**МКОУ «ТАЛЦУХСКАЯ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА»**

****

**План – конспект тематического урока**

**«Безопасность в сети Интернет»**

**Выполнил:** учитель информатики Аюбов Рамазан Курбанович.

Талсух 2018 г.

**Тема урока: «Безопасность в сети Интернет»**

**Форма занятия:** семинар.
**Цель:** воспитание ответственного отношения к использованию ресурсов интернета расширение знаний о киберугрозах, формирование навыков их распознавания и оценки рисков, рекомендации по грамотному использованию электронной почты, ознакомление с инструкциями по безопасному общению в чатах.

**Задачи:**

*Образовательные:*

* Умение безопасно находить нужную информацию в сети Интернет.
* Научить применять полученные знания в проектной деятельности.

*Развивающие:*

* Развивать умение анализировать и систематизировать имеющуюся информацию.

*Воспитательные*:

* Развивать навыки работы и общения в группе, а так же в чатах.

**План занятия:**

1. **Просмотр видеоролика «Безопасность в сети Интернет»**
2. **Обсуждение правил предотвращения киберугроз, которые встречаются при работе в Интернете.**
3. **Подведение итогов занятия**.

**Ход занятия.**

**I. Организационный момент**

**II. Фомирование новых знаний и умений.**

Занятие начинается с просмотра социального видеоролика «Безопасность в сети Интернет».[**https://www.youtube.com/watch?v=yTCcfc3i5NQ**](https://www.youtube.com/watch?v=yTCcfc3i5NQ)

**Теоретический материал урока**

Сегодня Интернет часть нашей жизни. Мы в Интернете ищем нужную для нас информацию, слушаем музыку, смотрим фильмы, общаемся с друзьями, совершаем различные покупки, учимся, работаем, отдыхаем. Фактически, часть нашей жизни уже проходить в Интернете. Эта виртуальная среда предъявляет свои требования к каждому из нас. И наш урок посвящен тому, чтобы еще раз вспомнить, что необходимо знать пользователю Интернета, на что обращать внимание, к чему относиться с осторожностью. Возможно, для многих это станет повторением пройденного, кому то поможет систематизировать имеющиеся знания, правильно оценить собственный опыт использования сети.

Оценивая умения и навыки, принято использовать понятие компетенция. Под компетенцией мы понимаем способность успешно решать задачи в определенной области. Применительно к Интернету мы рассматриваем 4 сетевых компетенции: техническую, информационную, коммуникативную, потребительскую.

Техническая компетенция – способность использовать для работы в Интернете технических средств и программ. Базовое представление о каналах связи и рисках в этой области.

Сегодня для работы в Интернете можно использовать разные устройства: компьютер, ноутбук, планшет, телефон. К Интернету все чаще подключаются и бытовая техника и другие устройства. При их использовании нужно соблюдать элементарные правила эксплуатации. Они известны большинству из нас.

Правильно подключать провода, периодически подзаряжать батареи. Однако, новые технические устройства и развитие техники предъявляют новые требования. Например, сенсорные экраны плохо работают при низких температурах и требуют дополнительной чистоты рук, а флешки и карты памяти стали такими миниатюрными, что их легко потерять. И вопрос сохранения личных данных зависит от внимательного отношения к собственным устройствам. Другая сторона вопроса эта программа, которая используется нами на наших устройствах. В каждой программе нужно уметь работать. Большинство программ имеют интуитивно-понятный интерфейс. Это означает, что с ними легко разобраться и пользоваться сразу после установки, но нужно понимать изучение правил использования программ открывают дополнительные возможности и позволяют работать более эффективно и комфортно. Иногда, программы содержать ошибки. В большинстве случаев разработчики находят эти ошибки и исправляют сами. Поэтому, важно своевременно устанавливать обновления для программного обеспечения. Следует помнить, что ошибки часто используют хакеры и своевременное обновление этого залог безопасного использования программного обеспечения. Рекомендуется использовать автоматическое обновление.

Другой угрозой является внедрение вредоносных программ, т.е. вирусы. Говоря о вредоносных программах, обычно выделяют собственно вирусы: сетевые черви, руткиты, шпионские программы.

О важности этой проблемы свидетельствуют многочисленные факты. Каждые девять секунд в США происходить преступление с использованием программных средств. Более 80 % компьютерных преступлений осуществляется через глобальную сеть Интернет, которая обеспечивает широкие возможности злоумышленникам для нарушений в глобальном масштабе. Если компьютер, являющийся объектом атаки, подключен к Интернету, то для «взломщика» нет большой разницы, где он находится – в соседней комнате или на другом континенте. Потери от хищения или повреждения компьютерных данных составляют более 100 млн долларов в год.

Преступники для совершения компьютерных преступлений широко используют вредоносные программы т.е. компьютерные вирусы. Сегодня большинство вредоносных программ создаются либо для того, чтобы рассылать спам, либо для того, чтобы красть у пользователя важные данные.

Все большее число детей школьного возраста пользуются социальными сетями. Им следует помнить, что излишняя болтливость в Интернете может стать причиной бед лично для них и их близких. Не следует разглашать семейную информацию: о материальном достатке, о деятельности своих родителей, о времени и местах нахождения близких людей, о семейных связах и пр., т.е. все то, может быть использовано в преступных целях. Скачивая из Интернета сомнительные программы или файлы Вы, сами того не зная можете скачать из сети компьютерный вирус, Вашу учетную запись или адрес электронной почты, могут взломает злоумышленник.

Одной из разновидностей спама являются «Нигерийские письма» или другое название «Угроза 419».

 **III. Обсуждение видеоролика «Безопасность в сети Интернет»**

**Источники вредоносных программ**

**Непроверенные ссылки**

**Скачивание файлов с непроверенных ресурсов**

**Программы непроверенного разработчика**

**Сомнительные заряженные сайты**

**Опасные баннеры**

**Заряженные флешки**

**Вредоносные программы могут:**

**Похищать пароли логины, контакты**

**Похищать данные банковских карт**

**Отправлять данные злоумышленникам**

**Делать скрытые скриншоты**

**Рассылать спам**

**Звонки и СМС на платные номера**

**Рассылать сообщения в социальных сетях**

**Включать удаленное управление компьютером**

**Вредоносные программы**

**ВИРУСЫ**

**РУТКИТЫ**

**СЕТЕВЫЕ ЧЕРВИ**

**ШПИОНСКИЕ ПРОГРАММЫ**

**Основные формы компьютерных преступлений:**

1. Несанкционированный ( неправомерный) доступ к информации
2. Нарушение работоспособности компьютерной системы
3. Нарушение целостности компьютерной информации.

**Как избежать заряжения компьютера**

**ИСПОЛЬЗУЙ АНТИВИРУС**

**С ОБНОВЛЕНИЯМИ**

**ИСПОЛЬЗУЙ СОВРЕМЕННЫЕ**

**ОПЕРАЦИОННЫЕ СИСТЕМЫ**

**ОГРАНИЧ ФИЗИЧЕСКИЙ**

**ДОСТУП К СВОЕМУ УСТРОЙСТВУ**

**СВОЕВРЕМЕННО ОБНОВЛЯЙ**

**ПРОГРАММЫ**

**ПРОВЕРЯЙ ВНЕШНЫЕ НОСИТЕЛИ**

**РАБОТАЙ ПОД УЧЕТКОЙ ПОЛЬЗОВАТЕЛЯ**

**НЕ ОТКРЫВАЙ ФАЙЛЫ, ПОЛЧЕННЫЕ**

 **ИЗ НЕНАДЕЖНЫХ ИСТОЧНИКОВ**

Наряду с программно-техническими средствами защиты информации действуют правовые, юридические меры защиты. В 1996 году в Уголовный кодекс РФ был впервые внесен раздел «Преступления в сфере компьютерной информации». Он определил меру наказания за некоторые виды преступления, ставших, к сожалению, распространенными: неправомерный доступ к компьютерной информации; создание, использование и распространение вредоносных программ для ЭВМ; умышленное нарушение правил эксплуатации ЭВМ и их сетей.

К защите информации относиться также и осуществление авторских и имущественных прав на интеллектуальную собственность, каковой является программное обеспечение.

**Правила безопасности в интернете.**

1. Используйте надежный пароль. Первое и главное правило сохранности Ваших данных, учетных записей, почтовой пересылки это надежный пароль! Много раз хакеры взламывали страницы в социальных сетях или почтовые адреса из-за того, что пользователь ставил простой пароль. Вы ведь не хотите, чтобы Ваши личную переписку узнал кто-то чужой? Используйте генератор паролей, чтобы получить надежный пароль (Источник- <http://genpas.narod.ru/>).
2. Заходите в интернет с компьютера, на котором установлен фаервол или антивирус с фаерволом. Это в разы уменьшит вероятность поймать вирус или зайти на вредоносный сайт.
3. Заведите один основной почтовый адрес и придумайте к нему сложный пароль. При регистрации на форумах, в соц. сетях и прочих сервисах Вы будете указывать его. Это необходимо если Вы забудете пароль или имя пользователя. Ни в коем случае не говорите, никому свой пароль к почте, иначе злоумышленник сможет через вашу почту получить доступ ко всем сервисам и сайтам, на которых указан Ваш почтовый адрес.
4. Если Вы хотите скачать какой-то материал из интернета, на сайте где не нужна регистрация, но от Вас требуют ввести адрес своей электронной почты, то, скорее всего, на Ваш адрес будут высылать рекламу или спам. В таких случаях пользуйтесь одноразовыми почтовыми ящиками.
5. Скачивайте программы либо с официальных сайтов разработчиков. Не скачивайте программы с подозрительных сайтов или с файлообменников. Так Вы уменьшите риск скачать вирус вместо программы.
6. Не нажимайте на красивые баннеры или рекламные блоки на сайтах, какими бы привлекательными и заманчивыми они не были. В лучшем случае, Вы поможете автору сайта получить деньги, а в худшем — получите вирус. Используйте плагины для браузеров, которые отключают рекламу на сайтах.
7. Если Вы работаете за компьютером, к которому имеют доступ другие люди (на роботе или в интернет кафе), не сохраняйте пароли в браузере. В противном случае, любой, кто имеет доступ к этому компьютеру, сможет зайти на сайт, используя Ваш пароль.
8. Не открывайте письма от неизвестных Вам пользователей (адресов). Или письма с оповещением о выигрыше в лотереи, в которой Вы просто не участвовали.
9. Не нажимайте на вплывающие окна, в которых написано, что Ваша учетная запись в социальной сети заблокирована. Это проделки злоумышленников! Если Вас вдруг заблокируют, Вы узнаете об этом, зайдя в эту социальную сеть, или администрация отправит Вам электронное письмо.
10. Периодическим меняйте пароли на самых важных сайтах. Так Вы уменьшите риск взлома вашего пароля.

 **IV. Подведение итогов.**