Министерство образования Оренбургской области
ГАПОУ «Педагогический колледж» г. Бугуруслана

Сборник методических разработок «Классные часы, посвященные безопасности в сети Интернет»

2019 г.

Сборник содержит разработки конспектов уроков (занятий) по теме «Информационная безопасность» в рамках дисциплины «Информатика», которые могут быть проведены в образовательных организациях для просвещения обучающихся (студентов) в вопросах информационной, сетевой и компьютерной безопасности. Данные конспекты были использованы учителями школ города и студентами выпускных групп колледжа при прохождении преддипломной практики в рамках Всероссийской акции «Сайты, которые выбирают дети».

Содержание

Предисловие

Уважаемые коллеги!

Ребенок, включенный в процесс познания, оказывается незащищенным от потоков информации. Давайте задумаемся, почему мы не оставим ребенка с незнакомым человеком? Правильно, мы не знаем его целей, а с неизвестной информацией в интернете, мультипликационным фильмом, книгой, авторов и целей которой мы не знаем, оставляем. Не комментируем, не обсуждаем, не возвращаемся к увиденному и прочитанному. Мы учим детей защищаться от плохого человека, вести себя в критической ситуации, возникающей в период стихийных бедствий. Не учим главному…

Информация, в мире которой ребенок находится с момента появления на свет, способна нести в себе информационные угрозы. Деформация и деструктивные изменения духовной сферы общества в форме искаженных нравственных норм и критериев, неадекватных социальных стереотипов и установок, ложных ориентаций и ценностей, влияют на состояние и процессы во всех основных сферах общественной жизни. Недостоверная, неэтичная, непристойная, деструктивная информация, исходящая от основных источников информации, а также от средств информационного воздействия, оказывает определенное влияние на получателя информации – ребенка. Когда мы радуемся, что ребенок, сидящий за компьютером, рядом с нами, мы не задумываемся над тем, что ребенок виртуально далеко от нас. Кто в этот момент управляет им? Кто манипулирует?

Культ жестокости, насилия, порнографии, пропагандируемый в СМИ, печатных изданиях неограниченной продажи, а также в компьютерных играх и др., ведет к неосознаваемому порой желанию подражать этому, способствует закреплению таких стереотипов поведения в их собственных привычках и образе жизни, снижает уровень пороговых ограничений и правовых запретов. Негативная информация несет вред здоровью (переутомление, психологическая зависимость, соматические заболевания, снижение работоспособности и др.), происходит переоценка нравственных норм, снижение интереса к искусству, чтению, перенос образцов поведения из виртуальной действительности в реальность и др.), ребенок испытывает трудности в обучении (отсутствие времени на чтение, выполнение домашнего задания, перегрузка излишней информацией, снижение успеваемости).

Мы, взрослые, отстаем от информационной грамотности детей, не подозревая, какой опасности они подвергаются. Многие не знают и не интересуются содержанием сайтов, которые посещает ребенок, в какие компьютерные игры играет, какую музыку слушает.

Насыщенность современной информационно-образовательной среды деструктивной, вредной для развития детей информацией приобретает катастрофические масштабы. Дети и подростки, в силу возраста не обладают способностью фильтровать качество информации. У них не сформированы критерии различия, они не видят опасностей и не осознают рисков, принимают всю информацию, не понимая, что она может быть противозаконной, неэтичной,

недостоверной, вредоносной. Информационное воздействие становится главным рычагом управления людьми. Современные информационно-коммуникативные технологии (ИКТ) меняют не только структуру отношений, но и образ жизни людей, мышление, механизмы функционирования семьи, общественных институтов, органов власти.

Педагоги способны быть проводниками детям в мир знаний, но в то же время не допустить, чтобы неустойчивая подростковая психика подвергалась информационному насилию, подготовить сознание детей к противодействию негативным информационным воздействиям, формировать информационную безопасность (навыки критического мышления), развивать способности к самоблокированию информации, учить отличать качественную информацию от некачественной.

Один из возможных путей разрешения проблемы информационной безопасности - обучение ребенка адекватному восприятию и оценке информации, ее критическому осмыслению на основе нравственных и культурных ценностей. Для полноценного развития ребенка не нужно создавать идеальную информационную среду, более важно и продуктивно заниматься развитием информационной безопасности личности ребенка.

В компетенции образовательной организации входит создание необходимых условий для охраны и укрепления здоровья обучающихся, на основа-нии которых мы выделили задачи педагогического характера для организации мероприятий по информационной безопасности:

1. формирование у обучающихся устойчивого убеждения в использовании информационных ресурсов;
2. формирования устойчивых поведенческих навыков в сфере информационной безопасности;
3. развитие у обучающихся способности распознать и противостоять негативной информации в Интернет-пространстве и СМИ, через обучение способам защиты от вредной информации.

Решение этих задач должно выполняться комплексно и систематически на каждом этапе работы в системе образовательной организации, с возможностью дополнения и варьирования по мере необходимости, исходя из результативности каждого этапа.

В методическом пособии представлены примерные материалы для проведения занятий по информационной безопасности. Они носят рекомен-дательный характер, с учетом действующего законодательства и научных тенденций по данной проблеме. Какие образовательные задачи Вы будете решать, проводя занятие с детьми и родителями, остается Вашим творческим и профессиональным выбором.

Просим серьезно ознакомиться с общими понятиями и содержанием проблемы информационной безопасности. Отнестись к понятию «информационная безопасность» как к научному феномену, сочетающему в себе педагогические, правовые, психологические аспекты.

Мы вместе! Ждем от Вас предложений, идей, материалов для обсуждения.

Конспект классного часа на тему «Урок медиабезопасности»

«Предупреждён – значит вооружён»

Цель: Способствовать формированию знаний о правилах безопасного пове-дения в современной информационной среде, в частности – сети Интернет.

Задачи:

1. Заставить задуматься о своем месте в этом мире.
2. Познакомить видами Интернет-угроз и противоправных посягательствах в сети Интернет.
3. Познакомить студентов с правилами медиабезопасности, с сайтами по-мощи в случае Интернет-угроз.
4. Сформировать чувство ответственности за свое пребывание в Интернет, за воспитание будущих поколений.
5. Продемонстрировать методику проведения подобных занятий для студентов.

Оборудование: анкеты для студентов, памятки для студентов, презентация, видеофрагменты («Безопасность в Интернете», «Развлечения и безопасность в Интернете», социальный ролик «Безопасный Интернет-детям!»), проектор, ПК.

Используемые понятия:

• **«Интернет-угроза»** - действие в сети Интернет, которое причиняет вред пользователю Интернета путем опубликования или пересылки не-коей информации, а также Интернет-коммуникация, направленная на причинение вреда собеседнику в Сети.

• **«Секта»** - религиозная организация.

• **«Вербовка»**, «Вербовать» - найти желающего на выполнение каких-либо работ.

• **«Киберунижение»** – распространение унижающей достоинство чело-века информации (изображение, видео, текста) в Интернете, а также использование Интернета для оскорблений и травли.

• **«Экстремистские группировки»** - организованные группы людей, занимающиеся преступной и опасной для людей деятельностью (напри-мер: убийство, нанесение тяжких телесных повреждений, массовые беспорядки, терроризм)

• **Терроризм** – массовое устрашение либо уничтожение людей.

Ход классного часа.

1. Организационный момент.

- Добрый день, ребята! Нашу встречу с вами я хочу начать со следующего стихотворения:

Ты есть, я есть, он есть,
А жизнь у каждого своя.
И ей цена – достоинство и честь,
Есть возраст переходных лет,
Какой бы сложной не была она.
Для многих начинается рассвет,
А кто-то погружается во тьму.
Ты есть, я есть, он есть,
Лишь вместе мы сумеем зло пресечь
И сохранить достоинство, чтоб жить.

2. Сообщение темы, цели, задач занятия.

- Сегодня наш классный час называется «Урок медиабезопасности». Как вы полагаете, о чем мы на этом уроке поговорим? *(ответы студентов)*

А кто может сказать, что такое медиабезопасноть? *(ответы студентов)*

Слово «медиабезопасность» сочетает в себе два термина – медиаграмотность и информационная безопасность.

В международном праве «***Медиаграмотность*** - грамотное использование детьми и их

преподавателями инструментов, обеспечивающих доступ к информации, развитие критического анализа содержания информации и привития коммуникативных навыков, содействие профессиональной подготовке детей и их педагогов в целях позитивного и ответственного использования ими информационных и коммуникационных технологий и услуг». В российском законодательстве «***Информационная безопасность детей*** – это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию». Такие понятия появились благодаря инициативе Уполномоченного при Президенте РФ по правам ребенка Павла Астахова, который сказал: «*Зачастую дети принимают все, что видят по телевизору и в Интернете, за чистую монету. В силу возраста, отсутствия жизненного опыта и знаний в области медаграмотности они не всегда умеют распознать манипулятивные техники, используемые при подаче рекламной и иной информации, не анализируют степень достоверности информации и подлинность ее источников. Мы же хотим, чтобы ребята стали полноценными гражданами своей страны – теми, кто может анализировать и критически относиться к информационной продукции. Они должны знать, какие опасности подстерегают их в сети и как их избежать*».

Я думаю, что каждый хочет жить в мире и безопасности, а это значит, что на душе будет радостно и спокойно. Мы не зря поднимаем сегодня этот вопрос. Как было бы здорово, если бы каждый человек соблюдал все правила приличия, был бы всегда доброжелателен. Но, к сожалению, так не бывает. И очень часто по чьей-то вине, нарушается мир другого человека.

С 1 сентября 2012 г. вступил в силу закон **«О защите детей от инфор-мации, причиняющий вред их здоровью и развитию»**. В связи с этим, каждый пользователь должен знать о правилах ответственного и безопасного поведения в современной информационной среде, способной нанести вред физическому и психическому здоровью человека.

Не многие знают, что более 80% вербовочного процесса детей, подростков и молодых людей проходит через Интернет! Сегодня мы рассмотрим наиболее распространённые виды Интернет-угроз, через которые злоумышленники воздействуют на человека, а так же узнаем о способах защиты от противоправных посягательств в сети Интернет и мобильной сотовой связи. Ведь не-даром поговорка гласит: **«Предупреждён – значит вооружён».**

3. Работа по теоретической части занятия.

Интернет – это не только пространство для поиска информации, ведения личной переписки, знакомства с новыми людьми и общения, это еще и источник опасности, которую можно предотвратить.

Для это нужно быть осведомленным о видах угроз, исходящих из Сети.

Какие угрозы встречаются наиболее часто? Прежде всего:

• Угроза заражения вредоносным ПО.

• Доступ к нежелательному содержимому. Это насилие, наркотики порнография, страницы подталкивающие молодежь к самоубийствам, анорексии (отказ от приема пищи), убийствам, страницы с националистической или откровенно фашистской идеологией и многое другое. Ведь все это доступно в Интернет без ограничений. Часто бывает так, что просмотр этих страниц даже не зависит от ребенка, ведь на многих сайтах отображаются всплывающие окна, содержащие любую информацию, чаще всего порнографического характера;

• Контакты с незнакомыми людьми с помощью чатов, электронной почты или социальных сетей. Все чаще и чаще злоумышленники используют эти каналы для того, чтобы заставить молодежь выдать личную информацию.

• Неконтролируемые покупки в Интернет-магазинах.

Подростки и молодые люди в возрасте 18-20 лет являются наиболее уязвимой группой и подвергаются наибольшей опасности. Они стремятся исследовать свою сексуальность, уйти из-под контроля родителей и завязать новые отношения вне семьи. Несмотря на то, что общение в Интернете может быть полностью анонимным, они больше подвержены опасности, даже если до конца не осознают возможные последствия.

Наиболее уязвимыми для злоумышленников являются следующие категории молодых людей:
• новички в Интернете, не знакомые с сетевым этикетом;
• недружелюбные пользователи;
• те, кто стремится попробовать все новое, связанное с острыми ощущениями;
• активно ищущие внимания и привязанности;
• бунтари;
• одинокие или брошенные;
• любопытные;
• испытывающие проблемы с сексуальной ориентацией;
• те, кого взрослые могут легко обмануть;
• те, кого привлекает субкультура, выходящая за рамки понимания их родителей.

Современный Интернет называют большой душеловкой? Как она работает? Мошенничество в Интернете существует столько же, сколько и сама Всемирная Сеть. На просторах Интернета оно подстерегает нас везде: в электронной почте, социальных сетях, на различных сайтах. Из года в год злоумышленники придумывают всё новые и новые уловки, направленные на то, чтобы обмануть своих потенциальных жертв. В отличие от таких интернет-угроз, как вирусы, троянские программы, программы-шпионы, СМС-блокеры, спам и др…, мошенничество примечательно тем, что мишень злумышленника – не компьютер, а человек у которого, как известно, свои сла-бости (н-р, страх, любопытство, легковерность…). Человек в наше время стал товаром. Рынок живого товара сейчас догоняет обороты наркотиков. По-этому, только сам пользователь может сделать свою жизнь в виртуальном пространстве безопасной.

По статистике, число детей и подростков – пользователей Интернета в России составляет около 14 млн. человек, из которых две трети выходят в Интернет ежедневно. Возраст начала самостоятельной работы в Сети для российских детей сейчас составляет 10 лет. Примерно 30% детей, пользующихся Интернетом, проводят в Сети ежедневно более трех часов в день.

Чтобы узнать, какова картина наших пользователей Интернета, проведем анонимное анкетирование. У каждого из вас есть анкета. Заполните ее. (заполняют и сдают). А теперь проанализируйте свои ответы: если вы получили больше ответов «ДА», то вам следует задуматься над тем, что вы подвергаетесь серьезной опасности не только стать жертвой угроз Интернета, но и иметь серьезную степень Интернет-зависимости.

- Как Вы думаете, какие угрозы в сети Интернет существуют для Вас? *(ответы студентов).* ***Верно. Рассмотрим некоторые из них.***

1. При общении в Сети у каждого обязательно появляются виртуальные знакомые и друзья. Такая форма общения очень часто привлекает преступников, т.к. различия кибербпреступлений от традиционных реальных преступных посягательств обусловлены особенностями интернет-среды: анонимностью, возможностью фальсификации, наличием огромной аудитории, возможностью достать жертву в любом месте и в любое время. Так очень легко завладеть вниманием собеседника, применяя приемы психологического воздействия, так называемый кибербуллинг - это нападения с целью нанесения психологического вреда, которые осуществляются через электронную почту, сервисы мгновенных сообщений, в чатах, социальных сетях, на web-сайтах, а также посредством мобильной связи. Такое многократно повторяемое агрессивное поведение имеет целью навредить человеку и базируется на дисбалансе власти (физической силы, социального статуса в группе). (*видеофрагмент «Безопасность в Интернете»*).

Наиболее опасными видами кибербуллинга являются **киберпреследование** - скрытое выслеживание жертвы с целью организации нападения, избиения, изнасилования и т.д., а также **хеппислепинг** — видеоролики с записями реальных сцен насилия.

Встречается в виртуальной среде и так называемый **буллицид** – доведение человека до самоубийства путем психологического насилия.

Для безопасности несовершеннолетнего особую угрозу представляют личные встречи с

виртуальными знакомыми в реальной жизни, о которых никто может ничего не знать.

2. Опасная для молодежи информация, способная причинить серьезный вред их здоровью, развитию и безопасности может содержаться ***на электронных ресурсах, содержащих материалы экстремистского и террористического характера.*** Не случайно сегодня очень часто возникает вопрос об участии молодых людей славянской, национальности никогда не бывавших в восточных странах, в незаконных террористических организациях и готовящих террористические акции на территории России. Одной из причин такой ситуации – это вовлечение этой части молодежи в незаконные действия путем Интернет-вербовки.

3. Особую опасность представляют для незрелой психики несовершеннолетних ***электронные ресурсы, созданные и поддерживаемые деструктивными религиозными сектами.***

Вот один из примеров: Оксана познакомилась в соц сетях с обаятельной девушкой. Разговорились, девушка пригласила Оксану прийти на вечеринку «Истинных сестер»: «У нас так здорово, мы так дружны и очень интересно проводим время». Оксана согласилась и через несколько дней попала в со-мнительную компанию, где надо было в обнаженном виде совершать странные обряды. Но члены секты под угрозой смерти запретили Оксане об этом кому-нибудь рассказывать. Оксана стала замкнутой и задумчивой, перестала хорошо учиться, с родителями почти не разговаривала. Ее постоянно мучил вопрос: как по¬кинуть секту?

4. Доверчивость и наивность детей нередко используют в своих целях компьютерные ***мошенники, спамеры, фишеры.*** Несовершеннолетнего пользователя взрослые преступники могут с использованием электронных ресурсов втянуть ***в совершение антиобщественных, противоправных, в том числе уголовно-наказуемых деяний.*** Известны случаи вовлечения подростков через Интернет:
• в действия, носящие оскорбительный и клеветнический характер;
• в экстремистскую деятельность;
• в преступную деятельность по изготовлению и сбыту наркотических средств и психотропных веществ и склонению к их потреблению несовершеннолетних, незаконному обороту оружия, взрывных устройств и взрывчатых веществ, сильнодействующих или ядовитых веществ в целях сбыта.

Вам следует знать, что указанные общественно опасные деяния, независимо от того, совершаются ли они с применением традиционных способов и средств или с использованием информационно-телекоммуникационных сетей, уголовно наказуемы, в том числе для подростков, достигших установленного законом возраста уголовной ответственности (16 лет, а за отдельные виды преступлений – с 14 лет).

5. ***Пропаганда наркотиков, насилия и жестокости, суицидального поведения, самоповреждений*** может быть весьма опасной для неокрепшей подростковой психики. Согласно Конвенции ООН о правах ребенка такие действия есть не что иное, как ***криминальная, в том числе коммерческая эксплуатация ребенка.***

6. ***Киберунижение и кибертравля.*** Они чаще встречаются в социальных сетях, на форумах и в чатах; для кибертравли используются также электронная почта и онлайн-мессенджеры (например, Аська, СМСки). Опасность распространения унижающей человека информации заключается в том, что в отличие от «обычного» унижения, сцены, изображающие сам процесс унижения, распространяются на неограниченный круг лиц. Таким образом, такие видео или фото могут быть доступны будущим друзьям и знакомым даже в случае переезда в другой город. Еще одна опасность заключается в том, что на данный момент удалить все экземпляры унижающих текстов или изображений из Интернета почти невозможно – ничто не мешает кому-то сохранить их на своем компьютере и опубликовать в Сети повторно даже через не-сколько лет.

Это не полный перечень тех опасностей, которые могут подстерегать вас в Интернете. Самое главное уметь применять элементарные правила без-опасности в Интернете. (*видеофрагмент «Развлечения и безопасность в Ин-тернете»*). Чтобы знать, как поступить, предлагаем вам свод правил поведе-ния в Интернете (*памятки для студентов*).

А что делать, если вы уже подверглись угрозе со стороны Интернет-мошенников или

стали членом Интернет-клубов сомнительного характера, или у вас проявляются признаки Интернет-зависимости? В этом случае есть возможность обратиться в службу «Горячей линии» Центра безопасного Ин-тернета в России. На «Горячую линию» можно попасть круглосуточно, набрав адрес www.saferunet.ru и нажав на красную кнопку «Горячая линия». Горячая линия принимает сообщения по следующим категориям противоправного контента:
- сексуальная эксплуатация несовершеннолетних;
- вовлечение детей в сексуальную деятельность (grooming);
- расизм, национализм, иные формы ксенофобии;
- киберунижение и кибертравля;
- сцены насилия над детьми;
- пропаганда и распространение наркотиков;
- пропаганда и публичное оправдание терроризма.

Отправка сообщения на «Горячую линию» производится анонимно и бесплатно. При этом могут быть не только текстовые формы обращения, но и пересылка ссылок на нежелательные ресурсы, которые могут быть оценены специалистами и закрыты.

Еще одним средством помощи детям и их родителям в области Интер-нет-угроз является линия помощи «Дети онлайн» – служба телефонного и онлайн консультирования для детей и взрослых по проблемам безопасного использования детьми и подростками Интернета и мобильной связи.

Обратиться на «Линию помощи» можно по телефону или через Интернет (все сведения у вас есть в правилах). На «Линии помощи» психологическую и информационную поддержку оказывают психологи факультета психологии МГУ имени М. В. Ломоносова и Фонда развития Интернет, прошедшие специальную подготовку по психологическому и информационному консультированию по проблемам безопасного использования детьми и под-ростками Интернета и мобильной связи.

В ряде случаев сотрудники «Линии помощи» перенаправляют посту-пивший запрос или рекомендует позвонившим самим обратиться в другие организации, с которыми сотрудничает служба «Дети онлайн». К ним относятся: специализированные телефоны доверия, горячие Линии (в частности, Горячая Линия по приему сообщений о детской порнографии Фонда «Дружественный Рунет»), службы психологической и социальной помощи, органы МВД (в частности, управление «К», которое занимается расследованиями в области киберпреступности).

В Оренбургской области работают также региональные службы помощи и детские телефоны доверия.

Владение правилами медиабезопасности являются важной составляющей каждого человека, так как вы все в будущем кто-то учитель, а кто-то родитель. На вас будет лежать ответственность за воспитание будущих поколений. Чтобы ваши дети росли в безопасности, научите их самым элементарным правилам пользования сетью, расскажите о возможных угрозах и будьте всегда рядом, если у него возникают какие-то проблемы. (*видеофрагмент «Социальный ролик «Безопасный Интернет – детям!»*).

В этом могут помочь специальные программы контентной фильтрации, т.е. программы, фильтрующие сайты и ресурсы Интернета на наличие нежелательной информации и ограничивающие возможность их просмотра. На рынке программных ресурсов на сегодняшний день существует множество программ выполняющих, так называемую функцию Родительского контроля. Наибольшей популярностью пользуются антивирусные программы, содержащие такую функцию. Они удобны тем, что позволяют защитить компьютер не только от вредоносных программ, но и ограничить время пребывания в сети и доступ ребенка к нежелательным сайтам. Это такие продукты как Антивирус Касперского Security или Crystal, Dr Web Security и другие. Есть и программы, созданные специально для ограничения контента.

6. Итог

Современный мир, который вас окружает, сложен и труден. Нужно быть очень умным, осторожным, сообразительным, чтобы жить в нем. Безопасность в этом мире зависит от

каждого из нас, прежде всего, от отношения к самому себе.

Природа создала всё для того, чтобы человек был счастлив. Деревья, яркое солнце, чистую воду, плодородную почву. И нас людей – сильных, красивых, здоровых, разумных. Человек рождается для счастья.

5. Рефлексия.

И в заключении я попрошу тех, кому этот урок стал интересным, полезным и кто считает, что Интернет должен стать для нас другом, хором сказать «***Я за безопасный Интернет!***». Всем спасибо.

Приложение 1.

Анкета для студентов

№ п/п	Вопрос	Да	Нет
1.	Часто ли вы замечаете, что находитесь в Интернете дольше запланированного времени?		
2.	Часто ли вы откладываете свои домашние дела из-за необходимости находиться в Интернете?		
3.	Используете ли вы смайлики в обычной, не электронной переписке?		
4.	Думаете ли вы, что без Интернета ваша жизнь стала бы скучна и неинтересна?		
5.	Находите ли вы себя усиленно думающим: «Чего бы еще поискать в Сети?»		
6.	Читая книгу, ищите ли вы полосу прокрутки с правой стороны, чтобы прокрутить текст?		
7.	Вы быстрее вспоминаете адрес своей странички в Интернете, чем номер мобильного телефона?		
8.	Часто ли вы говорите себе: «Еще несколько минут и выхожу», находясь в Интернете?		

Приложение 2.

Памятка для студентов

1. Основные правила безопасности в Интернете

Вы должны это знать:

* При регистрации на сайтах, старайтесь не указывать личную информацию, т.к. она может быть доступна незнакомым людям. Так же, не рекомендуется размещать свою фотографию, давая, тем самым, представление о том, как вы выглядите, посторонним людям.
* Используйте веб-камеру только при общении с друзьями. Проследите, чтобы по-сторонние люди не имели возможности видеть ваш разговор, т.к. он может быть записан.
* Если вы получили нежелательное письмо от незнакомых людей, не отвечайте на него. В случае, если Вы ответите на подобное письмо, отправитель будет знать, что вы пользуетесь своим электронным почтовым ящиком и будет продолжать посылать вам спам.
* Если вам пришло сообщение с незнакомого адреса, его лучше не открывать. Подобные письма могут содержать вирусы.
* Если вам приходят письма с неприятным и оскорбляющим вас содержанием, если кто-то ведет себя по отношению к вам неподобающим образом, сообщите об этом.
* Если вас кто-то расстроил или обидел, расскажите родителям. Родители самые близкие люди, они вас выслушают, помогут и защитят.
* Не желательно размещать персональную информацию в Интернете. Персональная информация — это номер вашего мобильного телефона, адрес электронной почты, домашний адрес и фотографии вас, вашей семьи или друзей.

* Не размещайте фото или видеоматериалы, содержащую изображение других лиц, без их согласия. Помните, если вы публикуете фото или видео в Интернете — каждый может посмотреть их.
* Не открывайте файлы, которые прислали неизвестные Вам людей. Вы не можете знать, что на самом деле содержат эти файлы – в них могут быть вирусы или фото/видео с «агрессивным» содержанием.
* Не добавляйте незнакомых людей в свой контакт лист в IM (ICQ, MSN messenger и т.д.)
* Помните, что виртуальные знакомые могут быть не теми, за кого себя выдают.
* Если рядом с вами нет родственников, не встречайтесь в реальной жизни с людьми, с которыми вы познакомились в Интернете. Если ваш виртуальный друг действительно тот, за кого он себя выдает, он нормально отнесется к вашей заботе о собственной без-опасности!
* Никогда не поздно рассказать взрослым, если вас кто-то обидел. Можно обратиться за помощью по адресам:
• «Горячая линия» Центра безопасного Интернета в России круглосуточно по адресу www.saferunet.ru, нажав на кнопку «Горячая линия»;

Линия помощи «Дети онлайн» – служба телефонного и онлайн консультирования для детей и взрослых по проблемам безопасного использования детьми и подростками Интернета и мобильной связи.

Обратиться на «Линию помощи» можно:
по телефону 8-800-250-00-15 (с 9 до 18 по рабочим дням, время московское).
по электронной почте helpline@detionline.com
на сайте www.detionline.com
• Единый детский Телефон Доверия - 8-800-200-01-22
• Региональная база службы «Детский телефон доверия» г. Оренбург - 64-63-07
• Горячая линия помощи детям и подросткам «Мы рядом!» г. Оренбург - 36-45-55
* Если вы встретили Интернет-ресурсы с агрессивным или незаконным содержанием, сообщите в полицию, к модератору ресурса или Роскомнадзор (заполнив специальную форму).

2. Памятка по безопасному поведению в Интернете

Для того чтобы обезопасить себя, свою семью, своих родителей от опасностей Интернета и причинения возможного ущерба, вы должен предпринимать следующие меры предосторожности при работе в Интернете:

•По возможности не сообщайте свои личные данные: имя, номер телефона, адрес проживания или учебы, любимые места отдыха или проведения досуга. Помните, что всё, что вы о себе сообщите в социальных сетях, чатах или форумах, может быть доступно, прочтено и использовано любым человеком в мире: Интернет прозрачен и глобален.

•Никогда не сообщайте в открытых источниках конфиденциальные данные: пароли или номера кредитных карт, пин-коды и другую финансовую информацию.

•При регистрации на интернетстраницах используйте нейтральное имя, а если потребуется выбрать пароль, используйте комбинацию из строчных и заглавных букв и цифр, по возможности сложную.

•Всегда сообщайте взрослым обо всех случаях в Интернете, которые вызвали у вас смущение или тревогу. И советуйтесь по сложным ситуациям, когда вы сталкиваетесь с чем-то необычным.

•Используйте защитные программы, антивирусы, фильтры электронной почты, программы для блокирования спама и нежелательных сообщений.

•Будьте сдержаны и, по возможности, вежливы в интернет-общении. Прекращайте любые контакты с теми, кто начинает задавать вам вопросы раздражающие, личного характера или содержащие сексуальные намеки. Обязательно расскажите об этом родителям.

Конспект урока по теме «Информационная безопасность»

Цель: формирование представления об информационной безопасности.
Задачи:
обучающие:
- познакомить с понятием информационной безопасности
- рассмотреть различные угрозы информационной безопасности
развивающие:
- совершенствовать коммуникативные навыки через умение излагать мысли, умение вести диалог
- определить план действий для предотвращения угрозы информаци-онной безопасности
воспитывающие:
- воспитывать ответственность за свои действия

План урока:
I. Организационный момент
II. Подготовка учащихся к усвоению нового материала
III. Теоретическая часть. Изучение нового материала
IV. Практическая часть. Первичное закрепление знаний
V. Домашнее задание
VI. Итог урока.

Оборудование и методические материалы: Мультимедийный проектор, ПК на РМУ, презентация, набор карточек, памятка для обучающихся.

Ход урока
I. Организационный момент
II. Подготовка к усвоению нового материала
- Тема урока «Информационная безопасность».
- Цель урока: Формирование представления об информационной без-опасности.

III. Теоретическая часть. Изучение нового материала
- Что такое «информационная безопасность»?

Дети высказывают свое мнение, как они понимают этот термин. Обобщая, учитель сообщает определение, которое записывается в тетрадь

Информационная безопасность - это защищенность информации от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации или ее владельцам.

- Какие воздействия могут нанести ущерб информации или владельцу, то есть что представляет угрозу информационной безопасности?

Дети делают свои предположения и определяются 7 направлений:
1. Кража личных данных, утечка информации
2. Вирусы, черви, трояны
3. Спам
4. Хакеры
5. Авторское право, нелицензионное ПО
6. Мошенничество
7. Дезинформация

- Задачи информационной безопасности сводятся к минимизации ущерба, а также к прогнозированию и предотвращению таких воздействий. Давайте разделимся на группы и установим, какие действия нужно предпри-нять, чтобы обезопасить себя от таких воздействий.

Работа группами по карточкам, обсуждение - 10 минут, затем представители от каждой группы сообщают всем свои методы защиты (принимая или оспаривая), учитель принимает участие в обсуждении - разрабатывается памятка

Кража личных данных, утечка информации

• старайтесь не «светить» номер кредитки в Сети;

• совершая онлайновую покупку, обращайте внимание на защищенность канала передачи данных;

• отслеживайте файлы cookies на жестком диске, регулярно прове-ряйте их принадлежность и удаляйте подозрительные.

Вирусы, черви, трояны

• приобретите хороший антивирусный пакет, установите его в ре-жиме максимальной безопасности, и своевременно обновляйте;

Спам

• не сообщайте посторонним ваш адрес электронной почты, осо-бенно тот, который предоставлен провайдером или особенно важен для вас;

• пользуйтесь почтовыми серверами с установленными фильтрами.

Хакеры

• никогда не храните пароли на винчестере (даже в зашифрованном виде), не ленитесь каждый раз набирать их вручную;

• отсоединяйтесь от Internet при подозрении на хакерскую атаку, запускайте антивирусную программу, изменяйте пароли;

• старайтесь меньше пользоваться общедоступными программами сомнительного происхождения;

• просматривайте чаще системный реестр на предмет подозритель-ных записей;

• обязательно делайте резервные копии данных на дискеты или CD R/RW;

Авторское право, нелицензионное ПО

• укрепление законодательной базы;

• пресекайте попытки воровства вашего творчества;

• используйте только лицензионное ПО.

Мошенничество (денежное надувательство).

• просто будьте более скептичными и менее доверчивыми.

Дезинформация.

• разумный скептицизм плюс ее проверка в других средствах массовой информации.

- Рассмотрим, как можно защитить информацию из своего файла от посторонних глаз, защитить файл от изменений.

Демонстрируется презентация.

Создание текстового файла, который требует пароль при открытии

1. Необходимо нажать в строке меню Сервис / Параметры
2. Появится окно Параметры, выбрать вкладку Безопасность
3. В поле Пароль для открытия файла ввести пароль, нажать Ок
4. Появится окно о подтверждении
5. Внимание!!! Не забудьте свой пароль!

Создание текстового файла, который не позволяет вносить изме-нения

1. Необходимо нажать в строке меню Сервис / Защитить документ
2. Появится справой стороны панель Защита документа
3. В поле Ограничение на редактирование поставить галочку и ука-зать вариант Только чтение
4. Нажать кнопку Да, включить защиту.

IV. Практическая часть. Первичное закрепление знаний

Создайте файлы:

• Работа 1, который требует пароль для открытия

• Работа 2, который не позволяет вносить изменения в файл

Обучающиеся создают и сохраняют файлы с необходимым условием

V. Домашнее задание

- Выучить записи в тетради. Ознакомить друзей с памяткой.

VI. Итог урока

Учитель подводит итог урока, выставляет оценки.

Приложение 1.

Набор карточек

1 группа Утечка или кража личных данных.

Суть: Ваша персональная информация может оказаться в чужих руках, что грозит печальными последствиями, вплоть до серьезного последствия.

Факты: Если у вас есть кредитная карта и банковский счет, то весьма собланительно выглядит перспектива оплаты услуг Internet-магазинов в режиме on-line. Действи-тельно, это ведь так удобно! Таким образом, в Европе за прошлый год счета «облегчились» на 533 млн $.

Защита:

2 группа Вирусы.

Суть: На ваш компьютер могут напасть вредоносные программы, уничтожающие данные или приводящие к неработоспособности всего компьютера.

Факты: Вирусов стоит бояться и в оффлайновой жизни, но на просторах Internet распространение вирусов может выливаться в настоящие эпидемии. Коварные создатели вредоносных программ используют почтовые сообщения. Приходится быть осторожными с программами, которые вы скачиваете из Internet.

Защита:

3 группа Спам.

Суть: Ваш почтовый ящик начинает переполняться несанкционированными рекламными сообщениями, делая практически невозможной нормальную обработку электронной почты.

Факты: Ленивые и неудачные торговцы, вместо того, чтобы заняться повышением уровня своих товаров и услуг, стремятся делать бизнес на некачественной рекламе.

Защита:

4 группа Хакеры.

Суть: В ваш компьютер могут проникнуть из Internet с целью кражи личной информации либо для использования вашего компьютера в качестве плацдарма для дальнейших атак.

Факты: Всего лишь пару лет можно было успокоить домашних пользователей, что хакерам нужен доступ только на крупные, мощные машины – теперь времена изменились. Даже информация о подключении к Internet-провайдеру (телефон+логин+пароль) – лакомая добыча для хакера.

Защита:

Приложение 2.

Памятка для обучающихся

БУДЬ БДИТЕЛЕН!

Утечка или кража личных данных.

• старайтесь не «светить» номер кредитки в Сети;

• совершая онлайновую покупку, обращайте внимание на защищенность ка-нала передачи данных;

• отслеживайте файлы cookies на жестком диске, регулярно проверяйте их принадлежность и удаляйте подозрительные.

Вирусы.

• приобретите хороший антивирусный пакет, установите его в режиме максимальной безопасности, и своевременно обновляйте;

Спам.

• не сообщайте посторонним ваш адрес электронной почты, особенно тот, ко-торый предоставлен провайдером или особенно важен для вас;

• пользуйтесь почтовыми серверами с установленными фильтрами.

Хакеры.

• никогда не храните пароли на винчестере (даже в зашифрованном виде), не ленитесь каждый раз набирать их вручную;
• отсоединяйтесь от Internet при подозрении на хакерскую атаку, запускайте антивирусную программу, изменяйте пароли;
• старайтесь меньше пользоваться общедоступными программами сомни-тельного происхождения;
• просматривайте чаще системный реестр на предмет подозрительных запи-сей;
• обязательно делайте резервные копии данных на дискеты или CD R/RW.

Нарушение авторского права.

• укрепление законодательной базы;
• пресекайте попытки воровства вашего творчества.

Вероятность дезинформации.

• разумный скептицизм плюс ее проверка в других средствах массовой ин-формации.

Денежное надувательство.

• просто будьте более скептичными и менее доверчивыми.

Конспект урока по теме «Безопасность в сети Интернет»

Цель урока: Познакомить с приемами безопасной работы в сети Интернет.

Задачи: Образовательные: Находить нужную информацию в сети Интенет, научить применять полученные знания в проектной деятельности.

Развивающие: Развивать умение анализировать и систематизировать имеющуюся информацию.

Воспитательные: развивать навыки работы в группе, формировать сознательность и внимание к информационно безопасности, прививать навыки безопасного использования сети Интернет.

Оборудование: компьютер с доступом в Интернет, видеопроектор, экран

План урока:

1. Организационный момент
2. Вступление в тему
3. Плюсы и минусы Интернета
4. Советы безопасности
5. Работа в группах
6. Подведение итогов

Ход урока:

1) Организационный момент.

2) Вступление в тему

Слово учителя: Развитие глобальной сети изменило наш привычный образ жизни, расширило границы наших знаний и опыта. Теперь появилась возможность доступа практически к любой информации, хранящейся на миллионах компьютерах во всём мире. Но с другой стороны, миллионы компьютеров получи доступ к вашему компьютеру. И не сомневайтесь, они воспользуются этой возможностью. И не когда-то, а прямо сейчас.

В повседневной жизни каждый из вас сталкивался с Интернетом. А давайте попробуем выяснить, что же такое Интернет? (*ученики дают определение*).

Интернет – всемирная глобальная компьютерная сеть для хранения и передачи информации. Просмотр видеоролика: «Знакомство с Интернетом»: http://www.youtube.com/watch?v=DOaxn1JB7vE

Что из этого вы уже знали? Что было новым для вас? (*ответы учащихся*) Для чего вы используете Интернет? (*ответы учащихся*)

Всегда ли безопасно использовать всемирную сеть?

3) Плюсы и минусы Интернета

Давайте немного подумаем, сейчас на доске у нас появятся высказывания, вы должны привести аргументы за или против .

Попробуйте привести аргументы, отражающие противоположную точ-ку зрения.

1. Интернет имеет неограниченные возможности дистанционного образования.
2. Интернет - это глобальный рекламный ресурс. И это хорошо!
3. Общение в Интернете - это плохо, потому что очень часто под-меняет реальное общение виртуальному.
4. Интернет является мощным антидепрессантом.
5. В Интернете можно узнать сведения о человеке (место проживания и адрес электронной почты, номер мобильного телефона). И это хорошо!

Какие опасности подстерегают нас в сети?

(*Интернет-зависимость, вредоносные и нежелательные программы, психологическое воздействие на человека, материалы нежелательного со-держания, Интернет-мошенники и др.) Давайте посмотрим, как нам уберечься от этих угроз*).

4) Советы безопасности

Перед тем как приступить к групповой работе (по 2 человека) давайте посмотрим с вами несколько видеороликов про безопасность в сети интернет, они вам помогут в дальнейшем в составлении памятки.

Учащимся предлагается к просмотру 3 видеоролика (по 2 мин.). Во время просмотра ребята должны подумать, какие советы они включили бы в свою памятку по безопасности в Интернете.

Просмотр видеоролика «Развлечения и безопасность в Интернете»: http://www.youtube.com/watch?v=3Ap1rKr0RCE

Просмотр видеоролика: «Остерегайся мошенничества в Интернете»: http://www.youtube.com/watch?v=AMCsvZXCd9w

Просмотр видеоролика «Как обнаружить ложь и остаться правди-вым в Интернете»: http://www.youtube.com/watch?v=5YhdS7rrxt8

Какие советы кажутся вам наиболее актуальными? Давайте составим вашу собственную памятку по безопасному общению в Интернете.

Работа в группе. Составление слайда «ПАМЯТКА БЕЗОПАСНОГО ПОЛЬЗОВАНИЯ ИНТЕРНЕТОМ».

5) Подведение итогов

Итогом урока станет памятка по безопасному поведению в сети интернет. В конце урока учащиеся высказывают свои мнения о значении Интернета и вопросов информационной безопасности.

Приложение 1.

ПАМЯТКА БЕЗОПАСНОГО ПОЛЬЗОВАНИЯ ИНТЕРНЕТОМ

1. Преступление против собственности

• Обращайте внимание на стоимость предлагаемой Вам услуги в интернете.
• Не отправляйте смс сервисам, которые вызывают у вас подозрение.
• Помните, бесплатный сыр - только в мышеловке.

2. Угрозы, направленные на наше эмоциональное и психическое состояние

•Ни под каким предлогом не соглашайтесь на разглашение личных данных: фамилий и имен, возраста, адресов электронной почты, номеров мобильных телефонов.
• Настороженно относитесь к сообщениям, содержащим призыв о помощи или предложения встречи.

3**. Угрозы, направленные на наше эмоциональное и психическое состояние**

• При работе с файлами будьте осторожны, убедитесь, что документ предназначался именно для Вас, проверьте, не является ли данный файл вирусом.
• Пользуйтесь антивирусным программным обеспечением, список рекомендованных программ можно найти на сайте «Управление К» и «Лиги безопасного интернета».

Конспект урока по теме «Безопасность в сети Интернет»

Цель: обратить внимание учащихся на возможные угрозы в сети Интернет, повысить грамотность учащихся в вопросах безопасности в сети, формиро-вать общепринятые нормы поведения в сети.

Задачи:

1. Знакомство учащихся с потенциальными угрозами, которые могут встретиться при работе в сети Интернет.
2. Выработка правила безопасного поведения в сети.
3. Выработка необходимости использования в сети общепринятых нравственных норм поведения.

Оборудование: компьютер, проектор, интерактивная доска, памятка учащимся;

Ожидаемые результаты:

- повышение уровня осведомленности учащихся о проблемах безопасности при использовании сети Интернет, потенциальных рисках при использовании Интернета, путях защиты от сетевых угроз.
- формирование культуры ответственного, этичного и безопасного использования Интернета.

План и этапы урока:

1. Введение
2. Объявление темы. Постановка задач
3. Просмотр социального ролика «Безопасный интернет – детям»
4. Сказка о золотых правилах безопасного поведения в Интернет
5. Физкультминутка
6. Рефлексия

Ход урока

1. Введение.

Создание проблемной ситуации

А сейчас я предлагаю вам отгадать загадки, чтобы понять, о чем пойдет речь на уроке.

Игра «Угадай-ка».

Что за чудо-агрегат
Может делать все подряд -
Петь, играть, читать, считать,
Самым лучшим другом стать? (*компьютер.*)

На столе он перед нами, на него направлен взор,
подчиняется программе, носит имя... (*монитор*).

Не зверушка, не летаешь, а по коврику скользишь
и курсором управляешь. Ты – компьютерная... (*мышь*).

Нет, она – не пианино, только клавиш в ней – не счесть! Алфавита там картина, знаки, цифры тоже есть.
Очень тонкая натура. Имя ей ... (*клавиатура*).

Сохраняет все секреты «ящик» справа, возле ног,
и слегка шумит при этом. Что за «зверь?». (*системный блок*).

Есть такая сеть на свете

Ею рыбу не поймать.
В неё входят даже дети,
Чтоб общаться, иль играть.
Информацию черпают,
И чего здесь только нет!
Как же сеть ту называют?
Ну, конечно ж... (*Интернет*)

2. Объявление темы. Постановка задач.

Как вы думаете, о чём мы сегодня будем говорить?

Правильно, мы с вами поговорим об интернете, точнее о безопасности в интернете. Мы живём в эпоху Интернета, без которого, увы, сейчас трудно справиться. Интернет заменил у нас многое. Это нам облегчило жизнь. Сейчас всего лишь при помощи одного небольшого устройства мы можем обмениваться мгновенными сообщениями, покупать книги или музыку, получать любую необходимую информацию и многое другое. Интернет ворвался в нашу жизнь.

У кого дома есть компьютер?

Как вы им пользуетесь?

А у кого дома есть Интернет?

А как вы думаете, какая опасность может подстерегать пользователей интернета? (*ответы детей*).

Мы можем найти в интернете любую информацию, но некоторые сайты могут быть заражены, и наш компьютер может «заболеть».

Поэтому постарайтесь запомнить основные правила безопасного интернета.

3. Просмотр социального ролика «Безопасный интернет – детям»

(Этот ролик создала Студия Mozga.ru, приняла участие в конкурсе «Безопасный интернет - детям!», проведённом Mail.ru.)

https://www.youtube.com/watch?v=789j0eDglZQ&feature=youtu.be

4. А сейчас послушайте сказку о золотых правилах безопасного по-ведения в Интернет

СКАЗКА

В некотором царстве, Интернет - государстве жил-был Смайл-царевич-королевич, который правил славным городом.

И была у него невеста – прекрасная Смайл-царевна-Королевна, день и ночь проводившая в виртуальных забавах.

Сколько раз предупреждал её царевич об опасностях, подстерегающих в сети, но не слушалась его невеста. Не покладая рук трудился Смайл-царевич, возводя город , заботился об охране своих границ и обучая жителей города основам безопасности жизнедеятельности в Интернет-государстве.

И не заметил он, как Интернет-паутина всё-таки затянула Смайл-царевну в свои коварные сети.

Погоревал – да делать нечего: надо спасать невесту.

Собрал он королевскую – дружину. Стали думать головы мудрые, как вызволить царевну из плена виртуального. И придумали они «Семь золотых правил безопасного поведения в Интернет», сложили их в котомку Смайл-царевичу, и отправился он невесту искать.

Вышел на поисковую строку, кликнул по ссылкам поганым, а они тут как тут: сообщества Змея-искусителя-Горыныча , стрелялки-убивалки Соло-вья-разбойника , товары заморские купцов шаповских, сети знакомств - зазывалок русалочьи… Как же найти-отыскать Смайл-царевну?

Крепко задумался Смайл-королевич, надел щит антивирусный, взял в руки меч-кладенец кодовый, сел на коня богатырского и ступил в трясину непролазную. Долго бродил он, и остановился на распутье игрища молодец-кого трёхуровневого, стал читать надпись на камне: на первый уровень по-падёшь – времени счёт потеряешь, до второго уровня добе-

рёшься – от родных-близких отвернёшься, а на третий пойдёшь - имя своё забудешь. И понял Смайл-царевич, что здесь надо искать невесту.

Взмахнул он своим мечом праведным и взломал код игрища страшного! Выскользнула из сетей разомкнувшихся Смайл-царевна, осенила себя паролем честным и бросилась в объятия своего суженого. Обнял он свою невесту горемычную и протянул котомочку волшебную со словами поучительными:«Вот тебе оберег от козней виртуальных, свято соблюдай наказы безопасные!»

1. Спрашивай взрослых

Если что-то непонятно, страшно или неприятно,
Быстро к взрослым поспеши,
Расскажи и покажи.

Всегда спрашивай родителей о незнакомых вещах в Интернете. Они расскажут, что безопасно делать, а что нет.

2. Установи фильтр

Как и всюду на планете,
Есть опасность в интернете.
Мы опасность исключаем,
Если фильтры подключаем.

Чтобы не сталкиваться с неприятной и огорчительной информацией в интернете, установи на свой браузер фильтр, или попроси сделать это взрослых — тогда можешь смело пользоваться интересными тебе страничками в интернете.

3. Не открывай файлы

Не хочу попасть в беду —
Антивирус заведу!
Всем, кто ходит в интернет,
Пригодится наш совет.

Не скачивай и не открывай неизвестные тебе или присланные незнакомцами файлы из Интернета. Чтобы избежать заражения компьютера вирусом, установи на него специальную программу — антивирус!

4. Не спеши отправлять SMS

Иногда тебе в сети,
Вдруг встречаются вруны.
Ты мошенникам не верь,
Информацию проверь!

Если хочешь скачать картинку или мелодию, но тебя просят отправить смс - не спеши! Сначала проверь этот номер в интернете – безопасно ли отправлять на него смс и не обманут ли тебя. Сделать это можно на специальном сайте.

5. Осторожно с незнакомцами

Злые люди в Интернете,
Расставляют свои сети.
С незнакомыми людьми
Ты на встречу не иди!

Не встречайся без родителей с людьми из Интернета вживую. В Интернете многие люди рассказывают о себе неправду.

6. Будь дружелюбен

С грубиянами в сети,
Разговор не заводи.
Ну и сам не оплошай –
Никого не обижай.

Общаясь в Интернете, будь дружелюбен с другими. Не пиши грубых слов! Ты можешь нечаянно обидеть человека, читать грубости так же неприятно, как и слышать.

7. Не рассказывай о себе

Чтобы вор к нам не пришёл,
И чужой нас не нашёл,
Телефон свой, адрес, фото,
В интернет не помещай,
И другим не сообщай.

Никогда не рассказывай о себе незнакомым людям: где ты живешь, учишься, свой номер телефона. Это должны знать только твои друзья и семья!

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

Тут и сказочке конец, а кто слушал - МОЛОДЕЦ!

Учитель: Какова мораль этой сказки?

А сейчас немного отдохнём и поиграем.

5. Физкультминутка

Игра «Вирусы»

Цель игры: Эмоциональная разрядка, снятие напряжения.

Вспомогательные материалы: Листы А4 двух цветов и лента, которой можно будет обозначить линию, разделяющую две команды.

Процедура проведения: Листы А4 нужно скомкать и сделать из них снежки двух разных цветов. Снежки одного цвета обозначают, например, вирусы, спам, зараженные файлы, снежки другого цвета – безопасная информация, безопасные файлы. Участники делятся на две команды так, чтобы расстояние между командами составляло примерно 3 м. В руках каждой команды снежки двух цветов, которые они, по команде ведущего, бросают другой команде. Задача: как можно быстрее закидать противоположную команду снежками, при этом успевая откидывать все «опасные» снежки и сохранять у себя все «безопасные». Ведущий засекает 10 секунд и, услышав команду «Стоп!», участники должны прекратить игру. Выигрывает та команда, на чьей стороне оказалось меньше «опасных» и больше «безопасных» снежков. Перебегать разделительную линию запрещено.

Учитель: Ребята, давайте попробуем почувствовать на себе вирусную атаку и постараться защититься от нее! Правила будут такие. Вам нужно разбиться на 2 команды. Но сначала из листочков бумаги черного и белого цвета сделаем снежки! Каждый должен сделать по 2 снежка белого и черного цвета. Черные снежки – «опасные», а белые – «безопасные». По моей команде начинаем бросать друг в друга снежки! Задача одной команды – как можно быстрее закидать противоположную команду снежками.

Также задача каждой команды – успеть откидывать все черные снежки и сохранять у себя белые.

Сейчас я вручу каждому памятку с правилами. Прочитайте правила и постарайтесь их выполнять (вручение памяток).

6. Рефлексия

Подведём итог нашего урока. Прочитайте предложение и продолжите.

Мне было интересно узнать…

Мне понравилось…

Меня удивило…

Мне захотелось…

Интернет может быть прекрасным и полезным средством для обучения, отдыха или общения с друзьями. Но – как и реальный мир – Сеть тоже может быть опасна!

Желаю, чтобы и в жизни, и на просторах Интернета у вас было всё просто отлично!

Памятки о правилах безопасного пользования интернетом остаются вам.

Приложение 1.

Памятка по безопасному поведению в Интернете

Это важно знать!

- Я не скажу о себе ничего (ни адреса, ни телефона, ни других сведений) без раз-решения родителей.
- Я никогда не передам по Интернет своей фотографии.
- Я никогда не встречусь ни с кем, кого знаю только по Интернет, без разрешения родителей. На встречу я пойду с отцом или с матерью.
- Я никогда не отвечу на сообщение, которое заставляет меня краснеть, будь то электронное письмо или общение в чате.
- Я буду разговаривать об Интернет с родителями.
- Я буду работать только тогда, когда они разрешат мне, и расскажу им обо всем, что я делал в Интернет.

Доклад на родительском собрании по теме «Профилактика интернет-угроз и угроз жизни подростков»

Целевая группа: родители (законные представители) студентов-подростков в возрасте 15-17 лет (I курса).

Цель: повышение эффективности профилактики подросткового суицида.

Задачи:

1. Повысить чувствительность родителей к проблемам подросткового возраста и их компетентность в области профилактики суицидального риска в семье.
2. Обсудить основные риски Интернета для детей и подростков.
3. Проинформировать родителей о возможностях получения различных видов профессиональной помощи (психологической, медицинской, юридиче-ской) в трудных ситуациях и ситуациях угроз жизни детей и подростков.

Текст выступления

Уважаемые родители!

Мы сегодня собрались с вами, чтобы обсудить очень непростую, тревожную проблему интернет-рисков и угроз жизни ваших детей - подростков. Поступающая сегодня информация о фактах ухода из жизни подростков, об угрозах жизни, о так называемых «группах смерти» у многих вызывает растерянность. Зачастую мы не знаем, как относиться к такой информации: то ли игнорировать эти угрозы, не обращать на них внимания, то ли бросаться спасать своих детей любой ценой? А ведь именно от реакции близких, от их умения вовремя распознать угрозу, от их искреннего желания и умения под-держать человека в ситуации угрозы жизни, зависит его благополучие, а не-редко и сама жизнь.

Чтобы предотвратить возможную беду, мы должны знать, почему подростки подвержены рискам и угрозам жизни, какие факторы провоцируют эти угрозы, и что могут и должны сделать родители для своих детей, чтобы не допустить рокового шага.

Подростковый возраст занимает промежуточное положение между детством и взрослостью. Происходят изменения на физиологическом и психологическом уровне, по-иному строятся взаимоотношения со взрослыми и сверстниками.

Подростковый возраст, прежде всего, сложен для самого человека, который неожиданно для себя вступил в этот период взросления. Появляется потребность в автономии, повышается критическая оценка наставлений взрослых, происходит некоторое ослабление контактов со взрослыми (прежде всего с родителями) — идет активный поиск своего «Я». Активная жизнь перемещается из дома во внешний мир.

Подросткам свойственно группироваться — входить в какую-либо значимую группу, быть принятым в нее, считаться своим. Большое значение они придают своему статусу в группе, среди сверстников. У них высока потребность в престиже, они стремятся следовать «моде»

как во внешнем облике, так и в занятиях, увлечениях.

Для подростков характерен интерес к проблеме смысла жизни, они осмысливают собственную роль и место в этой жизни.

Подростковый возраст является уязвимым с точки зрения переживания трудных ситуаций: мир в восприятии подростка предстает «черно-белым»: он не видит «полутонов» — подросток категоричен, а проблемы и трудности кажутся неразрешимыми. Кроме того, из-за гормональной перестройки организма снижена сопротивляемость стрессу.

Все эти и другие особенности закономерны и естественны в подростковом возрасте, однако при неблагоприятном стечении обстоятельств они могут явиться или быть специально использованы кем-то, что усиливает риски и угрозы жизни.

Что представляют собой риски и угрозы жизни подростка?

Рисками могут быть:

• жизненные обстоятельства или ситуации, воспринимаемые подрост-ком как невыносимо трудные, непреодолимые;

• пользование подростком интернет-ресурсами, через которые на него может оказываться опасное и зачастую разрушающее психику воздействие.

Что может стать неблагоприятными жизненными обстоятельствами?

• переживание обиды, одиночества, собственной ненужности, отчужденности и непонимания;

• действительная или мнимая утрата любви родителей, неразделенное чувство влюбленности, ревность;

• переживания, связанные со сложной обстановкой в семье, со смертью, разводом или уходом родителей из семьи;

• чувства вины, стыда, оскорбленного самолюбия, самообвинения (в т.ч. связанного с насилием в семье, т.к. зачастую подросток считает себя виноватым в происходящем и боится рассказать об этом);

• боязнь позора, насмешек или унижения;

• страх наказания (например, в ситуациях ранней беременности, серьезного проступка или правонарушения), страх последствий неуспешного вы-полнения какой-либо деятельности (например, неуспешной сдачи экзаменов);

• любовные неудачи, трудности в сексуальных отношениях, беременность;

• чувство мести, злобы, протеста, угроза или вымогательство;

• желание привлечь к себе внимание, вызвать сочувствие, избежать неприятных последствий, уйти от трудной ситуации, повлиять на другого человека;

• сочувствие или подражание товарищам, кумирам, героям книг или фильмов, следование «моде»;

• нереализованные потребности в самоутверждении, в принадлежности к значимой группе.

Эти обстоятельства могут отягощаться употреблением наркотиков, алкоголя, игровой или интернет-зависимостями, депрессивными со-стояниями.

Серьезная угроза жизни и благополучию подростка — опасные сайты в Интернете.

В Интернете были организованы и развернули свою деятельность деструктивные группы и сообщества, вовлекающие детей и подростков в «роковые» и смертельно опасные игры. Это, например, так называемые «группы смерти», которые готовят детей к добровольному уходу из жизни. Вот при-меры таких групп: «Синий кит», «Тихий дом», «Разбуди меня в 4:20» и т.д. Почти все суицидальные группы имеют в своем названии хештеги и аббревиатуры.

Хештег, изображаемый значком «решетка» #, позволяет другим пользователям находить все записи, обозначенные этим значком через поисковую систему социальной сети.

ВНИМАНИЕ! Озвучивать эти хештеги детям не следует, чтобы не вызвать у них интерес — «пойти по ссылкам и проверить, что там…»

Для вовлечения подростков в такие группы злоумышленники как раз и используют возрастные особенности подростков.

Система построена следующим образом: детей вовлекают в таинственную и опасную игру. Разработана система приема в группу, чтобы стать членом группы надо выполнять опасные задания, при этом, введен строгий за-прет на передачу информации взрослым. Прием в группу производится на основании получения как можно большего числа «лайков». У ребенка всячески поддерживается представление о том, что он никому не нужен в реальном мире, что здесь он только страдает, но есть дугой, счастливый мир, где он будет счастлив. Дети получают задания и должны их выполнить, записав выполнение на видео и выложив видео в сеть или отправив «куратору» группы. Ребенок «зарабатывает» себе статус, значимые связи и отношения.

В группе есть специальные люди, которые оценивают выполнение заданий и «поддерживают» веру ребенка в то, что он идет правильным путем, поощряя его деструктивное по сути поведение. Эксплуатируется стремление подростка принадлежать к значимой группе, создается эффект таинственности, членство в закрытой тайной группе подчеркивает «избранность» и значимость подростка. На определенном этапе игры, особенно, если подросток начинает бояться или понимать опасность участия в игре, «кураторы» начинают манипулировать семейными ценностями и интересами родных и близких подростка: ему внушается чувство вины, вплоть до угроз расправы над его близкими. Подросток боится стать причиной гибели дорогих ему людей и предпочитает уйти из жизни сам.

Как понять, что есть угроза?

Во-первых, важно не пропустить факторы риска — то, что может вызвать желание уйти из жизни.

Группу риска составляют подростки:

• находящиеся в сложной семейной ситуации (высокая занятость родителей, при которой общение с ребенком ограничено; болезненный развод родителей, предпочтение родителями одного ребенка по отношению к другому, жестокое обращение в семье, психически больные родственники);

• испытывающие серьезные проблемы в учебе;

• отличники, старающиеся все выполнить только на «отлично» и остро переживающие любые неудачи;

• не имеющие реальных друзей (при этом виртуальных (в интернете) может быть сколько угодно много);

• не имеющие устойчивых интересов, хобби;

• находящиеся в депрессивном состоянии или склонные к депрессиям;

• перенесшие тяжелую утрату;

• остро переживающие несчастную любовь (разрыв значимых любовных отношений);

• имеющие семейную историю суицида (или ставшие свидетелями суицида, либо сами пытавшиеся покончить с собой);

• употребляющие алкоголь, психоактивные вещества;

• имеющие недостатки физического развития, инвалидность, хронические соматические заболевания;

• совершившие серьезный проступок, уголовно наказуемый поступок (характеризующиеся криминальным поведением) или ставшие жертвой уголовного преступления (в т.ч. насилия);

• попавшие под влияние деструктивных групп (включая группы в соцсетях), религиозных сект или молодежных течений.

Признаки участия ребенка в «опасных» группах:

• резкое изменение фона настроения и поведения, преобладание по-давленного настроения;

• значительное время пребывания в Интернете (практически все свободное время), переживание тревоги, негативных эмоций при невозможности выхода в Интернет даже короткое время;

• общение в группе и просмотр видеосюжетов в ночное время, следствием чего являются трудности в пробуждении, ребенок выглядит не вы-спавшимся;

• сокрытие от взрослых своих страниц и действий в Интернете, нежелание ребенка обсуждать новости группы, свои действия в ней;

• ведение в сети одновременно нескольких страниц под разными именами, особенно от имени и девочки, и мальчика;

• выполнение различных заданий и их видеозапись, в том числе, связанных с агрессивными действиями по отношению к другим (к животным, к одноклассникам) или с самоповреждениями (например, порезы на руках или теле…);

• появление в речи и на страницах в сети рисунков, афоризмов, тегов, связанных с суицидальным поведением, например, «Раны на руках заглушают боль в душе», «Лети к солнцу», «Лифты несут людей в небеса» и др.

Признаки суицидальных намерений:

• высказывания о нежелании жить: «Было бы лучше умереть», «Не хочу больше жить», «Я больше не буду ни для кого проблемой», «Тебе больше не придется обо мне волноваться», «Хорошо бы заснуть и не проснуться», «Мне нельзя помочь», «Скоро все закончится», в т.ч. шутки, иронические замечания о желании умереть, о бессмысленности жизни;

• фиксация на теме смерти в рисунках, стихах, литературе, живописи, музыке; частые разговоры об этом, сбор информации о способах суицида (например, в Интернете);

• активная предварительная подготовка к выбранному способу совершения суицида (например, сбор таблеток, хранение отравляющих веществ, подъем на крышу дома, перила моста);

• сообщение друзьям о принятии решения о самоубийстве (прямое и косвенное); косвенные намеки на возможность суицидальных действий, например, помещение своей фотографии в черную рамку, употребление в переписке, разговорах суицидальных высказываний, символов;

• раздражительность, угрюмость, подавленное настроение, проявление признаков страха, беспомощности, безнадѐжности, отчаяния, чувство одиночества («меня никто не понимает, и я никому не нужен»), сложность контролирования эмоций, внезапная смена эмоций (то эйфория, то приступы отчаяния);

• негативные оценки своей личности, окружающего мира и будущего, потеря перспективы будущего;

• постоянно пониженное настроение, тоскливость. Ребенок считает, что у него ничего не получится, он ни на что не способен. Ребенок подавлен, безразличен, иногда ощущает вину перед окружающими;

• необычное, нехарактерное для данного ребенка поведение (более безрассудное, импульсивное, агрессивное; несвойственное стремление к уединению, снижение социальной активности у общительных детей, и наоборот, возбужденное поведение и повышенная общительность у малообщительных и молчаливых). Возможно злоупотребление алкоголем, психоактивными веществами;

• стремление к рискованным действиям, отрицание проблем;

• снижение успеваемости, пропуск занятий, невыполнение домашних заданий;

• символическое прощание с ближайшим окружением (раздача личных вещей, фото, подготовка и выставление ролика, посвященного друзьям и близким; дарение другим вещей, имеющих большую личную значимость; просит прощения у близких за все нанесенные ранее обиды);

• попытка уединиться: закрыться в комнате, убежать и скрыться от друзей (при наличии других настораживающих признаков).

Что делать, чтобы предотвратить беду?

1. Сохраняйте спокойствие

Если Вы получили информацию об угрозах жизни подростку, то, прежде всего, попытайтесь установить ее достоверность, обратитесь в образова-тельную организацию, где учится ребенок, в органы управления образованием или ближайшее отделение полиции.

При обнаружении сайтов в Интернете с опасным содержанием или узнав, что от кого-то исходит угроза жизни и благополучию ребенка, Вы можете обратиться в подразделение по

делам несовершеннолетних или оперативную часть полиции, или Роспотребнадзор.

Но не надо бежать и принимать срочных жестких мер по проверке пребывания детей в группах и сетях! Главное, что мы должны понимать, что да-же самые жесткие меры запретительного характера не гарантируют полную защиту детей и подростков от нежелательных воздействий.

2. Оцените степень своего участия в жизни ребенка

3. Установите, восстановите или укрепите доверительный контакт со своим ребенком

4. Поддерживайте доверительные отношения с ребенком, чтобы всегда быть в курсе проблем и трудностей ребенка, того, с кем общается ребенок реально и в сети, в какие группы входит.

5. Установите дома традицию ежедневного обсуждения проблем и трудностей, с которыми столкнулись члены семьи: делитесь с ребенком своими трудностями, показывайте, что все они разрешимы, говорите о способах разрешения проблем и людях, которые в этом помогают; спрашивайте о его проблемах и трудностях, вместе ищите способы их разрешения; говорите о том, что вместе вы всегда найдете выход из любой ситуации.

6. Контролируйте и регламентируйте пребывание ребенка в сети с помощью технических средств

Установите контроль интернет-трафика, лимит на услуги интернета на телефон, планшет или айпад, ограничение времени работы в интернете, на домашний компьютер установите специальные программные средства, которые помогут Вам защитить ребенка от нежелательной информации в Сети (они представлены на слайде).

Сообщите ребенку об установлении контроля и объясните свою позицию заботой о его безопасности и о безопасности всей семьи. Очень полез-но будет составить совместно с ребенком соглашение по использованию Интернета.

В нем должны быть прописаны права и обязанности каждого члена семьи.

7. Учите ребенка противостоять трудностям и справляться с ними

• Научите ребенка выражать свои эмоции в социально приемлемых формах (агрессию через активные виды спорта, физические нагрузки; ду-шевные переживания через доверительный разговор с близкими, приносящий облегчение);

• предложите ребенку завести тетрадь, в которой подросток будет рассказывать о своих переживаниях. Выложив эмоции на бумагу, он почувствует облегчение, освободившись от негативных мыслей.

8. Если Вы столкнулись с угрозой или заподозрили угрозу жизни Вашего ребенка, помните, что поддержка близких, их внимание, разговор по душам способны удержать от рокового шага

• Вызовите подростка на разговор,

• Задавайте вопросы,

• Подчеркивайте временный характер проблем, вселяйте надежду.

• Заверьте ребенка в своей поддержке

• Главное, чтобы разговор по душам не превратился в нравоучения.

9. Если Вы испытываете трудности, обратитесь за помощью к специалистам

Профессиональную помощь в ситуации угроз жизни могут оказать психологи и медицинские работники (врачи психиатры и психотерапевты).

Обращение не несет за собой никаких негативных последствий. В ситуации риска и угрозы жизни будет выявлена подлинная причина сильнейших негативных переживаний и оказана профессиональная помощь.

Информация о службах экстренной помощи в трудных ситуациях представлены на слайде.

Завершая разговор о интернет-рисках и угрозах жизни подростков подчеркнем, что главными средствами их профилактики являются ДОВЕРИЕ и КОНТРОЛЬ. Какими бы противоположными не казались нам эти понятия, в данной ситуации они сочетаемы. Тотальные

запреты не эффективны. Невозможно запретить проблемы, чувства и переживания ребенка, которые требуют выхода и разрешения.

В ситуациях интернет-рисков и угроз жизни, эффективно сочетание технического контроля с доверительным общением с ребенком, которое само по себе является способом контроля: только когда ребенок делится с родителями своими переживаниями, делами и трудностями, родители в курсе того, что с ним происходит, может осуществляться эффективный контроль, и может быть оказана необходимая поддержка в трудной для подростка жизненной ситуации.

В целом, важен комплексный подход к решению проблем, связанных с резкими перепадами настроения, различными зависимостями (включая компьютерную), девиантным поведением (в том числе, его клинических аспектов). Поэтому так важно быть чуткими к изменениям, которые происходят с ребенком.

Уважаемые родители! Обращайте внимание на эмоциональное состояние Вашего ребенка. Общайтесь, обсуждайте проблемы, учите их разрешать, внушайте оптимизм. Проявляйте бдительность. Если Вы не справляетесь сами, чувствуете неблагополучие в социальной, эмоциональной сфере Вашего ребенка, не стесняйтесь обращаться за помощью. Специалисты помогут Вам найти выход из трудной ситуации.

Приложение 1.

Памятка для родителей об информационной безопасности детей в возрасте от 13 до 17 лет

1. Создайте список домашних правил посещения Интернета при участии подростков и требуйте безусловного его выполнения. Обговорите с ребенком список запрещенных сайтов («черный список»), часы работы в Интернете, руководство по общению в Ин-тернете (в том числе в чатах).
2. Компьютер с подключением к сети Интернет должен находиться в общей комнате.
3. Не забывайте беседовать с детьми об их друзьях в Интернете, 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.
4. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
5. Необходимо знать, какими чатами пользуются Ваши дети. Поощряйте использование м дерируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.
6. Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из сети Интернет.
7. Приучите детей не выдавать свою личную информацию средствами электронной по-чты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.
8. Приучите детей не загружать программы без Вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
9. Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. 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.
10. Расскажите детям о порнографии в Интернете. Помогите им защититься от спама. Научите подростков не выдавать в Интернете своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.
11. Приучите себя знакомиться с сайтами, которые посещают подростки.
12. Научите детей уважать других в интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде — даже в виртуальном мире.
13. Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.

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

Если вы еще не знаете, как поговорить с ребенком об Интернете, обращайтесь на линию помощи «Дети Онлайн»

В целях проведения Единого урока по безопасности в сети Интернет просим обучающемуся пройти предварительную регистрацию на сайте www.Сетевичок.рф и родителю принять участие в опросе «Дети в Интернете глазами родителей» на сайте www.Родители.Сетевичок.рф .

Литература

1. Методические рекомендации: Методика организации недели «Безопас-ность Интернет»./ Авторы составители: Селиванова О. В., Иванова И. Ю., Примакова Е. А., Кривопалова И. В. - Тамбов, ИПКРО 2012.

2. Методические рекомендации по организации и проведению Единого урока для исполнительных органов государственной власти субъектов Российской Федерации, осуществляющих государственную политику в сфере общего образования, органов управления образованием муници-пальных образований и образовательных организаций в 2019 году. https://www.xn--d1abkefqip0a2f.xn--p1ai/index.php/proekty/urok

3. Методические рекомендации по основам информационной безопасно-сти для обучающихся общеобразовательных организаций с учётом ин-формационных, потребительских, технических и коммуникативных ас-пектов информационной безопасности направлены на организацию преподавания основ информационной безопасности в общеобразова-тельных организациях Российской Федерации. https://www.xn--d1abkefqip0a2f.xn--p1ai/index.php/proekty/urok

4. Безмалый В.Ф. Обеспечение безопасности детей при работе в Интернет. http://vladbez.spaces.live.com

5. Безмалый В.Ф. Современные угрозы в цифровом мире. http:/BEZMALY.WORDPRESS.COM

6. Сайт «Безопасность детей» Онлайн-Энциклопедия http://bezopasnost-detej.ru/

7. Сайт «Фонд развития Интернет» http://www.fid.su/

8. Журнал «Дети в информационном обществе» http://detionline.com