Информационная безопасность

Компьютерный вирус — вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ,а также распространять свои копии по разнообразным каналам связи

Виды вирусов

- Анти-антивирусный вирус
- Вирусная программа-червь
- MBR(Master Boot Record)
- Вирусы-спутники
- Полиморфные вирусы
- Скрипт-вирусы
- Спелс-вирусы
- Шифрованные вирусы

Вирус является программой, поэтому не содержащие программ объекты вирус может только испортить, но не заразить

Признаки заражения

- удаление данных;
- блокирование данных;
- изменение данных;
- копирование данных;
- замедление работы компьютеров и компьютерных сетей.

Что еще представляет угрозу вашему ПК?

Фишинг— вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям.

Троянские программы — это вредоносные программы, выполняющие несанкционированные пользователем действия.

Спам — это ненужные адресату электронные послания, рекламные письма и т. п., рассылаемые отдельными фирмами по Интернету или электронной почте, массовая рассылка коммерческой и иной рекламы или подобных коммерческих видов сообщений.

Макровирусы - это вирусы написанные на макроязыках. Для своего размножения такие вирусы используют возможности макроязыков, они переносятся от одного заражённого файла к другому.

Как реагировать на СПАМ?

Никакой реакции - это самая лучшая реакция на спам.

Как же защитить свой компьютер от вредоносного ПО?

Во-первых, вам обязательно потребуется антивирус.

Что такое антивирус?

Антивирусная программа (антивирус) — специализированная программа для обнаружения компьютерных вирусов, а также нежелательных программ вообще и восстановления заражённых такими программами файлов, а также для профилактики — предотвращения заражения файлов или операционной системы вредоносным кодом.

Самые известные антивирусные программы:
Kaspersky;
Avast;
Nod 32;
Dr.Web.

Как выбрать антивирус?

При выборе антивирусной программы важно учитывать её особенности, с которыми не менее важно ознакомиться. Ведь у каждого антивируса есть свои минусы и плюсы.

Как уменьшить ущерб, который могут нанести вредоносные программы?

Главный вред, который могут нанести вредоносные программы, - это потеря данных или паролей к закрытой информации.

Чтобы уменьшить возможный ущерб, рекомендуется регулярно делать резервные копии важных данных.
Если вы работаете в сети, желательно включать антивирус-монитор и брандмауэр .
Все новые файлы нужно проверять с помощью антивируса-сканера.
Не рекомендуется открывать подозрительные сообщения электронной почты , полученные с неизвестных адресов.
Опасно также переходить по ссылкам в тексте писем , с большой вероятностью они ведут на сайты , зараженные вирусами.

Что делать есть компьютер уже заражен?

Если компьютер заражён, нужно отключить его от компьютерной сети и запустить антивирус-сканер. Очень часто это позволяет удалить вирус , если его сигнатура есть в базе данных.
В другом случае можно попытаться найти в интернете бесплатную утилиту для лечения с новыми базами сигнатур .

В особо тяжелых случаях для уничтожения вирусов приходится полностью форматировать жесткий диск компьютера , при этом все данные теряются.

А так же не забывайте ВОВРЕМЯ обновлять базы сигнатур антивируса.

В заключении...

Мы создали эту памятку с целью предупреждения возможных угроз при использовании интернета.

Для безопасного использования сети интернет вам стоит соблюдать все перечисленные рекомендации и меры предосторожности. Ведь безопасность ваших данных напрямую связана с безопасностью вашего компьютера.