СПБ ГБПОУ КИТ, 103 ГРУППА

Презентация на тему:

“Вирусы и антивирусные программы”

Выполнил: Емельянцев Никита Игоревич
Преподаватель: Венедиктова Ольга Николаевна

К каким последствиям может привести заражение компьютерными вирусами?

1. Потеря важных данных (личная, финансовая, конфиденциальная).
2. Нарушение работоспособности системы.
3. Повреждение системных файлов.

Какие типы компьютерных вирусов существуют, чем они отличаются друг от друга и какова должна быть профилактика заражения?

Типы вирусов:

1. Рекламные
2. Блокировщики
3. Трояны
4. Маскировщики
5. Черви
6. Шпионы

Профилактика заражения:

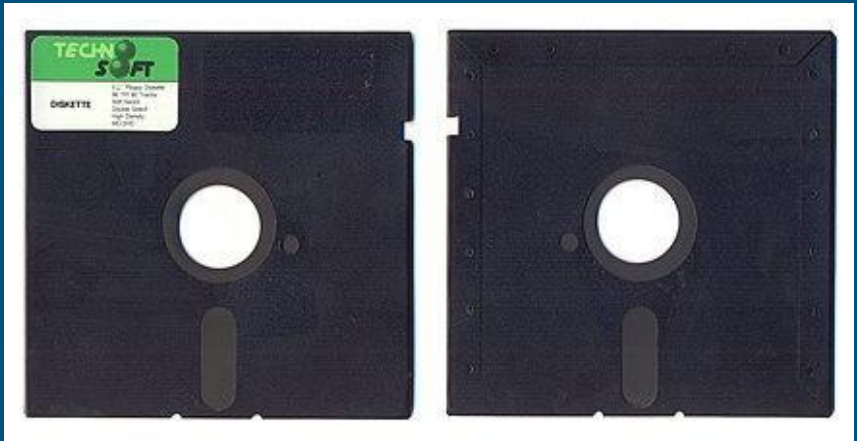
1. Установка антивируса.
2. Не скачивать подозрительные файлы.
3. Не заходить на непроверенные сайты в интернете.

Правила обращения с дискетами.

Запрещается:

1. Гнуть дискеты, вскрывать, нагревать.

   Также дискеты нужно беречь от влаги, вставлять в дисковод аккуратно и ровно, а хранить в специальных контейнерах.



Основные виды антивирусных программ.

1. Детекторы
2. Доктора
3. Ревизоры
4. Фильтры
5. Вакцины

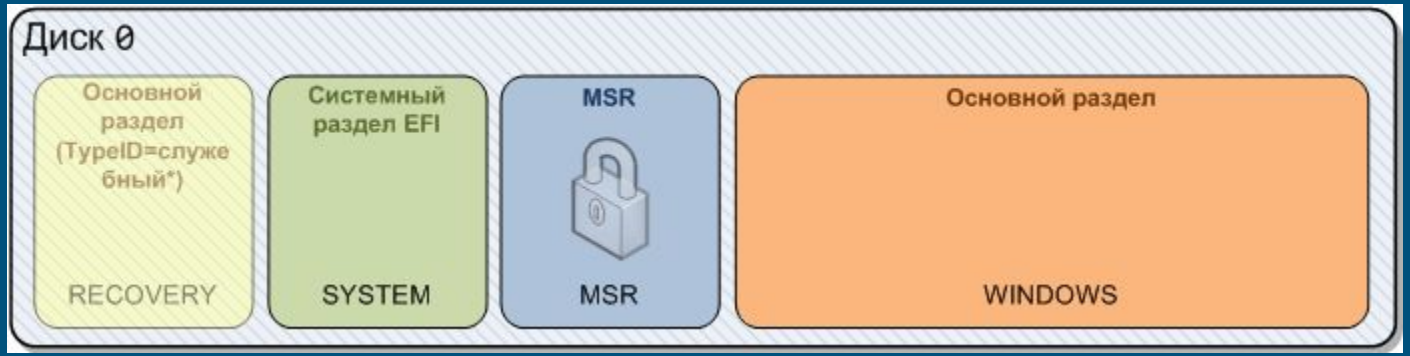
Как защитить компьютер от интернет-вирусов?

Основные моменты:

1. Установка антивируса
2. Не открывать подозрительные письма электронной почты
3. Быть аккуратным с интернет серфингом
4. Использование брандмауэра
5. Регулярное обновление системы

Почему даже чистая отформатированная дискета может стать источником заражения вирусом?

Некоторые вирусы могут лежать в системных разделах дискеты, поэтому даже после полного форматирования вредоносный файл все равно остается. Все это возможно благодаря опции “скрытый атрибут”.



Список известных вирусов (начиная от самых опасных, 2020 год)

1. Программа-вымогатель Clop - шифрует ваши файлы и требует заплатить выкуп хакерам за разблокировку.
2. Подставные обновления Windows - обманом устанавливаются пользователем, на самом деле являются программами-вымогателями.
3. Zeus Gameover - маскируется под обычную программу и получает доступ к вашим банковским данным и ворует ваши средства.
4. RaaS - программы-вымогатели как услуга (Ransomware as a Service) — это растущая индустрия в подпольных хакерских кругах. Любой человек может заплатить профессиональному хакеру или команде хакеров за организацию атаки.
5. Fleeceware - это вредоносные программы, которые снимают со счетов пользователей приложений крупные суммы даже после удаления данных приложений.

Источники:

Интернет-ресурсы:

1. http://www.e-biblio.ru/book/bib/01_informatika/infteh/book/docs/piece231.htm - типизация вирусов
2. https://ru.safetydetectives.com/blog/novye-virusy-i-vredonosnye-programmy/ - самые опасные вирусы
3. https://support.microsoft.com/ru-ru/windows/%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D0%B0-%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%B0-%D0%BE%D1%82-%D0%B2%D0%B8%D1%80%D1%83%D1%81%D0%BE%D0%B2-b2025ed1-02d5-1e87-ba5f-71999008e026 - защита компьютера от вирусов.

Спасибо за внимание!