



**Вирусы**

# Цель проекта:

- Ознакомить учеников 11 а класса с тем, что «убивает» их компьютер, благодаря чему происходят различные «глюки», поломки, повреждения.
- Ну, а если говорить в общем: то рассказать, что такое компьютерные вредоносные программы.

# Вредоносные программы

- **Вредоносная программа** — злонамеренная программа, то есть программа, созданная со злым умыслом или злыми намерениями.



# Симптомы заражения вредоносной программой:

- прекращение или сильное замедление работы интернета;
- усиление шума, исходящего от компьютера (создается усиленной работой жёстких дисков);
- изменение домашней страницы в браузере, автоматическое открытие окон с неизвестными вам страницами;
- блокировка доступа к некоторым антивирусным сайтам;
- изменение обоев на рабочем столе;
- появление новых неизвестных процессов в окне «Процессы» диспетчера задач;
- появление звука от работы флоппи-дисковода при отсутствии в нём дискеты;
- появление в реестре автозапуска новых приложений;
- запрет на изменение настроек компьютера в учётной записи администратора;
- невозможность запустить исполняемый файл (выдается сообщение об ошибке);
- всплывание окон системных сообщений с непривычным текстом, в том числе содержащих неизвестные веб-адреса и названия;
- мониторы интернета показывают фальшивую загрузку видеопрограмм, игр, порнороликов и порносайтов, которые вы не закатывали и не посещали;
- открывание и закрывание консоли CD-ROM;
- проигрывание звуков и/или изображений, демонстрация фотоснимков;
- перезапуск компьютера во время старта какой-либо программы;
- случайное и/или беспорядочное отключение компьютера.
- случайное аварийное завершение программ

# SpyWare - программы-шпионы

- Программой-шпионом (альтернативные названия - Spy, SpyWare, Spy-Ware, Spy Trojan) принято называть программное обеспечение, собирающее и передающее кому-либо информацию о пользователе без его согласия. Информация о пользователе может включать его персональные данные, конфигурацию его компьютера и операционной системы, статистику работы в сети Интернет.

# Пути попадания шпионского программного обеспечения на ПК:

- В ходе посещения сайтов Интернет. Наиболее часто проникновение шпионского ПО происходит при посещении пользователем хакерских и warez сайтов, сайтов с бесплатной музыкой и порносайтов. Как правило, для установки шпионского ПО применяются ActiveX компоненты или троянские программы категории TrojanDownloader по классификации лаборатории Касперского. Многие хакерские сайты могут выдать "крэк", содержащий шпионскую программу или TrojanDownloader для ее загрузки;
- В результате установки бесплатных или условно-бесплатных программ. Самое неприятное состоит в том, что подобных программ существует великое множество, они распространяются через Интернет или на пиратских компакт-дисках. Классический пример - кодек DivX, содержащий утилиту для скрытной загрузки и установки SpyWare.Gator. Большинство программ, содержащих SpyWare-компоненты, не уведомляют об этом пользователя

# Кейлоггер

- **Кейлоггер, кейлоггер, keylogger** — это программное обеспечение или аппаратное устройство, регистрирующее каждое нажатие клавиши на клавиатуре компьютера.



# Логическая бомба

- **Логическая бомба** — программа, которая запускается при определенных временных или информационных условиях для осуществления вредоносных действий (как правило, несанкционированного доступа к информации, искажения или уничтожения данных).
- Многие вредоносные программы, такие как вирусы или черви, часто содержат логические бомбы, которые срабатывают в заранее определенное время или при выполнении определенных условий, например, в пятницу 13-го или в день смеха.

# Компьютерный вирус-

- Это самораспространяющийся в информационной среде компьютеров программный код. Он может внедряться в исполняемые и командные файлы программ, распространяться через загрузочные секторы дискет и жестких дисков, документы офисных приложений, через электронную почту, **Web**-сайты, а также и по другим электронным каналам.

# Троянские программы:

Троянская программа (также — троян, троянец, троянский конь, трой) — вредоносная программа, проникающая на компьютер под видом безвредной — кодека, скринсейвера, хакерского ПО и т. д .

Для того, чтобы спровоцировать пользователя запустить троянца, файл программы называют служебным именем, маскируют под другую программу (например, установки другой программы), файл другого типа или просто дают привлекательное для запуска название, иконку и т. п. Злоумышленник может перекомпилировать существующую программу, добавив к её исходному коду вредоносный, а потом выдавать за оригинал или подменять его.

Трояны обладают множеством видов и форм, поэтому не существует абсолютно надёжной защиты от них.

# Ransomware

- **Ransomware** -категория вредоносных программ, блокирующих данные или работоспособность компьютера. Их действия не санкционированы пользователем компьютера; программа используется злоумышленниками с целью дальнейшего требования выкупа.

# Забавные вирусы:

- Вирус Под кайфом, или вирус Марихуаны:
- Вирус из каменного века компьютерной эры. Он поражал ранние версии системы DOS через дискетный привод. Впервые вирус был замечен в Новой Зеландии в 1988 году. Оригинальная версия его не причиняла особого вреда, на экране просто появлялось сообщение: «Ваш компьютер под кайфом. Легализуйте марихуану». Однако версии 90-х гг. вируса Под кайфом (распространялись под названиями Дональд Дак, Гавайи, Ростов, Смитсоиан, Каменная Мутация и др.) наносил уже значительный вред главной загрузочной записи и таблице размещения файлов на вашем жестком диске.

# Троянский конь — Комар

- Операционная система Symbian была мишенью для другого вируса в 2004 году – на этот раз Троянского комара. Эта программа, разработанная для борьбы с пиратством, поражала телефоны при попытке скачать нелегальную версию Комара, игры для смартфонов. Как только вирус попадал в телефон, он начинал отправлять СМС-сообщения по непомерной цене на элитные номера Великобритании, Германии, Нидерландов и Швейцарии без ведома владельцев. Избавиться от этого вируса было легко – надо было всего лишь удалить игру с устройства, что наверняка было бы сделано сразу же после получения километровых счетов за телефон.

# ИСТОЧНИКИ:

- <http://z-oleg.com/secur/articles/spyware.php>
- <http://ru.wikipedia.org/wiki/Keylogger>
- [http://www.seobuilding.ru/wiki/%D0%9B%D0%BE%D0%B3%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F\\_%D0%B1%D0%BE%D0%BC%D0%B1%D0%B0](http://www.seobuilding.ru/wiki/%D0%9B%D0%BE%D0%B3%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D0%B1%D0%BE%D0%BC%D0%B1%D0%B0)
- [http://www.frolov-lib.ru/antivirus/articles/mir\\_pk1/index.html](http://www.frolov-lib.ru/antivirus/articles/mir_pk1/index.html)
- [http://ru.wikipedia.org/wiki/%D0%A2%D1%80%D0%BE%D1%8F%D0%BD%D1%81%D0%BA%D0%B8%D0%B5\\_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D1%8B](http://ru.wikipedia.org/wiki/%D0%A2%D1%80%D0%BE%D1%8F%D0%BD%D1%81%D0%BA%D0%B8%D0%B5_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D1%8B)
- <http://av-school.ru/wiki/index.php/Ransomware>
- <http://habrahabr.ru/blogs/personal/97251/>