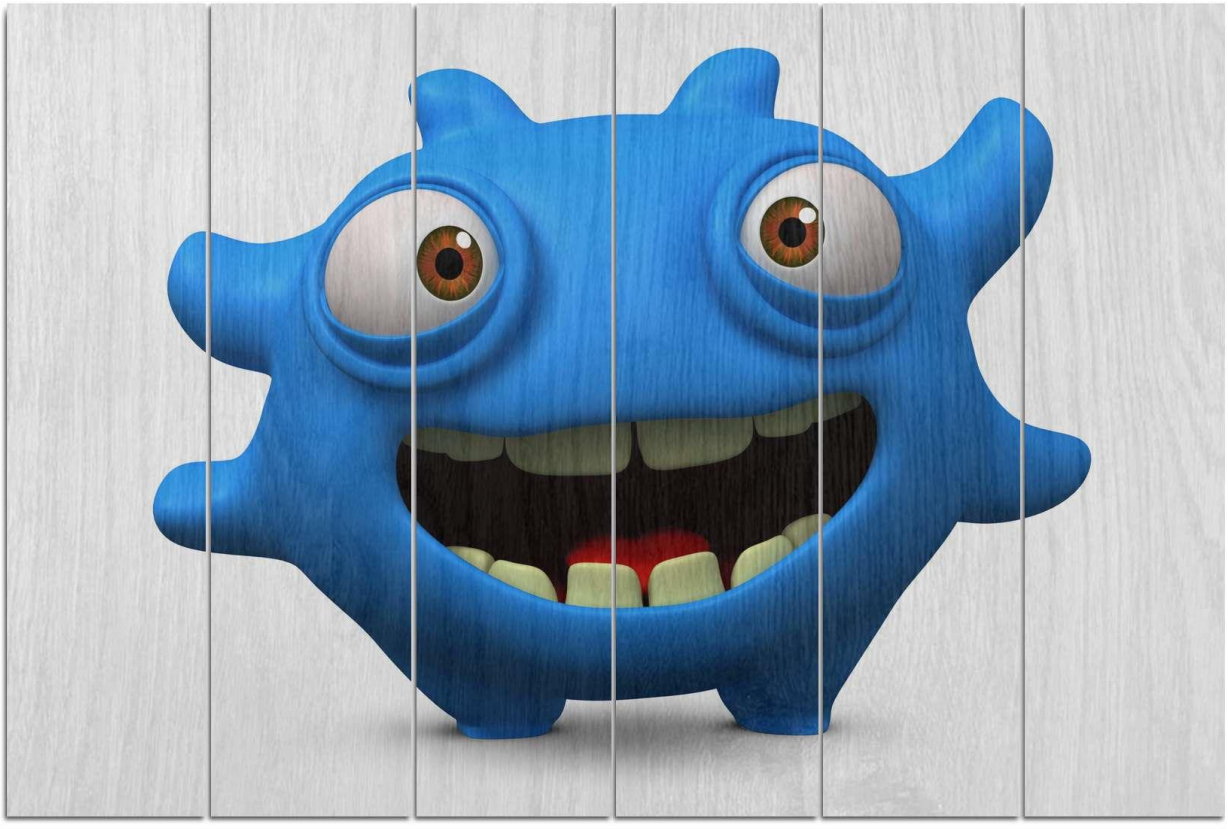
Компьютерные вирусы и антивирусные программы



КОМПЬЮТЕРНЫЕ ВИРУСЫ -

это программы, которые могут «размножаться» и скрытно внедрять свои копии: в файлы, загрузочные секторы дисков, документы и т.д.

По степени воздействия вирусы бывают:

неопасные, *действие которых приводит к:*

- *уменьшению свободной памяти на диске,*
- *графическим и звуковым эффектам;*

- ***опасные,*** *действие которых приводит к:*
  - *сбоям и зависанию компьютера;*
- ***очень опасные,*** *действие которых приводит к:*
  - *потере программ и данных (изменению или удалению файлов и каталогов)*
  - *форматированию винчестера и т.д.*

По среде обитания:

- **файловые** - *внедряются в исполняемые файлы, создают свои копии в различных каталогах, наиболее распространенный тип вирусов;*
- **загрузочные** - *записывают себя в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (Master Boot Record); были достаточно распространены в 1990-х, но практически исчезли с переходом на 32-битные операционные системы и отказом от использования дискет как основного способа обмена информацией;*

- **макровирусы** - *заражают файлы документов Word и электронных таблиц Excel; являются программами на макро-языках, встроенных в системы обработки данных;*
- **сетевые** – *передаются по сети: обычные (описаны выше), Интернет-черви, троянские программы (передаются во вложенных в почтовые сообщения файлах) и скрипт-вирусы (передаются через программы на языках JavaScript, VBScript).*

По алгоритмам:

- **файловые** - *внедряются в исполняемые файлы, создают свои копии в различных каталогах, наиболее распространенный тип вирусов;*
- **загрузочные** - *записывают себя в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (Master Boot Record); были достаточно распространены в 1990-х, но практически исчезли с переходом на 32-битные операционные системы и отказом от использования дискет как основного способа обмена информацией;*
- **макровирусы** - *заражают файлы документов Word и электронных таблиц Excel; являются программами на макро-языках, встроенных в системы обработки данных;*
- **сетевые** – *передаются по сети: обычные (описаны выше), Интернет-черви, троянские программы (передаются во вложенных в почтовые сообщения файлах) и скрипт-вирусы (передаются через программы на языках JavaScript, VBScript).*

По способу заражения:

- перезаписывающие - вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое;
- паразитические - при распространении своих копий обязательно изменяют содержимое файлов, оставляя сами файлы при этом полностью или частично работоспособными;
- вирусы-компаньоны - вирусы, не изменяющие заражаемых файлов: для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник, т. е. вирус.
- вирусы-ссылки - не изменяют физического содержимого файлов, однако при запуске зараженного файла «заставляют» ОС выполнить свой код;
- вирусы, заражающие исходные тексты программ;
- прочие способы заражения: существуют вирусы, которые не связывают свое присутствие с каким-либо выполняемым файлом. При размножении они копируют свой код в какие-либо каталоги дисков в надежде, что новые копии будут когда-либо запущены пользователем.

Стадии вируса:

- **Пассивная стадия**

Вирус практически не проявляет себя, стараясь оставаться незаметным. Получая управление на этой стадии, вирус отыскивает на других дисках компьютера системные или прикладные программы и внедряется в них. Продолжительность: от нескольких минут до нескольких лет.

- **Активная стадия, или вирусная атака**

Вирусная атака может начинаться одновременно на всех пораженных компьютерах или в разное время. Обычно атака начинается с выполнения некоторого общего для всех компьютеров условия

Как обнаружить хакерскую атаку:

- Подозрительно высокий исходящий трафик. Подобный компьютер может использоваться для скрытой рассылки спама или для размножения сетевых червей.
- Повышенная активность жестких дисков или подозрительные файлы в корневых директориях.
- Большое количество пакетов с одного и того же адреса, останавливаемые персональным межсетевым экраном.
- Постоянная антивирусная защита вашего компьютера сообщает о присутствии на компьютере троянских программ, хотя в остальном все работает нормально. Если

ваш антивирус сообщает о поимке подобных вредоносных программ, то это может являться признаком того, что ваш компьютер открыт для несанкционированного удаленного доступа.

Признаки заражения:

- Замедление работы компьютера
- Невозможность загрузки ОС
- Частые зависания и сбои в работе компьютера
- Вывод на экран непредусмотренных сообщений и изображений
- Подача непредусмотренных звуковых сигналов
- Произвольный запуск каких-либо программ
- Попытка какой-либо программы выйти в сеть Интернет
- Подозрительно высокий исходящий трафик
- Увеличение количества файлов и их размеров
- Знакомые говорят о сообщении, которое вы не посылали
- В электронной почте письма без обратного адреса и заголовка

Что делать, если компьютер заражён:

- Не паниковать
- Отключить компьютер от сети Интернет
- Отключить компьютер от локальной сети
- Установить антивирусную программу

Выполнить полную проверку компьютера.

Антивирусные программы:

- **Полифаги *(Kaspersky, Dr.Web)*:**
  - проверяют файлы, загрузочные секторы дисков и оперативную память и ищут известные и новые (неизвестные полифагу) вирусы;
  - могут обеспечивать проверку файлов в процессе их загрузки в оперативную память ***(мониторы)***
- **Ревизоры *(ADinf)*:**

- подсчитывают контрольные суммы для файлов на диске и хранят их в базе данных ;

- **Блокировщики *(в BIOS компьютера)*:**
  - перехватывают «вирусоопасные» ситуации и сообщают об этом пользователю.