Вирусы и антивирусные программы

Виды компьютерных вирусов.
Антивирусные программы.

Вообще, что такое вирус???

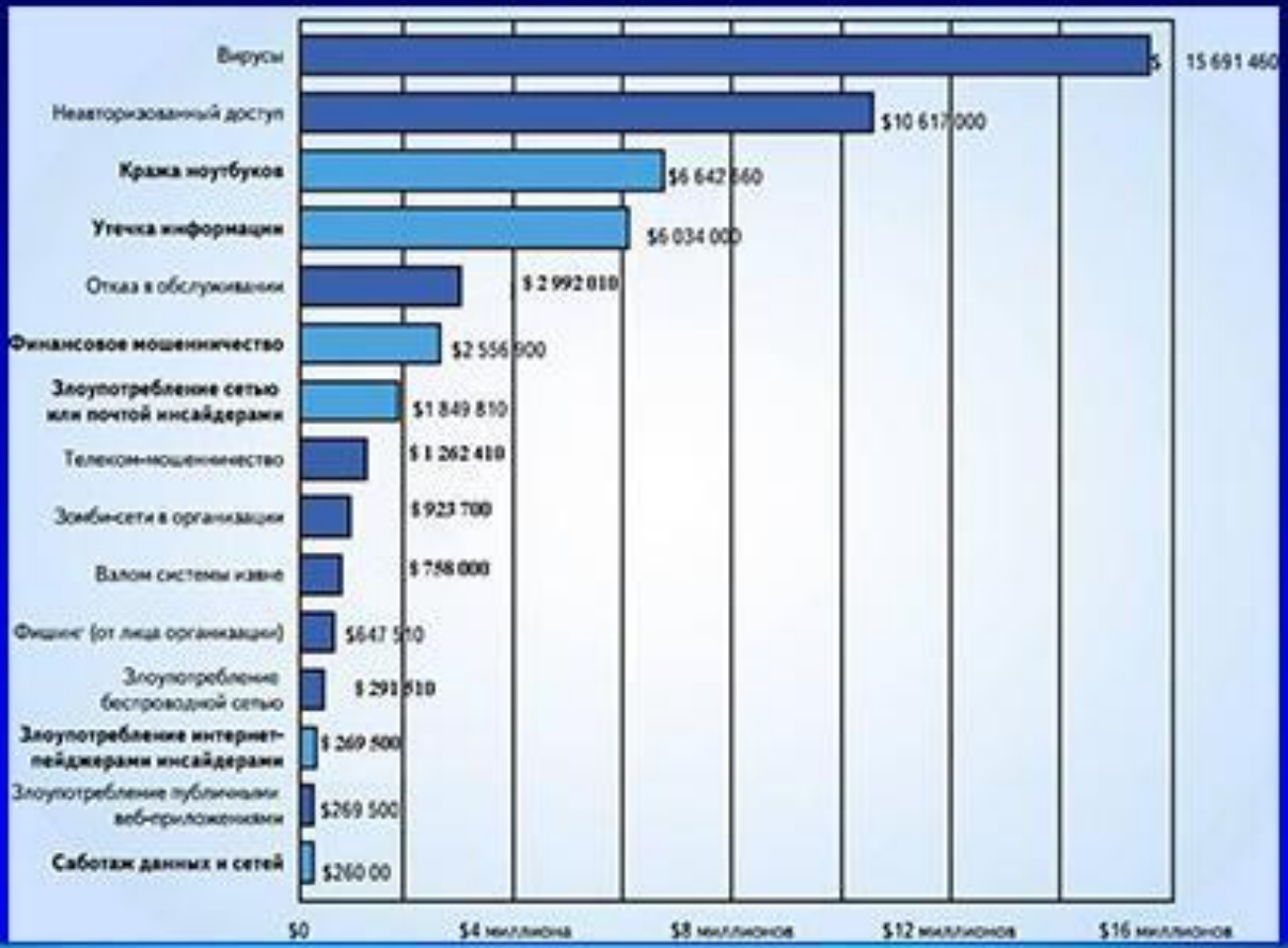
Прежде всего, вирус – это программа, которая может «размножаться» и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы.

Активизация компьютерного вируса может вызвать уничтожение программ и данных, и даже уничтожение составляющих компьютера (системного блока).

Признаки появления вирусов:

Неправильная работа нормально работающих программ
Частые зависания и сбои в работе ПК
Медленная работа ПК
Изменение размеров файлов
Исчезновение файлов и каталогов
Неожиданное увеличение количество файлов на диске
Уменьшение размеров свободной оперативной памяти
Вывод на экран неожиданных сообщений и изображений
Подача непредусмотренных звуковых сигналов
Невозможность загрузки Операционной Системы

Стоимость нанесенного вреда



Классификация вирусов

Загрузочные вирусы
Файловые вирусы
Макро-вирусы
Сетевые вирусы

Загрузочные вирусы

Заражают загрузочный сектор гибкого диска или винчестера.

При заражении дисков загрузочный вирус «заставляет» систему при ее перезапуске считать в память и отдать управление не программному коду загрузчика операционной системы, а коду вируса.

Файловые вирусы

при своем размножении тем или иным способом используют файловую систему операционной системы.

Файловые вирусы могут поражать исполняемые файлы различных типов (EXE, COM, BAT, SYS и др.).

Макро-вирусы

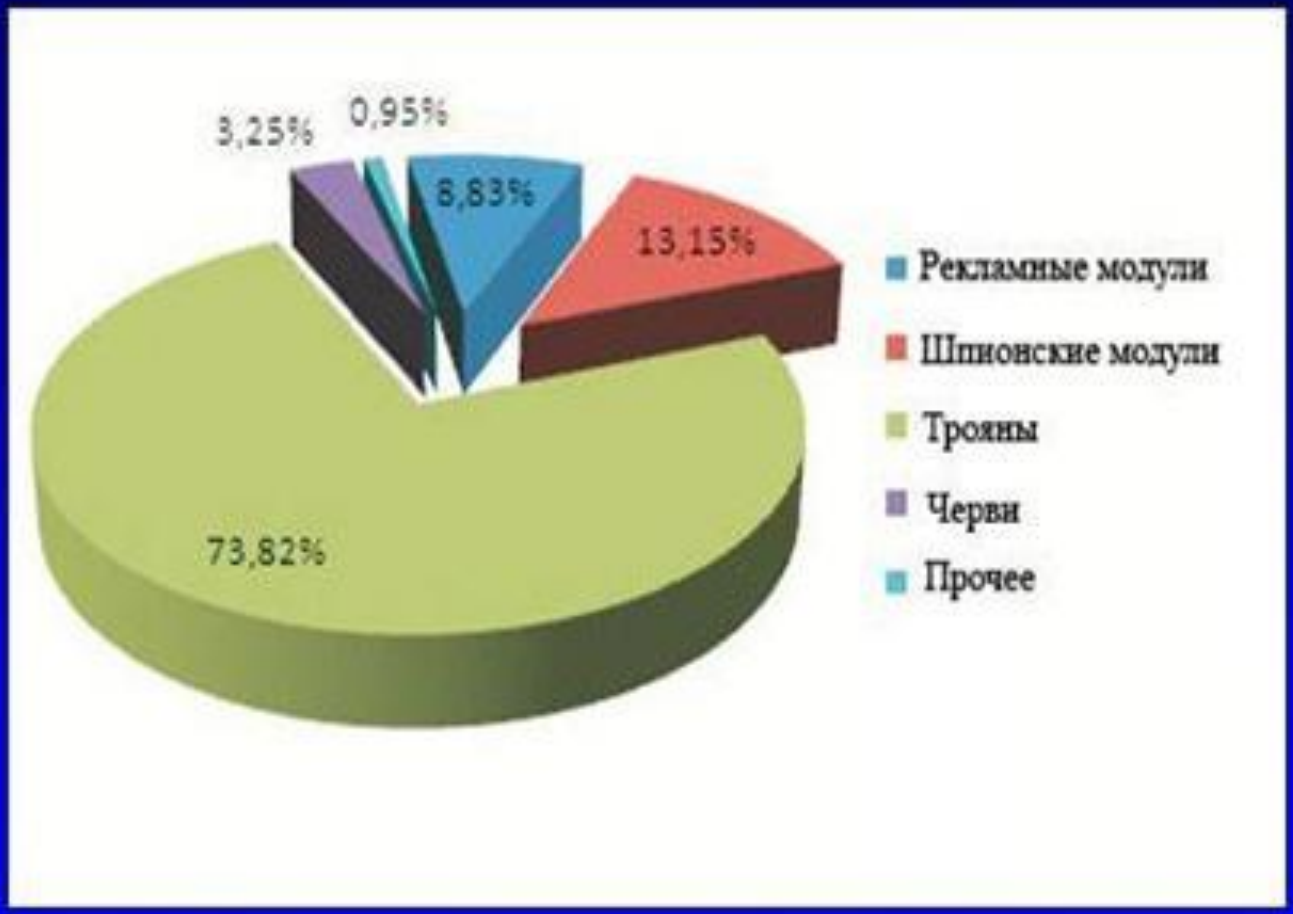
являются программами на языках, встроенных в некоторые системы обработки данных (текстовые редакторы, электронные таблицы и т.д.).
Для своего размножения такие вирусы используют возможности макро-языков и при их помощи переносят себя из одного зараженного файла (документа или таблицы) в другие.

Сетевые вирусы

для своего распространения используют протоколы и возможности локальных и глобальных компьютерных сетей.

Основным принципом работы сетевых вирусов является возможность передать и запустить свой код на удаленном компьютере.

Распространенные виды вирусов



Антивирусные программы

Для обнаружения, удаления и защиты от компьютерных вирусов разработаны специальные программы, которые позволяют обнаруживать и уничтожать вирусы. Такие программы называются антивирусными.

Их параметры...

Для быстрой и эффективной работы антивирусная программа должна отвечать некоторым параметрам:

Стабильность и надежность работы
Размеры вирусной базы программы
Многоплатформенность

Антивирусные блокировщики

Резидентные программы, которые перехватывают «вирусоопасные» ситуации и сообщают об этом пользователю. Например, «вирусоопасной» является запись в загрузочные сектора дисков, которую можно запретить с помощью программы BIOS Setup

Ревизоры

Принцип работы ревизоров основан на подсчете контрольных сумм для хранящихся на диске файлов. Эти суммы, а также некоторая другая информация (длины файлов, даты их последней модификации и др.) сохраняются в базе данных антивируса. При последующем запуске ревизоры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, то ревизоры сигнализируют о том, что файл был изменен или заражен вирусом.

Полифаги-мониторы

постоянно находятся в оперативной памяти компьютера и проверяют все файлы в реальном режиме времени.

Полифаги-сканеры производят проверку системы по команде пользователя.

Краткий обзор антивирусных программ

При выборе антивирусной программы необходимо учитывать не только процент обнаружения вирусов, но и способность обнаруживать новые вирусы, количество вирусов в антивирусной базе, частоту ее обновления, наличие дополнительных функций. Отличнейщим выбором является Антивирус Касперского.

Спасибо за внимание!

Презентация подготовлена для конкурса "Интернешка" учеником 10 класса Симоновым Александром МАОУСОШ с.Зарослое

http://interneshka.org/