Компьютерные вирусы. Антивирусные программы.

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

Компьютерные вирусы – программы, которые создают программисты специально для нанесения ущерба пользователям ПК. Их создание и распространение является преступлением.

Признаки проявления вирусов:

Неправильная работа программ;
Медленная работа компьютера;
Невозможность загрузки операционной системы;
Исчезновение файлов и каталогов;
Изменение размеров файлов;
Неожиданное увеличение количества файлов на диске;
Уменьшение размеров свободной операционной памяти;
Вывод на экран неожиданных сообщений и изображений;
Подача непредусмотренных звуковых сигналов;
Частые «зависания» и сбои в работе компьютера

Вирусы могут распространяться через:

- Исполняемые программы;
- Документы Word, Excel;
- Программное обеспечение компьютера;
- Web-страницы;
- Файлы из Интернета;
- Письма e-mail;
- Дискеты и компакт-диски.

Профилактика компьютерных вирусов:

Профилактика компьютерных вирусов:

- Иметь специальный загрузочный диск;
- Систематически проверять компьютер на наличие вирусов;
- Иметь последние версии антивирусных средств;
- Проверять все поступающие данные на наличие вирусов;
- Не использовать нелицензионные программные средства;
- Выбирать запрет на загрузку макросов при открытии документов Word и Excel;
- Выбрать высокий уровень безопасности в «Свойствах обозревателя»;
- Делать архивные копии файлов;

- Добавить в файл автозагрузки антивирусную программу сторож;

- Не открывать вложения электронного письма, если отправитель неизвестен.

Антивирусные программы — программы, которые предотвращают заражение компьютерным вирусом и ликвидируют последствия заражения.

Существуют несколько типов антивирусных программ, различающихся выполняемыми функциями.

1-Полифаги

2-Ревизоры

3-Блокировщики

Ревизоры

Принцип работы ревизоров (например, ADinf) основан на подсчете контрольных сумм для присутствующих на диске файлов. Эти контрольные суммы затем сохраняются в базе данных антивируса, как и некоторая другая информация: длины файлов, даты их последней модификации и пр.

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.

Недостаток ревизоров состоит в том, что они не могут обнаружить вирус в новых файлах (на дискетах, при распаковке файлов из архива, в электронной почте), поскольку в их базах данных отсутствует информация об этих файлах.

Блокировщики

- Антивирусные блокировщики - это программы, перехватывающие "вирусоопасные" ситуации и сообщающие об этом пользователю. К таким ситуациям относится, например, запись в загрузочный сектор диска. Эта запись происходит при установке на компьютер новой операционной системы или при заражении загрузочным вирусом.
- Наибольшее распространение получили антивирусные блокировщики в BIOS компьютера. С помощью программы BIOS Setup можно провести настройку BIOS таким образом, что будет запрещена (заблокирована) любая запись в загрузочный сектор диска и компьютер будет защищен от заражения загрузочными вирусами.
- *К достоинствам блокировщиков* относится их способность обнаруживать и останавливать вирус на самой ранней стадии его размножения.

Полифаги

- Самыми популярными и эффективными антивирусными программами являются антивирусные программы полифаги (например, Kaspersky Anti-Virus, Dr.Web).

  Для поиска известных вирусов используются так называемые *маски*.

  Маской вируса является некоторая постоянная последовательность программного кода, специфичная для этого конкретного вируса.

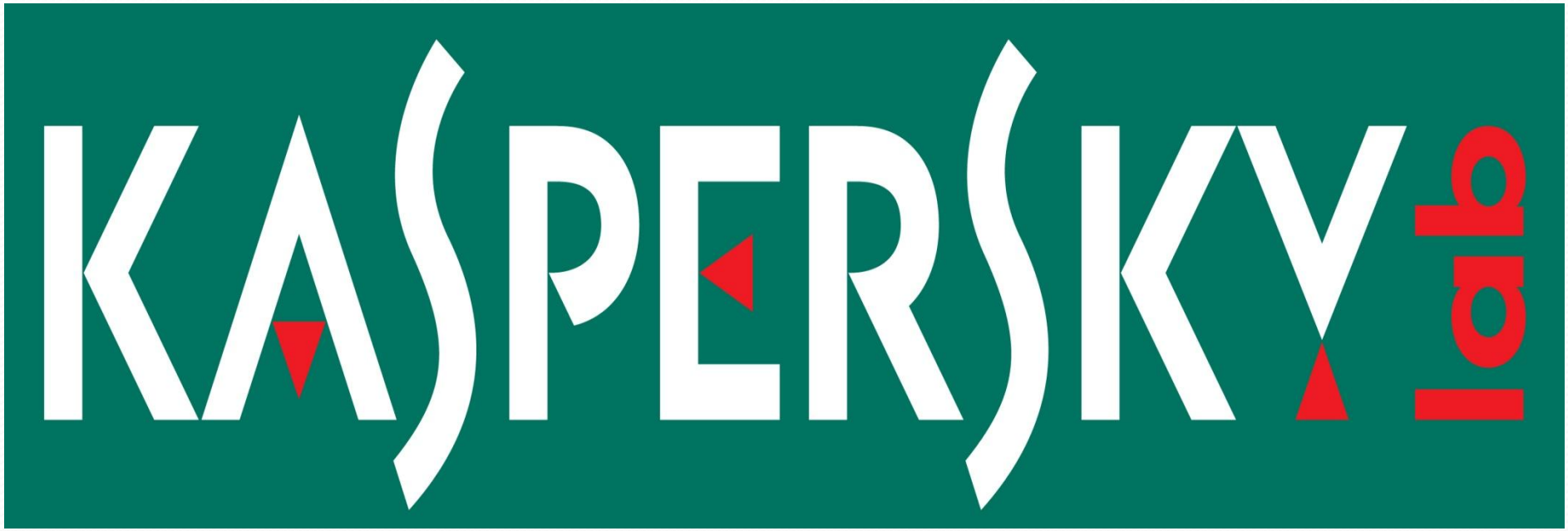
  Если антивирусная программа обнаруживает такую последовательность в каком-либо файле, то файл считается зараженным вирусом и подлежит лечению.

  Для поиска новых вирусов используются алгоритмы "эвристического сканирования", то есть анализ последовательности команд в проверяемом объекте. Если "подозрительная" последовательность команд обнаруживается, то полифаг выдает сообщение о возможном заражении объекта.

- Полифаги могут обеспечивать проверку файлов в процессе их загрузки в оперативную память. Такие программы называются *антивирусными мониторами*.

- К *достоинствам полифагов* относится их универсальность.

К *недостаткам* можно отнести большие размеры используемых ими антивирусных баз данных, которые должны содержать информацию о максимально возможном количестве вирусов, что, в свою очередь, приводит к относительно небольшой скорости поиска вирусов.


KASPERSKY
lab