

Тема урока:



Компьютерные вирусы и антивирусные программы.

Вредоносные программы



Это программы, наносящие вред
данным и программам,
хранящимся на компьютере



Типы вредоносных программ

- Вирусы, черви, троянские и хакерские программы;
- Шпионское, рекламное ПО, программы скрытого дозвона;
- Потенциально опасное ПО.



Компьютерные вирусы

Компьютерные вирусы - это вредоносные программы, которые могут «размножаться» и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы.



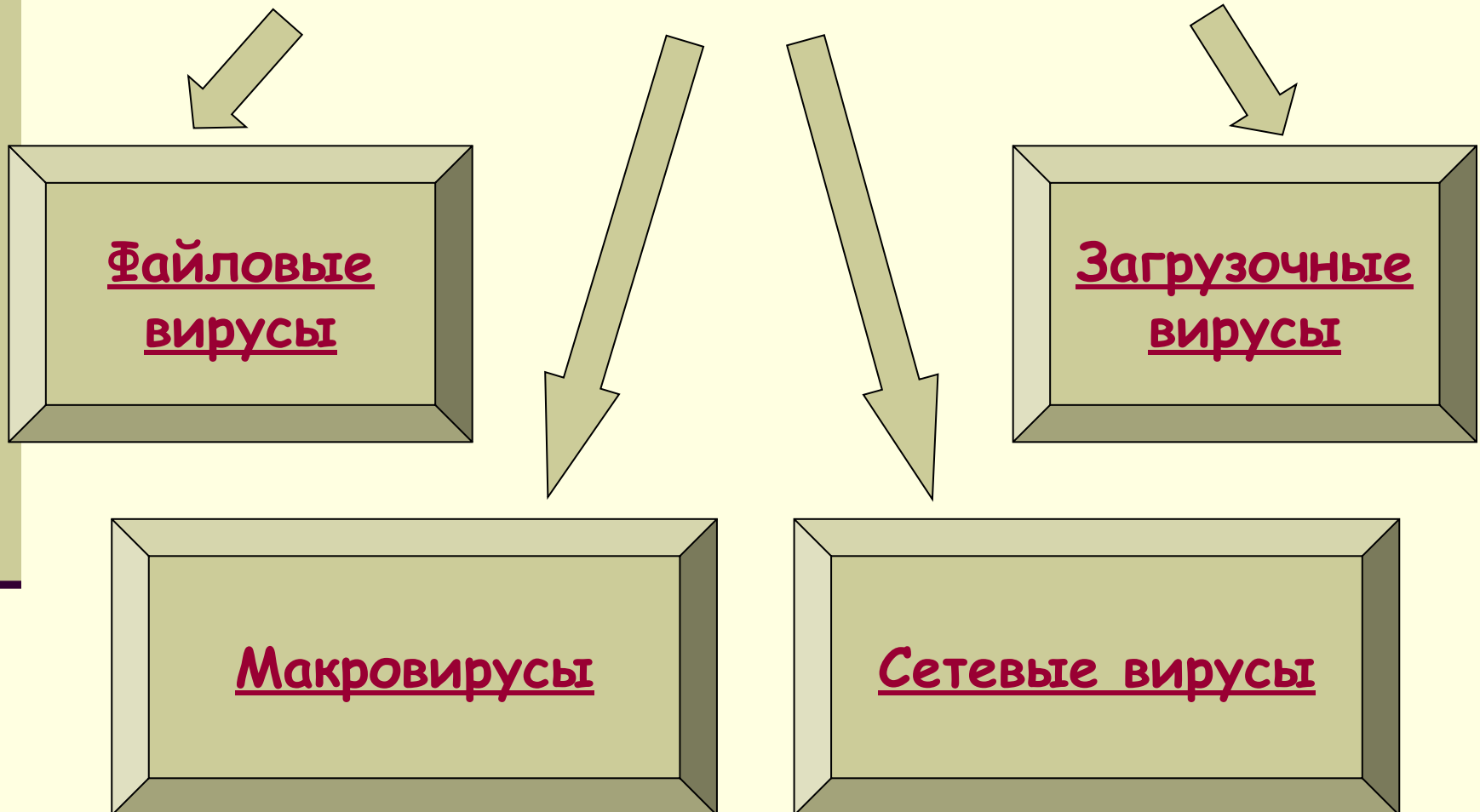
По способу заражения вирусы делятся на:



Резидентные - при заражении оставляют в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения и внедряется в них.

Нерезидентные вирусы - не заражают память компьютера и являются активными ограниченное время.

По «среде обитания» вирусы делятся на:



Загрузочные вирусы

Заражают загрузочный сектор диска. При заражении дисков загрузочные вирусы «подставляют» свой код вместо программы, получающей управление при загрузке операционной системы, и отдают управление не оригинальному коду загрузчика, а коду вируса.

В 1986 году началась первая эпидемия загрузочного вируса. Вирус-невидимка «Brain» «заражал» загрузочный сектор дискет. При попытке обнаружения зараженного загрузочного сектора вирус незаметно «подставлял» его незараженный оригинал.



Файловые вирусы

Внедряются в исполнимые файлы и активизируются при их запуске. После запуска заражённой программы вирусы находятся в оперативной памяти компьютера и могут заражать другие файлы до момента выключения компьютера или перезагрузки операционной системы.



В 1999 году началась эпидемия файлового вируса Win95.CIH, названного «Чернобыль» из-за даты активации - 26 апреля. Вирус уничтожал данные на жестком диске и стирал содержание BIOS.

Макровирусы



Заражают файлы документов, например, текстовых документов. После загрузки заражённого документа в текстовый редактор макровирус постоянно присутствует в оперативной памяти компьютера и может заражать другие документы. Угроза заражения прекращается только после закрытия текстового

В 1995 году началась эпидемия первого макро-вируса «Консерт» для текстового процессора Microsoft Word. Макро-вирус «Консерт» до сих пор широко распространен.

Сетевые вирусы

Передают по компьютерным сетям свой программный код и запускают его на компьютерах, подключенных к этой сети.

Заражение сетевым вирусом может произойти при работе с электронной почтой или при «путешествиях» по Всемирной паутине.



5 мая 2000 года началась всемирная эпидемия заражения почтовым вирусом с привлекательным названием I love you. Десятки миллионов компьютеров, подключенных к Интернет, получили почтовое сообщение, содержащее вложенный файл, который являлся вирусом.

Признаки заражения компьютера:



Вывод на экран непредусмотренных сообщений или изображений

Подача непредусмотренных звуковых сигналов

Неожиданное открытие и закрытие лотка CD/DVD дисководов

Произвольный запуск на компьютере каких-либо программ

Частые «зависания» и сбои в работе компьютера

Медленная работа компьютера при запуске программ

Исчезновение или изменение файлов и папок

Частое обращение к жесткому диску и (или) к дисководу ГМД

«Зависание» или неожиданное поведение браузера

Антивирусные программы

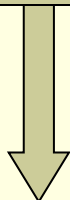
Обеспечивают комплексную защиту программ и данных на компьютере от всех типов вредоносных программ и методов их проникновения на компьютер.

Для защиты от вредоносных программ каждого типа в антивирусе предусмотрены отдельные компоненты.



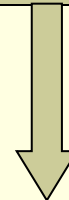
Поиск вредоносных программ

Известных



Сигнатуры
(некая постоянная
последовательность
программного кода,
специфичная для
конкретной
вредоносной
программы)

Новых



**Алгоритм
эвристического
сканирования**
(анализ
последовательности
команд
в проверяемом
объекте)

Функции защиты антивирусных программ



- Постоянная защита (антивирусный монитор);
- Защита по требованию пользователя (антивирусный сканер);

Действия при наличии признаков заражения ПК



1. Сохранить результаты работы на внешнем носителе

2. Отключить компьютер от локальной сети и Интернета, если он к ним был подключен

3. Если компьютер выдает ошибку, когда вы его включаете, то загрузиться в режиме защиты от сбоев или с диска аварийной загрузки Windows

4. Запустить антивирусную программу

Домашнее задание:

- §2.7. стр.69 – 71.

Устно отв. на вопросы: 1,2,3 стр.72

- Доклад, рисунок, листовку на тему «Компьютерные вирусы».
- *Письменно: 2.11 стр.72