**РЕКОМЕНДАЦИИ ДЛЯ РОДИТЕЛЕЙ (ЗАКОННЫХ ПРЕДСТАВИТЕЛЕЙ) О ВОЗМОЖНОСТЯХ ОРГАНИЗАЦИИ РОДИТЕЛЬСКОГО КОНТРОЛЯ ЗА ДОСТУПОМ ДЕТЕЙ В СЕТЬ ИНТЕРНЕТ**

**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 N 436-ФЗ (ред. от 28.07.2012) "О защите детей от информации, причиняющей вред их здоровью и развитию".

Цель данных методических рекомендаций - ознакомить 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, находясь в сети Интернет.

В социальном пространстве информация распространяется быстро, благодаря техническим возможностям. Сама информация часто носит противоречивый, агрессивный и 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 потоков информации. Пропаганда жестокости средствами массовой информации, возрастающая роль Интернета, отсутствие цензуры является не только социальной, но и педагогической проблемой.

Современный подросток все меньше общается в реальной жизни со сверстниками, друзьями, одноклассниками. В среднестатистической семье телевизор включен до 7-8 часов в день, а центром внимания детей является компьютер - по статистике, на школьников приходится около 3-4 часа в день, что равнозначно пяти урокам в школе. Современные гаджеты и Интернет заменили детям прогулки на улице, общение со сверстниками и родителями. 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 N 436-ФЗ (ред. от 28.07.2012) "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 среди детей 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:

1. информационная продукция для детей, не достигших возраста шести лет;

2. информационная продукция для детей, достигших возраста шести лет;

3. информационная продукция для детей, достигших возраста двенадцати лет;

4. информационная продукция для детей, достигших возраста шестнадцати лет;

5. 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. (например, контент интернетсайта); мобильный контент - мультимедийное наполнение, адаптированное для использования в мобильных устройствах (телефоны, смартфоны, коммуникаторы и т.д.): текст, графика, музыка, видео, игры, дополнительное программное обеспечение.

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.

В сети Интернет такую информацию можно встретить практически везде: в социальных сетях, блогах, персональных сайтах, видеохостингах и др. Не являются исключением и мобильные сервисы.

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 Интернетпровайдеров, 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:

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

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

3. 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).

Лучшие в мире системы контентной фильтрации используют URLфильтрацию, основанную на анализе и категоризации Интернет-ресурсов. Такой механизм признан 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 Интернетпровайдеров. 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: Internet Explorer, 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 с веб-приложением Avira Free SocialShield.

Использование функции родительского контроля подробно описано в инструкциях пользователя для антивируса.

Стоит обратить особое внимание на наличие функции родительского контроля при приобретении антивирусной программы или продлении лицензии на следующий год, сообщить о вашем желании распространителю программного обеспечения. 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.**

1. Фильтры web-сайтов.

Слова-запреты (фильтры). Вы задаете набор ключевых слов, и если что-либо из их 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>).

2. 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.

3. 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.

4. 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.

5. 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 аудит 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 служб и организаций (МВД, МЧС, Сестры и др.)

**Сервисы, позволяющие родителям контролировать использование Интернета детьми**

**КиберМама™** http://www.cybermama.ru - программа для ограничения времени работы на компьютере детей и подростков. Позволяет создавать расписание работы ребенка за компьютером и автоматически контролировать нежелательных игр и программ, блокировать доступ в Интернет. Программа проста и понятна в использовании и не требует от родителей специальных компьютерных навыков и знаний.

**NetKids** - сервис, который позволяет родителям контролировать использование интернета детьми. NetKids это: Блокировка доступа к опасным сайтам; Отчеты о посещенных сайтах; Мониторинг общения в социальных сетях; Контроль загрузки фотографий и личной информации; Отчеты о поисковых запросах; Мониторинг почтовых сообщений и записей в блогах. Вся работа осуществляется через удобный и понятный web-интерфейс.

**KinderGate Родительский Контроль 1.0.** Эта программа-фильтр (www.usergate.ru) предлагает 82 категории фильтрации веб-сайтов в 5 основных уровнях доступа (по умолчанию запрещен доступ к фишинговым ресурсам, сайтам с порнографическим контентам, а также к сайтам, содержащим вредоносный код). Самый высокий уровень фильтрации подразумевает, в числе прочего, запрет прокси-серверов, сайтов знакомств. Доступно создание расширенных правил, «черных» и «белых» списков для сайтов. Можно установить ограничение скачивания видео, звуковых файлов, изображений, архивов и EXE-файлов, документов. В программе реализован модуль морфологического анализа, позволяющий блокировать веб-страницы с нецензурной лексикой. Для ограничения времени, проводимого ребенком за компьютером, предусмотрен специальный инструмент «Расписание работы». Кроме этого, доступна статистика посещенных веб-ресурсов с указанием значений входящего и исходящего трафика, а также просмотр сообщений в сетях odnoklassniki.ru и vkontakte.ru.

**Интернет Цензор** - интернет-фильтр, предназначенный для блокировки потенциально опасных для здоровья и психики подростка сайтов. В основе работы программы лежит технология «белых списков», гарантирующая 100%-ную защиту от опасных и нежелательных материалов. Фильтр «Интернет Цензор» можно скачать бесплатно на официальном сайте. Программа содержит уникальные вручную проверенные «белые списки», включающие все безопасные сайты Рунета и основные иностранные ресурсы. Программа надежно защищена от взлома и обхода фильтрации. «Интернет Цензор» может использоваться как в домашних условиях, так и в образовательных учреждениях, библиотеках, музеях, интернет-кафе и иных местах, где возможно предоставление несовершеннолетним доступа в Интернет.

**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/securitv/default.aspx - Центр безопасности Microsoft

http://stopfraud.megafon.ru/parents/ - Безопасный Интернет от Мегафон

http://www.fid.su/proj ects/journal/ - Фонд развития Интернет. Журнал «Дети в информационном обществе»

http://www.mts .ru/help/useful data/safetv/ - 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/safetv/74/index.phtml - Фонд «Дружественный Рунет»

<http://netpolice.ru/filters/> -Фильтры NetPolice

http://www.SOCobraz.ru/index.php/Сообщество родителей - Сообщество родителей СОЦОБРАЗ

http://www.microsoft.com/ru-ru/securitv/familv-safetv/kids-social.aspx - Как помочь вашим детям более безопасно пользоваться сайтами социальных сетей?

http://windows.microsoft.com/ru-RU/windows7/products/features/parental-controls - Родительский контроль в Windows 7

http://plav.mirchar.ru/sovetv-roditelvam-po-obespechenivu-bezopasnosti-detev.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/do c/pam.pdf - Как защититься от интернет-угроз