**МКОУ «ТАЛЦУХСКАЯ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА»**

****

**План – конспект тематического урока**

**« Киберугрозы современности»**

**Выполнил:**  учитель информатики Аюбов Р.К.

Талсух 2018 г.

**План тематического урока для учащихся 8-9 классов, посвященного Интернет безопасности детей.**

**Тема урока:** «Киберугрозы современности: главные правила их распознавания и предотвращения»

**Форма занятия:** семинар.
**Цель:** расширение знаний о киберугрозах, формирование навыков их распознавания и оценки рисков.

**План занятия:**

1. Обсуждение правил предотвращения киберугроз, которые встречаются при работе в Интернете. Составление листовок «Правила защиты от киберугроз» (30 мин.);
2. Просмотр презентации «Безопасный Интернет». (10 мин.);
3. Подведение итогов занятия (5 мин.).

**Ход занятия.**

**I. Организационный момент**

**II. Теоретический материал урока**Занятие начинается показом социального видеоролика [«Безопасный интернет - детям!»](http://www.youtube.com/watch?v=9uvNVZMdeIk&feature=player_embedded).

После просмотра ролика учитель объявляет тему занятия и предлагает ученикам самим сформулировать цель занятия.

Каждый современный человек, ежедневно проводит время в интернете. Интернет может быть прекрасным и полезным средством для обучения, отдыха или общения с друзьями. Но – как и реальный мир – Сеть тоже может быть опасна: в ней появилась своя преступность, хулиганство, вредительство и прочие малоприятные явления.

В Интернете содержатся огромные массивы информации, которая является запрещенной для детей, так как может нанести вред их физическому и психическому здоровью, духовному и нравственному развитию. Террористы и националисты используют интернет-пространство для идеологической пропаганды, привлечения молодежи в свои ряды, для призыва к насилию и разрушению общественных институтов управления. Вы можете скачать из сети компьютерный вирус, Вашу учетную запись или адрес электронной почты, могут взломает злоумышленник.

В последнее время в Интернете появляется много материалов агрессивного и социально опасного содержания. Всем нужно помнить о существовании подобных угроз и уделять повышенное внимание вопросу обеспечения безопасности в Интернете.

**Можно выделить 3 группы серьезных киберугроз:**

* Шпионское программное обеспечение и другие вредоносные программы;
* Спамы;
* Фишинговые атаки.

**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.

Пользуясь этими правилами безопасности в интернете, Вы существенно уменьшите риск получить вирус на свой компьютер или потерять учетную запись на любимом сайте.

**III. Закрепление**

* **Работа с этой информацией:**
1. **Обсуждение и дополнение основных 10 правил.** Учащимся предлагается обсудить и дополнить эти основные правила с учетом уже имеющегося у них опыта работы в интернете. Все ответы детей записываются на доске. При обсуждении внимание учеников обращается на то, откуда могут исходить опасность. На первом месте в этом списке стоят социальные сети.

1. Рисуем инфографику. Учащимся предлагается нарисовать плакат в стиле современной инфографики, где размещаются основные правила безопасной работы в интернет.
* **Просмотр презентации** [**«Безопасный Интернет».**](https://downloader-default8d.disk.yandex.net/rdisk/f15bb43295789b54745459533ddaf005b0e76238a3e3caa4ba5bd2924d020e6a/562bf669/DFWERVFzCWAjXhetegj3DxMn6Efu4onSz-16AZzp13FgoR4Nislwr68whByA0kjpC94ZAfKK4VhDDw7ghBkHhQ%3D%3D?uid=0&filename=Urok-5-9_2-01.pptx&disposit)
* **Раздать листы с 10 основными правилами безопасности в интернете.**

**IV. Подведение итогов занятия.**

1. Помните, правила хорошего поведения действуют везде – даже в виртуальном мире.
2. Дети уважайте собственность других в Интернете. Не забывайте, что незаконное копирование и использование чужой работы – текста, музыки, компьютерных игр и других программ – является кражей.
3. На первом месте в этом списке, откуда могут исходить опасность, стоят социальные сети.

**V. Домашнее задание:**

1. Обсуждение с родителями правилами безопасности в интернете и дополнение основных 10 правил;
2. Рисуем инфографику;
3. Ознакомиться с темой «Информационная безопастность» (§ 27 стр. 190-194, учебник Информатика и ИКТ, И.Г. Семакин и др.).