

Вируссы!!!



Вируссы!!!



Компьютерный вирус — вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи с целью нарушения работы программно-аппаратных комплексов, удаления файлов, приведения в негодность структур размещения данных, блокирования работы пользователей или же приведения в негодность аппаратных комплексов компьютера.



Отличительными особенностями компьютерных вирусов являются:

- 1) маленький объем;
- 2) самостоятельный запуск;
- 3) многократное копирование кода;
- 4) создание помех для корректной работы компьютера



Основные источники вирусов:

- 1. дискета, на которой находятся зараженные вирусом файлы;**
- 2. компьютерная сеть, в том числе система электронной почты и Internet:**
- 3. жесткий диск, на который попал вирус в результате работы с зараженными программами;**
- 4. вирус, оставшийся в оперативной памяти после предшествующего пользователя.**



Имеются несколько признаков классификации существующих вирусов:

- по среде обитания;
- по области поражения;
- по особенности алгоритма;
- по способу заражения;

УКТИВНЫМ ВОЗМОЖНОСТЯМ.

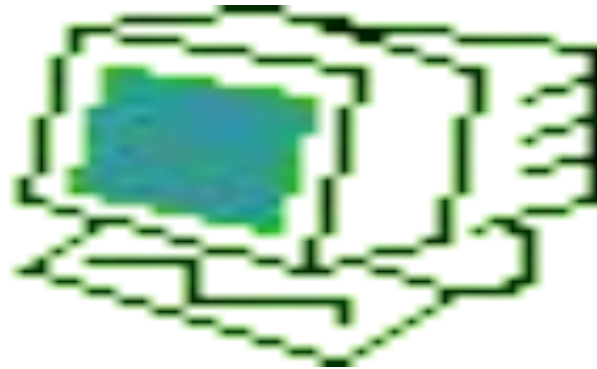


По методу существования в компьютерной среде вирусы делятся на такие виды:

- 1. Резидентные**
- 2. Нерезидентные**



Резидентный вирус находится в памяти компьютерной системы и является активным, перехватывая обращения операционной системы к различным программам и внедряются в них.



Нерезидентный вирус не заражают память компьютерной системы и остаются активными ограниченное время .

По величине вредных воздействий вирусы можно разделить на:

- **неопасные, влияние которых ограничивается уменьшением свободной памяти на диске, графическими, звуковыми и другими внешними эффектами;**
- **опасные, которые могут привести к сбоям и зависаниям при работе компьютера;**
- **очень опасные, активизация которых может привести к потере программ и данных (изменению или удалению файлов и каталогов), форматированию винчестера и так далее.**



Основные ранние признаки заражения компьютера вирусом:

- уменьшение объема свободной оперативной памяти;
- замедление загрузки и работы компьютера;
- непонятные (без причин) изменения в файлах, а также изменения размеров и даты последней модификации файлов;
- ошибки при загрузке операционной системы;
- невозможность сохранять файлы в нужных каталогах;
- непонятные системные сообщения музыкальные и визуальные
- эффекты и т.д.



Признаки активной фазы вируса:

невозможность загрузки файлов или операционной системы;

исчезновение файлов;

форматирование жесткого диска.



По среде обитания различают:

1. Файловые вирусы — наиболее распространенный тип вирусов. Эти вирусы внедряются в выполняемые файлы и активизируются при их запуске. После запуска зараженного файла вирус находится в оперативной памяти компьютера и может заражать другие файлы вплоть до момента выключения компьютера или перезагрузке компьютера. Все файловые вирусы резидентны, и их лечение затруднено, т.к. даже после удаления зараженных файлов с дисков, вирус остается в оперативной памяти и возможно повторное заражение файлов.

Профилактическая защита от файловых вирусов состоит в том, что не рекомендуется запускать на исполнение файлы не проверенные антивирусными программами.



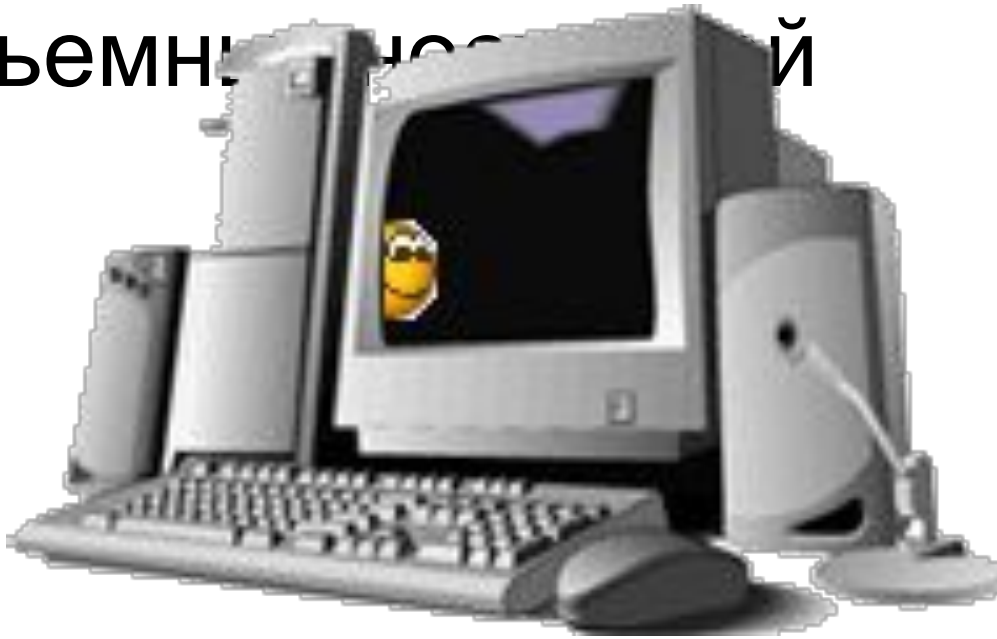
2. Загрузочные вирусы записывают себя в загрузочный сектор диска или в сектор системного загрузчика жесткого диска. Вирусы начинают работу при загрузке компьютера и обычно становятся резидентными.

При заражении дисков загрузочные вирусы подставляют свой код вместо программы, получающей управление при загрузке системы и отдавая управление не оригинальному коду загрузочного сектора, а коду вируса.

При заражении диска вирус переносит оригинальный загрузочный сектор



Профилактическая защита от
загрузочных вирусов состоит в
отказе от загрузки
операционной системы со
съёмными носителями



3. Макровирусы заражают файлы широко используемых пакетов обработки данных. Эти вирусы представляют собой программы, написанные на встроенных в эти пакеты языках программирования. Наибольшее распространение получили макровирусы для приложений Microsoft Office.



Профилактическая защита от макровирусов состоит в предотвращении запуска вирусов, т.к. при открытии документа в приложениях Microsoft Office сообщается о присутствии в них вирусов и предлагает запретить их загрузку.



Общие средства, помогающие предотвратить заражение и его разрушительные последствия:

- резервное копирование информации (создание копий файлов и системных областей жестких дисков);
- избежание пользования случайными и неизвестными программами. Чаще всего вирусы распространяются вместе с компьютерными программами;
- перезагрузка компьютера перед началом работы, в частности, в случае, если за компьютером работали другие пользователи;
- ограничение доступа к информации, в частности физическая защита дисков во время копирования файлов с нее.



Антивирусная программа — это компьютерная программа, которая выявляет, предотвращает и выполняет определенные действия, чтобы блокировать или удалять вредоносные программы



Для борьбы с вирусами существуют программы, которые можно разбить на основные группы:

- мониторы,
- детекторы,
- доктора,
- ревизоры,
- вакцины.



Программы-мониторы (программы-фильтры) располагаются резидентно в

ОП компьютера, перехватывают и сообщают пользователю об обращениях ОС, которые используются вирусами для размножения и нанесения ущерба.

Пользователь имеет возможность разрешить или запретить выполнение этих обращений. К преимуществу таких

программ относится возможность обнаружения неизвестных вирусов. Использование программ-фильтров позволяет обнаруживать вирусы на ранней стадии заражения компьютера.

Программы-детекторы

проверяют, имеется ли в файлах и на дисках специфическая для данного вируса комбинация байтов.

При ее обнаружении

выводится

соответствующее

сообщение. Недостаток —

возможность защиты только

от известных вирусов.





Программы-доктора (фаги)

восстанавливают зараженные программы путем удаления из них тела вируса. Обычно эти программы рассчитаны на конкретные типы вирусов и основаны на сравнении последовательности кодов, содержащихся в теле вируса, с кодами проверяемых программ. Программы-доктора необходимо периодически обновлять с целью получения новых версий, обнаруживающих новые виды

Программы-ревизоры

анализируют изменения
состояния файлов и
системных областей диска.

Проверяют состояние
загрузочного сектора,
длину, атрибуты и время
создания файлов;

контрольную сумму кодов
Пользователю сообщается
выявлении несоответствий.



Программы-вакцины

модифицируют программы и риски так, что это не отражается на работе программ, но вирус, от которого производится вакцинация, считает программы или диски уже зараженными.

Существующие антивирусные программы в основном относятся к классу гибридных (детекторы-доктора, доктора-ревизоры и п



Недостатки антивирусных программ

- ∅ Ни одна из существующих антивирусных технологий не может обеспечить полной защиты от вирусов.
- ∅ Антивирусная программа забирает часть вычислительных ресурсов системы, нагружая центральный процессор и жёсткий диск.
- ∅ Антивирусные программы могут видеть угрозу там, где её нет (ложные срабатывания).
- ∅ Различные методы шифрования и упаковки вредоносных программ делают даже известные вирусы не обнаруживаемыми антивирусным программным обеспечением.

