***Родительское собрание***

***в 7-9 классах***

***на тему " Интернет - территория безопасности»***

Подготовила Селезнева А.В. – кл. руководитель 8 класса

**Форма проведения:** родительское собрание

**Целевая аудитория:** родители обучающихся.

**Цель:** повышение осведомленности и информированности родителей о безопасности детей в Интернете и о возможности использования его ресурсов.

**Задачи:**

* Показать родителям важность и значимость проблемы формирования у детей сетевого этикета.
* Рассказать родителям о правилах общения в Интернете.
* Ознакомить родителей с источниками информации по проблеме безопасности ребенка в Интернете.

**Вид собрания:** тематическое

**Форма собрания:** беседа

**Оборудование:** ноутбук, проектор, экран, мультимедийная презентация «Безопасность детей в сети Интернет», памятка для родителей «Как защититься от интернет-угроз, бланки для подведения итогов**,** тест *«Существует ли реальная опасность для ребенка стать интернет-зависимым или он просто активный пользователь».*

***Подготовительные мероприятия:***

- анкетирование учащихся по теме собрания;

- подготовка буклета для родителей по теме собрания.

***Ход родительского собрания***

1. **Организационный момент.**
2. **Мотивация к деятельности. Тренинг.**

Добрый день, уважаемые родители! Я очень рада встрече с Вами.

* ***Работа в группах.***

Вспомните свое детство. Какие главные развлечения у вас всплывают в памяти? Какими играми Вы были увлечены? Как организовывали свободное время? Сформулируйте и запишите на листах бумаги.

На основании только что проделанной работы составьте от группы общий список «Досуг моего детства».

* ***Слово родителям***

Прошу представителей групп озвучить списки игр.

*(родители зачитывают названия игр и занятий для проведения досуга с комментариями)*

Судя по ответам, игры Вашего детства были немного иными, чем игры ваших детей. «Салки», «Казаки-разбойники», «Прятки», «Глухой телефон» и т.д., чтение интересных книг о великих открытиях, исторических романов также позволяло с пользой провести свободное время.

Современные дети совсем по-другому смотрят на организацию досуга. Сегодня главное развлечение для ребенка – компьютер. Мы с вами живем в непростой, но очень увлекательный век, век всеобщей информатизации компьютерных технологий, цифровых инноваций и господства всезнающей, все умеющей, все дозволяющей Сети.

Интернет вошел в каждый дом.

Мы, наши дети, активно пользуемся всеми возможностями Интернета: участвуем в социальных сетях, смотрим фильмы, клипы, слушаем музыку, играем, пишем в блоги; сеть предлагает все больше и больше возможностей.

Среда Интернета может оказаться небезопасной для ребенка: контакты с незнакомыми людьми с помощью чатов или электронной почты, доступ к нежелательному содержимому, угроза вовлечения в экстремистские сообщества, заражения вредоносным ПО, другие опасности.

Родители должны быть информированы не только о возможной опасности для ребенка, но и способах обеспечения его безопасности в сети Интернет

* ***Работа в группах.***

Обсудите в группах и зафиксируйте на листах бумаги плюсы и минусы пользования компьютером и Сетью Интернет.

* ***Слово родителям***

Прошу представителей групп озвучить плюсы и минусы пользования компьютером и Сетью Интернет.

*(выступление родителей)*

Как видите, плюсов оказалось достаточно много, но и минусы родители не пропустили без внимания.

**Вывод:** Интернет является прекрасным источником для новых знаний, помогает в учебе, занимает досуг. Но, в то же время, Сеть таит в себе много опасностей.

***Вопросы.***

Чем является компьютер в вашей семье? Приведите примеры ситуаций из вашей жизни, связанных с положительными и отрицательными эмоциями по поводу использования компьютера.

Какую пользу извлекает Ваш ребенок при использовании сети Интернет?

Какие опасности ждут Вашего ребенка в сети Интернет?( подчеркнуть опасность вовлечения в экстремистские группировки)

**III. Анализ, обсуждение ситуаций и разработка рекомендаций.**

Интернет предоставляет детям и молодежи невероятные возможности для совершения открытий, общения и творчества. Прекрасное место для обучения, для общения с друзьями, для отдыха, для заведения новых знакомств.

Через Интернет дети и подростки открывают для себя мир, формируют собственную личность. Но, как и реальный мир, Сеть не безопасна, в виртуальном мире мы можем встретить все те же проблемы, что и в реальном.

И главная задача взрослых – обеспечение безопасности работы ребенка с мировой паутиной. Следует понимать, что, подключаясь к Интернету, ребенок встречается с целым рядом угроз, о которых он может даже и не подозревать. Проблема защиты детей в Сети находит самый широкий резонанс, и это не случайно.

Многие дети выходят в Интернет без контроля со стороны родителей, они самостоятельно постигают премудрости сети. Обратимся к статистике:

- около 50% детей выходят в Сеть без контроля взрослых.

- 19% детей иногда посещают порносайты, еще 9% делают это регулярно.

- 38% детей, просматривают страницы о насилии

- 16% детей просматривают страницы с расистским содержимым
- 25% пятилетних детей активно используют Интернет.

-14,5% детей назначали встречи с незнакомцами через Интернет, 10% из них ходили на встречи в одиночку, а 7% никому не сообщили, что с кем–то встречаются.

Но существует несколько способов оградить ребёнка от просмотра сайтов с нежелательным содержанием. Самым надёжным считают родительский контроль или используют программные ограничения просмотра нежелательных ресурсов – специальные настройки антивирусных модулей, фаерволов, специализированные программы для настройки «детского» и «взрослого» доступа в сеть. И можно создать специальную «детскую» учётную запись компьютера, применяя функции родительского контроля операционной системы, либо настраивая все подключения к сети соответствующим образом. Этот вариант отличается большей надёжностью и сложностью «обойти» детским пытливым умом сделанные родителями подключения, а также невозможностью доступа к родительским файлам и кэшу браузера, оставшемуся в памяти компьютера после пользования сетью старшими пользователями.

В основном дети не считают, что Интернет представляет угрозу. За компьютером с выходом в сеть Интернет проводят от 1 до 3 часов. Многие имеют личные странички на сайте «В контакте», ведут переписку с друзьями, знакомыми, играют в сетевые игры.

**IV. Основные угрозы для детей в сети Интернет**

**1. Системы мгновенного обмена сообщениями**

Системы обмена мгновенными сообщениями (например, MSN Messenger, Yahoo! Messsenger, Google Talk, ICQ…) стали широко используемым каналом общения для молодых людей. Это не могло остаться незамеченным со стороны кибер-преступников, которые быстро сделали его основным каналом для своей деятельности.

**Одна из самых опасных угроз** заключается в том, что преступники, используя данные программы, обманывают детей и подростков и представляются им другим человеком, чем они есть на самом деле.

В этих программах пользователи авторизуются с использованием адреса электронной почты и пароля. Например, если кто-то узнает данные другого пользователя и подключится к программе от его лица, то остальные люди, с которыми этот пользователь общается, будут думать, что они общаются именно с данным пользователем, хотя это не так. Если Вы обмениваетесь информацией или файлами с этим псевдо-пользователем, то преступник сможет легко ими завладеть. Именно по этой причине очень важно не распространять любую конфиденциальную информацию (персональные данные, фактический адрес проживания, банковские реквизиты и пр.) через подобные небезопасные каналы связи, как системы обмена мгновенными сообщениями.

Другая опасность состоит еще в том, что к подобным преступлениям часто прибегают педофилы. Их задача – собрать сведения о детях и подростках, а затем договориться с ними о реальной встрече или заставить их пойти на встречу. Педофилы зачастую представляются другими молодыми людьми, профессиональными фотографами или т.п.

Образование – это самый лучший способ защитить детей от подобного рода угроз. Посоветуйте им не общаться с незнакомцами, причем не только в онлайне, но и в обычном мире. Дети должны обладать достаточной уверенностью, чтобы быть способными открыто обсуждать с родителями или учителями свои проблемы.

Другой **потенциальный риск** в обмене мгновенными сообщениями – это инфицирование вирусами и вредоносными кодами. Почти 60% червей (вредоносные коды, которые распространяют сами себя), обнаруженных антивирусной лабораторией PandaLabs на протяжении первого полугодия, были созданы для распространения через системы обмена мгновенными сообщениями. Некоторые из них созданы для кражи паролей к онлайн-банкам. В этом случае в большей степени рискуют сами родители, потому что будут украдены их банковские данные, и, следовательно, могут пропасть их деньги.

Существуют простые способы, которые могут быть полезны для предотвращения случаев проникновения вредоносных кодов на компьютеры через системы обмена мгновенными сообщениями: не открывайте файлы и не нажимайте на ссылки, которые Вы получили через эти системы. По крайней мере, не делайте этого, пока точно не убедитесь, что человек, который их Вам прислал, является именно тем, кем он себя называет.

**2. Электронная почта**

**Электронная почта** – это другой источник опасности для молодых ребят. В этом случае также существует несколько угроз:

* Во-первых, это спам. Очень часто данный тип нежелательной почты используется для рекламы различных предложений: от казино до лекарств. Дети более подвержены доверять сообщениям, которые представлены в данных письмах, со всеми вытекающими отсюда последствиями. Они могут получить доступ к онлайн-казино и проиграть большую сумму денег, или они могут купить лекарства или даже наркотики с большим риском для своего здоровья.
* Далее, существуют ложные предложения работы. Это не представляет серьезную опасность для детей, но может являться таковой для подростков. Обычно эти сообщения содержат фантастические условия работы. Они обещают большие зарплаты без каких-либо усилий. Все, что в таких случаях необходимо, - это номер банковского счета, куда будут перечисляться деньги, а затем, в обмен на комиссию, получателя попросят перевести эти средства на другой банковский счет. Это выглядит слишком хорошо, чтобы быть правдой, и любой здравомыслящий взрослый человек насторожиться от такого предложения. Однако молодые люди ищут легких денег. В результате этого они непроизвольно становятся соучастником преступления, т.к. целью подобных финансовых переводов является «отмывание» преступных денег.
* Другой риск связан с вирусами и вредоносными программами, которые могут попасть на компьютер. Как правило, они распространяются через сообщения в электронной почте, которые имеют определенную тематику (реклама новых фильмов, эротические фотографии, скачивание игр и т.д.) и предлагают пользователям нажать на ссылку или скачать файл, являющиеся причиной инфекции. Данная техника известна как «социальная инженерия». Многие взрослые люди становятся жертвами данной техники, что уж говорить про детей, которые очень легко могут стать жертвами.

Лучший способ защитить детей и подростков от этих угроз – это **научить их быть бдительными по отношению к письмам из неизвестных источников**. Они должны знать, что большинство из написанного в этих письмах является ложью, и что они никогда не

должны открывать файлы или нажимать на ссылки в письмах подобного рода.

**3. Программы обмена файлами**

Обмен файлами в сетях является еще одним из основных источников распространения инфекций. Большинство вредоносных кодов (преимущественно, черви) копируются в папки с этими программами под заманчивыми именами (названия фильмов, программ и т.д.) для того, чтобы привлечь внимание других пользователей, которые захотят скачать эти файлы и запустить их на своих компьютерах.

По сути дела, это еще один вариант социальной инженерии: названия файлов могут быть умышленно созданы таким образом, чтобы привлечь именно детей и подростков, которые по незнанию скачают вредоносные программы на свои компьютеры.

Именно по этой причине детям следует знать, какие файлы они могут скачивать, а какие скачивать нельзя. Более того, очень хорошая идея – это **проверять каждый скаченный файл с помощью решения безопасности** до момента их первого открытия / запуска.

Если при запуске файла возникает ошибка или открывается диалоговое окно с вопросом о лицензии или предложением скачать дополнительный кодек, то подобные действия должны сразу же Вас заставить быть бдительным, потому что, скорее всего, данный файл содержит в себе вирусы или другое вредоносное программное обеспечение.

**4. Социальные сети и блоги**

Сайты социальных сетей (например, Facebook, MySpace, одноклассники, Вконтакте) широко используются для распространения фотографий и видео, общения с людьми и пр., так же как и блоги. В обоих случаях необходимо создавать персональный профиль для того, чтобы получить к ним доступ. Эти профили, зачастую, содержат такую конфиденциальную информацию как имя, возраст и т.д.

Детям следует постоянно напоминать, что необязательно предоставлять эту информацию, а достаточно только указать адрес электронной почты и имя, которое может быть псевдонимом. Нельзя распространять такую информацию, как возраст, адрес проживания, а также свои фотографии и видео.

Многие подростки используют блоги в качестве своих персональных дневников. Как правило, такие онлайн-журналы содержат значительно более широкую информацию, чем следовало бы публиковать. Крайне важно предотвратить публикацию любых данных, которые могли бы идентифицировать пользователя как ребенка или подростка, а также содержать информацию о месте проживания, учебы и другую персональную конфиденциальную информацию.

Аналогично, в некоторых социальных сетях, например в MySpace, есть возможность обмениваться файлами с другими пользователями. Необходимо отдельно обратить внимание ребенка на то, какими файлами он может обмениваться с другими пользователями и кому он может разрешить просматривать эту информацию. Совсем не сложно, например, разместить свои фотографии, но защитить их паролем, который будет доступен только своим друзьям и семье.

Родителям следует знать об этих новых сервисах, а также о том, как они работают и какие риски они представляют для пользователей. Родители также должны быть способны проинструктировать своих детей о том, как использовать эти сервисы правильно и безопасно.

**5. Мобильные телефоны с выходом в Интернет**

Стремительное распространение сотовых телефонов во всем мире сделало их одним из основных направлений для проведения кибер-атак за последние несколько лет. Исследование показало, что такие технологии как Bluetooth (позволяет обмениваться файлами между устройствами по беспроводному каналу) и высокоскоростной доступ в Интернет сделали сотовые телефоны очень уязвимыми для атак.

В настоящее время сотовые телефоны широко используются детьми и подростками. Соответственно, они сталкиваются с точно такими же рисками, как и при использовании ПК, подключенного к Интернету.

Во-первых, сейчас широко распространены системы обмена мгновенными сообщениями для сотовых телефонов. Дети могут войти в чаты в любой момент, при этом не важно, где они находятся физически, и столкнуться с теми рисками, о которых мы подробно говорили выше: кража персональных данных, педофилы, распространение вирусов и вредоносных программ и т.д.

Спам также начинает одолевать сотовые телефоны. За последние несколько лет SMS-сообщения с рекламой всех типов продуктов и сервисов наводнили сотовые телефоны во всем мире. Большая часть подобной рекламы – это реклама порнографии. Это означает, что дети могут столкнуться с подобной информацией не только при выходе в Интернет со своего компьютера, но и при использовании собственного мобильного телефона.

В результате, родители также должны контролировать то, как дети пользуются своими сотовыми телефонами. Поэтому мы рекомендуем родителям покупать своим детям сотовые телефоны без встроенных функций, которые могли бы подвергать их такому риску (подключение к Интернету, SMS, наличие Bluetooth и т.д.), а подросткам необходимо объяснять, как следует безопасно использовать свой сотовый телефон. Постоянно напоминайте им, чтобы они не отвечали на сообщения из подозрительных и неизвестных источников и не соглашались на встречу с незнакомцами.

**V *Рекомендации психологов для профилактики Интернет-зависимости у детей:***

Ограничьте количество времени, которое дети могут проводить в Интернете. Убедитесь, что ребенок пользуется Сетью во время, отведенное домашнему заданию, для учебы, а не для развлечений.

Не ставьте компьютер в комнате ребенка. Установите компьютер в гостиной или в своей комнате – там, где вы сможете легко контролировать то, что ваш ребенок делает в Интернете. С помощью современных мобильных телефонов можно подключиться к Сети для общения, игр и просмотра сайтов. Неважно, с помощью какого устройства ребенок будет уходить в виртуальный мир. Важно не допустить, чтобы виртуальная реальность не стала для него домом.

Выясните, что ваш ребенок любит делать в Интернете. Некоторые онлайн-игры, в которых действие происходит в фантастических мирах с тысячами игроков по всему миру, например, World of Warcraft, действительно увлекают.

Не подавайте детям плохой пример. Не проводите слишком много времени у компьютера,. Активный отдых всей семьей поможет ребенку переключиться на реальную жизнь. Займите ребенка другими вещами, настольными или спортивными играми. Найдите ему занятие по душе. Тогда Интернет станет подспорьем в учебе, вспомогательным средством поиска информации и общения, а не способом ухода от реальности и бегства от проблем.

**Советы по безопасности, или Как Вы можете защитить своих детей**

Создайте список домашних правил Интернета при участии детей.

Используйте программы по защите детей в сети.

Существует ряд программ, позволяющих защитить собственного ребенка от посещения, нежелательных сайтов.

Программа «Интернет-Цензор» – Интернет—фильтр, предназначенный для блокировки потенциально опасных для здоровья и психики подростка сайтов.

Хотите оградить ребенка от опасных и вредных сайтов? Используйте бесплатное программное обеспечение «Интернет Цензор» - это быстро и очень просто!

Лучшее решение для защиты ребенка в Интернете! В основе работы Интернет Цензора лежит технология "белых списков", гарантирующая 100% защиту от опасных и нежелательных материалов. Программа содержит уникальные вручную проверенные "белые списки", включающие все безопасные сайты Рунета и основные иностранные ресурсы. Программа надежно защищена от взлома и обхода фильтрации.

Более подробную информацию о программе, возможность бесплатно скачать программу вы можете на странице http://www.icensor.ru/soft/

Родителям демонстрируется работа с данной программой, показывается, как можно добавить сайт в «белый» или «черный» список.

**Подведение итогов**

Итак, уважаемые родители, давайте подведем итог нашей сегодняшней встречи. Главное помнить: Ваша задача распознать интернет-зависимость ребенка на ранней стадии и установить пределы на пользование Интернетом. А также определиться с интересами ребенка, найти общие дела, которые отвлекут вашего сына или дочь от виртуального общения, дав понять, что маме и папе не безразлично, чем интересуется их ребенок, чему отдает предпочтения.

**Все, что ребенок может прочитать, посмотреть или послушать в сети Интернет, несет определенную информацию, и только от Вашего контроля зависит, будет ли она развивать его творческое мышление, помогать ребенку в процессе обучения, или напротив, повлияет отрицательно.**

Беседуйте с детьми об их друзьях в Интернете и о том, чем они занимаются так, как если бы вы говорили о чем-то другом.

Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернету.

Позволяйте детям заходить на детские сайты только с хорошей репутацией.

Научите детей никогда не выдавать личную информацию по электронной почте, в чатах, системах мгновенного обмена сообщениями, регистрационных формах, личных профилях и при регистрации на конкурсы в Интернете.

Научите детей не загружать программы без вашего разрешения — они могут ненарочно загрузить вирус или шпионскую программу.

Чтобы ребенок не мог заниматься чем-то посторонним без вашего ведома, создайте для него учетную запись с ограниченными правами.

Приучите детей сообщать вам, если что-либо или кто-либо в Сети тревожит их или угрожает. Оставайтесь спокойными и напомните детям, что они в безопасности, если рассказали вам об этом. Похвалите их и побуждайте подойти еще раз, если случай повторится.

Расскажите детям о порнографии в Интернете и направьте их на хорошие сайты о здоровье и половой жизни.

Настаивайте на том, чтобы дети предоставили вам доступ к своей электронной почте, чтобы вы могли убедиться, что они не общаются с незнакомцами.

Расскажите детям об ответственном поведении в Интернете. Ребята ни в коем случае не должны использовать Сеть для хулиганства, сплетен или угроз другим.

Если вы обеспокоены безопасностью ребенка при его работе в Интернете или при использовании мобильной связи;

Если ребенок подвергся опасности или стал жертвой сетевых преследователей и мошенников;

Обратитесь на линию помощи «Дети онлайн». Эксперты помогут решить проблему, а также проконсультируют по вопросу безопасного использования детьми мобильной связи и Интернет;

Позвоните по телефону 8−800−25−000−15 (звонок по России бесплатный, прием звонков осуществляется по рабочим дням с 9−00 до 18−00 мск).

Или направьте Ваше письмо по адресу: helpline@detionline.com

Подробнее о Линии помощи вы можете узнать на сайте http://detionline.com

И последний мой совет Вам – будьте внимательны к своим детям!

* Предлагаю Вам тест ***«Существует ли реальная опасность для ребенка стать интернет-зависимым или он просто активный пользователь»*** (см. Приложение 1), который поможет Вам разобраться именно в Вашей ситуации. Пройдите его дома, когда у вас будет время все обдумать и в спокойной обстановке сделать вывод и принять решение.

*(тест предлагается на листах-распечатках)*

1. **Подведение итогов (рефлексия)**

Наша встреча подходит к концу. Надеюсь, Вы получили для себя ту порцию информации, которая поможет Вам и вашим детям не стать интернет-зависимыми.

Прошу Вас продолжить фразы:

***Я понял(а), что необходимо всегда...***

***Я получил(а) для себя...***

***Для меня здоровье моего ребенка...***

***Мне бы хотелось еще поговорить о...***

Благодарю наших гостей за беседу, а Вас, уважаемые родители, за неравнодушное отношение к проблеме интернет-зависимости и активность участия в обсуждении данной проблемы.

**Приложение №1**

**Тест**

***«Существует ли реальная опасность для ребенка стать интернет-зависимым или он просто активный пользователь».***

Ответьте на вопросы и суммируйте все баллы. Поставьте за ответ

*«никогда» - 1 балл*

*«редко» - 2 балла*

*«иногда» - 3 балла*

*«часто» - 4 балла*

*«всегда» - 5 баллов*

* Подросток проводит за компьютером более четырех часов в сутки?
* Не начал ли он пренебрегать учебой и прежними увлечениями после покупки компьютера?
* Крик и агрессивная реакция обычны для подростка, когда выпытаетесь отвлечь его от Интернета?
* Как часто подросток жертвует сном ради ночных подключений к Интернету?
* Как часто вам кажется, что ваш ребенок говорит и думает об Интернете даже тогда, когда он отключен от него?
* Уходит ли подросток от ответа на вопрос, что его так привлекает во Всемирной паутине?
* Отказывается ли ваш ребенок от встреч с друзьями или от свидания с любимым человеком ради подключения к Сети?
* Подросток, приходя домой, первым делом проверяет электронную почту?
* Вы уплачиваете довольно значительные суммы по телефонным счетам из-за подключений вашего ребенка к Интернету?

***Результаты***

**10-20 баллов.** Пока все очень неплохо и для волнений нет оснований: ваш ребенок обычный средний пользователь: Интернета. Если он подолгу находится во Всемирной паутине, то это вызвано в основном учебной деятельностью. Постарайтесь не очень давить

на подростка и не настаивайте на сокращении времени, которое он проводит в Интернете.

**21-35 баллов.** Следует подумать о том, как уберечь вашего ребенка от проблем, связанных с Интернетом. Попробуйте убедить подростка, что нездоровый интерес к Интернету искусственно подогревается теми, кто на этом зарабатывает, а ему необходимо готовиться к будущей профессиональной деятельности.

**36-50 баллов.** Следует бить во все колокола и использовать радикальные меры. У подростка уже сформировалась зависимость. Если он не осознает этого, не давайте ему денег на оплату подключений или совсем избавьтесь от компьютера. Попробуйте увлечь его чем-то другим. Если не получается, нужно обратиться к психотерапевту.