**Что такое вирус.**

Компьютерные вирусы — вредоносные само распространяющиеся программы; основным признаком компьютерного вируса является его способность создавать собственные копии (не всегда похожие на оригинал) и внедрять их в исполняемые объекты (программы, системные области…)

Вредоносный программный код, обычно замаскированный под что-нибудь привлекательное (например, фотография популярного спортсмена) или полезное и выполняющий незапланированные либо нежелательные действия, например повреждение данных.

(Virus – лат.) - вид программ, характеризующихся способностью скрытого от пользователя саморазмножения для поражения других программ, компьютеров или сетей.

В общем случае компьютерный вирус - это небольшая программа, которая приписывает себя в конец исполняемых файлов, драйверов, или "поселяется" в загрузочном (BOOT) секторе диска. При запуске заражённых программ и драйверов вначале происходит выполнение вируса, а уже потом управление передаётся самой программе. Если же вирус "поселился" в загрузочном секторе, то его активизация происходит в момент загрузки операционной системы с такого диска. В тот момент, когда управление принадлежит вирусу, обычно выполняются различные неприятные для пользователя, но необходимые для продолжения жизни данного вируса действия. Это нахождение и заражение других программ, порча данных и т. д. Вирус может также остаться в памяти резидентно и продолжать вредить до перезагрузки компьютера. После окончания работы вируса управление передаётся заражённой программе, которая обычно работает "как ни в чём не бывало", маскируя тем самым наличие в системе вируса. К сожалению, очень часто вирус обнаруживается слишком поздно, когда большинство программ уже заражено. В этих случаях потери от зловредных действий вируса могут быть очень велики.

В последнее время появились так называемые макровирусы. Они передаются вместе с документами, в которых предусмотрено выполнение макрокоманд (например, документы текстового редактора Word), отсюда и их название. Макровирусы представляют собой макрокоманды, которые предписывают переносить тело вируса в другие документы, и, по возможности, совершать различные вредные действия. Наибольшее распространение в настоящее время получили макровирусы, заражающие документы текстового редактора Word и табличного редактора Excel.

***Как проявляют себя вирусы***

Проявления вирусов весьма различны. Это:

* + Сильное замедление работы компьютера.
	+ Неожиданное появление на экране посторонних фраз.
	+ Появление различных видеоэффектов (например, перевёртывание экрана).
	+ Пропадание информации с экрана.
	+ Генерация различных звуков.
	+ Некоторые программы перестают работать, а другие ведут себя очень странно.
	+ На дисках появляется большое количество испорченных файлов данных, текстовых файлов.
	+ Разом рушится вся файловая система на одном из дисков.
	+ Операционная система неожиданно перестаёт видеть винчестер.
	+ Произвольно изменяется длина отдельных файлов.
	+ Неожиданные проблемы с 32-х битным доступом к диску и файлам в Windows 3.11 или Windows 95.
	+ Стирание всех незащищённых от стирания пользовательских файлов и системных файлов
	+ Самопроизвольный неограниченный «разгон» видеокарты и процессора, что приводит к их перегреву и поломке
	+ Подмена существующих драйверов на драйвера, неподходящие к данной системе, что приводит к возникновению большого количества ошибок , замедлению работы системы и остановке работы важных сервисных программ
	+ Скачивание при подключённом Интернет-соединении большого количества ненужной, опасной информации, мусора и других вирусов

Разные вирусы могут вести себя по-разному. Некоторые только размножаются, не совершая вредных действий, другие же сразу после заражения совершают множество очень неприятных действий. Есть такие, которые вначале ведут себя незаметно, а по прошествии какого-то времени вдруг разом портят все данные (скажем, форматируется винчестер).

**Что может и чего не может компьютерный вирус.**

***Файлы, подвергающиеся заражению***

Компьютерный вирус может заразить очень ограниченное число файлов. Перечислим эти файлы. В первую очередь это исполняемые файлы с расширением .com и .ехе, затем - драйверы устройств с расширениями .sys и тем же .ехе. динамические библиотеки (расширение dll) и. наконец, оверлейные модули исполняемых файлов (как правило, имеют расширение .ovl).

Существуют вирусы, заражающие пакетные .bat файлы, но эти вирусы крайне примитивны и поступают очень просто: они вставляют в пакетные файлы команды своего вызова. Поймать такие вирусы не представляет труда.

Также могут быть подвергнуты заражению файлы документов и шаблонов редакторов, в которых при открытии документа предусмотрено выполнение макрокоманд. В частности, это .doc и .dot файлы текстового редактора Word, .xls и ,xlt файлы табличного редактора Excel.

Ни при каких условиях не могут быть подвергнуты заражению текстовые (.txt) и графические файлы (.tif, .gif, .bmp и т. п.), файлы данных и информационные файлы.

***Случаи, когда можно заразить свой компьютер***

**Заразиться компьютерным вирусом можно только в очень ограниченном количестве случаев. Это:**

Запуск на компьютере исполняемой программы, заражённой вирусом.

Загрузка компьютера с дискеты, содержащей загрузочный вирус.

Подключение к системе заражённого драйвера.

Открытие документа, заражённого макровирусом.

Установка на компьютере заражённой операционной системы.

**Компьютер не может быть заражён, если:**

На него переписывались текстовые и графические файлы (за исключением файлов, предусматривающих выполнение макрокоманд).

На нём производилось копирование с одной дискеты на другую при условии, что ни один файл с дискет не запускался.

На компьютере производится обработка принесённых извне текстовых и графических файлов, файлов данных и информационных файлов (за исключением файлов, предусматривающих выполнение макрокоманд).

Переписывание на компьютер заражённого вирусом файла ещё не означает заражения его вирусом. Чтобы заражение произошло нужно либо запустить заражённую программу, либо подключить заражённый драйвер, либо открыть заражённый документ (либо, естественно, загрузиться с заражённой дискеты).

Иначе говоря, заразить свой компьютер можно только в том случае, если запустить на нём непроверенные программы и (или) программные продукты, установить непроверенные драйвера и (или) операционные системы, загрузиться с непроверенной системной дискеты или открыть непроверенные документы, подверженные заражению макровирусами.

Не стоит приписывать все сбои в работе оборудования или программ действию компьютерного вируса. Вирус - это обычная программа причём небольшого размера, и она не может совершать никаких сверхъестественных действий.

**Типы вирусов**

**Вирусы - спутники.** Наиболее примитивный тип вирусов. Для каждого файла с расширением .ехе создают файл с тем же именем, но с расширением .com. содержащий тело вируса. При запуске файла операционная система вначале ищет .com файлы, а потом .ехе файлы. Поэтому вначале управление получает вирус, а затем уже он сам вызывает необходимый ехе файл.

**Файловые вирусы.** Поражают файлы с расширением .com, .ехе, реже .sys или оверлейные модули .ехе файлов. Эти вирусы дописывают своё тело в начало, середину или конец файла и изменяют его таким образом, чтобы первыми получить управление. Некоторые из этих вирусов не заботятся о сохранение заражаемого файла, в результате чего он оказывается неработоспособным; и, что самое печальное, такой файл нельзя восстановить. Часть этих вирусов остаётся в памяти резидентно.

**Загрузочные вирусы.** Поражают загрузочные сектора дисков. Инфицирование новых дисков происходит в тот момент, когда в заражённый компьютер вставляют новую дискету и начинают с ней работать. Часто вирус не

помешается целиком в загрузочной записи, туда пишется только его начало, а продолжение тела вируса сохраняется в другом месте диска. После запуска остаются в памяти резидентно.

**Вирусы, сочетающие в себе свойства файловых и загрузочных вирусов.** Такие вирусы могут поражать как файлы, так и загрузочные сектора.

**Вирусы DIR\*.** Интересный класс вирусов, появившийся недавно. Эти вирусы изменяют файловую систему диска очень хитрым образом. В таблице размещения файлов (FAT) для всех исполняемых файлов ссылки на начало заменяются ссылками на тело вируса. Адреса же начала файлов в закодированном виде помещаются в неиспользуемые элементы директории. В результате, как только вы запускаете любую программу, управление автоматически получает вирус. Он остаётся в памяти резидентно и при работе восстанавливает правильные ссылки на начала файлов. Если диск, заражённый вирусом DIR, попадает на чистый компьютер, считать с него данные, естественно, оказывается невозможным (читается только один кластер). При попытке протестировать файловую структуру - скажем Norton Disk Doctor - на экран выдаётся сообщение об огромном количестве ошибок, но стоит запустить хоть одну программу с заражённого диска, как файловая система тут же "восстанавливается".На самом же деле происходит инфицирование ещё одного компьютера.

**Макровирусы**. Весьма оригинальный класс вирусов (хотя вирусами в полном смысле этого слова их даже нельзя назвать), заражающий документы, в которых предусмотрено выполнение макрокоманд. При открытии таких документов вначале исполняются макрокоманды (специальные программы высокого уровня), содержащиеся в этом документе, -макровирус как раз ипредставляет собой такую макрокоманду. Таким образом, как только будет открыт заражённый документ,вирус получит управление и совершит все вредный действия (в частности, найдёт и заразит ещё не заражённые документы).

***Механизмы защиты вирусов от обнаружения***

Как правило вирусы легко обнаруживаются по особым участкам кода тела вируса. Правда, в последнее время широкое распространение получили два новых типа вирусов - вирусы-невидимки (или стелс-вирусы) и самомодифицирующиеся вирусы (вирусы-призраки).

**Стелс-вирусы** (от английского stealth - Стелс-вирус - вирус, тем или иным способом скрывающий свое присутствие в системе.) реализуют очень хитрый механизм, затрудняющий их обнаружение. При заражении эти вирусы остаются в памяти резидентно и при обращении к заражённым файлам и областям диска подменяют информацию так, что "заказчик" получает её в незаражённом, исходном виде. Достигается это перехватыванием обращений DOS и установкой своих векторов прерываний. Увидеть такой вирус можно либо на незаражённом компьетере (например, загрузившись с заведомо чистой дискеты), либо в том случае, когда программа не пользуется средствами DOS а напрямую обращается к диску.

**Вирусы-призраки** маскируются с помощью другого механизма. Эти вирусы постоянно модифицируют себя таким. образом', что не содержат одинаковых фрагментов. Такие вирусы хранят своё тело в закодированном виде и постоянно меняют параметры этой кодировки. Стартовая же часть, занимающаяся декодированием непосредственно самого тела, может генерироваться весьма сложным способом. При переносе вируса данного типа с компьютера на компьютер код вируса изменяется таким образом, что уже не имеет ничего общего со своим предыдущим вариантом. А часть вирусов может самомодифицироваться и в пределах одного компьютера. Обнаружение таких вирусов весьма осложнено, хотя часть антивирусных программ пытается находить их по участкам кода, характерным для стартовой части.

**\* - DIR** - Поле в ячейке управления ресурсами, показывающее направление RM-ячейки по отношению к потоку данных, с которым эта ячейка связана. Источник данных устанавливает DIR=0, получатель - DIR=1.

**Что делать, если заражение уже произошло**

***Стандартные действия при заражении вирусом***

Вы должны:

1. Сразу же выключить питание, чтобы вирус перестал распространяться дальше. Единственное, что можно сделать до выключения питания, - это сохранить результаты текущей работы. Не следует использовать горячую перезагрузку (Ctrl+Alt+Del), т. к. некоторые вирусы при этом сохраняют свою активность.
2. Войти в SETUP и включить загрузку с диска А:. Заодно рекомендуется проверить правильность всех установок, включая параметры жёстких дисков. Если произошли какие-либо изменения, то необходимо восстановить старые значения.
3. Ни в коем случае не запускать ни одной программы, находящейся на жёстком диске.
4. Необходимо загрузиться с дискеты (она должна быть защищена от записи) и запустить по очереди программы-детекторы, находящиеся на дискете. Если одна из программ обнаружит загрузочный вирус, то его можно тут же удалить, аналогично надо поступить и при наличии вируса DIR. Учтите, что вирусов может быть много.
5. Если программа-детектор обнаружит файловый вирус, то возможны два варианта действий. Если у вас

установлена программа-ревизор с лечащем модулем, то восстановление файлов лучше делать с ее помощью.

Если такое программы нет. то необходимо воспользоваться для лечения одним из детекторов. Испорченные файлы (если, конечно, они не текстовые и не файлы данных) необходимо удалить.

1. После того как все вирусы удалены, необходимо заново перенести операционную систему на жёсткий диск (с помощью команды SYS).
2. Необходимо проверить целостность файловой системы на винчестере (с помощью CHKDSK) и исправить все повреждения. Если таких повреждений очень много, то перед исправлением файловой структуры необходимо попытаться скопировать наиболее важные файлы на дискеты.
3. Необходимо ещё раз проверить жёсткий диск на наличие вирусов, если таковых не оказалось, то можно перезагрузиться с винчестера. После перезагрузки винчестера необходимо оценить потери от действий вируса. Если повреждений очень много, то проще заново переформатировать винчестер (при необходимости сохранив самые важные файлы).
4. Необходимо восстановить все необходимые файлы и программы с помощью архива - и для страковки, ещё раз загрузившись с дискеты, протестировать винчестер. Если снова будет обнаружен вирус, то- вам не повезло, ваш архив также заражён вирусом. В этом случае вы должны протестировать весь ваш архив.
5. Если всё в порядке, то необходимо проверить все дискеты, которые могли оказаться заражёнными вирусом и при необходимости пролечить их. Не забудьте только отключить загрузку с диска А:.
6. После того как вирус дезактивирован, вы можете продолжать свою работу. Рекомендуется только подключить на некоторое время одну из программ-фильтров.

***Нестандартные ситуации***

Во время вирусной атаки может возникнуть ряд нестандартных ситуаций. Рассмотрим их.

Если у вас установлен менеджер диска, то при загрузки с дискеты часть дисков может быть недоступна. Тогда
необходимо пролечить вначале все доступные на данный момент диски, затем загрузиться с жёсткого системного диска
и пролечить все оставшиеся логические диски. *i*

Если при загрузке с дискеты выясняется, что система просто "не видет" ваш винчестер, то скорее всего вирус повредил таблицу разбиения жёсткого диска. В этом случае необходимо ещё раз проверить установки SETUP и попытаться восстановить разбиение с помощью Norton Disk Doctor (или, если вы хорошо представляете себе свои действия, с помощью Norton Disk Edit). Если это не поможет, то, увы, вся информация с винчестера потеряна, остаётся только воспользоваться программой FDISK.

Если вы столкнулись с неизвестным вирусом, то дело обстоит несколько сложнее. Во-первых, вы можете воспользоваться программой-ревизором, если она у вас установлена. Вполне возможно, что она поможет обезвредить ваш вирус. Если её нет или она не помогла, то остаётся только заново перенести операционную систему, а затем удалить с него все исполняемые и пакетные файлы, драйверы и оверлейные файлы, после чего восстановить их из архива. Можно также воспользоваться услугами антивирусной скорой помощи.

И в заключение одно замечание. Не стоит приписывать все ваши неприятности действиям вируса. Говорить же о действии неизвестного вируса, а тем более прибегать к радикальным мерам следует только тогда, когда не остаётся никаких сомнений. Стоит вначале попытаться восстановить файлы, и, только если это не удаётся, удалить их.

Ситуация, сложившаяся сейчас в области вирусной безопасности, весьма стабильна. Различные организации (исключая, конечно, Институтские учебные центры, на которых пробуют свои силы юные авторы вирусов) подвергаются вирусным атакам весьма редко, - не говоря уже об индивидуальных пользователях.

***Антивирусы.***

**Антивирус** - это программа, предназначенная для сканирования и распознавания на компьютере пользователя программ или скриптов, макросов, которые могут причинить вред пользователю или существенно замедлить работу компьютера.

**Антивирус** - защита на уровне сервера от корреспонденции, содержащей вредоносный для почтового клиента код. К использованию необязательна, потому должна быть включена клиентом самостоятельно.

Антивирусных программ на данный момент существует много, и для того, чтобы найти оптимальный вариант, может потребоваться много времени, чтобы подобрать наилучший антивирус для ваших целей.

В данной статье рассматриваются практически все известные и популярные антивирусы, и я надеюсь, что после ее прочтения вы выберете для себя лучший антивирус.

Самым оптимальным вариантом на мой взгляд является получивший широкое распространение антивирус **Avast!.**

**Avast! 4 Home Edition - полноценный бесплатный антивирус** специально разработанный для использования на домашнем компьютере. Любое коммерческое использование Avast 4 в коммерческих целях запрещено. При выполнении обоих этих условий антивирус является бесплатным.

\*окно со «шкурой» (скином) по умолчанию

Для установки бесплатного антивируса Avast! 4 Home Edition нужно **скачать** его **последнюю версию**, инсталлировать на Вашем компьютере, **зарегистрироваться на сайте производителя** и, получив лицензионный код, в течение 60 дней ввести его в программу. Все это абсолютно **бесплатно**.

#### Основные характеристики Avast!:

- Высокий уровень выявления **вирусов, троянов и червей**.
- Резидентный (в режиме реального времени) и обычный сканер.
- **Сканирование архивов**.
- Проверка входной и исходной электронной почты.
- Глубокая интеграция в систему. Проверить тот или иной файл можно непосредственно из проводника Windows, щелкнув по нему правой кнопкой мыши и выбрав надпись "Сканировать... ".
- Карантин Avast! изолирован от операционной системы, что обеспечивает большую безопасность работы. Ни один файл, сохраняемый в карантине не может быть запущен.
- Интуитивно понятен интерфейс Avast!. Есть русский язык.
- Большое количество настроек.
- "Нетяжелые" автоматические или запланированные обновления вирусных баз (20-80 KB). Возможность обновления "вручную".
- Поддержка шкур (скинов) Avast!. Основной пакет содержит три скина, дополнительные можно скачать с официального сайта. (http;//www.avast.com)

**Список самых распространённых антивирусов на 23.09.07г.:**

|  |
| --- |
| **AntiVir PersonalEdition for Windows 98/ME & NT/2000/XP** |
|  | Размер: 14-16MB | ОС: Windows 9x/ME/NT/2K/XP | Версия: |
| Тип: freeware | Производитель: [**H+BEDV**](http://www.free-av.com/)  |   |
| Антивирус определяющий и способный удалить более 50 тысяч вирусов, включаямакро-вирусы. Имеет встроенную систему авто-обновления через internet. **При всем при этом программа абсолютно бесплатна.** |

|  |
| --- |
| **Naomi 3.2.90** |
|  | Размер: 1,3MB | ОС: Windows 9x/ME/NT/2K/XP | Версия: |
| Тип: Freeware version | [**Наличие**](http://www.radiance.m6.net/) **домашней страницы** | 3.2.90 |
| Прежде всего эта программа предназначается для родителей, которые хотят ограничить своим детям доступ к непристойным интернет-ресурсам. Кроме того, рекомендуется применять Naomi в учебных учреждениях. При своей работе утилита контролирует содержимое, загружаемое из интернета, и запрещает доступ к различным порно-сайтам, а также сайтам, содержащим насилие и пропаганду терроризма, азартные игры и т.д. Такая фильтрация осуществляется по ссылкам и ключевым словам (поддерживается 10 языков), отображаемым на веб-странице. Программа не нуждается ни в каких настройках, можно только задать пароль, чтобы было невозможно отключить фильтрацию интернет-контента без ввода соответствующего пароля. При обнаружении сайта непристойного содержания программа отключает (закрывает) окно браузера.Размер: 1.3Mb |

|  |
| --- |
| **McAfee PreScan v1.0** |
|  | Размер: 3,22MB | ОС: Windows 9x/ME/NT/2K/XP | Версия: |
| Тип: Freeware version | [Наличие](http://www.radiance.m6.net/) домашней страницы | 1.0 |
| McAfee анонсировал антивирус, который начинает работать во время загрузки Microsoft Windows, что обеспечивает больше гибкости и контроля над продуктом.  McAfee PreScan интегрируется с программным обеспечением управления безопасностью ePO 3.0/3.5 и Protection Pilot 1.1. Продукт включает движок 4400 antivirus engine, сканирование и очистку FAT и NTFS, а также сканирование сменных устройств. Антивирусные утилиты, которые сканируют систему во время загрузки Windows до загрузки остальных приложений, увеличивают шанс обнаружения вредоносного ПО до того как оно успеет принести вред. |

|  |
| --- |
| **Panda Antivirus Platinum 7.0** |
|

|  |
| --- |
|  |

 | Размер:24,8 MB | ОС: Windows 9x/ME/NT/2K/XP | Версия: |
| Тип:Evaulation version | Производитель:[Panda software](http://www.pandasoftware.com/) | Язык: Engl. |
| Panda Antivirus Platinum 7 — это инновационное антивирусное решение, отлично адаптированное к потребностям небольших организаций и профессионалов. Программа защищает компьютер и от вирусов, и от хакеров.Благодаря таким встроенным функциям, как межсетевой экран и блокиратор скриптов, Platinum 7 гарантирует защиту от вирусов, хакеров и других опасностей, связанных с сетью Интернет, в рамках единого и простого в использовании продукта[**.**](http://www.demvar.lv/soft/bezopastnost/Panda%20Antivirus%20Platinum%207.07.01.rar) |

|  |
| --- |
| **McAfee Anti-Spyware Enterprise 8.0 Retail** |
|  | Размер: 11,5MB | ОС: Windows 9x/ME/NT/2K/XP | Версия: |
| Тип: Freeware version | [Наличие](http://www.radiance.m6.net/) домашней страницы | 8.0 |
| McAfee Anti-Spyware Enterprise - это простое в установке, управлении и мониторинге средство, специально разработанное в соответствии с уникальными требованиями компаний любого размера. Данный продукт поддерживается одной из ведущих антивирусных исследовательских организаций в мире - McAfee® AVERTTM, и обеспечивает всестороннюю защиту от шпионского ПО.McAfee Anti-Spyware Enterprise интегрируется с продуктами McAfee® VirusScan® Enterprise 7.1 и 8.0i, добавляя необходимый уровень защиты от угроз шпионского ПО для компаний любого масштаба. Продукт легко внедряется и управляется с единой консоли с помощью масштабируемого средства управления: McAfee® ePolicy Orchestrator® (ePOTM) для крупных корпораций или McAfee® ProtectionPilotTM - для компаний малого и среднего размера.    Возможности Продукта :- использует фоновое сканирование для обнаружения, превентивного блокирования и безопасного удаления нежелательных программ до того, как они установятся на компьютер, включая жесткие диски, память, реестр Windows и другие области;- включает возможность традиционного сканирования по требованию (для обнаружения и немедленного удаления) с использованием огромной базы данных о потенциально нежелательных программах, включая cookies;- управляется централизованно с помощью McAfee ePO и McAfee ProtectionPilot, предоставляя системному администратору наглядную картину и возможность контроля, необходимые для настройки политики безопасности систем, повышения уровня защищенности, а также получения полных конфигурируемых отчетов. - является плагином для продуктов McAfee VirusScan Enterprise 7.1 и McAfee VirusScan Enterprise 8.0- поддерживается McAfee AVERT, сочетающей исследовательскую лабораторию мирового уровня по изучению вредоносного кода с экспертными знаниями в области защиты от вторжений профессионалов McAfee® IntruShield®, McAfee® Entercept® и McAfee® Foundstone® . |

|  |
| --- |
| **McAfee Personal Firewall Plus 7.0.150 Retail** |
|  | Размер: 5,1MB | ОС: Windows 9x/ME/NT/2K/XP | Версия: |
| Тип: Freeware version | [Наличие](http://www.radiance.m6.net/) домашней страницы | 7.0.150 |
| McAfee Personal Firewall Plus представляет из себя персональный межсетевой экран с широкими возможностями. В программе используется технология Sandbox, позволяющая организовать эффективную защиту рабочей станции обеспечивая контроль несанкционированного доступа и модификации реестра, запуска и остановки сервисов и использования файловой системы.Благодаря новым функциям брандмауэр McAfee Personal Firewall Plus стал более полнофункциональным и менее назойливым. Он непосредственно интегрирован с сайтом HackerWatch.org компании McAfee, на котором содержится подробная информация о конкретных нападениях и предупреждения о вспышках вирусов, а также мировая карта активности хакеров. Функция Advanced Worm Protection блокирует распространение червей, а Smart Recommendations автоматически настраивает конфигурацию более 700 известных программ, сокращая число перерывов в работе пользователя.McAfee Personal Firewall Plus прост в инсталляции, а число красных всплывающих окон с предупреждениями уменьшается по мере того, как брандмауэру становятся известны программы, которым разрешен доступ в Интернет. |

|  |
| --- |
| **Антивирус Stop! 5.0 Scaner** |
|   | Размер: 5,79MB | ОС: Windows 9x/ME/NT/2K/XP | Версия: |
| Тип: Freeware version | [Наличие](http://www.radiance.m6.net/) домашней страницы | 5.0 |
| Антивирус Stop! 5.0 Scanner — исключительно простой в эксплуатации антивирус для домашних пользователей. Cовременный, эффективный антивирусный продукт, способный обнаружить и удалить все известные типы троянских программ, интернет-червей и вредоносных программ. Anti-Spyware Total Protection — защита не только от вирусов и червей. Speed Scan Technology — сверхбыстрое сканирование. Rapidly Live Update — обновление антивируса каждый час. Сканирование архивов и почтовых баз. Анализатор кода, обнаруживающий новые вирусы. Простой и удобный интерфейс. С 1 июля 2006 — совершенно бесплатно[**.**](http://www.demvar.lv/soft/bezopastnost/stop%20scanner5/free-stop5-key-jun2007.reg)  |

|  |
| --- |
| **NOD 32 Antivirus System** |
|

|  |
| --- |
|  |

 | Размер: 6,76MB - 7,2MB | ОС: Windows 9x/ME/NT/2K/XP | Версия:2.7 |
| Тип:Тестовая версия | Производитель:[ESET](http://www.nod32.com.ua/index.php) | Язык: Rus |
| NOD 32 Antivirus System от Eset Software обеспечивает хорошо сбалансированную безупречную защиту персональных компьютеров и корпоративных систем, работающих на платформах Microsoft Windows 95/98/ME/NT/2000/2003/XP, UNIX/Linux, Novell, MS DOS, а также для почтовых серверов Microsoft Exchange Server, Lotus Domino и других.    Вирусы, черви, троянские программы и другой вредоносный код теперь находятся на безопасном расстоянии от ваших бесценных данных. Передовые методы обнаружения используемые в програмном обеспечении защищают даже от будущих потенциальных опасностей и от большинства новых червей и вирусов.    Главным преимуществом NOD32 является его быстрая работа, невероятное низкое потребление системных ресурсов и не раз доказанная способность ловить 100% вирусов.Тестовая версия предназначена для некоммерческого использования, а только для тестирования продукта. Тестовый период 30 дней. После окончания этого срока NOD32 должен быть удален с компьютера или куплен. Компания ESET не может нести ответственность за какие-либо повреждения полученные в результате использования или инсталляции тестовой версии NOD32. |

|  |
| --- |
| **Dr.Web® для Windows версия 4.32b** |
|

|  |
| --- |
|  |

 | Размер: 4,35MB | ОС: Windows 9x/ME/NT/2K/XP | Версия:4,32b |
| Тип:Evaulation version | Производитель:[Dr.Web®](http://www.drweb.ru/)  | Язык: |
| Вышла исправленная версия 4.31b антивирусной программы Dr.Web® для Windows 95/98/Me/NT/2000/XP, DOS/386, OS/2, Novell NetWare, версий Dr.Web® для почтовых и файловых серверов. Главной особенностью новой версии является возможность детектирования интернет-червей, распространяющихся в закрытых паролем ZIP-архивах. Помимо этого, версия 4.31b содержит следующие дополнения и исправления: - усовершенствован алгоритм проверки GZIP, ZIP и RAR архивов; - добавлена возможность ввода исключаемых из проверки путей по маске; - усовершенствован механизм проверки startup файлов, что привело к снижению времени их проверки; - в рамках проверки startup файлов добавлен алгоритм проверки BHO-объектов Explorer; - доработан алгоритм работы планировщика и программы автоматического обновления[**.**](http://www.demvar.lv/soft/bezopastnost/DrWeb4%5B1%5D.31b.zip) |

|  |
| --- |
| **Kaspersky Anti-Virus Windows Workstation v4.5.0.95** |
|

|  |
| --- |
|  |

 | Размер: 13,2MB | ОС: Windows 9x/ME/NT/2K/XP |
| Тип:Evaulation version | Производитель:[Лаборатория Касперского](http://www.antivirus.lv/default.asp?l=ru) |
| Важнейший элемент создания всеобъемлющей антивирусной защиты корпоративной сети - надежная защита рабочих станций. Созданный лучшими мировыми антивирусными экспертами, Антивирус Касперского™ для Wintel рабочих станций решает эту проблему наиболее эффективно, создавая надежный барьер на пути проникновения вирусов в сеть[**.**](http://www.demvar.lv/soft/bezopastnost/Kaspersky_Anti-Virus_Personal_Pro_v4.5.0.94.rar)  |

|  |
| --- |
| **Kaspersky Anti-Virus Personal v4.5.0.95** |
|

|  |
| --- |
|  |

 | Размер: 13,1MB | ОС: Windows 9x/ME/NT/2K/XP | Версия:45095 |
| Тип:Evaulation version | Производитель:[Лаборатория Касперского](http://www.antivirus.lv/default.asp?l=ru) | Язык: Engl. |
| Антивирус Касперского® Personal был специально разработан для защиты персонального компьютера. Простые интерфейсы, централизованное управление, автоматическая работа - позволяют продукту функционировать в фактически фоновом режиме до тех пор, пока вашему компьютеру и вашим данным не будет грозить опасность. В случае попытки проникновения вируса, продукт автоматически определит источник угрозы и эффективно нейтрализует ее при вашем минимальном участии. Более 90% вирусов поступают по электронной почте, поэтому Антивирус Касперского® Personal включает в себя специальные средства защиты - проверяя входящую и выходящую почту и контролируя ваши базы почтовых сообщений. Используя наш продукт, вы можете быть уверенными в безопасности подключений к интернету и любых устанавливаемых программ. Вы сможете полностью забыть о проблеме вирусов под защитой Антивируса Касперского® Personal[**.**](http://www.demvar.lv/soft/bezopastnost/Kaspersky_Anti-Virus_Personal_Pro_v4.5.0.94.rar) |

|  |
| --- |
| **Kaspersky Anti-Virus Personal Pro v4.5.0.95** |
|

|  |
| --- |
|  |

 | Размер: 14,2MB | ОС: Windows 9x/ME/NT/2K/XP | Версия:45095 |
| Тип:Evaulation version | Производитель:[Лаборатория Касперского](http://www.antivirus.lv/default.asp?l=ru) | Язык: Engl. |
| Антивирус Касперского® Personal Pro является последним технологическим достижением "Лаборатории Касперского" в области защиты домашнего компьютера от вирусных угроз. Помимо обычных антивирусных функций, в Антивирус Касперского® Personal Pro встроены уникальные технологические компоненты, позволяющие пользователю отслеживать все происходящие на компьютере изменения и контролировать поведение документов в формате MS Office, обеспечивая эти документы дополнительным уровнем безопасности. Антивирус Касперского® Personal Pro представляет собой уникальный набор компонент, некоторые из которых были ранее были доступны только для корпоративных пользователей программных продуктов компании. Теперь все эти средства антивирусной борьбы доступны для домашнего использования. Объединенные единым центром управления, они позволяют противостоять большинству угроз и обеспечивают пользователя максимально доступным уровнем безопасности[.](http://www.demvar.lv/soft/bezopastnost/Kaspersky_Anti-Virus_Personal_Pro_v4.5.0.94.rar) [подробнее...](http://www.antivirus.lv/products.asp?l=ru&p=personalpro.asp)  |

|  |
| --- |
| **Kaspersky Anti-Virus Personal Pro v4.5.0.94** |
|

|  |
| --- |
|  |

 | Размер: 14,1MB | ОС: Windows 9x/ME/NT/2K/XP | Версия:45094 |
| Тип:Evaulation version | Производитель:[Лаборатория Касперского](http://www.antivirus.lv/default.asp?l=ru) | Язык: Engl. |
| Антивирус Касперского™ Personal Pro является последним технологическим достижением Лаборатории Касперского в области защиты домашнего компьютера от вирусных угроз. Помимо обычных антивирусных функций, в Антивирус Касперского™ Personal Pro встроены уникальные технологические компоненты, позволяющие пользователю отслеживать все происходящие на компьютере изменения в компьютере и контролировать поведение документов в формате MS Office, обеспечивая эти документы дополнительным уровнем безопасности. Возможности: 100% защита от макро-вирусов. Защита даже от неизвестных вирусов. Надежный контроль целостности данных. Комплексная проверка почтовой корреспонденции. Защита мест хранения данных. Проверка памяти запущенных программ[.](http://www.demvar.lv/soft/bezopastnost/Kaspersky_Anti-Virus_Personal_Pro_v4.5.0.94.rar) |

|  |
| --- |
| **Symantec Norton AntiSpam 2004** |
|

|  |
| --- |
|  |

 | Размер: 18,7MB | ОС: Windows 9x/ME/NT/2K/XP | Версия: |
| Тип:Evaulation version | Производитель:[Symantec](http://www.symantec.com/)  | Язык: Engl. |
| Разработанная компанией Symantec программа Norton AntiSpam™ 2004 позволяет предотвратить попадание ненужных сообщений в почтовый ящик пользователя. Программа, совместимая с любым почтовым клиентом POP3, производит многоуровневую фильтрацию входящих сообщений электронной почты, выявляя и помечая "макулатурные" письма; при этом вся нужная корреспонденция доставляется без задержки. Кроме того, Norton AntiSpam отсекает рекламные заголовки и всплывающие окна, делая прогулку по Интернету куда более приятной[.](http://www.demvar.lv/soft/bezopastnost/Norton_AntiSpam_2004.rar) |

|  |
| --- |
| **Panda Platinum Internet Security 2004 Full + Update** |
|

|  |
| --- |
|  |

 | Размер: 27,1MB | ОС: Windows 9x/ME/NT/2K/XP | Версия: |
| Тип:Evaulation version | Производитель:[Panda software](http://www.pandasoftware.com/) | Язык: Engl. |
| Комплексное решение по обеспечению информационной безопасности. Включает защиту от вирусов, хакеров, спама, программ-шпионов и других Интернет-угроз.Ключевые характеристики: Антивирус - Обнаруживает и уничтожает все типы вирусов во время получения/отправки электронной почты, загрузки файлов или работы в Интернете. Благодаря усовершенствованному механизму UltraFast антивирус будет работать незаметно для Вас.Брандмауэр - Превращает Ваш компьютер в крепость, чтобы защитить его от хакеров, пытающихся украсть, разрушить или уничтожить Вашу информацию. Защита от программ-шпионов - Блокирует программы-шпионы на веб страницах: программы, которые записывают и сообщают о Ваших передвижениях по Интернету (adware, spybots, keyloggers и другие) или программы, которые незаметно подключают Ваш модем к дорогостоящим платным линиям («дозвонщики»)[.](http://www.demvar.lv/soft/bezopastnost/Panda%20Antivirus%20Platinum%202004.rar)  |

|  |
| --- |
| **Titanium Antivirus 2004 eng** |
|

|  |
| --- |
|  |

 | Размер: 23,11MB | ОС: Windows 9x/ME/NT/2K/XP | Версия: |
| Тип:Evaulation version | Производитель:[Panda software](http://www.pandasoftware.com/) | Язык: Engl. |
| Panda Titanium Antivirus 2004 - многофункциональный, быстрый антивирус, который действительно подойдет для "домашних" (не серверных или производственных) задач. Данное ПО хорошо подойдет для пользователя начального уровня. Надо помнить, что, как и любой антивирус, он не обеспечит 100% гарантию безопасности вашего компьютера. Так что будьте бдительны [!](http://www.demvar.lv/soft/bezopastnost/Panda_Antivirus_Titanium_2004.rar) |

За предоставленную информацию благодарю ABYSS, и наших латвийских коллег (DEMVAR SIA 2001-2007, Latvija )