

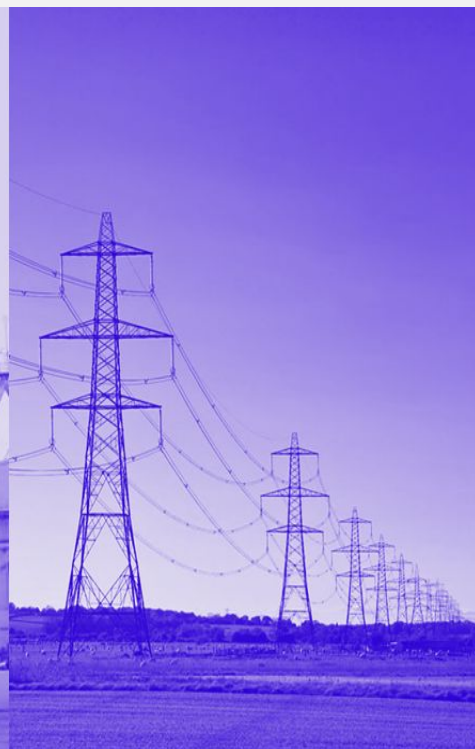
Совместный проект

1



Лекция:
«Как работает компьютерный
иммунитет?»

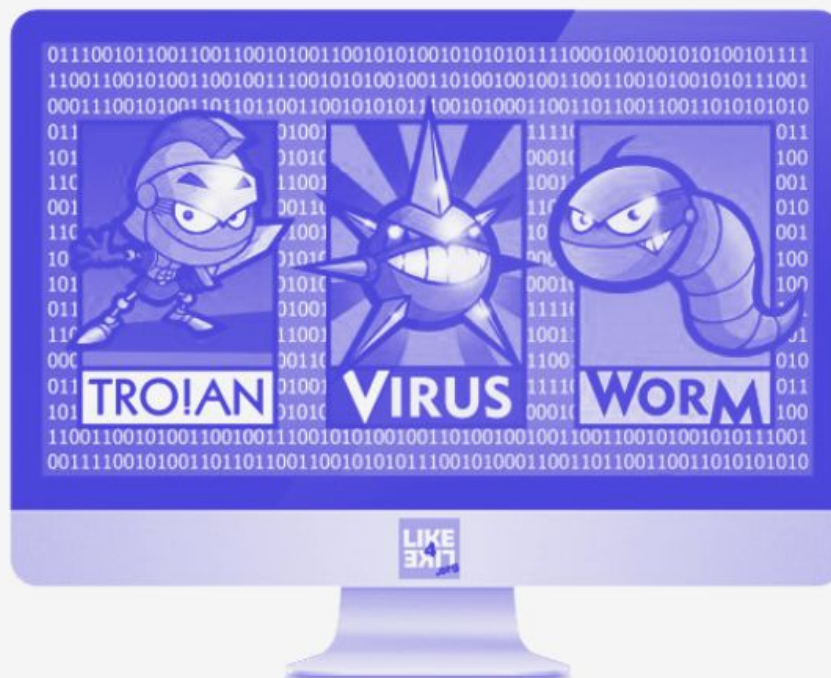
Где используются компьютеры?



Вредоносные программы

Это специально созданные программы для разрушения и кражи информации.

- п Влияют на выполнение компьютерных операций;
- п Искажают или удаляют данные;
- п Замедляют выполнение компьютерных операций;
- п 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 удастся вылечить, то удалить его.
- ▯ Постоянно обновляться.
- ▯ Не давать вредоносной программе себя отключить.



Как работает антивирус?

п «Поиск по отпечаткам пальцев».

п Метод анализа поведения.

Поиск по отпечаткам пальцев

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



Плюсы и минусы метода поиска «по отпечаткам»

Плюсы

- п Маленькое количество ложных срабатываний
- п Высокая точность обнаружения вредоносных файлов

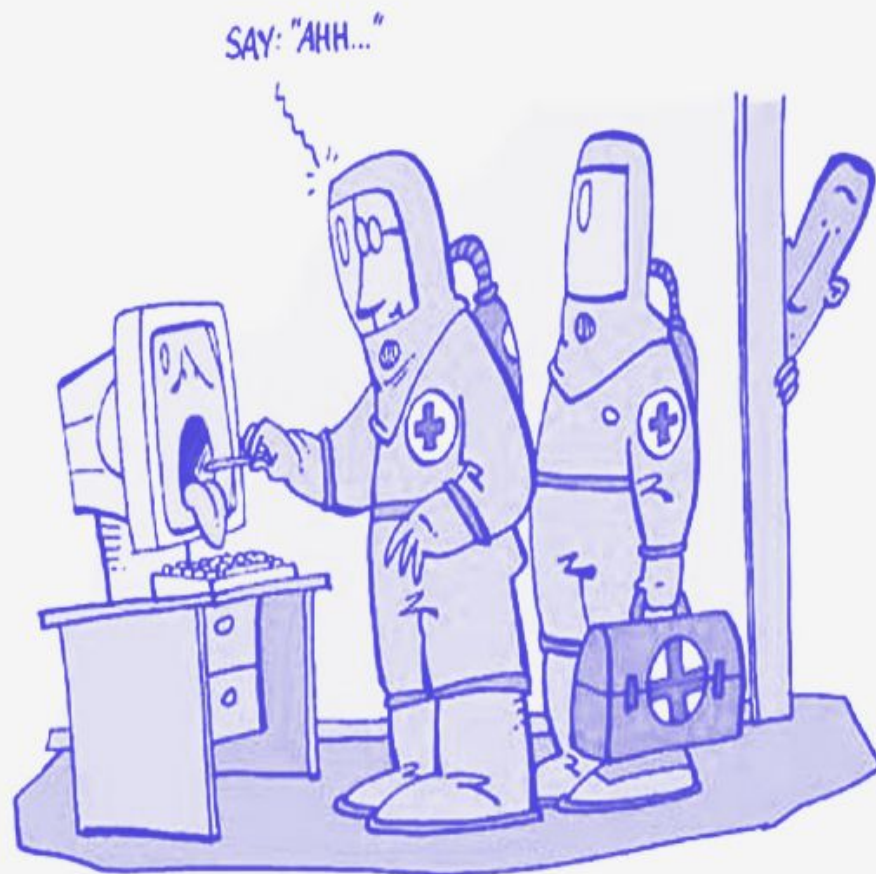
Минусы

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



Метод анализа поведения

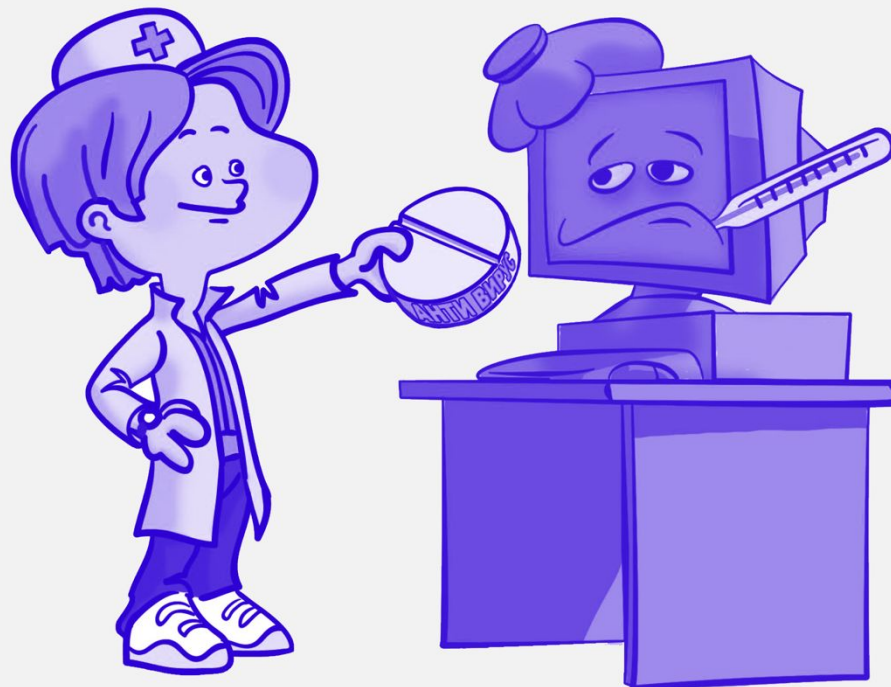
Эвристик – это код, который проверяет файл на некоторые характерные признаки заражения.



Эвристик — компьютерный врач

Что может делать?

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



Является ли антивирус абсолютно надежным?

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.

