

Муниципальное бюджетное общеобразовательное
учреждение средняя общеобразовательная школа №2
с. Раевский муниципального района Альшеевский район
Республики Башкортостан



Классный час
«Безопасность в Интернете»

11 класс

Классный руководитель Шагапова З.В.

с. Раевский, 2017 г.

Классный час «Безопасность в Интернете»

Цели:

- 1) познакомить обучающихся с опасностями, которые могут подстергать нас в Интернете, с правилами сетевого этикета; повысить внимание к вопросу обеспечения безопасности детей в Интернете;
- 2) развивать умение избегать опасностей в сети Интернет, отличать достоверные сведения от недостоверных, избегать вредной и опасной информации;
- 3) воспитывать культуру поведения в сети Интернет, используя правила сетевого этикета.

«...Важная задача для нас – научить людей пользоваться новыми современными технологиями так, чтобы они смогли защитить себя и свою семью».

*Ольга Дергунова,
Президент Microsoft России и СНГ*

30 мая 2011 года на заседании Президиума Государственного совета и Комиссии по реализации национальных проектов и демографической политики было предложено провести в школах в первый день нового учебного года уроки медиа-безопасности. Даная инициатива была поддержана Президентом России Д. А. Медведевым. Поэтому сегодня мы проводим урок-медиабезопасности.

Необходимость проведения такого урока возникла в результате того, что Интернет постепенно проникает в каждую организацию, учебные заведения, в наши дома. Число пользователей Интернета в России стремительно растёт, причём доля молодёжи 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 не удивительно: ведь в Интернете можно найти информацию для реферата, сообщения, 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 появилась своя преступность, хулиганство, вредительство и прочие малоприятные явления. Виртуальность общения предоставляет людям с недобрыми намерениями дополнительные возможности причинить вред детям. В последнее время появилось много материалов агрессивного и социально опасного содержания. Поэтому необходимо помнить о существовании подобных угроз и уделять повышенное внимание вопросу обеспечения безопасности в Интернете.

Медиа-безопасность. Это задача семейного и школьного воспитания. Это знание элементарных правил отбора информации, а также умение ею пользоваться. Знакомство с правилами ответственного и безопасного поведения в современной информационной среде, способах защиты от противоправных посягательств в сети Интернет и мобильной (сотовой) связи. Зная эти правила, вы должны научиться

критически относиться к сообщениям СМИ (вт.ч. и электронных), мобильной связи, научиться отличать достоверные сведения от недостоверных, уметь избежать вредной и опасной информации.

Обеспечение государством информационной безопасности детей, защита физического умственного и нравственного развития несовершеннолетних, а также их человеческого достоинства во всех медиа-услугах и электронных СМИ – требование международного права.

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, причиняющий вред их здоровью и развитию» устанавливает правила медиа-безопасности детей при обороте на территории России продукции СМИ. Закон определяет информационную безопасность детей как состояние защищённости, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью, физическому, психическому, духовному и нравственному развитию. Кроме того, принят Федеральный закон Российской Федерации от 21 июля 2011 года № 251-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О защите детей от информации, причиняющий вред их здоровью и развитию», направленный на защиту детей от разрушительного и травмирующего их психику информационного воздействия, переизбытка жестокости и насилия в общедоступных источниках массовой информации, от информации, способной развивать в ребёнке порочные наклонности, сформировать у ребёнка искажённую картину мира и неправильные жизненные установки.

Давайте попытаемся разобраться какие же опасности могут подстергать нас в Интернете?

Преступники в интернете

Вредоносные программы

Интернет мошенничество и хищение данных с кредитной карты

Азартные игры

Онлайновое пиратство

Интернет - дневники

Интернет-хулиганство

Недостоверная информация

Материалы нежелательного содержания

ДЕЙСТВИЯ, КОТОРЫЕ ПРЕДПРИНИМАЮТ 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, пытаясь 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.

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.

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 – 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.

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.

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.

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.

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

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.

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

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.

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.

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.

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.

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

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

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

Достоинство Интернета – в том, что он расширяет среду общения до размеров Земного шара. Написал несколько слов, нажал на кнопку, - и письмо ушло, хоть соседу по парте, хоть президенту. В этой простоте кроются опасности: возникает иллюзия доступности и вседозволенности, которая ещё усугубляется тем, что при электронном общении мы не видим лица собеседника и не всегда можем правильно понять его реакцию.

За время существования Интернета сформировался целый кодекс поведения в Сети, для его обозначения иногда используется специальный термин «нетикет» (сетикет) – соединение слов «net» (сеть) и этикет. Одной из важных задач медиа-безопасности является умение общаться в социальных сетях, не обижая своих виртуальных друзей, и избегать выкладывать в Сеть компрометирующую информацию или оскорбительные комментарии. Правила сетевого этикета просты и похожи на правила поведения в реальной жизни: не грубить, не отвлекаться от заданной темы, недопустимо попусту тратить чужое время, следить за своим языком, следить за правописанием (с появлением компьютера правила русского языка никто не отменял, и читать неграмотный текст с экрана также неприятно, как и на бумаге).

- А сейчас вашему вниманию предоставляется сказка

«Золотые правила безопасности в Интернете»

В некотором царстве, Интернет – государстве жил-был Смайл-царевич-Тьютор-Королевич, который правил славным городом СоцОБРАЗом. И была у него невеста – прекрасная Смайл-царевна – Он - лайн-Королевна, день и ночь проводившая в виртуальных забавах. Сколько раз предупреждал её царевич об опасностях,

подстерегающих в сети, но не слушалась его невеста. Не покладая рук трудился Смайл-царевич, возводя город СоцОБРАЗ, заботился об охране своих границ, обучая жителей города основам безопасности жизнедеятельности в Интернет-государстве. И не заметил он, как Интернет-паутина всё-таки затянула Смайл-царевну в свои коварные сети. Погоревал – да делать нечего: надо спасти невесту. Собрал он рать королевскую- СоцОбразову - дружину дистанционную и организовал «Регату» премудрую. Стали думать головы мудрые, как вызволить царевну из плена виртуального и придумали они «Семь безопасных правил поведения в Интернете». Сложили их в котомку Смайл-царевичу и отправился он невесту искать. Вышел на поисковую строку, кликнул по ссылкам, а они тут как тут: стелялки-убивалки Соловья- разбойника, порно-сообщества Змея-искусителя-Горыноча, товары заморские купцов шоповских, сети знакомств –зазывалок русалочьих... Как же найти отыскать Смайл-царевну? Крепко задумался Тьютор-королевич, надел щит антивирусный, взял в руки меч-кладенец кодовый, сел на коня богатырского и ступил в трясины непролазную. Долго бродил он , отбиваясь от реклам шоповских зазывающих и спамав завлекающих и остановился на распутье игрища молодецкого трёхуровневого. Стал читать надпись на камне, мохом заросшую: на первый уровень попадёшь – времени счёт потеряешь, до второго уровня доберёшься – от родных-близких отречёшься, а третий пойдёшь – имя своё забудешь, и понял Смай-царевич, что здесь надо искать невесту. Взмахнул он своим мечом праведным и взломал код игрища страшного! Выскользнула из сетей разомкнувшихся Смайл-царевна, осенила себя паролем честным и бросилась в объятия своего суженного. Обнял он свою невесту горемычную и протянул котомочку волшебную со словами поучительными: «Вот тебе оберег от козней виртуальных, свято соблюдай наказания виртуальные!»

- Всегда помни своё Интернет-королевское имя (E-mail, логин, пароли) и кланяйся всем подряд (не регистрируйся везде без надобности)
- Не поддавайся ярким рекламным указателям и не ходи тропинками путанными на подозрительные сайты: утонуть в трясине можно!
- Если пришло письмо о крупном выигрыше – это «Лохотрон-грамота»: просто так выиграть невозможно, а если хочешь зарабатывать, нужно участвовать в полезных обучающих проектах!
- Чтобы не забыть тропинку назад и вернуться во время, бери с собой клубок волшебный (заводи себе будильник, садясь за компьютер)!
- Если хочешь дружить с другими царствами-государствами, изучай полезные социальные сервисы, они помогут тебе построить «Мой королевский мир», свой царский блог, форум для глашатаев важных- друзей званых!
- Не забывай обновлять антивирусную программу – иначе вирус Серый Волк съест весь твой компьютер!
- Не скачивай нелегальные программные продукты – иначе пираты потопят твой корабль в бурных волнах Интернет!

Залилась сослезливой слезами дева красная, дала своему наречённому слово честное, что не будет пропадать в забавах виртуальных, а станет трудиться на благо народа своего СоцОБРАЗа, сама начнёт обучаться и помогать будет люду заблудшему и погрязшему в трясине сетевой. И зажили они дружно и счастливо с мечтою расширит границы образовательные.

Интернет- новая среда взаимодействия людей. Помните простые рекомендации, изложенные в хорошо известных образах:

-Повернись избушка, ко мне передом, к лесу задом! Современный Интернет не только обширная, но и настраиваемая среда обитания! В нём хорошо тому, кто может обустроить в нём собственное пространство и научиться управлять им. Записывайте свои впечатления в блог, создавайте галереи своих фотографий и видео, включайте в друзья людей, которым вы доверяете. Тогда вместо бессмысленного блуждания по сети ваше Интернет общение будет приносить пользу и вам, и другим людям.

- Не пей из болотца! Козлёночком станешь! Даже когда мы испытываем жажду, мы не будем пить из грязной лужи. Также и в среде Интернет, случайно оказавшись в месте, которое производит отталкивающее впечатление агрессивного и замусоренного пространства, лучше покинуть его, поборов чувство любопытства. Это защитит нас от негативных эмоций, а наш компьютер от вирусов, «червяков» и другого вредоносного программного обеспечения.

-Волку дверь не открывай! Создатели интернет позаботились о том, чтобы мы были защищены от тех, кто хочет причинить нам какой-либо вред. У них ничего не получится, если только мы сами не откроем им дверь- не сообщим им наши пороки или другую важную информацию, не загрузим на свой компьютер сомнительные файлы или не дадим возможность пользоваться нашей сетью незнакомым людям. Но именно так мы поступаем в обычной жизни, когда сначала спрашиваем «Кто там?». А только потом открываем дверь! А сейчас попытайтесь из предложенных вариантов выбрать (на ваш взгляд) три основных правила безопасного поведения в сети

1. Не забывай обновлять антивирусник;

2. Не регистрируйся, где попало, не пиши все данные о себе;

3. Не открывай все сайты подряд, ходи по Интернету с определенной целью.

4. Некоторое ограничение во времени (не "целыми днями")

5. Родительский контроль

6. Школьный контроль