**«Как защитить ребенка
от негативного контента в СМИ и Интернет?»**

**Информация для родителей**

   Слово «контент» происходит от английского «content»  - содержание. Контент – любой вид информации (текст, аудио, видео, изображение), составляющий содержание информационного продукта. Под  «контентом» в широком смысле понимают наполнение сайта. В более узком смысле слова «контент сайта» (site content) - это материалы, размещенные на нем: в основном тексты, а также картинки и музыка. Вебсервисы контентом не являются. Самые характерные примеры контент-сайтов - интернет-СМИ и библиотеки, т.е. подборки текстов.

**Классификация интернет-угроз**

   Во Всемирной паутине существует определённая классификация Интернет-угроз. Юных пользователей сети могут подстерегать опасности. Их условно можно разделить на интернет-угрозы, связанные с безопасностью компьютера, с которого совершается выход в интернет, и интернет-угрозы психологического характера для детей и молодежи.  Классификация угроз в Сети по четырем группам риска: контентные риски, коммуникационные риски, электронные риски, потребительские риски.
   Некоторые Интернет-ресурсы могут причинить вред здоровью и развитию детей и подростков. Одни вовлекают детей в зависимость, другие разжигают национальную рознь, третьи негативно влияют на их психическое развитие, разрушают способность к реальному общению, влияют на мировоззрение, а также предлагают различные виды мошенничества и т. д. Отказываться от благ информационных технологий бессмысленно, но бесконтрольный доступ детей к Интернету может привести к:

* Киберзависимости,
* Заражению вредоносными программами при скачивании файлов,
* Нарушению нормального развития ребенка,
* Неправильному формированию нравственных ценностей,
* Знакомству с человеком с недобрыми намерениями.

   Как защитить детей от информации, причиняющей вред их здоровью и развитию, какие меры нужно принимать, чтобы уберечь их от пропаганды насилия и жестокости в журналах, газетах, Интернете и других средствах массовой информации?
   В последние годы в мире и стране принят ряд важнейших законодательных актов, направленных на предупреждение наиболее серьезных угроз здоровья детей. Созданы новые государственные и общественные институты: учреждена должность Уполномоченного при Президенте Российской Федерации по правам ребенка, в ряде субъектов Российской Федерации создан институт уполномоченного по правам ребенка, учрежден Фонд поддержки детей, находящихся в трудной жизненной ситуации. Увеличился объем финансирования социальных расходов из федерального бюджета и бюджетов субъектов Российской Федерации, приняты новые меры социальной поддержки семей с детьми.
   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. Обеспечение государством информационной безопасности детей, защита их физического, умственного и нравственного развития во всех аудиовизуальных медиа-услугах и электронных СМИ - это требование международного права (Рекомендации Европейского Парламента и Совета ЕС от 20.12.2006 **«О защите несовершеннолетних и их человеческого достоинства в Интернете»**),
   Федеральный закон Российской Федерации от 28 июля 2012 г. N 139-ФЗ **«О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию»** и отдельные законодательные акты Российской Федерации» охватывает практически все виды информационной продукции, включая СМИ, Интернет, сотовую связь и др. Он вносит изменения во многие законные акты Российской Федерации. Поправки, внесенные в закон **«О защите детей от информации, причиняющей вред их здоровью и развитию»** ( 29 декабря 2010 года №  436-ФЗ), впервые более подробно регламентируют способы маркировки контента и описывают процедуры экспертизы «информационной продукции».
   Законом вносится предложение об ограничении в Сети «мест доступных для детей» и предусматривается ответственность операторов и администраторов Сайтов, которые не принимают административных и организационных мер, технических и программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и развитию.

**Обеспечение безопасности детей в СМИ и Интернет**

   Одним из основных направлений в борьбе за информационную безопасность детей является **просвещение родителей.** По данным статистики, половина российских подростков знает о Всемирной паутине и умеет работать в ней гораздо больше и лучше своих мам и пап. Уровень знаний родителей о программах и модулях по защите детей от негативной информации также очень и очень низкий. Сегодня многие из них встают перед проблемой - как же ограничить доступ ребенка к компьютеру, как ограничить время, пребывания в Интернет и защитить от порно-наркотиков-матов? Присмотр за детьми в интернете называется термином «родительский контроль».
  **Родительский контроль** — это программы и службы, которые позволяют родителям и опекунам отслеживать, как ребенок использует компьютер: от фильтрации веб-содержимого и управления контактами электронной почты до ограничений на общение детей через Интернет.
   Цель таких средств — **обеспечить безопасность ребенка в Интернете.**Эти инструменты иногда называют семейными настройками или настройками семейной безопасности. Существует множество программ по родительскому контролю, многие из них являются частью программ-антивирусов. Некоторые функции родительского контроля предусмотрены в операционной системе. Но настоящий родительский контроль обеспечивают только специализированные программы:
   **Анаферон** http://netkidscontrol.ru/anaferon. для блокировки сайтов, потенциально опасных для здоровья и психики учащихся.
   **Инетернет-фильтры** (Интернет Цензор и NetPolice).
   В основе работы программы **Интернет Цензор** 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. Интернет Цензор может использоваться как в домашних условиях, так и в организациях – образовательных учреждениях, библиотеках, музеях, интернет-кафе и иных местах, где возможно предоставление несовершеннолетним доступа в Интернет. **NetPolice**— программное обеспечение для фильтрации сайтов по их содержимому, не позволяет получить доступ к определённым сайтам или услугам сети Интернет. Система позволяет блокировать веб-сайты с содержимым, не предназначенным для просмотра. http://netpolice.ru — официальный сайт интернет-фильтра NetPolice.
   В рамках проекта **«Ребенок в Сети»** каждый пользователь может бесплатно скачать и установить новое комплексное решение безопасности**Panda Internet Security 2012**, которое предоставляет максимальную защиту от всех типов угроз, включая защиту от вирусов, шпионов, хакеров, спама, мошенников и пр. Функция родительского контроля позволяет не только ограничить ребенка от доступа к нежелательным сайтам в Интернете (порнография, наркотики, онлайн-казино и пр.), но и дистанционно подключаться к компьютеру.

|  |
| --- |
| **Правила работы в сети Интернет**1. Не входите на незнакомые сайты.
2. Если к вам по почте пришел файл Word или Excel, даже от знакомого лица, прежде чем открыть, обязательно проверьте его на вирусы.
3. Если пришло незнакомое вложение, ни в коем случае не запускайте его, а лучше сразу удалите и очистите корзину.
4. Никогда не посылайте никому свой пароль.
5. Старайтесь использовать для паролей трудно запоминаемый набор цифр и букв.
6. При общении в Интернет не указывайте свои личные данные, а используйте псевдоним (ник).
7. Без контроля взрослых ни в коем случае не встречайтесь с людьми, с которыми познакомились в сети Интернет.
8. Если в сети необходимо пройти регистрацию то постарайтесь выполнить ее так, чтобы в ней не было указано никакой личной информации.
9. Не всей информации, которая размещена в Интернете, можно верить.
10. Не оставляйте без присмотра компьютер с важными сведениям на экране.
11. Не сохраняйте важные сведения на общедоступном компьютере.

**Рекомендации родителям**1. Посещайте Интернет вместе с детьми. Поощряйте ваших детей делиться с вами их успехами и неудачами в деле освоения Интернет;
2. Объясните детям, что если в Интернет что-либо беспокоит их, то им следует не скрывать этого, а поделиться с вами своим беспокойством;
3. Объясните ребенку, что при общении в чатах, использовании программ мгновенного обмена сообщениями, использовании он-лайн игр и других ситуациях, требующих регистрации, нельзя использовать реальное имя, помогите вашему ребенку выбрать регистрационное имя, не содержащее никакой личной информации;
4. Объясните ребенку, что нельзя выдавать свои личные данные, такие как домашний адрес, номер телефона и любую другую личную информацию, например, номер школы, класс, любимое место прогулки, время возвращения домой, место работы отца или матери и т. д.;
5. Объясните своему ребенку, что в реальной жизни и в Интернет нет разницы между неправильными и правильными поступками;
6. Научите ваших детей уважать собеседников в Интернет. Убедитесь, что они понимают, что правила хорошего тона действуют одинаково в Интернет и в реальной жизни;
7. Скажите им, что никогда не стоит встречаться с друзьями из Интернет. Ведь люди могут оказаться совсем не теми, за кого себя выдают;
8. Объясните детям, что далеко не все, что они могут прочесть или увидеть в Интернет– правда. Приучите их спрашивать о том, в чем они не уверены;
9. Не забывайте контролировать детей в Интернет с помощью специального программного обеспечения. Это поможет вам отфильтровывать вредоносное содержание, выяснить, какие сайты на самом деле посещает ваш ребенок и что он там делает.
 |

**Возраст детей от 7 до 8 лет**

    В Интернете ребенок старается посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей. Поэтому родителям (законным представителям) особенно полезны будут те отчеты, которые предоставляются программами по ограничению использования Интернета, т. е. **Родительским контролем**.
  При этом важно, чтобы у ребенка не было ощущения, что за ним ведется постоянное наблюдение. Однако, родителям полезно знать, какие сайты посещает их ребенок. Дети в данном возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах. Они любят играть в сетевые игры и путешествовать по Интернет, используя электронную почту, заходить на сайты и чаты.

**Рекомендации по безопасности детей от 7 до 8 лет**

* Создайте список домашних правил посещения Интернет 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 этого хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь;
* Компьютер с подключением в Интернет 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 ПО;
* 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 только сайты с хорошей репутацией;
* Не забывайте беседовать с детьми об их друзьях в Интернет, как если бы речь шла о друзьях в реальной жизни;
* Не делайте «табу» из вопросов половой жизни, так как в Интернет дети могут легко наткнуться на порнографию или сайты «для взрослых»;
* Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и 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.

**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 боле чувствительны к сексуальным домогательствам в Интернет. В данном возрасте родителям часто уже весьма сложно контролировать своих детей, так как об Интернет они уже знают значительно больше своих родителей. Тем не менее, особенно важно строго соблюдать правила Интернет-безопасности - соглашение между родителями и детьми. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернет.
   Следует обратить внимание на необходимость содержания родительских паролей (паролей администраторов) в строгом секрете и обратить внимание на строгость этих паролей.

**Рекомендации по безопасности детей
в возрасте от 13 до 17 лет**

* Создайте список домашних правил посещения Интернет при участии подростков и требуйте безусловного его выполнения. Укажите список запрещенных сайтов («черный список»), часы работы в Интернет, руководство по общению в Интернет (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 Интернет, 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 модерируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.
* Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из сети Интернет.
* Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернет.
* Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
* Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.
* Расскажите детям об опасности порнографии в Интернет. Помогите им защититься от спама. Научите подростков не выдавать в Интернет своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.
* Приучите себя знакомиться с сайтами, которые посещают подростки.
* 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

*Использовались материалы:*

**Безмалый, В. Ф.** Обеспечение безопасности детей при работе в Интернет [Электронный ресурс] / В. Ф. Безмалый. URL: <http://www.ifap.ru/library/book331.pdf> (дата обращения 28.10.2013)