

Муниципальное бюджетное общеобразовательное учреждение
«Щекинская средняя общеобразовательная школа»

Конспект урока на тему:
**«Правила безопасного поведения
в Интернете»**



Подготовила
учитель информатики
МБОУ «Щекинская СОШ»
Лупанова Т.В.

с.Щекино 2014 г.

Урок «Интернет-безопасность»

Цель: обеспечение информационной безопасности несовершеннолетних обучающихся и воспитанников путем привития им навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде.

Задачи:

- 1) информирование обучающихся о видах информации, способной причинить вред здоровью и развитию несовершеннолетних, запрещенной или ограниченной для распространения на территории Российской Федерации, а также о негативных последствиях распространения такой информации;
- 2) информирование обучающихся о способах незаконного распространения такой информации в информационно- телекоммуникационных сетях, в частности, в сетях Интернет и мобильной (сотовой) связи (в том числе путем рассылки SMS-сообщений незаконного содержания);
- 3) ознакомление обучающихся с международными принципами и нормами, с нормативными правовыми актами Российской Федерации, регулирующими вопросы информационной безопасности несовершеннолетних;
- 4) обучение детей и подростков правилам ответственного и безопасного пользования услугами Интернет и мобильной (сотовой) связи, другими электронными средствами связи и коммуникации, в том числе способам защиты от противоправных и иных общественно опасных посягательств в информационно-телекоммуникационных сетях, в частности, от таких способов разрушительного воздействия на психику детей, как кибербуллинг (жестокое обращение с детьми в виртуальной среде) и буллицид (доведение до самоубийства путем психологического насилия);
- 5) предупреждение совершения обучающимися правонарушений с использованием информационно-телекоммуникационных технологий.

В ходе уроков Интернет - безопасности обучающиеся должны научиться делать более безопасным и полезным свое время пребывания в сети Интернет и иных информационно-телекоммуникационных сетях, а именно:

- критически относиться к сообщениям и иной информации, распространяемой в сетях Интернет, мобильной (сотовой) связи, посредством иных электронных средств массовой коммуникации;
- отличать достоверные сведения от недостоверных, вредную для них информацию от безопасной;
- избегать навязывания им информации, способной причинить вред их здоровью, нравственному и психическому развитию, чести, достоинству и репутации;
- распознавать признаки злоупотребления их неопытностью и доверчивостью, попытки вовлечения их в противоправную и иную антиобщественную деятельность;
- распознавать манипулятивные техники, используемые при подаче рекламной и иной информации;
- критически относиться к информационной продукции, распространяемой в информационно-телекоммуникационных сетях;
- анализировать степень достоверности информации и подлинность ее источников;
- применять эффективные меры самозащиты от нежелательных для них информации и контактов в сетях.

ХОД УРОКА

Интернет постепенно проникает в каждую организацию, общественное учреждение, учебное заведение, в наши дома. Число пользователей Интернета в России стремительно растет, причем доля молодежи и совсем юной аудитории среди пользователей Всемирной паутины очень велика. Для многих, особенно молодых людей, он становится информационной средой, без которой они не представляют себе жизнь. И это неудивительно: ведь в Интернете можно найти информацию для реферата или курсовой, послушать любимую мелодию, купить понравившуюся книгу или обсудить горячую тему на многочисленных форумах.

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 появились своя преступность, хулиганство, вредительство и прочие малоприятные явления. Виртуальность общения предоставляет людям с недобрыми намерениями дополнительные возможности причинить вред детям. В последнее время в Интернете появляется много материалов агрессивного и социально опасного содержания.

Фильм «Детская безопасность в Интернете»

К настоящему времени проблема безопасности детей в Интернете, без преувеличения, стала глобально значимой проблемой. Вся семья международных организаций системы ООН уже более десяти лет занимается ее решением. Лидеры по внедрению информационных технологий в повседневную жизнь и нормативному регулированию информационных отношений – США и Европейский союз – уже вплотную столкнулись с необходимостью решения всего спектра проблем: как регулировать доступ детей в Интернет и контролировать их пребывание в Интернете? Как защищать детей от преступных действий со стороны злоумышленников, которые очень активно используют Интернет для своих вредных, незаконных и аморальных целей?

Международные стандарты в области информационной безопасности детей нашли отражение и в российском законодательстве.

Принятый 29 декабря 2010 года Федеральный закон Российской Федерации № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" устанавливает правила медиа-безопасности детей при обороте на территории России продукции СМИ, печатной, аудиовизуальной продукции на любых видах носителей, программ для компьютеров и баз данных, а также информации, размещаемой в информационно-телекоммуникационных сетях и сетях подвижной радиотелефонной связи.

Закон определяет информационную безопасность детей как состояние защищенности, при котором отсутствует риск, связанный с причинением информацией (в том числе распространяемой в сети Интернет) вреда их здоровью, физическому, психическому, духовному и нравственному развитию.

Кроме того, принят Федеральный закон Российской Федерации от 21 июля 2011 г. № 252-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "О защите детей от информации, причиняющей вред их здоровью и развитию", направленный на защиту детей от разрушительного, травмирующего их психику информационного воздействия, переизбытка жестокости и насилия в общедоступных источниках массовой информации, от информации, способной развить в ребенке порочные наклонности, сформировать у ребенка искаженную картину мира и неправильные жизненные установки.

Фильм «Безопасный интернет – детям»

Учитель: А сейчас я попрошу вас продолжить четверостишие
Где найти подругу Олю?
Прочитать, что было в школе?
И узнать про все на свете?
Ну, конечно, (делает паузу, чтобы могли хором сказать) в
ИНТЕРНЕТЕ!

У вас ребята есть право на информацию. Это провозглашает статья 13
Конвенции о правах ребенка.

Статья 13

1. Ребенок имеет право свободно выражать свое мнение; это право включает свободу искать, получать и передавать информацию и идеи любого рода, независимо от границ, в устной, письменной или печатной форме, в форме произведений искусства или с помощью других средств по выбору ребенка.

Ведущий: Но так ли безопасен Интернет? (Ответы детей)

А может ли Интернет стать безопасным? Ответить на этот вопрос мы попробуем найти в течение нашего занятия.

Слайд

Вопрос 1 Какие опасности подстерегают нас в Интернете?

Преступники в Интернете

Преступники преимущественно устанавливают контакты с детьми в чатах, при обмене мгновенными сообщениями, по электронной почте или на форумах. Для решения своих проблем многие подростки обращаются за поддержкой. Злоумышленники часто сами там обитают; они стараются привлечь подростка своим вниманием, заботливостью, добротой и даже подарками, нередко затрачивая на эти усилия значительное время, деньги и энергию. Обычно они хорошо осведомлены о музыкальных новинках и современных увлечениях детей. Они выслушивают проблемы подростков и сочувствуют им. Но постепенно злоумышленники вносят в свои беседы оттенок сексуальности или демонстрируют материалы откровенно эротического содержания, пытаются ослабить моральные запреты, сдерживающие молодых людей. Некоторые преступники могут действовать быстрее других и сразу же заводить сексуальные беседы. Преступники могут также оценивать возможность встречи с детьми в реальной жизни.

Фильм «Дикий мир Интернета»

Вредоносные программы

К вредоносным программам относятся вирусы, черви и «троянские кони» – это компьютерные программы, которые могут нанести вред вашему компьютеру и хранящимся на нем данным. Они также могут снижать скорость обмена данными с Интернетом и даже использовать ваш компьютер для распространения своих копий на компьютеры ваших друзей, родственников, коллег и по всей остальной глобальной Сети.

В ЧЕМ СОСТОИТ МОШЕННИЧЕСТВО?

Среди Интернет-мошенничеств широкое распространение получила применяемая хакерами техника «phishing», состоящая в том, что в фальшивое электронное письмо включается ссылка, ведущая на популярный узел, но в действительности она приводит пользователя на мошеннический узел, который выглядит точно так же, как официальный. Убедив пользователя в том, что он находится на официальном узле, хакеры пытаются склонить его к вводу паролей, номеров кредитных карт и другой секретной информации, которая потом может и будет использована с ущербом для пользователя.

Азартные игры

Разница между игровыми сайтами и сайтами с азартными играми состоит в том, что на игровых сайтах обычно содержатся настольные и словесные игры, аркады и головоломки с системой начисления очков. Здесь не тратятся деньги: ни настоящие, ни игровые. В отличие от игровых сайтов, сайты с азартными играми могут допускать, что люди выигрывают или проигрывают игровые деньги. Сайты с играми на деньги обычно содержат игры, связанные с выигрышем или проигрышем настоящих денег.

Онлайновое пиратство

Онлайновое пиратство – это незаконное копирование и распространение (как для деловых, так и для личных целей) материалов, защищенных авторским правом – например, музыки, фильмов, игр или программ – без разрешения правообладателя.

Интернет-дневники

Увлечение веб-журналами (или, иначе говоря, блогами) распространяется со скоростью пожара, особенно среди подростков, которые порой ведут интернет-дневники без ведома взрослых. Последние исследования показывают, что сегодня примерно половина всех веб-журналов принадлежат подросткам. При этом двое из трех раскрывают свой возраст; трое из пяти публикуют сведения о месте проживания и контактную информацию, а каждый пятый сообщает свое полное имя. Не секрет, что подробное раскрытие личных данных потенциально опасно.

Фильм «История одного знакомства в сети»

Интернет-хулиганство

Так же как и в обычной жизни, в Интернете появились свои хулиганы, которые осложняют жизнь другим пользователям Интернета. По сути, они те же дворовые хулиганы, которые получают удовольствие, хамя и грубя окружающим.

Недостоверная информация

Интернет предлагает колоссальное количество возможностей для обучения, но есть и большая доля информации, которую никак нельзя назвать ни полезной, ни надежной. Пользователи Сети должны мыслить критически, чтобы оценить точность материалов; поскольку абсолютно любой может опубликовать информацию в Интернете.

Материалы нежелательного содержания

К материалам нежелательного содержания относятся: материалы порнографического, ненавистнического содержания, материалы суицидальной направленности, сектантские материалы, материалы с ненормативной лексикой.

У людей, которые часто сидят в Интернете проявляется Интернет-зависимость

ФИЛЬМ «Интернет-зависимость»

Признаки компьютерной зависимости:

1. Когда родители просят отвлечься от игры на компьютере, но ребенок начинает демонстрировать острый эмоциональный протест;
2. Ребенок раздражается при вынужденном отвлечении;
3. Ребенок не может самостоятельно спланировать окончание игры на компьютере;
4. Ребенок забывает о домашних делах и приготовлении уроков;
5. Сбивается режим дня, режим питания и сна;
6. Прием пищи у ребенка происходит без отрыва от игры на компьютере;
7. Ощущение эмоционального подъема во время игры на компьютере;
8. Общение со сверстниками имеет только определенную тематику «компьютер»;
9. Сильное желание быстрее оказаться дома и сесть за любимую игру.

Доказано, что при появлении подобных признаков могут возникнуть нарушения в работе желудочно-кишечного тракта, могут появиться болевые ощущения в области позвоночника, запястий рук. Регулярное раздражение глазных яблок может способствовать появлению головных болей и проблем со зрением. Развивается бессонница, нервное истощение. Ребенок начинает грубить родителям и окружающим.

Конкурс буклетов "Правила поведения в сети Интернет"

Физ. минутка «Собери рукопожатия».

Участникам предлагается в течение 10 секунд пожать руки как можно большего числа других людей.

Обсуждение.

- Кому сколько человек удалось поприветствовать? У кого-то возник психологический дискомфорт? Если – да, то чем он был вызван?

Анализ ситуации.

Общаясь в Интернете, мы очень часто добавляем незнакомых людей в свои социальные сети и общаемся с ними. Мы не знаем про них ничего, только их Ники. Как много информации про человека мы можем узнать от Ника или рукопожатия? Однако, очень важно знать, что есть рядом люди, готовые выслушать, оказать поддержку, помочь в трудную минуту.

Учитель предлагает ответить на главный вопрос урока – «Как сделать работу в сети безопасной?»

ВОПРОС 2

Как этих опасностей избежать?

Преступники в Интернете

Прекращайте любые контакты по электронной почте, в системе обмена мгновенными сообщениями или в чатах, если кто-нибудь начинает задавать вам вопросы личного характера или содержащие сексуальные намеки. Никогда не соглашайтесь на личную встречу с людьми, с которыми вы познакомились в Интернете.

Фильм «Опасности Интернета для девушек, женщин»

Вредоносные программы

А) Никогда не открывайте никаких вложений, поступивших с электронным письмом, за исключением тех случаев, когда вы ожидаете получение вложения и точно знаете содержимое такого файла.

Б) Скачивайте файлы из надежных источников и обязательно читайте предупреждения об опасности, лицензионные соглашения и положения о конфиденциальности.

В) Регулярно устанавливайте на компьютере последние обновления безопасности и антивирусные средства.

Анкета «Осторожно, вирус!»

Интернет-мошенничество и хищение данных с кредитной карты

А)Посещая веб-сайты, нужно самостоятельно набирать в обозревателе адрес веб-сайта или пользоваться ссылкой из «Избранного» (Favorites); никогда не нужно щелкать на ссылку, содержащуюся в подозрительном электронном письме.

Б) Контролируйте списание средств с ваших кредитных или лицевых счетов. Для этого можно использовать, например, услугу информирования об операциях со счетов по SMS, которые предоставляют многие банки в России.

Азартные игры

Помните, что нельзя играть на деньги. Ведь в основном подобные развлечения используются создателями для получения прибыли. Игроки больше теряют деньги, нежели выигрывают. Играйте в не менее увлекательные игры, но которые не предполагают использование наличных или безналичных проигрышей/выигрышей.

Онлайновое пиратство

Помните! Пиратство, по сути, обычное воровство, и вы, скорее всего, вряд ли захотите стать вором. Знайте, что подлинные (лицензионные) продукты всегда выгоднее и

надежнее пиратской продукции. Официальный производитель несет ответственность за то, что он вам продает, он дорожит своей репутацией, чего нельзя сказать о компаниях – распространителях пиратских продуктов, которые преследуют только одну цель – обогатиться и за счет потребителя, и за счет производителя. Лицензионный пользователь программного обеспечения всегда может рассчитывать на консультационную и другую сервисную поддержку производителя, о чем пользователь пиратской копии может даже не вспоминать. Кроме того, приобретая лицензионный продукт, потребитель поддерживает развитие этого продукта, выход новых, более совершенных и удобных версий. Ведь в развитие продукта свой доход инвестирует только официальный производитель

Интернет-дневники

Никогда не публикуйте в них какую-либо личную информацию, в том числе фамилию, контактную информацию, домашний адрес, номера телефонов, название школы, адрес электронной почты, фамилии друзей или родственников, свои имена в программах мгновенного обмена сообщениями, возраст или дату рождения. Никогда не помещайте в журнале провокационные фотографии, свои или чьи-либо еще, и всегда проверяйте, не раскрывают ли изображения или даже задний план фотографий какую-либо личную информацию.

Интернет-хулиганство

Игнорируйте таких хулиганов. Если вы не будете реагировать на их воздействия, большинству гриферов это, в конце концов, надоест и они уйдут.

Недостоверная информация

Всегда проверяйте собранную в Сети информацию по другим источникам. Для проверки материалов обратитесь к другим сайтам или СМИ – газетам, журналам и книгам

Материалы нежелательного содержания

Используйте средства фильтрации нежелательного материала (например, MSN Premium's Parental Controls или встроенные в Internet Explorer®). Научитесь критически относиться к содержанию онлайн-материалов и не доверять им.

Заключение

Если вы будете соблюдать эти правила пользования Интернетом, то он будет безопасным. Что же делать, если неприятность все же произошла? Нужно обязательно рассказать все взрослому или позвонить по телефону Линии помощи «Дети онлайн» 8 800 25 000 15. Всегда есть выход! Ты имеешь на это право!

Ребята, а давайте ответим на вопрос, который был в начале нашего занятия.

А может ли Интернет быть безопасным?

(Возможные ответы: да, если соблюдать правила, критически оценивать информацию, не сообщать личную информацию и т.д.) Молодцы! Думаю, что зная свои права, вы будете более защищенными в виртуальном мире.

Да и наш кластер – теперь ваш помощник! Повесьте его около своего компьютера, и он обязательно поможет вам. Спасибо за работу. Надеюсь, что Интернет - просторы будут для вас безопасны.

Анкета для учащихся

1. Назовите самые распространенные признаки компьютерной зависимости?

2. Знаете ли Вы развитию каких заболеваний способствует ненормированная работа на компьютере? Назовите их.

3. Какие опасности вы видите для себя как для пользователя в Интернете? Назовите их.

4. Знаете ли Вы как правильно и без ущерба для здоровья пользоваться Интернетом?_____

5. Как Вы оцениваете информацию в Интернете с точки зрения её достоверности? Вы верите всему, что написано в Интернете, что обсуждается в чатах?

6. Знакомы ли Вы с этикетом общения в чатах, форумах, при отправке сообщений по электронной почте?

7. С какой целью вы выходите в сеть Интернет?

8. Знаете ли вы правила организации поиска информации в Интернет? Назовите их.

9. Каково ваше отношение к спаму? Как против него бороться, и является ли он информационной опасностью?

10. Устаёте ли Вы от информации? И если да, то от какой?

11. Знаете ли вы что такое компьютерный вирус?

12. С какими признаками проявления вирусов вам приходилось сталкиваться в практике работы на ПК?

13. Какие действия вы предпримите, если заподозрите, что компьютер заражён?

Рекомендации родителям, с помощью которых посещение сети Интернет (далее – Интернет) может стать менее опасным для детей:

- посещать Интернет вместе с детьми, поощрять детей делиться с родителями их успехами и неудачами в деле освоения Интернет;

- объяснять детям, что если в Интернет что-либо беспокоит их, то им следует не скрывать этого, а поделиться с близкими своим беспокойством;

- объяснить ребенку, что при общении в чатах, использовании программ мгновенного обмена сообщениями (типа ICQ, Microsoft Messenger и т.д.), использовании он-лайн игр и других ситуациях, требующих регистрации, нельзя использовать реальное имя;

- помочь ребенку выбрать регистрационное имя, не содержащее никакой личной информации. Объяснить ребенку, что нельзя выдавать свои личные данные, такие как домашний адрес, номер телефона и любую другую личную информацию, например, номер школы, класс, любимое место прогулки, время возвращения домой, место работы отца или матери и т.д. Объяснить, что в реальной жизни и в Интернет нет разницы между неправильными и правильными поступками;

- научить детей уважать собеседников в Интернет. Убедить их в том, что бы они понимали, что правила хорошего тона действуют одинаково в Интернет и в реальной жизни;

- объяснить детям, что никогда не стоит встречаться с друзьями из Интернет. Люди могут оказаться совсем не теми, за кого себя выдают;

- приучить детей спрашивать о том, в чем они не уверены так, как далеко не все, что дети могут прочесть или увидеть в Интернет - правда.

- установить контроль над посещением детей Интернет с помощью специального программного обеспечения. Это поможет отфильтровывать вредоносное содержание, выяснить, какие сайты на самом деле посещает ваш ребенок и что он там делает.

- установить правила использования домашнего компьютера и постараться найти разумный баланс между нахождением в Интернет и физической нагрузкой ребенка. Кроме того, необходимо, чтобы компьютер стоял не в детской комнате, а в комнате взрослых.

- выработать семейное соглашение о работе детей в Интернет

Если дети хотят посещать Интернет, следует выработать вместе с ними соглашение по использованию Интернет.

В нем необходимо однозначно описать права и обязанности детей, четко сформулировать ответы на следующие вопросы:

- какие сайты могут посещать дети и что они могут там делать;
- сколько времени дети могут проводить в Интернет;
- что делать, если детей что-то беспокоит при посещении Интернет;
- как защитить личные данные;
- как следить за безопасностью;
- как вести себя вежливо;
- как пользоваться чатами, группами новостей и службами мгновенных сообщений.