Департамент образования администрация г. Перми
Муниципальное бюджетное учреждение
«Центр психолого-педагогической, медицинской и социальной помощи» г. Перми

РАССМОТРЕНО

утверждено на заседании
НМС МБУ «ЦППМСП» г. Перми
Протокол № 4 от 29.12.2022г.

СОГЛАСОВАНО
_____О.В. Полторак,
начальник управления
воспитания и социализации
департамента образования
администрации города Перми

УТВЕРЖДАЮ
_____ О.А. Митина
и.о. директора МБУ
«ЦППМСП» г. Перми

ПРОГРАММА
киберурока «Урок медиабезопасности. «Предупреждён – значит вооружён»
(для учащихся 11 класса)

г. Пермь, 2022

73. КИБЕРУРОК
«Урок медиабезопасности
«Предупреждён – значит вооружён» (для 11 класса)

Цель: Способствовать формированию знаний о правилах безопасного поведения в совре- менной информационной среде, в частности – сети Интернет.

Задачи:

Заставить задуматься о своем месте в этом мире.

Познакомить видами Интернет-угроз и противоправных посягательствах в сети Интернет.

Познакомить студентов с правилами медиабезопасности, с сайтами помощи в случаеИнтернет-угроз.

Сформировать чувство ответственности за свое пребывание в Интернет, за воспитаниебудущих поколений.

Продемонстрировать методику проведения подобных занятий для учащихся

- **Оборудование:** анкеты, памятки, 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 некоей 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 человека 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 (например: убийство, нанесение тяжких телесных повреждений, массовые беспорядки, терроризм)
- **Терроризм** – массовое устрашение либо уничтожение людей.

Ход киберурока.

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 урок называется «Урок медиабезопасности». Как вы полагаете, очем мы на этом уроке поговорим? *(ответы)*

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

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 медаграмот- ности 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 каких избежать*».

Я думаю, что каждый хочет жить в мире и безопасности, а это значит, что на душе будетрадостно и спокойно. Мы не зря поднимаем сегодня этот вопрос. Как было бы здорово, еслибы каждый человек соблюдал все правила приличия, был бы всегда доброжелателен. Но, ксожалению, 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 информации, причиняющий вред их здоровью и развитию»**. В связи с этим, каждый пользователь должен знатьо 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 недаром 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), убий- ствам, страницы с националистической или откровенно фашистской идеологией и многое другое. Ведь все это доступно в Интернет без ограничений. Часто бывает так, что просмотрэтих 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 социальныхсетей. Все чаще и чаще злоумышленники используют эти каналы для того, чтобы заставитьмолодежь 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, чтообщение 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 молодыхлюдей:

- 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? Мошенниче-

ство 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 слабости (н-р, страх, любопытство, легковерность…). Человек в наше время стал товаром. Рынок

живого товара сейчас догоняет обороты наркотиков. Поэтому, 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).* ***Верно. Рассмотрим некоторые из них.***

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.

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 готовящихтеррористические акции на территории России. Одной из причин такой ситуации – это вовлечение этой части молодежи в незаконные действия

путем Интернет-вербовки.

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 сомнительную 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 покинуть секту?

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).

1. 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.***

2. 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 дажечерез несколько лет.

Это не полный перечень тех опасностей, которые могут подстерегать вас в Интернете. Самое главное уметь применять элементарные правила безопасности в Интернете. (*видеофрагмент «Развлечения и безопасность в Интернете»*). Чтобы знать, как поступить, предлагаем вам свод правил поведения 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 признакиИнтернет-зависимости? В этом случае есть возможность обратиться в службу «Горячей линии» Центра безопасного Интернета 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 этоммогут 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 Интернет-угроз являетсялиния помощи «Дети онлайн» – служба телефонного и онлайн консультирования для детейи взрослых по проблемам безопасного использования детьми и подростками Интернета и мобильной связи.

Обратиться на «Линию помощи» можно по телефону или через Интернет (все сведения увас 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 подросткамиИнтернета и мобильной связи.

В ряде случаев сотрудники «Линии помощи» перенаправляют поступивший 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 кибер-преступности).

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 сегодняшнийдень 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 учащихся:

№ п/п	Вопрос	Да	Нет
1.	Часто ли вы замечаете, что находитесь в Интернетедольше 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 быеще 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 Учащихся:
Основные правила безопасности в Интернете

Вы должны это знать:

* При регистрации на сайтах, старайтесь не указывать личную информацию, т.к. она можетбыть 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 посторонниелюди 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 безопасности!
* Никогда не поздно рассказать взрослым, если вас кто-то обидел.

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 ииспользовано 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-тонеобычным.

•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.