государственное бюджетное общеобразовательное учреждение Самарской области средняя общеобразовательная школа № 1 «Образовательный центр» имени Героя Советского Союза М.Р.Попова ж.-д.ст.Шентала муниципального района Шенталинский Самарской области

Методическая разработка занятия по внеурочной деятельности по информационной безопасности на тему «Безопасность в сети Интернет»

8-9 классы

Выполнила: Павлова Е.В.,
учитель информатики
ГБОУ СОШ №1 «ОЦ» ж.- д. ст. Шентала

2021г

Цель занятия: изучить опасные угрозы сети Интернет и методы борьбы с ними;

Задачи:

Образовательная: закрепить понятие «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;

Развивать универсальные учебные действия:

Личностные: Формирование культурного пользователя Интернета. Развитие навыка постановки задачи и нахождения способа её решения. Формирование навыков критического мышления. Способствование всестороннему и гармоничному развитию каждого ребёнка.

Метапредметные: Освоение способов регуляции действий при работе в группе, организация и осуществление сотрудничества с учителем и учащимися. Усвоение умений принимать решения в конкретной жизненной ситуации.

Предметные: Овладение основами безопасного пользования интернет - сетями.

Дидактические основы урока:

Методы обучения: словесные, наглядные, практические.

Тип урока: объяснение нового материала.

Формы учебной работы учащихся: фронтальная.

Оборудование: ПК, проектор, экран, 11 компьютеров, тетради, презентация «Безопасность в сети Интернет».

Ход занятия

1. **Организационный момент, 1-3 мин.:**

В современное время средства коммуникации стали неотъемлемой частью повседневной жизни людей. Число пользователей Интернета неуклонно растет с каждым днём, а самыми активными среди них являются молодые люди, подростки и дети. Именно поэтому учить грамотно и безопасно проводить время в сети Интернет на сегодняшний день необходимо.

Зачастую уже с юного возраста дети могут находиться в мировой сети без контроля взрослых. Между тем, перечень рисков, с которыми можно столкнуться, достаточно обширен: проникновение вирусов и вредоносных программ, мошенничество, кража личной информации, оскорбления, преследования, домогательства к детям.

Итак, наше сегодняшнее мероприятие посвящено проблеме безопасности при использовании сети Интернет, потенциальных рисках при использовании Интернета, путях защиты от сетевых угроз. И тему нашего занятия вы видите на экране «Безопасность в сети Интернет». **(Слайд 1)**

(Слайд 2) *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)

Молодцы!

2. **Объяснение нового материала (27-30 мин.):**

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.

(Слайд 4) Компью́терный ви́рус — разновидность компьютерных программ или вредоносный код, отличительной особенностью которых является способность к размножению (саморепликация).

(Слайд 5) Классификация

В настоящее время не существует единой системы классификации и именования вирусов. Принято разделять вирусы на следующие группы.

(Слайд 6) 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.

(Слайд 7) По поражаемым операционным системам и платформам

- DOS
- Microsoft Windows
- Unix
- Linux

(Слайд 8) 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.

(Слайд 9) По языку, на котором написан вирус

- ассемблер
- высокоуровневый язык программирования
- скриптовый язык
- и др.

(Слайд 10) 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.

(Слайд 11) 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).

(Слайд 12) 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.

(Слайд 13) По инициативе Европейской комиссии в 2004 году был учрежден праздник Международный День безопасного Интернета (Safer Internet Day). И с тех пор вышел далеко за пределы Европы. Его отмечают более 70 стран мира, в том числе и Россия. Отмечается ежегодно во второй вторник февраля.

(Слайд 14) Его цель – пропаганда более безопасного и более ответственного использования онлайн-технологий и мобильных телефонов, особенно среди детей и молодежи во всем мире.

Поэтому сегодня я расскажу вам о том, как обезопасить себя, свих друзей, свой личный или рабочий компьютер, чтобы не стать жертвой сетевых угроз. **(Слайд 15)**

1. ***Установите комплексную систему защиты.*** **(Слайд 16)**

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*****. (Слайд 17)**

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.*** **(Слайд 18)**

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 19)**

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.*** **(Слайд 20)**

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. **(Слайд 21)**

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. **(Слайд 22)**

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. **(Слайд 23)**

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. **(Слайд 24)**

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. **(Слайд 25)**

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.

3. Итог урока (2-3 мин.);

Наше занятие подошло к концу. Подумайте, что нового оно вам дало? Изменилось ли ваше отношение с сети Интернет после нашего занятия? Если да, то каким образом?

Надеемся, что используя знания, полученные на нашем занятии, вы никогда не станете жертвой Интернет-мошенников. И всегда помните, что в любой сложной или непонятной ситуации вам могут помочь взрослые-родители и педагоги. **(Слайд 26)**

Всего доброго!