

Компьютерные вирусы. Антивирусные программы.



Работу выполнила Маркина Анастасия.
Презентация подготовлена для конкурса
"Интернешка" <http://interneshka.org/>

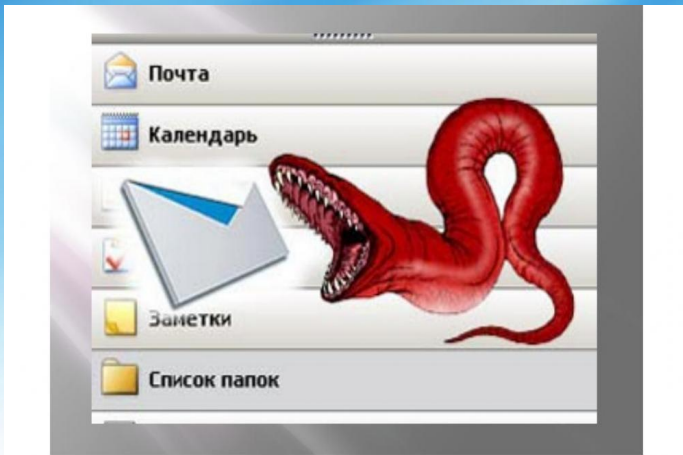
Содержание.

1. Что такое компьютерный вирус?
2. Классификация вирусов.
3. Антивирусная программа.
4. Типы антивирусных программ.
5. Спасибо за внимание.

Что такое компьютерные

вирусы?

- **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



Что такое компьютерные вирусы?



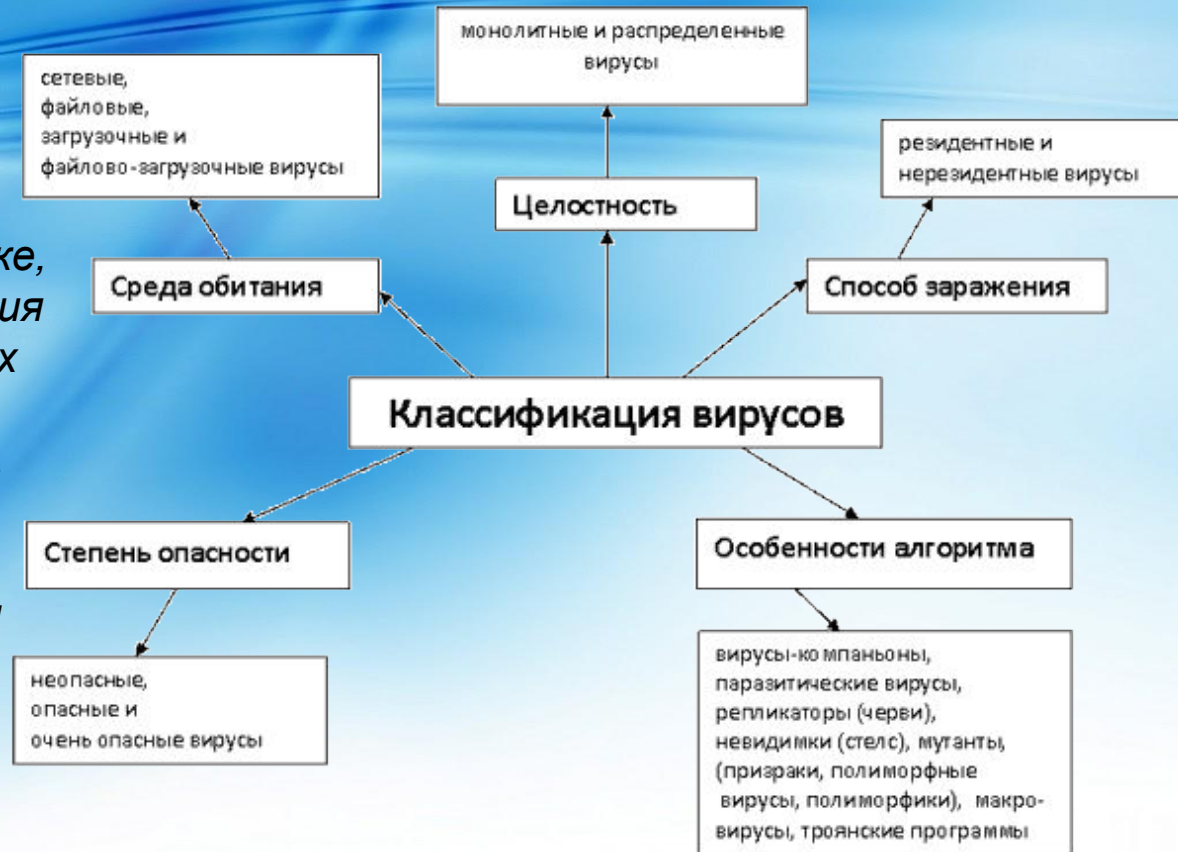
- Активизация вируса может вызвать уничтожение программ и данных.. Первая эпидемия произошла в 1986г (вирус «Brain» - мозг по англ.) Всемирная эпидемия заражения почтовым вирусом началась 5 мая 2000г, когда компьютеры по сети Интернет получили сообщения «Я тебя люблю» с вложенным файлом, который и содержал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



Классификация вирусов.

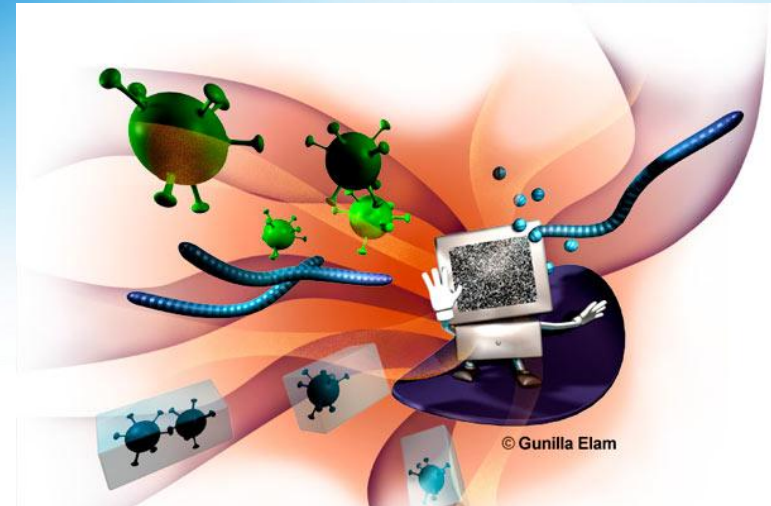
По масштабу вредных воздействий компьютерные вирусы делятся на:

- * **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 потере программ и данных (изменение, удаление), форматированию винчестера и тд.



Классификация вирусов.

- 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



Классификация вирусов.

- * **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.

- **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.



Типы антивирусных программ.

- **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.



*Будьте осторожнее в
Интернете.
Находитесь только на
проверенных сайтах.
Спасибо за внимание!!!*

