

***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 нелегитимной 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

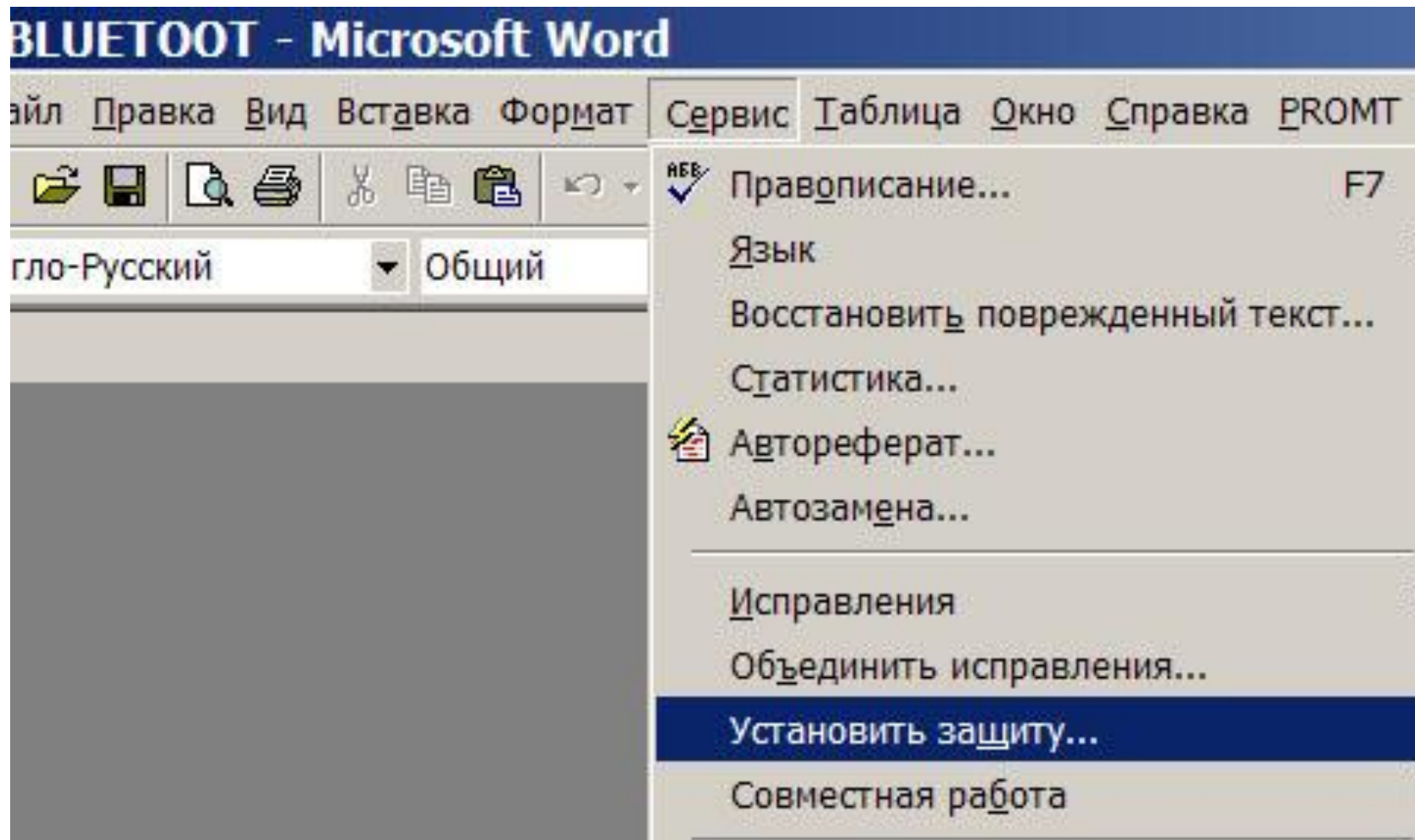
1. Физическое ограничение доступа
(отдельные помещения)
2. Парольная защита: (пароль должен быть достаточно сложным)
 - при включении компьютера (в SETUP)
 - при входе в операционную систему
 - при доступе к файлам
 - С помощью стандартных или специальных программ

(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

The image shows a dialog box titled "Защита документа" (Document Protection). The title bar includes a question mark icon and a close button (X). The main content area contains the instruction "Запретить любые изменения, кроме" (Prohibit any changes, except) followed by three radio button options: "записи исправлений" (record is corrections), "вставки примечаний" (insert per notes), and "ввода данных в поля форм:" (enter data in form fields:). A "Разделы..." (Sections...) button is positioned to the right of the third option. Below these options is a horizontal line, followed by the text "Пароль (необязателен):" (Password (optional):) and an empty text input field. At the bottom of the dialog are two buttons: "ОК" (OK) and "Отмена" (Cancel).

Защита документа ? X

Запретить любые изменения, кроме

- записи исправлений
- вставки примечаний
- ввода данных в поля форм: Разделы...

Пароль (необязателен):

ОК Отмена

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 записи
 - Локальные политики
 - Политика аудита
 - Назначение прав пользователя
 - Параметры безопасности
 - Политики открытого ключа
 - Файловая система EFS
 - Политики ограниченного использования
 - Политики безопасности IP на "Локальные"

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, Опытн...
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, Опытн...
Изменение параметров среды оборудования	Администраторы
Изменение системного времени	Администраторы, Опытные пользовате...
Локальный вход в систему	Гость, Администраторы, Пользователи, О...
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...	
Отказывать 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

The image shows a Windows XP file properties dialog for a file named 'OutpostInstall'. The dialog has several tabs: 'Общие', 'Версия', 'Совместимость', 'Цифровые подписи', and 'Сводка'. The 'Общие' tab is active, displaying file details such as type (Application), description (Agnitum Outpost Firewall 1.0), location (C:\Downloads), size (2.49 MB), and creation/modification dates. A security warning is present at the bottom, stating the file was obtained from another computer and is locked for protection. An 'Advanced Attributes' dialog is overlaid on top, showing options for indexing and compression. The 'Advanced Attributes' dialog has a title bar with a question mark and a close button. It contains a message: 'Установите подходящие параметры для этого файла.' Below this are two sections: 'Атрибуты индексирования и архивации' with checked options for 'File ready for archiving' and 'Index contents for fast search'; and 'Атрибуты сжатия и шифрования' with unchecked options for 'Compress contents to save disk space' and 'Encrypt contents to protect data'. A 'Подробнее...' button is next to the encryption option. At the bottom of the 'Advanced Attributes' dialog are 'OK' and 'Отмена' buttons. In the background, the 'Общие' tab of the main dialog shows 'Атрибуты' (None checked), 'Безопасность' (Warning), and 'Дополнительно...' (Advanced...) buttons. At the bottom of the main dialog are 'OK', 'Отмена', and 'Применить' buttons. On the right side of the main dialog, a 'Разделы...' button is visible.

Свойства: OutpostInstall

Общие | Версия | Совместимость | Цифровые подписи | Сводка

Outpost Install

Тип файла: Приложение

Описание: Agnitum Outpost Firewall 1.0

Размещение: C:\Downloads

Размер: 2.49 МБ (2 617 008 байт)

На диске: 2.49 МБ (2 617 344 байт)

Создан: 12 марта 2005 г., 17:00:56

Изменен: 12 марта 2005 г., 17:00:56

Открыт: 21 марта 2005 г., 21:53:45

Атрибуты: Только чтение Скрытый

Безопасность: Этот файл получен с другого компьютера и, возможно, был заблокирован с целью защиты компьютера.

Дополнительные атрибуты

Установите подходящие параметры для этого файла.

Атрибуты индексирования и архивации

- Файл готов для архивирования
- Индексировать содержимое для быстрого поиска

Атрибуты сжатия и шифрования

- Сжимать содержимое для экономии места на диске
- Шифровать содержимое для защиты данных

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 DiskWiper)
- Особые программы (утилиты) восстановления затертых файлов
(Ontrack EasyRecovery,
MARI Lab File Recovery for Office –
документы Office, даже после
форматирования диска)

Политика безопасности

The image shows a Windows Administrative Tools window titled "Администрирование". The main pane displays "Локальные параметры безопасности" (Local Security Policy). The left sidebar shows a tree view of security policies, with "Локальные политики" (Local Policies) expanded and "Политика безопасности" (Security Policy) selected. The main area shows a list of policies with their corresponding security parameters.

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,...
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	
Запуск операций по обслуживанию т...	Администраторы

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**, *malicious* — злонамеренный и *software* — 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
 - распространяются по компьютерной сети
- файловые
 - внедряются в выполняемые файлы
- загрузочные
 - внедряются в загрузочный сектор диска (Boot-сектор)
- резидентные
 - находятся в памяти, активны до выключения компьютера
- нерезидентные
 - не заражают память, являются активными ограниченное время
- Макровирусы
 - 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)

Троянская программа

(также — троян, троянец, троянский конь, трóй) — программа, используемая злоумышленником для сбора информации, её разрушения или модификации, нарушения работоспособности компьютера или использования его ресурсов в неблагоприятных 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** (*руткит*, от англ. *root kit*, то есть «набор root'a») — программа или набор программ для скрытия следов присутствия злоумышленника или вредоносной программы в системе.

нежелательное проникновение по сети проект *Honeynet*

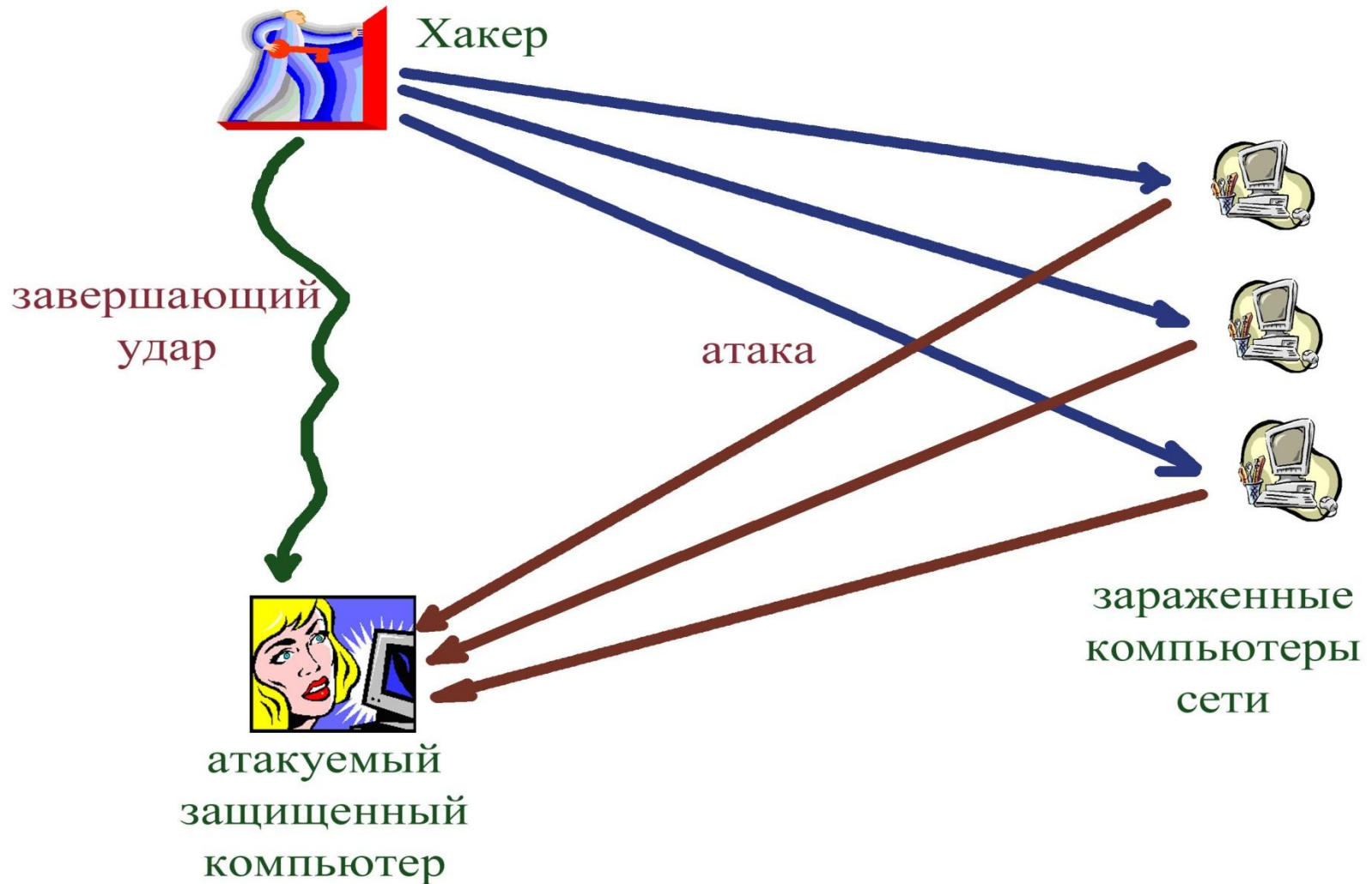
Длительное исследование сети с помощью подставных компьютеров
2005г.

- Каждые 10-100 сек. попытка проникновения в компьютер
- Для заражения используется широкий спектр уязвимостей, имеющих 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% приходится на веб-приложения.
- средним 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 трафике 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 nvsvfcsz
Юрист-Оформление ли...	_Юрист-Решение на оружие г
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 хbww

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>

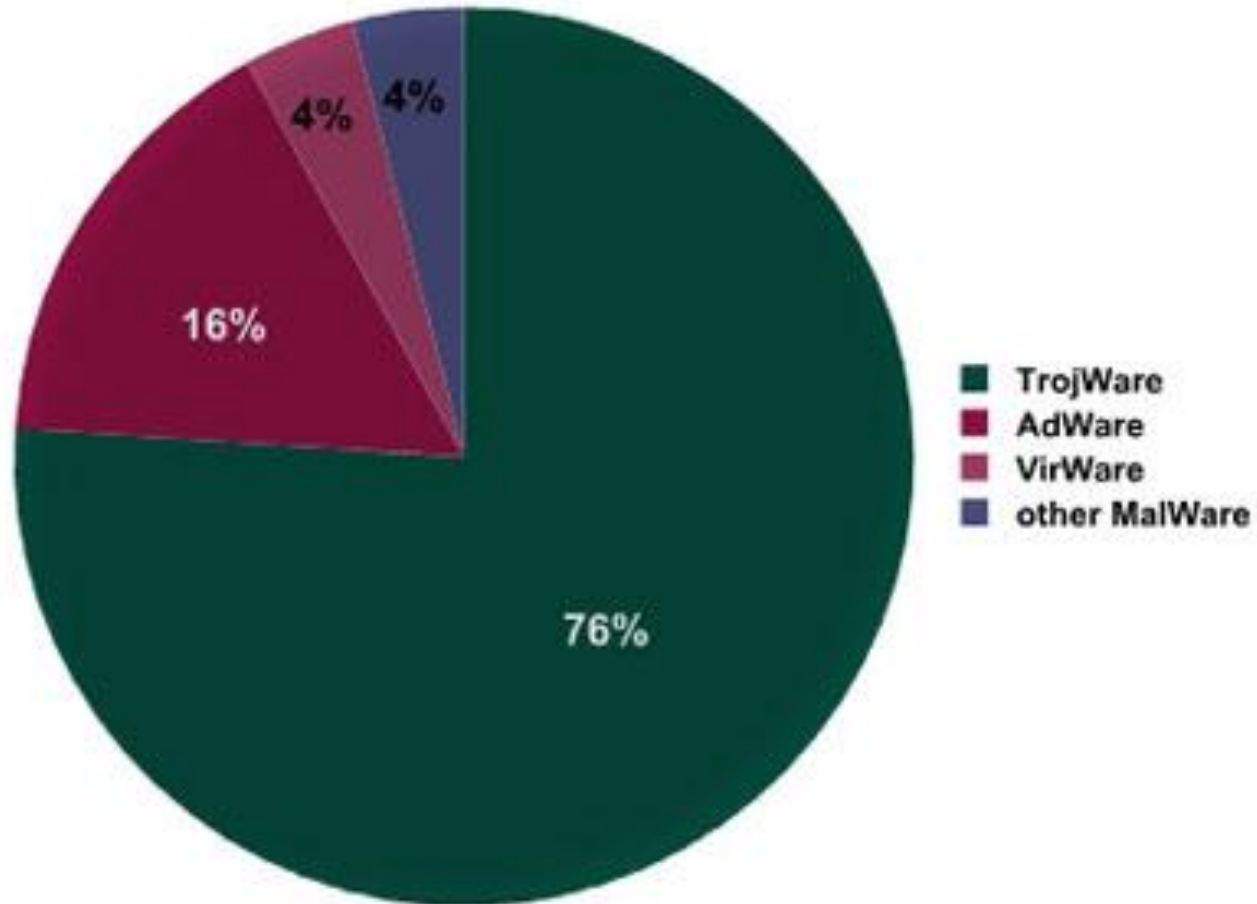
ФИШИНГ

Фйшинг (англ. *phishing*, от *password* — пароль и *ishing* — 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:

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:

Очистить

Цвета...

Шрифты...

Языки...

Оформление...

ОК

Отмена

Применить

Подключение

Программы

Дополнительно

Общие

Безопасность

Содержание

Выберите зону Интернета, чтобы присвоить ей уровень безопасности.



Интернет

Местная
интрасетьНадежные
узлыОграниченные
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

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

OK

Отмена

OK

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.*

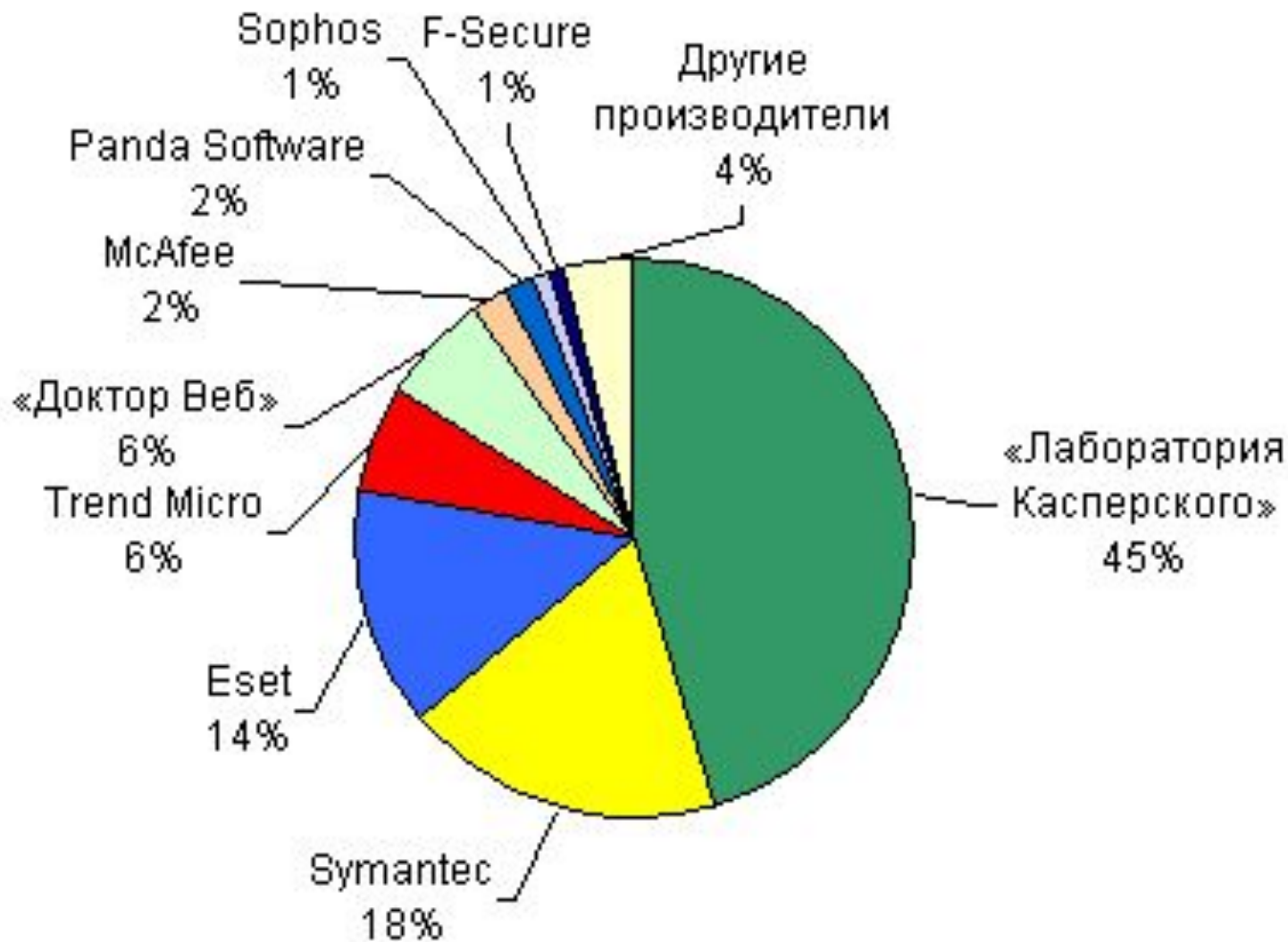
По прогнозам в 2009 году в мире появится более 20 млн новых вредоносных программ, поэтому несмотря на то, что **сигнатурный** подход по-прежнему будет использоваться и развиваться, будущее - в превентивной и проактивной защите компьютера пользователя.

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
- Agtinum Outpost Antivirus Pro
- Pc-Cillins
- Adinf
- CleanCIH
- Avast! Home edition (бесплатный)
- ClamWin AntiVirus (бесплатный)
- AVG Antivirus (бесплатный)
- *Не устанавливайте две антивирусных программы!*

Будьте внимательны!

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
- 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

Auto-Protect

Provides continuous protection from viruses and other malicious threats.

[More Info](#)

Subscription Service

	Virus Definitions	02.03.2007
	Renewal Date	23.02.2008
	Automatic LiveUpdate	On

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 6.0 Personal

Ad-aware™ 6.0
Copyright 2000-2003 Lavasoft Sweden. All rights reserved.

Состояние
Начать
Ad-Watch
Plug-ins
Справка

Состояние Ad-Aware 6

Статус инициализации

➔ Референс-файл 01R347 26.10.2004 загружен [Детали](#)

Статистика

Статус Ad-watch	Не загружен	Reset
Последняя проверка	17.03.2005 22:42:41	
Удалено объектов всего	97	
Всего проверок	6	
Объектов игнорировано	0	Открыть Ignore-list
Объектов в Карантине	97	Открыть Карантин-list

Статус **OK**. Ad-Aware 6 инициализирован [Проверка обновлений](#)

Готово [➔ Старт](#)

LAVASOFT

Ad-aware 6 Personal, Build 6.181

Ad-Aware[®] se

Copyright 1998-2004 Lavasoft AG. 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

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

Ad-Aware SE



75 objects will be removed. Continue?



OK



Cancel

gfile



Next

Нежелательная почта

Ответить всем
 Переслать
 Отправить/получить
 Найти
 Организовать

От	Тема	Размер	Получено	Отправле
utuz		28 Кбайт	Пт 11.11.2005 12:56	Пт 11.11.2005 12:56
Vladimir [mailto:vladimir@utuz.ru]		3 Кбайт	Пт 11.11.2005 1:36	Чт 10.11.2005 23:56
Anastasi [mailto:anastasi@utuz.ru]		3 Кбайт	Пн 07.11.2005 9:29	Пн 07.11.2005 9:29
Vladimir [mailto:vladimir@utuz.ru]		5 Кбайт	Вс 06.11.2005 2:56	Вс 06.11.2005 2:56
Vladimir [mailto:vladimir@utuz.ru]		4 Кбайт	Сб 05.11.2005 21:01	Сб 05.11.2005 21:01
Anastasi [mailto:anastasi@utuz.ru]		2 Кбайт	Чт 03.11.2005 15:58	Чт 03.11.2005 15:58
Dshop [mailto:dshop@utuz.ru]		12 Кбайт	Вт 01.11.2005 19:41	Вт 01.11.2005 19:41
Vytis Vilii [mailto:vytis.vilii@utuz.ru]		2 Кбайт	Вс 30.10.2005 2:43	Вс 30.10.2005 2:43
IST/DMS- [mailto:ist@dms-utuz.ru]		6 Кбайт	Чт 27.10.2005 21:35	Чт 27.10.2005 21:35
Vytis Vilii [mailto:vytis.vilii@utuz.ru]		577 Кбайт	Ср 26.10.2005 18:19	Ср 26.10.2005 18:19
znakov@utuz.ru		4 Кбайт	Вс 16.10.2005 13:21	Вс 16.10.2005 13:21
Alexandre [mailto:alexandre@utuz.ru]		2 Кбайт	Сб 15.10.2005 23:12	Сб 15.10.2005 23:12
jennyfer [mailto:jennyfer@utuz.ru]		2 Кбайт	Сб 15.10.2005 7:43	Сб 15.10.2005 7:43
Alexandre [mailto:alexandre@utuz.ru]		3 Кбайт	Пт 14.10.2005 21:18	Пт 14.10.2005 21:18

Открыть
Печать

Ответить
Ответить всем
Переслать

Просмотреть вложения ▶

Отметить к исполнению...
 Пометить как непрочтенные
Категории...

Найти все ▶
Нежелательная почта ▶

- Добавить нежелательных отправителей**
- Добавить в список взрослых отправителей**

Удалить
 Переместить в папку...

 Параметры...

Уважаемый Лео
 Во вторник по р
 К сожалению, п
 оказалась незаг
 Прошу меня пр
 Игорь

Отправители нежелательной почты



nonameoczka@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...

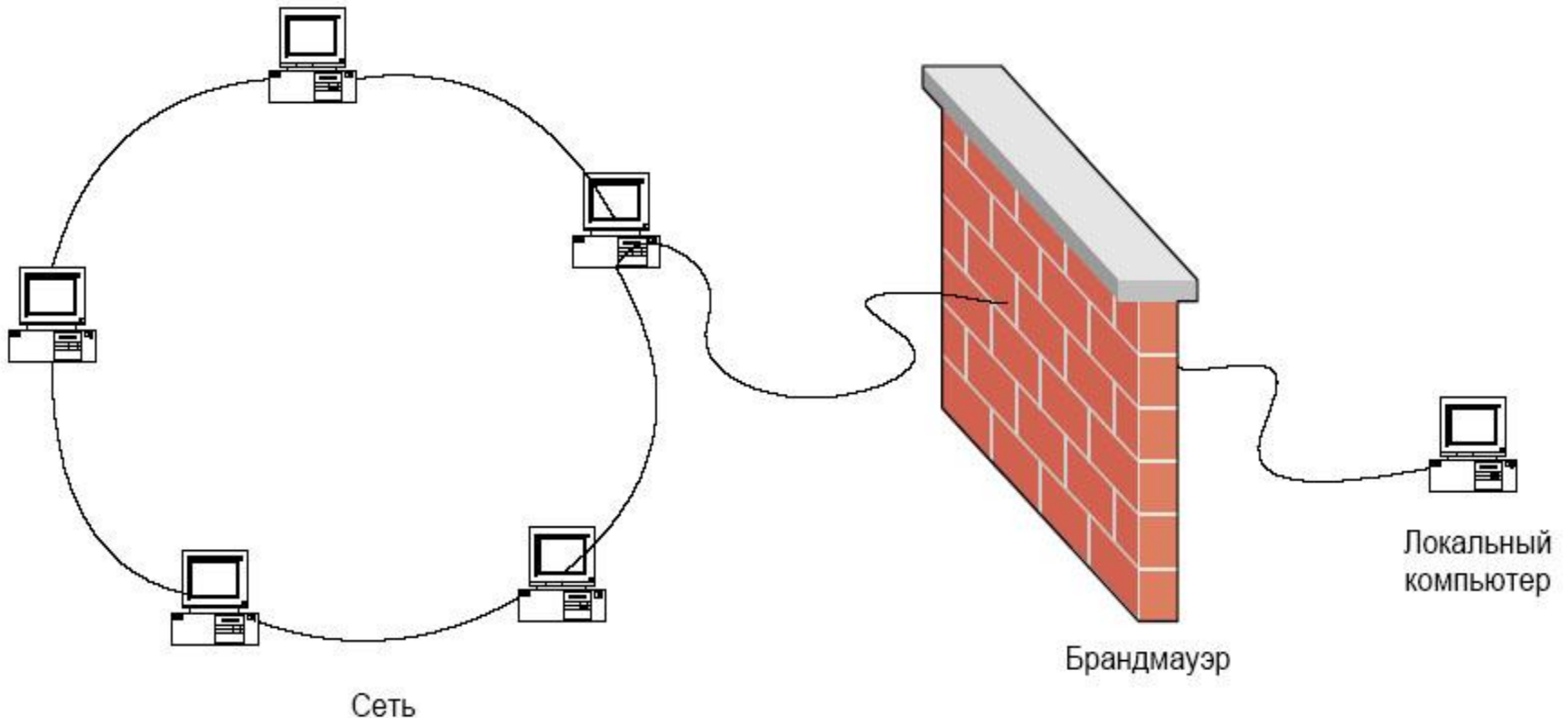
Изменить...

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



Iratific 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

Центр обеспечения безопасности Windows

Центр обеспечения безопасности
Помогите защитить свой компьютер

Ресурсы

- Получить последние сведения о безопасности и вирусах от корпорации Майкрософт
- Проверить наличие последних обновлений от Windows Update
- Получить поддержку по вопросам безопасности
- Справка по Центру обеспечения безопасности
- Изменить способ оповещений Центром обеспечения безопасности

Основы безопасности

Центр обеспечения безопасности помогает управлять параметрами безопасности Windows. Чтобы помочь защитить компьютер, включите все три основных компонента безопасности. Если они не включены, следуйте указаниям. Чтобы снова вернуться в Центр обеспечения безопасности, откройте панель управления.
[Какие новые компоненты Windows помогают защитить компьютер?](#)

Брандмауэр **ВЫКЛЮЧЕНО**

Обнаружено, что компьютер не защищен брандмауэром. Щелкните "Рекомендации" для получения указаний по исправлению. [Как брандмауэр помогает защитить компьютер?](#)

Примечание: система Windows не определяет все брандмауэры.

[Рекомендации...](#)

Автоматическое **ПРОВЕРЬТЕ ПАРАМЕТРЫ**

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)

Создать правило для IEXPLORE.EXE



Microsoft Internet Explorer запрашивает исходящее соединение с

Удаленная служба: HTTP (TCP:80)

Удаленный адрес: www.ya.ru

Действия Outpost Firewall:

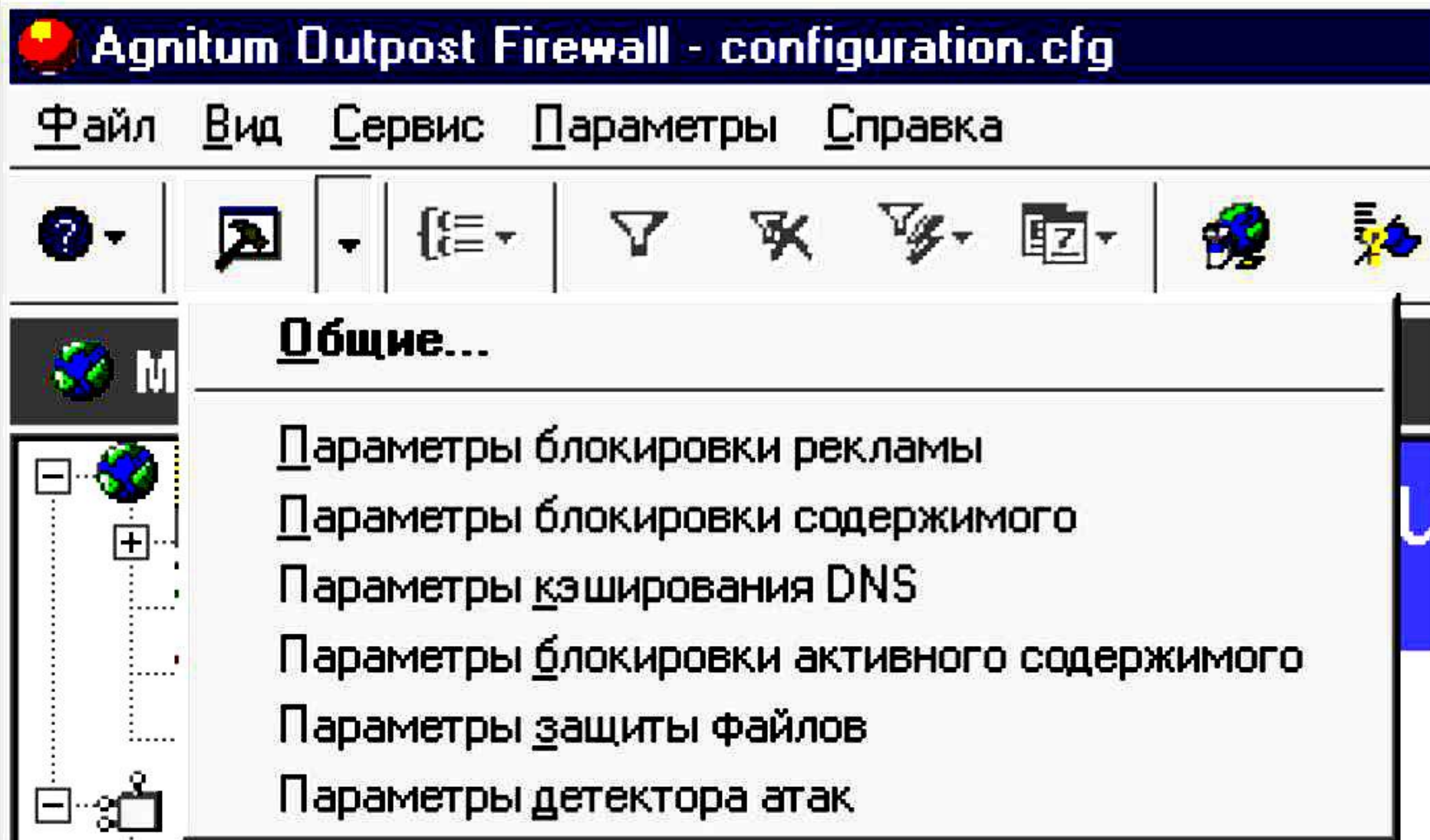
- Разрешить этому приложению выполнять любые действия
- Запретить этому приложению выполнять какие-либо действия
- Создать правило на основе стандартного Internet Explorer

Разрешить однократно

Блокировать однократно

OK

Параметры настройки



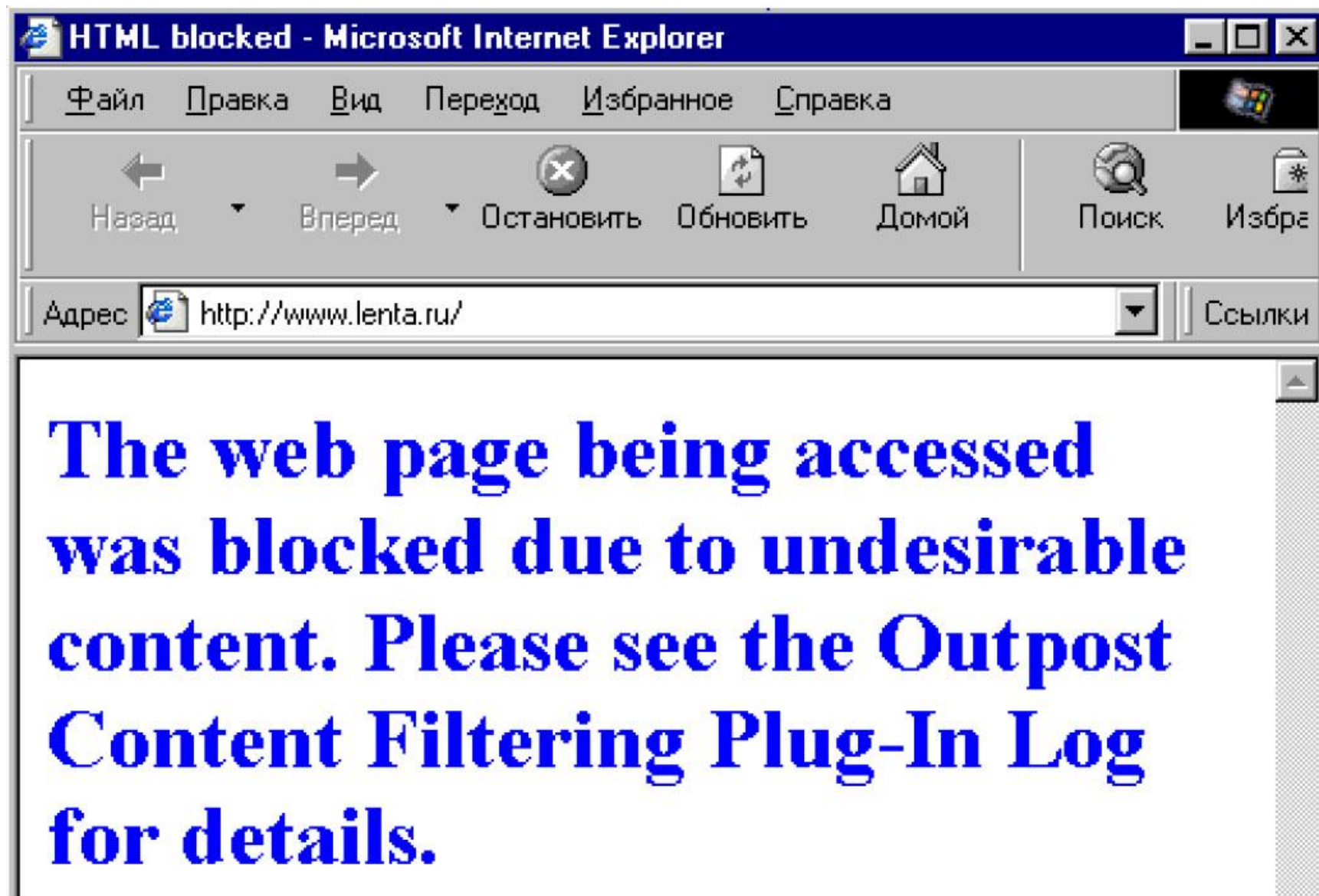
The image shows a screenshot of the Agnitum Outpost Firewall configuration window. The title bar reads "Agnitum Outpost Firewall - configuration.cfg". The menu bar includes "Файл", "Вид", "Сервис", "Параметры", and "Справка". The toolbar contains various icons for help, search, and configuration. The left sidebar shows a tree view with a globe icon and a minus sign. The main content area is titled "Общие..." and lists several configuration options:

- Параметры блокировки рекламы
- Параметры блокировки содержимого
- Параметры кэширования DNS
- Параметры блокировки активного содержимого
- Параметры защиты файлов
- Параметры детектора атак

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](#)



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\MemoriRu ToolbarLite\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 	
 Microsoft Router Identifier C:\WINDOWS\system32\tracert.exe	 Allow Block Custom	
 Microsoft Volume Shadow Copy Service C:\WINDOWS\system32\dlhhost.exe	Auto 	

[Add...](#)[Modify...](#)[Remove...](#)