**ПЛАН УРОКА №66**

 *ИНФОРМАТИКА* (по рабочему плану)

|  |  |  |
| --- | --- | --- |
| **дата** | **группа** | **РАЗДЕЛ 3. Средства информационных и коммуникационных технологий** |
| **Тема 3.3. Безопасность, гигиена, эргономика, ресурсосбережение.** |
| **Тема урока:** Защита информации, антивирусная защита |
| ***03.06.2020*** | **22 туризм** | **Распределение урока на основные этапы – урока** |
| Проверка посещаемости по журналу | Вопросы учащихся по предыдущему уроку | Повторение предыдущего материала | Изложение нового материала | Упражнения для закрепления пройденного материала | Задание на дом |
| **часы** | ***час***  | 5 | 5 | 5 | 15 | 10 | 5 |
| **цели** | *Изучение ПК и его деталей* |
| *Изучение понятий информатики* |
| *Проблемы при изучении информатики* |
| **Наглядные пособия к уроку** | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*Плакаты, схемы, иллюстрации наглядные и персональные компьютеры .* |
| **Основные вопросы для повторения** |
| **№****п/п** | **Содержание вопросов** |
| 1. | *Как организовывать интерес к уроку у учащихся* |
| 2. | *Что такое информатизация* |
| 3. | *Что такое измерение информации* |
| 4. | *Как измеряется информация* |
| **Изложение темы (узловые вопросы)** |
| **№****п/п** | **Содержание вопросов** |
| 1. | *Среда программирования* |
| 2. | *Языки программирования* |
| 3. | *Школьный алгоритмический* |
| 4. | *Бейсик, паскаль* |
| **Закрепление темы:** |
| **№****п/п** | **Содержание вопросов** |
| 1. | *Математические операции* |
| 2. | *Элементарные функции* |
| 3. | *Структура программы* |
| 4. | *Основные операторы для построения линейных алгоритмов* |
| **Домашнее задание**  |
| **№****п/п** | **Содержание вопросов** |
| 1. | *Персональный компьютер его организация* |
| 2. | *Конспектировать* |
| 3. | *Подведение итогов за день* |
| 4. | *Домашнее задание* |

**Мастер п/о:** *Алиева Ф.Г.*

*Информатика, 1 курс*

*03.06.2020г.*

*22 группа, туризм*

**Тема: Защита информации, антивирусная защита**

Антивирусные средства защиты.

Количество людей, пользующихся компьютером и сотовым телефоном, имеющим выход в Интернет, постоянно растет. Зна­чит, возрастает возможность обмена данными между ними по элект­ронной почте и через Всемирную сеть. Это приводит к росту угро­зы заражения компьютера вирусами, а также порчи или хищения информации чужими вредоносными программами, ведь основ­ными источниками распространения вредоносных программ яв­ляются электронная почта и Интернет. Правда, заражение может также произойти через дискету или CD-диск.

**Компьютерный вирус** — это целенаправленно созданная про­грамма, автоматически приписывающая себя к другим программным продуктам, изменяющая или уничтожающая их. Компьютерные вирусы могут заразить компьютерные программы, привести к потере дан­ных и даже вывести компьютер из строя.

Компьютерные вирусы могут распространяться и проникать в операционную и файловую систему ПК только через внешние магнитные носители (жесткий и гибкий диски, компакт-диски) и через средства межкомпьютерной коммуникации.

Вредоносные программы можно разделить на три класса: *черви, вирусы и троянские программы*.

**Черви** — это класс вредоносных программ, использующих для распространения сетевые ресурсы. Используют сети, электронную почту и другие информационные каналы для заражения компьютеров.

**Вирусы** — это программы, которые заражают другие програм­мы — добавляют в них свой код, чтобы получить управление при запуске зараженных файлов.

**Троянские программы** — программы, которые выполняют на поражаемых компьютерах несанкционированные пользователем действия, т.е. в зависимости от каких-либо условий уничтожают информацию на дисках, приводят систему к зависанию, воруют конфиденциальную информацию и т.д.

В зависимости *от среды обитания* вирусы можно разделить на *сетевые, файловые, загрузочные и файлово-загрузочные.*

**Сетевые** вирусы распространяются по различным компьютер­ным сетям.

**Файловые** вирусы внедряются главным образом в исполняемые модули, т.е. в файлы, имеющие расширения СОМ и ЕХЕ.

**Загрузочные** вирусы внедряются в загрузочный сектор диска или сектор, содержащий программу загрузки сис­темного диска.

**Файлово-загрузочные** вирусы заражают файлы и загрузочные сектора дисков.

*По способу заражения* вирусы разделяются *на резидентные и нерезидентные*.

**Резидентный** вирус при заражении компьютера оставляет в опе­ративной памяти свою резидентную часть, которая потом пере­хватывает обращение операционной системы к объектам зараже­ния (файлам, загрузочным секторам дисков и т.д.) и внедряется в них.

**Нерезидентные** вирусы не заражают память компьютера и явля­ются активными ограниченное время.

*По степени воздействия* выделяют **неопасные** вирусы, которые не мешают работе компьютера, **опасные**, которые могут привести к различным нарушениям в работе компьютера, и **очень опасные**, воздействие которых может привести к потере программ, унич­тожению данных, стиранию информации в системных областях диска.

Для обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов специальных программ, которые позволяют обнаруживать и уничтожать вирусы. Такие программы называются **антивирусными***.*

Различают следующие виды антивирусных программ:

1. **Программы-детекторы** осуществляют поиск характерной для конкретного вируса сиг­натуры в оперативной памяти и файлах и при обнару­жении выдают соответствующие сообщение. Недостатком таких антивирусных программ является то, что они могут находить только те вирусы, которые известны разра­ботчикам таких программ.
2. **Программы-доктора** или **флаги** не толь­ко находят зараженные вирусами файлы, но и возвращают файлы в исходное состояние. В начале своей работы флаги ищут вирусы в оперативной памя­ти, уничтожая их, и только затем переходят к «лечению» файлов.
3. **Программы-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. Обнаружение изменения выводится на экран монитора.
4. **Программы-фильтры** или **сторожа**, представляют собой не­большие резидентные программы, предназначенные для обна­ружения подозрительных действий при работе компьютера, ха­рактерных для вирусов:
	* попытка коррекции файлов с расшире­ниями СОМ и ЕХЕ;
	* изменение атрибутов файла;
	* прямая запись на диск по абсолютному адресу;
	* запись в загрузочные сектора диска;
	* загрузка резидентной программы.

При попытке вирусной атаки сторож посылает сообщение и предлагает запретить или разрешить соответствующие действия.

1. **Программы - вакцины** или **иммунизаторы** — это резидентные программы, предотвращающие заражение файлов.

Признаки заражения компьютера вирусом. Существует ряд при­знаков, свидетельствующих о заражении компьютера:

* + вывод на экран непредусмотренных сообщений или изобра­жений;
	+ подача непредусмотренных звуковых сигналов;
	+ неожиданное открытие и закрытие лотка CD-ROM-устрой­ства;
	+ произвольный, без вашего участия, запуск на компьютере каких-либо программ;
	+ вывод на экран предупреждения о попытке какой-либо из программ вашего компьютера выйти в Интернет, хотя вы никак не инициировали такое ее поведение (при наличии установлен­ной на вашем компьютере соответствующей антивирусной про­граммы).

Однако не всегда такие признаки вызываются присутствием вирусов. Иногда они могут быть следствием других причин. На­пример, в случае с почтой зараженные сообщения могут рассы­латься с вашим обратным адресом, но не с вашего компьютера.

Существуют и косвенные признаки заражения вашего компь­ютера:

* частые зависания и сбои в работе компьютера;
* медленная работа компьютера при запуске программ;
* невозможность загрузки операционной системы;
* исчезновение файлов и каталогов или искажение их содержи­мого;
* частое обращение к жесткому диску, когда часто мигает лам­почка на системном блоке;
* Microsoft Internet Explorer зависает или ведет себя неожидан­ным образом, например окно программы невозможно закрыть.

В 90 % случаев наличие косвенных симптомов вызвано сбоем в аппаратном или программном обеспечении. Несмотря на это при их появлении рекомендуем провести полную проверку компьюте­ра на наличие вирусов.

Если вы заметили, что ваш компьютер ведет себя подозри­тельно, придерживайтесь следующих правил.

1. Не паникуйте!
2. Отключите компьютер от Интернета.
3. Отключите компьютер от локальной сети, если он к ней был подключен.
4. Если симптом заражения заключается в том, что вы не може­те загрузиться с жесткого диска компьютера, т. е. компьютер вы­дает ошибку, когда вы его включаете, попробуйте загрузиться в режиме защиты от сбоев или с диска аварийной загрузки Windows.
5. Прежде чем предпринимать какие-либо действия, сохраните результаты вашей работы, записав их на внешний носитель (дис­кету, CD-диск, флэш-карту).
6. Установите антивирусную программу, если вы этого еще не сделали.
7. Получите последние обновления антивирусных баз.
8. Установите необходимые настройки антивирусной программы и запустите полную проверку.

**Мастер п/о:** *Алиева Ф.Г.*