

Муниципальное бюджетное общеобразовательное учреждение, средняя школа №9.
Нижегородская область, г. о. г. Выкса.
Школьная научно-практическая конференция.
Отделение: 9.

Информационная безопасность

Работу выполнил:
ученик 10 „Б” класса
Чередниченко Никита
Вячеславович

Научный руководитель:
учитель МБОУ СШ №9
Михайлова Татьяна
Аркадьевна.

Выкса
2020-2021

Цель проекта: ознакомление обучающихся со способами безопасного использования информационных ресурсов.

Задачи:

1. Изучить признаки заражения компьютерных систем.
2. Изучить антивирусное ПО.
3. Изучить и проанализировать вирусные программы.
4. Описать методы защиты от вирусов.
5. Рекомендовать пользователям способы по безопасному использованию информации.

Содержание

- 1.Что такое Информационная безопасность.
- 2.Кибератаки:
 - 2.1.Что такое кибератака.
 - 2.2.Виды кибератак.
 - 2.3.Киберпреступления.
- 3.Вирусы:
 - 3.1.История Вируса.
 - 3.2.Виды вирусов.
- 4.Сетевые черви.
 - 4.1.Что такое сетевой червь.
 - 4.2.Виды сетевых червей.
- 5.Антивирусы.
 - 5.1.История антивируса.
 - 5.2.Виды антивирусов.
- 6.Вредоносные программы.
 - 6.1.Признаки заражения.
 - 6.2.Методы защиты от вирусов.
- 7.Заключение.
- 8.Литература.

Что такое информационная безопасность.

Информационная безопасность (ИБ) – это состояние информационной системы, при котором она наименее восприимчива к вмешательству и нанесению ущерба со стороны третьих лиц.



Что такое кибератака.

Простыми словами **Кибератакой** является массовый взлом компьютерных сетей, либо массовое заражение компьютеров вирусами. Примером кибератаки можно считать повальное заражение компьютеров «вирусом-вымогателем», произошедшее 12 мая 2017 года. От этой атаки пострадали компьютеры в России, Великобритании, Украине и многих других странах.



Виды кибератак.

- Удаленное проникновение (remote penetration);
- Локальное проникновение (local penetration);
- Сетевые сканеры (network scanners);
- Сканеры уязвимостей (vulnerability scanners);
- Взломщики паролей (password crackers);
- Анализаторы протоколов (sniffers).



Киберпреступления.

- В России в 2021 году сумма причиненного ущерба только от дистанционных (телефонных) мошенничеств составила 45 миллиардов рублей, а общий ущерб от киберпреступности оценивается в пределах 90 миллиардов рублей. Для сравнения, в 2020 году ущерб от киберпреступлений оценивался в районе 70 миллиардов рублей.

Хакерские группировки:

- Darkside
- Bronze Union
- Calypse
- Chamel Gang
- Cobalt
- Cozyduke
- FancyBear

И др.

История вируса

Термин вирус появился в 1945 году - Вице-адмирал ВМФ США Грейс Муррей Хоппер столкнулась со сбоем электронно-счетных машин, в них случайно залетел мотылёк. Адмирал назвала эту проблему жуком (bug).

Первым действующим вирусом является игра Darwin, изобретённая в 1961 году компанией Bell Telephone Laboratories. В этой игре программы загружались в оперативную память компьютера и сражались за инф. ресурсы.



Виды вирусов

- Троянская программа (Троян);
- Программы шпионы;
- Программа-блокировщик (баннер);
- Загрузочные вирусы;
- Эксплойт;
- Фарминг;
- Руткит;
- Программный вирус.



Что такое сетевой червь.

- **Сетевой червь** — разновидность вредоносной программы, самостоятельно распространяющейся через локальные и глобальные (Интернет) компьютерные сети.



Виды сетевых червей.

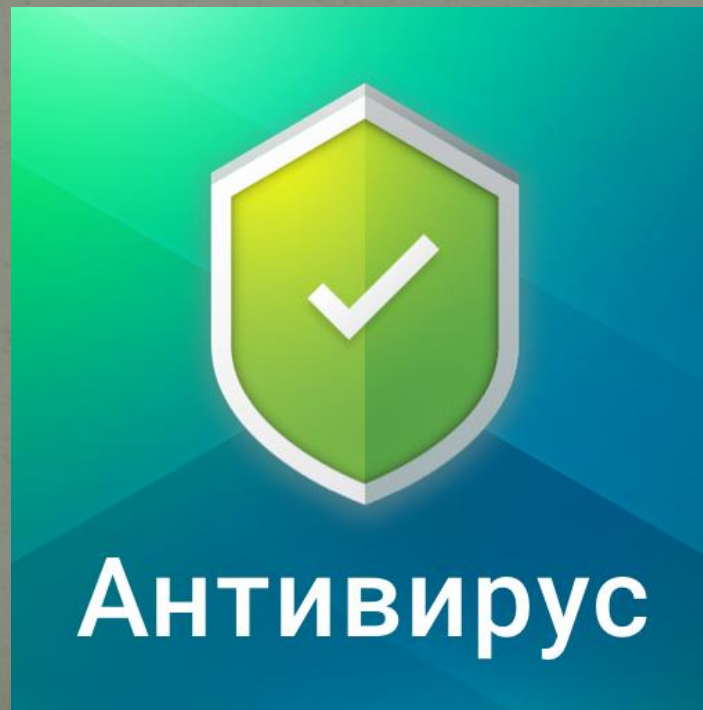
- Почтовый червь;
- Сетевой червь;
- Червь чата;
- Червь файлообменника;
- Червь мессенджера;
- Другие черви.



История Антивируса

Первый антивирус DRPROTECT был создан Джи Вонг в 1985 году. Он представляли собой набор из нескольких десятков сигнатур.

Чтобы подстроиться под тенденцию «индустрии вирусов», в 1992 году появилась программа MtE — генератор полиморфного (постоянно меняющегося) кода и другие системы защиты.



Виды антивирусов

Антивирусные программы разделяются по признаку размещения в оперативной памяти:

- Резидентные;
- Нерезидентные.
- По виду (способу) защиты от вирусов различают:
- Программы-детекторы;
- Программы-доктора;
- Программы-вакцины;
- Программы-ревизоры;
- Программы-мониторы;
- Программы-фильтры (сторожа).



Признаки заражения:

Самые распространённые:

- блокировка доступа к официальным сайтам антивирусных компаний;
- появление всплывающих окон или системных сообщений с непривычным содержанием;
- Перезапуск, отключение компьютера без причины;
- снижение производительности компьютера;
- быстрая утечка памяти на жёстком диске.



Методы защиты от вирусов.

Методы, основанные на *анализе содержимого файлов* :

- Метод сканирования сигнатур вирусов;
- Метод проверка целостности;
- Метод сканирования подозрительных команд.

Методы регламентации порядка работы с файлами и программами:

- Факт изменения данных;
- Метод отслеживания поведения программ.



Заключение

- В интернете полно мошенников, готовых украсть личную информацию. Что бы её защитить от нез. лиц следует:
 - Придумывать сложные пароли и часто их менять
 - Постоянно обновлять своё устройство
 - Сканировать каждый подозрительный файл перед использованием
 - Проводить диагностику компьютера на наличие вирусов не менее чем раз в неделю

Литература

- <https://obuchonok.ru/node/6208>
- <https://plusworld.ru/daily/cat-security-and-id/v-2021-godu-ushherb-ot-kiberprestuplenij-v-rossii-sostavil-90-milliardov-rublej/>
- <https://www.ptsecurity.com/ru-ru/research/hacker-groups/>
- Видео-сюжет -
<https://cloud.mail.ru/stock/4W6BsUfPs5j1XjoiCWycbapH>