КОМПЬЮТЕРНЫЕ ВИРУСЫ И АНТИВИРУСНЫЕ ПРОГРАММЫ

Компьютерный вирус – специально созданная (человеком злоумышленником) небольшая программа, способная к саморазмножению (т.е. без участия человека), засорению компьютера и выполнению других нежелательных действий, воровству паролей, данных, денежных средств и т.д.

История компьютерных вирусов

Самые первые вирусы были безобидными. Это были эксперименты – типа одного из первых вирусов “Creeper”, который просто выводил сообщение
“I’M A CREEPER: CATCH ME IF YOU CAN” Я CREEPER : поймай меня если сможешь.
Их распространение ограничивалось домашними сетями. Это было в 1971 году.

Первая эпидемия была вызвана **вирусом Brain (от англ. «мозг»)** (также известен как **Пакистанский вирус**), который был разработан братьями **Амджатом** и **Базитом Алви** в **1986 г**. и был обнаружен **летом 1987 г**.

Вирус заразил только в США более 18 тысяч компьютеров.

Программа должна была наказать местных пиратов, ворующих программное обеспечение у их фирмы.

В программке значились имена, адрес и телефоны братьев.

Однако неожиданно для всех The Brain вышел за границы Пакистана и заразил сотни компьютеров по всему миру.

Признаки заражения

✓Замедление работы компьютера и уменьшение размера свободной оперативной памяти;

✓Программы перестают работать или появляются различные ошибки в программах;

✓На экран выводятся посторонние символы и сообщения, появляются различные звуковые и видеоэффекты;

✓Размер некоторых исполнимых файлов и время их создания изменяются;

✓Некоторые файлы и диски оказываются испорченными;

✓Компьютер перестает загружаться с жесткого диска.

Что заражают вирусы

Заражают

- ✓ программы – **.exe, .com**
- ✓ загрузочные сектора дисков и дискет
- ✓ командные файлы – **.bat**
- ✓ драйверы – **.sys**
- ✓ библиотеки – **.dll**
- ✓ документы с макросами – **.doc, .xls, .mdb**
- ✓ *Web*-страницы со скриптами

Не заражают

- ✓ текст – **.txt**
- ✓ рисунки – **.gif, .jpg, .png, .tif**
- ✓ звук (**.wav, .mp3, .wma**)
- ✓ видео (**.avi, .mpg, .wmv**)
- ✓ любые данные без программного кода

Классификация компьютерных вирусов

По среде обитания

файловые

Внедряются в программы и активизируются при их запуске.

После запуска зараженной программы вирусы находятся в ОЗУ и могут заражать другие файлы до момента выключения ПК или перезагрузки операционной системы.

макровирусы

Заражают файлы документов.
После загрузки зараженного документа в соответствующее приложение макровирус постоянно присутствует в оперативной памяти и может заражать другие документы.

сетевые

Могут передавать по компьютерным сетям свой программный код и запускать его на ПК, подключенных к этой сети.

Заражение сетевым вирусом может произойти при работе с электронной почтой или при «путешествиях» по Всемирной сети.

Сетевые вирусы

Распространяются через компьютерные сети, используют ошибки в защите *Windows, браузеров, почтовых программ и* др.

- ✓**Почтовые черви –** распространяются через электронную почту в виде приложения к письму или ссылки на вирус в Интернете; рассылают себя по всем обнаруженным адресам
- ✓**Сетевые черви** – проникают на компьютер через «дыры» в системе, могут копировать себя в папки, открытые для записи
- ✓**IRC-черви, IM-черви –** распространяются через IRC-чаты и интернет-пейджеры (*ICQ*, *AOL*, *Windows Messenger*, *MSN Messenger*)
- ✓**P2P-черви** – распространяются через файло обменные сети P2P (*peer-to-peer)*

ЧЕРВЬ «I LOVE YOU»

Успешно атаковал десятки миллионов компьютеров Windows **в 2000 году**, когда был разослан в виде вложения в электронное сообщение.

В теме письма содержалась строка **«ILoveYou»**, а к письму был приложен скрипт **«LOVE-LETTER-FOR-YOU.TXT.vbs».**

Расширение «.vbs» было по умолчанию скрыто, что и заставило ничего не подозревающих пользователей думать, что это был простой текстовый файл.

При открытии вложения червь рассылал копию самого себя всем контактам в адресной книге Windows, а также на адрес, указанный как адрес отправителя. Он также совершал ряд вредоносных изменений в системе пользователя.

Червь нанёс ущерб мировой экономике в размере **более 10 миллиардов долларов**, поразив **более 3 миллионов ПК по всему миру**, за что вошёл в Книгу рекордов Гиннеса, как самый разрушительный компьютерный вирус в мире.

Троянские программы

Позволяют получать управление удаленным компьютером, распространяются через компьютерные сети, часто при установке других программ (зараженные инсталляторы)

- ✓**Backdoor –** программы удаленного администрирования
- ✓**воровство паролей** (доступ в Интернет, к почтовым ящикам, к платежным системам)
- ✓**шпионы** (введенный с клавиатуры текст, снимки экрана, список программ, характеристики компьютера, промышленный шпионаж)
- ✓**DOS-атаки** (англ. *Denial Of Service* – отказ в обслуживании) –массовые атаки на сайты по команде, сервер не справляется с нагрузкой
- ✓**прокси-сервера** – используются для массовой рассылки рекламы (спама)
- ✓**загрузчики** (англ. *downloader*) – после заражения скачивают на компьютер другие вредоносные программы

Способы заражения

- ✓запустить зараженный файл;
- ✓загрузить компьютер с зараженной дискеты или диска;
- ✓при автозапуске CD(DVD)-диска или флэш-диска;
- ✓открыть зараженный документ с макросами (*Word* или *Excel*);
- ✓открыть сообщение e-mail с вирусом;
- ✓открыть *Web*-страницу с вирусом;
- ✓разрешить установить активное содержимое на *Web*-странице.

Антивирусные программы

Критерии выбора антивируса

- ✓Надежность и удобство в работе
- ✓Качество обнаружения вирусов
- ✓Существование версий под все популярные платформы
- ✓Скорость работы
- ✓Наличие дополнительных функций и возможностей

Антивирусные программы

Антивирусные программы

Сканеры

Используются для **периодической проверки ПК** на наличие вирусов.

После запуска проверяются файлы и оперативная память , в случае обнаружения вирусов обеспечивается их нейтрализация.

Сторожа

Постоянно находятся в оперативной памяти ПК.

Обеспечивают проверку файлов в процессе их загрузки в ОЗУ.

Антивирусные программы

Коммерческие

- ✓AVP = Antiviral Toolkit Pro (www.avp.ru) – Е. Касперский
- ✓DrWeb (www.drweb.com) – И. Данилов
- ✓Norton Antivirus (www.symantec.com)
- ✓McAfee (www.mcafee.ru)
- ✓NOD32 (www.eset.com)

Бесплатные

- ✓Avast Home (www.avast.com)
- ✓Antivir Personal (free-av.com)
- ✓AVG Free (free.grisoft.com)

Правовая охрана программ и данных

Документы Российской Федерации

- ✓Конституция Российской Федерации ст. 44
- ✓Гражданский Кодекс Российской Федерации
- ✓Закон об авторском праве и смежных правах 1993г.
- ✓Закон Российской Федерации «О правовой охране программ для ЭВМ и баз данных» 1992г.

Знак охраны авторского права

Правовая охрана программ и данных

Статья 272. Неправомерный доступ к компьютерной информации

Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, - **наказывается**:

- ✓штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда
- ✓или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев,
- ✓либо исправительными работами на срок от шести месяцев до одного года,
- ✓либо лишением свободы на срок до двух лет.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Нарушение правил эксплуатации ЭВМ лицом, имеющим доступ к ЭВМ, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, **наказывается:**

- ✓лишением права занимать определенные должности или заниматься определенной деятельностью до пяти лет,
- ✓либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов,
- ✓либо ограничением свободы на срок до двух лет.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ

Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, а равно использование либо распространение таких программ или машинных носителей с такими программами, - **наказываются**

- ✓лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда
- ✓или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.