Сценарий беседы
«Безопасный интернет-детям»

Место проведения: ЦДОДиМ «АРТ», актовый зал
Адрес: ул. Острошицкая, 9
Участники: учащиеся Первомайского района
Автор - составитель: Бесан Анна Сергеевна (культорганизатор ЦДОДиМ «АРТ»)

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

Задачи:

- информирование учащихся о видах информации, способной причинить вред здоровью и развитию младших школьников, а также о негативных последствиях распространения такой информации;
- информирование учащихся о способах незаконного распространения такой информации в сетях Интернет и мобильной (сотовой) связи (в том числе путем рассылки SMS-сообщений незаконного содержания);
- обучение детей правилам ответственного и безопасного пользования услугами Интернет, в том числе способам защиты от опасных посягательств в сетях, в частности, от таких способов разрушительного воздействия на психику детей, как кибербуллинг (жестокое обращение с детьми в виртуальной среде);
- профилактика формирования у учащихся Интернет-зависимости и игровой зависимости (игромании, гэмблинга);

Ведущий: Кибербезопасность – это реализация мер по защите систем, сетей и программных приложений от цифровых атак. Сегодня мы не представляем свою жизнь без компьютера и сети Интернет. В настоящее время ведется множество неоднозначных разговоров о пользе и вреде всемирной сети. Дети и подростки - активные пользователи интернета, ведь он предоставляет подрастающему поколению невероятные возможности для совершения открытий, общения и творчества. Но у любого явления есть свои светлые и темные стороны, и зачастую дети и молодежь в полной мере не осознают все возможные проблемы, с которыми они могут столкнуться в сети.

Ведущий: Как должны родители и взрослые помочь детям избежать всевозможные неприятности, чтобы сделать их пребывание в интернете более безопасным, научить их ориентироваться во всемирной сети? Простого ответа не существует. Риски могут быть разными в зависимости от возраста и компьютерной грамотности ребенка.

Возможные риски, с которыми могут столкнуться дети в интернете:

Риск первый - это безопасность личной информации на собственном компьютере, что означает защиту от вирусов, вредоносного ПО и постоянное обновление программного обеспечения. Как защитить в этом случае своих детей? Прежде всего, повысить уровень защиты данных. Это можно сделать путем использования настроек фильтра и параметров фильтрации содержимого, которые доступны во многих программах. Кроме того, велика угроза заражения вредоносным ПО. Ведь для его распространения и проникновения в компьютеры используется целый спектр методов. Среди них можно отметить не только почту, компакт-диски, дискеты и прочие сменные носители информации или скачанные из Интернет файлы. Дети, неискушенные в вопросах социальной инженерии, могут легко попасться на уловки злоумышленника.

Риск второй - разглашение контактных данных. В Интернете (чатах, социальных сетях и т.п.) дети могут общаться с другими детьми и заводить новых друзей, что подразумевает обмен определенной личной информацией, по которой можно установить личность ребенка, контактную информацию (полное имя, почтовый адрес и номер телефона), подробности его быта, режима дня и т.д. Личность человека можно также установить, связав различные типы предоставленных данных (например, название школы, спортивного клуба, места проживания и т.д.). Подобная информация может быть использована в преступных целях.

Риск третий - это доступ к нежелательному содержимому. Это может быть насилие, наркотики, страницы, подталкивающие к самоубийствам, отказу от приема пищи, убийствам, страницы с националистической или откровенно фашистской идеологией и многое-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. Такая информация часто бывает заманчивой и может оказывать сильное психологическое давление на детей и подростков, которые не способны до конца осознать смысл происходящего и отказаться от просмотра и изучения сайтов с подобным содержимым. Влияние подобного рода информации на еще неокрепшую психику детей и подростков непредсказуемо; под впечатлением от таких сайтов дети могут пострадать не только в эмоциональном плане, но также прямой урон может быть нанесен и их физическому здоровью.

Риск четвертый - контакты с незнакомыми людьми. С подобными рисками можно столкнуться при общении в чатах, онлайн-мессенджерах (ICQ, Skype, MSN и др.), социальных сетях, на сайтах знакомств, форумах, блогах и т.д. Примерами таких коммуникационных рисков могут быть:

кибербуллинг, незаконные контакты (например, груминг), знакомства в сети и встречи с интернет-знакомыми и др.

Ведущий: Для детей и молодежи Интернет главным образом является социальной средой, в которой можно не только встречаться с друзьями, но и с незнакомцами. В Интернете пользователя могут обидеть, запугать или даже оскорбить. С появлением киберпространства набирает обороты такое явление, как кибербуллинг (bullying,от bully – драчун, задира, грубиян, насильник), обозначающее запугивание, унижение, травлю, физический или психологический террор, осуществляемый в виртуальной среде с помощью интернета и мобильного телефона и направленный на то, чтобы вызвать у другого страх и тем самым подчинить его себе. Запугивание в школе обычно заканчивается вместе с занятиями, но в Интернете обидчик может настигнуть свою жертву в любое время. Ведь запугивание или оскорбление в Интернете легко осуществимо с технической точки зрения: для отправки злонамеренного сообщения или публикации оскорбительного текста, доступного широкой аудитории, требуется несколько щелчков мышью. К тому же, в отличие от реального мира, виртуальность дает возможность анонимности и обеспечивает низкую вероятность наказания.

Ведущий: Особенно опасным риском является **груминг** – установление дружеских отношений с ребенком с целью личной встречи, вступления с ним в сексуальные отношения, шантажа и эксплуатации.

Риск пятый - неконтролируемые покупки. Несмотря на то, что покупки через Интернет пока еще являются экзотикой для большинства из нас, однако недалек тот час, когда эта угроза может стать весьма актуальной. Необходимо объяснить ребенку, что любые покупки, совершаемые в Интернете или по мобильному телефону, должны осуществляться взрослым, либо осуществляться с его разрешения. Всегда совместно принимайте решение о том, стоит ли воспользоваться теми или иными услугами, предлагаемыми в интернете.

Риск шестой - интернет-зависимость. Интернет-зависимость – навязчивое желание войти в интернет, находясь офлайн и неспособность выйти из интернета, будучи онлайн.

Ведущий: Практически каждый пятый ребенок в России безуспешно пытается уменьшить проводимое в интернете время, часами блуждает в интернете без особой цели и чувствует себя дискомфортно, когда не имеет к нему доступа. В 10% случаев дети пренебрегают семьей, друзьями или школой, не спят или не едят из-за интернета.

Ведущий: Подводя итог, можно прийти к общим рекомендациям, как обезопасить своего ребенка при пользовании Интернетом:

- Установите компьютер в общей для всей семьи комнате

  В этом случае разговор об Интернете и наблюдение за его использованием станет естественным в повседневной жизни. Обсуждение проблем может стать проще, если компьютер находится в общей комнате. Кроме того, Интернетом можно пользоваться вместе.

- Обсуждайте Интернет

  Проявляйте интерес к действиям ребенка и его друзей как в Интернете, так и в реальной жизни. Расскажите ребенку о прекрасных и увлекательных вещах, которые возможны в Интернете, а также о трудностях, с которыми можно столкнуться. Обсудите с ребенком действия, которые необходимо предпринять, если чувствуется неловкость в какой-либо ситуации в Интернете.

- Узнайте больше об использовании компьютера

  Если вы сами являетесь пользователем Интернета, вам будет проще определить правильную тактику для детей и помочь им найти в Интернете полезный материал. И тем не менее, постоянно повышайте собственный уровень компьютерной грамотности, чтобы знать, как обеспечить безопасность детей (например, посещение курсов, чтение специальной литературы, консультации с экспертами). И регулярно знакомьте всех членов вашей семьи с базовыми принципами безопасной работы на компьютере и в Интернете.

- Используйте Интернет вместе

  Найдите сайты, которые подходят для детей, или узнайте о способах поиска полезной информации: запланируйте совместную туристическую поездку, просмотрите образовательные сайты для помощи в школьных заданиях или найдите информацию об увлечениях детей. Просматривая веб-сайты в Интернете вместе, можно также помочь ребенку оценить значимость найденной информации. Можно добавить любимые сайты в папку «Избранное», чтобы совместно просмотренные ранее веб-сайты можно было открыть одним щелчком мыши.

- Договаривайтесь с ребенком о способе и времени использования Интернета

  Может оказаться полезным согласовать с ребенком время, которое он проводит за компьютером, а также список веб-сайтов, которые он может посещать. Это необходимо обсудить с детьми и прийти к определенному решению, которое всех устраивает.

- Установите доверительные отношения с ребенком

Это поможет избежать последствий столкновения ребенка с негативным опытом в Интернете. Положительный эмоциональный контакт ребенка с родителями поможет расположить его к трудному разговору о том, что произошло. Ребенок должен вам доверять и понимать, что вы тоже обеспокоены и хотите разобраться в ситуации и помочь ему, но ни в коем случае не наказать. (источник - https://posh1.hmaoschool.ru/site/pub?id=59)

Социальные сети

Ведущий: Для современных детей Интернет равно соцсети. Именно там они (да и многие взрослые) проводят больше всего времени и именно там возможно все — и взлом, и нежелательный контент. Скорее всего, вам известна печальная история игры «Синий кит» (а также «Тихий дом», «Разбуди меня в 4:20», «Море китов», «Млечный путь», и другие названия) — российская городская легенда, зародившаяся в начале 2016 года. Якобы существующая игра, финальной целью которой является совершение самоубийства. Она лишний раз напомнила родителям о необходимости защиты своих детей в интернет-пространстве.

Что делать?

Чтобы оградить ребенка от вредной информации, проследите, чтобы он:

Не вводил личные данные — адрес, номер телефона; номера банковских карт;

Меньше выкладывал личных фото и видео;

Не указывал геолокации и местоположение;

Не демонстрировал финансовое положение семьи;

Периодически менял пароль;

Не принимал заявки в друзья от незнакомых людей.

Вирусы

Ведущий: Компьютерный вирус может повредить и уничтожить важные данные на компьютере. Чаще всего распространяются через интернет. Даже опытный пользователь ПК не застрахован от случайного скачивания вирусного файла.

Что делать?

Ведущий: Использовать операционные системы с высоким уровнем защиты от вирусов; которые можно обновлять через официальный сайт;

Установить антивирусную программу известного производителя с автоматическим обновлением;

Ограничить доступ к компьютеру для посторонних лиц;

Не открывать файлы из непроверенных источников.

WI-FI

Ведущий: Сейчас практически в любом кафе, аэропорту и вокзале можно пользоваться благом цивилизации — бесплатным интернет-доступом. Однако общедоступные Wi-Fi точки не всегда безопасны.

Что делать?

Ведущий: Не использовать общедоступный Wi-Fi для передачи личных данных; Отключить функцию «Подключение к Wi-Fi автоматически».

Инициатива родителей

Ведущий: Мы любим постить фото детей, увы, не всегда это хорошо. Последний подобный случай, всколыхнувший соцсети, — фотосессия несовершеннолетних моделей в нижнем белье, которые опубликовала дизайнер из Одессы. Поэтому задумайтесь, стоит ли постить фото дочек в купальниках и т.д. Также не давайте разрешения постить фото ваших детей с различных мероприятий. Если вам фото не нравятся, вы можете потребовать от организаторов удалить фото. Помните, что ваши дети могут стать жертвами хейтеров (враг, недруг, склочник, ненавистник - тот, кто испытывает ненависть к какому-либо человеку).

Разглашение контактных данных

Ведущий: В интернете (чатах, социальных сетях, и т.п.) дети могут общаться с другими детьми и заводить новых друзей, что подразумевает, обмен определенной личной информацией по которой можно установить личность ребенка и контактную информацию (полное имя, почтовый адрес, номер телефона и др.)

Подобная информация может быть использована в преступных целях.

Что делать?

Ведущий: Обговорите с детьми возможные опасные последствия предоставления личной информации и те ситуации, когда рекомендуется скрывать личную информацию (с учетом возраста и психологической уравновешенности каждого ребенка);

Помните: никогда не следует сообщать пороли никому, даже давним друзьям. Кроме того, пароль необходимо регулярно менять. Научите этому своих детей;

Интернет является общественным местом. Перед публикацией любой информации или своих фотографий (а так же фотографий других людей) следует помнить, что любой человек в мире сможет получить доступ к этой информации;

Ребенок должен знать, что в любой момент может поговорить с родителями об отрицательном опыте полученном в Интернете, понимая, что получит поддержку и помощь от взрослых, а не порицание и наказание.

Памятка для пользователя интернета

Ведущий: Когда ты регистрируешься на сайтах, старайся не указывать персональную информацию в Интернете (это номер вашего мобильного телефона, адрес электронной почты, домашний адрес и фотографии вас, вашей семьи или друзей).

2. Используй веб - камеру только при общении с друзьями. Проследи, чтобы посторонние люди не имели возможности видеть ваш разговор, так как он может быть записан.

3. Ты должен знать, что если ты публикуешь фото или видео в Интернете - каждый может посмотреть их.

4. Нежелательные письма от незнакомых людей называются «Спам». Если ты получил такое письмо, не отвечай на него. Если ты ответишь на подобное письмо, отправитель будет знать, что ты пользуешься своим электронным почтовым ящиком, и будет продолжать посылать тебе спам.

5. Если тебе пришло сообщение с незнакомого адреса, его лучше не открывать. Вы не можете знать, что на самом деле содержат эти файлы. В них могут быть вирусы или фото/видео с «агрессивным» содержанием.

6. Не добавляй незнакомых людей в свой контакт.

7. Если тебе приходят письма с неприятным и оскорбляющим тебя содержанием, если кто-то ведет себя в твоем отношении неподобающим образом, сообщи об этом взрослым.

8. Если рядом с тобой нет взрослых, не встречайся в реальной жизни с людьми, с которыми ты познакомился в Интернете. Если твой виртуальный

друг действительно тот, за кого он себя выдает, он нормально отнесется к твоей заботе о собственной безопасности!

Интернет-это скопление одиночества. Мы вроде вместе, но каждый один. Иллюзия общения, иллюзия дружбы, иллюзия жизни.

Советы

1. Используйте реальный мир для расширения социальных контактов.

2. Определите свое место и цель в реальном мире. Ищите реальные пути быть тем, кем хочется.

3. Ищите друзей в реальности. Виртуальный мир дает только иллюзию принадлежности к группе и не развивает никаких действительных навыков общения.

4. Наполняйте жизнь положительными событиями, поступками.

5. Имейте собственные четкие взгляды, убеждения.

6. Избегайте лживости и анонимности в виртуальной реальности.

7. Научитесь контролировать собственное время и время за компьютером.

АНКЕТА

1.Часто ли Вы замечаете, что проводите онлайн больше времени, чем намеревались?

2.Часто ли Вы пренебрегаете домашними делами, чтобы провести больше времени в сети?

3.Часто ли Вы заводите новые знакомства с пользователями Интернет, находясь онлайн?

4.Часто ли Вы проверяете электронную почту, раньше чем сделать что-то другое, более необходимое?

5.Часто ли страдают Ваши успехи в учёбе, так как Вы слишком много времени проводите в сети?

6.Часто ли Вы занимаете оборонительную позицию и скрытничаете, когда Вас спрашивают, чем Вы занимаетесь в сети?

7.Часто ли Вы ощущаете, что жизнь без Интернета скучна, пуста и безрадостна?

8.Часто ли Вы ругаетесь, кричите или иным образом выражаете свою досаду, когда кто-то пытается отвлечь Вас от пребывания в сети?

9.Часто ли Вы пренебрегаете сном, засиживаясь в Интернете допоздна?

10.Часто ли Вы выбираете провести время в Интернете, вместо того, чтобы выбраться куда-либо с друзьями?

11.Часто ли Вы испытываете депрессию, подавленность или нервозность, если не имеете возможности выйти в сеть?

12. У Вас больше виртуальных друзей, чем реальных?

На каждый вопрос нужно ответить «да» или «нет», за каждый ответ «да» ставится один балл, за ответ «нет» - ноль баллов. Подсчитайте баллы и напишите крупно на своем листе их количество.

Посмотрите на полученный результат.

Если вы набрали от 0 до 4 баллов- вам пока ничего не угрожает, сеть один из способов времяпровождения.

От 5 – до 8 баллов – у вас практически сформировалась зависимость от виртуального общения, но еще не поздно остановиться.

Более 8 баллов - Виртуальное общение полностью заменило вам реальность .

Мы за компьютером сидим,
Уткнувшись в монитор.
Мы пленены буквально им,
И пишем всякий вздор.
Нет, чтобы встать из-за стола
Так всем нам просто лень;
Вот так нас сильно завлекла
Компьютерная сеть!
А мышцы шеи и спины
Дряхлеют и болят.
Они ведь так напряжены
Который год подряд!
Вот для ленивых и больных,
Желая им помочь,
Я написала этот стих,
Чтоб боль прогнать их прочь!
И если вам размяться лень,
А боль скрутила вас –
Его читайте каждый день
Не менее трёх раз!