ПРАВИТЕЛЬСТВО
КУРГАНСКОЙ ОБЛАСТИ
ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ И НАУКИ
КУРГАНСКОЙ ОБЛАСТИ

ул. Ленина, 35, г. Курган, 640000
телефон (8-3522) 46-14-41, факс 46-05-73
сайт: https://don45.kurganobl.ru
эл. почта: don@kurganobl.ru

от 22.12.2022 № ИСХ.08-08376/22

на № _____

Руководителям
муниципальных органов
управления образованием

Руководителям
учреждений, подведомственных
Департаменту образования и науки
Курганской области

На базе ГБУ «Центр помощи детям» создана Служба мониторинга безопасности социальных сетей (далее – Служба мониторинга).

Службой мониторинга безопасности социальных сетей на сайте ГБУ «Центр помощи детям» в разделе Методическая гостиная с октября 2022 года открыт и постоянно пополняется подраздел «Безопасный интернет».

В нем в настоящее время размещены и доступны для скачивания:

- Инструкция по мониторингу социальных сетей.
- Инструкция по подаче заявления об обнаружении неприемлемого или противоправного контента в Роскомнадзор.
- Инструкция пошаговая для педагогов.
- Маркеры агрессивного поведения.
- Маркеры суицидального поведения.
- Маркеры вовлечения в деструктивные сообщества.

Кроме того, размещены «Полезные ресурсы для родителей», в которых есть информация о том, куда можно обратиться за консультацией по разным вопросам обучения и воспитания несовершеннолетних.

Все материалы были направлены письмами Департамента образования и науки Курганской области в адрес муниципальных органов управления образованием и подведомственных учреждений для использования в работе.

Для организации профилактической работы необходимо информировать родителей (законных представителе) о необходимости родительского контроля за доступом детей в сеть Интернет.

Приложение на 13 л. в 1 экз.

Заместитель директора
Департамента образования и науки
Курганской области

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 156422dc533bcfd9a6b984de9cfc1f9cea34b8c1
Владелец: **Хлебников Иван Николаевич**
Действителен: с 06.12.2022 по 29.02.2024

И.Н. Хлебников

Исп. Саможена Елена Ивановна,
(3522) 44-98-58

Приложение

Департамент образования и науки Курганской области
ГБУ «Центр помощи детям», г. Курган

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
для родителей (законных представителей) об организации родительского контроля за доступом детей в сеть Интернет

Курган 2022

Методические рекомендации для родителей (законных представителей) об организации родительского контроля за доступом детей в сетьИнтернет: Методические рекомендации. – ГБУ «Центр помощи детям» 2022 г.
Составители: Павлов Д.К.

Введение

Согласно российскому законодательству, 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.

Данные методические рекомендации разработаны в соответствии с Федеральным законом от 29.12.2010 № 436-ФЗ (ред. от 28.07.2012) «О защите детей от информации, причиняющей вред их здоровью и развитию».

Цель данных методических рекомендаций - ознакомление родителей (законных представителей) с возможностью и необходимостью организации родительского контроля за доступом детей в сеть Интернет. Методические рекомендации предназначены для родителей (законных представителей), т.к. обеспечение безопасности детей в сети Интернет невозможно без привлечения родителей. Часто родители не понимают и недооценивают угрозы, которым подвергается их ребенок, использующий сеть Интернет.

Словарь

Аватар (аватарка, ава) - изображение, которое пользователь выбирает в качестве представления своего аккаунта или сообщества; главное фото на страничке пользователя.

Аккаунт - учетная запись пользователя в социальных сетях. Живой аккаунт - аккаунт человека, не рекламный, не бот, аккаунт, который ведется: постятся фотографии и т.д. (не заброшенный).

Бот - пустой аккаунт, созданный при помощи специальных программ.

Группа - тематическая страничка, созданная пользователем соцсети или представителем компании, целью которой является привлечение к себе целевой аудитории (читателей, потенциальных клиентов) или же перенаправление ее представителей в блоги, в интернет-магазины, другие сообщества. На странице публикуется профильный контент, новости и пр. Подходит для дискуссий и обмена мнениями.

Директ - функция в Instagram, которая позволяет обмениваться личными сообщениями внутри соцсети.

Комментарий - запись пользователя под постом или в обсуждении.

Контент - размещаемый в сообществах текстовый, аудио-, видео- и фотоматериал.

Лайв (**стрим**) - прямая трансляция.

Лайк (кнопка с изображением сердечка, «Нравится») – действие пользователя, выражающее одобрение, принятие и поддержку по отношению к публикуемому контенту.

Логин - имя учетной записи пользователя в соцсетях.

Подписчик - человек, подписанный на определенный аккаунт или сообщество. Фоловер (фолловер, фоловик) - пользователь который подписался на ваш аккаунт в Instagram.

Пост - формат контента в социальных сетях. В зависимости от специфики сети может включать в себя текст, фото, видео, аудио, документ, опрос, ссылку, карту и т.п.

Репост - дублирование какого-либо поста в своем аккаунте или сообществе, одно из ключевых действий в социальной сети, позволяющее поделиться чужим постом с сохранением ссылки на источник.

Сообщество - сущность, которая описывает любое объединение людей в социальных сетях. Создавая сообщество ВКонтакте, вы можете создать и группу, и страницу, и мероприятие.

Социальная сеть - интернет-ресурс, который помогает пользователям глобальной сети находить друг друга и общаться, обмениваясь различными видами контента (текстовыми сообщениями, фото, видео или аудио- файлами) и т.д. Представляет собой базу пользовательских аккаунтов (профилей), связанных между собой. По своему желанию пользователь может добавить или удалить какие-то связи своего аккаунта с другими. В большинстве своем они предоставляют пользователям возможности общения посредством электронной почты или сервисов мгновенного обмена сообщениями.

Стикеры - динамические или статические изображения, которыми можно выражать свои эмоции в личных сообщениях и комментариях.

Сторис (истории) - короткие посты в формате видео или фото в Инстаграм, Вконтакте и Фейсбук, которые показываются в отдельном разделе над основной лентой. Они действуют всего 24 часа, потом автоматически удаляются.

Фейковый аккаунт - аккаунт ненастоящих людей с неверной информацией, а также взломанная страница реального пользователя.

Хештеги – система кликабельных меток и тегов, способ систематизации информации. Хештеги обозначаются с помощью добавления к тому или иному слову значка решетки (#).

Чат - представляет собой сервис, который делает возможным обмен текстовыми сообщениями в Интернете в режиме реального времени. Одновременное общение в чате возможно между неограниченным числом пользователей благодаря особому программному обеспечению.

Общий анализ проблемы и необходимость защиты детей в сети Интернет

Последние годы были ознаменованы большим количеством громких инцидентов, связанных с негативными последствиями нарушений информационной безопасности детей. В России проживает почти 33 миллиона детей в возрасте до 18 лет. Многие из них начинают активно пользоваться интернетом с 14 лет, а некоторые с более раннего возраста.

В современном цифровом социальном пространстве информация распространяется быстро. Сама информация иногда носит противоречивый, негативный характер и влияет на социально-нравственные ориентиры общественной жизни. В связи с этим, возникает проблема информационной безопасности, без решения которой не представляется возможным полноценное развитие не только личности, но и общества. Современный школьник, включенный в процесс познания, оказывается незащищенным от разных потоков информации. Пропаганда жестокости средствами массовой информации, возрастающая роль Интернета, отсутствие цензуры является не только социальной, но и педагогической проблемой.

Центром внимания детей является компьютер и смартфон - по статистике, на школьников приходится около 3-4 часа в день. Сегодня в обществе актуальна следующая проблема – неограниченный доступ ребенка к сети Интернет.

В России 1 сентября 2012 года вступил в силу Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 28.07.2012 года) «О защите детей от информации, причиняющей вред их здоровью и развитию».

Данный закон регулирует отношения, связанные с защитой детей от травмирующего их психику информационного воздействия, жестокости и насилия в общедоступных СМИ. К информации, запрещенной для оборота среди детей, относится информация:

- побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;
- способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;
- обосновывающая или оправдывающая допустимость насилия и (или) жестокости, либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных настоящим Федеральным законом;
- отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;
- оправдывающая противоправное поведение;
- содержащая нецензурную брань;
- содержащая информацию порнографического характера.

Оборот такой информации не допускается в местах, доступных для детей, без применения административных и организационных мер, технических, программно-аппаратных средств защиты детей от такой информации.

Детей и подростков, без всякого сомнения, нужно защищать от разрушающего информационного воздействия на их несформировавшуюся личность. Кроме этого, информационная продукция, запрещенная для детей, не может распространяться в предназначенных для детей образовательных организациях, детских медицинских,

санаторно-курортных, физкультурно-спортивных организациях, организациях культуры, организациях отдыха и оздоровления детей или на расстоянии менее чем сто метров от границ территории этих организаций.

В Законе определяются виды информации, распространение которой среди детей определенных возрастных категорий ограничено, к ней относится информация:

- представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия;
- вызывающая у детей страх, ужас или панику, в том числе представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий;
- представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;
- содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

Распространение такой информационной продукции допускается среди детей определенных возрастных групп при соблюдении обладателем информации установленного законом порядка доступа детей к информации (в частности, при условии, что в информационной продукции содержится идея торжества добра над злом, сострадание к жертве насилия, осуждение насилия, а изображение и описание насилия, жестокости, антиобщественных действий носит ненатуралистический, кратковременный или эпизодический характер и т.п.).

Законом устанавливается классификация информационной продукции по пяти возрастным категориям:

- Информационная продукция для детей, не достигших возраста шести лет.
- Информационная продукция для детей, достигших возраста шести лет.
- Информационная продукция для детей, достигших возраста двенадцати лет.
- Информационная продукция для детей, достигших возраста шестнадцати лет.
- Информационная продукция, запрещенная для детей.

Контентные риски. Что это такое и как их избежать?

Контент – это наполнение или содержание какого-либо информационного ресурса: текст, графика, музыка, видео, звуки и т.д.

Мультимедийное наполнение, адаптированное для использования в мобильных устройствах (смартфоны, коммуникаторы и т.д.): текст, графика, музыка, видео, игры, дополнительное программноеобеспечение.

Информация нежелательного характера, которая несет в себе контентные риски, – это различные информационные ресурсы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие противозаконную, неэтичную и вредоносную информацию.

К противозаконной, неэтичной и вредоносной информации относятся:

- пропаганда насилия, жестокости и агрессии;
- разжигание расовой ненависти, нетерпимости по отношению к другим людям по национальным, социальным, групповым признакам;
- пропаганда суицида;
- пропаганда азартных игр;
- пропаганда и распространение наркотических и отравляющих веществ;
- пропаганда деятельности различных сект, неформальных молодежных движений;
- эротика и порнография;
- нецензурная лексика и т.д.

Такие виды информации в сети Интернет можно встретить практически везде: в социальных сетях, блогах, персональных сайтах, видеохостингах и др.

Размещение противозаконной информации в сети Интернет преследуется по

закону. Это относится в первую очередь к распространению наркотических веществ, порнографических материалов, особенно с участием несовершеннолетних, призывам к разжиганию национальной розни и экстремистским действиям. В российском законодательстве есть возможность в соответствии со статьями уголовного кодекса привлечь к административной и уголовной ответственности за распространение подобного негативного контента владельцев сайтов, а также авторов электронных текстов и видеопродукции.

Неэтичный, противоречащий принятым в обществе нормам морали и социальным нормам, контент не запрещен к распространению, но может содержать информацию, способную оскорбить пользователей и оказать вредоносное воздействие. Подобная информация не попадает под действие уголовного кодекса, но может оказать негативное влияние на психику человека, особенно ребенка. Примерами таких материалов могут служить широко распространенные в сети изображения сексуального характера, порнография, агрессивные онлайн-игры, азартные игры, информация о нездоровом образе жизни, принесении вреда здоровью и жизни, нецензурная брань, оскорбления и др.

Неэтичная и вредоносная информация может быть направлена на манипулирование сознанием и действиями различных групп людей. Такая информация часто бывает заманчивой и оказывает сильное психологическое давление на детей и подростков, которые не способны до конца осознать смысл происходящего и отказаться от просмотра и изучения сайтов с негативным содержимым. Влияние подобного рода информации на еще неокрепшую психику детей и подростков непредсказуемо. Под воздействием таких сайтов может пострадать не только психика, но и физическое здоровье ребенка.

Вредоносный контент может привести к заражению компьютера вирусами и потере важных данных. Особенно опасными с этой точки зрения является просмотр через сеть Интернет тех или иных видеоматериалов. Очень многие распространители негативного контента преследуют определенную цель заразить компьютер, чтобы в дальнейшем иметь возможность манипулировать данными и действиями зараженного компьютера, получить деньги незаконным способом. Такие действия преследуются по закону в соответствии со ст. 272, 273, 274 Уголовного кодекса РФ.

Контентная фильтрация домашнего интернета родителями.

Для ограничения доступа детей к нежелательному, опасному контенту в настоящее время имеется возможность выбрать как коммерческое, так и свободно распространяемое программное обеспечение, сервисы, тарифные опции Интернет-провайдеров, специальные возможности антивирусных программ.

Принцип работы этих систем обычно строится на черных (запрещенных) и белых (разрешенных) списках, либо на основе фильтрации. Наиболее широкое распространение получили три алгоритма фильтрации:

- фильтрация по ключевым словам, (конкретные слова и словосочетания используются для включения блокировки веб-сайта);

- динамическая фильтрация (содержимое запрашиваемого веб-ресурса анализируется в момент обращения, загрузка страниц ресурса в браузер блокируется, если содержимое определяется как нежелательное);

- URL-фильтрация (запрашиваемая страница или целый домен, например, dosug.nu, могут быть определены или категорированы как нежелательный ресурс, вследствие чего доступ к таким страницам блокируется).

Большинство систем контентной фильтрации используют URL- фильтрацию, основанную на анализе и категоризации Интернет-ресурсов. Данный алгоритм является наиболее эффективным методом фильтрации контента.

Для ограничения доступа несовершеннолетних лиц к нежелательному или опасному контенту с настольных компьютеров и мобильных устройств можно использовать дополнительные опции, предлагаемые большинством Интернет-

провайдеров. Для этого необходимо обратиться в службу технической поддержки провайдера (телефон данной службы обычно указан в договоре) и высказать пожелание подключения данной услуги. Далее необходимо следовать инструкциям оператора.

Можно также использовать специализированное программное обеспечение и сервисы. Наиболее популярные, некоммерческие версии: SkyDNS, NetPolice Child, Eyes Relax, Parental Control Bar, Norton Online Family, NetPolice Lite. Помимо этого, существует возможность введения ограничения доступа к нежелательным сайтам путем установки дополнений (расширений) в Интернет-браузерах, таких как: Mozilla FireFox, Chrome, Opera и других.

Обращаем внимание, что на домашних компьютерах также можно задействовать антивирусные программы с функцией «Родительский контроль», которые могут защитить ребенка от нежелательного контента. В основном это коммерческие продукты: Kaspersky Internet Security 2012, Kaspersky Crystal, Kaspersky Internet Security 7.0, KinderGate Родительский контроль, ChildWebGuardian, Spector Pro 6.0, КиберМама, Eset Nod32 и других.

Однако существуют и бесплатные продукты, например, Avira Free Antivirus 2013.

Практически все современные разработчики антивирусных пакетов имеют в своём арсенале продукты для обеспечения безопасности ребенка в сети, блокировки нежелательного и опасного контента.

Возможности родительского контроля.

Фильтры web-сайтов.

Слова-запреты (фильтры). Вы задаете набор ключевых слов, и если что-либо изих списка обнаруживается на web-странице, то она не открывается.

Создание белого списка. Более жесткий способ контроля, когда вы самостоятельно составляете белый список сайтов, которые может посещать ребенок.

Создание черного списка. В черном списке указываются сайты, на которые ребенку заходить запрещено. Приложение работает с базой данных, где содержатся сайты для взрослых.

Крайне желательно, чтобы список регулярно обновлялся через Интернет, иначе появление новых ресурсов быстро сделает защиту неактуальной.

Родители могут расширять черный список сайтов на свое усмотрение, при желании, используя автоматизированную информационную систему ведения и использования базы данных о сайтах, содержащих запрещённую к распространению в России информацию, утвержденную Постановлением Правительства Российской Федерации от 26 октября 2012 года № 1101 «О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет», и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено»» (https://reestr.rublacklist.net).

Ограничение времени, проводимого ребенком за компьютером.

Определяйте расписание пользования компьютером и Интернетом: выбирайте допустимое время суток и продолжительность работы. Так вам не придется прогонять ребенка от компьютера и вступать в конфликт - сеанс закончится сам собой.

Установка запретов на использование детьми отдельных программ.

Во избежание различных недоразумений родители могут ограничить список используемых ребенком программных продуктов. Большинство современных операционных систем имеют в своем составе инструмент доступа пользователей к программным продуктам, что дает возможность ограничения доступа ребенка к нежелательным программным продуктам.

Управление доступом к игровым приложениям.

Возможности родительского контроля позволяют помочь детям играть в безопасные, дружелюбные, занимательные и обучающие игры, соответствующие их

возрасту. В частности, родители могут блокировать как все игры, так и только некоторые из них. Дополнительно родители могут устанавливать разрешение или запрет на доступ к отдельным играм, исходя из допустимой возрастной оценки и выбора типа содержимого.

Журнал отчетов о работе ребенка за компьютером.

С целью анализа того, чем занимался ребенок за компьютером в отсутствие взрослых, какие программы запускал, какие сайты просматривал в Интернете, с кем общался и т.д., родительский контроль ведет запись всех действий подрастающего пользователя. В журнал записываются адреса посещенных детьми страниц Интернета. В некоторых программах журнал с отчетом можно получать по электронной почте, что очень удобно, если родитель находится вне дома, и хочет просмотреть, какие сайты посещал ребенок.

Как помочь ребенку, если он уже столкнулся с Интернет-угрозой.

- Установите положительный эмоциональный контакт с ребенком, расположите его к разговору о том, что случилось. Расскажите о своей обеспокоенности тем, что с ним происходит. Ребенок должен Вам доверять и знать, что Вы хотите разобраться в ситуации и помочь ему, а не наказать.

- Постарайтесь внимательно выслушать рассказ о том, что произошло, понять насколько серьезно произошедшее и насколько серьезно это могло повлиять на ребенка.

- Если ребенок расстроен чем-то увиденным (например, кто-то взломал его профиль в социальной сети), или он попал в неприятную ситуацию (потратил Ваши или свои деньги в результате интернет-мошенничества и пр.) —- постарайтесь его успокоить и вместе с ним разберитесь в ситуации — что привело к данному результату, какие неверные действия совершил сам ребенок, а где Вы не рассказали ему о правилах безопасности в Интернете.

- Если ситуация связана с насилием в Интернете по отношению к ребенку, то необходимо выяснить информацию об агрессоре, выяснить историю взаимоотношений ребенка и агрессора, выяснить существует ли договоренность о встрече в реальной жизни; узнать были ли такие встречи и что известно агрессору о ребенке (реальное имя, фамилия, адрес, телефон, номер школы и т.п.), жестко настаивайте на избегании встреч с незнакомцами, особенно без свидетелей, проверьте все новые контакты ребенка за последнее время.

- Соберите наиболее полную информацию о происшествии, как со слов ребенка, так и с помощью технических средств - зайдите на страницы сайта, где был Ваш ребенок, посмотрите список его друзей, прочтите сообщения. При необходимости скопируйте и сохраните эту информацию - в дальнейшем это может Вам пригодиться (например, для обращения в правоохранительные органы).

- Если Вы не уверены в оценке серьезности произошедшего с Вашим ребенком, или ребенок недостаточно откровенен с Вами или вообще не готов идти на контакт, или Вы не знаете как поступить в той или иной ситуации — обратитесь к специалисту (телефон доверия, горячая линия и др.), где Вам дадут рекомендации о том, куда и в какой форме обратиться, если требуется вмешательство других служби организаций (МВД, МЧС, Сестры и др.).

Информационная безопасность

Экспертами и членами Временной комиссии Совета Федерации по развитию информационного общества в рамках выполнения рекомендаций парламентских слушаний «Актуальные вопросы обеспечения безопасности и развития детей в информационном пространстве», которые прошли в Совете Федерации 17 апреля 2017 г., были разработаны методические рекомендации о размещении на информационных стендах, официальных интернет-сайтах и других информационных ресурсах общеобразовательных организаций и органов, осуществляющих управление

в сфере образования, информации о безопасном поведении и использовании сети «Интернет» (далее - методические рекомендации). В данных методических рекомендациях содержится памятка для родителей об информационной безопасности детей и памятка для обучающихся об информационной безопасности.

Общие правила для родителей.

Независимо от возраста ребенка используйте программное обеспечение, помогающее фильтровать и контролировать информацию, но не полагайтесь полностью на него. Ваше внимание к ребенку - главный метод защиты.

Если Ваш ребенок имеет аккаунт на одном из социальных сервисов (LiveJournal, blogs.mail.ru, vkontakte.ru и т.п.), внимательно изучите, какую информацию помещают его участники в своих профилях и блогах, включая фотографии и видео.

Проверьте, с какими другими сайтами связан социальный сервис Вашего ребенка. Странички Вашего ребенка могут быть безопасными, но могут и содержать ссылки на нежелательные и опасные сайты (например, порносайт, или сайт, на котором друг упоминает номер сотового телефона Вашего ребенка или Ваш домашний адрес)

Поощряйте Ваших детей сообщать обо всем странном или отталкивающем и не слишком остро реагируйте, когда они это делают (из-за опасения потерять доступ к Интернету дети не говорят родителям о проблемах, а также могут начать использовать Интернет вне дома и школы).

Будьте в курсе сетевой жизни Вашего ребенка. Интересуйтесь, кто их друзья в Интернете так же, как интересуетесь реальными друзьями.

Возраст от 7 до 8 лет

- Создайте список домашних правил посещения Интернета при участии детей и требуйте его выполнения.
- Требуйте от Вашего ребенка соблюдения временных норм нахождения за компьютером. Покажите ребенку, что Вы наблюдаете за ним не потому, что Вам это хочется, а потому что Вы беспокоитесь о его безопасности и всегда готовы ему помочь.
- Компьютер с подключением к Интернету должен находиться в общей комнате под присмотром родителей.
- Используйте специальные детские поисковые машины.
- Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
- Создайте семейный электронный ящик, чтобы не позволить детям иметь собственные адреса.
- Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего программного обеспечения.
- Приучите детей советоваться с Вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.
- Научите детей не загружать файлы, программы или музыку без вашего согласия.
- Не разрешайте детям использовать службы мгновенного обмена сообщениями.
- В «белый» список сайтов, разрешенных для посещения, вносите толькосайты с хорошей репутацией.
- Не забывайте беседовать с детьми об их друзьях в Интернете, как если бы речь шла о друзьях в реальной жизни.
- Не делайте «табу» из вопросов половой жизни, так как в Интернете дети могут легко наткнуться на порнографию или сайты «для взрослых».

- Научите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

Возраст детей от 9 до 12 лет

В данном возрасте дети, как правило, уже наслышаны о том, какая информация существует в Интернете. Совершенно нормально, что они хотят это увидеть, прочесть, услышать. При этом нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств Родительского контроля.

Учитывая это необходимо:

- Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.
- Требуйте от Вашего ребенка соблюдения норм нахождения за компьютером.
- Наблюдайте за ребенком при работе за компьютером, покажите ему, что Вы беспокоитесь о его безопасности и всегда готовы оказать ему помощь.
- Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.
- Используйте средства блокирования нежелательного контента какдополнение к стандартному Родительскому контролю.
- Не забывайте принимать непосредственное участие в жизни ребенка, беседовать с детьми об их друзьях в Интернете.
- Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернету.
- Позволяйте детям заходить только на сайты из "белого" списка, который создайте вместе с ними.
- Научите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.
- Научите детей не загружать программы без Вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
- Создайте Вашему ребенку ограниченную учетную запись для работы на компьютере.
- Научите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Напомните детям, что они в безопасности, если сами рассказали вам о своих тревогах и опасениях.

Расскажите детям о порнографии в Интернете.

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

Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

Возраст детей от 13 до 17 лет

В этом возрасте подростки активно используют поисковые машины, пользуются электронной почтой, службами мгновенного обмена сообщениями, скачивают музыку и фильмы. Мальчикам в этом возрасте больше по нраву сметать все ограничения, они жаждут грубого юмора, азартных игр, картинок «для взрослых». Девочки предпочитают общаться в чатах, при этом они гораздо более чувствительны к сексуальным домогательствам в Интернете.

Зачастую в данном возрасте родителям уже весьма сложно контролировать своих детей, так как об Интернете они уже знают значительно больше своих родителей. Тем не менее, не отпускайте детей в «свободное плавание» по Интернету.

Старайтесь активно участвовать в общении ребенка в Интернете.

Важно по-прежнему строго соблюдать правила Интернет-безопасности - соглашение между родителями и детьми. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернете. Следует обратить внимание на необходимость содержания родительских паролей (паролей администраторов) в строгом секрете и обратить внимание на строгость этих паролей.

Советы по безопасности в этом возрасте от 13 до 17 лет

- 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 Интернете (в том числе в чатах).

- Компьютер с подключением к сети Интернет должен находиться в общей комнате.

- 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.

- Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

- Необходимо знать, какими чатами пользуются Ваши дети. Поощряйте использование моделируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.

- Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из сети Интернет.

- Научите детей не выдавать свою личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.

- Научите детей не загружать программы без Вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.

- Научите 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.

- 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 почтовыефильтры.

- Научите детей уважать других в интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде - даже в виртуальном мире.

- Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.

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

- Приучите себя знакомиться с сайтами, которые посещают подростки.

Постоянно контролируйте использование Интернета Вашим ребенком! Это не нарушение его личного пространства, а мера предосторожности и проявление Вашей родительской ответственности и заботы.

Старайтесь быть родителем – другом!

Полезные сайты для родителей

http://www.nachalka.com/bezopasnost – Безопасность детей в Интернете

http://detionline.com/ – Дети России Онлайн. Сделаем Интернет безопаснее вместе

http://www.ifap.ru/library/book099.pdf – Безопасность детей в Интернете
http://www.microsoft.com/ru-ru/security/default.aspx – Центр безопасности Microsoft

http://stopfraud.megafon.ru/parents/ – Безопасный Интернет от Мегафон
http://www.fid.su/projects/journal/ – Фонд развития Интернет. Журнал «Дети в информационном обществе»

http://www.mts.ru/help/useful_data/safety/ – Безопасный Интернет от МТС
http://safe.beeline.ru/index.wbp – Безопасный Интернет от Билайн
http://www.saferunet.ru/ – Центр безопасного Интернета в России
http://www.friendlyrunet.ru/safety/74/index.phtml – Фонд «Дружественный Рунет»

http://netpolice.ru/filters/ – Фильтры NetPolice

http://www.socobraz.ru/index.php/Сообщество_родителей – СОЦОБРАЗ.

http://www.microsoft.com/ru-ru/security/family-safety/kids-social.aspx – Как помочь вашим детям более безопасно пользоваться сайтами социальных сетей?

http://play.mirchar.ru/sovety-roditelyam-po-obespecheniyu-bezopasnosti-detey.html

– Консультации для родителей по обеспечению безопасности детей в Интернет **http://www.internet-kontrol.ru/** –Защита детей от вредной информации в сети Интернет

http://www.oszone.net/6213/ – Обеспечение безопасности детей при работе в Интернет

http://wiki.saripkro.ru/index.php/Интернет-безопасность_для_родителей – Интернет-безопасность для родителей

http://www.sch169.ru/doc/pam.pdf – Как защититься от интернет-угроз

Список использованной литературы:

1. О защите детей от информации, причиняющей вред их здоровью и развитию: федеральный закон от 29.12.2010 N 436-ФЗ [Электронный ресурс] // СПС Консультант Плюс.
2. Гендина Н. И. Основы информационной культуры школьника: учебно-методический комплекс для учащихся 5-7-х классов общеобразовательных организаций / Н. И. Гендина, Е. В. Косолапова. – М.: РШБА, 2017. – 432 с.
3. Безопасный интернет – детям! Полезные советы для тебя и твоих друзей [Электронный ресурс]: сайт // Министерство внутренних дел Российской Федерации.
4. Линия помощи «Дети онлайн» [Электронный ресурс]: сайт. – Режим доступа: http://detionline.com/.
5. Методические рекомендации по контролю за использованием несовершеннолетними сети Интернет во внеучебное время. Методические рекомендации / Сост. О.В. Пикулик, С.В. Синаторов. – Саратов: ГАОУ ДПО «СарИПКиПРО». – 2012. – 39 с.
6. Правила поведения учащихся в современной информационной среде [Электронный ресурс]: сайт. – Режим доступа: http://5319sc5.edusite.ru/DswMedia/ravila_povedenija_v_inv_srede.pdf
7. Сайт «Безопасность детей» Онлайн Энциклопедия
Журнал «Дети в информационном обществе» - Режим доступа: http://detionline.com/journal/numbers/28