# Вредоносное программное обеспечение

# План занятия:

- Понятие вредоносного ПО
- Виды вредоносного ПО
- Признаки заражения компьютера
- Антивирусные средства

# Вредоносное ПО - это

программное обеспечение, которое разрабатывается для получения несанкционированного доступа к вычислительным ресурсам ЭВМ, а также данным, которые на ней хранятся

# Компьютерный вирус - это

это специально написанная, небольшая по размерам программа, которая может «приписывать» себя к другим программам, создавать свои копии и внедрять их в файлы, системные области компьютера, а также выполнять различные нежелательные действия на компьютере

# Первые прототипы будущих вирусов

**Программы – кролики (rabbits)**

# Первый сетевой вирус

В конце 60-х годов обнаружена первая саморазмножающаяся по сети программа

Creeper (Вьюнок)

**“i'm the creeper ... catch me, if you can”**
**«я вьюнок ... поймай меня, если сможешь»**

# Первые антивирусные средства

## Reaper (Жнец)

распространялся по сети подобно Вьюнку,
но уничтожал копию последнего

# Свойства вирусов:

- способность к саморазмножению;
- высокая скорость распространения
- избирательность поражаемых систем
- способность «заражать» еще незараженные системы
- трудность борьбы
- быстрота появления модификаций (мутация)

# Классификация вирусов:

- по среде обитания вируса
- по способу заражения среды обитания
- по деструктивным возможностям
- по особенностям алгоритма вируса
- по методу распространения

# Классификация по методу распространения

- эксплойты
- логические бомбы
- троянские программы
- компьютерные вирусы
- сетевые черви

# Эксплойт - это

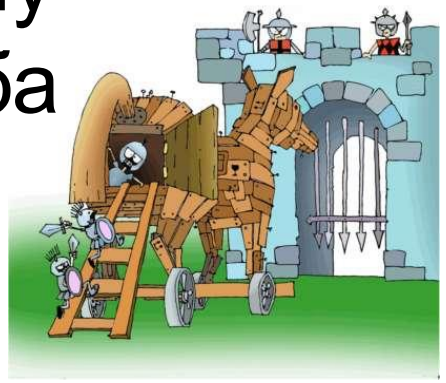
теоретически безобидный набор данных, некорректно воспринимаемый программой, работающей с такими данными

# Логическая бомба

срабатывает при определённом условии, и неотделима от полезной программы-носителя

# Троянская программа

программа, которая, являясь частью другой программы с известными пользователю функциями, способна втайне от него выполнять некоторые дополнительные действия с целью причинения ему определенного ущерба



# Компьютерный вирус

это специально написанная, небольшая по размерам программа, которая может «приписывать» себя к другим программам, создавать свои копии и внедрять их в файлы, системные области компьютера, а также выполнять различные нежелательные действия на компьютере

# Сетевой червь

вредоносная программа, которая может самостоятельно размножаться по сети

# Симптомы заражения:

- автоматическое открытие окон с незнакомым содержимым при запуске компьютера
- блокировка доступа к официальным сайтам антивирусных компаний, или же к сайтам, оказывающим услуги по «лечению» компьютеров от вредоносных программ
- появление новых неизвестных процессов в окне «Процессы» диспетчера задач Windows
- появление в ветках реестра, отвечающих за автозапуск, новых записей
- запрет на изменение настроек компьютера в учётной записи администратора

# Симптомы заражения:

- невозможность запустить исполняемый файл
- появление всплывающих окон или системных сообщений с непривычным текстом, в том числе содержащих неизвестные веб-адреса
- перезапуск компьютера во время старта какой-либо программы
- случайное и/или беспорядочное отключение компьютера
- случайное аварийное завершение программ

# Основные меры обеспечения безопасности

- использование современных ОС, не дающих изменять важные файлы без ведома пользователя
- своевременная установка обновлений
- включение режима автоматического обновления
- использовать программное обеспечение с проактивной защитой от угроз
- работа на персональном компьютере исключительно под правами пользователя

# Основные меры обеспечения безопасности

- ограничение физического доступа к компьютеру посторонних лиц
- использование внешних носителей информации только от проверенных источников
- запрет на открытие компьютерных файлов, полученных от ненадёжных источников
- использование персонального Firewall, контролирующего выход в сеть Интернет с персонального компьютера на основании политик, которые устанавливает сам пользователь

# Антивирус - это

компьютерная программа, которая помогает предотвратить заражение файлов или операционной системы вредоносным ПО, а также обнаруживает вредоносные программы

# Виды антивирусных программ:

- программы-детекторы
- программы-доктора или фаги
- программы-ревизоры
- программы-фильтры
- программы-вакцины или иммунизаторы

# Программы-детекторы

осуществляют поиск характерною для конкретного вируса кода (сигнатуры) в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение. Недостатком таких антивирусных программ является то, что они могут находить только те вирусы, которые известны разработчикам таких программ

# Программы-доктора или фаги

не только находят зараженные вирусами файлы, но и «лечат» их т. е. удаляют из файла тело программы-вируса, возвращая файл в исходное состояние. В начале своей работы фаги ищут вирусы в оперативной памяти, уничтожая их, и только затем переходят к «лечению» файлов. Среди фагов выделяют полифаги, т. е. программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов

# Программы-ревизоры

относятся к самым надежным средствам защиты от вирусов. Ревизоры запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным. Обнаруженные изменения выводятся на экран монитора. Как правило, сравнение состояний производят сразу после загрузки операционной системы. При сравнении проверяются длина файла, контрольная сумма файла, дата и время модификации, другие параметры.

# Программы-фильтры или «сторожа»

представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов. При попытке какой-либо программы произвести некоторые действия «сторож» посылает пользователю сообщение и предлагает запретить или разрешить соответствующее действие. Они полезны, так как способны обнаружить вирус на самой ранней стадии его существования до размножения. Однако, они не «лечат» файлы и диски. Славятся своей «назойливостью».

# Вакцины или иммунизаторы

резидентные программы, предотвращающие заражение файлов. Вакцины применяют, если отсутствуют программы-доктора, «лечащие» этот вирус. Вакцинация возможна только от известных вирусов. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедрится.




**Задание: необходимо сопоставить название вредоносного ПО с его описанием.**

| Классификация по среде обитания | | | |
|---|---|---|---|
| Вид | Ответ | Описание | Пример |
| 1. Сетевые | | 1. Внедряются в выполняемые файлы | |
| 2. Файловые | | 2. Внедряются в загрузочный сектор диска | |
| 3. Загрузочные | | 3. Распространяются по компьютерной сети | |
| **Классификация по способу заражения** | | | |
| Вид | Ответ | Описание | Пример |
| 1. Резидентные | | 1. Находятся в памяти, активны до выключения компьютера | |
| 2. Нерезидентные | | 2. Не заражают память, являются активными ограниченное время | |
| **Классификация по деструктивным возможностям** | | | |
| Вид | Ответ | Описание | Пример |
| 1. Безвредные | | 1. Могут привести к серьезным сбоям в работе | |
| 2. Неопасные | | 2. Уменьшают свободную память, создают звуковые, графические и прочие эффекты | |
| 3. Опасные | | 3. Могут привести к потере программ или системных данных | |
| 4. Очень опасные | | 4. Практически не влияют на работу; уменьшают свободную память на диске в результате своего распространения | |
| **Классификация по особенности алгоритма вируса** | | | |
| Вид | Ответ | Описание | Пример |
| 1. Вирусы – «спутники» | | 1. Примитив, содержит большое количество ошибок | |
| 2. Вирусы – «черви» | | 2. Создают для EXE-файлов файлы-спутники с расширением .COM | |
| 3. «Паразитические» | | 3. Пишутся на WordBasic, живут в документах Word, переписывают себя в Normal.dot | |
| 4. «Студенческие» | | 4. Распространяются по сети, рассылают свои копии, вычисляя сетевые адреса | |
| 5. «Спид» - вирусы | | 5. Не имеют ни одного постоянного участка кода, труднообнаруживаемы | |
| 6. Вирусы – призраки | | 6. Перехватывают обращения DOS к пораженным файлам или секторам и подставляют вместо себя незараженные участки | |
| 7. Макровирусы | | 7. Изменяют содержимое дисковых секторов или файлов | |

***Критерии оценки задания:***

«5» ставится, если курсант выполнил задание полностью (правильно заполнены поля «Ответ» и «Пример», с небольшим количеством ошибок).

«4» ставится, если курсант выполнил задание не полностью (не заполнено поле «Пример», а поле «Ответ» заполнено верно).

«3» ставится, если курсант выполнил задание с ошибками (допущены ошибки при заполнении поля «Ответ»).

«2» ставится, если курсант не выполнил задание.

# Домашнее задание:

Источники для выполнения:

1. Голицына О.Л., Максимов Н.В., Партыка Т.Л., Попов И.И. Информационные технологии. – учебник. –М.:Инфра-М,2006.
2. http://www.securitylab.ru – эл. ресурс
3. http://www.securelist.com – эл. ресурс
4. http://help-antivirus.ru – эл. ресурс

Будьте бдительны…

они где-то рядом…