Исследовательский проект "Компьютерные вирусы: виды, удаление и способы защиты от них".

Выполнил учащиеся 11 класса
Шведчиков Иван Александрович
Руководитель: Кашарная Людмила Николаевна

Глинищево 2022

Актуальность работы

Пользователей ПК становиться все больше и они подвергнуты к заражению вирусов на свой компьютер. Многие пользователи уже имеют зараженные файлы. Поэтому работа, направленная на развитие компьютерной безопасности, очень важна и актуальна.

Цель проекта

Рассмотреть особенности различных компьютерных вирусов, способы их удаления, защита от них, и получение знаний для дальнейшего пользования.

Задачи проекта:

- Узнать, какие вирусы существуют, понять их функции.
- Выяснить как бороться с вирусами.
- Поинтересоваться о популярных антивирусах.

Методы исследования: работа с интернет-ресурсами и анализ.

Гипотеза: существуют антивирусные программы, которые способны выявить вирусы, хранящиеся на компьютере

Раздел компьютерные вирусы

Компьютерный вирус — вид вредоносных программ способных внедряться в код других программ, системные области памяти, загрузочные секторы и распространять свои копии по разнообразным каналам связи.

Черви заражают уже множество файлов вашем компьютере, например все exe файлы, системные файлы, загрузочные сектора и тд.

Вирусы бывают:

- Файловые
- Загрузочные
- Макровирусы

Типы компьютерных вирусов:

- Троянские программы
- Шпионы
- Вымогатели
- Руткиты
- Botnet
- Кейлогеры

Пути заражения компьютерных вирусов:

- Уязвимость ОС
- Браузеры
- Глупость пользователя
- Сменные носители

Удаление вирусов

Для обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов антивирусных программ:

1. **Программы-детекторы**
2. **Программы-доктора или фаги**
3. **Программы-ревизоры (инспектора)**
4. **Программы-фильтры (мониторы)**
5. **Сканер**

Меры предосторожности:

1. **Не работать под привилегированными учётными записями без крайней необходимости.**
2. **Не запускать незнакомые программы из сомнительных источников.**
3. **Отключать потенциально опасный функционал системы.**
4. **Не заходить на подозрительные сайты, обращать внимание на адрес в адресной строке обозревателя.**
5. **Пользоваться только доверенными дистрибутивами.**
6. **Постоянно делать резервные копии важных данных и иметь образ системы со всеми настройками для быстрого развёртывания.**
7. **Выполнять регулярные обновления часто используемых программ, особенно тех, которые обеспечивают безопасность системы.**
8. **Выполняете ежедневное сканирование.**

Обзор некоторых ативирусных программ