Министерство образования и молодежной политики Ставропольского края

Ставропольская краевая молодежная общественная организация
«Творческий союз «Звездный ветер»

ОСНОВЫ БЕЗОПАСНОГО ИНТЕРНЕТА:
методические материалы

Материалы
социально ориентированного проекта
«Навигатор жизни»

Ставрополь - 2017

Основы безопасного Интернета:
методические материалы

Автор-составитель: Жукова Е.В., гласный специалист министерства образования и молодежной политики Ставропольского края.

Верстка: О.В. Скиперская, президент Ставропольской краевой молодежной общественной организации «Творческий союз «Звездный ветер».

Основы безопасного Интернета: методические материалы // Материалы социально ориентированного проекта «Навигатор жизни», реализуемого при поддержке Федерального агентства по делам молодежи . 2017 г. –60 с.

Методические материалы разработаны в рамках реализации социального проекта «Навигатор жизни», направленного на распространение научных знаний и проведение просветительской работы среди молодежи по формированию знаний, навыков активного и пассивного противодействия деструктивным воздействиям угроз безопасности человека.

Методические материалы изданы за счет средств государственной поддержки, выделенных в качестве гранта в соответствии с соглашением № 17-ю от 30.09.2016 года о предоставлении гранта победителю конкурса молодежных проектов Всекавказского молодежного форума – юридическому лицу.

Уважаемые коллеги!

Предлагаем вашему вниманию комплект методических рекомендаций по проведению урока безопасного поведения в сети Интернет.

В настоящее время, в период стремительного развития информационных технологий, Интернет стал неотъемлемой частью образовательного процесса и жизни в целом. Использование Интернета в образовательной деятельности связано со многими позитивными факторами. Оно дает возможность формирования позитивной траектории социализации обучающегося, подготовки его к решению жизненно важных проблем, предоставление выбора «виртуального» социального окружения.

Использование ресурсов и сервисов сети Интернет в системе образования позволяет:

- существенно повысить наглядность и доступность учебного материала за счет использования дополнительной информации (в том числе аудиовизуальной) с высокой степенью актуальности;
- облегчить работу учителя при подготовке к урокам;
- снизить отрицательное влияние нежелательных Интернет-ресурсов на школьников, что имеет место при неупорядоченном, стихийном использовании ими ресурсов сети Интернет.

Вместе с тем, существующие риски негативного влияния сети Интернет на здоровье пользователя связаны с использованием недопустимого объема информации, представляемой на экране, ее несоответствием возрастным и индивидуальным особенностям обучаемого, существованием киберугроз, которыми изобилует Интернет. Развитие и обеспечение информационной грамотности признаны эффективной мерой противодействия посягательствам на детей с использованием сети Интернет.

Работа с обучающимися должна проводиться в зависимости от их возрастных особенностей.

Достичь высоких результатов в воспитании невозможно без привлечения родителей. Очень часто родители не понимают и недооценивают угрозы, которым подвергается школьник, находящийся в сети Интернет. Родители, с ранних лет передавая ребенку знания основ безопасности дома и на улице, между тем «выпуская» его в Интернет не представляют себе, что точно также нужно обучить его основам безопасности в сети.

Комплексное решение поставленной задачи со стороны семьи и школы позволит значительно сократить риски причинения различного

рода ущерба ребенку со стороны сети Интернет. Ребенок абсолютно беззащитен перед потоком информации, сваливающейся на него из сети. Наша задача выработать в нем критическое мышление.

Материалы методических рекомендаций могут быть использованы для проведения по данной тематике: классного часа, урока-экскурсии или иного внеклассного занятия во внеурочной деятельности школьного педагога или в форме занятия в системе дополнительного образования.

Цель данных рекомендаций – обеспечение методический поддержки педагогов, организующих и проводящих занятия по интернет безопасности детей путем привития им навыков ответственного и безопасного поведения в среде Интернет.

Обеспечение информационной безопасности и воспитание информационной культуры должно стать приоритетным направлением работы образовательной организации.

1. Материал для проведения урока «Общая безопасность в интернете»

В наши дни интернет стал неотъемлемой частью нашей жизни. С его помощью мы получаем информацию, общаемся, обмениваемся данными, оплачиваем товары и услуги, отправляем документы для поступления в вузы и делаем многое другое.

Главное преимущество этого ресурса в его глобальности и доступности информации в интернете для большинства человечества. Вы обращали внимание, что сегодня практически у каждого есть под рукой хотя бы один, а то и два гаджета. По мнению социологов, россияне, например, проводят в интернете не менее трех часов ежедневно.

Еще одно преимущество интернета в том, что с его помощью расстояние между людьми на планете сегодня резко сократилось, общение со всем миром стало обыденным и легким, а доступ к любой информации – простым и быстрым. Благодаря глобальной сети нынче на поиск нужной информации, на проведение финансовых, технологических и общественных операции затрачивается намного меньше времени.

Сегодня каждый может написать и опубликовать в сети статью на любую тему, и у него найдутся читатели и поклонники. Мы не говорим о социальных сетях с целым ворохом друзей.

Упражнение. Интернет в мире и мир в Интернете
Задача: осознать влияние Интернета на общество в целом и образ жизни отдельного человека в частности.
Необходимые материалы: видеоролик Google «BigTent: Как бы выглядел мир, если бы Интернет изобрели тысячи лет назад» (http://www.YouTube.com/watch?v=TMJMjyyEAZU/).
Время проведения: 15 минут.
Рекомендуемый возраст: 6-9 класс.
Процедура проведения:
Интернет — это одно из величайших изобретений, которое кардинальным образом изменило наш мир. С целью оценки масштаба этого влияния ведущий предлагает группе посмотреть видеоролик «BigTent в Москве», а затем обсудить его.
Обсуждение:
- На ваш взгляд, что еще изменилось бы, если бы Интернет существовал уже тысячи лет? Как выглядел бы современный мир, если бы Интернет еще не был изобретен?
- В чем заключаются основные преимущества существования Интернета в сравнении с жизнью в офлайновую эпоху?

Вместе с тем интернет таит в себе опасности — о них необходимо знать, чтобы избегать их.

В первую очередь, когда заходит речь о пагубном воздействии всемирной паутины, на ум приходит интернет-зависимость. А ведь это не просто какой-то мифический термин.

Научно доказано, что около 10% пользователей интернета зависимы от него, причем треть из них считают интернет таким же важным как дом, еда и вода. В Южной Корее, Китае и Тайване интернет-зависимость уже расценивают как проблему национального масштаба.

Однако не только этим может навредить интернет. Слишком долгое пребывание за монитором сказывается не лучшим образом на зрении, нахождение длительное время в неправильных позах – пагубно влияет на опорно-двигательный аппарат.

К недостаткам интернета можно отнести наличие в нем информации, способной навредить психике. С помощью сети мошенники могут узнать личную информацию о человеке и использовать ее в своих целях. А еще всемирная паутина нередко становится распространителем вирусов, способных навредить компьютерной системе.

Упражнение. Киберфанаты против киберскептиков

Задачи:

-осознание наличия в Интернете широкого спектра возможностей по поиску различного рода полезной информации;

- осознание наличия в Интернете негативной, вредной и опасной информации;

- осознание того, что информацию в Интернете нельзя оценивать однозначно негативно или позитивно, и поэтому важно научиться разбираться в качестве информации и уметь оценивать ее пользу и вред.

Необходимые материалы: доска, фломастеры, листочки с клейким краем двух цветов.

Время проведения: 35 минут.

Рекомендуемый возраст: 7-9 класс.

Процедура проведения:

Данное упражнение позволяет актуализировать знания школьников о различных видах информации в Интернете, а также их представления о позитивном и негативном контенте в Сети. Предложенный способ работы позволяет обсудить возможности и риски информации в Интернете, опираясь на опыт и знания самих участников.

В помощь учителю в качестве примеров «плюсов» сети Интернет можно привести наличие новой, полезной, разнообразной информации; общение; доступность информации (быстро, бесплатно, удобно искать); развлечения, игры; помощь в учебе; доступность музыки, фильмов, книг; возможность заработать; покупка товаров.

В качестве примеров «минусов» можно выделить чрезмерное использование, интернет-зависимость; вред для здоровья; ненужная информация, реклама, спам; вирусы; негативная, недостоверная, опасная, нецензурная информация; мошенничество и вымогательство.

Упражнение состоит из двух этапов.

Этап 1. Сбор данных (10 минут)

Ведущий раздает участникам листочки с клейким краем: по три — одного цвета и по три — другого, например красного и зеленого. Затем он просит участников написать на зеленых листочках, какая информация в Интернете, по их мнению, является полезной и нужной, а на красных — какая информация может быть вредной, негативной или опасной. На выполнение этого задания дается 5 минут. Затем ведущий проводит на доске вертикальную линию, которая делит пространство пополам. Левая половина доски сверху обозначается знаком «+» (позитивный контент), а правая — знаком «-» (нега- тивный контент). Участники должны подойти к доске и приклеить свои листочки, накоторых обозначена полезная информация в Интернете, на половину

доски, отмеченную «+», а листочки, на которых обозначена негативная информация, — на половину доски, отмеченную «-». После этого все садятся на места, и ведущий предлагает обсудить полученный результат. Как правило, школьники легче и активнее обсуждают позитивную информацию, которую они находят в Интернете.

Обсуждение:

- Что было легче вспомнить: полезные или вредные виды информации в Интернете?
- Чем «позитивная» сторона доски отличается от «негативной»? Почему?
- Хотели бы вы что-то еще добавить на доску или изменить что-то на ней? Почему?

Этап 2. Анализ данных (25 минут)

Ведущий озаглавливает левую половину доски (флип-чарта) со знаком «+» — «Киберфанаты», а правую со знаком «-» — «Киберскептики». Он объясняет, что киберфанаты — это большие поклонники и защитники Интернета, считающие, что он дает много возможностей пользователям, а киберскептики — те, кто могут покритиковать Интернет и считают, что в Сети много негативной информации, которая легкодоступна и оказывает плохое влияние на людей. Он просит каждого из участников выбрать для себя наиболее подходящую для них группу — «Киберфанаты» или «Киберскептики» — и подойти к соответствующей половине доски.

Обсуждение:

- Почему киберфанатов получилось больше, чем киберскептиков (или наоборот)?
- Как вы думаете, кого в мире больше: киберфанатов или киберскептиков? Почему?

Далее собравшиеся в группы участники получают задания: киберфанаты — проанализировать все листочки с позитивной информацией, киберскептики — с негативной. Если группы сильно различаются по количеству участников, ведущий просит добровольцев (их можно выделить из тех, кто причисляет себя в равной мере и к киберфанатам, и к киберскептикам) перейти в другую команду.

Задача каждой группы состоит в том, чтобы проанализировать информацию на своей стороне доски и сформулировать пять основных аргументов в пользу своей позиции. Ведущий предлагает участникам в группах:

- подсчитать количество повторяющихся ответов;

- классифицировать все ответы и выделить 5-7 категорий;
- дополнить результаты на доске, если, по мнению группы, на ней не хватает каких-то важных категорий.

На выполнение этого задания группам дается 10 минут. Затем группам предоставляется возможность защитить свою позицию в дискуссии, которая проводится в форме дебатов. Каждая группа по очереди приводит свои аргументы. От каждой группы в дебатах участвует одному представителю, остальные помогают ему и подсказывают. Ведущий выступает модератором дебатов и следит за тем, чтобы аргументы были конструктивными и не повторялись. Выступления представителей групп и получившиеся классификации позитивной и негативной информации обсуждаются классом.

Обсуждение

- На основании каких критериев можно оценить информацию в Интернете как полезную и как вредную?
- Какие существуют способы защиты от негативной информации в Сети?
- Какая позитивная информация может помочь в борьбе с негативной?
- Узнали ли вы что-то новое о возможностях получения информации в Интернете?

Одна из самых серьезных проблем, с которой могут столкнуться пользователи Всемирной сети, - это интернет-мошенничество.

Мошенники могут быть хорошо оснащены и использовать самые разные инструменты и мето-ды — например, вирусное программное обеспечение (вирусы), поддельные сайты, мошеннические письма, перехват и подбор паролей к учетным записям в социальных сетях и почтовых сервисах.

2. Вирусы

Вирусы могут распространяться с помощью вложенных файлов и ссылок в электронных письмах, в сообщениях в социальных сетях, на съемных носителях, через зараженные сайты. При этом сообщение с вирусом может быть получено как от постороннего человека, так и от знакомого, но уже зараженного участника социальной сети или почтовой переписки. Зараженными могут быть сайты, как специально созданные в целях мошенничества, так и обычные, но имеющие уязвимости информационной безопасности.

Сегодня большинство вредоносных программ создаются либо для того, чтобы рассылать спам, либо для того, чтобы красть у пользователя важные данные. Если данные действительно важные и дорогостоящие, то для их похищения злоумышленники специально разрабатывают троян, который гарантированно будет работать на компьютерах в той организации, откуда нужно украсть данные.

Осуществить внедрение такого вредоносного ПО обычно гораздо проще не через интернет, а с помощью записанных на флэшках «троянов».

Флэшки могут подбрасываться как в здание, где располагается организация, так и размещаться, скажем, на парковке рядом с ним, где их с большой долей вероятности наверняка найдёт именно сотрудник нужной организации. Поэтому если вы нашли на улице или в здании флэшку, не торопитесь радостно вставлять её в свой компьютер – лучше сначала отдайте системному администратору, который просканирует её и при необходимости обезвредит.

Бывают и более банальные, но не менее эффективные способы заразить компьютер недостаточно осторожного пользователя. Например, от знакомого по Skype Вам может прийти сообщение в духе «Посмотри, на этой фотографии он так похож на нашего друга (одноклассника)!», ну и, конечно, ссылка на саму эту фотографию. При переходе по ссылке фотография почему- то не открывается в браузере, а сохраняется на жесткий диск, но мало кто на это обращает внимание. Хотя они-то как раз и должны насторожить! В общем, когда «фото» не открывается, пользователь «входит» в папку с ним, и видит, что это не просто abcd.jpg, а abcd.jpg.scr, то есть, исполняемый файл, а его компьютер уже заражен вирусом

Рекомендации:

- Использовать антивирусное программное обеспечение с обновленными базами вирусных сигнатур.
- Не открывать вложенные файлы или ссылки, полученные по электронной почте, через социальную сеть или другие средства коммуникаций в интернете, не удостоверившись, что файл или ссылка не содержит вирус.
- Внимательно проверять доменное имя сайта (например, www.yandex.ru), так как злоумышленники часто используют похожие имена сайтов, чтобы ввести жертву в заблуждение (например, www.yadndex.ru).
- Обращать внимание на предупреждения браузера или поисковой машины о том, что сайт может угрожать безопасности компьютера.

- Не подключать к своему компьютеру непроверенные съемные носители.

- Не поддаваться на провокации злоумышленников, например, с требованием перевести деньги или отправить SMS, чтобы снять блокировку компьютера.

Упражнение. Детективное агентство

Задача: обсуждение действий по обеспечению технической безопасности в ситуациях столкновения с вредоносными программами.

Необходимые материалы: доска или флип-чарт, распечатанные кейсы для участников (рабочая тетрадь), распечатанные решения кейсов для ведущего.

Время проведения: 20 минут.

Рекомендуемый возраст: 7-9 класс.

Процедура проведения:

Данное упражнение позволяет выявить, насколько грамотно учащиеся умеют действовать в ситуации столкновения с техническими проблемами при работе в Интернете, и познакомить их со способами решения подобных проблем. Ведущий делит участников на четыре команды. Он предлагает участникам побыть в роли сотрудников особого детективного агентства в сфере компьютерной безопасности. В это агентство обращаются люди, которые столкнулись с техническими проблемами при использовании Интернета. Задача сотрудников агентства — помочь людям не только решить проблему, но и дать рекомендации о том, как не попадать в похожие ситуации вновь. Командам раздаются кейсы, время на их решение и обсуждение — 10 минут. Далее каждая команда по очереди кратко представляет проблему и предлагает решение. Остальные участники могут задавать вопросы и участвовать в дискуссии. Ведущий по необходимости дополняет и корректирует ответы участников.

Обсуждение:

- Что на ваш взгляд важнее: знание и личная бдительность пользователя или хорошие программные средства защиты (например, антивирус)? Почему?

- Какие основные правила безопасного поведения в Интернете вы сегодня узнали?

Ключи к заданиям для учителя

1. Можно порекомендовать Коле создать несколько почтовых ящиков. Один — для регистрации на различных ресурсах. Второй — для личной и деловой переписки, и этот ящик никогда не следует использовать для регистрации аккаунтов и указывать в Интернете. Также, чтобы важные

письма не уходили в спам, необходимо создать фильтр в настройках почты для адреса этого отправителя — тогда письма от него всегда будут попадать во «Входящие».

2. Катя часто заходит в социальные сети со своего смартфона, на котором не установлен антивирус. Самая очевидная причина частых взломов — троянская программа, которая ворует пароли каждый раз, когда Катя их вводит. Кате необходимо установить антивирус на свой смартфон и выполнить полную проверку устройства. Только после того, как вредоносная программа будет обнаружена, нужно поменять пароль в очередной раз. Следует помнить о том, что каждое устройство, с помощью которого пользователь входит в свой аккаунт, должно быть защищено от вредоносных программ.

3. Оля совершила шесть неправильных действий.

1. Оля была невнимательна, когда вводила пароль и логин на сайте. Она не проверила адрес в адресной строке. Официальный адрес социальной сети — http://odnoklassniki.ru/. Скорее всего, это был фишинговый сайт.

2. Оля оставила злоумышленникам свой номер телефона.

3. Оля позвонила на телефон якобы «Службы поддержки», то есть мошенников.

4. Оля перешла по незнакомой ссылке, которую ей продиктовали.

5. Оля скачала неизвестную программу.

Оле необходимо установить антивирус на компьютер и мобильный телефон, а также подключить услугу у своего сотового оператора, которая позволяет ограничивать получение нежелательных смс-собщений с коротких номеров и отправку смс-собщений на короткие номера.

Чтобы восстановить аккаунт мамы, нужно зайти на официальный сайт «Одноклассников», заполнить заявку на восстановления пароля. Новый пароль придет на номер телефона или адрес почты, указанный ее мамой при регистрации на сайте. Возможно, аккаунт вообще не взломан.

4. Ни в коем случае не стоит отсылать смс на короткий номер. Саша может попробовать получить код разблокировки на сайте антивирусов Dr.Web или KasperskyLab. Также производители антивирусов рекомендуют скачивать и устанавливать специальные утилиты, размещенные на их официальных сайтах. Саша может попробовать запустить диспетчер задач и отключить работающую программу с вирусом. Если эти меры не помогут, необходимо будет обратиться ко взрослым или в службу поддержки. В любом случае после устранения проблемы необходимо будет установить на пострадавший компьютер лицензионный антивирус. Саше нужно знать, как ведет себя компьютер при заражении различными

вредоносными программами, чтобы быть готовым правильно среагировать в подобной ситуации.

3. Мошеннические письма

Одной из разновидностей спама являются «Нигерийские письма». Этот вид мошенничества называется так потому, что письма особое распространение получили в Нигерии, причем еще до распространения Интернета они распространялись по обычной почте, начиная с середины 1980 годов.

С появлением интернета «Нигерийские письма» стали нарицательным понятием. Как правило, у получателя письма просят помощь в многомиллионных операциях, обещая солидные проценты с сумм. Если получатель согласится, у него выманиваются всё большие суммы денег на сборы, взятки и т. д. В худших вариантах жертве предлагается полулегально прибыть в Нигерию, где его либо арестовывали за незаконное прибытие в страну и у него вымогаются деньги за освобождение, либо похищали с целью получения выкупа.

Мошенничество профессионально организовано: у мошенников есть офисы, работающий факс, часто мошенники связаны с правительственными организациями, и попытка получателя письма провести самостоятельное расследование не обнаруживает противоречий в легенде. Сделка подаётся как «безвредное» беловоротничковое преступление, что мешает жертве обратиться к властям.

Разумеется, обещанных денег жертва в любом случае не получает: их просто не существует. Спамеры оперативно реагируют на ситуацию в мире, отслеживая очаги нестабильности. Поэтому постоянно появляются новые разновидности «Нигерийских» писем — например, «кенийские» или «филиппинские». Во время войны в Ираке активно шли спамерские рассылки «иракского» спама.

Рекомендации:

- Внимательно изучить информацию из письма. Проверить достоверность описанных фактов. Если в письме предлагается большая выгода за незначительное вознаграждение, скорее всего, оно мошенническое.
- Игнорировать такие письма.

Упражнение. Нигерийские письма
Задача: научиться обнаруживать мошеннические письма.

Необходимые материалы: доска или флип-чарт, распечатанные письма для участников (рабочая тетрадь).

Время проведения: 20 минут.

Рекомендуемый возраст: 7-9 класс.

Процедура проведения:

Учитель делит аудиторию на несколько групп. Каждой группе предлагается образец «нигерийского письма» (рабочая тетрадь) и задание:

1. Внимательно прочитайте текст письма.
2. Выделите в нем моменты, указывающие на то, что это спам.
3. Перечислите факты, указанные в письме, которые кажутся вам недостоверными, подозрительными.

После того, как группы выполнят задание, начинается коллективное обсуждение. Результаты работы группы представляет один ученик. Все остальные ученики могут задавать вопросы и высказывать свое мнение.

Учитель на доске записывает главные особенности «Нигерийских писем», которые нашли ученики, дополняет, систематизирует.

Обсуждение:

- Как можно распознать «нигерийское письмо»?
- Как вы думаете кто авторы «нигерийских писем»?
- Какую цель преследуют авторы «нигерийских писем»?
- Можно ли считать безвредными «нигерийские письма»?

4. Получение доступа к аккаунтам в социальных сетях и других сервисах

Злоумышленники часто стремятся получить доступ к аккаунтам жертвы, например, в социальных сетях, почтовых и других сервисах. Украденные аккаунты они используют, например, для распространения спам-писем и вирусов.

Мошенники могут получить доступ к учётной записи жертвы следующими способами:

- Заставить жертву ввести свои данные на поддельном сайте.
- Подобрать пароль жертвы, если он не является сложным.
- Восстановить пароль жертвы с использованием «секретного вопроса» или введенного ящика электронной почты.
- Перехватить пароль жертвы при передаче по незащищенным каналам связи.

Как правило, для кражи данных об аккаунтах используются фишинговые сайты. Фишинг (англ. phishing, от fishing — рыбная ловля, выуживание) — вид интернет-мошенничества, целью которого является

получение доступа к конфиденциальным данным пользователей — логинам и паролям. Злоумышленники создают фишинговые сайты, копирующие интерфейс известных ресурсов, а жертвы вводят на них свои логины и пароли, не понимая, что сайты поддельные.

Рекомендации:

- Использовать сложные пароли (сложные пароли состоят как минимум из 10 символов, включают буквы верхнего и нижнего регистра, цифры и специальные символы, не содержат имя пользователя и известные факты о нем).
- Никому не сообщать свой пароль.
- Для восстановления пароля использовать привязанный к аккаунту мобильный номер, а не секретный вопрос или почтовый ящик.
- Не передавать учетные данные — логины и пароли — по незащищенным каналам связи (незащищенными, как правило, являются открытые и общедоступные wi-fi сети).
- Внимательно проверять доменные имена сайтов, на которых вводятся учетные данные.

Упражнение. Угадай пароль

Задача: осознание рисков, связанных с ненадежностью пароля.
Необходимые материалы: флип-чарт или доска, маркеры.
Время проведения: 15 минут.
Рекомендуемый возраст: 6-9 класс.

Процедура проведения:

Упражнение направлено на то, чтобы продемонстрировать участникам основные риски, связанные с ненадежностью пароля в Интернете. В ходе упражнения участники выступают в роли злоумышленников и «взламывают» аккаунт от почты, подбирая пароль из четырех символов.

Ведущий выбирает одного участника, который на листке пишет пароль из четырех разных цифр и, закрывая листок от всех, передает его ведущему. Кроме ведущего никто больше не должен видеть пароль. Всем остальным участникам ведущий предлагает на некоторое время представить себя в роли злоумышленников, которые хотят взломать пароль, открывающий доступ к аккаунту от почты. Они должны угадать эти четыре цифры и их порядок.

Ведущий объясняет участникам, что есть разные способы и программы, помогающие злоумышленникам взламывать пароли. В данном случае у участников есть «программа» в лице ведущего, который после каждой попытки сообщает «взломщикам», сколько цифр

из названной комбинации есть в пароле. Причем ведущий не должен называть, какая цифра или какие цифры верные. Например, он может ответить, что в предложенной комбинации одна цифра из четырех входит в загаданный пароль. Как правило, участники легко угадывают четыре цифры, которые есть в комбинации. Задача считается решенной, когда пароль отгадан.

Подводя итоги, ведущий объясняет участникам, что данный метод подбора паролей является очень распространенным способом взлома аккаунта и его применяют настоящие злоумышленники. Специально созданные для этого программы способны перебирать большое количество комбинаций символов за короткий промежуток времени, делают это намного быстрее человека. Чем проще пароль, тем легче его взломать, поэтому необходимо знать ключевые правила создания, использования и хранения паролей, чтобы сократить риск взлома аккаунта.

Обсуждение:

- Как вы думаете, легко ли настоящим злоумышленникам взломать простой пароль?
- Можно ли придумать такой пароль, который очень сложно взломать?

5. Защита личных данных и другой конфиденциальной информации в Интернете

Право на неприкосновенность частной жизни — фундаментальное право человека, находящееся на одно уровне с правом на жизнь и свободой совести. Оно действует и в виртуальной среде.

Современные школьники с легкостью и энтузиазмом пользуются самыми различными сервисами и приложениями: пишут во Вконтакте и Facebook, выкладывают фотографии в Instagram, «чекинятся» с помощью Foursquare (геолокационный сервис, помогающий пользователям узнать, где были их друзья, и найти новые интересные места, чтобы провести время), используют карты для навигации, заказывают такси с помощью мобильных приложений и т. п. Но мало кто задумывается, что эти сервисы умеют определять местоположение пользователя и используют это в своих целях.

Location-based service — тип информационных и развлекательных услуг, основанных на определении текущего местоположения мобильного устройства пользователя. Некоторые сервисы, основанные на местоположении (например, Foursquare), являются развлекательными и построены по принципу социальных сетей, некоторые сервисы

помогают работать с местоположением (карты, навигаторы, пробки) и больше используются в практических целях.

LBS-сервисы в наше время стали незаменимы для многих людей. Такие сервисы позволяют быстрее и проще получить нужную информацию. В частности, при работе с онлайн-сервисами на мобильных телефонах использование LBS-функций позволяет получить контент, связанный с местом нахождения пользователя. Однако активное использование LBS делает особенно актуальным вопрос конфиденциальности пользовательских данных.

Важно научить юных пользователей Интернета внимательно относиться ко всему, что они сами размещают о себе в Сети. В различных интернет-сервисах можно включить специальные настройки приватности и делиться определенной информацией с ограниченным кругом лиц, а сервисы автоматического определения местоположения, о которых шла речь выше, можно в принципе отключить (родителям это желательно сделать на мобильных устройствах ребенка). Одновременно важно объяснить детям, насколько важно оставлять определенную информацию за пределами социальных сетей: например, не делать «чекинов» в каждой точке маршрута в течение дня или не сообщать в социальной сети, что вся семья уехала в отпуск на несколько месяцев, оставив пустой квартиру.

В отличие от взрослых современные подростки настолько привыкли открыто делиться информацией в социальном пространстве, что не всегда понимают, что в определенных случаях следуют соблюдать осторожность и элементарную бдительность.

Важным аспектом защиты неприкосновенности частной жизни является информирование пользователей и предоставление людям информации, которая позволяет им понимать и управлять сбором и использованием данных о них. Конфиденциальность данных в Интернете зависит от способности контролировать как объем предоставляемой личной информации, так и список лиц, которые имеют доступ к этой информации.

Упражнение. Аватар

Задача: обсуждение особенностей самопрезентации в Интернете.

Необходимые материалы: бумага и карандаши.

Время проведения: 15 минут.

Рекомендуемый возраст: 6–9 класс.

Процедура проведения:

Данное упражнение проводится с целью знакомства участников группы с понятием самопрезентации в социальных сетях, в частности, с помощью аватаров. В начале упражнения ведущий спрашивает

участников, знают ли они, что такое аватар. Заслушав несколько ответов, ведущий подводит итог, используя информацию о значении слова «аватар».

Аватар, аватара, ава, аватарка (юзерпик; от англ. userpicture — картинка пользователя) — графическое представление пользователя. Может быть двухмерным изображением (картинкой, фотографией) на форумах, в чатах, социальных сетях, мессенджерах либо трехмерной моделью в виртуальных мирах, многопользовательских играх. Термин «аватар» позаимствован из философии индуизма, в переводе с санскрита — «нисхождение». Используется для обозначения явления Бога из духовного мира. Самые известные — дашаватары или дасаватары — десять великих аватар Вишну.

Особое внимание участников следует обратить на то, что аватар является визитной карточкой профиля пользователя в социальных сетях и других сервисах для общения.

Затем ведущий раздает участникам бумагу и карандаши и предлагает им за три минуты нарисовать свой аватар. Участники не должны подписывать листы и показывать друг другу свои рисунки, для этого участники располагаются каждый за своим столом или на расстоянии друг от друга. Ведущий предупреждает о необходимости завершать работу точно в отведенное время.

После того как все участники выполнят задание, ведущий собирает рисунки и прикрепляет их к доске. Участники разглядывают рисунки и пытаются угадать, чей это аватар.

После можно переходить к обсуждению результатов упражнения.

Обсуждение:

- Какие аватары больше всего понравились участникам и почему?
- Какие образы использовались участниками для создания аватаров и почему? Какие образы используются ими при создании профилей в различных социальных сетях, почему?
- Как вы думаете, какую роль аватары играют в процессе общения в социальных сетях?

6. Достоверность информации

Несмотря на то, что современные школьники способны отыскать в Интернете все, что угодно, часто они не задумываются о качестве той информации, которую они используют. Вследствие одной из своих особенностей — свободы информационных потоков — Интернет оказался питательной средой для распространения ложных сведений.

Даже объективная информация, попадая в Интернет, со временем претерпевает изменения: намеренно или случайно искажается пользователями, устаревает, но практически никогда не исчезает, а только накапливается.

Часто в потоке информации бывает не так просто выделить ценные материалы. Благодаря тому, что в Интернете каждый имеет право голоса, мнения профессионалов перемешиваются с не всегда компетентными бытовыми точками зрения, научная информация вытесняется псевдонаучными текстами субъективного характера, а «проверка временем» часто замещает собой достоверность информации.

Дезинформация пользователя в Интернете может происходить умышленно, ради привлечения внимания (мигающие баннеры с кричащими названиями, например «Найден секрет вечной молодости!», «Она рассказала всю правду о своей жизни!» и т. п.), ради политических манипуляций, умышленных розыгрышей и др. В иных ситуациях дезинформация происходит в силу некомпетентности авторов или нехватки точных сведений.

В Интернете существуют крупные ресурсы, где вымысел полностью замещает правду, например «Абсурдопедия». Статьи этой «энциклопедии» написаны по всем законам научной справки, но в полном соответствии с лозунгом «Факты — ничто, фарс — все». Эта фраза как нельзя лучше объясняет природу интернет-юмора. На сайте можно ознакомиться с теоремой о неравенстве полов, узнать, как клонировать динозавра и т. п. Читая «Абсурдопедию», пользователь не сомневается, что перед ним ложная информация, поданная в парадоксальной манере.

В современной журналистике второе рождение переживает жанр «газетной утки». Речь идет о фэйковых (от англ. fake — подделка) новостях, призванных намеренно ввести читателей в заблуждение. Многие фэйки настолько сложно отличить от правды, что информация расходится по Интернету с колоссальной скоростью и порой даже попадает на телевидение, прежде чем кто-нибудь распознает обман. Примером может служить новостное агентство FogNews.ru или один из самых популярных англоязычных псевдоновостных порталов TheOnion.com, специализирующиеся на создании фэйковых новостей. Попав на эти сайты, сложно сходу сообразить, что все прочитанное является вымыслом, потому что большая часть статей выглядит весьма убедительно. Новости составлены по всем законам жанра, включая ссылки на авторитетные источники. Однако стоит обратить внимание на информационные поводы: МКС будет собирать космический мусор с помощью огромного магнита, созданного в Сколково, а в прошлую пятницу сквозь всемирно известную Щель Времени в наши дни из XVIII

века выпал кот короля Фридриха Вильгельма и т. п. Разумеется, подобный сетевой юмор рассчитан на адекватного читателя, который в нагромождении наукообразных слов способен распознать полную чушь.

Как в Интернете отличить фэйк от правды?

Существует ряд приемов, с помощью которых можно идентифицировать фэйки, представленные даже в самом завуалированном виде. В первую очередь, новость, которая подается как правдивое сообщение, но при этом повествует о невероятных фактах и сомнительных событиях, скорее всего, является недостоверной. Часто в таких новостях используются ссылки даже на вызывающие доверие источники. В этом случае необходимо удостовериться в действительности ссылок. Если источником указан иностранный сайт, стоит ознакомиться с оригиналом. Очень часто в подобных новостях авторы ссылаются на неопределенные источники фактов: «по исследованиям ученых», «как сообщили конфиденциальные источники» и т. п.

Ложное сообщение выдает и манера изложения. В текстах используются обобщения, преувеличения и наукообразные слова. Необходимо обращать внимание на любые логические неточности, очевидные несоответствия, эмоциональные высказывания. Особенно должны настораживать броские заголовки статей и баннеры, призывающие прочитать горячую новость. Такие заверения, как «Это не легенда!» или «Это не розыгрыш!», на деле могут означать прямо противоположное.

Существует множество различных критериев, которыми можно оперировать при оценке достоверности информации. Один из способов — анализ сообщения. Здесь можно следовать классическому журналистскому подходу четырех шагов.

1. Подтверждение информации как минимум в трех независимых друг от друга источниках (так называемое «Правило трех»). Прежде чем принять за истину какую-либо информацию в Интернете, необходимо проверить ее еще как минимум в двух независимых друг от друга источниках. Если факт подтверждается несколькими ресурсами, стоит проверить, не являются ли они клонами друг друга.

2. Сопоставление полученной информации с уже известной по этой теме. В поисках какого-либо материала не стоит полагаться на первые попавшиеся источники. Сбор сведений из нескольких авторитетных источников, сопоставление разных точек зрения на проблему, а также опора на здравый смысл всегда позволит выяснить, является ли информация надежной и достоверной.

3. Проверка достоверности полученной информации у авторитетных экспертов. Если того требует необходимость, можно

проверить информацию, проконсультировавшись с экспертами в данной области. Сегодня в Интернете собрано множество различных советов и рекомендаций, в том числе напрямую связанных с жизнью и здоровьем. Как можно догадаться, далеко не все из них являются правдой, а некоторые могут представлять серьезную опасность. Если какая-то информация вызывает сомнение, то лучше обратиться к человеку, в профессионализме которого вы уверены.

4. Запрос у источника информации дополнительных деталей, подтверждающих истинность основного сообщения. Еще один способ — обратиться к автору информации напрямую. Если на сайте нет контактов автора или же он вообще не указан, то, скорее всего, такая информация является перепечаткой, соответственно она могла утратить свою точность и истинный смысл.

Помимо традиционных способов проверки информации, Интернет предоставляет особые возможности, например недоступные при проверке печатных текстов. В Интернете можно выяснить статус документа, рейтинг источника и его популярность, частоту использования данного материала другими источниками, получить сведения о компетентности и статусе автора материала с помощью специальных поисковых сервисов Интернета, проанализировать сайт, на котором находится информация, оценить квалификацию его авторов и т. п.

Таким образом, умение анализировать информацию в Интернете, подвергать ее критической оценке, сопоставлять различные факты и данные, а также бдительность и здравый смысл — необходимые условия для оценки надежности и достоверности информации в Сети.

Упражнение. Проверь информацию: мадагаскарская руконожка, или ай-ай

Задача: знакомство со способами объективной оценки информации в Интернете.

Необходимые материалы: компьютер с доступом к Интернету, проектор, по возможности компьютерный класс, где участники смогут работать группами по 3–5 человек, раздаточные материалы.

Время проведения: 30 минут.

Рекомендуемый возраст: 6-9 класс.

Процедура проведения:

При оценке достоверности информации можно опираться на ряд приемов, которые недоступны при анализе, например, печатных текстов. Данное упражнение знакомит школьников со способами объективной оценки информации в Интернете. Ориентируясь на предложенную

схему анализа сайтов, они учатся проверять источники информации и на этой основе делать выводы о достоверности предложенной информации.

В начале занятия ведущий спрашивает, смотрели ли участники мультфильм «Мадагаскар», и, если да — знают ли они, какое животное послужило прототипом героя Мориса — советника Короля лемуров. Правильный ответ: Мадагаскарская руконожка Ай-ай. Узнать подробнее об этом существе они смогут в следующем упражнении.

Участникам необходимо оценить предложенную информацию по ряду критериев, которые позволяют судить о надежности (достоверности) источников информации и принимать решение, в какой степени можно доверять информации на том или ином сайте в Интернете. Ведущий разбивает участников на четыре группы по 3–6 человек. Каждой группе предоставляется персональный компьютер или ноутбук с доступом в Интернет, специальная форма — лист со списком вопросов для анализа, а также карточки с заданиями.

Каждая группа оценивает один из предложенных сайтов, вытянув карточку. Ведущий отмечает, что участники всех групп в итоге должны заполнить предложенный бланк с вопросами, и на основе этого принять решение: можно считать информацию на данном сайте достоверной или нет. На выполнение задания дается 7 минут. Каждая группа анализирует предложенный сайт, затем подсчитывается количество положительных ответов. Представители групп рассказывают о своем сайте и выносят вердикт: верят они представленной на нем информации или нет.

Информация о предложенных сайтах для учителя:

1. Журнал ГЕОленок. Информация достоверна, грамотна, полна. Есть вопрос об актуальности, так как статья за 2005 год. Возможно, появились новые данные о руконожках (например, статистика).

2. Городская социальная сеть города Томска. Источник не научный, можно ознакомиться с информацией, но для использования в докладах, рефератах и т. п. лучше найти более надежный источник.

3. «Википедия» — хороший обзор информации, но всегда нужно проверять ее источники. Подходит для краткой справки, для более подробного обзора нужно находить первоисточники

4. Авторский сайт, созданный не специалистом. Постоянно обновляется, можно обратиться к автору напрямую и задать интересующие вопросы.

5. Научно-популярный сайт о лемурах, нет рекламы, но информация собрана любителями — для серьезной научной работы нужно будет обращаться к первоисточникам, но для школьного реферата по биологии, например, подойдет.

6. Сайт, созданный любителями, о животных. Информация свежая: новости постоянно обновляются. Нет рекламы

Информация про Мадагаскарскую руконожку для ведущего

Мадагаскарская руконожка (Daubentonia madagascariensis), или ай- ай, — млекопитающее животное из отряда полуобезьян, обитает в бамбуковых зарослях Мадагаскара. Открыл этот вид естествоиспытатель Пьер Соннер, во время работы на берегах Мадагаскара. По всем признакам ученые отнесли руконожку к особому виду лемуров. Однако, внешне ай-ай совсем не похож на обезьяну. Скорее всего, он сродни диковинной кошке или белке. Да и размерами напоминает обычного домашнего кота. Вес зверька невелик, всего 3 кг. По своим габаритам руконожка также не очень велика. В длину вместе с головой достигает всего 40 см. Зато довольно пушистый хвост руконожки, напоминающий хвост белки, гораздо длиннее тела, целых 60 см!

Длинный хвост подчеркивает маленький размер животного. Но самая удивительная особенность ай-ай — третий палец на передних конечностях. С его помощью зверек делает массу необходимых вещей. Это и расческа для меха, и своеобразное приспособление для питья (когда зверек утоляет жажду, он повисает на задних конечностях над водой, обмакивает в нее средний палец и затем тщательно облизывает его), для добычи и потребления корма. Когда-то ай-ай были довольно широко распространены в лесах Мадагаскара. Но после Второй мировой войны местные жители начали активно вырубать и выжигать девственные леса, расчищая место под поля для посевов, пастбищ и плантаций. Надо ли говорить, что подобная политика привела к нарушению всего экологического равновесия на уникальном острове.

Мадагаскар, давно изолированный от континента, обладает совершенно неповторимой флорой и фауной. В смертельной опасности оказалось множество эндемичных видов, и в том числе руконожки. К 1972–1974 годам в береговых лесах на востоке и северо-западе острова их оставалось всего около 50 штук. Так как естественных лесов, в которых жили зверьки, практически не осталось, они переселились на плантации. А там их, естественно, стали убивать как вредителей, хотя раньше местные жители относились к зверькам с большим почтением, считая, что в них вселяются души умерших.

Для увеличения численности ай-ай разводят в неволе, а позже возвращают их в дикую природу. Первая колония руконожек была создана в Центре приматов при Дьюкском университете в США. Вторая была основана в 1990 году в зоопарке, созданном Джеральдом Даррелом, на острове Джерси. Об этом Даррелл написал в своей книге «Юбилей ковчега». Экспедицией Даррелла были отловлены шесть

зверьков (две самки, два самца и два детеныша), которые и составили основу колонии. В августе 1992 году в специально построенном для ай-ай павильоне родился первый детеныш. Чуть раньше, в апреле того же года, в Дьюкском центре также родился первый маленький ай-ай, который вообще был первым малышом, родившимся в неволе вне Мадагаскара. Еще четыре колонии руконожек сейчас существуют в зоопарке города Сан-Франциско, в Винсеннском зоопарке в Париже и в двух зоопарках на острове Мадагаскар. Так что, возможно, удивительным ай-ай и удастся выжить.

Обсуждение:

- Знали ли вы раньше о существовании подобного животного? Если да, то, что именно вы о нем знали?
- Помогла ли информация, представленная на сайте, получить достаточно полное и объективное представление о Мадагаскарской руконожке?
- Считаете ли вы полученную информацию достаточно надежной? Почему?
- Можно ли утверждать, что в Интернете есть абсолютно надежные сайты?

7. Безопасность коммуникации в Интернете

Ведущей деятельностью подростков является общение со сверстниками. Умение распознавать потенциальные риски в процессе общения в Интернете, предотвращать их и справляться при столкновении с ними, то есть обеспечивать безопасность своей коммуникации в Сети, — очень важно.

Особое внимание необходимо обратить на ключевые коммуникационные риски, связанные с взаимодействием между подростками и другими пользователями в Интернете. К таким рискам относят общение с незнакомцами, агрессию и сексуальные домогательства.

Как показало исследование цифровой компетентности российских подростков, каждый третий школьник 12–17 лет сталкивался с коммуникационными рисками, которые возникают в процессе общения и межличностного взаимодействия в Сети. При столкновении с каким-либо риском, особенно впервые, дети и подростки зачастую не знают, как поступить.

Как показало исследование «Дети России онлайн», большинство российских школьников общаются в Интернете с людьми, которых они знают в реальной жизни. В то же время почти каждый второй ребенок

11–16 лет общается с теми, кто не связан с их реальной жизнью. Причем с возрастом количество таких контактов значительно вырастает.

Так, если только треть детей 11–12 лет имеют такие интернет-контакты, то в возрасте 15–16 лет больше половины школьников общаются с теми, с кем они познакомились в Сети.

Чаще всего такие контакты дети заводят в виртуальных мирах, онлайн-играх и чатах. Однако помимо возможностей накопления социального капитала в виде интернет-знакомых, такая практика может быть довольно рискованной.

Большое количество френдов в социальных сервисах работает на популярность подростка, поэтому многие знакомятся и добавляют в списки друзей всех подряд. Таким образом, они допускают незнакомых людей к своей личной информации и могут подвергнуть себя риску. Как, например, 16-летняя школьница из Голландии, которая забыла установить настройки приватности встречи. Это приглашение было моментально растиражировано, и в результате домой к девушке пришли 4 000 человек.

Такие случаи не редкость: в Гамбурге на день рождения к девочке пришли 1 500 пользователей Facebook, увидевших приглашение, а в США на празднование 15-летия Ребекки Джавело собрались прийти 21 000 пользователей, из-за чего пришлось отменить вечеринку и вызвать отряд полиции для охраны дома.

Настройки конфиденциальности публикаций — необходимая мера для обеспечения безопасности личных данных. Некоторую информацию не стоит публиковать вовсе. Как, например, сделала одна девушка из Австралии: она выложила в социальной сети свою фотографию с пачкой денег. Это фото заинтересовало преступников, которые вскоре наведались домой к ее матери с ножом и дубинкой. К счастью, женщина не пострадала, а грабителям пришлось довольствоваться небольшой суммой денег, так как фото было сделано в другом доме. Но этот случай показал, насколько опасна может быть необдуманная публикация в Сети.

Доступ случайных интернет-знакомых к личной информации не единственная проблема. Когда общения в Сети становится недостаточно, многие хотят перенести его в реальную жизнь. Как показало исследование «Дети России онлайн», 47 % детей общались в Интернете с кем-либо, с кем они никогда не общались в реальной жизни, а каждый пятый (21 %) лично встречался с интернет-знакомыми.

Девочки немного чаще, чем мальчики соглашаются на такие встречи. Причем по мере взросления таких встреч становится больше. При этом только у пятой части детей, ходивших на встречи с онлайн-знакомыми, родители знали об этом.

Треть детей, встречавшихся с незнакомцами из Интернета, довольно активны в поиске новых друзей в Сети: за последний год они познакомились как минимум с пятью людьми. Причем большинство этих новых знакомых никак не связаны с реальным кругом общения ребенка. Каждый третий ребенок из тех, кто ходил на личные встречи, пережил негативный опыт разочарования. Большинство этих детей рассказывали о том, что собирались на встречу и даже брали с собой сопровождающего. Но чаще всего это были их сверстники, только каждый десятый ребенок говорил взрослым о том, что идет на встречу с интернет-знакомым, и единицы брали с собой взрослого.

Подавляющая часть детей не знает, как поступать, если на встрече с интернет-знакомым произошло что-то плохое. Мало кто пытается предпринять какие-либо действия, чтобы впоследствии оградить себя от обидчика. Половина детей обращаются за социальной поддержкой, но чаще всего к друзьям. В этой ситуации именно взрослые — родители и учителя — должны объяснять детям, каким образом нужно вести себя с людьми, с которыми они знакомятся в Интернете.

Упражнение. Кто твой друг?

Задачи:

- демонстрация рисков, связанных с общением с незнакомцами в Интернете;
- выделение признаков, на которые следует обращать внимание при знакомстве с другими людьми в Интернете;
- обсуждение правил поведения, которых следует придерживаться при общении с незнакомцами в Интернете;
- поиск способов, как обезопасить себя при встрече в реальной жизни с интернет-знакомыми.

Необходимые материалы: набор карточек №1, набор карточек №2.

Время проведения: 35 минут.

Рекомендуемый возраст: 7–9 класс.

Процедура проведения:

Данное упражнение проводится с целью информирования участников об основных рисках, связанных с общением с незнакомцами в Сети. Ведущий предлагает группе разделиться на шесть команд, каждая из которых получает карточку с историей о знакомстве в Интернете и вопросами к ней (набор карточек №1, рабочая тетрадь).

Перед главным героем истории стоит выбор, встречаться ему или не встречаться со своим онлайн-знакомым в реальности. Каждой группе предстоит в течение 10 минут выполнить следующие задания:

1. обсудить свою историю;

2. принять решение: согласиться ли на встречу с онлайн-знакомым;

3. ответить на вопросы.

У ведущего остается набор пронумерованных карточек (набор карточек №2) с фактами и «реальными» историями онлайн-знакомых из заданий участников.

Ситуация 1.

Кто это? Анатолий, 19 лет, живет в Санкт-Петербурге, делает бизнес в онлайн-играх, продавая артефакты и персонажей. Анатолий хочет заработать, продав очередной магический щит. Также он планирует надавить на Ваню при встрече, чтобы выкупить Ваниного персонажа за бесценок и перепродать.

Особенности ситуации: У Вани нет никаких реальных свидетельств того, что Коля — тот, за кого себя выдает. Однажды «Коля» оправдал доверие Вани, действительно передав ему оплаченный товар, однако нет никаких оснований полагать, что на этот раз «Коля» поступит так же.

Возможное решение: Обсудить ситуацию с родителями (возможно, также стоит спросить разрешения на трату денег), получить их разрешение пойти на встречу одному или с кем-то из взрослых, выбрать для встречи людное место, сообщить родителям, куда и когда планируется идти.

Ситуация 2.

Кто это? Вика, 18 лет. Обсуждала с Машей свои чувства и переживания. Недавно записалась в студию танцев, где действует акция: «Приведи друга — получи скидку и подарок!».

Особенности ситуации: Хотя девушки переписывались на достаточно откровенные и личные темы, у Маши нет никаких свидетельств, что Вика говорила о себе правду.

Возможное решение: Обсудить ситуацию с родителями, рассказать им о Вике, получить их разрешение пойти на занятия танцами одной или с кем-то из взрослых, встретиться с Викой на занятиях.

Ситуация 3.

Кто это? Фанаты группы «Пикник», возраст — от 15 до 57. Личная встреча может привести к негативным последствиям.

Особенности ситуации: Хотя Аня общается онлайн с данными людьми уже давно, все они остаются незнакомцами в реальности и могут скрывать свои мотивы и поступки. Встреча проходит в слишком

позднее время и слишком далеко, чтобы по ее окончании возвращаться домой одной.

Возможное решение: Получить разрешение родителей, попросить кого-то из взрослых сопровождать Аню на этой встрече.

Ситуация 4.

Кто это? Максим, 37 лет, безработный.

Особенности ситуации: Нет никаких доказательств того, что Саша — тот, за кого себя выдает. Голос по телефону не всегда выдает возраст говорящего. Онлайн-переписка длится всего неделю. Саша, по-видимому, много спрашивал о Даше и мало рассказывал о себе. Саша был чрезмерно настойчив. После вечернего сеанса в кино пришлось бы слишком поздно возвращаться домой.

Возможное решение: Перед тем, как добавить Сашу в друзья, поинтересоваться у общих знакомых — действительно ли они знают Сашу в реальности или добавили просто так. Расспросить друзей, кто такой Саша. Не рассказывать о себе слишком много (информация о месте жительства и т. п.). Обсудить ситуацию с родителями, получить их разрешение. Предложить встретиться Саше первый раз среди общих знакомых и в присутствии кого-то из взрослых, которым доверяешь.

Ситуация 5.

Кто это? Алексей, 23 года, любитель карточных ролевых игр.

Особенности ситуации: У Виктора нет никаких доказательств, что Алексей — тот, за кого себя выдает. Встреча назначена в достаточно позднее время.

Возможное решение: Обсудить ситуацию с родителями, пойти на встречу вместе с кем-то из взрослых.

Ситуация 6.

Кто это? Владимир, 50 лет, хочет познакомиться с молодой девушкой для романтических отношений.

Особенности ситуации: У Наташи нет никаких доказательств, что Анна — та, за кого себя выдает. Уважаемые модельные агентства не будут искать моделей по фотографиям в социальной сети.

Возможное решение: Обсудить ситуацию с родителями, получить их разрешение пойти на встречу в сопровождении кого-то из взрослых

После обсуждения каждой группе предстоит огласить свое решение и ответы на вопросы. Члены группы по очереди зачитывают вариант профиля, отвечают на первый вопрос, второй вопрос и т. д. После того как участники ответили, пойдут ли они на встречу с этим

человеком, по номеру задания учитель достает карточку с «фактами» и рассказывает о «реальном» человеке, скрывающемся за профилем.

Завершая упражнение, ведущий демонстрирует участникам видеоролик «Развлечения и безопасность в Интернете» (http://www.YouTube.com/watch?v=3Ap1rKr0RCE&list=PLD70B32DF5C50A1D7/).

Обсуждение:

- Легко ли вам было принять решение? Если вы сомневались, то почему?
- Как вы решаете, кого добавлять к себе в друзья? Часто ли вы первым добавляете совершенно незнакомых людей?
- На что вы обращаете внимание, когда читаете профиль?
- Как вы решали, стоит ли встречаться с этим человеком? На что вы обратили внимание, а что, возможно, упустили?
- Как нужно поступать, если интернет-знакомый предлагает встретиться? Как обезопасить себя на встрече?
- Какие возможности предоставляет Интернет для знакомства и поиска новых друзей?
- На что следует обращать внимание при знакомстве в Интернете? Как следует себя вести? Что можно рассказывать, а что нет?
- Каким образом можно использовать возможности Интернета для знакомства с другими людьми, не подвергая себя риску?

8. Агрессия в Интернете: троллинг и кибербуллинг

Другой вид коммуникационных рисков — это вероятность столкновения с агрессией в Сети. Иллюзия анонимности и безнаказанности приводит к тому, что некоторые пользователи дают выход агрессии в Интернете, оскорбляя других пользователей или провоцируя их на конфликт.

Подобное поведение в Интернете называют «троллингом». Тролли публикуют провокационные сообщения, чтобы вызвать негативную реакцию пользователей и разжечь спор между участниками коммуникации. Троллинг может быть прямым (оскорбления участников, нарушение правил ресурса, подстрекание, ссоры) и замаскированным (сообщения не по теме, возвращение к другой острой теме, завуалированные сообщения, на первый взгляд позитивные). Тролли хотят получить реакцию в виде прямого конфликта. В перепалке с таким пользователем очень легко потерять над собой контроль и самому стать троллем.

Тролли могут стремиться вызвать раздражение участников коммуникации, но также их целью может быть унижение конкретного человека. В таком случае троллинг может переходить в целенаправленную травлю, или буллинг. По определению Игоря Кона, под буллингом обычно понимается запугивание, унижение, травля, физический или психологический террор, направленный на то, чтобы вызвать у другого страх и тем самым подчинить человека себе.

Во все времена это была одна из серьезных проблем подростковой среды. Развитие инфокоммуникационных технологий привело к распространению кибербуллинга — агрессивного, умышленного действия, совершаемого группой лиц или одним лицом с использованием электронных форм контакта, повторяющегося неоднократно и продолжительного во времени в отношении жертвы, которой трудно защитить себя.

Виртуальная среда, в которой происходит кибербуллинг, позволяет агрессорам чувствовать себя менее уязвимыми и менее ответственными за свои действия. Анонимность — основной фактор, отличающий кибербуллинг от обычного буллинга, осуществляемого в непосредственном контакте. Другие отличия проявляются в том, что кибербуллинг происходит вне школы, более скрыто и зачастую не позволяет видеть эмоциональные реакции жертвы.

Особенно актуальна эта проблема для пользователей 11–12 лет: почти треть детей этой возрастной группы становится жертвой буллинга чаще одного раза в неделю, что значительно превышает показатели в других возрастных группах. Нередко сами школьники выступают агрессорами. В России каждый четвертый ребенок признался, что за последний год обижал или оскорблял других людей в реальной жизни или в Интернете. При этом в России субъектов буллинга в два раза больше, чем в среднем по европейским странам.

Кибербуллинг — интернет-проблема, берущая начало в реальной жизни. Каждый десятый российский школьник сталкивается с буллингом в Сети. При этом, как показывают результаты исследования Фонда Развития Интернет, каждый второй ребенок, ставший жертвой кибербуллинга, также сталкивается с буллингом лицом к лицу. В европейских странах дети подвергаются кибербуллингу в среднем в два раза реже. Во многом, как и в случае с риском онлайн-знакомств, это связано с тем, что в Европе и США уже много лет в школах работают программы обучения цифровой грамотности, позволяющие существенно повысить навыки безопасного использования Интернета детьми.

Как дети справляются с такими ситуациями? Чаще всего они отдают предпочтение активным стратегиям совладания с ситуацией, причем каждый шестой из жертв буллинга выбирал конфронтационную

стратегию и таким образом сам мог стать агрессором. Нередко жертвы кибербуллинга формируют свои собственные стратегии в форме конкретных способов противодействия агрессорам в Интернете.

Значимым способом справляться с трудными онлайн-ситуациями оказался поиск информационной, эмоциональной и действенной поддержки. Большинство детей ищет социальную поддержку онлайн, в первую очередь у друзей. Показательно, что доля детей, обращающихся за помощью к родителям, в России ниже, чем в Европе. Среди 10 % детей, которые становились жертвами кибербуллинга, только каждый пятый родитель был осведомлен об этом (21 %), а более половины были уверены, что их ребенок не сталкивался с подобным риском (61 %). Очень мало кто из детей обращается за помощью к учителям или специалистам. Далеко не все дети умеют применять специальные онлайн-стратегии борьбы с кибербуллингом. Так, блокировка агрессора оценивается как высокоэффективная, но ее применяет только каждый третий ребенок, ставший жертвой онлайн-буллинга. Эти результаты подчеркивают необходимость развития программ по повышению цифровой грамотности взрослых: как родителей, так и специалистов, работающих с детьми.

Нередко дети могут являться одновременно как жертвами, так и агрессорами, поэтому важно обучать их тому, что поступки в онлайн-среде могут иметь существенные последствия в реальной жизни.

Во многих странах принимаются меры по борьбе с буллингом и кибербуллингом на уровне государственной политики (программы по предотвращению столкновения с цифровыми рисками, информационные кампании, обучение преподавателей). В некоторых странах, например в Канаде, приняты законы в отношении кибербуллинга в школьной среде. Так, в Онтарио кибербуллинг является правонарушением, которое может повлечь за собой временное или окончательное исключение агрессора из учебного заведения. В Европейских странах реализуются программы, которые направлены на обучение позитивному и безопасному использованию Интернета и в которых профилактике кибербуллинга придается большое значение. Во Франции с подачи Министерства образования совместно с рядом общественных организаций школьные учреждения получают информацию и рекомендации по предотвращению кибербуллинга. Одновременно интернет-компании развивают механизмы саморегулирования, с помощью которых пользователи могут пожаловаться на неприемлемый, в том числе агрессивный контент.

Упражнение. Не корми тролля

Задачи:

- знакомство с понятием буллинга и кибербуллинга;
- обсуждение последствий кибербуллинга.

Необходимые материалы: карточки с историями.

Время проведения: 30 минут.

Рекомендуемый возраст: 8–9 класс.

Процедура проведения:

Упражнение проводится с целью информирования участников о кибербуллинге как форме троллинга, его возможных последствиях и о способах противодействия.

Ведущий предлагает участникам разделиться на три группы. Участники могут объединиться в группы самостоятельно или по жребию: для этого, например, можно использовать разноцветные карточки.

Каждая группа получает карточку с историей о кибербуллинге и вопросами. В течение 5 минут участники в группах изучают свою историю и готовят ответы на предложенные вопросы. Ведущему следует подчеркнуть, что все истории основаны на реальных фактах.

После обсуждения представитель каждой группы зачитывает классу свою историю и представляет ответы на вопросы. После того, как все группы выступят, ведущий начинает общую дискуссию.

Обсуждение:

- Как вы думаете, могли бы такие истории произойти в вашей школе?
- Как чувствуют себя ученики, которые пострадали в результате этих историй (Соня, Миша, Лиза, Даша)?
- Как и почему возникают подобные ситуации? Кто может оказаться пострадавшим?

9. Секстинг и груминг

Во все времена подростки обсуждали между собой интимные темы. В наши дни разговоры о сексе перекочевали из узкого круга близких друзей в интернет-пространство.

Сегодня в России только начинают обращать внимание на такое явление как секстинг, хотя в ряде стран (например, в США, Канаде и Великобритании) о таком виде активности известно довольно давно. Слово «секстинг» (от англ. sex и texting) означает общение на тему секса посредством мобильного телефона или через Интернет.

Почти треть российских школьников встречали или получали лично сообщения сексуального характера в Интернете, причем более 15 % — раз в месяц и чаще. 4 % детей сами отправляют или пишут сексуальные сообщения. По проценту детей, получающих или сталкивающихся с сообщениями сексуального характера в Интернете, Россия опережает все европейские страны. Каждый четвертый подросток, столкнувшийся с секстингом, расстроился из-за этого. Девочки несколько сильнее и дольше переживают из-за получения сексуальных сообщений, чем мальчики. Дети 11–12 лет расстраиваются сильнее и переживают дольше, чем дети 13–16 лет.

Столкнувшиеся с секстингом подростки, как правило, остаются один на один с этой ситуацией: большинство из них ничего не предпринимает и никому ничего не рассказывает — ни родителям, ни друзьям. Таким образом, старшие и более опытные люди, которые могли бы поддержать ребенка, если он расстроен, найти нужные слова, помочь решить проблему и дать объективную оценку ситуации, ничего не знают.

Чаще всего подростки используют выжидательную стратегию. Каждый четвертый из пострадавших детей ждет, что проблема решится сама собой. Значительно реже подростки пробуют решить проблему сами (15 %) или пытаются заставить другого человека оставить их в покое (14 %).

Интернет-среда способствует растормаживанию и дает выход типичному для подростков интересу к общению на сексуальные темы. В то же время это серьезно повышает риск груминга — установления дружеских отношений с ребенком с целью сексуальной эксплуатации. Знакомство чаще всего происходит в чате, на форуме или в социальной сети от имени ровесника ребенка. Общаясь в процессе межличностного контакта («в привате»), неизвестное лицо входит в доверие к ребенку, пытаясь узнать личную информацию и договориться о встрече.

Данной проблеме обычно уделяется мало внимания, однако груминг — один из наиболее серьезных рисков для детей и подростков в Интернете. А если учесть, что наши дети, в отличие от их европейских сверстников, в большинстве своем никому не рассказывают о том, с чем столкнулись в Сети, то риск оказаться беззащитными перед преступниками возрастает еще больше.

Даже если ситуация не развернулась столь опасно, сам по себе опыт встречи с порнографией и непристойностями — очень нежелательный и преждевременный опыт.

10. Безопасность платежей в интернете

Фиктивные звонки от платежных сервисов

Мошенник может позвонить и представиться сотрудником банка или Яндекс.Денег и попросить продиктовать какие-либо платежные данные, например, пароль или код, пришедший на телефон. Его цель – выманить платежные данные, с помощью которых можно украсть деньги с карты или кошелька.

Рекомендации:

- Помнить, что банки и платежные сервисы никогда не просят сообщать – ни по почте, ни по телефону – пароль, пин-код или код из SMS.

- Никому не сообщать пароли, пин-коды и коды из SMS от своего кошелька или банковской карты.

Выманивание SMS-пароля незнакомцем

Пользователю может прийти SMS от банка или платежного сервиса с паролем для совершения платежа. Сразу после этого может позвонить человек, который скажет, что ввел этот номер мобильного телефона по ошибке и попросит сообщить код из SMS, которое только что пришло пользователю. На самом деле код из SMS — это пароль не к счету незнакомца, а к счету пользователя, с помощью которого злоумышленник может поменять настройки кошелька или интернет-банка, украсть деньги и т.д.

Рекомендации:

- Никому не сообщать пароли, пин-коды и коды из SMS, которые приходят на мобильный номер от банков, платежных сервисов, а также мобильных операторов.

Фальшивые письма от платежных сервисов

Пользователь может получить фальшивое письмо от имени Яндекс.Денег, своего банка или других платежных сервисов. Например, о том, что его счет заблокирован и для разблокировки необходимо перейти по ссылке и ввести свои данные. Единственная цель таких писем — заставить пользователя перейти на поддельный (фишинговый) сайт и ввести там свои персональные данные, которые будут украдены. В дальнейшем эти данные могут быть использованы, например, для доступа к счету пользователя. Кроме того, на таком сайте компьютер может быть заражен вирусом.

Рекомендации:

- Помнить, что платежные сервисы и банки никогда не рассылают сообщения о блокировке счета по электронной почте.

- Не переходить по ссылкам из таких писем и не вводить свои пароли на посторонних сайтах, даже если они очень похожи на сайт банка, Яндекс.Денег или другого платежного сервиса.

- Перед вводом своих платежных данных на каких-либо сайтах проверять название сайта в браузере. Например, вместо money.yandex.ru фальшивый сайт может называться money.yanex.ru

Фальшивые выигрыши в лотереи

Пользователь может получить сообщение (по телефону, почте или SMS), что выиграл некий приз, а для его получения необходимо «уплатить налог», «оплатить доставку» или просто пополнить какой-то счет в Яндекс.Деньгах. При этом, конечно же, никакого обещанного приза пользователь не получит.

Признаки фальшивой лотереи:

- Пользователь никогда не принимал участие в этой лотерее и вообще ничего о ней не знает;

- Пользователь никогда не оставлял своих личных данных на этом ресурсе или в этой организации, от имени которой приходит письмо;

- Сообщение составлено безграмотно, с орфографическими ошибками;

- Почтовый адрес отправителя – общедоступный почтовый сервис. Например, gmail.com, mail.ru, yandex.ru.

Фальшивые сайты авиабилетов

В интернете появилось множество сайтов, продающих поддельные авиабилеты. Цены на таких сайтах выгодно отличаются от других официальных онлайн- площадок для покупки билетов. Дизайн сайта при этом может выглядеть вполне аккуратно, а процесс платежа казаться привычным. На электронную почту даже придет подтверждающая бронь. Тем не менее, покупка билета будет фиктивной, о чем пользователь может узнать только уже в аэропорту или позвонив в авиакомпанию.

Рекомендации:

- Перед покупкой услуги или товара на незнакомом сайте обязательно нужно проверять отзывы о нём в интернете. Если не удается найти положительные отзывы или нет вообще никаких пользовательских сообщений об этом ресурсе, это должно насторожить. Сайт может быть создан за один день, а закрыться уже на следующий

или даже сразу после того, как на нем будет совершено несколько покупок.

Слишком выгодные покупки

Выгодную, но фальшивую покупку могут предложить пользователю где угодно – в интернет-магазине, в группе в соцсети, по электронной почте. На первый взгляд, объяснение может быть правдоподобное: подарили – не понравилось, это — распродажа конфискованного на границе товара и т.д. Оплатить такой товар предлагается онлайн — переведя деньги на банковскую карту, электронный кошелек или мобильный номер.

Рекомендации:

- Не доверять объявлениям о подозрительно дешевых товарах.
- Перед покупкой искать отзывы в интернете об интернет-магазине или частном продавце, который предлагает товар. Если информации нет или ее недостаточно, отказаться от покупки.

Фальшивые квитанции

Подделать могут не только сайт, но и бумажную квитанцию – например, за ЖКУ. (Также по поддельным квитанциям могут предлагать оплатить доставку книг, журналов и т.д. Для этих случаев действуют рекомендации из пункта «Слишком выгодные покупки».)

Рекомендации:

- Проверять реквизиты, указанные в платежке. Если они не совпадают с прежними, не оплачивать по счету. Информацию о смене реквизитов можно проверить по официальным телефонам (на квитанции они могут быть неверные).
- Проверять номер своего лицевого счета, указанный на платежке за ЖКУ. Он всегда один.
- Обратить внимание на дату получения платежки. Как правило, мошенники приносят поддельные квитанции раньше официальной даты оплаты, чтобы успеть собрать свои платежи.
- Настроить онлайн-платежи на заранее проверенные реквизиты и платить только по ним через проверенные сайты (сервис «Городские платежи», интернет-банк «Сбербанк.Онлайн» и др.)

Выпрашивание денег со взломанных аккаунтов в соцсетях или мессенджерах

Мошенник может попросить денег в долг под видом знакомого – например, через взломанный аккаунт в соцсетях или Skype. При этом перевести деньги он может попросить любым удобным способом – на электронный кошелек, банковскую карту, через интернет-банк.

Рекомендации:

- Всегда лучше перезвонить знакомому и уточнить, правда ли он сейчас нуждается в деньгах.

- Если возможности позвонить нет, можно задать какой-нибудь проверочный вопрос, ответ на который может знать только знакомый.

Фальшивые SMS якобы от знакомого

Мошенник может прислать SMS родителям пользователя с неизвестного номера, но якобы от имени пользователя. Например: «Мама, я попал в аварию, срочно нужны деньги, переведи их, пожалуйста, на этот номер телефона». «Папа, у меня проблемы, я в больнице, срочно нужны деньги, кинь их, пожалуйста, на этот кошелек. Маме не говори». Цель мошенника – выманить деньги у близких пользователя: они сами переведут их на указанный мобильный номер, электронный кошелёк или банковскую карту (в зависимости от того, какой способ будет указан в SMS).

Рекомендации:

- Связаться лично с пользователем, от имени которого прислано SMS, чтобы проверить информацию. Например, позвонить ему.

Бесплатное скачивание файлов с подпиской

Часто, чтобы скачать бесплатный файл или посмотреть видео в хорошем качестве без рекламы, сайты предлагают ввести мобильный номер. Если сделать это, включится подписка и с указанного номера могут начать списываться деньги.

Рекомендации:

- Не указывать свой мобильный номер на незнакомых сайтах.

- Если подписка уже оформлена, позвонить в службу поддержки оператора и попросить отключить её.

Платежные данные, которые нельзя **раскрывать**

Что делать? — если...

…вы потеряли карту. Срочно позвоните в банк, попросите ее заблокировать и перевыпустить. Желательно, с новым номером. Пока вы не заблокируете карту, любой, у кого она окажется в руках, сможет воспользоваться ей — например, оплатить дорогую покупку в интернет-магазине.

...вам пришло уведомление о платеже, который вы не совершали. Подайте в банк заявление о чарджбеке (отмене операции). В нём максимально подробно опишите произошедшее. Банк рассмотрит ваше обращение и вернет вам деньги. Не затягивайте с подачей заявления,

чтобы обработка вашего чарджбека успела произойти в срок от 30 до 60 дней с момента совершения операции.

...вы забыли пароль от электронного кошелька. Зайдите на сайт платежного сервиса и нажмите на ссылку "Восстановить пароль", система запросит мобильный номер, к которому привязан кошелёк. Укажите его, и на него придёт SMS с кодом для восстановления пароля.

Безопасность при оплате картами

Не сообщайте номер карты другим людям

Избежать проблем несложно, если придерживаться следующих **рекомендаций:**

- Храните банковскую карту в надежном месте.
- Не держите записанные пароли и коды рядом с картой.
- Заведите отдельную карту для покупок в интернете.
- Используйте для покупок в интернете только личный компьютер.
- Регулярно обновляйте антивирусную защиту компьютера.
- Старайтесь делать покупки в известных и проверенных интернет-магазинах.
- Перед подтверждением оплаты убедитесь, что в адресе платежной страницы в браузере указан протокол https. Только этот протокол обеспечивает безопасную передачу данных.
- Подключите в банке услугу SMS-уведомлений, чтобы получать сведения о всех совершаемых платежах.
- Сохраняйте отчеты об оплате и доставке товаров, которые вы получаете по электронной почте.
- Регулярно просматривайте в интернет-банке историю выполненных операций по вашим картам.

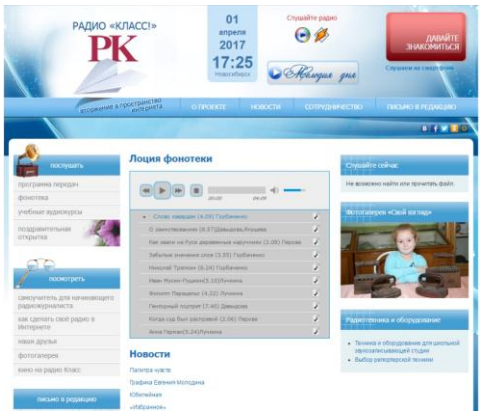
11. Использование Интернет-радио и Интернет-телевидения в образовательном процессе

На современном этапе информатизации образования образовательная функция журналистики получает новое наполнение. Это связано с изменением типа коммуникации, используемой журналистикой, что обеспечивает возможность организации диалоговых отношений. Данный процесс обусловлен развитием Интернет-журналистики, диалоговость которой является ее сущностным свойством. В этом процессе особую роль занимают Интернет-радио и Интернет-телевидение, обеспечивающие информационное взаимодействие всех участников образовательного процесса, освещая проблемы учебно-воспитательной, научно-исследовательской и просветительской деятельности как научных и образовательных учреждений, так и отдельных исследователей и педагогов.

Преимуществом Интернет-радио относительно эфирного радиовещания является возможность слушать его в любой точке планеты, где имеется доступ к сети Интернет.

Вместе с Интернет-радио активно развивается и Интернет-телевидение. Однако отличия в способах работы не позволяют считать Интернет- телевидение, занимающее все внимание зрителя, альтернативой Интернет-радио, режим работы которого позволяет слушателю параллельно заниматься другой работой (например, посещать сайты).

Каналы, позиционируемые себя как образовательное Интернет-телевидение или радио, представлены, в основном, познавательными программами, транслирующими музыкальные и театральные произведения, короткометражные фильмы для детей, документальные и научно-популярные фильмы. В отдельных случаях можно наблюдать трансляцию образовательных программ, способствующих лучшему пониманию и усвоению общеобразовательных предметов, а также дисциплин профессионального образования.



В качестве примера можно привести такие образовательные каналы, ведущие Интернет-вещание в России, как: Интернет-радио «КЛАСС!» http://radioclass.edu54.ru, транслирующее циклы познавательных и образовательных программ по трем направлениям – предметному,

профессиональному и культурному, где представлена информация о различных видах искусства; образовательный телевизионный канал «ПРОСВЕЩЕНИЕ» http://www.prosveshenie.tv, направленный на развитие образования, повышение престижа и социальной значимости научной деятельности, привлечение молодежи в науку, пропаганду достижений науки и техники, социализацию молодежи; телеканал «Юность.RU» http://yunostru.ru, транслирующий короткометражные фильмы для детей, способствующие лучшему пониманию некоторых предметов школьной программы и др.

Еще одной возможностью Интернет-радио и Интернет-телевидения можно отметить освещение научно-исследовательской и просветительской деятельности. Среди примеров такой возможности общероссийский образовательный телеканал телекомпании СГУ ТВ http://www.sgutv.ru, имеющий обширную видеотеку с записями лекций и передач выдающихся деятелей науки, искусства и т.д., а также телеканал Research Channel https://www.youtube.com/user/ResearchChannel, на котором освещаются работы исследователей, представляются различные научные открытия.

Еще одной возможностью является формирование образовательной среды средствами Интернет-радио и Интернет-телевидения.

Целями формирования такой образовательной среды могут быть:

- трансляция фрагментов лекций педагогов страны и зарубежья по наиболее актуальным вопросам различных областей образования;

- трансляция международных, всероссийских и региональных научно- практических конференций, образовательных семинаров, круглых столов и пр. для школьников;

- организация интервью с известными педагогами, ведущими учеными различных научных областей.

Современный уровень развития сети Интернет позволяет достаточно легко создать собственный вариант школьного Интернет-радио или Интернет-телевидения.

Одной из таких возможностей является использование существующих Web-сервисов для хранения и воспроизведения аудио-видео файлов (типа YouTube). В качестве примера действующего в Ставропольском крае Интернет-телеканалов можно привести Первый молодежный канал - https://www.youtube.com/channel/UCjlWlC1jhfoTvbC58CLScSw, рассказывающий об основных событиях в молодежной среде Ставрополья.

12. Организация сетевого взаимодействия учащихся с использованием возможностей социальных сетей и сервисов

Для современной школы важное значение приобретает организация коллективной научно-образовательной и творческой деятельности учащихся с использованием возможностей сети Интернет. Особый интерес при этом представляют возможности социальных сетей и сервисов для педагогической практики в творческих коллективах учащихся.

Говоря о творческих коллективах учащихся, имеются в виду не стихийно сформировавшиеся сетевые сообщества учащихся, а управляемые педагогами-профессионалами группы учащихся, в которых обучение организовано на основе современных образовательных сетевых технологий.

Понятно, что использовать только методы традиционного обучения в данном случае недостаточно, а важнейшими условиями формирования творческой активности учащихся являются соответствующее содержание учебного материала. Определяющими для сетевого взаимодействия являются не только совместная деятельность, но и само информационное взаимодействие (общение, коммуникация, диалог), связанные с этой совместной деятельностью.

Социальные сети и сервисы позволяют пользователям, действуя совместно, обмениваться информацией, хранить ссылки и документы, реализующие возможности технологий Мультимедиа, Гипертекст совместно создавать и редактировать публикации.

Такие социальные сервисы обеспечивают для учебной деятельности внутри сетевых сообществ следующие возможности:

- доступ к бесплатным и свободным электронным ресурсам учебного назначения;
- самостоятельное создание сетевого учебного контента;
- наблюдение за деятельностью других участников сетевого сообщества;

обращение друг к другу за разъяснениями;

- мотивирование помощи друг другу для успешного завершения работы; создание проблемных, поисковых, исследовательских и других совместных проектов учебного назначения.

Основные социальные сервисы

Вики (WikiWiki, http://ru.community.wikia.com/wiki) – приложение, поддерживающее коллективную работу множества авторов над общей коллекцией взаимосвязанных гипертекстовых записей.

Вики-систему можно рассматривать как эффективное средство для организации педагогической деятельности и коллективного создания творческих работ, как элемент сетевого учебного курса. В них участники совместно работают над созданием и редактированием гипертекстовых страниц. Вики – это достаточно простая и полная модель коллективного гипертекста, когда возможность создавать и редактировать любую запись имеет каждый участник сетевого сообщества. Это делает вики перспективным средством для коллективного написания гипертекстов, современной электронной доской, на которой могут писать группы и сети удаленных пользователей.

Возможно несколько способов размещения в сети собственного вики-проекта:

1) Использование площадки для вики-хостинга.

В настоящее время в сети Интернет большое количество сайтов предлагают возможность разместить и поддерживать свой собственный вики-проект. Наиболее популярными хостинг- площадками для таких вики-проектов являются Wikia (http://www.wikia.com) и Wikispaces (http://www.wikispaces.com).

2) Использование одной из российских площадок, на которых развернуты образовательные вики-проекты.

Наиболее крупным образовательным вики-сайтом является сайт Letopisi.Ru (http://letopisi.org) − общероссийский образовательный проект с международным участием, который существует уже более десяти лет. Участники этого учебного проекта добавляют к энциклопедии новые публикации и связывают их между собой.

Заслуживают внимания и региональные учебные вики-проекты, такие как:

ИнтеВики − обучающая площадка для проведения учебных проектов, тренингов программы Intel «Обучение для будущего»;

Псковская ВикиВики (http://wiki.pskovedu.ru/index.php) – проект, созданный на базе Псковского регионального центра дистанционного обучения;

Саратовская СарВики (http://wiki.saripkro.ru) Саратовского института повышения квалификации и переподготовки работников образования;

Тольяттинский вики-портал (http://wiki.tgl.net.ru) − открытая Интернет- площадка для поддержки творчества учителей, методистов, студентов и школьников.

Блог (от англ. blog или Web log – Интернет-дневник) – Web-сайт, основное содержимое которого составляют регулярно добавляемые записи, содержащие текст, графические объекты или аудио-, видео

материалы. Уже обиходным выражением стало слово «блоггинг» — постоянное ведение записей. Как правило, блоги – это личные записи, напоминающие дневник, но дневник публичный. Часто здесь содержатся аннотированные ссылки на другие Интернет-ресурсы. Каждому из сообщений, опубликованных в блоге, присваивается свой постоянный URL-адрес, по которому к сообщению можно обратиться. Наличие постоянной ссылки играет важную роль при установлении отношений между пользователями и сообщениями: если у сообщения нет устойчивого сетевого адреса, то оно не имеет статуса сетевого документа, на такое сообщение нельзя сослаться из другого документа, и оно не может быть найдено программными средствами.

Сетевой дневник можно использовать в различных **целях**, таких как:

- специфический персональный информационный помощник, хранящий записи и ссылки, для письма и размышлений с помощью компьютера;
- среда для записей событий собственной научной, деловой или личной жизни для себя, семьи или друзей (очевидно, что такая форма организации той или иной деятельности удобнее, чем рассылка массовых e-mail сообщений);
- платформа для ведения личного или коллективного сайта (такой сайт легко поддерживать, его обновление не требует специальных знаний);
- среда для сетевого сообщества, что вполне допустимо и оправданно, так как многие блоги предоставляют возможность публиковать в текстовых сообщениях мультимедийные и HTML-фрагменты, создавать перекрестные связи между несколькими ветвями дискуссий.

В педагогической практике блог может выполнять следующие **функции**:

- Официальные и неформальные записи директоров и учителей. Как правило, учащиеся и педагоги контактируют в условиях официальной школьной среды. Через блоги учителя и администраторы учебного заведения могут дать учащимся и их родителям доступ к неформальному обучению.
- Дневники учащихся. Для многих учащихся ведение сетевых дневников стало привычным, поэтому у администрации школ и учителей появляется возможность знакомиться с жизнью учащихся через наблюдение за их сетевой активностью.
- Web-сайты школ, построенные на технологии блогов. Многие сайты, кроме собственно сообщений, позволяют формировать на

странице блога подборки ссылок, календари, анкеты для опросов, размещать видеофрагменты и т.д.

- Блог-конспект, где размещено учебное содержание какой-либо темы.

- Создание сетевых сообществ учителей и учащихся, в которые объединяются многие учебные блоги.

Популярные платформы для создания личного блога

В сети имеется немало платформ, позволяющих создать личный блог. Их выбор обычно определяется функциональными возможностями, количеством знакомых блоггеров, которые уже есть на этой площадке, отсутствием рекламы.

Назовем только наиболее распространенные из них:

- Всевозможные социальные сети (например, «Вконтакте» https://vk.com), позволяющие делиться текстовой, видео- и аудиоинформацией, проводить опросы и т.д.

- Twitter (http://twitter.com) – микроблоггинг, позволяющий пользователям писать короткие текстовые заметки (не более 140 символов), является значительно более оперативным, чем блоги. В ходе создания новой записи Twitter показывает количество оставшихся символов, и это приучает авторов к точности и лаконичности.

- LiveJournal (Живой Журнал) — имеет множество инструментов для поддержки сетевых сообществ. Каждый пользователь или каждое сообщество Живого Журнала создают и формируют свою страницу, на которой появляются новые сообщения. Каждая из них создает свой новостной поток в формате RSS. Подписка на новости с любой страницы Живого Журнала выглядит как формирование «ленты друзей». Добавить человека в список своих друзей внутри Живого Журнала означает подписку на новости, которые этот человек пишет в своем сетевом дневнике. В результате множества таких «добавлений друзей» или подписок на RSS-обновления новостных потоков у каждого пользователя Живого Журнала формируется так называемая «френд-лента», где представлены новости, на которые он подписался.

- Blogger (http://www.blogger.com) – Web-сервис, позволяющий вести блог любому пользователю почтовой системы Google и создать индивидуальный стиль своей страницы. Сервис Blogger дает возможность пользователям открывать любое число блогов и проводить несложные опросы в ученических и учительских блогах. Кроме того, авторы блога могут редактировать CSS шаблоны страниц, публиковать записи блога по электронной почте и добавлять на страницу информационные потоки с персональных поисковых систем Google, о проведении конференций, с общедоступных новостных лент RSS.

- WordPress (http://wordpress.org) — платформа, которая позволяет вести блоги на удаленном сервере или установить систему как на своем компьютере, так и в локальной сети учебного заведения. WordPress поддерживает возможность размещения блогов на сервере пользователя. Порядок создания блога практически не отличается от действий в Живом Журнале. Приложение WordPress позволяет любому желающему развернуть свой собственный индивидуальный или коллективный блог.

Средства сетевых коммуникаций, которые можно использовать в образовательном процессе:

- средства коллективной работы социальных сетевых сервисов: вики- системы, блоги, Web-чаты, теги, закладки;
- социальные сети уже существующие или созданные организаторами сетевого взаимодействия (например, www.dnevnik.ru);
- видео- и телеконференции учебного назначения;
- учебные форумы, организация на форумах дискуссий, проблемных, поисковых, исследовательских, эвристических и других форм учебных Web-проектов;
- средства, предоставляемые сервисами поисковых систем (Google, Yandex);
- средства прямых речевых и визуально-речевых контактов (например, Skype).

Материал для проведений родительского собрания, родительского лектория, заседания родительского клуба «Основные правила защиты наших детей от Интернет опасностей»

Интернет постепенно проникает в каждую организацию, общественное и учебное учреждение, в наши дома. Число пользователей Интернета в России стремительно растет и молодеет, доля молодежи и совсем юной аудитории среди пользователей Всемирной сети очень велика. Для многих из них, он становится информационной средой, без которой они не представляют себе жизнь. Вместе с тем, 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.

Согласно ст. 5 Федерального Закона от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», к информации, запрещенной для распространения среди детей, относится информация:

1) побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;

2) способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;

3) обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, 112 предусмотренных настоящим Федеральным законом;

4) отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;

5) оправдывающая противоправное поведение;

6) содержащая нецензурную брань;

7) содержащая информацию порнографического характера.

Для защиты детей от опасностей в Интернете необходима активная позиция родителей. И, это не удивительно: ведь в Интернете можно найти информацию для реферата или доклада, послушать любимую мелодию, проверить свои знания в интернет конкурсах или

on-line тестированиях, 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 в Интернете появляется много материалов агрессивного и социально опасного содержания.

Взрослым нужно помнить о существовании подобных угроз и уделять повышенное внимание вопросу обеспечения безопасности детей в Интернете.

Правило 1. Установите вместе с детьми четкие правила посещения сайтов. Определите, какие сайты они могут посещать, какие – посещать нельзя. Выберите сайты, которые можно посещать вашему ребенку, и заблокируйте доступ к неподходящим материалам. Настройте параметры безопасности вашего компьютера.

Правило 2. Помогите детям выбрать правильное регистрационное имя и пароль. Убедитесь в том, что они не содержат никакой личной информации.

Правило 3. Объясните детям необходимость защиты их конфиденциальности в сети Интернет. Настаивайте на том, чтобы они никогда не выдавали своего адреса, номера телефона или другой личной информации; например, места учебы или любимого места для прогулки.

Правило 4. Не позволяйте Вашему ребенку встречаться с онлайн-знакомыми без Вашего разрешения или в отсутствии взрослого человека. Если ребенок желает встретиться с новым интернет-другом, следует настоять на сопровождении ребенка на эту встречу.

Интересуйтесь тем, куда и с кем ходит ваш ребенок. Общение в Интернете может повлечь за собой коммуникационные риски, такие как незаконные контакты (например, груминг, кибербуллинг и др.).

Даже если у большинства пользователей чат-систем (веб-чатов или IRC) добрые намерения, среди них могут быть и злоумышленники. В некоторых случаях они хотят обманом заставить детей выдать личные данные, такие как домашний адрес, телефон, пароли к персональным страницам в Интернете и др. В других случаях они могут оказаться преступниками в поисках жертвы.

Специалисты используют специальный термин «**груминг**», обозначающий установление дружеских отношений с ребенком с целью вступления в сексуальный контакт. Знакомство чаще всего происходит в чате, на форуме или в социальной сети от имени ровесника ребенка.

Общаясь лично («в привате»), злоумышленник входит в доверие к ребенку, пытается узнать личную информацию и договориться о встрече.

Предупреждение груминга:

Будьте в курсе, с кем контактирует в Интернете ваш ребенок, старайтесь регулярно проверять список контактов своих детей, чтобы убедиться, что они лично знают всех, с кем они общаются.

Объясните ребенку, что нельзя разглашать в Интернете информацию личного характера (номер телефона, домашний адрес, название/номер школы и т.д.), а также пересылать интернет-знакомым свои фотографии.

Если ребенок интересуется контактами с людьми намного старше его, следует провести разъяснительную беседу.

Не позволяйте Вашему ребенку встречаться с онлайн- знакомыми без Вашего разрешения или в отсутствии взрослого человека. Если ребенок желает встретиться с новым интернет-другом, следует настоять на сопровождении ребенка на эту встречу.

Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание, хулиганство, социальное бойкотирование с помощью различных интернет-сервисов.

Предупреждение кибербуллинга:

Объясните детям, что при общении в Интернете они должны быть дружелюбными с другими пользователями, ни в коем случае не писать грубых слов – читать грубости также неприятно, как и слышать.

Научите детей правильно реагировать на обидные слова или действия других пользователей. Объясните детям, что нельзя использовать Сеть для хулиганства, распространения сплетен или угроз. Старайтесь следить за тем, что Ваш ребенок делает в Интернете, а также следите за его настроением после пользования Сетью.

На что следует обращать внимание родителям, чтобы вовремя заметить, что ребенок стал жертвой кибербуллинга:

1) Беспокойное поведение. Даже самый замкнутый школьник будет переживать из-за происходящего и обязательно выдаст себя своим поведением. Депрессия и нежелание идти в школу – самые явные признаки того, что ребенок подвергается агрессии.

2) Неприязнь к Интернету. Если ребенок любил проводить время в Интернете и внезапно перестал это делать, следует выяснить причину. В редких случаях детям действительно надоедает проводить время в Сети. Однако в большинстве случаев внезапное нежелание пользоваться Интернетом связано с проблемами в виртуальном мире.

3) Нервозность при получении новых сообщений. Негативная реакция ребенка на звук электронного письма должна насторожить

родителя. Если ребенок регулярно получает сообщения, которые расстраивают его, поговорите с ним и обсудите содержание этих сообщений.

Правило 5. Научите детей уважать других в Интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде – даже в виртуальном мире.

Правило 6. Настаивайте, чтобы дети уважали собственность других в Интернете. Объясните, что незаконное копирование и использование чужой работы – текста, музыки, компьютерных игр и других программ – является кражей.

Правило 7. Обращайте внимание, сколько времени проводят ваши дети в Интернете, чтобы вовремя заметить признаки возникающей интернет- зависимости.

Предвестниками «**интернет-зависимости**» (синонимы: интернет-аддикция, виртуальная аддикция) и зависимости от компьютерных игр («**геймерство**») являются:

навязчивое стремление постоянно проверять электронную почту;
предвкушение следующего сеанса онлайн;
увеличение времени, проводимого онлайн;
увеличение количества денег, расходуемых онлайн.

Если Вы считаете, что ваши дети, страдают от чрезмерной увлеченности компьютером, что наносит вред их здоровью, учебе, отношениям в обществе, приводит к сильным конфликтам в семье, то Вы можете обратиться к специалистам, занимающимся этой проблемой. Они помогут построить диалог и убедить зависимого признать существование проблемы и согласиться получить помощь. Например, на сайте «Дети онлайн» www.detionline.com открыта линия телефонного и онлайн-консультирования, которая оказывает психологическую и информационную поддержку детям и подросткам, столкнувшимся с различными проблемами в Интернете.

Контролируйте деятельность детей в Интернете с помощью современных программ. Они помогут отфильтровать вредное содержимое, выяснить, какие сайты посещает ребенок и с какой целью. Однако открытое, честное общение всегда предпочтительнее вторжения в личную жизнь. Поощряйте детей делиться с вами их опытом в Интернете. Посещайте Сеть вместе с детьми. Если ваш ребенок ведет интернет дневник, регулярно посещайте его. Будьте внимательны к вашим детям! Помните, что никакие технологические ухищрения не могут заменить простое родительское внимание к тому, чем занимаются дети за компьютером.

Советы по безопасности для детей разного возраста

Что могут делать дети в сети Интернет в возрасте 5-6 лет?

Для детей такого возраста характерен положительный взгляд на мир. Они гордятся своим умением читать и считать, а также любят делиться своими идеями. Несмотря на то, что дети в этом возрасте очень способны в использовании игр и работе с мышью, все же они сильно зависят от вас при поиске детских сайтов. Как им помочь делать это безопасно?

- В таком возрасте желательно работать в Интернет только в присутствии родителей;
- Обязательно объясните вашему ребенку, что общение в Интернет – это не реальная жизнь, а своего рода игра. При этом постарайтесь направить его усилия на познание мира;
- Добавьте детские сайты в раздел Избранное. Создайте там папку для сайтов, которые посещают ваши дети;
- Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю;
- Научите вашего ребенка никогда не выдавать в Интернет информацию о себе и своей семье;
- Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет.

Возраст от 7 до 8 лет

Как считают психологи, для детей этого возраста абсолютно естественно желание выяснить, что они могут себе позволить делать без разрешения родителей. В результате, находясь в Интернет ребенок будет пытаться посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей. Поэтому в данном возрасте особенно полезны будут те отчеты, которые вам предоставит Родительский контроль или то, что вы сможете увидеть во временных файлах Интернет (папки c:\Users\User\AppData\Local\Microsoft \Windows\Temporary Internet Files в операционной системе Windows).

В результате, у вашего ребенка не будет ощущения, что вы глядите ему через плечо на экран, однако, вы будете по-прежнему знать, какие сайты посещает ваш ребенок.

Стоит понимать, что дети в данном возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах. Дети этого возраста любят играть в сетевые игры и путешествовать по Интернет. Вполне возможно, что они используют электронную почту и могут заходить на сайты и чаты, не рекомендованные родителями.

По поводу использования электронной почты хотелось бы заметить, что в данном возрасте рекомендуется не разрешать иметь свой собственный электронный почтовый ящик, а пользоваться семейным, чтобы родители могли контролировать переписку. Помочь вам запретить ребенку использовать внешние бесплатные ящики сможет такое программное обеспечение, как Kaspersky Internet Security со встроенным родительским контролем.

Что можно посоветовать в плане безопасности в таком возрасте?

- Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения;
- Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером;
- Покажите ребенку, что вы наблюдаете за ним не потому что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь;
- Приучите детей, что они должны посещать только те сайты, которые вы разрешили, т.е. создайте им так называемый «белый» список Интернет с помощью средств Родительского контроля.
- Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей;
- Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю;
- Создайте семейный электронный ящик, чтобы не позволить детям иметь собственные адреса;
- Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего ПО;
- Приучите детей советоваться с вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей;
- Научите детей не загружать файлы, программы или музыку без вашего согласия;
- Используйте фильтры электронной почты для блокирования сообщений от конкретных людей или содержащих определенные слова или фразы.
- Не разрешайте детям использовать службы мгновенного обмена сообщениями;
- В «белый» список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией;
- Не забывайте беседовать с детьми об их друзьях в Интернет, как если бы речь шла о друзьях в реальной жизни;

- Не делайте «табу» из вопросов половой жизни, так как в Интернет дети могут легко наткнуться на порнографию или сайты «для взрослых»;

- Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

9-12 лет

В данном возрасте дети, как правило, уже наслышаны о том, какая информация существует в Интернет. Совершенно нормально, что они хотят это увидеть, прочесть, услышать. При этом нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств Родительского контроля.

Советы по безопасности в этом возрасте:

- Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения;

- Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером;

- Покажите ребенку, что вы наблюдаете за ним не потому что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь;

- Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей;

- Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю;

- Не забывайте беседовать с детьми об их друзьях в Интернет;

- Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернет;

- Позволяйте детям заходить только на сайты из «белого» списка, который создайте вместе с ними;

- Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернет;

- Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение;

- Создайте вашему ребенку ограниченную учетную запись для работы на компьютере;

- Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях;

- Расскажите детям о порнографии в Интернет;

- Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами;

- Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

13-17 лет

В данном возрасте родителям часто уже весьма сложно контролировать своих детей, так как об Интернет они уже знают значительно больше своих родителей. Тем не менее, особенно важно строго соблюдать правила Интернет-безопасности – соглашение между родителями и детьми. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернет. Следует обратить внимание на необходимость содержания родительских паролей (паролей администраторов) в строгом секрете и обратить внимание на строгость этих паролей.

Советы по безопасности в этом возрасте

В этом возрасте подростки активно используют поисковые машины, пользуются электронной почтой, службами мгновенного обмена сообщениями, скачивают музыку и фильмы. Мальчикам в этом возрасте больше по нраву сметать все ограничения, они жаждут грубого юмора, азартных игр, картинок «для взрослых». Девочки предпочитают общаться в чатах, при этом они гораздо боле чувствительны к сексуальным домогательствам в Интернет. Что посоветовать в этом возрасте?

- Создайте список домашних правил посещения Интернет при участии подростков и требуйте безусловного его выполнения. Укажите список запрещенных сайтов («черный список»), часы работы в Интернет, руководство по общению в Интернет (в том числе в чатах);

- Компьютер с подключением к Интернет должен находиться в общей комнате. Часы работы в Интернет могут быть легко настроены при помощи средств Родительского контроля

- Не забывайте беседовать с детьми об их друзьях в Интернет, о том, чем они заняты таким образом, будто речь идет о друзьях в реальной жизни. Спрашивайте о людях, с которыми дети общаются

посредством служб мгновенного обмена сообщениями чтобы убедиться, что эти люди им знакомы.

- Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

- Необходимо знать, какими чатами пользуются ваши дети. Поощряйте использование моделируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.

- Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из Интернет. • Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернет.

- Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.

- Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

- Расскажите детям о порнографии в Интернет.

- Помогите им защититься от спама. Научите подростков не выдавать в Интернет своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.

- Приучите себя знакомиться с сайтами, которые посещают подростки.

- Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.

- Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что по закону дети не могут играть в эти игры.

Как выявить вовлеченность ребенка в «группы смерти»

Сегодня большую опасность для детей и подростков представляют игры, организованные в сети Интернет создателями так называемых групп смерти. Большое распространение данные сообщества получили в социальных сетях «ВКонтакте», «Инстаграм». Суть игры заключается в том, что отобранный участник должен выполнить 50 заданий, преимущественно их необходимо осуществлять ранним утром (время, когда организм не вышел из состояния сна и, таким образом, на подсознательном уровне происходит более эффективное воздействие).

На протяжении отведенного на выполнение заданий времени ребенок подвергается запугиванию, что если он перестанет играть, то погибнут его близкие и родственники. Итогом всей игры является сведение счетов с жизнью самим ребенком.

Меры по противодействию данному явлению ведутся государственными структурами, общественными организациями и администрациями соцсетей, но все они будут малоэффективны без внимания и контроля тех, кто непосредственно находится рядом с каждым ребенком, - родителей.

Этапы вступления в игру:

Ребенок делает запрос о вступлении в группу, которую нашел самостоятельно, либо пишет послание с хештегами, и его находят администраторы.

Сначала администраторы внимательно изучают страницы, затем проводят опрос и дают задания в виде головоломок. Затем ребенку присваивается номер.

Далее задания обретают более жестокую форму. Детей заставляют резать вены, жечь кожу и протыкать ее иглой, и тому подобное. Необходимо прислать фото как доказательство. Испытания могут быть более опасного характера, например, перебежать дорогу на красный свет.

Последний этап квеста – самоубийство. Перед этим группу подростков добавляют в специальный чат, где обсуждаются варианты суицида. Чаще всего – это прыжок с большой высоты. Все задания дети получают с 4 до 5 утра, когда родители крепко спят. Таким образом, удается достичь полной секретности – родители могут и не догадываться о настроении ребенка.

Признаки того, что ребенок вступил в сообщества, призывающие к суициду

Хэштеги на стене и под фотографиями

Хэштег — слово или фраза, которым предшествует символ #. Пользователи могут объединять тематическую группу сообщений, картинок по теме. Для того, чтобы посмотреть эту группу, достаточно кликнуть мышкой по хэштегу.

Обратите внимание, есть ли на странице ребенка фотографии или записи со следующими хэштегами:

#ff33
#f57
#f58
#d28

#тихийдом
#морекитов
#домкитов
#китыплывутвверх
#млечныйпуть
#150звёзд
#хочувигру
#няпока
#рина
#разбудименяв4.20

«Рина - в честь девушки, которая в конце ноября 2015 года свои счеты с жизнью, известная в соцсетях под ником Ирина Камбалина (имя изменено на Рина).

«Тихий дом» — это якобы особое состояние сознания, попав в которое, человек не может выбраться назад.

Вы должны понимать, что группы развиваются, и хэштеги также могут меняться.

Участники квеста начинают рисовать китов и бабочек. Казалось бы, ничего странного, но за этим стоит настоящая подготовка к самоубийству. Эти животные выбраны не случайно – киты выбрасываются на берег, бабочки живут несколько дней.

На стене ребенок делает посты стихотворений о просьбе взять в игру, дать номер, фразы и цитаты о китах и бабочках.

Пример:
Хочу в игру
Дай мне номер
Дай инструкцию
Найди. Меня. Где я?

Болезненно, и взывая в унисон ветру,
Наши киты один за другим
Выбрасываются
На бритвенный берег.

- Ребенок меняет свою фамилию на ХОЛОД, ЗИМА, КИТ, ЛИС.
- Ребенок сидит «ВКонтакте» рано утром (3-5 часов утра).
- Закрывание лица руками либо одеждой на фотографиях, демонстрирование указательного пальца на таких снимках, загруженных - признак депрессивного состояния ребенка.

Если вы заметили вышеперечисленные признаки, то необходимо предпринимать меры и обратиться в специальные службы.

Что делать?

Наблюдать за ребенком.

НАБЛЮДАТЬ, а не следить и вмешиваться в личную жизнь! Просматривайте иногда страницу «ВКонтакте» на наличие соответствующих картинок, постов на стене и хэштегов.

Но ни в коем случае не нарушайте личное пространство ребенка!

Наблюдение должно быть не только в социальной сети и в реальной жизни. Проанализируйте свое отношение к ребенку, его взаимоотношения с одноклассниками и друзьями.

Существуют признаки того, что у ребенка суицидальные мысли (ознакомиться с ними можно литературе по психологии, интернете, организовать тематическое родительское собрание с приглашенными специалистами).

Не следует рассказывать ребенку о подобных сообществах и напрямую спрашивать состоит ли он в них. Иначе вы спровоцируете интерес у ребенка к этому явлению, что может повлечь за собой последствия

ПОМНИТЕ, что «смертельные квесты» только провоцируют детей на самоубийство, но причиной является депрессия! Киты, единороги, бабочки, крокодилы, тараканы – завтра будут другие символы, вы их не успеете и заметить.

Здесь вам помогут:

Всероссийский «Детский телефон доверия»: 8-800-200-122 (бесплатно, круглосуточно).

Центр суицидальной превенции: 8-3452-50-66-39 (бесплатно, круглосуточно).

Горячая линия Уполномоченного по правам ребенка: 8-3452-55-67-07.

Группа «ВКонтакте» Спасение детей от кибер преступлений https://vk.com/spasti_detei информация и киберпреступлениях.

Сайт «Лига безопасного интернета» http://www.ligainternet.ru

http://rkn.gov.ru – официальный сайт Роскомнадзора.

Литература

1. Роберт И.В., Мартиросян Л.П., Мухаметзянов И.Ш., Прозорова Ю.А., Яламов Г.Ю., Усенков Д.Ю., Бажилина А.В. Методические рекомендации по проведению в общеобразовательных организациях тематических уроков, посвященных дню интернета. – М., 2014 г.;
2. Методические рекомендации для педагогических работников общеобразовательных организаций по Интернет безопасности детей. - ФГАОУ ДПО «Академия повышения квалификации и профессиональной переподготовки работников образования»,М.,2014 г.;
3. Солдатова Г., Зотова Е., Лебешева М., Шляпников В. Интернет: возможности, компетенции, безопасность. Методическое пособие для работников системы общего образования. — М.: Google, 2013;
4. Болотина Т.В., Павлова С.А., Прутченков А.С. Методические рекомендации по организации и проведению в общеобразовательных организациях Российской Федерации Всероссийского урока безопасности школьников в сети Интернет.

Для заметок

Содержание

ОСНОВЫ БЕЗОПАСНОГО ИНТЕРНЕТА:
методические материалы

Материалы
социально ориентированного проекта
«Навигатор жизни»

Ставрополь - 2017