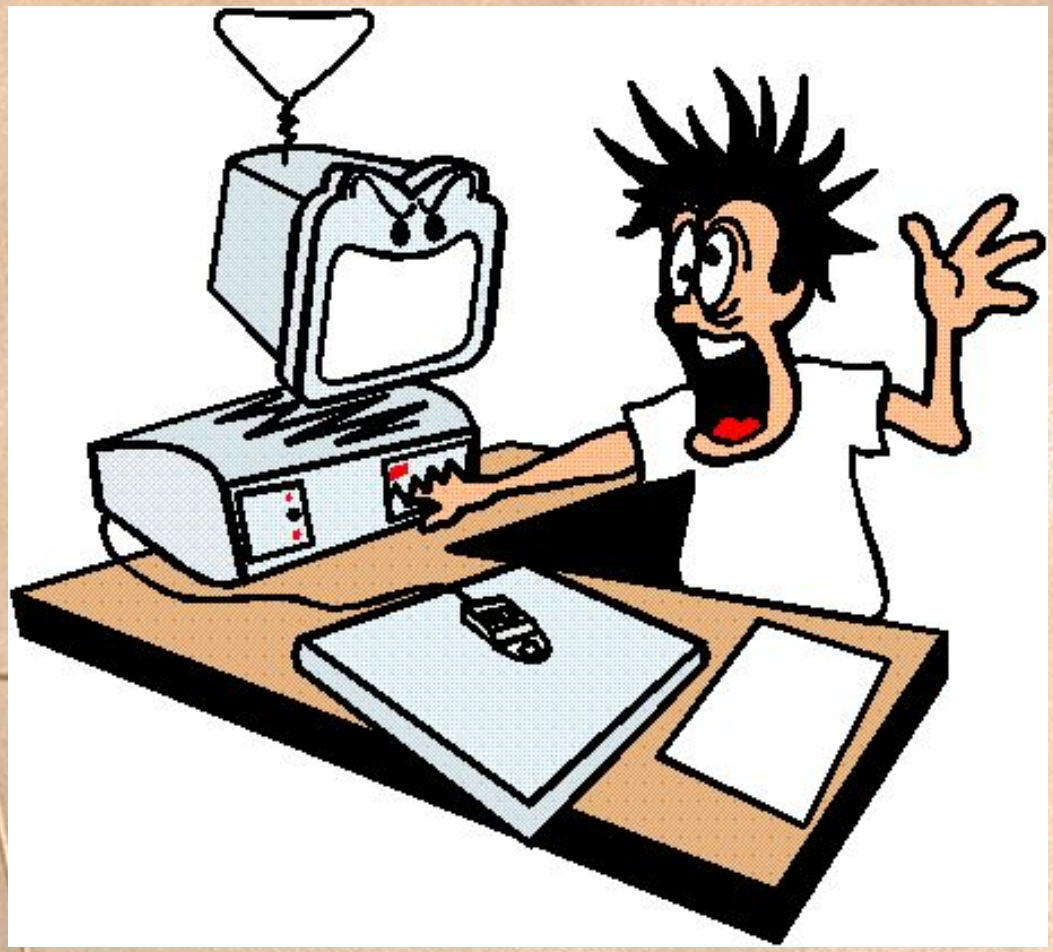
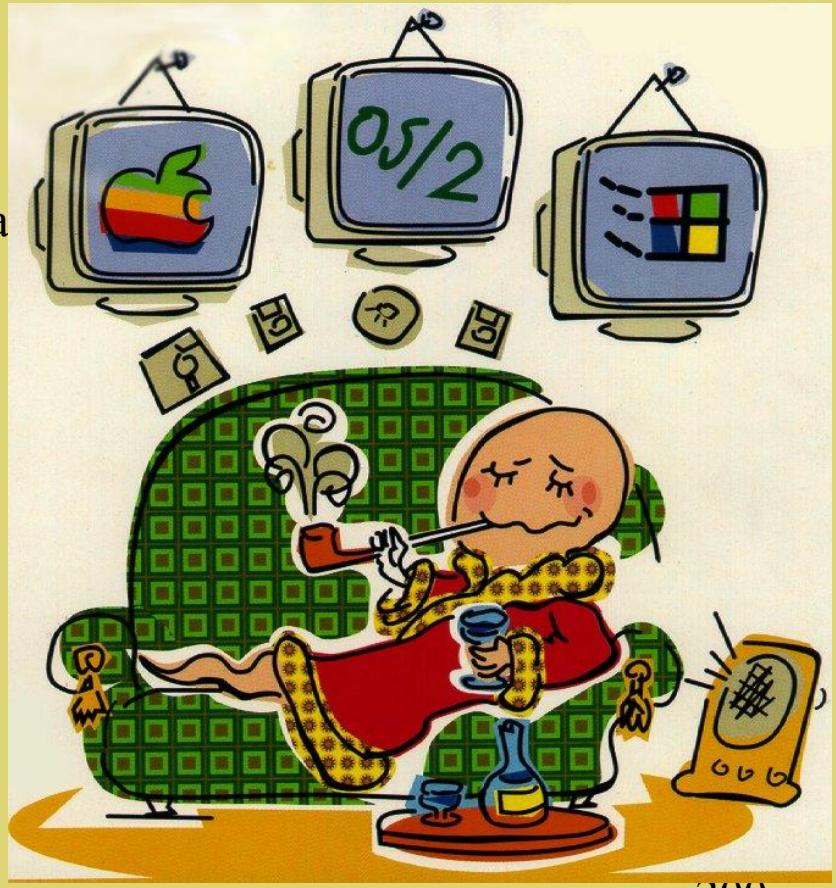
Компьютерные вирусы



Что такое?

Компьютерные вирусы - специально написанные программы, способные самопроизвольно присоединяться к другим программам, создавать свои копии и внедрять их в файлы, системные области компьютера и в вычислительные сети с целью нарушения работы программ, порчи файлов и каталогов, создания всевозможных помех в работе компьютера**.**



Могут быть разрушительными или проявляться в виде помехи, например:

- замена и/или удаление части или всего фа
- форматирование диска,
- разрушение таблицы размещения файлов
- искажение сообщений программы

пользователя и т. п.

Вирусы-помехи могут выводить на экран информацию, затрудняющую чтение сообщений программ.

В настоящее время насчитывается несколько тысяч различных вирусов и их количество продолжает возрастать.

Например, только в глобальной сети Internet ежемесячно появляются не менее 200 вирусов.

Способы распространения компьютерных вирусов

можные каналы проникновения вирусов в компьютер - накопители на сменных носителях информации, главным образом на дискетах, а также средства межкомпьютерной связи.

К последним относятся компьютерные сети, электронная почта, система BBS (Bulletin Board System — доска объявлений) и любая другая непосредственная связь между компьютерами.

Наиболее опасным является распространение вирусов по компьютерной сети, так как в этом случае за короткий промежуток времени может быть заражено большое количество компьютеров. Имеются даже специальные сетевые вирусы, предназначенные для функционирования в сетях.

При запуске инфицированной программы вирус старается отыскать незараженные программы и внедриться в них, а затем производит разрушительные действия.

Классификация компьютерных вирусов

- *Компьютерный вирус* – это программный код, встроенный в другую программу, в документ, или в определенные области носителя данных и предназначенный для выполнения несанкционированных действий на несущем компьютере.
- Так, например, вирусный код может воспроизводить себя в теле других программ (этот процесс называется *размножением*). По прошествии определенного времени, создав достаточное количество копий, программный вирус может перейти к разрушительным действиям – нарушению работы программ и операционной системы, удалению информации, хранящейся на жестком диске и т.д.. Этот процесс называется *вирусной атакой*.
- Вирусы классифицируют по различным признакам.

1. По среде обитания

- ***Сетевые*** вирусы распространяются по различным сетям, т.е. при передаче информации с одного компьютера на другой, соединенные между собой сетью, например Интернет.
- ***Файловые*** вирусы заражают исполнительные файлы и загружаются после запуска той программы, в которой он находится. Файловые вирусы могут внедряться и в другие файлы, но записанные в таких файлах, они не получают управление и теряют способность к размножению.
- ***Загрузочные*** вирусы внедряются в загрузочный сектор дискет или логических дисков, содержащий программу загрузки.
- ***Файлово-загрузочные*** вирусы заражают одновременно файлы и загрузочные сектора диска.

2. По способу заражения среды обитания.

- ***Резидентный вирус*** при заражении 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.
- ***Нерезидентный вирус*** не заражает память компьютера и является активным ограниченное время. Активизируется в определенные моменты, например, при обработке документов текстовым редактором.

3. По деструктивным (разрушительным) возможностям

- ***Безвредные*** вирусы проявляются только в том, что уменьшают объем памяти на диске в результате своего распространения.
- ***Неопасные***, так же уменьшают объем памяти, не мешают работе компьютера, такие вирусы порождают графические, звуковые и другие эффекты.
- ***Опасные вирусы***, которые могут привести к различным нарушениям в работе компьютера, например к зависанию или неправильной печати документа.
- ***Очень опасные***, действие которых может привести к потере программ, данных, стиранию информации в системных областях памяти и даже приводить к выходу из строя движущихся частей жесткого диска при вводе в резонанс.

4. По особенностям алгоритма

- **Паразитические** – это одни из самых простых вирусов. Они изменяют содержимое файлов и секторов диска и могут быть достаточно легко обнаружены и уничтожены.
- **Вирусы-репликаторы** (черви) распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии.
- **Вирусы невидимки** (стелс-вирусы) – вирусы, которые очень трудно обнаружить и обезвредить, так как они перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего незараженные участки диска.
- **Мутанты** (призраки) содержат алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов. Такие вирусы самые сложные в обнаружении.
- **Троянские программы** (квазивирусы) не способны к самораспространению, но очень опасны, так как, маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков.
- **Спутники** – вирус, который не изменяет файл, а для выполнимых программ (exe) создают одноименные программы типа com, которые при выполнении исходной программы запускаются первыми, а затем передают управление исходной выполняемой программе.
- **Студенческие вирусы** представляют собой самые простые и легко обнаруживаемые вирусы.

Однако четкого разделения между ними не существует, и все они могут составлять комбинацию вариантов взаимодействия - своеобразный вирусный "коктейль".

5. Макровирусы

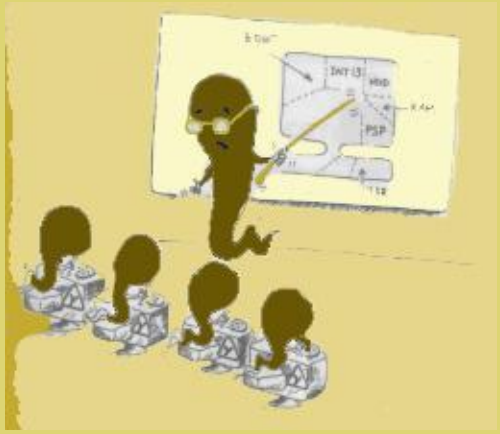
- Эта особая разновидность вирусов поражает документы, выполненные в некоторых прикладных программах, имеющих средства для исполнения так называемых *макрокоманд.*
- В частности, к таким документам относятся документы текстового процессора Microsoft Word. Заражение происходит при открытии файла документа в окне программы, если в ней не отключена возможность исполнения макрокоманд. Как и для других типов вирусов, результат атаки может быть как относительно безобидным, так и разрушительным.

Защита от компьютерных вирусов

Компьютерный вирус аналогичен природному вирусу. Поэтому меры защиты от него включают в себя аналогичный комплекс средств:

Профилактика;

Диагностика;



Лечение.

Профилактика

К ***профилактическим*** средствам относятся:

- перекрытие путей проникновения вирусов в компьютер;
- исключение возможности заражения и порчи вирусами, проникшими в компьютер, других файлов.

Диагностика

- ***Диагностические*** средства позволяют обнаруживать вирусы в компьютере и распознавать их тип.

Лечение

- ***Лечение*** состоит в удалении вирусов из зараженных программных средств и восстановлении пораженных файлов.
- Защитный комплекс основывается на применении антивирусных программ и проведении организационных мероприятий

Организационные мероприятия, производимые для защиты от компьютерных вирусов

Вирусы попадают в компьютер только вместе с программным обеспечением. Поэтому самым важным в защите от вирусов является ***использование незараженных программ,*** так как главным источником вирусов являются незаконные, так называемые «пиратские» копии программного обеспечения.

Особенно опасны компьютерные игры и различного рода развлекательные программы, которые чаще других являются разносчиками компьютерной инфекции. Поэтому первым и наиважнейшим правилом антивирусной защиты является следующее:

Необходимо использовать только лицензионно-чистые программы от надежных поставщиков

Рекомендации

- приобретайте все программы в фирменной упаковке у надежного поставщика;
- не пользуйтесь без крайней необходимостью чужими дискетами;
- не запускайте на выполнение программы, назначение которых неизвестно или непонятно.
- не передавайте свои дискеты чужим лицам для использования, чтобы не заразить ваши дискеты;
- ограничьте доступ к вашему ПК посторонних лиц и запретите им пользоваться своими дискетами без вашего разрешения;
- перед началом работы на ПК после другого лица осуществите холодный перезапуск ПК, чтобы удалить из ОЗУ возможно присутствующие там резидентные вирусы;
- при работе на одном ПК нескольких пользователей разделите жесткий диск на несколько логических и разграничьте право доступа к различным дискам;
- включайте программы антивирусной защиты в файл AUTOEXEC.BAT;
- не ограничивайтесь использованием только одного антивирусного программного продукта. Новые вирусы появляются постоянно, и для их выявления требуются новые антивирусные программы;
- гибкие магнитные диски используйте, по возможности, с защитой от записи

Антивирусные программы

- Программные средства антивирусной защиты обеспечивают диагностику (обнаружение) и лечение (нейтрализацию) вирусов.

Краткий обзор антивирусных программ

- При выборе антивирусной программы необходимо учитывать не только процент обнаружения вирусов, но и способность обнаруживать новые вирусы, количество вирусов в антивирусной базе, частоту ее обновления, наличие дополнительных функций.
- В настоящее время серьезный антивирус должен уметь распознавать не менее 25000 вирусов. Это не значит, что все они находятся "на воле". На самом деле большинство из них или уже прекратили свое существование или находятся в лабораториях и не распространяются. Реально можно встретить 200-300 вирусов, а опасность представляют только несколько десятков из них.
- Существует множество антивирусных программ. Рассмотрим наиболее известные из них.

Антивирусные программы

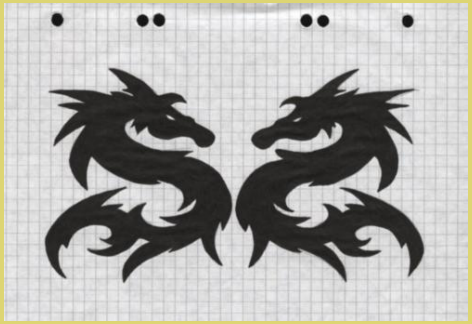
- *Программы-детекторы* обеспечивают поиск и обнаружение вирусов в оперативной памяти и на внешних носителях, и при обнаружении выдают соответствующее сообщение. Различают детекторы универсальные и специализированные.
- **Универсальные детекторы** в своей работе используют проверку неизменности файлов путем подсчета и сравнения с эталоном контрольной суммы. Недостаток универсальных детекторов связан с невозможностью определения причин искажения файлов.
- **Специализированные детекторы** выполняют поиск известных вирусов по их сигнатуре (повторяющемуся участку кода). Недостаток таких детекторов состоит в том, что они неспособны обнаруживать все известные вирусы.

Детектор, позволяющий обнаруживать несколько вирусов, называют **полидетектором**.Недостатком таких антивирусных про грамм является то, что они могут находить только те вирусы, которые известны разработчикам таких программ. .

- ***Программы-доктора*** (фаги), не только находят зараженные вирусами файлы, но и "лечат" их, т.е. удаляют из файла тело программы вируса, возвращая файлы в исходное состояние. В начале своей работы фаги ищут вирусы в оперативной памяти, уничтожая их, и только затем переходят к "лечению" файлов. Среди фагов выделяют **полифаги**, т.е. программы-доктора, предназначенные для поиска и уничто-жения большого количества вирусов.
- Учитывая, что постоянно появляются новые вирусы, программы-детекторы и программы-доктора быстро устаревают, и требуется регулярное обновление их версий.

Программы-ревизоры относятся к самым надежным средствам защиты от вирусов. Ревизоры запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным. Обнаруженные изменения выводятся на экран видеомонитора. Как правило, сравнение состояний производят сразу после загрузки операционной системы. При сравнении проверяются длина файла, код циклического контроля (контрольная сумма файла), дата и время модификации, другие параметры.

- Программы-ревизоры имеют достаточно развитые алгоритмы, обнаруживают стелс-вирусы и могут даже отличить изменения версии проверяемой программы от изменений, внесенных вирусом.



- ***Программы-фильтры*** (сторожа) представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов. Такими действиями могут являться:
- • попытки коррекции файлов с расширениями COM и EXE;
- • изменение атрибутов файлов;
- • прямая запись на диск по абсолютному адресу;
- • запись в загрузочные сектора диска.
- • загрузка резидентной программы.
- При попытке какой-либо программы произвести указанные действия "сторож" посылает пользователю сообщение н предлагает запретить или разрешить соответствующее действие. Программы-фильтры весьма полезны, так как способны обнаружить вирус на самой ранней стадии его существования до размножения.

Однако они не "лечат" файлы и диски. Для уничтожения вирусов требуется применить другие программы, например фаги. К недостаткам программ-сторожей можно отнести их "назойливость" (например, они постоянно выдают предупреждение о любой попытке копирования исполняемого файла), а также возможные конфликты с другим программным обеспечением.

Поскольку функции детектора, ревизора и сторожа дополняют друг друга, то в современные антивирусные комплекты программ обычно входят компоненты, реализующие все эти функции. При этом часто функции детектора и ревизора совмещаются в одной программе.

- ***Вакцины*** (иммунизаторы) - это резидентные программы, предотвращающие заражение файлов. Вакцины применяют, если отсутствуют программы-доктора, "лечащие" этот вирус. Вакцинация возможна только от известных вирусов. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедрится. В настоящее время программы-вакцины имеют ограниченное применение.
- Существенным недостатком таких программ является их ограниченные возможности по предотвращению заражения от большого числа разнообразных вирусов.

Несмотря на все принятые профилактические меры, стопроцентной гарантии защиты от вирусов в настоящее время не существует.

Поэтому в целях восстановления разрушенной вирусом информации и удаленных зараженных программ, которые не удалось вылечить программами антивирусной защиты, необходимо соблюдать еще одно правило антивирусной защиты:

Всегда имейте резервные копии программ и файлов данных на дискете, магнитной ленте и/или другом ПК не менее чем в двух экземплярах.

Убытки

- Несмотря на огромные усилия конкурирующих между собой антивирусных фирм, убытки, приносимые компьютерными вирусами, не падают и достигают астрономических величин в сотни миллионов долларов ежегодно. При этом следует иметь в виду, что антивирусные программы и "железо" не дают полной гарантии защиты от вирусов. Зачастую как пользователи, так и профессионалы-программисты не имеют достаточных навыков "самообороны", а их представления о вирусе порой являются весьма поверхностными.
- Борьба с компьютерными вирусами является борьбой человека с человеческим же разумом. Эта борьба является борьбой умов, поскольку задачи, стоящие перед вирусологами, ставят такие же люди. Одни придумывают новый вирус - а другим с ним разбираться.