



Презентация подготовлена для конкурса по информатике (от АО «Лаборатория Касперского»)



## НАНЕСЕНИЯ УЩЕРБА ПОЛЬЗОВАТЕЛЯМ ПК.

ОТЛИЧИТЕЛЬНЫМИ ОСОБЕННОСТЯМИ КОМПЬЮТЕРНЫХ ВИРУСОВ ЯВЛЯЮТСЯ:

- 1) **МАЛЕНЬКИЙ ОБЪЕМ;**
- 2) **САМОСТОЯТЕЛЬНЫЙ ЗАПУСК;**
- 3) **МНОГОКРАТНОЕ КОПИРОВАНИЕ КОДА;**
- 4) **СОЗДАНИЕ ПОМЕХ ДЛЯ КОРРЕКТНОЙ РАБОТЫ КОМПЬЮТЕРА .**

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 потери программ и данных (изменение, удаление), форматированию винчестера и тд.

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

- \* **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!

**РЕЗИДЕНТНЫЕ ВИРУСЫ** ПРЕДСТАВЛЯЮТ СОБОЙ ПРОГРАММЫ, ПРИСУТСТВУЮЩИЕ В ОПЕРАТИВНОЙ ПАМЯТИ ЛИБО ХРАНЯЩИЕ ТАМ СВОЮ АКТИВНУЮ ЧАСТЬ, КОТОРАЯ ПОСТОЯННО ЗАРАЖАЕТ ТЕ ИЛИ ИНЫЕ ОБЪЕКТЫ ОПЕРАЦИОННОЙ СИСТЕМЫ.

**НЕРЕЗИДЕНТНЫЕ ВИРУСЫ** ЗАГРУЖАЮТСЯ ЛИШЬ ВО ВРЕМЯ ОТКРЫТИЯ ЗАРАЖЕННОГО ФАЙЛА ИЛИ РАБОТЫ С ИНФИЦИРОВАННЫМ ПРИЛОЖЕНИЕМ.

По особенностям алгоритма работы различают:

- **Простейшие вирусы** – вирусы, которые при распространении своих копий обязательно изменяют содержимое дисковых секторов или файлов, поэтому его достаточно легко обнаружить.
- **Вирусы-спутники (компаньоны)** – вирус, который не внедряется в сам исполняемый файл, а создает его зараженную копию с другим расширением.
- **Стелс-вирус (невидимка)** – вирусы, скрывающие свое присутствие в зараженных объектах, подставляя вместо себя незараженные участки.
- **Полиморфные вирусы (мутанты)** – вирусы, модифицирующие свой код таким образом, что копии одного и того же вируса не совпадали.
- **Макровирус** – вирусы, которые заражают документы офисных приложений.
- **Троянская программа** – программа, которая маскируется под полезные приложения (утилиты или даже антивирусные программы), но при этом производит различные шпионские действия. Она не внедряется в другие файлы и не обладает способностью к саморазмножению.
- **Черви** – это вредительские компьютерные программы, которые способны саморазмножаться, но, в отличие от вирусов не заражают другие файлы. Свое название черви получили потому, что для распространения они используют компьютерные сети и электронную почту.



**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.

**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.

**ПОПУЛЯРНЫЕ АНТИВИРУСЫ**

AVAST FREE ANTIVIRUS 2016

AVIRA FREE ANTIVIRUS

COMODO INTERNET SECURITY PREMIUM

AVG ANTIVIRUS FREE 2016

360 TOTAL SECURITY

MICROSOFT SECURITY ESSENTIALS

PANDA FREE ANTIVIRUS

360 TOTAL SECURITY ESSENTIAL

COMODO ANTIVIRUS

AD-AWARE FREE ANTIVIRUS+



