Государственное общеобразовательное казенное учреждение Иркутской области «Специальная (коррекционная) школа № 14 г. Иркутска»

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

Составила:

Акопян Шогакат Дерениковна

ГОКУ  СКШ № 14 г. Иркутска

*г. Иркутск*

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

**Цель:** формирование навыков безопасного поведения в информационном пространстве сети Интернет.
 **Задачи:**

ознакомить учащихся:

– с правилами ответственного и безопасного поведения в современной информационной среде, способах защиты от противоправных посягательств в сети Интернет;

– как критически относиться к сообщениям в СМИ (в т.ч. электронных), как отличить достоверные сведения от недостоверных, как избежать вредной и опасной для них информации, как распознать признаки злоупотребления их доверчивостью и сделать более безопасным свое общение в сети Интернет;

– как общаться в социальных сетях (сетевой этикет), не обижая своих виртуальных друзей, и избегать выкладывать в сеть компрометирующую информацию или оскорбительные комментарии и т.д.

**Методы и формы обучения:** словесный (дискуссия, рассказ), видеометод, наглядный (демонстрация)

**Оборудование:** компьютер, мультимедиа, экран.

**Ведущие понятия занятия:** интернет, угроза, безопасность, информация, угроза информационной безопасности.

**Ход занятия**

**I. Мотивация к деятельности.**

Где найти подругу Олю?
Прочитать, что было в школе?
И узнать про все на свете?
Ну конечно, в ИНТЕРНЕТЕ!
Там музеи, книги, игры,
Музыка, живые тигры!
Можно все, друзья, найти
В этой сказочной сети!

**(слайд 1)**

Тема сегодняшнего занятия **“Безопасность в сети Интернет”** .

**Цель нашего урока:** формирование навыков безопасного поведения в информационном пространстве сети Интернет.
**(Слайд 2)**

**Интернет** – это объединенные между собой компьютерные сети, глобальная мировая система передачи информации с помощью информационно-вычислительных ресурсов.

**Интернет**– это безграничный мир информации. Здесь ты найдёшь много интересного и полезного для учёбы. В Интернете можно общаться со знакомыми и даже заводить друзей. Но кроме хорошего, в виртуальном мире есть и плохое. Неправильное поведение в Интернете может принести вред не только тебе, но также твоим родным и близким.

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.

**(слайд 3).**

**Безопасность** — многозначное понятие, характеризующее в первую очередь защищённость и низкий уровень риска для человека, общества или любых других субъектов, объектов или их систем.

**(Слайд 4).**

**Информация** — сведения о чём-либо, независимо от формы их представления.

**Угроза информационной безопасности** — совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства в информационной сфере.

**( Слайд 5)**

**Беседа с классом по вопросам :**

1.Чем является компьютер в вашей семье? Приведите примеры ситуаций из вашей жизни, связанных с положительными и отрицательными эмоциями по поводу использования компьютера.

2.Что дает Вам интернет?

(Предполагаемые ответы: общение с друзьями, родственниками; доступ к новой информации и развлечениям; возможность учиться новому, знакомиться с новыми людьми и т.д. Бесконечный поток информации на любую тему- от медицины до науки и техники; - подробнейший материал обо всех видах искусства; - массу полезной информации для студентов и школьников; - сведения для тех, кто ищет работу; - справки об отдыхе, развлечениях, спорте и самых разных товарах. В Интернет можно отыскать различные справочники, словари, энциклопедии и географические карты).

**II. Анализ, обсуждение ситуаций и разработка рекомендаций.**

**(Слайд 6)**

**Самые опасные угрозы сети Интернет**

* Вредоносные программы
* Кража информации
* Халатность сотрудников
* Хакерские атаки
* Финансовое мошенничество
* Спам
* 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.

**(Слайд 7)**

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

**Осторожно: вирусы и другие вредоносные программы**

В Интернет ты заходишь через компьютер. Это может быть школьный или библиотечный компьютер, твой личный или тот, которым пользуется вся семья. Любому компьютеру могут повредить вирусы, их еще иногда называют вредоносными программами. Они могут **уничтожить** важную информацию **или украсть** деньги через Интернет. **Для защиты компьютера** на нём установлены специальные защитные программы и фильтры. Не меняй ничего в их настройках! **Не сохраняй подозрительные файлы** и не открывай их. Если антивирусная защита компьютера не рекомендует, **не заходи на сайт, который считается «подозрительным».** Никому **не сообщай свой логин с паролем** и не выкладывай их в Интернете – относись к ним так же бережно, как к ключам от квартиры.

**(Слайд 8)**

**Физкультминутка**

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.

**(Слайд 9)**

**Борьба с сетевыми угрозами (слайды)**

**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.

**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 Outlookи Windows Mail помогают блокировать потенциально опасные вложения.

**Пользуйтесь браузерами Mozilla Firefox, Google Chrome и Apple Safari!**

* Большинство червей и вредоносных скриптов ориентированы под Internet Explorer и Opera.
* IE до сих пор удерживает первую строчку в рейтинге популярности, но лишь потому, что он встроен в Windows.
* Opera очень популярна в России из-за ее прозрачного удобства и реально большого числа настроек.
* Уровень безопасности сильно хромает как у одного, так и у второго браузера, поэтому лучше им и не пользоваться вовсе.

**Обновляйте операционную систему Windows!**

* 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.

**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.

**Пользуйтесь лицензионным программным обеспечением!**

* 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!

**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 — 2-4 часа, но чтобы взломать семисимвольный пароль, потребуется 2-4 года.
* Лучше использовать пароли, комбинирующие буквы разных регистров, цифры и разные значки.

**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 обсуждаете в сети, и новых Интернет-знакомых, это поможет вам реально оценивать информацию, которую вы видите в сети и не стать жертвой обмана.

**III. Закрепление.**

**1. Какую информацию нельзя разглашать в Интернете?**

1. Свои увлечения .

2. Свой псевдоним .

3. Домашний адрес.

**2. Чем опасны социальные сети?**

1. Личная информация может быть использована кем угодно в разных целях .

2. При просмотре неопознанных ссылок компьютер может быть взломан .

3. Все вышеперечисленное верно .

**3. Виртуальный собеседник предлагает встретиться, как следует поступить?**

**1.** Посоветоваться с родителями и ничего не предпринимать без их согласия .

**2.** Пойти на встречу одному .

**3.** Пригласить с собой друга .

**4. Что в Интернете запрещено законом?**

1. Размещать информацию о себе.

2. Размещать информацию других без их согласия .

3. Копировать файлы для личного использования .

**5. Действуют ли правила этикета в Интернете?**

1. Интернет - пространство свободное от правил .

2. В особых случаях .

3. Да, как и в реальной жизни.

Для родителей можно предоставить памятку на родительском собрании.

**Памятка для родителей:**

1. Поговорите с детьми о том, чем они занимаются в интернете.
2. Помните, что безопасность ваших детей в Интернете, на 90% зависит от вас, поэтому создайте свой собственный список правил работы ребенка в Интернете и повесьте его на стену около компьютера.
3. Конфидециальность: при общении использовать только имя или ник (псевдоним), который лучше чтобы придумал сам родитель и оно не несло личной информации, не сообщать посторонним людям номер телефона, адрес, место учебы и прочую важную информацию, не высылать свои фотографии Установите и регулярно обновляйте антивирусную программу.
4. Контролируйте приобретение ребенком компьютерных дисковс играми, чтобы они не причинили вреда детскому здоровью и психике.
5. Всегда держите компьютер в центре внимания, узнавайте, для чего ваши дети используют Интернет.
6. Научите детей рассказывать вам даже о малейшем беспокойстве, что что-то пошло не так.
7. Расскажите детям о мошенниках и прочих "плохих" людях в Сети, которые могут выдавать себя за других, поэтому надо отказываться от встреч с ними. Научите ребенка говорить "Нет".
8. Не забудьте рассказать об авторском праве, что неправомерное использование чужого материала может быть уголовно наказуемым.
9. Расскажите, что далеко не все, что есть в интернете - правда, всегда нужно уточнять у родителей.

**IV. Рефлексия. Подведение итогов работы.** Учащиеся высказывают свое мнение, оправдались ли их ожидания от проделанной работы.

 Оценка учащимися занятия (на доску крепятся звездочки. Красная – занятие понравилось; зеленая – занятие оставило равнодушным; синяя – занятие не понравилось).