Совместный проект

ПОЛИТЕХ | KASPERSKY lab

Лекция:
«Как работает компьютерный иммунитет?»

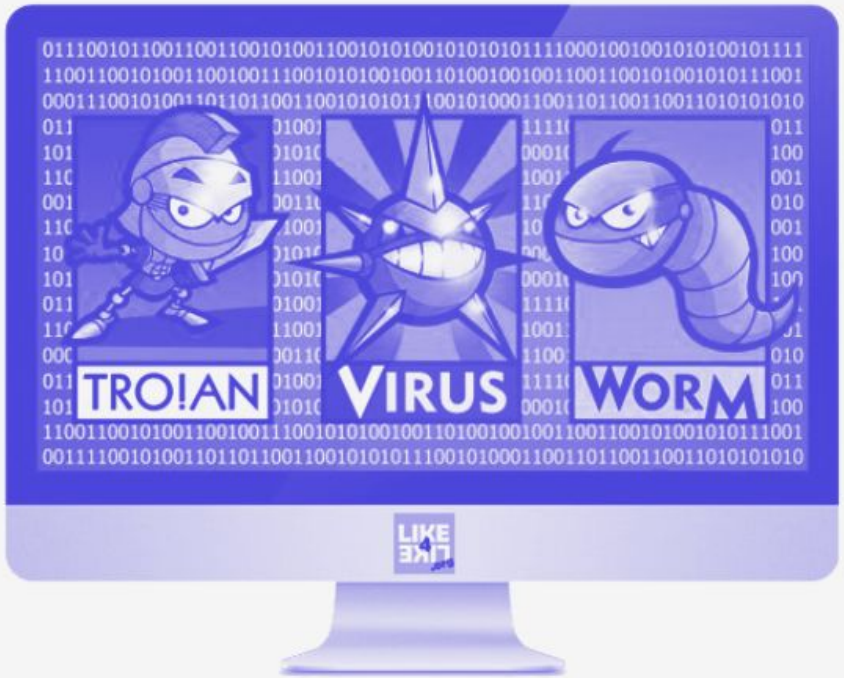
2016

Где используются компьютеры?

Вредоносные программы

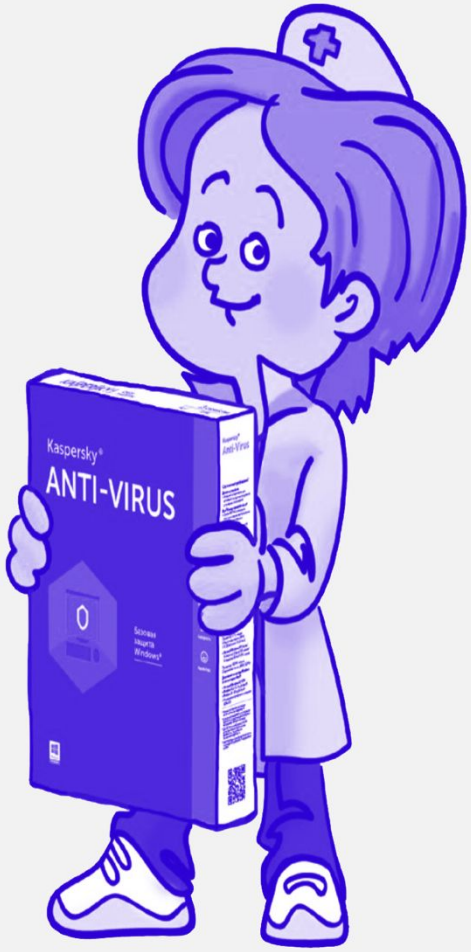
Это специально созданные программы для разрушения и кражи информации.

- Влияют на выполнение компьютерных операций;
- Искажают или удаляют данные;
- Замедляют выполнение компьютерных операций;
- Вызывают проблемы в работе компьютера, вплоть до его отключения.



Что такое антивирус?

Антивирус — любая программа для обнаружения компьютерных вирусов, и восстановления зараженных такими программами файлов, а также для профилактики — предотвращения заражения компьютера вредоносными программами.



Что должен уметь антивирус?

- Предупреждать заражения.
- Если компьютер все-таки заразился, то находить вредоносные программы.
- Лечить зараженные файлы.
- Если файл не удается вылечить, то удалить его.
- Постоянно обновляться.
- Не давать вредоносной программе себя отключить.

Как работает антивирус?

- «Поиск по отпечаткам пальцев».
- Метод анализа поведения.

Поиск по отпечаткам пальцев

- Антивирус, просматривая файл, обращается к словарю с известными вирусами.
- Каждый файл имеет свой Уникальный отпечаток, который называется хешем.

Плюсы и минусы метода поиска «по отпечаткам»

Плюсы

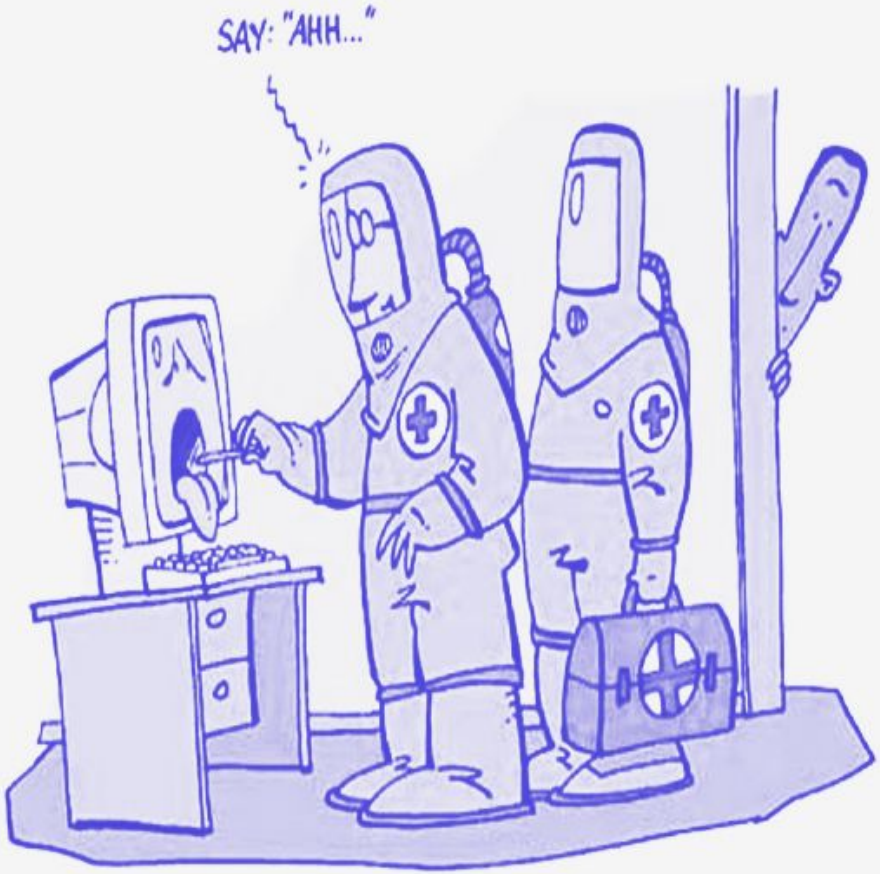
- Маленькое количество ложных срабатываний
- Высокая точность обнаружения вредоносных файлов

Минусы

- Беззащитность перед новыми вирусами
- Беззащитность перед «мутированием» и «запутыванием» кода
- Необходимость постоянного обновления «словаря»

Метод анализа поведения

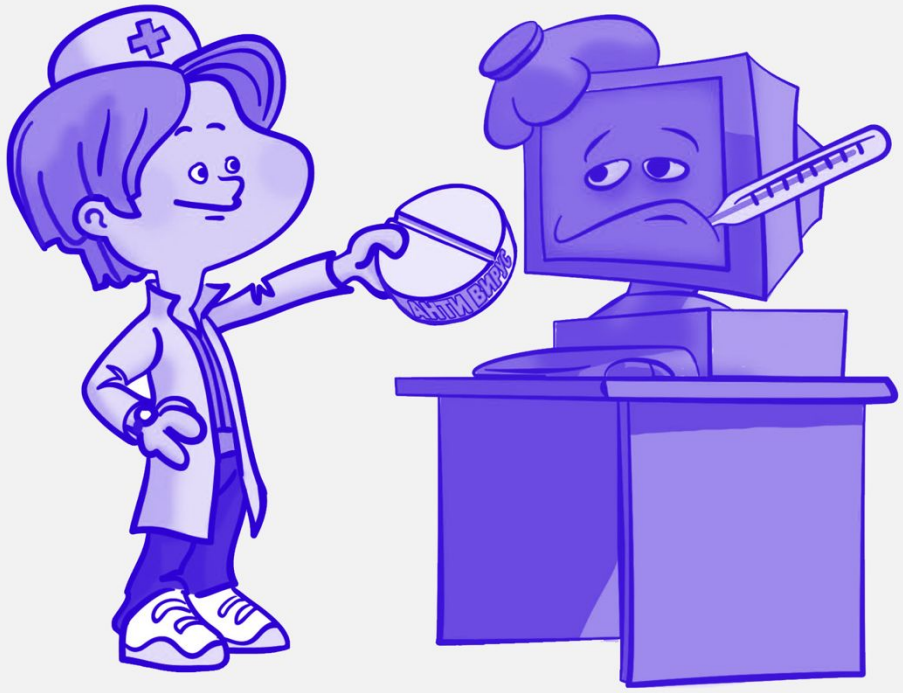
Эвристик – это код, который проверяет файл на некоторые характерные признаки заражения.



Эвристик — компьютерный врач

Что может делать?

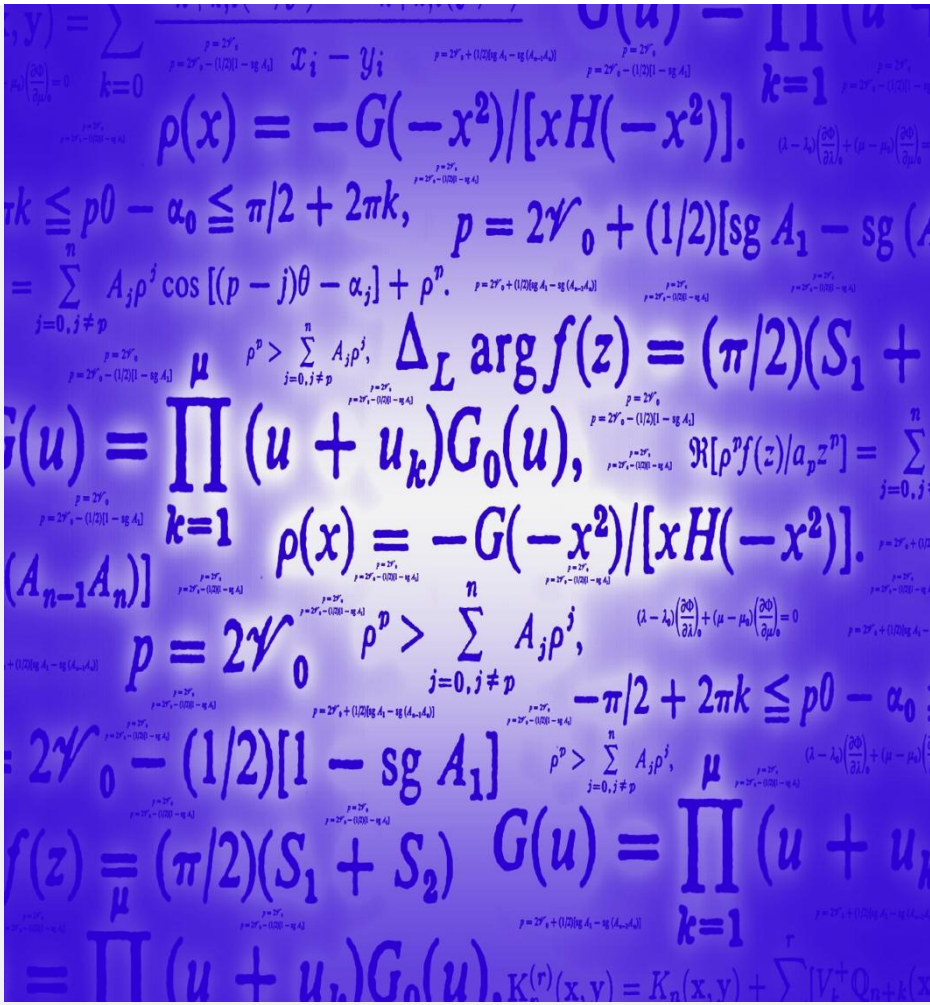
- Работать с программным кодом.
- Пошагово выполнять инструкций кода.
- Запускать программы в «песочнице».
- Собирать статистику по Нескольким программам.
- Искать скрытых болезней системы.



Является ли антивирус абсолютно надежным?

Математики доказали, что не существует алгоритма, который позволит сразу определить является ли программа вредоносной или нет.

Ни один из антивирусов не дает стопроцентной гарантии



Выводы

- Кроме вредоносных программ, есть и хорошие программы, которые называются антивирусами.
- Антивирус может предотвращать заражение, находить и лечить зараженные файлы.
- Ни один антивирус не дает стопроцентной защиты.