**ГКОУ «Орджоникидзевская ООШ**

**Тляратинского района»**

**ПЛАН**

**урока на тему :**

**«Безопасность в сети ИНТЕРНЕТ»**

**Провёл учитель информатики**

**АЛИЕВ Х.А.**

**(презентация прилагается)**

**2015 год.**

**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;

**Предварительная подготовка учащихся**: материал, изученный на предыдущих уроках информатики;

**Предварительная подготовка учителя:** изучение материала урока, написание конспекта, создание презентации, создание теста, подготовка видеофрагмента;

**Дидактические основы урока**:

*Методы обучения:* словесные, наглядные, практические.

*Тип урока:*объяснение нового материала;

*Формы учебной работы учащихся:*фронтальная, индивидуальная работа.

**Оборудование:** ПК, проектор, интерактивная доска (или экран), 12 компьютеров, тетради, презентация «Безопасность в сети Интернет».

**План урока:**

1. Организационный момент (1-2 мин.);
2. Введение в тему (3-5 мин.);
3. Объяснение нового материала (30-35 мин.);
4. Физкультминутка (1 мин.);
5. Самостоятельная работа (7-10 мин.);
6. Итог урока (2-3 мин.);

**Ход урока:**

1. **Организационный момент, 1-2 мин.:**

сообщение темы урока (занесение темы в тетрадь), его целей и задач;

краткий план деятельности.

1. **Введение в тему, 3-5 мин.:**

подготовить детей к восприятию темы;

нацелить на продуктивную работу.

Сегодня наш урок посвящен теме «Безопасность в сети Интернет». (Слайд 1)

Примечание. Учащиеся записывают в тетрадь основные определения самостоятельно по ходу лекции.

(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!

1. **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)

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

**Классификация**(Слайд 5)

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

**По поражаемым объектам**(Слайд 6-11)

*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**(Слайд 12-13)

1. DOS
2. Microsoft Windows
3. Unix
4. Linux

**По технологиям, используемым вирусом**(Слайд 14-17)

*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**(Слайд 18-19)

1. ассемблер
2. высокоуровневый язык программирования
3. скриптовый язык
4. и др.

**По дополнительной вредоносной функциональности**(Слайд 20-24)

*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 25-26) 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 27) 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.

1. **Физкультминутка (1 мин)**

Но сначала, мы немножко отдохнем и проведем физкультминутку. (Слайд 28)

Мы все вместе улыбнемся,

Подмигнем слегка друг другу,

Вправо, влево повернемся

И кивнем затем по кругу.

Все идеи победили,

Вверх взметнулись наши руки.

Груз забот с себя стряхнули

И продолжим путь науки.

Итак, как же бороться с сетевыми угрозами? (Слайд 29)

1. ***Установите комплексную систему защиты.*** (Слайд 30)

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.

1. ***Будьте осторожны с электронной почтой***(Слайд 31)

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.

1. ***Пользуйтесь браузерами Mozilla Firefox, Google Chrome и Apple Safari.***(Слайд 32)

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 недостатков как у одного, так и у второго браузера, поэтому лучше ими не пользоваться вовсе.

1. ***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.

1. ***Не отправляйте SMS-сообщения.***(Слайд 34)

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.

1. ***Пользуйтесь лицензионным ПО.***(Слайд 35)

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!

1. ***Используйте брандмауэр.***(Слайд 36)

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.

1. ***Используйте сложные пароли.***(Слайд 37)

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.

1. ***Делайте резервные копии.***(Слайд 38)

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.

1. ***Функция «Родительский контроль» обезопасит вас.***(Слайд 39)

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.(Слайд 40).

1. **Самостоятельная работа (7-10 мин.);**

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…*

1. Административному кодексу
2. Трудовому кодексу
3. Уголовному кодексу
4. Гражданскому кодексу

***2****Какой классификации вирусов на сегодняшний день не существует?*

1. По поражаемым объектам
2. По поражаемым операционным системам и платформам
3. По количеству поражаемых файлов
4. По дополнительной вредоносной функциональности

***3****Какой из приведенных паролей является более надежным*

1. 123456789
2. qwerty
3. annaivanova
4. 13u91A\_Ivanova

***4****Для того, чтобы антивирусные программы обеспечивали наилучшую безопасность вашего ПК, необходимо:*

1. Установить несколько антивирусных программ
2. Удалить все файлы, загруженные из сети Интернет
3. Своевременно обновлять антивирусные базы
4. Отключить компьютер от сети Интернет

***5****Какой из браузеров считается менее безопасным, чем остальные:*

1. Mozilla Firefox
2. Internet Explorer
3. Google Chrome
4. Opera

***6****Какие действия не рекомендуется делать при работе с электронной почтой?*

1. Отправлять электронные письма
2. Добавлять в свои электронные письма фотографии
3. Открывать вложения неизвестной электронной почты
4. Оставлять электронные письма в папке Отправленные

***7****Что необходимо сделать, если на экране появилось окно с просьбой отправить SMS для дальнейшей работы?*

1. Отправить SMS сообщение
2. Выполнить форматирование жесткого диска
3. Перезагрузить компьютер
4. Не отправлять SMS сообщение

***8****Согласно какому документу в России проводится правой ликбез по вопросам защиты информации в ЭВМ?*

1. Трудовому кодексу РФ
2. Доктрине информационной безопасности РФ
3. Стратегии развития информационного общества РФ
4. Конвенции о правах ребенка

***9****Зачем необходимо делать резервные копии?*

1. Чтобы информация могла быть доступна всем желающим
2. Чтобы не потерять важную информацию
3. Чтобы можно было выполнить операцию восстановления системы
4. 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?*

1. Перезагрузить компьютер
2. Отформатировать жесткий диск
3. Закрыть сайт и выполнить проверку ПК
4. Выключить компьютер.

**Итог урока (2-3 мин.);**