

**Конспект урока по информатике и ИКТ
в 7 классе на тему
“Компьютерные вирусы и антивирусные программы”**

Урок: Информатика, 7 класс.

Тема: Компьютерные вирусы и антивирусные программы

Тип урока: урок изучения нового материала.

Оборудование: ноутбук, проектор, выход в Интернет.

Цель урока: ознакомить учащихся с путями распространения и методами борьбы с компьютерными вирусами

Предметные:

Сформировать понятие компьютерного вируса;

Классифицировать компьютерные вирусы;

Ознакомится с основными методиками борьбы с вирусами;

Метапредметные:

развитие творческого мышления, необходимого для познания практической деятельности

Личностные:

Формировать умения управлять своей познавательной деятельностью.

создать условия для воспитания желания активного участия в образовательном процессе;

| Этап урока | Содержание этапа (деятельность учителя и деятельность обучающихся) | Педагогическая целесообразность этапа |
|--------------------------|--|---|
| 1.Организационный момент | Приветствие класса, контроль отсутствующих, техника безопасности в кабинете информатики | |
| 2.Постановка целей урока | Компьютер – это электронный аналог человека. Человек, как любой биологический организм, подвергается воздействию различных вирусов? Сколько существует компьютерных вирусов, как они классифицируются, как они ведут себя попав в организм «компьютера»? Каковы последствия заражения вирусами компьютера? | Рассказ о целях урока |
| 3.Актуализация знаний | Сравните общие признаки человека и компьютера. Сравните их функциональные возможности. Почему болеет человек? Причины возникновения заболевания разные вирусы и микробы. Чтобы от них защититься, необходимо соблюдать правила личной гигиены. Почему заразившийся человек только через несколько дней чувствует недомогание? | Демонстрация ЭОР (Раздел «Ниша для паразита») |

| | | |
|--|---|--|
| | <p>Так как компьютер сконструирован по аналогии с человеком он тоже может болеть.</p> <p>Приходилось ли вам встречаться с этой проблемой в процессе эксплуатации компьютера?</p> <p>Каким должен быть вирус по вашему представлению?</p> | |
| <p>4. Теоретический материал урока «вирусы и их классификация»</p> | <p>Мы с вами говорили о том, что компьютер можно в чем-то сравнить с человеком. Человек, как биологический организм подвержен различным воздействиям внешней среды, в том числе и различным заболеваниям, причинами возникновения которых, часто, являются вирусы и бактерии, проникающие в организм человека извне.</p> <p>Попробуйте описать этапы и последствия заражения человека каким-либо вирусом. Особенности:</p> <ul style="list-style-type: none"> · проникновение вируса в организм человека происходит извне; · способность вируса к саморазмножению; · активизация некоторых вирусов не сразу после проникновения в организм, а через некоторое время. <p>А может ли компьютер заразиться вирусом? Каким должен быть этот вирус по вашему представлению?</p> <p>1) Понятие «компьютерный вирус»</p> <p>Итак, действительно, компьютер может заразиться. И причиной заражения действительно является вирус, только компьютерный. Это название пришло из биологии именно по признаку способности к саморазмножению. Вирусы представляют собой небольшие вредоносные программы, которые запускаются на компьютере без ведома его хозяина и выполняют различные нежелательные действия. При этом вирусы могут быть как почти безобидными, так и весьма неприятными.</p> <p>Компьютерный вирус – это программа, которая может создавать свои копии и внедрять их в файлы, загрузочные секторы дисков, сети. При этом копии сохраняют возможность дальнейшего распространения. Часто вирусы обладают разрушительным действием.</p> <p>2) Пути распространения компьютерных вирусов</p> <p>Давайте подумаем, каковы пути распространения вирусов. (Вирусы могут попасть в ПК так же как любая другая программа). В противоположность обычным</p> | <p>Демонстрация ЭОР (Раздел «Компьютерные вирусы и вредоносные программы»)</p> |

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.

3) 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.

4) История компьютерной вирусологии

Первые вирусы появились давно, еще на заре эпохи ЭВМ, и не всегда были вредоносными. Например, в конце 60-х в лаборатории Хегох 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.

5) 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.

6) 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.

7) Классификация вирусов

Существует несколько разных классификаций вредоносных программ.

Наиболее распространенная из них делит *вирусы по среде их обитания*. Согласно ей компьютерные вирусы бывают файловые, сетевые, загрузочные и макровирусы.

Файловые вирусы – это программы, которые поражают исполняемые файлы операционной системы и пользовательских приложений. Чаще всего они внедряются в файлы с расширениями com, exe, bat, sys, dll. Такие вирусы обнаружить и обезвредить проще всего. Радует также, что проявить свою вредоносную активность они могут только после запуска зараженной программы.

Нередко из файловых вирусов

выделяют отдельный подтип, который называют **макровирусами**. Они также обитают в файлах, но не программ, а документах пользователя и шаблонах (doc, dot, xls, mdb и др.). Для их создания используется язык макрокоманд. Поэтому, чтобы обезопасить себя от макровирусов, необходимо отключить автозапуск макросов при открытии документов.

Сетевые вирусы в качестве среды обитания используют глобальную или локальные компьютерные сети. Они не сохраняют свой код на жестком диске компьютера, а проникают напрямую в оперативную память ПК. Вирусы этого типа за способность вычислять сетевые адреса других машин, находясь в памяти компьютера, и самостоятельно рассылать по этим адресам свои копии называют сетевыми червями. Такой вирус может находиться одновременно в памяти нескольких компьютеров. Сетевые вирусы обнаружить сложнее, чем файловые. Сетевые вирусы распространяются с большой скоростью и могут сильно замедлить работу аппаратного обеспечения компьютерной сети.

Среда обитания **загрузочных вирусов** – специальные области жестких и гибких дисков, которые служат для загрузки операционной системы. Для заражения вирусы используют главную загрузочную запись винчестера. Загрузочный вирус подменяет оригинальную запись и перехватывает управление системой. Такие вирусы обнаружить и удалить сложнее всего, поскольку они начинают свою работу еще до загрузки антивирусных приложений. Они же представляют наибольшую опасность.

Еще одна существующая *классификация вирусов* – по их деструктивным 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 строя программ и ОС или рассекречивании конфиденциальных данных.

Все компьютерные вирусы бывают двух типов – резидентные и нерезидентные.

Резидентные вирусы представляют собой программы, присутствующие в оперативной памяти либо хранящие там свою активную часть, которая постоянно заражает те или иные объекты операционной системы.

Нерезидентные вирусы загружаются лишь во время открытия зараженного файла или работы с инфицированным приложением.

Как несложно догадаться, наибольшую опасность представляют резидентные вирусы, так как время их активной работы ограничивается только выключением или перезагрузкой всей системы, а не отдельного приложения.

По особенностям алгоритма работы различают:

Простейшие вирусы – вирусы, которые при распространении своих копий обязательно изменяют содержимое дисковых секторов или файлов, поэтому его достаточно легко обнаружить.

Вирусы-спутники (компаньоны) - вирус, который не внедряется в сам исполняемый файл, а создает его зараженную копию с другим расширением.

Стелс-вирус (невидимка) – вирусы, скрывающие свое присутствие в зараженных объектах, подставляя вместо себя незараженные участки.

Полиморфные вирусы (мутанты) – вирусы, модифицирующие свой код таким образом, что копии одного и того же вируса не совпадали.

Макровирус – вирусы, которые заражают документы офисных приложений.

Троянская программа – программа, которая маскируется под полезные

| | | |
|--|--|---|
| | <p>приложения (утилиты или даже антивирусные программы), но при этом производит различные шпионские действия. Она не внедряется в другие файлы и не обладает способностью к саморазмножению.</p> <ul style="list-style-type: none"> · Черви – это вредительские компьютерные программы, которые способны саморазмножаться, но, в отличие от вирусов не заражают другие файлы. Свое название черви получили потому, что для распространения они используют компьютерные сети и электронную почту. <p>Сегодня наиболее распространены так называемые сетевые черви, а также макровирусы.</p> <p>8) Профилактика появления компьютерных вирусов</p> <p>Одним из основных методов борьбы с вирусами является, как и в медицине, своевременная профилактика. Подумайте, какие средства помогают предотвратить заражение ПК?</p> <ul style="list-style-type: none"> · резервное копирование наиболее ценных данных; · создание дистрибутивного и системного диска; · хранение всех регистрационных и парольных данных не на ПК; · проверка всей поступающей извне информации на вирусы, как на дискетах, CD-ROM, так и по сети; · использование «свежих» антивирусных программ, регулярная проверка компьютера на наличие вирусов. | |
| <p>5. Теоретический материал урока «антивирусное ПО»</p> | <p>Антивирусные программы</p> <p>Итак, особое место в этом списке занимают программные средства защиты – антивирусные программы. К какому виду ПО они относятся? (Системному ПО).</p> <p>Антивирусная программа (антивирус) - программа, позволяющая выявлять вирусы, лечить зараженные файлы и диски, обнаруживать и предотвращать подозрительные действия.</p> <p>Существует несколько типов антивирусных программ, различающихся выполняемыми функциями.</p> <ul style="list-style-type: none"> · Полифаги. Просмотр содержимого файлов, расположенных на дисках компьютера, а также содержимого оперативной | <p>Демонстрация ЭОР (Раздел «Антивирусное программное обеспечение»)</p> |

| | | |
|---------------------------|---|---|
| | <p>памяти компьютера с целью поиска вирусов.</p> <p>Ревизоры. В режиме предварительного сканирования создает базу данных с контрольными суммами и другой информацией, позволяющей впоследствии контролировать целостность файлов (контроль над изменениями, которые происходят в файловой системе ПК).</p> <p>Блокировщики. Проверка на наличие вирусов запускаемых файлов, перехват «вирусоопасных» ситуаций.</p> <p>Ни один тип антивирусных программ по отдельности не дает полной защиты от вирусов. Поэтому в современные антивирусные комплекты программ обычно входят компоненты, реализующие все эти функции.</p> | |
| 6. Закрепление материала | Класс путем «мозгового штурма» отвечает на вопросы теста. Учитель комментирует ответы учащихся. В заключении дети получают памятки «Основные меры по защите компьютера от заражения вирусами» | Проведение интерактивного теста, комментарии к ответам учащихся |
| 7. Самостоятельная работа | Учащиеся пересаживаются за отвечать на тест самостоятельно. | Домашнее задание записано в электронном дневнике |
| 8. Домашнее задание | <p>7. Домашнее задание.</p> <p>1) Повторить тему с помощью электронной презентации и конспекта урока.</p> <p>2) Ознакомиться с памяткой «Основные меры по защите компьютера от заражения вирусами».</p> <p>3) Заполнить в виде файла таблицу и выслать на электронную почту учителя.</p> <p>Приложение 1.</p> | Домашнее задание записано в электронном дневнике |

| Тип вируса | Источник заражения | Объект заражения | Последствия заражения |
|-------------------|---------------------------|-------------------------|------------------------------|
| Загрузочные | | | |
| Файловые | | | |
| Макро-вирусы | | | |
| Сетевые | | | |

ПЕРЕЧЕНЬ ИСПОЛЬЗУЕМЫХ НА ДАННОМ УРОКЕ ЭОР

| № | Название ресурса | Тип, вид ресурса | Форма предъявления информации (иллюстрация, презентация, видеофрагменты, тест, модель и т.д.) | Гиперссылка на ресурс, обеспечивающий доступ к ЭОР |
|----|--|------------------|--|---|
| 1. | «Убить дракона» | текст | <i>текст</i> | http://school-collection.edu.ru/catalog/res/a6eea4f3-a746-9a0e-1628-19e07ed1fa66/view/ |
| 2. | Компьютерные вирусы и антивирусные программы | Анимация | <i>презентация</i> | http://fcior.edu.ru/card/28568/kompyuternye-virusy-i-antivirusnye-programmy.html |
| 3. | Компьютерные вирусы и антивирусные программы | Анимация | <i>тест</i> | http://fcior.edu.ru/card/28660/kompyuternye-virusy-i-antivirusnye-programmy.html |
| 4. | Информационная безопасность | Анимация | <i>презентация</i> | http://school-collection.edu.ru/catalog/res/87d97129-025d-455d-85c8-d7b6becf58ae/view/ |
| 5. | Компьютерные вирусы и антивирусные программы | Анимация | <i>тест</i> | http://fcior.edu.ru/card/28676/kompyuternye-virusy-i-antivirusnye-programmy.html |
| 6. | Компьютерные вирусы | Анимация | <i>презентация</i> | http://festival.1september.ru/articles/573484/pril.ppt |

| | | | | |
|----|---|-------|--------------|---|
| 7. | Памятка «Основные меры по защите компьютера от заражения вирусами» | текст | <i>текст</i> | http://festival.1september.ru/articles/573484/pril2.doc |
|----|---|-------|--------------|---|