

## **Конспект урока по теме: "Вредоносные и антивирусные программы. Компьютерные вирусы и защита от них"**

**Тип урока:** комбинированный урок.

### **Цели урока:**

- *Методическая:* показать эффективность применения компьютерной технологии при изучении темы.
- *Учебная:* дать знания о видах компьютерных вирусов, путях их распространения, об антивирусных программах и способах их использования на практике.
- *Развивающая:* развивать умение составлять конспект, компьютерную грамотность, познавательную активность учащихся, коммуникативных навыков.
- *Воспитательная:* воспитывать чувство ответственности, самостоятельность при принятии решений, толерантность, эрудицию, согласование.

### **Требования к знаниям:**

#### ***Учащиеся должны знать:***

- определение понятия «компьютерный вирус»;
- классификацию компьютерных вирусов;
- определение понятия «антивирусная программа»;
- типы антивирусных программ;
- правила предупреждения появления компьютерных вирусов;
- признаки заражения ПК компьютерным вирусом.

#### ***Учащиеся должны уметь:***

- обнаруживать и удалять вирусы с различных носителей.

### **Оснащение и методическое обеспечение урока:**

- ноутбуки;
- программное обеспечение: пакет MS Office 2013, антивирусная программа Eset NOD 32;
- опорный конспект, карточки с анкетой, инструкция о проведении практической работы;
- учебники, справочники, словари, интернет, телефоны, планшеты;
- доска, мел.

### **Методы работы:**

1. Словесный (беседа, изложение материала).
2. Наглядный (демонстрация учебного материала, опорный конспект).

3. Самостоятельная работа (работа по созданию презентаций, рисунков, диаграмм).
4. Практическая работа.

### **Ход урока.**

1. Орг.момент (1 мин).
2. Повторение (3 мин).
3. Работа в парах и группах (10-15 мин).
4. Выполнение практической работы (3-5 мин).
5. Анкетирование (1-2 мин).
6. Обсуждение (10-15 мин).
7. Подведение итогов, выставление оценок (3 мин).
8. Домашнее задание (2 мин).

#### **1. Орг.момент.**

Добрый день, коллеги! Здравствуйте, ребята! Давайте все подарим друг другу улыбку. Улыбка всеильна и стоит награды. Всего лишь улыбка - и Вам будут рады!

#### **2. Повторение.**

Сегодня на уроке мы проведем семинар, а пока давайте вспомним, что мы уже узнали о компьютерных вирусах и антивирусах при подготовке к семинару. Давайте ответим на вопросы теста.

#### **Выполнение теста.**

##### **1. Что такое компьютерный вирус?**

- 1) Прикладная программа.
- 2) Системная программа.
- 3) Программа, выполняющая на компьютере несанкционированные действия.
- 4) База данных.

##### **2. Основные типы компьютерных вирусов:**

- 1) Аппаратные, программные, загрузочные .
- 2) Программные, загрузочные, макровирусы.
- 3) Файловые, программные, макровирусы.
- 4) Файловые, загрузочные.

##### **3. Этапы действия программного вируса:**

- 1) Размножение, вирусная атака.
- 2) Запись в файл, размножение.
- 3) Запись в файл, размножение, уничтожение программы.
- 4) Размножение, уничтожение программы.

#### **4. В чем заключается размножение программного вируса?**

- 1) Программа-вирус один раз копируется в теле другой программы.
- 2) Вирусный код неоднократно копируется в теле другой программы.
- 3) Программа-вирус поражает многократно другие программы.
- 4) Вирусный код один раз копируется в теле другой программы.

#### **5. Что называется вирусной атакой?**

- 1) Неоднократное копирование кода вируса в код программы.
- 2) Отключение компьютера в результате попадания вируса.
- 3) Нарушение работы программы, уничтожение данных, форматирование жесткого диска.
- 4) Частое зависание компьютера и замедление его работы.

#### **6. Какие существуют методы реализации антивирусной защиты?**

- 1) Аппаратные и программные.
- 2) Программные, аппаратные и организационные.
- 3) Только программные.
- 4) Только аппаратные.

#### **7. Какие существуют основные средства защиты?**

- 1) Резервное копирование наиболее ценных данных.
- 2) Аппаратные средства.
- 3) Программные средства.
- 4) Аппаратные и программные средства.

#### **8. Какие существуют вспомогательные средства защиты?**

- 1) Аппаратные средства.
- 2) Программные средства.
- 3) Аппаратные средства и антивирусные программы.
- 4) Аппаратные и программные средства.

#### **9. На чем основано действие антивирусной программы?**

- 1) На ожидании начала вирусной атаки.
- 2) На сравнении программных кодов с известными вирусами.
- 3) На удалении зараженных файлов.
- 4) На обнаружении и удалении вируса.

#### **10. Какие программы относятся к антивирусным?**

- 1) AVP, DrWeb, Norton AntiVirus, AVAST.
- 2) MS-DOS, MS Word, AVP.
- 3) MS Word, MS Excel, Norton Commander.
- 4) DrWeb, Microsoft Security Essentials, MS Word, MS Excel.

### **Критерии оценки теста:**

- 9-10 правильных ответов – “5”
- 7-8 правильных ответов – “4”
- 5-6 правильных ответов – “3”
- меньше 5 – “2”

### **3. Работа в парах и группах.**

Учащиеся создают небольшие презентации (3-5 слайдов), работая в группах. По ходу выполнения работы, а также в ходе дальнейшего обсуждения заполняют лист с опорным конспектом.

### **4. Выполнение практической работы.**

Учащиеся, справившиеся с презентацией, выполняют практическую работу «Защита от вирусов: обнаружение и лечение». (Инструкция по проведению практической работы в приложении).

### **5. Анкетирование.**

В ходе выполнения работы все учащиеся и гости на уроке заполняют анкету. Анкетирование закрытое. Интересует ответ на вопрос: Какой антивирусной программой вы пользуетесь?

Обработкой результатов анкетирования займется 1 из учащихся по желанию.

### **6. Обсуждение.**

От каждой группы выступает по 1 представителю. Остальные учащиеся дополняют ответы.

1. Выступление Емельянова Вячеслава «Компьютерный вирус и классификация вирусов».
2. Выступление Чикалкиной Екатерины «Антивирусные программы. Виды антивирусов».
3. Выступление Шалаева Никиты «История компьютерных вирусов».
4. Выступление Андриянова Никиты с анализом анкет «Рейтинг антивирусных программ».
5. Выступление Кредышева Михаила «Распространение компьютерных вирусов».

6. Выступление Воробьевой Марии «Профилактика и лечение».
7. Выступление Семенова Кирилла «Правила защиты информации».
8. Выступление Фридрих Артема о результатах проведения практической работы.

**7. Подведение итогов, выставление оценок.**

**8. Домашнее задание:**

- 1. Дописать и выучить ОК (опорный конспект).**
- 2. Провести исследовательскую работу (по желанию):**
  - Рейтинг используемых антивирусных программ.
  - Способы обновления антивирусных программ.
- 3. Подготовить реферат на одну из тем (по желанию):**
  1. Антивирусные программы.
  2. Виды компьютерных вирусов.
  3. Методы борьбы с компьютерными вирусами.
- 4. Создать буклет-памятку «Правила защиты информации» (по желанию).**

**Практическая работа**  
**«Защита от вирусов: обнаружение и лечение»**

**Цель работы:** научиться использовать антивирусную программу ESET NOD32 Smart Security для проверки компьютера и дисков на наличие вирусов и его излечения.

**Задание:** Проверить диск E на наличие вирусов с использованием антивирусной программы.

**Ход практической работы:**

1. Запустите программу **ESET NOD32**.
2. Поиск вирусов - выбрать проверяемый диск (*предложенную флешку диск E или диск C*).
3. При обнаружении вирусов нажать кнопку «Лечить все» – «Удалить».
4. Просмотреть статистику

### Памятка

#### «Основные меры по защите компьютера от заражения вирусами»

- Необходимо оснастить компьютер современными антивирусными программами и постоянно обновлять их версии.
- При работе в глобальной сети обязательно должна быть установлена программа – фильтр (сторож, монитор).
- Перед считыванием с флеш-карт информации, следует всегда проверять эти диски на наличие вирусов.
- При переносе на свой компьютер файлов в архивированном виде необходимо их проверять сразу же после разархивации.
- Целесообразно делать архивные копии ценной информации на других носителях информации.
- Не следует оставлять флешку при включении или перезагрузке ПК, так как это может привести к заражению загрузочными вирусами.
- Следует иметь в виду, что невозможно заразиться вирусом, просто подключившись к Internet. Чтобы вирус активизировался, программа, полученная с сервера из сети, должна быть запущена на клиенте.
- Получив электронное письмо, к которому приложен исполняемый файл, не следует запускать этот файл без предварительной проверки. По электронной почте часто распространяются “троянские кони”.