

Основы работы на ЭВМ

Занятие 4: вредоносные программы;
угрозы, возникающие в Интернете

Фенстер Александр Геннадьевич
<http://9131.fenster.name>

«Вредоносные программы»

- Компьютерные вирусы
- Троянские программы
- Программы-шпионы

Сейчас более подробно рассмотрим
каждый из трёх видов

Компьютерные вирусы

- Компьютерный вирус – программа, способная самостоятельно размножаться
 - внедрение в другие программы
 - самостоятельные программы
 - Зачастую (но не всегда) выполняют разрушающие действия с данными, хранящимися на компьютере
 - Первые вирусы: 1980е годы
-

Троянские программы



- Программа, запускающаяся на компьютере пользователя и выполняющая нежелательные действия:
 - сбор данных и отправка их третьим лицам
 - удаление или порча данных
 - использование ресурсов компьютера
 - нарушение защиты компьютера
- Сама не размножается, т. е. не является компьютерным вирусом в строгом смысле

Программы-шпионы

- Программа, скрытным образом устанавливаемая на компьютер для отслеживания действий пользователя
 - какие сайты посещает
 - запись нажатий на клавиатуру (пароли, данные кредитных карт и т. п.)
 - показ пользователю нежелательной рекламы в процессе работы
-

Распространение вредоносных программ

- Через устройства переноса данных:
 - дискеты (раньше), флэшки
 - 1. вредоносная программа помещает на флэшку себя и файл автозапуска autorun.inf.
 - 2. Когда флэшка вставляется в компьютер с включённым автозапуском, вредоносная программа запускается
-

Распространение вредоносных программ

- По электронной почте
 - вложения (аттачи) могут содержать вредоносные программы
 - часто они маскируются под картинки или скринсейверы, например:
 - photo.jpg.exe
 - something.zip.scr
 - пользователь щёлкает по вложению, программа запускается
-

Распространение вредоносных программ

- Через «дыры» в безопасности операционных систем
 - программы практически всегда содержат ошибки
 - может оказаться, что произвольный пользователь имеет возможность запустить произвольную программу на чужом компьютере
 - не все вовремя ставят обновления для операционной системы!
-

Причиняемый вред

1. Возможная потеря данных
 2. Разглашение важной информации:
 - пароли
 - номера банковских карт
 3. Большое количество рекламы
 4. Медленная работа компьютера из-за кучи запущенного «мусора»
 5. Рассылка спама с вашего компьютера
-

Как бороться?

- Три основных пункта:
 1. Антивирусная программа
 2. Файрвол
 3. Не запускать программы, полученные неизвестно откуда!
-

Антивирусные программы

- Антивирус Касперского, Dr. Web, McAfee, NOD32, Norton Antivirus, ...
 - Основные режимы работы:
 - монитор: проверка всех открываемых и скачиваемых файлов
 - сканер: проверка всех файлов на диске по расписанию
 - регулярное автоматическое обновление «антивирусных баз»
-

Файрвол = брандмауэр = межсетевой экран

- Программа или аппаратное устройство, запрещающее некоторые сетевые соединения
- Обычно настраивается правило «запретить всё, кроме ...» и перечисляются только нужные сервисы
- Формат правил, например, такой:
 - разрешить подключение по порту 80
 - разрешить подключение к login.icq.com:5190