**Тема занятия «КОМПЬЮТЕРНЫЕ ВИРУСЫ»**

**«АНТИВИРУСНЫЕ СРЕДСТВА»**

**Изучите теоретический материал.**

***Компьютерный вирус*** – это специальная компьютерная программа обычно малая по размеру, которая способна «размножаться» и «заражать» другие программы. Другими словами она многократно копирует свой код и присоединяет его к кодам других программ.

Программа, внутри которой находится вирус, называется **«зараженной».**

***Кто же создает вирусы?***

Вирусы создают квалифицированные программисты, либо студенты. Количество новых программных вирусов постоянно растет и видоизменяется, поэтому пользователь компьютера должен знать о природе вирусов, способах заражения вирусами и защиты от них.

***Вирус -*** специально написанная программа способная к самовоспроизведению. Присоединяясь к другим программам, способна создавать свои копии и внедрять в них файлы системной области компьютера с целью нарушения работы программ, порчи файлов и каталогов, создание всевозможных помех в работе компьютера.

Основными путями проникновения вирусов в компьютер является съемные диски и компьютерные сети

***Пути распространения компьютерных вирусов***

Давайте подумаем, каковы пути распространения вирусов. (Вирусы могут попасть в ПК так же как любая другая программа). В противоположность обычным бациллам, компьютерные вирусы не передаются по воздуху: так как вирусы – это программы – средой их обитания служит только различная компьютерная техника.

Как на ПК может попасть вредоносная программа? (Через зараженные дискеты, диски, флеш-карты, посредством Интернета или по локальной сети). Обычно вирус внедряется в какой-либо документ или программу, и в начале работы вы можете не заметить ничего необычного. Однако через некоторое время вирус проявит свою разрушительную силу.

***Признаки появления компьютерных вирусов***

Назовем основные признаки проявления компьютерных вирусов.

•    неправильная работа нормально работавших программ;  
•    медленная работа компьютера;  
•    невозможность загрузки ОС;  
•    исчезновение файлов и каталогов;  
•    изменение размеров файлов;  
•    неожиданное увеличение количества файлов на диске;  
•    уменьшение размеров свободной оперативной памяти;  
•    вывод на экран неожиданных сообщений и изображений;  
•    подача непредусмотренных звуковых сигналов;  
•    частые зависания и сбои в работе компьютера.

***История компьютерной вирусологии***

Первые вирусы появились давно, еще на заре эпохи ЭВМ, и не всегда были вредоносными. Например, в конце 60-х в лаборатории Xerox была создана специальная программа, являющаяся прообразом современных вирусов, которая самостоятельно путешествовала по локальной вычислительной сети и проверяла работоспособность включенных в нее устройств.

Однако позднее программы-вирусы стали разрабатываться со злым умыслом. Есть сведения, что некоторые компании специально инфицировали компьютеры конкурентов, чтобы таким образом шпионить за ними или вывести из строя их информационные системы.

***Слухи и заблуждения***

Порой боязнь вирусов причиняет больше неприятностей, чем сами вирусы. В свое время распространялось много заведомо ложных сообщений об угрозе якобы сверхопасных вирусов.

Необходимо знать, что ни один из вирусов не способен вывести из строя комплектующие компьютера. Максимум, на что способны некоторые вирусы, - это уничтожить информацию на жестком диске, что приведет к повреждению ОС и приложений. Хотя даже в этом случае ситуация может стать для вас фатальной, если вирус уничтожит важные документы.

***Создатели компьютерных вирусов***

Человек, который «пишет» вирусы называет себя вирьмейкером. Кто же занимается созданием вредоносных программ? В наши дни созданием вирусов обычно занимаются энтузиасты – одиночки. Ими могут быть и профессиональные программисты, и исследователи и обычные студенты, начинающие изучать программирование. Причем в настоящее время имеются десятки программ для автоматической генерации вирусов – конструкторы.

Что является стимулом для такой деятельности – сказать сложно. Это может быть как чувство мести, так и желание самоутвердиться. Первым вирусным конструктором, который получил широкое распространение, стал VCL (Virus Creation Laboratory), созданный в 1992 году.

**Классификация вирусов.**

паразитические

репликаторы

троянские

невидимки

мутанты

***по особенностям алгоритмов***

опасные

очень опасные

неопасные

***по степени воздействия***

***По среде обитания***

сетевые

файловые

загрузочные

файлово-загрузочные

***По способу заражения***

резидентные

нерезидентные

**Вирусы выделяют по следующим признакам:**

1. По среде обитания:

- сетевые, распространяющиеся по компьютерной сети;

- файловые, внедряющиеся в выполняемый файл;

-загрузочные, внедряющиеся в загрузочный сектор жесткого диска.

2. по способу заражения:

- резидентные, загружаемые в память ПК;

- нерезидентные, не заражающие память ПК и остающиеся активными ограниченное время.

3. По возможностям:

•   **Безвредные вирусы** – оказывают незначительное влияние на работу ПК, занимая часть системных ресурсов. Нередко пользователи даже не подозревают об их присутствии.

•   **Неопасные вирусы** – также занимают часть ресурсов компьютера, но об их присутствии пользователь знает хорошо. Обычно они проявляются в виде визуальных и звуковых эффектов и не вредят данным пользователя.

•    **Опасные вирусы** – программы, которые нарушают нормальную работу пользовательских приложений или всей системы.

•    **Очень опасные вирусы** – программы, задача которых заключается в уничтожении файлов, выводе из стоя программ и ОС или рассекречивании конфиденциальных данных.

**Основные признаки проявления вирусов:**

1. прекращение работы или неправильная работа ранее успешно функционировавших программ;

2. медленная работа компьютера;

3. исчезновение файлов и папок или искажение содержимого;

4. изменение размеров файла;

5. неожиданное значительное увеличение файлов на диске;

6. уменьшение размера оперативной памяти;

7. частые зависания и сбои в работе компьютера.

**Основные группы вирусов:**

1. загрузочные вирусы – заражают программу начальной загрузки компьютера, которая храниться в загрузочном секторе винчестера, и запускается при загрузке компьютера;

2. файловые вирусы внедряются главным образом в файлы, имеющие расширение COM, EXE.

3. загрузочно – файловые вирусы заражают как файлы, так и загрузочные сектора дисков;

4. драйверные вирусы заражают драйверы устройств компьютера;

5. сетевые вирусы распространяются в сетях, объединяющих многие десятки и сотни тысяч компьютеров.

**Загрузочные вирусы делятся на:**

- макро – вирусы;

- «Червь».

**Особенностью червей**, отличающих их от других вирусов, является то, что они не несут в себе ни какой вредоносной нагрузки, кроме саморазмножения, целью которого является замусоривание памяти, и как следствие, затормаживание работы операционной системы.

**Сетевые черви**

К данной категории относятся программы, распространяющие свои копии по локальным и/или глобальным сетям с целью:

1. ***проникновения на удаленные компьютеры;***
2. ***запуска своей копии на удаленном компьютере;***
3. ***дальнейшего распространения на другие компьютеры в сети.***

Для своего распространения сетевые черви используют разнообразные компьютерные и мобильные сети: электронную почту, системы обмена мгновенными сообщениями, файлообменные (P2P) и IRC-сети, LAN, сети обмена данными между мобильными устройствами (телефонами, карманными компьютерами) и т. д.

**Каналы распространения:**

***Дискеты, диски.***

Самый распространённый канал заражения в 1980-90 годы. Сейчас практически отсутствует из-за появления более распространённых и эффективных каналов и отсутствия флоппи-дисководов.

***Флеш-накопители (флешки).***

В настоящее время USB-флешки заменяют дискеты и повторяют их судьбу — большое количество вирусов распространяется через съёмные накопители, включая цифровые фотоаппараты, цифровые видеокамеры, цифровые плееры (MP3-плееры), сотовые телефоны. Использование этого канала преимущественно обусловлено возможностью создания на накопителе специального файла ***autorun.inf,***в котором можно указать программу, запускаемую Проводником Windows при открытии такого накопителя. Флешки — основной источник заражения для компьютеров, не подключённых к сети Интернет.

***Электронная почта.***

Сейчас один из основных каналов распространения вирусов. Обычно вирусы в письмах электронной почты маскируются под безобидные вложения: картинки, документы, музыку, ссылки на сайты.

***Системы обмена мгновенными сообщениями.***

Так же распространена рассылка ссылок на якобы фото, музыку либо программы, в действительности являющиеся вирусами, по ICQ и через другие программы мгновенного обмена сообщениями.

***Веб-страницы.***

Возможно также заражение через страницы Интернет ввиду наличия на страницах всемирной паутины различного «активного» содержимого.

***Интернет и локальные сети (черви)***

Черви — вид вирусов, которые проникают на компьютер-жертву без участия пользователя. Черви используют так называемые «дыры» (уязвимости) в программном обеспечении операционных систем, чтобы проникнуть на компьютер.

***Антивирусные средства***

Программы, позволяющие обнаруживать и уничтожать вирусы, называются антивирусными программами.

**Основные типы антивирусных программ:**

1. **Программы – детекторы** обнаруживают файлы, зараженные одним из известных вирусов.
2. **Фаги, программы – доктора, программы – вакцины** не только находят зараженные вирусами файлы, но и «Лечат» их, т.е. удаляют из файла тело программы вируса, восстанавливая программу в том состоянии, в котором она находилась до заражения вирусом.
3. **Программы – ревизоры** относятся к самым надежным средствам защиты от вирусов. Ревизоры запоминают исходное состояние программ тогда, когда компьютер еще не заражен вирусом, а затем периодически сравнивает текущее состояние с исходным.
4. **Программы – фильтры, или «сторожа»,** - это небольшие программы постоянно находящиеся в памяти компьютера. Они контролируют операции компьютера и обнаруживают подозрительные действия при работе компьютера.

Для борьбы с вирусами разрабатываются **антивирусные программы**. Говоря медицинским языком, эти программы могут выявлять (диагностировать), лечить (уничтожать) вирусы и делать прививку “здоровым” программам.

Различают следующие виды антивирусных программ:

* Программы – детекторы (сканеры);
* Программы – доктора (или фаги, дезинфекторы);
* Программы – ревизоры;
* Программы – фильтры (сторожа, мониторы);
* Программы – иммунизаторы.

Программы – **детекторы** рассчитаны на обнаружение конкретных вирусов и основаны на сравнении характерной (спецификой) последовательности байтов (сигнатур или масок вирусов), содержащихся в теле вируса, с байтами проверяемых программ. Программы – детекторы нужно регулярно обновлять, так как они быстро устаревают и не могут выявлять новые виды вирусов.

Следует подчеркнуть, что программы – детекторы могут обнаружить только те вирусы, которые ей “известны”, то есть, сигнатуры этих вирусов заранее помещены в библиотеку антивирусных программ.

Таким образом, если проверяемая программа не опознается детектором как зараженная, то еще не следует считать, что она “здорова”. Она может быть инфицирована новым вирусом, который не занесен в базу данных детектора.

Для устранения этого недостатка программы – детекторы стали снабжаться блоками эвристического анализа программ. В этом режиме делается попытка обнаружить новые или неизвестные вирусы по характерным для всех вирусов кодовым последовательностям. Наиболее развитые эвристические механизмы позволяют с вероятностью около 80% обнаружить новый вирус.

Программы – **доктора** не только находят файлы, зараженные вирусами, но и лечат их, удаляя из файла тело программы – вируса. Программы – доктора, которые позволяет лечить большое число вирусов, называют полифагами.

В России получили широкое распространение программы – детекторы, одновременно выполняющие и функции программ – докторов. Наиболее известные представители этого класса – AVP (Antiviral Toolkit Pro, автор – Е. Касперский), Aidstest (автор – Д. Лозинский) и Doctor Web (авторы – И. Данилов, В. Лутовин, Д. Белоусов).

**Ревизоры** – это программы, которые анализируют текущее состояние файлов и системных областей диска и сравнивают его с информацией, сохраненной ранее в одном из файлов ревизора. При этом проверяется состояние BOOT – сектора, FAT – таблицы, а также длина файлов, их время создания, атрибуты, контрольные суммы.

Контрольная сумма является интегральной оценкой всего файла (его слепком). Получается контрольная сумма путем суммирования по модулю для всех байтов файла. Практически всякое изменение кода программы приводит к изменению контрольной суммы файла.

**Антивирусы – фильтры** – это резидентные программы (сторожа), которые оповещают пользователя обо всех попытках какой – либо программы выполнить подозрительные действия. Фильтры контролируют следующие операции:

* Обновление программных файлов и системной области диска;
* Форматирование диска;
* Резидентное размещение программ в ОЗУ.

Обнаружив попытку выполнения таких действий, сторож (монитор) сообщает об этом пользователю, который окончательное решение по выполнению данной операции. Заметим, что она не способна обезвредить даже известные вирусы. Для “лечения” обнаруженных фильтром вирусов нужно использовать программы – доктора.

К последней группе относятся наименее эффективные **антивирусы – вакцинаторы** (иммунизаторы). Они записывают в вакцинируемую программу признаки конкретного вируса так, что вирус считает ее уже зараженной, и поэтому не производит повторное инфицирование. Этот вид антивирусных программ морально устарел.

**ЗАДАНИЯ:**

**Письменно ответить на вопросы:**

1. Что такое компьютерные вирусы.
2. Признаки проявления вирусов.
3. Программы борьбы с компьютерными вирусами.
4. Методы защиты от компьютерных вирусов.
5. Каково строение вируса?
6. Как распространяются вирусы?
7. Как действуют вирусы?
8. Как активизируются вирусы?
9. Как избежать заражения?
10. Как избавиться от вируса?
11. Какова ответственность за нанесенный вред?
12. Зачем создают вирусы?
13. Что вирусы могут?
14. Что вирусы не могут?
15. Перечислите основные классификационные признаки вирусов.
16. Какие вирусы различают по среде обитания?
17. Какие вирусы различают по способу заражения?
18. Какие вирусы можно выделить по степени воздействия?
19. Какие вирусы различают по особенностям алгоритмов?
20. Из каких этапов состоит жизненный цикл вирусов?
21. Перечислите меры по защите от вирусов.
22. Какие программы называют антивирусными?
23. Перечислите основные виды антивирусных программ.
24. Какие программы относят к программам-детекторам?
25. Что делают программы доктора, какие среди них выделяют и для чего они предназначены?
26. Как себя ведут программы-ревизоры?
27. Что относят к программам-фильтрам, или «сторожам», для чего они предназначены?

28. Что делают программы вакцины, или иммунизаторы?

***Задание 1.***

Подумайте в чем сходство и различие биологического и компьютерного вируса. Заполните таблицу:

|  |  |
| --- | --- |
| *Сходства* | *Различия* |
| 1.  2.  3. | 1.  2.  3. |

***Задание 2.***

Какие вирусы могут заразить следующие объекты:

А) файл Реферат.doc;

Б) файл Setup.exe;

В) электронное письмо;

Г) файл Товарооборот.xls;

Д) файл Лето.bmp

***Задание 3.***

Перечислите объекты компьютерной системы, заражение которых приведет к незначительным и необратимым последствиям. Заполните таблицу:

|  |  |
| --- | --- |
| *Незначительные разрушительные последствия* | *Необратимые разрушительные последствия* |
| 1.  2.  3. | 1.  2.  3. |

Присылать задания в группу **в контакте в сообщения сообщества**:

<https://vk.com/club200357550>

Название файла, пример: дата, фамилия, имя (если в контакте вы называетесь по-другому): *16.11.20 Карапетян Арсен*

**Срок исполнения задания: 24.12.2020.**