**Конспект для урока информатики "Компьютерные вирусы. Антивирусные программы"**

**1. Актуализация знаний**

- На прошлых уроках мы с вами рассмотрели основные виды программного обеспечения. Давайте вспомним, что такое ПО? (ПО - вся совокупность программ, используемых на компьютере).  
- Зачем компьютеру необходимо ПО? (Программное обеспечение позволяет компьютеру выполнять определенную работу).  
- На какие группы делится все ПО? (Системное ПО, прикладное ПО, системы программирования).  
- Что относится к системным программам? (Программы, необходимые для работы компьютера).  
- Приведите примеры системных программ (Операционные системы, драйверы, утилиты).  
- Что такое прикладное ПО? (Программы, предназначенные для выполнения конкретных задач пользователя).  
- Примеры прикладного ПО? (Текстовые, графические процессоры, игры)  
- Что такое системы программирования? (Это программы для создания новых программ на языках программирования).  
- К какой группе программ относятся антивирусные программы? (системное ПО). Почему? (Они необходимы для корректной работы всей компьютерной системы).

Тема урока: «Компьютерные вирусы и антивирусные программы». Цель нашей работы - познакомиться с основами компьютерной вирусологии, научиться обнаруживать вирусы и бороться с ними.

Мы с вами говорили о том, что компьютер можно в чем-то сравнить с человеком. Человек, как биологический организм подвержен различным воздействиям внешней среды, в том числе и различным заболеваниям, причинами возникновения которых, часто, являются вирусы и бактерии, проникающие в организм человека из вне.

Попробуйте описать этапы и последствия заражения человека каким-либо вирусом. Особенности:

* проникновение вируса в организм человека происходит из вне;
* способность вируса к саморазмножению;
* активизация некоторых вирусов не сразу после проникновения в организм, а через некоторое время.

А может ли компьютер заразиться вирусом? Каким должен быть этот вирус по вашему представлению?

**2. Изучение нового материала**

**1) Понятие «компьютерный вирус»**

Итак, действительно, компьютер может заразиться. И причиной заражения действительно является вирус, только компьютерный. Это название пришло из биологии именно по признаку способности к саморазмножению. Вирусы представляют собой небольшие вредоносные программы, которые запускаются на компьютере без ведома его хозяина и выполняют различные нежелательные действия. При этом вирусы могут быть как почти безобидными, так и весьма неприятными.

**Компьютерный вирус** – это программа, которая может создавать свои копии и внедрять их в файлы, загрузочные секторы дисков, сети. При этом копии сохраняют возможность дальнейшего распространения. Часто вирусы обладают разрушительным действием.

**2) Пути распространения компьютерных вирусов**

Давайте подумаем, каковы пути распространения вирусов. (Вирусы могут попасть в ПК так же как любая другая программа). В противоположность обычным бациллам, компьютерные вирусы не передаются по воздуху: так как вирусы – это программы – средой их обитания служит только различная компьютерная техника.

Как на ПК может попасть вредоносная программа? (Через зараженные дискеты, диски, флеш-карты, посредством Интернета или по локальной сети). Обычно вирус внедряется в какой-либо документ или программу, и в начале работы вы можете не заметить ничего необычного. Однако через некоторое время вирус проявит свою разрушительную силу.

**3) Признаки появления компьютерных вирусов**

Назовем основные признаки проявления компьютерных вирусов.

* неправильная работа нормально работавших программ;
* медленная работа компьютера;
* невозможность загрузки ОС;
* исчезновение файлов и каталогов;
* изменение размеров файлов;
* неожиданное увеличение количества файлов на диске;
* уменьшение размеров свободной оперативной памяти;
* вывод на экран неожиданных сообщений и изображений;
* подача непредусмотренных звуковых сигналов;
* частые зависания и сбои в работе компьютера.

**4) История компьютерной вирусологии**

Первые вирусы появились давно, еще на заре эпохи ЭВМ, и не всегда были вредоносными. Например, в конце 60-х в лаборатории Xerox была создана специальная программа, являющаяся прообразом современных вирусов, которая самостоятельно путешествовала по локальной вычислительной сети и проверяла работоспособность включенных в нее устройств.

Однако позднее программы-вирусы стали разрабатываться со злым умыслом. Есть сведения, что некоторые компании специально инфицировали компьютеры конкурентов, чтобы таким образом шпионить за ними или вывести из строя их информационные системы.

**5) Слухи и заблуждения**

Порой боязнь вирусов причиняет больше неприятностей, чем сами вирусы. В свое время распространялось много заведомо ложных сообщений об угрозе якобы сверхопасных вирусов.

Необходимо знать, что ни один из вирусов не способен вывести из строя комплектующие компьютера. Максимум, на что способны некоторые вирусы, - это уничтожить информацию на жестком диске, что приведет к повреждению ОС и приложений. Хотя даже в этом случае ситуация может стать для вас фатальной, если вирус уничтожит важные документы.

**6) Создатели компьютерных вирусов**

Человек, который «пишет» вирусы называет себя вирьмейкером. Кто же занимается созданием вредоносных программ? В наши дни созданием вирусов обычно занимаются энтузиасты – одиночки. Ими могут быть и профессиональные программисты, и исследователи и обычные студенты, начинающие изучать программирование. Причем в настоящее время имеются десятки программ для автоматической генерации вирусов – конструкторы.

Что является стимулом для такой деятельности – сказать сложно. Это может быть как чувство мести, так и желание самоутвердиться. Первым вирусным конструктором, который получил широкое распространение, стал VCL (Virus Creation Laboratory), созданный в 1992 году.

**7) Классификация вирусов**

Существует несколько разных классификаций вредоносных программ.

Наиболее распространенная из них делит *вирусы по среде их обитания*. Согласно ей компьютерные вирусы бывают файловые, сетевые, загрузочные и макровирусы.

* **Файловые вирусы** – это программы, которые поражают исполняемые файлы операционной системы и пользовательских приложений. Чаще всего они внедряются в файлы с расширениями com, exe, bat, sys, dll. Такие вирусы обнаружить и обезвредить проще всего. Радует также, что проявить свою вредоносную активность они могут только после запуска зараженной программы.
* Нередко из файловых вирусов выделяют отдельный подтип, который называют **макровирусами**. Они также обитают в файлах, но не программ, а документах пользователя и шаблонах (doc, dot, xls, mdb и др.). Для их создания используется язык макрокоманд. Поэтому, чтобы обезопасить себя от макровирусов, необходимо отключить автозапуск макросов при открытии документов.
* **Сетевые вирусы** в качестве среды обитания используют глобальную или локальные компьютерные сети. Они не сохраняют свой код на жестком диске компьютера, а проникают напрямую в оперативную память ПК. Вирусы этого типа за способность вычислять сетевые адреса других машин, находясь в памяти компьютера, и самостоятельно рассылать по этим адресам свои копии называют сетевыми червями. Такой вирус может находиться одновременно в памяти нескольких компьютеров. Сетевые вирусы обнаружить сложнее, чем файловые. Сетевые вирусы распространяются с большой скоростью и могут сильно замедлить работу аппаратного обеспечения компьютерной сети.
* Среда обитания **загрузочных вирусов** – специальные области жестких и гибких дисков, которые служат для загрузки операционной системы. Для заражения вирусы используют главную загрузочную запись винчестера. Загрузочный вирус подменяет оригинальную запись и перехватывает управление системой. Такие вирусы обнаружить и удалить сложнее всего, поскольку они начинают свою работу еще до загрузки антивирусных приложений. Они же представляют наибольшую опасность.

Еще одна существующая *классификация вирусов – по их деструктивным возможностям*.

* **Безвредные вирусы** – оказывают незначительное влияние на работу ПК, занимая часть системных ресурсов. Нередко пользователи даже не подозревают об их присутствии.
* **Неопасные вирусы** – также занимают часть ресурсов компьютера, но об их присутствии пользователь знает хорошо. Обычно они проявляются в виде визуальных и звуковых эффектов и не вредят данным пользователя.
* **Опасные вирусы** – программы, которые нарушают нормальную работу пользовательских приложений или всей системы.
* **Очень опасные вирусы** – программы, задача которых заключается в уничтожении файлов, выводе из стоя программ и ОС или рассекречивании конфиденциальных данных.

*Все компьютерные вирусы бывают двух типов – резидентные и нерезидентные.*

* **Резидентные вирусы** представляют собой программы, присутствующие в оперативной памяти либо хранящие там свою активную часть, которая постоянно заражает те или иные объекты операционной системы.
* **Нерезидентные вирусы** загружаются лишь во время открытия зараженного файла или работы с инфицированным приложением.

Как несложно догадаться, наибольшую опасность представляют резидентные вирусы, так как время их активной работы ограничивается только выключением или перезагрузкой всей системы, а не отдельного приложения.

*По особенностям алгоритма работы* различают:

* **Простейшие вирусы** – вирусы, которые при распространении своих копий обязательно изменяют содержимое дисковых секторов или файлов, поэтому его достаточно легко обнаружить.
* **Вирусы-спутники (компаньоны)** - вирус, который не внедряется в сам исполняемый файл, а создает его зараженную копию с другим расширением.
* **Стелс-вирус (невидимка)** – вирусы, скрывающие свое присутствие в зараженных объектах, подставляя вместо себя незараженные участки.
* **Полиморфные вирусы (мутанты)** – вирусы, модифицирующие свой код таким образом, что копии одного и того же вируса не совпадали.
* **Макровирус** – вирусы, которые заражают документы офисных приложений.
* **Троянская программа** – программа, которая маскируется под полезные приложения (утилиты или даже антивирусные программы), но при этом производит различные шпионские действия. Она не внедряется в другие файлы и не обладает способностью к саморазмножению.
* **Черви** – это вредительские компьютерные программы, которые способны саморазмножаться, но, в отличие от вирусов не заражают другие файлы. Свое название черви получили потому, что для распространения они используют компьютерные сети и электронную почту.

Сегодня наиболее распространены так называемые сетевые черви, а также макровирусы.

**8) Профилактика появления компьютерных вирусов**

Одним из основных методов борьбы с вирусами является, как и в медицине, своевременная профилактика. Подумайте, какие средства помогают предотвратить заражение ПК?

1. Резервное копирование наиболее ценных данных;
2. создание дистрибутивного и системного диска;
3. хранение всех регистрационных и парольных данных не на ПК;
4. проверка всей поступающей извне информации на вирусы, как на дискетах, CD-ROM, так и по сети;
5. использование «свежих» антивирусных программ, регулярная проверка компьютера на наличие вирусов.

**9) Антивирусные программы**

Итак, особое место в этом списке занимают программные средства защиты – антивирусные программы. К какому виду ПО они относятся? (Системному ПО).

**Антивирусная программа (антивирус)** - программа, позволяющая выявлять вирусы, лечить зараженные файлы и диски, обнаруживать и предотвращать подозрительные действия.

Существует несколько типов антивирусных программ, различающихся выполняемыми функциями.

1. **Полифаги**. Просмотр содержимого файлов, расположенных на дисках компьютера, а также содержимого оперативной памяти компьютера с целью поиска вирусов.
2. **Ревизоры**. В режиме предварительного сканирования создает базу данных с контрольными суммами и другой информацией, позволяющей впоследствии контролировать целостность файлов (контроль над изменениями, которые происходят в файловой системе ПК).
3. **Блокировщики**. Проверка на наличие вирусов запускаемых файлов, перехват «вирусоопасных» ситуаций.

Ни один тип антивирусных программ по отдельности не дает полной защиты от вирусов. Поэтому в современные антивирусные комплекты программ обычно входят компоненты, реализующие все эти функции.

**3. Дополнительная информация**

В начале 1970-х годов в прототипе современного интернета - военной компьютерной сети APRAnet - был обнаружен вирус Creeper. Эта программа была в состоянии самостоятельно войти в сеть через модем и передать свою копию удаленной системе. На зараженных системах вирус обнаруживал себя сообщением: "I'M THE CREEPER: CATCH ME IF YOU CAN". Это был назойливый, но в целом безобидный вирус.  
1981 году появился вирус Elk Cloner. Он записывался в загрузочные сектора дискет, к которым шло обращение. В те времена это казалось невероятным и вызывало у рядовых пользователей устойчивую связь между вирусами и внеземными цивилизациями, пытающимися завоевать мир. Впечатление от вируса усиливалось его проявлениями: Elk Cloner переворачивал изображение на экране, заставлял мигать текст, выводил разнообразные сообщения.  
В 1983 году Лен Эйделман впервые употребляет термин "вирус" в применении к саморазмножающимся компьютерным программам. В этот же году Фред Коэн, родоначальник современной компьютерной вирусологии, на семинаре по компьютерной безопасности демонстрирует вирусоподобную программу, способную внедряться в другие объекты, а годом позже дает научное определение термину "компьютерный вирус".  
В 1986 году зарегистрирована первая глобальная эпидемия вируса. Вирус Brain, заражающий загрузочные сектора дискет, в течение нескольких месяцев распространился практически по всему миру. Вслед за обнаружением Brain один за другим стали появляться научно-фантастические романы, посвященные вирусам.   
В декабре 1987 произошла первая известная повальная эпидемия сетевого вируса "Christmas Tree". За четыре дня (9-13 декабря) вирус парализовал сеть IBM VNet - она была забита его копиями. При запуске вирус выводил на экран изображение рождественской елочки и рассылал свои копии всем пользователям сети, чьи адреса присутствовали в системных файлах.  
1988 год - глобальная эпидемия. Вирус Jerusalem обнаружил себя сам: в пятницу, 13-го, он уничтожал все запускаемые на зараженном компьютере файлы. Ноябрь 1988: повальная эпидемия настоящего сетевого вируса, получившего название червь Морриса. Вирус заразил более 6000 компьютерных систем в США (включая Исследовательский центр NASA). В это время стали появляться первые компании-разработчики антивирусного программного обеспечения.  
Декабрь 1989 года: некий злоумышленник разослал по разным адресам 20.000 дискет, содержащих "троянца". Через 90 загрузок операционной системы на зараженном ПК программа делала невидимыми все файлы и оставляла на диске только один читаемый файл - счет, который следовало оплатить и отослать по указанному адресу. 1989 году свою карьеру антивирусного эксперта начал Евгений Касперский, позже основавший компанию "Лаборатория Касперского".  
В 90-х годах количество вирусов растет в геометрической прогрессии. В июле 1990 г. произошел серьезный инцидент с английским компьютерным журналом PC Today. К каждому номеру журнала бесплатно прилагался флоппи-диск, как оказалось впоследствии, зараженный вирусом DiskKiller. Было продано более 50.000 копий журнала. Комментарии излишни.  
Июль 1992: появление первых конструкторов вирусов. Они позволяли людям создавать свои собственные вирусы различных типов и модификаций.  
В конце XX – начале XXI века электронная почта и Интернет укрепили свои позиции как наиболее опасные источники вредоносных программ.  
В январе разразилась глобальная эпидемия интернет-червя Happy99. Далее - глобальная эпидемия вируса "Melissa". Сразу же после заражения системы он считывал адресную книгу почтовой программы и незаметно рассылал по первым 50 найденным адресам свои копии.  
В четверг 4 мая 2000 года был обнаружен новый опасный вирус, притворяющийся признанием в любви! - "червь" LoveLetter, который распространяется по электронной почте под заголовком "ILOVEYOU". ILOVEYOU наносит значительный ущерб данным, содержащимся на диске зараженного компьютера. «Конечно, ведь это так интересно. Получив сообщение, в котором говорится, что вас любят, вы непременно поспешите открыть его и посмотреть, что внутри».

2001 год - новый вирус Zoher — автоматизированное письмо счастья "Zoher" распространяется по электронной почте в виде вложенных файлов. Таким образом, при попытке прочтения письма, вирус активизируется самостоятельно, если на компьютере не установлена специальная заплатка для почтовой программы.  
Тело письма содержит весьма длинный текст на итальянском языке.  
Его перевод примерно следующий:  
«С этим письмом вам придет счастье! Не просто счастье, а счастье с большой буквы С! Даже больше — счастье с большими буквами С и Ь! Мы на мелочи времени не тратим! С сегодняшнего дня к вам придет удача, но только в том случае, если вы отправите это письмо всем, кого вы знаете. Если вы сделаете это, то:  
а) ваша мужская сила будет как у Кинг Конга до конца вашей жизни  
б) светофор перед вами всегда будет зеленым, или, хотя бы, желтым  
в) вы поймаете всех Покемончиков  
г) (для мужчин) когда отправитесь на рыбалку, то выловите не простую рыбку, а Сирену, по ошибке рожденную не с хвостом, а с красиыми женскими ножками  
д) (для женщин) вы родитесь Сиреной с женскими ножками, а вас поймает мужчина вашей мечты  
Если же вы не отправите это письмо всем вашим знакомым в течение 40 секунд, то вас ждут неприятности! Вы попадете во множество трагикомических ситуаций, ваша жизнь станет одним большим приколом, который только вам не будет казаться смешным … и т.п.»

**1) Понятие «компьютерный вирус»**

Итак, действительно, компьютер может заразиться. И причиной заражения действительно является вирус, только компьютерный. Это название пришло из биологии именно по признаку способности к саморазмножению. Вирусы представляют собой небольшие вредоносные программы, которые запускаются на компьютере без ведома его хозяина и выполняют различные нежелательные действия. При этом вирусы могут быть как почти безобидными, так и весьма неприятными.

**Компьютерный вирус** – это программа, которая может создавать свои копии и внедрять их в файлы, загрузочные секторы дисков, сети. При этом копии сохраняют возможность дальнейшего распространения. Часто вирусы обладают разрушительным действием.

**2) Пути распространения компьютерных вирусов**

Давайте подумаем, каковы пути распространения вирусов. (Вирусы могут попасть в ПК так же как любая другая программа). В противоположность обычным бациллам, компьютерные вирусы не передаются по воздуху: так как вирусы – это программы – средой их обитания служит только различная компьютерная техника.

Как на ПК может попасть вредоносная программа? (Через зараженные дискеты, диски, флеш-карты, посредством Интернета или по локальной сети). Обычно вирус внедряется в какой-либо документ или программу, и в начале работы вы можете не заметить ничего необычного. Однако через некоторое время вирус проявит свою разрушительную силу.

**3) Признаки появления компьютерных вирусов**

Назовем основные признаки проявления компьютерных вирусов.

* неправильная работа нормально работавших программ;
* медленная работа компьютера;
* невозможность загрузки ОС;
* исчезновение файлов и каталогов;
* изменение размеров файлов;
* неожиданное увеличение количества файлов на диске;
* уменьшение размеров свободной оперативной памяти;
* вывод на экран неожиданных сообщений и изображений;
* подача непредусмотренных звуковых сигналов;
* частые зависания и сбои в работе компьютера.

**4) История компьютерной вирусологии**

Первые вирусы появились давно, еще на заре эпохи ЭВМ, и не всегда были вредоносными. Например, в конце 60-х в лаборатории Xerox была создана специальная программа, являющаяся прообразом современных вирусов, которая самостоятельно путешествовала по локальной вычислительной сети и проверяла работоспособность включенных в нее устройств.

Однако позднее программы-вирусы стали разрабатываться со злым умыслом. Есть сведения, что некоторые компании специально инфицировали компьютеры конкурентов, чтобы таким образом шпионить за ними или вывести из строя их информационные системы.

**5) Слухи и заблуждения**

Порой боязнь вирусов причиняет больше неприятностей, чем сами вирусы. В свое время распространялось много заведомо ложных сообщений об угрозе якобы сверхопасных вирусов.

Необходимо знать, что ни один из вирусов не способен вывести из строя комплектующие компьютера. Максимум, на что способны некоторые вирусы, - это уничтожить информацию на жестком диске, что приведет к повреждению ОС и приложений. Хотя даже в этом случае ситуация может стать для вас фатальной, если вирус уничтожит важные документы.

**6) Создатели компьютерных вирусов**

Человек, который «пишет» вирусы называет себя вирьмейкером. Кто же занимается созданием вредоносных программ? В наши дни созданием вирусов обычно занимаются энтузиасты – одиночки. Ими могут быть и профессиональные программисты, и исследователи и обычные студенты, начинающие изучать программирование. Причем в настоящее время имеются десятки программ для автоматической генерации вирусов – конструкторы.

Что является стимулом для такой деятельности – сказать сложно. Это может быть как чувство мести, так и желание самоутвердиться. Первым вирусным конструктором, который получил широкое распространение, стал VCL (Virus Creation Laboratory), созданный в 1992 году.

**7) Классификация вирусов**

Существует несколько разных классификаций вредоносных программ.

Наиболее распространенная из них делит *вирусы по среде их обитания*. Согласно ей компьютерные вирусы бывают файловые, сетевые, загрузочные и макровирусы.

* **Файловые вирусы** – это программы, которые поражают исполняемые файлы операционной системы и пользовательских приложений. Чаще всего они внедряются в файлы с расширениями com, exe, bat, sys, dll. Такие вирусы обнаружить и обезвредить проще всего. Радует также, что проявить свою вредоносную активность они могут только после запуска зараженной программы.
* Нередко из файловых вирусов выделяют отдельный подтип, который называют **макровирусами**. Они также обитают в файлах, но не программ, а документах пользователя и шаблонах (doc, dot, xls, mdb и др.). Для их создания используется язык макрокоманд. Поэтому, чтобы обезопасить себя от макровирусов, необходимо отключить автозапуск макросов при открытии документов.
* **Сетевые вирусы** в качестве среды обитания используют глобальную или локальные компьютерные сети. Они не сохраняют свой код на жестком диске компьютера, а проникают напрямую в оперативную память ПК. Вирусы этого типа за способность вычислять сетевые адреса других машин, находясь в памяти компьютера, и самостоятельно рассылать по этим адресам свои копии называют сетевыми червями. Такой вирус может находиться одновременно в памяти нескольких компьютеров. Сетевые вирусы обнаружить сложнее, чем файловые. Сетевые вирусы распространяются с большой скоростью и могут сильно замедлить работу аппаратного обеспечения компьютерной сети.
* Среда обитания **загрузочных вирусов** – специальные области жестких и гибких дисков, которые служат для загрузки операционной системы. Для заражения вирусы используют главную загрузочную запись винчестера. Загрузочный вирус подменяет оригинальную запись и перехватывает управление системой. Такие вирусы обнаружить и удалить сложнее всего, поскольку они начинают свою работу еще до загрузки антивирусных приложений. Они же представляют наибольшую опасность.

Еще одна существующая *классификация вирусов – по их деструктивным возможностям*.

* **Безвредные вирусы** – оказывают незначительное влияние на работу ПК, занимая часть системных ресурсов. Нередко пользователи даже не подозревают об их присутствии.
* **Неопасные вирусы** – также занимают часть ресурсов компьютера, но об их присутствии пользователь знает хорошо. Обычно они проявляются в виде визуальных и звуковых эффектов и не вредят данным пользователя.
* **Опасные вирусы** – программы, которые нарушают нормальную работу пользовательских приложений или всей системы.
* **Очень опасные вирусы** – программы, задача которых заключается в уничтожении файлов, выводе из стоя программ и ОС или рассекречивании конфиденциальных данных.

*Все компьютерные вирусы бывают двух типов – резидентные и нерезидентные.*

* **Резидентные вирусы** представляют собой программы, присутствующие в оперативной памяти либо хранящие там свою активную часть, которая постоянно заражает те или иные объекты операционной системы.
* **Нерезидентные вирусы** загружаются лишь во время открытия зараженного файла или работы с инфицированным приложением.

Как несложно догадаться, наибольшую опасность представляют резидентные вирусы, так как время их активной работы ограничивается только выключением или перезагрузкой всей системы, а не отдельного приложения.

*По особенностям алгоритма работы* различают:

* **Простейшие вирусы** – вирусы, которые при распространении своих копий обязательно изменяют содержимое дисковых секторов или файлов, поэтому его достаточно легко обнаружить.
* **Вирусы-спутники (компаньоны)** - вирус, который не внедряется в сам исполняемый файл, а создает его зараженную копию с другим расширением.
* **Стелс-вирус (невидимка)** – вирусы, скрывающие свое присутствие в зараженных объектах, подставляя вместо себя незараженные участки.
* **Полиморфные вирусы (мутанты)** – вирусы, модифицирующие свой код таким образом, что копии одного и того же вируса не совпадали.
* **Макровирус** – вирусы, которые заражают документы офисных приложений.
* **Троянская программа** – программа, которая маскируется под полезные приложения (утилиты или даже антивирусные программы), но при этом производит различные шпионские действия. Она не внедряется в другие файлы и не обладает способностью к саморазмножению.
* **Черви** – это вредительские компьютерные программы, которые способны саморазмножаться, но, в отличие от вирусов не заражают другие файлы. Свое название черви получили потому, что для распространения они используют компьютерные сети и электронную почту.

Сегодня наиболее распространены так называемые сетевые черви, а также макровирусы.

**8) Профилактика появления компьютерных вирусов**

Одним из основных методов борьбы с вирусами является, как и в медицине, своевременная профилактика. Подумайте, какие средства помогают предотвратить заражение ПК?

1. Резервное копирование наиболее ценных данных;
2. создание дистрибутивного и системного диска;
3. хранение всех регистрационных и парольных данных не на ПК;
4. проверка всей поступающей извне информации на вирусы, как на дискетах, CD-ROM, так и по сети;
5. использование «свежих» антивирусных программ, регулярная проверка компьютера на наличие вирусов.

**9) Антивирусные программы**

Итак, особое место в этом списке занимают программные средства защиты – антивирусные программы. К какому виду ПО они относятся? (Системному ПО).

**Антивирусная программа (антивирус)** - программа, позволяющая выявлять вирусы, лечить зараженные файлы и диски, обнаруживать и предотвращать подозрительные действия.

Существует несколько типов антивирусных программ, различающихся выполняемыми функциями.

1. **Полифаги**. Просмотр содержимого файлов, расположенных на дисках компьютера, а также содержимого оперативной памяти компьютера с целью поиска вирусов.
2. **Ревизоры**. В режиме предварительного сканирования создает базу данных с контрольными суммами и другой информацией, позволяющей впоследствии контролировать целостность файлов (контроль над изменениями, которые происходят в файловой системе ПК).
3. **Блокировщики**. Проверка на наличие вирусов запускаемых файлов, перехват «вирусоопасных» ситуаций.

Ни один тип антивирусных программ по отдельности не дает полной защиты от вирусов. Поэтому в современные антивирусные комплекты программ обычно входят компоненты, реализующие все эти функции.

**1. Понятие "компьютерного вируса" и его свойства**

Компьютерный вирус - это вредоносный самораспространяющийся в информационной среде программный код. Он может внедряться в исполняемые и командные файлы программ, распространяться через загрузочные секторы дискет и жестких дисков, документы офисных приложений, через электронную почту, Web-сайты, по другим электронным каналам. Проникнув в компьютерную систему, вирус может ограничиться безобидными визуальными или звуковыми эффектами, но может и вызвать потерю или искажение данных, утечку личной и конфиденциальной информации. В худшем случае компьютерная система, пораженная вирусом, окажется под полным контролем злоумышленника.

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

Основную массу вирусов создают студенты и школьники, которые только что изучили язык ассемблера, хотят попробовать свои силы. Значительная часть таких вирусов их авторами часто не распространяется.

Вторую группу составляют также молодые люди (чаще - студенты), которые еще не полностью овладели искусством программирования, но уже решили посвятить себя написанию и распространению вирусов. Как правило, они создают многочисленные модификации "классических" вирусов, либо вирусы крайне примитивные и с большим числом ошибок. Выход конструкторов вирусов, при помощи которых можно создавать новые вирусы даже при минимальных знаниях об операционной системе и ассемблере значительно облегчил им работу.

Став старше и опытнее, многие из подобных вирусописателей попадают в третью, наиболее опасную группу, которая создает и запускает в мир "профессиональные" вирусы. Это тщательно продуманные и отлаженные программы. Такие вирусы нередко используют достаточно оригинальные алгоритмы, недокументированные и мало кому известные способы проникновения в системные области данных.

Четвертая группа авторов вирусов - "исследователи". Эта группа состоит из талантливых программистов, которые занимаются изобретением принципиально новых методов заражения, скрытия, противодействия антивирусам и т.д. Они же придумывают способы внедрения в новые операционные системы, конструкторы вирусов и полиморфик-генераторы. Эти программисты пишут вирусы не ради собственно вирусов, а скорее ради "исследования" потенциалов "компьютерной вирусологии".

При заражении компьютера вирусом важно его обнаружить, для этого следует знать основные признаки его проявления:

- прекращение работы или неправильная работа ранее успешно функционировавших программ;

- медленная работа компьютера;

- невозможность загрузки операционной системы;

- исчезновение файлов и каталогов или искажение их содержимого;

- изменение даты и времени модификации файлов;

- изменение размера файлов;

- неожиданное значительное увеличение количества файлов на диске;

- существенное уменьшение размера свободной оперативной памяти;

- вывод на экран непредусмотренных сообщений или изображений;

- подача непредусмотренных звуковых сигналов;

- частые зависания и сбои в работе компьютера.

Следует отметить, что вышеперечисленные явления необязательно вызываются присутствием вируса, а могут быть следствием других причин. Поэтому всегда затруднена правильная диагностика состояния компьютера. 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.

**2. Классификация компьютерных вирусов**

На сегодняшний день известны десятки тысяч различных вирусов. Несмотря на такое изобилие, число типов вирусов, отличающихся друг от друга механизмом распространения и принципом действия, весьма ограниченно. Существуют и комбинированные вирусы, которые можно отнести одновременно к нескольким типам. Таким образом, вирусы можно классифицировать по следующим признакам:

- среде обитания;

- способу заражения среды обитания;

- степени воздействия;

- особенностям алгоритма.

1. В зависимости от **среды обитания** вирусы делят на:

1) сетевые – распространяются по различным компьютерным сетям;

2) файловые - 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. Получив управление, вирус может заразить другие программы, внедриться в оперативную память компьютера и т.д. Некоторые из этих вирусов не заботятся о сохранение заражаемого файла, в результате чего он оказывается неработоспособным и не подлежащим восстановлению;

3) загрузочные - получают управление на этапе инициализации компьютера, еще до начала загрузки ОС. При заражении дискеты или жесткого диска загрузочный вирус заменяет загрузочную запись BR или главную загрузочную запись MBR. При начальной загрузке компьютера BIOS считывает загрузочную запись с диска или дискеты, в результате чего вирус получает управление еще до загрузки ОС. Затем он копирует себя в конец оперативной памяти и перехватывает несколько функций BIOS. В конце процедуры заражения вирус загружает в память компьютера настоящий загрузочный сектор и передает ему управление. Далее все происходит, как обычно, но вирус уже находится в памяти и может контролировать работу всех программ и драйверов;

4) файлово–загрузочные – комбинированные вирусы, объединяющие свойства файловых и загрузочных. В качестве примера можно привести широко распространенный когда-то файлово-загрузочный вирус OneHalf. Проникая в компьютер с ОС MS-DOS, этот вирус заражает главную загрузочную запись. Во время загрузки вирус постепенно шифрует секторы жесткого диска, начиная с самых последних секторов. Вирус OneHalf использует различные механизмы маскировки.

2. По **способу заражения среды обитания** вирусы делятся на:

1) резидентные - при заражении (инфицировании) компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т. п.) и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера;

2) нерезидентные вирусы не заражают память компьютера и являются активными ограниченное время.

3. По **степени воздействия** вирусы можно разделить на:

1) неопасные, не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках, действия таких вирусов проявляются в каких-либо графических или звуковых эффектах;

2) опасные вирусы, которые могут привести к различным нарушениям в работе компьютера;

3) особо опасные, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

4. По **особенностям алгоритма**:

Большое разнообразие вирусов вызывает трудности в их классификации по данному признаку.

1) Простейшие вирусы - паразитические, они изменяют содержимое файлов и секторов диска и могут быть достаточно легко обнаружены и уничтожены;

2) вирусы-невидимки (стелс-вирусы) – пытаются скрыть свое присутствие в компьютере. Они имеют резидентный модуль, постоянно находящийся в оперативной памяти компьютера. Этот модуль перехватывает обращения к дисковой подсистеме компьютера. Если ОС или другая программа считывают файл зараженной программы, то вирус подставляет настоящий, незараженный, файл программы. Для этого резидентный модуль может временно удалять вирус из зараженного файла. После окончания работы с файлом он заражается снова. Загрузочные стелс-вирусы действуют по такой же схеме. Когда какая-либо программа считывает данные из загрузочного сектора, вместо зараженного подставляется настоящий загрузочный сектор.

3) макрокомандные вирусы. Файлы документов Microsoft Office могут содержать в себе небольшие программы для обработки этих документов, составленные на языке Visual Basic for Applications. Это относится и к базам данных Access, а также к файлам презентаций Power Point. Такие программы создаются с использованием макрокоманд, поэтому вирусы, живущие в офисных документах, называются макрокомандными. Макрокомандные вирусы распространяются вместе с файлами документов. Чтобы заразить компьютер таким вирусом, достаточно просто открыть файл документа в соответствующем приложении. Распространнености данного вида вирусов в немалой степени способствует популярность Microsoft Office. Они могут изменять зараженные документы, оставаясь незамеченными долгое время.

Кроме вирусов принято выделять еще, по крайней мере, три вида вредоносных программ. Это троянские программы, логические бомбы и программы-черви. Четкого разделения между ними не существует: троянские программы могут содержать вирусы, в вирусы могут быть встроены логические бомбы и др.

4) Троянские программы - по основному назначению троянские программы совершенно безобидны или даже полезны. Но когда пользователь запишет программу в свой компьютер и запустит ее, она может незаметно выполнять вредоносные функции. Чаще всего троянские программы используются для первоначального распространения вирусов, для получения удаленного доступа к компьютеру через Интернет, кражи данных или их уничтожения;

5) логические бомбы - программа или ее отдельные модули, которые при определенных условиях выполняют вредоносные действия. Логическая бомба может, например, сработать по достижении определенной даты или тогда, когда в базе данных появится или исчезнет запись, и т. д. Такая бомба может быть встроена в вирусы, троянские программы и даже в обычные программы;

6) программы-черви нацелены на выполнение определенной функции, например, на проникновение в систему и модификацию данных. Можно, скажем, создать программу-червь, подсматривающую пароль для доступа к банковской системе и изменяющую базу данных. Широко известная программа-червь была написана студентом Корнельского университета Робертом Моррисом. Червь Морриса был запущен в Интернет 2 ноября 1988 г. и за 5 часов смог проникнуть более чем на 6000 компьютеров. Некоторые вирусы-черви (например, Code Red) существуют не внутри файлов, а в виде процессов в памяти зараженного компьютера. Это исключает их обнаружение антивирусами, сканирующими файлы и оставляющими без внимания оперативную память компьютера;

7) вирусы в системах документооборота - документы, хранящиеся в базах данных таких систем документооборота, как Lotus Notes и Microsoft Exchange, тоже могут содержать вирусы, точнее, вредоносные макрокоманды. Они могут активизироваться при выполнении каких-либо действий над документом (например, когда пользователь щелкает кнопку мышью). Поскольку такие вирусы расположены не в файлах, а в записях баз данных, для защиты от них требуются специализированные антивирусные программы;

8) новые и экзотические вирусы. По мере развития компьютерных технологий совершенствуются и компьютерные вирусы, приспосабливаясь к новым для себя сферам обитания. Так, новый вирус W32/Perrun, сообщение о котором есть на сайте компании Network Associates, способен распространяться… через файлы графических изображений формата JPEG. Сразу после запуска W32/Perrun ищет файлы с расширением .JPG и дописывает к ним свой код. Надо сказать, что данный вирус не опасен и требует для своего распространения отдельной программы. Среди других "достижений" создателей вредоносных программ заслуживает внимания вирус Palm.Phage. Он заражает приложения "наладонных" компьютеров PalmPilot, перезаписывая файлы этих приложений своим кодом. Появление таких вирусов, как W32/Perrun и Palm.Phage, свидетельствует о том, что в любой момент может родиться компьютерный вирус, троянская программа или червь нового, неизвестного ранее типа, либо известного типа, но нацеленного на новое компьютерное оборудование. Новые вирусы могут использовать неизвестные или не существовавшие ранее каналы распространения, а также новые технологии внедрения в компьютерные системы.

**3. Антивирусные программы**

Антивирус - это программа, предназначенная для сканирования и распознавания на компьютере пользователя программ или скриптов (скрипт - текстовый файл, содержащий секции, параметры секций и значения параметров секций, описывающие действия, которые необходимо выполнить интерпретатору скрипта), макросов (макрос - это набор команд, которые можно применить, нажав всего лишь одну клавишу). С помощью макроса можно автоматизировать любое действие, которое выполняется в используемом приложении, которое может причинить вред пользователю или существенно замедлить работу компьютера.

Антивирусные программы можно разделить на несколько типов:

- **Детекторы**. Их назначение - лишь обнаружить вирус. Детекторы вирусов могут сравнивать загрузочные сектора дискет с известными загрузочными секторами, формируемыми операционными системами различных версий, и таким образом обнаружить загрузочные вирусы или выполнять сканирование файлов на магнитных дисках с целью обнаружения сигнатур известных вирусов. Такие программы в чистом виде в настоящее время редки.

- **Доктора** (Фаги. Фаг) - это программа, которая способна не только обнаружить, но и уничтожить вирус, т.е. удалить его код из зараженных программ и восстановить их работоспособность (если возможно). Известнейшим в России фагом является Aidstest, созданный Д.Н.Лозинским. Одна из последних версий обнаруживает более 8000 вирусов. Aidstest для своего нормального функционирования требует, чтобы в памяти не было резидентных антивирусов, блокирующих запись в программные файлы, поэтому их следует выгрузить, либо, указав опцию выгрузки самой резидентной программе, либо воспользоваться соответствующей утилитой.

- **Ревизоры**. Программа-ревизор контролирует возможные пути распространения программ-вирусов и заражения компьютеров. Программы-ревизоры относятся к самым надежным средствам защиты от вирусов и должны входить в арсенал каждого пользователя. Ревизоры являются единственным средством, позволяющим следить за целостностью и изменениями файлов и системных областей магнитных дисков. Наиболее известна в России программа-ревизор ADinf, разработанная Д.Мостовым.

- **Вакцины**. Так называются антивирусные программы, ведущие себя подобно вирусам, но не наносящие вреда. Вакцины предохраняют файлы от изменений и способны не только обнаружить факт заражения, но и в некоторых случаях "вылечить" пораженные вирусами файлы. В настоящее время антивирусные программы-вакцины широко не применяются, так как в прошлые годы некоторыми некорректно работающими вакцинами был нанесен ущерб многим пользователям.

Для нахождения вирусов Dr Web использует программу эмуляцию процессора, т.е. он моделирует выполнение остальных файлов с помощью программной модели микропроцессора I-8086 и тем самым создает среду для проявления вирусов и их размножения. Таким образом, программа Dr Web может бороться не только с полиморфными вирусами, но и вирусам, которые только еще могут появиться в перспективе.

Основными функциональными особенностями Dr Web являются:

· защита от червей, вирусов, троянов, полиморфных вирусов, макровирусов, spyware, программ-дозвонщиков, adware, хакерских утилит и вредоносных скриптов;

· обновление антивирусных баз до нескольких раз в час, размер каждого обновления до 15 KB;

· проверка системной памяти компьютера, позволяющая обнаружить вирусы, не существующие в виде файлов (например, CodeRed или Slammer);

· эвристический анализатор, позволяющий обезвредить неизвестные угрозы до выхода соответствующих обновлений вирусных баз.

Любой современный антивирусный продукт - это не только набор отдельных технологий детектирования, но и сложная система защиты, построенная на собственном понимании антивирусной компанией того, как нужно обеспечивать безопасность от вредоносных программ.

Антивирус Касперского Personal предназначен для антивирусной защиты персональных компьютеров, работающих под управлением операционных систем Windows 98/ME, 2000/NT/XP, от всех известных видов вирусов, включая потенциально опасное программное обеспечение. Программа осуществляет постоянный контроль всех источников проникновения вирусов - электронной почты, интернета, дискет, компакт-дисков и т.д. Уникальная система эвристического анализа данных эффективно нейтрализует неизвестные вирусы. Можно выделить следующие варианты работы программы (они могут использоваться как отдельно, так и в совокупности):

· Постоянная защита компьютера - проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов.

· Проверка компьютера по требованию - проверка и лечение как всего компьютера в целом, так и отдельных дисков, файлов или каталогов. Такую проверку вы можете запускать самостоятельно или настроить ее регулярный автоматический запуск.

Программа создает надежный барьер на пути проникновения вирусов через электронную почту. Антивирус Касперского Personal автоматически осуществляет проверку и лечение всей входящей и исходящей почтовые корреспонденции по протоколам POP3 и SMTP и эффективно обнаруживает вирусы в почтовых базах. Программа поддерживает более семисот форматов архивированных и сжатых файлов и обеспечивает автоматическую антивирусную проверку их содержимого, а также удаление вредоносного кода из архивных файлов формата ZIP, CAB, RAR, ARJ, LHA и ICE. В состав Антивируса Касперского включен специальный компонент, обеспечивающий защиту файловой системы компьютера от заражения - Файловый Антивирус. Он запускается при старте операционной системы, постоянно находится в оперативной памяти компьютера и проверяет все открываемые, сохраняемые и запускаемые вами или программами файлы.

**Компьютерные вирусы. Антивирусные программы**

**Компьютерные вирусы** – программы, которые создают программисты специально для нанесения ущерба пользователям ПК. Их создание и распространение является преступлением.

Вирусы могут размножаться, и скрыто внедрять свои копии в файлы, загрузочные сектора дисков и документы. Активизация вируса может вызвать уничтожение программ и данных.. Первая эпидемия произошла в 1986г (вирус «Brain» - мозг по англ.) Всемирная эпидемия заражения почтовым вирусом началась 5 мая 2000г, когда компьютеры по сети Интернет получили сообщения «Я тебя люблю» с вложенным файлом, который и содержал вирус.

**Отличительными особенностями компьютерных вирусов** являются: 1) маленький объем; 2) самостоятельный запуск; 3) многократное копирование кода; 4) создание помех для корректной работы компьютера

**По масштабу вредных воздействий** компьютерные вирусы делятся на:

\* ***Безвредные*** – не влияют на работу ПК, лишь уменьшают объем свободной памяти на диске, в результате своего размножения

\* ***Неопасные*** – влияние, которых ограничивается уменьшением памяти на диске, графическими, звуковыми и другими внешними эффектами;

\* ***Опасные*** – приводят к сбоям и зависаниям при работе на ПК;

\* ***Очень опасные*** – приводят к потери программ и данных (изменение, удаление), форматированию винчестера и тд.

**По среде обитания** компьютерные вирусы бывают:

\* ***Файловые вирусы*** способны внедряться в программы и активизируются при их запуске

Из ОП вирусы заражают другие программные файлы (com, exe, sys) меняя их код вплоть до момента выключения ПК. Передаются с нелегальными копиями популярных программ, особенно компьютерных игр. Но не могут заражать файлы данных (изображения, звук)

\* ***Загрузочные вирусы*** передаются через зараженные загрузочные сектора при загрузке ОС и внедряется в ОП, заражая другие файлы. Правила защиты:1)Не рекомендуется запускать файлы сомнительного источника (например, перед загрузкой с диска А – проверить антивирусными программами); 2) установить в BIOS ПК (Setup) защиту загрузочного сектора от изменений

\* ***Макровирусы*** - заражают файлы документов Word и Excel. Эти вирусы являются фактически макрокомандами (макросами) и встраиваются в документ, заражая стандартный шаблон документов. Угроза заражения прекращается после закрытия приложения. При открытии документа в приложениях Word и Excel сообщается о присутствии в них макросов и предлагается запретить их загрузку. Выбор запрета на макросы предотвратит загрузку от зараженных, но и отключит возможность использования полезных макросов в документе

\* ***Сетевые вирусы*** – распространяются по компьютерной сети.

При открытии почтового сообщения обращайте внимание на вложенные файлы!

**Антивирусная программа -** программа, предназначенная для борьбы с компьютерными вирусами.

В своей работе эти программы используют различные принципы для поиска и лечения зараженных файлов.

Для нормальной работы на ПК каждый пользователь должен следить за обновлением антивирусов.

Если антивирусная программа обнаруживает вирус в файле, то она удаляет из него программный код вируса. Если лечение невозможно, то зараженный файл удаляется целиком.

Имеются различные типы антивирусных программ – полифаги, ревизоры, блокировщики, сторожа, вакцины и пр.

**Типы антивирусных программ:**

***Антивирусные сканеры*** – после запуска проверяют файлы и оперативную память и обеспечивают нейтрализацию найденного вируса

***Антивирусные сторожа (мониторы)*** – постоянно находятся в ОП и обеспечивают проверку файлов в процессе их загрузки в ОП

***Полифаги*** – самые универсальные и эффективные антивирусные программы. Проверяют файлы, загрузочные сектора дисков и ОП на поиск новых и неизвестных вирусов. Занимают много места, работают не быстро

***Ревизоры*** – проверяют изменение длины файла. Не могут обнаружить вирус в новых файлах (на дискетах, при распаковке), т.к. в базе данных нет сведений о этих файлах

***Блокировщики*** – способны обнаружить и остановить вирус на самой ранней стадии его развития (при записи в загрузочные сектора дисков). Антивирусные блокировщики могут входить в BIOS Setup

**Компьютерные вирусы и антивирусные программы**   

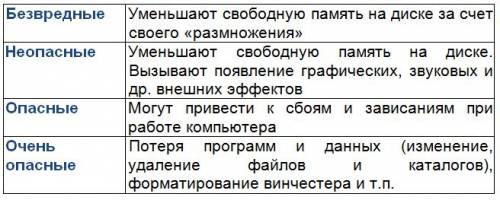

**Компьютерный вирус — специально созданная компьютерная программа, способная самопроизвольно присоединяться к другим программам, создавать свои копии, внедрять их в файлы с целью нарушения работы других программ, порчи файлов и каталогов.**

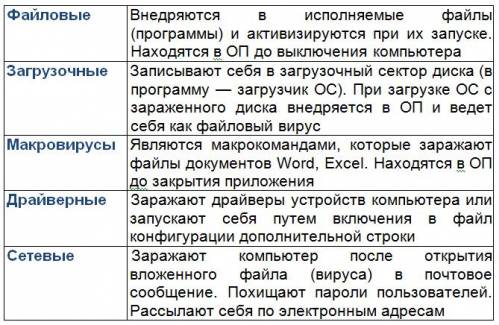
**Признаки проявления вирусов:**

* неправильная работа программ;
* медленная работа компьютера;
* невозможность загрузки операционной системы;
* исчезновение файлов и каталогов;
* изменение размеров файлов;
* неожиданное увеличение количества файлов на диске;
* уменьшение размеров свободной операционной памяти;
* вывод на экран неожиданных сообщений и изображений;
* подача непредусмотренных звуковых сигналов;
* частые «зависания» и сбои в работе компьютера.

**Вирусы могут распространяться через:**

* исполняемые программы;
* документы Word, Excel;
* программное обеспечение компьютера;
* web-страницы;
* файлы из Интернета;
* письма e-mail;
* дискеты и компакт-диски.

**Классификация вирусов по масштабу вредных воздействий**   
[](http://dpk-info.ucoz.ru/_pu/0/78272558.jpg)

**Классификация вирусов по среде обитания**   
[](http://dpk-info.ucoz.ru/_pu/0/86484775.jpg)

**Профилактика компьютерных вирусов:**

* иметь специальный загрузочный диск;
* систематически проверять компьютер на наличие вирусов;
* иметь последние версии антивирусных средств;
* проверять все поступающие данные на наличие вирусов;
* не использовать нелицензионные программные средства;
* выбирать запрет на загрузку макросов при открытии документов Word и Excel;
* выбрать высокий уровень безопасности в «Свойствах обозревателя»;
* делать архивные копии файлов;
* добавить в файл автозагрузки антивирусную программу сторож;
* не открывать вложения электронного письма, если отправитель неизвестен.

**Антивирусные программы — программы, которые предотвращают заражение компьютерным вирусом и ликвидируют последствия заражения.**   
  
Существуют несколько типов антивирусных программ, различающихся выполняемыми функциями.   
  
**Полифаги**

Самыми популярными и эффективными антивирусными программами являются антивирусные программы полифаги (например, Kaspersky Anti-Virus, Dr.Web).   
Для поиска известных вирусов используются так называемые *маски*.   
**Маской вируса является некоторая постоянная последовательность программного кода, специфичная для этого конкретного вируса.**  
Если антивирусная программа обнаруживает такую последовательность в каком-либо файле, то файл считается зараженным вирусом и подлежит лечению.  
Для поиска новых вирусов используются алгоритмы "эвристического сканирования", то есть анализ последовательности команд в проверяемом объекте. Если "подозрительная" последовательность команд обнаруживается, то полифаг выдает сообщение о возможном заражении объекта.

Полифаги могут обеспечивать проверку файлов в процессе их загрузки в оперативную память. Такие программы называются *антивирусными мониторами.*

К *достоинствам полифагов* относится их универсальность. К *недостаткам* можно отнести большие размеры используемых ими антивирусных баз данных, которые должны содержать информацию о максимально возможном количестве вирусов, что, в свою очередь, приводит к относительно небольшой скорости поиска вирусов.

**Ревизоры**

Принцип работы ревизоров (например, ADinf) основан на подсчете контрольных сумм для присутствующих на диске файлов. Эти контрольные суммы затем сохраняются в базе данных антивируса, как и некоторая другая информация: длины файлов, даты их последней модификации и пр.

При последующем запуске ревизоры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, то ревизоры сигнализируют о том, что файл был изменен или заражен вирусом.

*Недостаток ревизоров* состоит в том, что они не могут обнаружить вирус в новых файлах (на дискетах, при распаковке файлов из архива, в электронной почте), поскольку в их базах данных отсутствует информация об этих файлах.

**Блокировщики**

Антивирусные блокировщики - это программы, перехватывающие "вирусоопасные" ситуации и сообщающие об этом пользователю.К таким ситуациям относится, например, запись в загрузочный сектор диска. Эта запись происходит при установке на компьютер новой операционной системы или при заражении загрузочным вирусом.

Наибольшее распространение получили антивирусные блокировщики в BIOS компьютера. С помощью программы BIOS Setup можно провести настройку BIOS таким образом, что будет запрещена (заблокирована) любая запись в загрузочный сектор диска и компьютер будет защищен от заражения загрузочными вирусами.

*К достоинствам блокировщиков* относится их способность обнаруживать и останавливать вирус на самой ранней стадии его размножения.