежелательной почты".

Брандмауэр (Firewall)

Регулятор доступа в компьютерную сеть.
Проверяет входящие и выходящие потоки данных



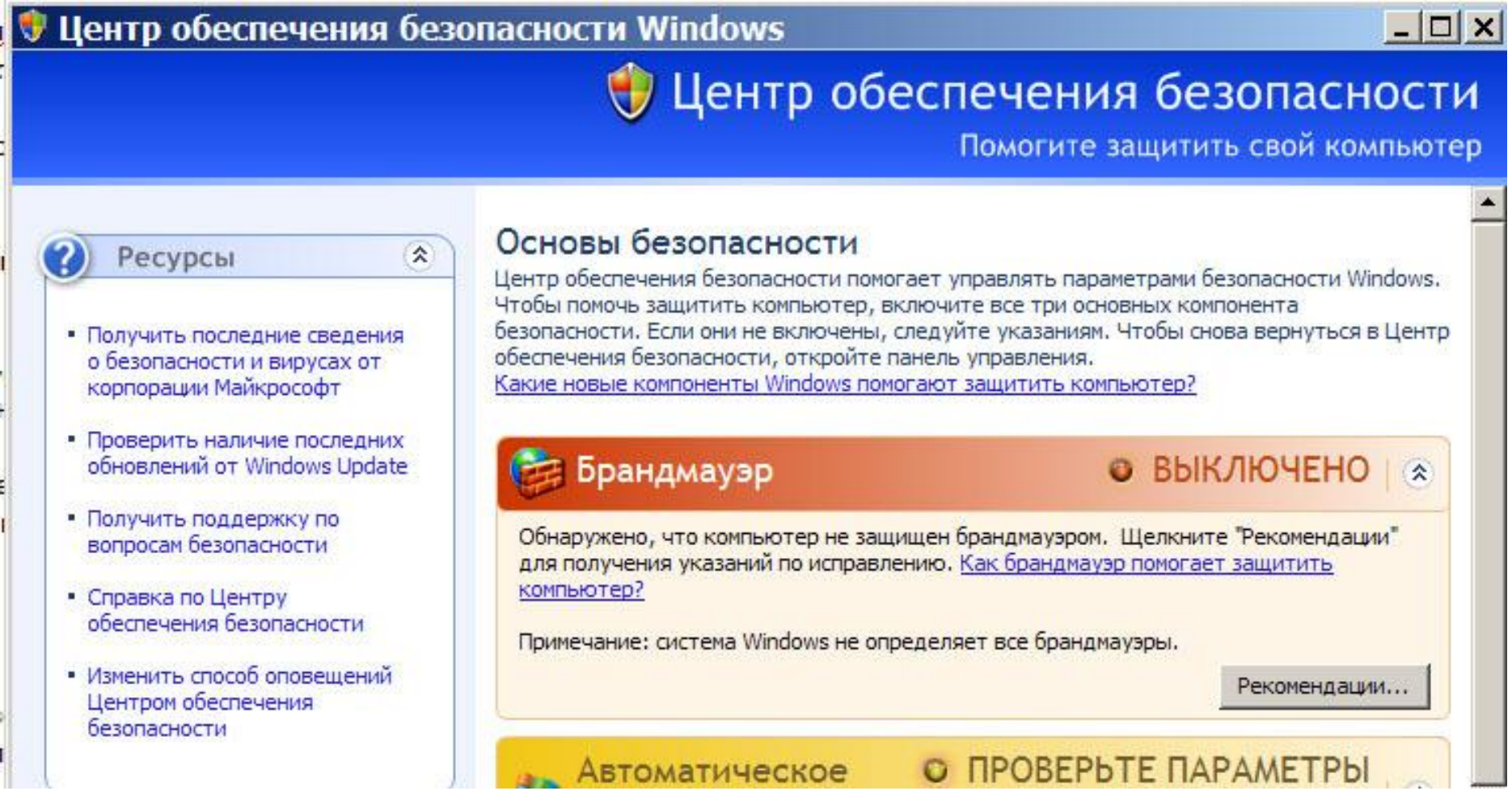
Traffic Logs:

Time	Action	Direction	Proto...	Local IP	Local...	Remote Host	Remote ...	Application
03/21/2005 11:12:03 PM	Allowed	Outbou...	TCP	213.145.35.132	2220	ad.adriver.ru	80	C:\Program
03/21/2005 11:12:53 PM	Blocked	Inbound	TCP	213.145.35.132	1025	213.145.35.46	3417	C:\WINDO
03/21/2005 11:12:57 PM	Blocked	Inbound	TCP	213.145.35.132	1025	213.145.35.46	3417	C:\WINDO
03/21/2005 11:13:02 PM	Blocked	Inbound	TCP	213.145.35.132	1025	213.145.35.46	3417	C:\WINDO
03/21/2005 11:13:37 PM	Blocked	Inbound	TCP	213.145.35.132	2745	213.145.35.46	4337	-na
03/21/2005 11:13:40 PM	Blocked	Inbound	TCP	213.145.35.132	2745	213.145.35.46	4337	-na
03/21/2005 11:13:46 PM	Blocked	Inbound	TCP	213.145.35.132	2745	213.145.35.46	4337	-na
03/21/2005 11:13:52 PM	Blocked	Inbound	TCP	213.145.35.132	1025	213.145.35.111	2846	C:\WINDO
03/21/2005 11:13:55 PM	Allowed	Outbou...	TCP	213.145.35.132	2222	pop.inbox.ru	110	C:\Program
03/21/2005 11:13:56 PM	Blocked	Inbound	TCP	213.145.35.132	1025	213.145.35.111	2846	C:\WINDO
03/21/2005 11:13:56 PM	Allowed	Outbou...	TCP	213.145.35.132	2224	pop.mail.ru	110	C:\Program
03/21/2005 11:13:57 PM	Allowed	Outbou...	TCP	213.145.35.132	2226	mail.zebrateleco...	25	C:\Program
03/21/2005 11:13:59 PM	Allowed	Outbou...	TCP	213.145.35.132	2228	pop.mail.ru	110	C:\Program
03/21/2005 11:14:00 PM	Allowed	Outbou...	TCP	213.145.35.132	2230	pop3.psycholog...	110	C:\Program
03/21/2005 11:14:01 PM	Blocked	Inbound	TCP	213.145.35.132	3140	213.145.35.46	4824	-na
03/21/2005 11:14:02 PM	Blocked	Inbound	TCP	213.145.35.132	1025	213.145.35.111	2846	C:\WINDO
03/21/2005 11:14:03 PM	Blocked	Inbound	TCP	213.145.35.132	3140	213.145.35.46	4824	-na
03/21/2005 11:14:09 PM	Blocked	Inbound	TCP	213.145.35.132	3140	213.145.35.46	4824	-na
03/21/2005 11:14:22 PM	Blocked	Inbound	TCP	213.145.35.132	80	213.145.35.46	1274	-na

Виды:

- Аппаратные (специализированные компьютеры)
- Программные (программа на компьютере пользователя)
- Стандартные
- Специальные (OutPost, Ontrack)

Стандартный Брандмауэр Windows XP sp2



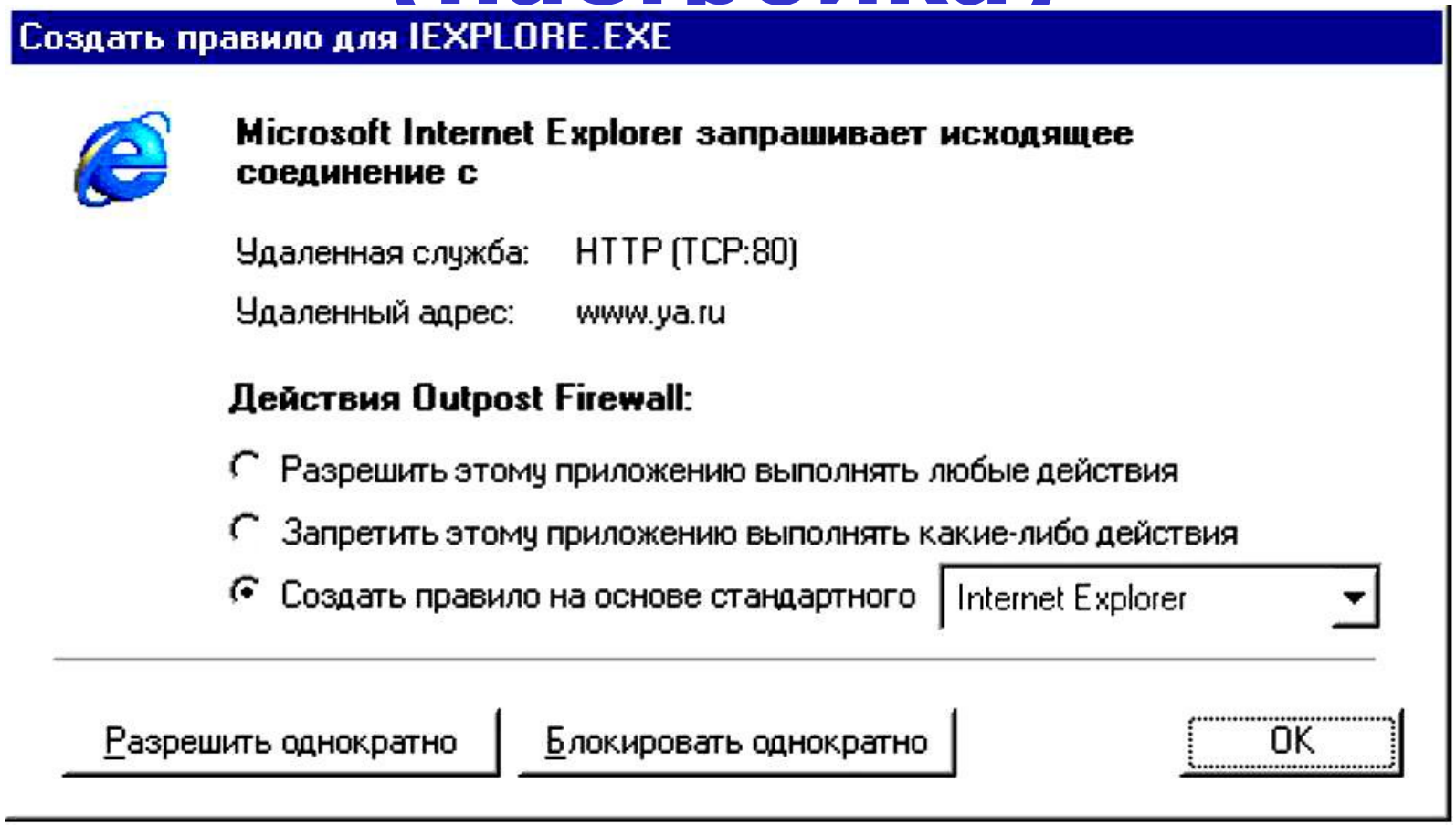
OutPost

Русский интерфейс, Дает возможности:

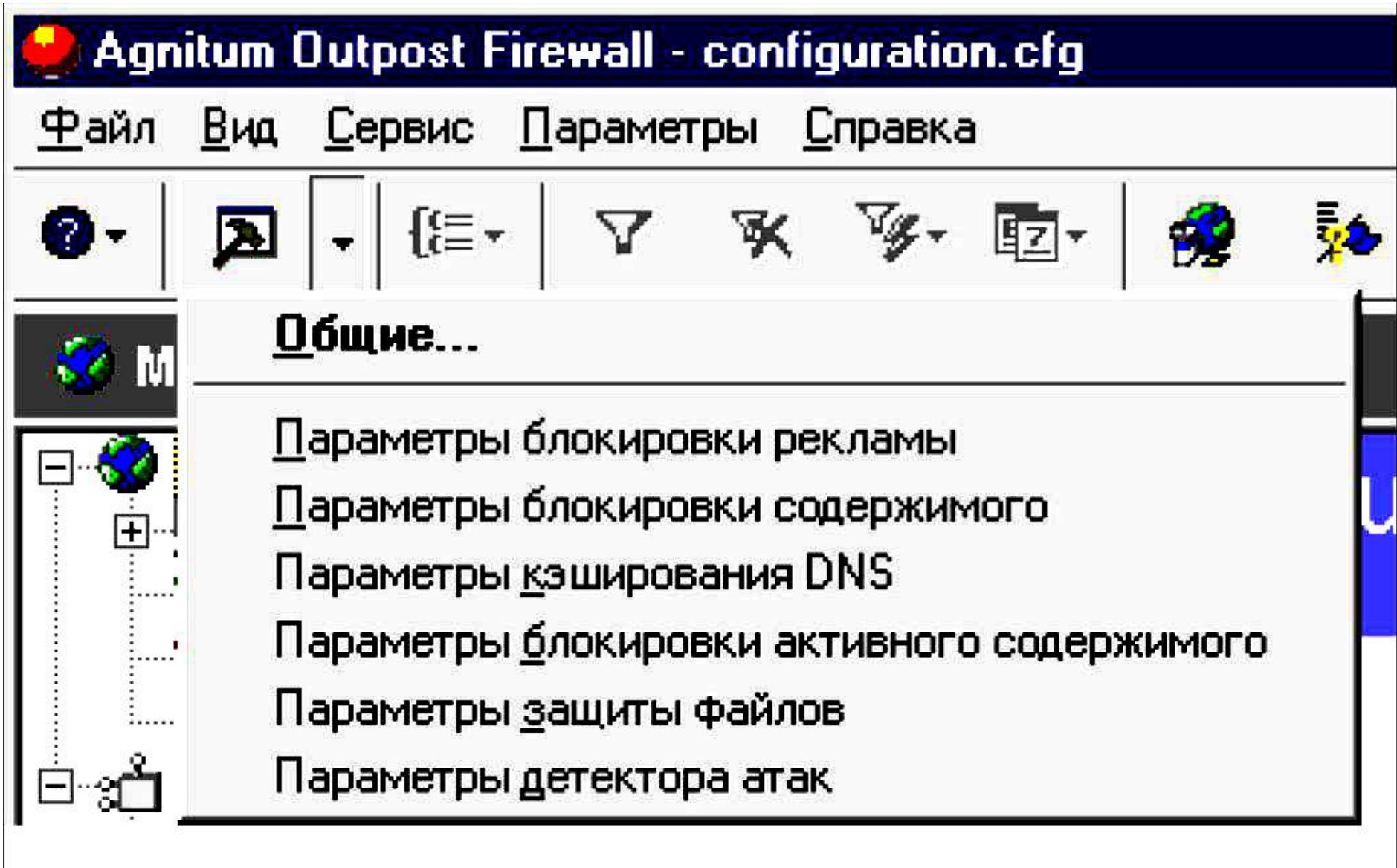
- Ограничить список приложений, получающих доступ в сеть;
- Запретить или ограничить поступление на локальный компьютер незатребованной информации, в частности:
  - банерной рекламы;
  - всплывающих окон в Web-страницах;
  - данных с определенных Web-страниц.
- Ограничить или запретить использование программных компонент, встроенных в Интернет-страницы

- Ограничить или запретить использование cookie.
- Определить зону «дружественных» IP-адресов
- Осуществлять проверку поступающих по электронной почте присоединенных файлов.
- Выдавать предупреждение при попытке атаковать Ваш компьютер из сети и предотвращать такие попытки.
- Сделать компьютер невидимым в сети
- Использовать DNS кэш

Предупреждение о сетевом взаимодействии (настройка)



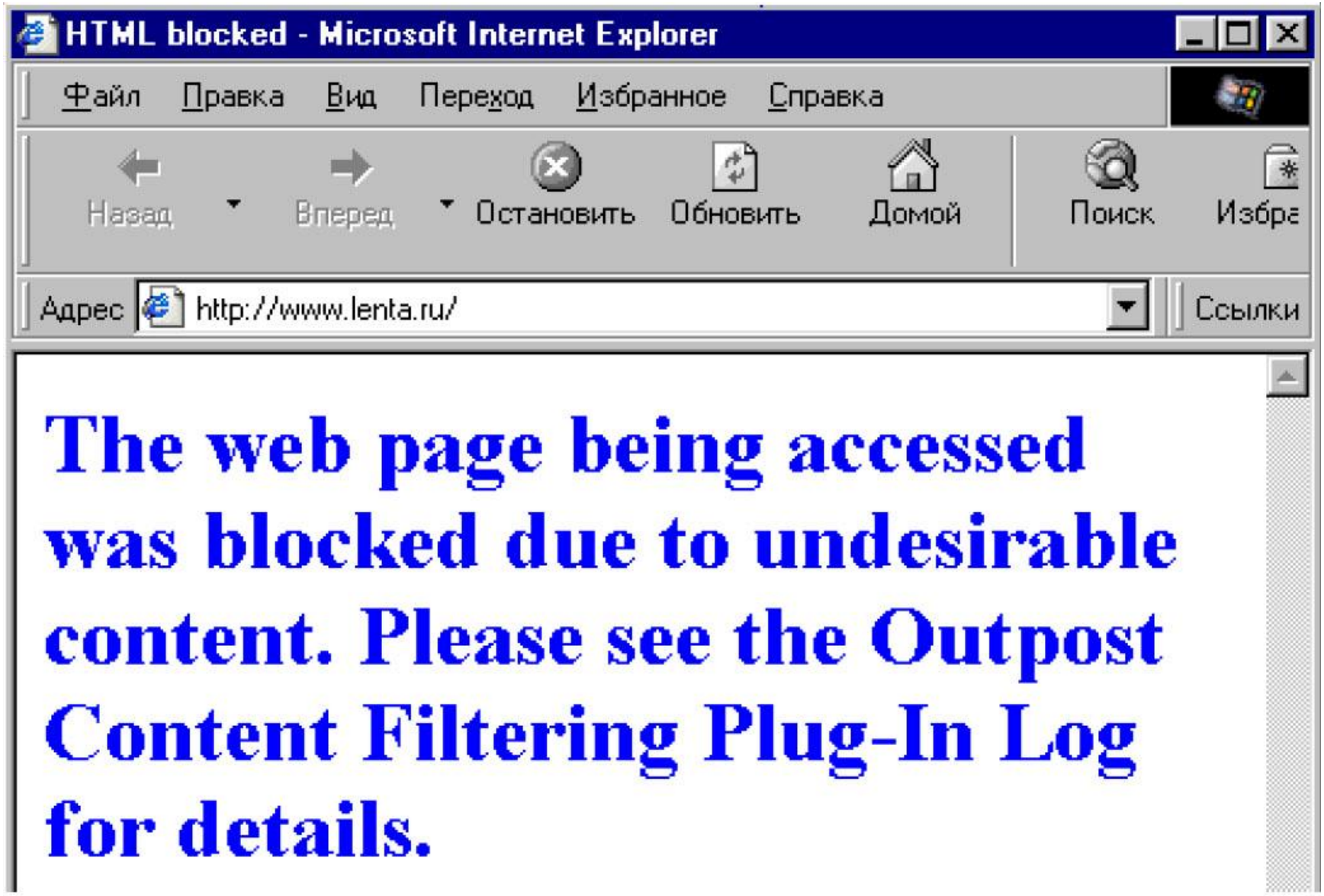
Параметры настройки

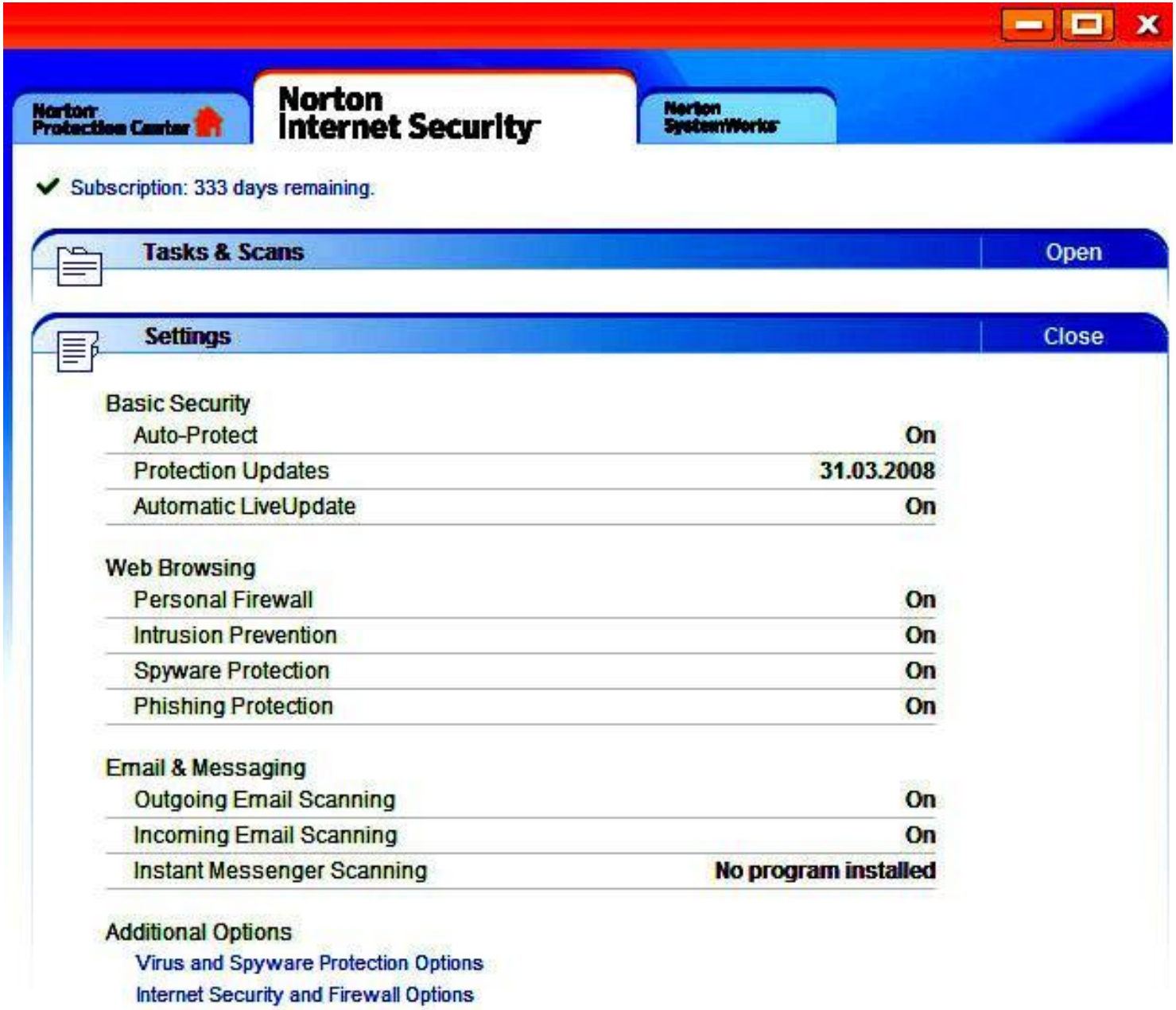


Параметры блокирования web-страниц

- По размеру графических файлов
- По тексту на страницах
- По адресу

Пример блокировки по содержанию




Norton Protection Center
Norton Internet Security
Norton SystemWorks
Subscription: 333 days remaining.
Tasks & Scans
Open
Settings
Close
Basic Security
Auto-Protect On
Protection Updates 31.03.2008
Automatic LiveUpdate On
Web Browsing
Personal Firewall On
Intrusion Prevention On
Spyware Protection On
Phishing Protection On
Email & Messaging
Outgoing Email Scanning On
Incoming Email Scanning On
Instant Messenger Scanning No program installed
Additional Options
Virus and Spyware Protection Options
Internet Security and Firewall Options


Norton Internet Security
Internet Security and Firewall Options
Help
System
General Settings
Personal Firewall
General Settings
Program Control
Trust Control
Advanced Settings
Intrusion Prevention
General Settings
AutoBlock
LiveUpdate
General Settings
Security Inspector
General Settings
PERSONAL FIREWALL: Program Control
Create custom Internet access settings for individual programs.
Program
Access
memolite_im
C:\Program Files\MemoriRuToolbarLite\memolite_im.exe
Custom
Microsoft Generic Host Process for Win32 Services
C:\WINDOWS\system32\svchost.exe
Auto
Microsoft Internet Explorer
C:\Program Files\Internet Explorer\iexplore.exe
Custom
Microsoft Outlook
C:\Program Files\Microsoft Office\Office12\OUTLOOK.EXE
Auto
Microsoft Printer Spooler Service
C:\WINDOWS\system32\spoolsv.exe
Custom
Allow
Block
Custom
Microsoft Router Identifier
C:\WINDOWS\system32\tracert.exe
Microsoft Volume Shadow Copy Service
C:\WINDOWS\system32\dllhost.exe
Auto
Add...
Modify...
Remove...