**Урок по теме "Защита информации от вредоносных программ "**

**11 класс**

***Тема: «Защита информации от вредоносных программ»***

***Цели урока:***

1. Познакомить учащихся с различными видами компьютерных вирусов,

способов их распространения и профилактикой.

2*.* развивать теоретическое, критическое, творческое, аналитическое

мышление, формировать компьютерную грамотность учащихся, воспитывать информационную культуру учащихся, внимательность, аккуратность, дисциплинированность.

***Тип урока****:* комбинированный.

***Оборудование и используемое ПО:***

Компьютерный класс, ПК для каждого обучающегося, ПК для учителя, мультимедиа

проектор, экран и приложение:

ПРИЛОЖЕНИЕ 1. Защита информации от вредоносных программ — мультимедийная

презентация, созданная в среде MS PowerPoint

***План урока:***

I. Организационный момент, 2 мин.

II. Актуализация знаний, 5 мин.

III. Изучение нового материала, 28 мин.

IV. Закрепление изученного материала, 7 мин.

V. Подведение итогов урока. Рефлексия, 2.

***Ход урока:***

I. *Организационный момент*

Приветствие, проверка присутствующих. Объяснение темы, цели и хода урока.

Учитель: Сегодня мы приступаем к изучению новой темы: «Защита информации от

вредоносных программ ».

Задача урока: на уроке мы должны усвоить определение термина «компьютерный

вирус», разобраться с классификацией компьютерных вирусов, путем заражения,

способами профилактики и методами борьбы с компьютерными вирусами.

**II. Актуализация знаний**

Попросить детей назвать несколько общих признаков человека и компьютера. Сравнить

их по функциональным возможностям.

Далее высказать мысль о том, что человек, как биологический организм, подвержен

различным воздействиям внешней среды, и в том числе и различным заболеваниям,

причинами возникновения которых, иногда, являются вирусы и бактерии, проникающие в организм человека из вне.

Затем попросить детей попробовать описать этапы и последствия заражения человека

каким-либо вирусом и сделать акцент на следующие моменты:

• проникновение вируса в организм человека происходит из вне;

• способность вируса к саморазмножению;

• активизация некоторых вирусов не сразу после проникновения в организм, а через

некоторое время.

Потом спросить учащихся, может ли компьютер заразиться вирусом? Каким должен быть этот вирус по их представлению?

**III. Изучение нового материала**

***Учитель***: Вредоносными программами являются программы, наносящие вред данным и

программам, хранящимся на компьютере.

***Учитель***: Какие вы знаете вредоносные программы?

***Ученики*** отвечают

***Учитель:*** Основными типами вредоносных программ являются:

**• компьютерные вирусы;**

**• сетевые черви;**

**• троянские программы;**

**• программы показа рекламы (от англ. adware) и программы-шпионы, занимающиеся**

**сбором персональной информации о компьютере и пользователе (от англ. spy- ware);**

**• хакерские утилиты.**

За создание, использование и распространение вредоносных программ в России и

большинстве стран предусмотрена уголовная ответственность.

Компьютерные вирусы являются вредоносными программами, которые могут

«размножаться» и скрытно внедрять свои копии в исполнимые файлы, загрузочные

секторы дисков и документы. Активизация компьютерного вируса может вызывать

уничтожение программ и данных.

*Признаки заражения компьютера:*

• вывод на экран непредусмотренных сообщений;

• подача непредусмотренных звуковых сигналов;

• неожиданное открытие и закрытие лотка CD/DVD;

• произвольный запуск на компьютере каких-либо программ;

• частые «зависания» и сбои в работе компьютера;

• медленная работа компьютера при запуске;

• исчезновение или изменение файлов и папок;

• частое обращение к жѐсткому диску.

Учитель: Что может являться источником «заражения» компьютера?

Ученики отвечают.

Учитель: Источником «заражения» компьютера является:

• Дискета, на которой находятся заражѐнные вирусом файлы.

• Компьютерная сеть.

• Жѐсткий диск, на который попал вирус.

• Вирус, оставшийся в оперативной памяти после предшествующего пользователя.

**Классификация вирусов:**

По способу сохранения и исполнения своего кода вирусы можно разделить на:

1) файловые;

2) загрузочные;

3) макро;

4) скрипт-вирусы .

***Файловые вирусы*** различными способами внедряются в исполнимые файлы

(командные файлы 1.bat, программы \*.ехе, системные файлы \*.сот и \*.sys, программные

библиотеки \*.dll и др.) и обычно активизируются при их запуске. После запуска

зараженного файла вирус находится в оперативной памяти компьютера и является

активным (т. е. может заражать другие файлы) вплоть до момента выключения

компьютера или перезагрузки операционной системы.

*Профилактическая защита от файловых вирусов* состоит в том, что не рекомендуется запускать на исполнение файлы, полученные из сомнительного источника и предварительно не проверенные антивирусными программами.

***Загрузочные вирусы*** заражают загрузочный сектор гибкого или жесткого диска.

Принцип действия загрузочных вирусов основан на алгоритмах запуска операционной

системы при включении или перезагрузке компьютера. При заражении дисков

загрузочные вирусы «подставляют» свой код вместо программы, получающей

управление при загрузке системы, и отдают управление не оригинальному коду

загрузчика, а коду вируса.

*Профилактическая защита от таких вирусов* состоит в отказе от загрузки

операционной системы с гибких дисков и установке в BIOS вашего компьютера защиты

загрузочного сектора от изменений.

Наибольшее распространение получили ***макро-вирусы*** для интегрированного

офисного приложения Microsoft Office (Word, Excel, PowerPoint и Access). Макро-вирусы

фактически являются макрокомандами (макросами) на встроенном языке

программирования Visual Basic for Applications (VBA), которые помещаются в документ.

Вредные действия макро-вирусов реализуются с помощью встроенных макросов

(вставки текстов, запрета выполнения команд меню приложения и т. д.).

*Профилактическая защита от макро-вирусов* состоит в предотвращении запуска

вируса. При открытии документа в приложениях Microsoft Office сообщается о

присутствии в них макросов (потенциальных вирусов) и предлагается запретить их

загрузку. Выбор запрета на загрузку макросов надежно защитит ваш компьютер от

заражения макро-вирусами, однако отключит и полезные макросы, содержащиеся в

документе.

***Скрипт-вирусы***. Особой разновидностью вирусов являются активные элементы

(программы) на языках JavaScript или VBScript, которые могут содержаться в файлах

Web- страниц. Заражение локального компьютера происходит при их передаче по

Всемирной паутине с серверов Интернета в браузер локального компьютера.

*Профилактическая защита от скрипт-вирусов* состоит в том, что в браузере можно

запретить получение активных элементов на локальный компьютер.

**По величине вредных воздействий вирусы можно разделить на:**

1) **безвредные**, т.е. никак не влияющие на работу компьютера (кроме уменьшения

свободной памяти на диске в результате своего распространения);

2) неопасные, влияние которых ограничивается уменьшением свободной памяти на диске

и графическими, звуковыми и пр. эффектами;

3) **опасные** вирусы, которые могут привести к серьезным сбоям в работе компьютера;

4) **очень опасные**, в алгоритм работы которых заведомо заложены процедуры, которые

могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти, и даже, как гласит одна из непроверенных компьютерных легенд, способствовать быстрому износу движущихся частей механизмов - вводить в резонанс и разрушать головки некотоорых типов винчестеров.

**Схема работы компьютерных вирусов:**

***Заражение*** (происходит при запуске инфицированной программы или при обращении к

носителю, имеющему вредоносный код в системной области; обычно код вируса сначала

поступает в оперативную память работающего компьютера, откуда он копируется на

запоминающие устройства).

***Размножение*** (происходит как серия последовательных заражений; в первую очередь

поражаются файлы самой операционной системы, чем чаще срабатывает механизм, тем

больше файлов поражается).

***Атака*** (последняя фаза развития вируса; во время атаки вирус производит более или

менее разрушительные действия и при этом непременно проявляет себя).

**Действия при наличии признаков заражения компьютера:**

Прежде чем предпринимать какие-либо действия, необходимо сохранить

результаты работы на внешнем носителе (дискете, СD- или DVD-диске, флэш-

карте и пр.). Далее необходимо:

• отключить компьютер от локальной сети и Интернета, если он к ним был

подключен;

• если симптом заражения состоит в том, что невозможно загрузиться с

жесткого диска компьютера (компьютер выдает ошибку, когда вы его выключаете)

* попробовать загрузиться в режиме защиты от сбоев или с диска аварийной загрузки Windows;

• запустить антивирусную программу.

**Принцип** работы ***антивирусных*** программ основан на проверке файлов, загрузочных секторов дисков и оперативной памяти, поиске в них известных и новых вирусов, лечении «заражѐнных» вирусами файлов или их удалении.

1. Рассмотрим антивирусную программу **Антивирус Касперского**.

В его состав входят:

Kaspersky Anti Virus Сканер,

Kaspersky AntiVirus Монитор,

Kaspersky AntiVirus Центр управления.

AVP Сканер имеет удобный пользовательский

интерфейс, большое количество настроек, выбираемых пользователем, а также одну из

самых больших в мире антивирусных баз, что гарантирует надежную защиту от

огромного числа самых разнообразных вирусов: полиморфных или самошифрующихся

вирусов; стелс-вирусов или вирусов-невидимок; макро вирусов, заражающих документы

Word и таблицы Excel.

AVP Сканер проверяет на наличие вирусов оперативную память, файлы, включая

архивные и упакованные, системные сектора, содержащие Master Boot Record,

загрузочный сектор (Boot-сектор) и таблицу разбиения диска (Partition Table).

AVP Монитор – резидентный модуль, находящийся постоянно в оперативной памяти

компьютера и отслеживающий все файловые операции в системе. Позволяет обнаружить

и удалить вирус до момента реального заражения системы в целом.

AVP Центр управления обеспечивает удобный пользовательский интерфейс, создание,

сохранение и загрузку большого количества различных настроек, механизм проверки

целостности антивирусной системы, мощную систему помощи.

IV. **Закрепление изученного материала**

Практическое задание. Провести комплексную проверку компьютера с помощью

программы «Антивирус Касперского».

1 Проверка флеш-карты на вирусы.

Самый частый путь попадания вирусов в компьютер – с флеш-карты. При

установке любой флеш-карты рекомендуется сразу провести проверку на вирусы, прежде

чем открывать документы с карты или сохранять на нее файлы. Для проверки выполните

следующие действия:

1. Зайти в «Мой компьютер»

2. Навести курсор мыши на значок диска флеш-карты

3. Вызвать контекстное меню нажатием правой кнопкой «мыши»

2. Проверка компьютера на вирусы и обновление антивирусных баз.

Не реже 1 раза в неделю рекомендуется проводить полную проверку компьютера

на вирусы. Перед тем, как проводить проверку компьютера, необходимо обновить

антивирусные базы. Для этого:

1. Навести курсор мыши на значок «Антивируса Касперского» в правом

нижнем углу экрана на панели задач

Рисунок 5 – Значок «Антивируса Касперского»

2. Вызвать правой кнопкой «мыши» контекстное меню

Рисунок 6 – Запуск обновления

3. Запустить пункт «Обновление». Запуститься процесс обновления (рисунок 7).

После завершения обновления необходимо запустить проверку компьютера. Для этого контекстном меню выбрать пункт «Проверка Моего Компьютера»

3. Выборочная проверка дискет, флеш-накопителей, логических дисков на вирусы.

1. Открываем антивирусную программу «Касперский» щелкнув два раза левой

кнопкой «мыши» на значке в правом нижнем углу экрана на панели задач (рисунок 9)

2. Нажимаем надпись «Поиск вирусов» (рисунок 10)

а) Версия для Windows XP; б) Версия для Windows 7.

3. Выбираем галочками объекты проверки и нажимаем значок

(рисунок)

V. Подведение итогов урока

**Тест по теме: *«Защита информации*» 11 кл.**

**1. Защита информации в системах и сетях -это**   
A. системное обеспечение надежности информации;   
B. процесс обработки информации;   
C. программы -ревизор;   
D. аппаратное средство;   
E. программное средство.   
**2. Объект защиты информации - это**  
A. структурный компонент системы, содержащий информацию, подлежащей защите;   
B. совокупность данных, содержащая информацию, подлежащей защите;   
C. операционная система;   
D. драйверы;   
E. архиваторы;   
**3. Элемент защиты информации - это**   
A. структурный компонент системы, содержащий информацию, подлежащей защите;   
B. совокупность данных, содержащая информацию, подлежащей защите;   
C. узел связи;   
D. накопители;   
E. средства отображения информации;   
**4. Защитить информацию – это значит**   
A. обеспечить физическую целостность информации;   
B. не допустить несанкционированного получения информации;   
C. использовать антивирусные программы;   
D. использовать программу -ревизор.   
E. все ответы правильные;   
**5. Какая из ниже перечисленных программ является ревизором:**   
A. Adinf;  B. DrWeb;  C. Sherif;  D. Aidstest;  E. Dir-I.   
**5. Что делает программа-детектор:**   
A. находит зараженные файлы и лечит их;   
B. ищет вирусы с известной сигнатурой;   
C. сравнивает исходное состояние файла с текущим;   
D. обнаруживает подозрительные действия;   
E. предотвращает заражение файлов.   
**6. Программа доктор (фаг):**   
A. ищет вирусы с известной сигнатурой;   
B. предотвращает заражение файлов;   
C. находит зараженные файлы и лечит их;   
D. сравнивает исходное состояние файла с текущим;   
E. обнаруживает подозрительные действия.   
**7. Программа-ревизор:**   
A. обнаруживает подозрительные действия;   
B. предотвращает заражение файлов;   
C. ищет вирусы с известной сигнатурой;   
D. сравнивает исходное состояние файла с текущим;   
E. находит зараженные файлы и лечит их.   
**8. Программа-фильтр:**   
A. предотвращает заражение файлов;   
B. ищет вирусы с известной сигнатурой;   
C. сравнивает исходное состояние файла с текущим;   
D. находит зараженные файлы и лечит их;   
E. обнаруживает подозрительные действия.   
392. Какая программа находит зараженные файлы и лечит их   
A. Программа-фильтр.   
B. Программа-вакцина.   
C. Программа-ревизор.   
D. Программа доктор (фаг).   
E. Программа-детектор.   
**9. Программа-вакцина:**   
A. модифицируют программы и диски   
B. находит зараженные файлы и лечит их;   
C. сравнивает исходное состояние файла с текущим;   
D. обнаруживает подозрительные действия;   
E. ищет вирусы с известной сигнатурой.   
**10. Методы защиты от компьютерных вирусов**   
A. Общие средства защиты, профилактические меры, специализированные программы;   
B. Троянский Конь, профилактические меры, специализированные программы;   
C. Общие средства защиты, профилактические меры, программы закладки и сетевые черви;   
D. Win9E.CIH, профилактические меры, специализированные программы;   
E. Общие средства защиты, профилактические меры, Win9E.CIH.   
**11. Разновидности средств защиты информации**   
A. копирование информации, разграничение доступа;   
B. копирование информации, программы закладки и сетевые черви;   
C. Троянский Конь, разграничение доступа;   
D. копирование информации, Троянский Конь ;   
E. программы закладки и сетевые черви.   
**12. Что такое антивирус?**   
A. Это специальная программа, написанная для конкретных вирусов;   
B. 100% защита от вируса;   
C. Загрузочные файлы;   
D. модифицирующие программы;   
E. резидентные файлы.   
**13. Устройство управления (УУ) вырабатывает:**   
A. переработку информации, хранимой в оперативной памяти (ОП);   
B. сигналы, обеспечивающие выборку и выполнение команд;   
C. хранение промежуточных результатов;   
D. обработку данных;   
E. связывает пользователя с внешним миром.   
**14. К печатающим устройствам относятся**:   
A. НГМД;  B. НЖМД;  C. НГМД и НЖМД;  D. Стример;  E. Принтер.   
**15. Основное преимущество командного режима управления системой состоит**:   
A. в простоте необходимых технических и программных средств;   
B. в высокой скорости взаимодействия пользователя с системой;   
C. в простоте, наглядности и удобстве взаимодействия с системой;   
D. в простоте достижения результатов;   
E. все ответы верны.   
**16. Для командного режима управления системой MS DOS характерно:**A. минимальные требования к мощности компьютера;   
B. необходимость знать правила написания команд;   
C. все ответы верны;   
D. невысокая скорость взаимодействия из-за необходимости ввода команд с клавиатуры;   
E. простая программная реализация.

***Закрепление изученного материала***

Демонстрация презентации, работа с карточками.

***Домашнее задание***

Изучение материала учебника.

Разработка мониторинга популярности современных антивирусных программ в графическом виде.