

Родительское собрание на тему "Безопасность детей в сети Интернет"

XXI век на дворе: Интернет вошел в каждый дом.

Сеть информирует, учит, продвигает, рекламирует, продает, покупает, следит, контролирует, консолидирует, словом, живет, как настоящее живое общество.

Мы, наши дети, и даже их бабушки и дедушки 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 содержанию, угроза 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.

Цель: просвещение родителей по теме "Безопасность детей в сети Интернет".

Подготовительные мероприятия:

- анкетирование учащихся по теме собрания;
- подготовка буклета для родителей по теме собрания.

Ход родительского собрания

I. Мотивация к деятельности. Тренинг.

Родители рассаживаются по кругу лицом друг к другу, передавая из рук в руки приятный на ощупь мягкий мячик, высказывают свою точку зрения и аргументы по предлагаемому вопросу. Первый вопрос – мячик передают по часовой стрелке, второй вопрос – мячик передают против часовой стрелки и т.д.

Вопросы.

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

Что сделаем, чтобы не повторять ежедневно: "Ты опять весь день просидел (а) за компьютером"?

Какую пользу извлекает Ваш ребенок при использовании сети Интернет?

Какие опасности ждут Вашего ребенка в сети Интернет?

II. Анализ, обсуждение ситуаций и разработка рекомендаций.

Еще недавно компьютеры были скорее роскошью, но уже сейчас являются чуть ли не "предметом первой необходимости".

Результаты анкетирования детей класса показали, что:

100 % детей имеют дома компьютер

В среднем ежедневно дети проводят за ним по 4 часа в день

Из видов деятельности, преобладающих в общении с компьютером, дети на первое место поставили – компьютерные игры. 96% из них каждый день играют в компьютерные игры, причем 51% может начать играть, даже не пообедав.

На втором месте – общение в Сети. 70% пользуются Интернетом – из них 100% общаются в социальных сетях, 63% - играют в сетевые онлайн игры.

Далее дети выбирают прослушивание музыки, рисование, печать документов соответственно 46%, 135 и 1%

38% -при определении рейтинга использования свободного времени на I место поставили компьютер, исключив при этом занятия спортом, прогулки на воздухе, общение с семьей.

Сегодня мы с вами остановимся на особенно важной проблеме современных школьников – зависимости от сети Интернет.

Зависимость в медицинском смысле определяется как навязчивая потребность в приеме привычного вещества, сопровождающаяся ростом толерантности и выраженными симптомами. Рост толерантности означает привыкание ко всё большим и большим дозам.

Интернет-зависимость – это навязчивая потребность в использовании Интернета.

Существует 5 типов Интернет-зависимости:

бесконечный веб-серфинг — постоянные «путешествия» по Интернету с целью поиска информации.

пристрастие к виртуальному общению и виртуальным знакомствам, характеризуется большими объёмами переписки, постоянным участием в чатах, форумах, избыточностью знакомых и друзей из Интернета.

игровая зависимость — навязчивое увлечение сетевыми играми.

навязчивая финансовая потребность — игра по сети в азартные игры, ненужные покупки в интернет-магазинах.

киберсексуальная зависимость — навязчивое влечение к посещению порносайтов.

Интернет-зависимость характеризуется сильным желанием ребенка быть в сети, что приводит к нежеланию проводить время с семьей и друзьями, спать, посещать и делать уроки. Ребенок может перестать следить за своим внешним видом, начинает болезненно реагировать на просьбы отвлечься от компьютера, терять контроль за своим временем, лгать, причем уход от реальности может усиливаться день ото дня.

Родители должны уметь распознать признаки надвигающейся зависимости, прежде чем она станет реальной проблемой. Но это легче сказать, чем сделать.

Зависимость от Интернета все чаще называют чумой XXI века. В отличие от сигарет или наркотиков запретить Интернет нельзя – глобальная Сеть прочно вошла в нашу жизнь. Интернет – необходимый инструмент, которым ребенку в новом тысячелетии предстоит пользоваться постоянно.

Подростковый возраст — время быстрых изменений в жизни. Хотя дети все еще сильно зависят от своих родителей, они уже хотят некоторой свободы. Ребята начинают интересоваться окружающим миром, и отношения с друзьями становятся для них настоящим важными.

Дети этого возраста используют Интернет для разработки школьных проектов. Кроме того, они загружают музыку, пользуются электронной почтой, играют в онлайн-игры и заходят на фанатские сайты своих кумиров. Их любимый способ общения — мгновенный обмен сообщениями.

Данные, показывают, что дети начинают пользоваться Интернетом в самом раннем возрасте, и роль, которую Глобальная сеть играет в жизни подростков, значительна.

Дети опережают взрослых по количеству времени, которое они проводят в Интернете. В возрасте между 8 и 13 годами дети составляют половину общего числа пользователей Интернета

Более 90% подростков 8-16 лет сталкивались с порнографией в сети

44 % детей, регулярно использующих Интернет, хоть один раз подвергались сексуальным домогательствам при виртуальном общении, 11 % подверглись этому несколько раз.

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.

38% детей просматривают страницы о насилии

16% детей просматривают страницы с расистским содержанием

Согласно исследованию, проведенному в 2006 году в Польше, почти 1/3 родителей (28,4%) не осознает опасностей, с которыми могут встретиться их дети в Интернете

Сегодня мы с вами вместе попробуем разобраться в том, какие опасности ждут ребенка в сети и как его от них оградить.

Основные угрозы для детей в сети Интернет

1. Системы мгновенного обмена сообщениями

Системы обмена мгновенными сообщениями (например, MSN Messenger, Yahoo! Messenger, 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 онлайн, 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 P2P-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 одолевает 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.

Итак, вот несколько рекомендаций общих 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. Вместе с ребенком составьте подробный план с указанием, на что тратится время, проводимое за компьютером. Это поможет сократить время на бездумное обновление странички одноклассников в ожидании нового сообщения, чтение новостей ради самого процесса чтения и т.д.

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. Известны случаи, когда взрослые люди достигали крайней степени истощения, не в силах оторваться от любимой игры, не говоря уже о таких «мелочах», как разводы, потеря работы и т.д. Кроме того, во многих играх, чтобы добиться успеха, нужно не только проводить в игре много часов в день, необходимо также вкладывать в своего персонажа реальные деньги, обменивая их на игровую валюту. Не получив денег на игру от родителей, ребенок может пойти на обман или воровство.

Не подавайте детям плохой пример. Не проводите слишком много времени у компьютера, не берите с собой за город ноутбук или планшет. 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.

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 ненароком 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!

III. Рефлексия.

Предлагается обвести свою ладошку и на каждом пальце написать следующее:

Большой палец – над эти я еще хотел (а) бы поработать

Указательный палец – здесь мне были даны конкретные указания

Средний палец – мне совсем не понравилось

Безымянный палец – психологическая атмосфера

Мизинец – мне здесь не хватило

Благодарю за внимание!

Список использованных ресурсов:

Азбука безопасности. В Интернете <http://azbez.com/safety/internet>

Акции детского портала Tvidi.Ru. "Правила безопасности в сети Интернет" <http://www.fid.su/projects/saferinternet/year/actions/tvidi/>

Анкета «Интернет и пятиклассники». http://ludmilakarnazhitska.blogspot.com/2010/11/blog-post_21.html

Безопасность детей в Интернете <http://www.obzh.info/novosti/novoe/bezopasnost-detei-v-internete.html>

Копилочка активных методов обучения <http://www.moi-universitet.ru/ebooks/kamo/kamo/>

Материалы сайта «Интернешка» <http://interneshka.net/>