|  |
| --- |
| Цель урока: изучить опасные угрозы сети Интернет и методы борьбы с ними. Задачи:  Образовательная: познакомиться с понятием «Интернет», «Вирус», изучить приемы безопасности при работе в сети Интернет;  Развивающая: развитие интереса к предмету, информационной культуры; формирование приёмов логического мышления; развитие способность анализировать и обобщать, делать выводы;  Воспитательная: воспитание аккуратности, точности, самостоятельности, привитие навыки групповой работы, сотрудничества;  Здоровьесберегающая: соблюдение санитарных норм при работе с компьютером, соблюдение правил техники безопасности, оптимальное сочетание форм и методов, применяемых на уроке;   Оборудование: ПК, проектор, экран, тетради, презентация «Безопасность в сети Интернет».   Ход урока:  (сопровождается показом слайдов презентации)   1. Организационный момент.  сообщение темы урока, его целей и задач;   краткий план деятельности.  2. Введение в тему подготовить детей к восприятию темы;  нацелить на продуктивную работу.  Сегодня наш урок посвящен теме «Безопасность в сети Интернет» Интернет – это объединенные между собой компьютерные сети, глобальная мировая система передачи информации с помощью информационно-вычислительных ресурсов.  На сегодняшний день практический каждый человек, так или иначе, пользуется сетью Интернет. Возможности Интернет безграничны: учеба, поиск необходимой информации, перевод денежных средств, отдых и многое другое. Однако, многие пользователи даже не задумываются о том, какая опасность поджидает нас во всемирной паутине.  Давайте подумаем и вспомним, какие угрозы вы уже встречали во время работы за компьютером, а может, о каких-то угрозах, вы слышали от своих друзей? (ответ учащихся)  3. Объяснение нового материала. А теперь давайте обратимся к статистике в сети Интернет. Рейтинг самых опасных угроз распределяется следующим образом (Слайд 3):  1. Вредоносные программы  2. Кража информации  3. Халатность сотрудников  4. Хакерские атаки  5. Финансовое мошенничество  6. Спам  7. Аппаратные и программные сбои  Как вы видите, угроз достаточно много и все они связаны между собой, например, из-за халатности сотрудников может произойти кража информации, а кража информации в свою очередь, может быть связана с финансовым мошенничеством.  Но, конечно же, лидером среди угроз являются вирусы. Давайте посмотрим, что такое вирусы, и какими они бывают.  Компью́терный ви́рус —Ν разновидность компьютерных программ или вредоносный код, отличительной особенностью которых является способность к размножению (саморепликация).  Классификация . В настоящее время не существует единой системы классификации и именования вирусов. Принято разделять вирусы на следующие группы.  По поражаемым объектам Файловые вирусы. Это вирусы-паразиты, которые при распространении своих копий обязательно изменяют содержимое исполняемых файлов, при этом файлы, атакованные вирусом, в большинстве случаев полностью или частично теряют работоспособность)  Загрузочные вирусы. Это компьютерные вирусы, записывающиеся в первый сектор гибкого или жесткого диска и выполняющиеся при загрузке компьютера.  Скриптовые вирусы. Требуют наличия одного из скриптовых языков (Javascript, VBScript) для самостоятельного проникновения в неинфицированные скрипты.  Макровирусы. Это разновидность компьютерных вирусов разработанных на макроязыках, встроенных в такие прикладные пакеты ПО, как Microsoft Office.  Вирусы, поражающие исходный код. Вирусы данного типа поражают или исходный код программы, либо её компоненты (OBJ-, LIB-, DCU- файлы) а так же VCL и ActiveX компоненты.  По поражаемым операционным системам и платформам  DOSΝ   Microsoft WindowsΝ   UnixΝ   LinuxΝ  По технологиям, используемым вирусом  Полиморфные вирусы. Вирус, который при заражении новых файлов и системных областей диска шифрует собственный код.  Стелс-вирусы. Вирус, полностью или частично скрывающий свое присутствие в системе, путем перехвата обращений к операционной системе, осуществляющих чтение, запись, чтение дополнительной информации о зараженных объектах (загрузочных секторах, элементах файловой системы, памяти и т. д.)  Руткит. Программа или набор программ для скрытия следов присутствия злоумышленника или вредоносной программы в системе.  По языку, на котором написан вирус   ассемблерΝ   высокоуровневый языкΝ программирования   скриптовый языкΝ   и др.Ν  По дополнительной вредоносной функциональности  Бэкдоры. Программы, которые устанавливает взломщик на взломанном им компьютере после получения первоначального доступа с целью повторного получения доступа к системе  Шпионы. Spyware — программное обеспечение, осуществляющее деятельность по сбору информации о конфигурации компьютера, деятельности пользователя и любой другой конфиденциальной информации без согласия самого пользователя.  Ботнеты. Это компьютерная сеть, состоящая из некоторого количества хостов, с запущенными ботами — автономным программным обеспечением. Обычно используются для нелегальной или неодобряемой деятельности — рассылки спама, перебора паролей на удалённой системе, атак на отказ в обслуживании.   Каждый день появляются все новые и новые вирусы. Вам необходимо знать, что создание и распространение вредоносных программ (в том числе вирусов) преследуется в России согласно Уголовному кодексу РФ (глава 28, статья 273).  Также в нашей стране существует доктрина информационной безопасности РФ, согласно которой в России должен проводиться правовой ликбез в школах и вузах при обучении информатике и компьютерной грамотности по вопросам защиты информации в ЭВМ, борьбы с компьютерными вирусами, детскими порносайтами и обеспечению информационной безопасности в сетях ЭВМ.   Поэтому сегодня я расскажу вам о том, как обезопасить себя, свих друзей, свой личный или рабочий компьютер, чтобы не стать жертвой сетевых угроз.  . Как же бороться с сетевыми угрозами?  1. Установите комплексную систему защиты.  Установка обычного антивируса – вчерашний день. Сегодня актуальны так называемые «комплексные системы защиты», включающие в себя антивирус, файрволл, антиспам-фильтр и еще пару-тройку модулей для полной защиты вашего компьютера. Новые вирусы появляются ежедневно, поэтому не забывайте регулярно обновлять базы сигнатур: лучше всего настроить программу на автоматическое обновление.  2. Будьте осторожны с электронной почтой  Не стоит передавать какую-либо важную информацию через электронную почту. Установите запрет открытия вложений электронной почты, поскольку многие вирусы содержатся во вложениях и начинают распространяться сразу после открытия вложения. Программы Microsoft Outlook и Windows Mail помогают блокировать потенциально опасные вложения.  3. Пользуйтесь браузерами Mozilla Firefox, Google Chrome и Apple Safari.  Большинство червей и вредоносных скриптов ориентированы под Internet Explorer и Opera. В рейтинге популярности лидирует IE, но лишь потому, что он встроен в Windows. Браузер Opera очень популярен в России из-за ее призрачного удобства и очень большого числа настроек. Уровень безопасности имеет ряд недостатоков как у одного, так и у второго браузера, поэтому лучше ими не пользоваться вовсе.  4. Обновляйте операционную систему Windows. (Слайд 33)  Постоянно обновляйте операционную систему Windows. Корпорация Microsoft периодически выпускает специальные обновления безопасности, которые могут помочь защитить компьютер. Эти обновления могут предотвратить вирусные и другие атаки на компьютер, закрывая потенциально опасные точки входа.  5. Не отправляйте SMS-сообщения.  Сейчас очень популярны сайты, предлагающие доступ к чужим SMS и распечаткам звонков, также очень часто при скачивании файлов вам предлагают ввести свой номер, или внезапно появляется блокирующее окно, которое якобы можно убрать с помощью отправки SMS.  При отправке SMS, в лучшем случае, можно лишиться 300-600 рублей на счету телефона – если нужно будет отправить сообщение на короткий номер для оплаты, в худшем – на компьютере появится ужасный вирус.  Поэтому никогда не отправляйте SMS-сообщения и не вводите свой номер телефона на сомнительных сайтах при регистрации.  6. Пользуйтесь лицензионным ПО.  Если вы скачиваете пиратские версии программ или свеженький взломщик программы, запускаете его и сознательно игнорируете предупреждение антивируса, будьте готовы к тому, что можете поселить вирус на свой компьютер. Причем, чем программа популярнее, тем выше такая вероятность.  Лицензионные программы избавят Вас от подобной угрозы!  7. Используйте брандмауэр.  Используйте брандмауэр Windows или другой брандмауэр оповещают о наличии подозрительной активности при попытке вируса или червя подключиться к компьютеру. Он также позволяет запретить вирусам, червям и хакерам загружать потенциально опасные программы на компьютер.  8. Используйте сложные пароли.  Как утверждает статистика, 80% всех паролей — это простые слова: имена, марки телефона или машины, имя кошки или собаки, а также пароли вроде 123. Такие пароли сильно облегчают работу взломщикам. В идеале пароли должны состоять минимум из семи, а лучше двенадцати символов. Время на подбор пароля из пяти символов — два-четыре часа, но чтобы взломать семисимвольный пароль, потребуется два-четыре года. Лучше использовать пароли, комбинирующие буквы разных регистров, цифры и разные значки.  9. Делайте резервные копии. При малейшей угрозе ценная информация с вашего компьютера может быть удалена, а что ещё хуже – похищена. Возьмите за правило обязательное создание резервных копий важных данных на внешнем устройстве – флеш-карте, оптическом диске, переносном жестком диске.  10. Функция «Родительский контроль» обезопасит вас.  Для детской психики Интернет – это постоянная угроза получения психологической травмы и риск оказаться жертвой преступников.  Не стремитесь утаивать от родителей круг тем, которые вы обсуждает в сети, и новых Интернет-знакомых, это поможет вам реально оценивать информацию, которую вы видите в сети и не стать жертвой обмана.   Соблюдая эти не сложные правила, вы сможете избежать популярных сетевых угроз.   5. Самостоятельная работа Закрепление материала - компьютерное тестирование.  А теперь, давайте проверим, насколько внимательно вы сегодня слушали данный материал.   Займите места за компьютером.  Загрузите⎫ программу My Test Student.   Выберите файл «Безопасность в сети Интернет» Тест содержит 10 вопросов, в каждом вопросе есть только один правильный ответ.  По результатам теста, вы увидите окно со своим результатам. Оценка, которую поставит вам компьютер, и будет вашей оценкой за сегодняшний урок.  Тест:  1. Закончите предложение: Создание и распространение вредоносных программ (в том числе вирусов) преследуется в России согласно…  A. Административному кодексу  B. Трудовому кодексу  C. Уголовному кодексу  D. Гражданскому кодексу  2. Какой классификации вирусов на сегодняшний день не существует?  A. По поражаемым объектам  B. По поражаемым операционным системам и платформам  C. По количеству поражаемых файлов  D. По дополнительной вредоносной функциональности  3. Какой из приведенных паролей является более надежным  A. 123456789  B. qwerty  C. annaivanova  D. 13u91A\_Ivanova  4. Для того, чтобы антивирусные программы обеспечивали наилучшую безопасность вашего ПК, необходимо:  A. Установить несколько антивирусных программ  B. Удалить все файлы, загруженные из сети Интернет  C. Своевременно обновлять антивирусные базы  D. Отключить компьютер от сети Интернет  5. Какой из браузеров считается менее безопасным, чем остальные:  A. Mozilla Firefox  B. Internet Explorer  C. Google Chrome  D. Opera  6. Какие действия не рекомендуется делать при работе с электронной почтой?  A. Отправлять электронные письма  B. Добавлять в свои электронные письма фотографии  C. Открывать вложения неизвестной электронной почты  D. Оставлять электронные письма в папке Отправленные  7. Что необходимо сделать, если на экране появилось окно с просьбой отправить SMS для дальнейшей работы?  A. Отправить SMS сообщение  B. Выполнить форматирование жесткого диска  C. Перезагрузить компьютер  D. Не отправлять SMS сообщение  8. Согласно какому документу в России проводится правой ликбез по вопросам защиты информации в ЭВМ?  A. Трудовому кодексу РФ  B. Доктрине информационной безопасности РФ  C. Стратегии развития информационного общества РФ  D. Конвенции о правах ребенка  9. Зачем необходимо делать резервные копии?  A. Чтобы информация могла быть доступна всем желающим  B. Чтобы не потерять важную информацию  C. Чтобы можно было выполнить операцию восстановления системы  D. Чтобы была возможность распечатать документы  10. Что необходимо сделать, если на сайте в Интернет, вдруг появилось сообщение о быстрой проверке ПК с просьбой перезагрузки компьютера?  A. Перезагрузить компьютер  B. Отформатировать жесткий диск  C. Закрыть сайт и выполнить проверку ПК  D. Выключить компьютер.   6.Подведение итогов |