**Практическая работа**

**Защита информации, антивирусная защита**

1. **Цель работы:** рассмотреть понятия: компьютерный вирус, антивирусная программа, архив, программа архивации; виды вирусов и антивирусных программ; меры профилактики ПК от компьютерных вирусов. Научиться работать с архивами, антивирусными программами.
2. **Оборудование**: компьютер; лекционный материал; ресурсы сети Интернет.
3. **Теоретические сведения** к практической работе представлены в презентации «Вирусы и архивы».

**Задание №1. Используя презентацию, ответьте на вопросы:**

|  |  |
| --- | --- |
| **Вопрос** | **Ответ** |
| Что такое компьютерный вирус? | это специально написанная программа, которая при запуске способна распространяться **без участия человека и выполнять вредоносные действия.** |
| В чем состоит принцип работы вируса? | **выполнять вредоносные действия.** |
| Перечислите вредные действия вирусов. | * звуковые и зрительные эффекты * имитация сбоев ОС и аппаратуры * перезагрузка компьютера * разрушение файловой системы * уничтожение информации * шпионаж – передача секретных данных * массовые атаки на сайты Интернет |

**Задание №2. Запишите признаки заражения ПК вирусом.**

|  |  |
| --- | --- |
| **№** | **Признак** |
|  | * + замедление работы компьютера |
|  | * + перезагрузка или зависание компьютера |
|  | * + неправильная работа ОС или прикладных программ |
|  | * + изменение длины файлов |
|  | * + появление новых файлов |
|  | * + уменьшение объема оперативной памяти |
|  | * + рассылка сообщений *e-mail* без ведома автора |
|  |  |
|  |  |
|  |  |

**Задание №3. Проанализируйте и запишите, какие типы файлов подвержены заражению?**

|  |  |
| --- | --- |
| **Типы файлов, подверженные заражению** | **Типы файлов, не подверженные заражению** |
| * программы – **\*.exe, \*.com** | * текст – **\*.txt** |
| * загрузочные сектора дисков и дискет | * рисунки – **\*.gif, \*.jpg, \*.png, \*.tif** |
| * командные файлы – **\*.bat** | * звук (**\*.wav, \*.mp3, \*.wma**) |
| * драйверы – **\*.sys** | * видео (**\*.avi, \*.mpg, \*.wmv**) |
| * библиотеки – **\*.dll** | * любые данные (без программного кода) |
| * документы с макросами – **\*.doc, \*.xls, \*.mdb** |  |
| * *Web-*страницы со скриптами |  |
|  |  |

**Задание №4. Проанализируйте и запишите основные способы заражения ПК.**

|  |  |
| --- | --- |
| **№** | **Способ заражения ПК** |
| 1 | запустить зараженный файл |
| 2 | * + загрузить компьютер с зараженной дискеты или диска; |
| 3 | * + при автозапуске CD(DVD)-диска или флэш-диска; |
| 4 | * + открыть зараженный документ с макросами (*Word* или *Excel*)*;* |

**Запишите меры профилактики заражения ПК вирусом:**

|  |  |
| --- | --- |
| **№** | **Способ профилактики** |
| 1 |  |
| 2 |  |
| 3 |  |
| 4 |  |
| 5 |  |
| 6 |  |

**Задание №5. Запишите классификацию вирусов в виде таблицы**

|  |  |  |
| --- | --- | --- |
| **№** | **Вид (название) вируса** | **Особенность вируса** |
|  | **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 (сканирование – поиск уязвимых компьютеров в сети) |
|  | **IRC-черви, IM-черви** | распространяются через IRC-чаты и интернет-пейджеры (*ICQ*, *AOL*, *Windows Messenger*, *MSN Messenger*) |
|  | **P2P-черви** | распространяются через файлообменные сети P2P (*peer-to-peer)* |
|  | **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 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Задание №6 Сравните виды антивирусных программ, дайте им краткую характеристику.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Вид** | **Характеристика** | **Достоинства** | **Недостатки** |
| 1 | Антивирусы-сканеры | * умеют находить и лечить **известные им** вирусы в памяти и на диске; * используют базы данных вирусов; * ежедневное обновление баз данных через Интернет. | * лечат известные им вирусы | * не могут предотвратить заражение * чаще всего не могут обнаружить и вылечить неизвестный вирус |
| 2 | Антивирусы-мониторы | * перехватывают действия, характерные для вирусов и блокируют их (форматирование диска, замена системных файлов); * блокируют атаки через Интернет; * проверяют запускаемые и загружаемые в память файлы (например, документы *Word*); * проверяют сообщения электронной почты; * проверяют *Web-*страницы; * проверяют сообщения ICQ | * непрерывное наблюдение * блокируют вирус в момент заражения * могут бороться с неизвестными вирусами | * замедление работы компьютера * в случае ошибки ОС может выйти из строя |

**Задание №7. Перечислите функции, выполняемые антивирусом Касперского.**

|  |  |
| --- | --- |
| **№** | **Функция** |
| 1 | * **Файловый антивирус** (проверка файлов в момент обращения к ним) |
| 2 | * **Почтовый антивирус** (проверка входящих и выходящих сообщений) |
| 3 | * **Веб-антивирус** (Интернет, проверка *Web*-страниц) |
| 4 | * **Проактивная защита** (попытки обнаружить неизвестные вредоносные программы):   + слежение за реестром   + проверка критических файлов   + сигналы о «подозрительных» обращениях к памяти |
| 5 | * **Анти-шпион** (борьба с Интернет-мошенничеством) |
| 6 | * **Анти-хакер** (обнаружение сетевых атак) |

**Задание №8 Сформулируйте алгоритм проверки файлов на вирус с помощью антивируса Касперского.**

|  |  |
| --- | --- |
| **№** | **Описание действия** |
| 1 |  |
| 2 |  |
| 3 |  |
| 4 |  |
| 5 |  |
| 6 |  |
| 7 |  |
| 8 |  |

**Задание №9 Проверка файла на вирус в режиме онлайн.** Перейдите на сайт <https://www.virustotal.com/ru/> Загрузите файл задания практической работы. Проверьте файл на вирус. Запишите результат проверки и алгоритм действий.

|  |  |  |
| --- | --- | --- |
| Результат проверки файла (скриншот): | |  |
| **№** | **Описание действия** | |
| 1 |  | |
| 2 |  | |
| 3 |  | |
| 4 |  | |
| 5 |  | |
| 6 |  | |
| 7 |  | |
| 8 |  | |

**Задание №10 Используя презентацию, ответьте на вопросы:**

|  |  |
| --- | --- |
| **Вопрос** | **Ответ** |
| Что такое архивация? | создание резервных копий (на CD, DVD). Цели:   * + сохранить данные на случай сбоя на диске   + объединить группу файлов в один архив   + зашифровать данные с паролем |
| Что такое сжатие файлов? | **Сжатие файлов** – это уменьшение их размера. Цели:   * + уменьшить место, которое занимают файлы на диске   + уменьшить объем данных для передачи через Интернет |
| Перечислите типы сжатия. | * + **без потерь:** сжатый файл можно восстановить в исходном виде, зная алгоритм сжатия     - тексты     - программы     - данные   + **с потерями**: при сжатии часть информации безвозвратно теряется     - фотографии (**\*.jpg**)     - звук (**\*.mp3**)     - видео (**\*.mpg**) |
| Какие типы файлов можно сжать без потерь? | * + - тексты     - программы     - данные |
| Какие типы файлов можно сжать с потерями? | * + - фотографии (**\*.jpg**)     - звук (**\*.mp3**)     - видео (**\*.mpg**) |
| Каков принцип сжатия файлов? | Сжатие возможно, если в данных есть повторяющиеся символы или цепочки символов, сжатие «устраняет» эту **избыточность**. |

**Задание №11**

1.Поместите файл практической работы в архив, названный вашей фамилией.

2.Сделайте снимок экрана, отображающий созданный архив и вставьте его в документ.

Снимок:

3.Сформулируйте алгоритм помещения файлов в архив.

|  |  |
| --- | --- |
| **№** | **Описание действия** |
| 1 |  |
| 2 |  |
| 3 |  |
| 4 |  |
| 5 |  |
| 6 |  |
| 7 |  |
| 8 |  |

**Задание №12**

1.Скопируйте из сетевой папки архивный файл Задание.rar.

2.Извлеките файлы, помещенные в архив.

3.Откройте текстовый файл Задание.

4.Сделайте снимок экрана.

5.Поместие снимок экрана в документ.

Снимок:

6.Сформулируйте алгоритм извлечения файлов из архива.

|  |  |
| --- | --- |
| **№** | **Описание действия** |
| 1 |  |
| 2 |  |
| 3 |  |
| 4 |  |
| 5 |  |
| 6 |  |
| 7 |  |
| 8 |  |

Поместите выполненную работу на сетевой ресурс – папку Контроль.

**Задание №13. Сделайте вывод по работе:**

Я познакомился:

Я научился (повторил):

Это важно для:

Оцените свою работу по приведенным ниже критериям. Запишите, какие трудности вам не удалось преодолеть.

Критерии оценки:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Умение | Умею делать хорошо | Получается не всегда | Над этим мне надо поработать |
|  | Поиск информации. |  |  |  |
|  | Структурировать информацию (в процессе заполнения таблицы) |  |  |  |
|  | Оценивать свою учебную деятельность по заданным критериям. |  |  |  |
|  | Формулировать алгоритм действий. |  |  |  |
|  | Выполнять проверку файлов на вирус. |  |  |  |
|  | Помещать файл в архив и извлекать файл из архива. |  |  |  |
|  | Работать с сетевой папкой. |  |  |  |

Мои затруднения:

|  |  |  |
| --- | --- | --- |
| № задания | Весовой коэффициент | Моя оценка |
| Задание 1 | 1 |  |
| Задание 2 | 1 |  |
| Задание 3 | 1 |  |
| Задание 4 | 1 |  |
| Задание 5 | 2 |  |
| Задание 6 | 1 |  |
| Задание 7 | 1 |  |
| Задание 8 | 1 |  |
| Задание 9 | 2 |  |
| Задание 10 | 1 |  |
| Задание 11 | 2 |  |
| Задание 12 | 2 |  |
| Задание 13 | 2 |  |
| ИТОГО: | 18 |  |

11-13 баллов удовлетворительно

14-16 баллов хорошо

17-18 баллов отлично

Мое количество баллов \_\_\_\_

Моя оценка \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_