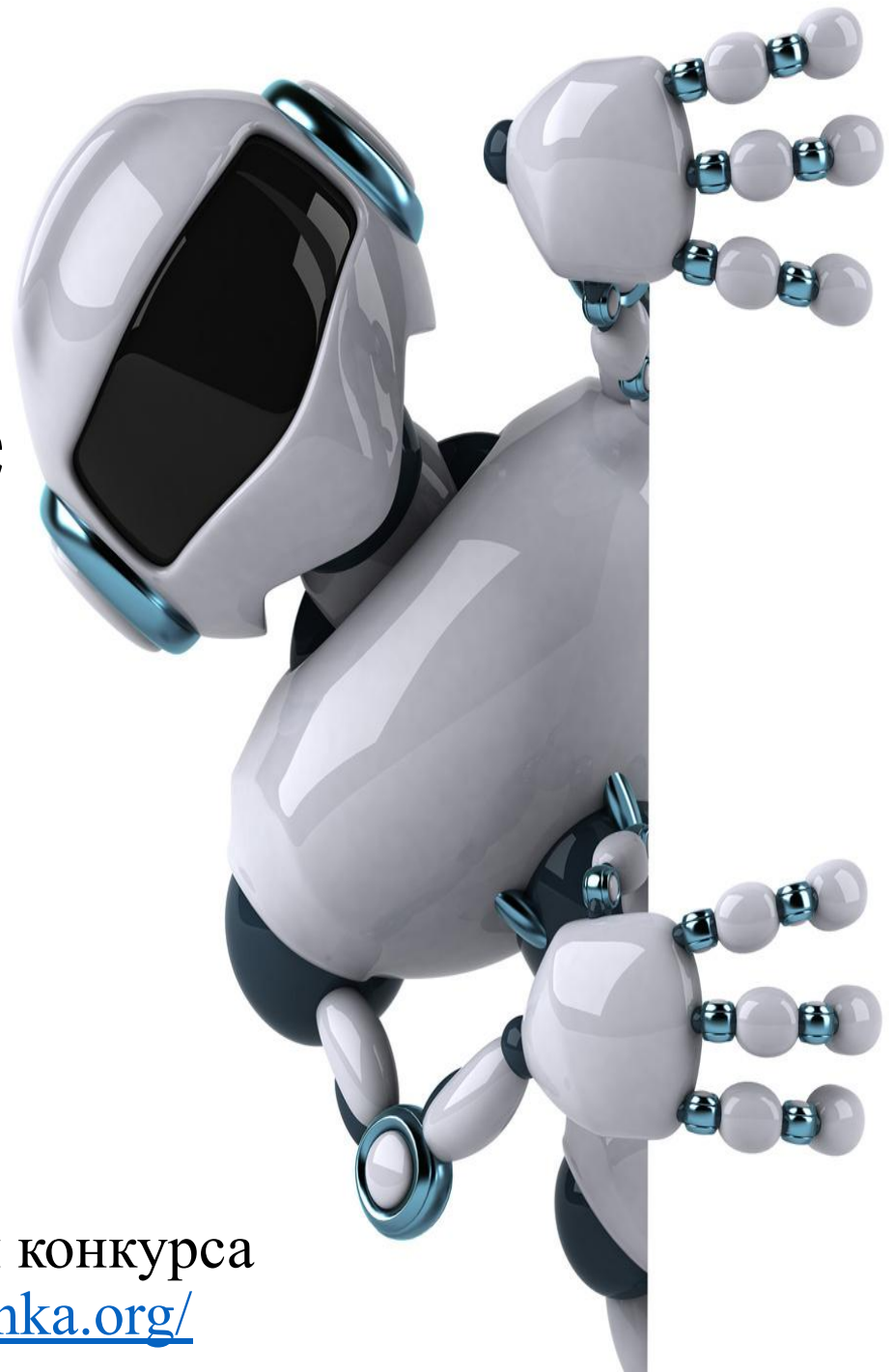


Компьютерные вирусы. Антивирусные программы



Презентация подготовлена для конкурса
"Интернешка" <http://interneshka.org/>

Компьютерный вирус

Компьютерный вирус – это программа, способная создавать свои копии, внедрять их в различные объекты или ресурсы компьютерных систем, сетей и производить определенные действия без ведома пользователя.



Первая эпидемия произошла в 1986 г. (вирус «Brain» - мозг по англ.)

Всемирная эпидемия заражения почтовым вирусом началась 5 мая 2000 г., когда компьютеры по сети Интернет получили сообщения «Я тебя люблю» с вложенным файлом, который и содержал вирус.

✓ **В среднем в день появляется около 300 новых разновидностей компьютерных вирусов**

Стадии существования компьютерных вирусов

- *латентная* (вирус не проявляет себя, не предпринимает никаких действий);
- *инкубационная* (вирус создаёт свои копии и внедряет их в свою среду обитания);
- *активная* (вирус всё также размножается, но уже начинает проявлять себя).



Особенности компьютерного вируса



- маленький объем;
- самостоятельный запуск;
- многократное копирование кода;
- создание помех для корректной работы компьютера

Классификация компьютерных вирусов

По масштабу вредных воздействий

- **Безвредные**
- **Неопасные**
- **Опасные**
- **Очень опасные**

По среде обитания

- **Файловые вирусы**
- **Загрузочные вирусы**
- **Макровирусы**
- **Сетевые вирусы**

По способу заражения

- **Резидентные**
- **Нерезидентные**

По целостности

- **Монолитные**
- **Распределенные**

Деление вирусов по масштабу вредных воздействий

Безвредные

- не влияют на работу ПК, лишь уменьшают объем свободной памяти на диске, в результате своего размножения

Неопасные

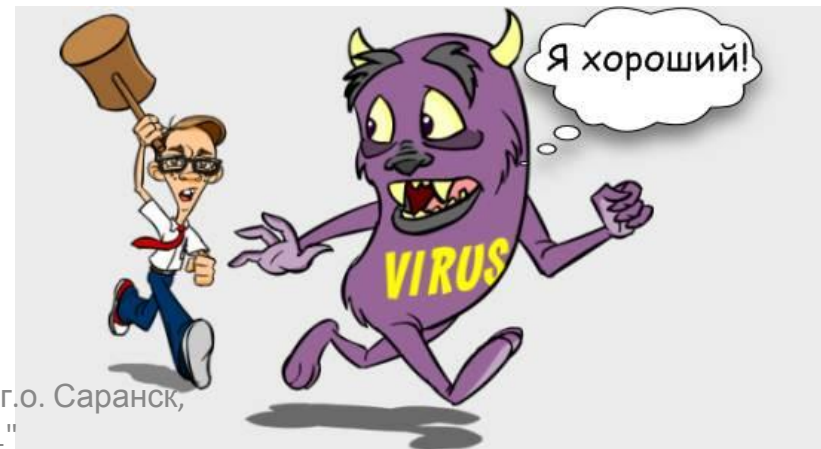
- влияние, которых ограничивается уменьшением памяти на диске, графическими, звуковыми и другими внешними эффектами

Опасные

- приводят к сбоям и зависаниям при работе на ПК

Очень опасные

- приводят к потере программ и данных (изменение, удаление), форматированию винчестера.



Деление вирусов по среде обитания

Файловые вирусы

- способны внедряться в программы и активизируются при их запуске

Загрузочные вирусы

- передаются через зараженные загрузочные сектора при загрузке ОС и внедряется в ОП, заражая другие файлы.

Файлово-загрузочные

- способны заражать и загрузочные секторы и файлы

Макровирусы

- заражают файлы документов Word и Excel;
- являются фактически макрокомандами (макросами) и встраиваются в документ, заражая стандартный шаблон документов;
- угроза заражения прекращается после закрытия приложения

Сетевые вирусы

- распространяются по компьютерной сети.



Деление вирусов по способу заражения

Резидентные

- оставляют в оперативной памяти свою резидентную часть, которая затем перехватывает обращения программ к ОС и внедряется в них. Свои деструктивные действия вирус может повторять многократно.

Нерезидентные

- не заражают оперативную память и проявляют свою активность лишь однократно при запуске зараженной программы.



Деление вирусов по целостности

Монолитные

- программа вируса - единый блок, который можно обнаружить после инфицирования.

Распределенные

- программа разделена на части. Эти части содержат инструкции, которые указывают компьютеру, как собрать их воедино, чтобы воссоздать вирус.



Различные вирусы выполняют различные действия

Выводят на экран мешающие текстовые сообщения ;

Создают звуковые и видео-эффекты;

Замедляют работу ЭВМ, постепенно уменьшают объем свободной оперативной памяти;

Увеличивают износ оборудования;

Вызывают отказ отдельных устройств, зависание или перезагрузку компьютера и крах работы всей ЭВМ;

Уничтожают FAT, форматируют жесткий диск, стирают BIOS, уничтожают данные, стирают антивирусные программы;

Выводят из строя системы защиты информации

Симптомы вирусного заражения ЭВМ

- Замедление работы некоторых программ;
- Увеличение размеров файлов;
- Появление не существовавших ранее «странных» файлов;
- Уменьшение объема доступной оперативной памяти (по сравнению с обычным режимом работы);
- Внезапно возникающие разнообразные видео и звуковые эффекты;
- Появление сбоев в работе ОС;
- Запись информации на диски в моменты времени, когда этого не должно происходить;
- Прекращение работы или неправильная работа ранее нормально функционировавших программ.



Антивирусная программа

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

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.



Типы антивирусных программ

Антивирусные сканеры

- после запуска проверяют файлы и оперативную память и обеспечивают нейтрализацию найденного вируса

Антивирусные 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.

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).

Меры по защите ЭВМ от заражения вирусами

- Оснащение ЭВМ современными антивирусными программами и регулярное обновление их версий.
- Установка программы-фильтра при работе в глобальной сети.
- При переносе на свой ПК файлов в архивированном виде проверка их сразу после разархивации.
- Создание архивных копий ценной информации на других носителях информации.
- Не оставлять дискету в дисковом диске при включении или перезагрузки ПК, т.к. возможно заражение загрузочными вирусами. Наличие аварийной загрузочной дискеты, с которой можно будет загрузиться, если система откажется сделать это обычным образом.
- При установке большого программного продукта вначале проверить все дистрибутивные файлы, а после инсталляции продукта повторно произвести контроль наличия вирусов.

