

Памятка для родителей об информационной безопасности детей

Определение термина "информационная безопасность детей" содержится в Федеральном законе N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию", регулирующим отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию. Согласно данному закону "информационная безопасность детей" - это состояние защищенности, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию.

В силу Федерального закона N 436-ФЗ информацией, причиняющей вред здоровью и (или) развитию детей, является:

1. информация, запрещенная для распространения среди детей;
2. информация, распространение которой ограничено среди детей определенных возрастных категорий.
3. К информации, запрещенной для распространения среди детей, относится:
4. информация, побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в т.ч. причинению вреда своему здоровью, самоубийству;
5. способность 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;
6. обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям и животным;
7. отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;
8. оправдывающая противоправное поведение;
9. содержащая нецензурную брань;
10. содержащая информацию порнографического характера.

К информации, распространение которой ограничено среди детей определенного возраста, относится:

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

С учетом этого Вам предлагаются правила работы в сети Интернет для различных возрастных категорий, соблюдение которых позволит обеспечить информационную безопасность ваших детей.

Общие правила для родителей:

1. 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.
2. 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.
3. 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).
4. Поощряйте Ваших детей сообщать обо всем странном или отталкивающим 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 колледжа).
5. Будьте в курсе сетевой жизни Вашего ребенка. Интересуйтесь, кто их друзья в Интернет так же, как интересуетесь реальными друзьями.

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

1. 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).
2. Компьютер с подключением к сети Интернет должен находиться в общей комнате.
3. 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.
4. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
5. Необходимо знать, какими чатами пользуются Ваши дети. Поощряйте использование модерлируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.
6. Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из сети Интернет.
7. Приучите 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.

8. Приучите детей не загружать программы без Вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
9. Приучите 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.
10. 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 почтовые фильтры.
11. Приучите себя знакомиться с сайтами, которые посещают подростки.
12. Научите детей уважать других в интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде - даже в виртуальном мире.
13. Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.
14. Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закону.

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

Внимание! Ваш ребенок легко может столкнуться с теми, кто предложит ему купить наркотики в сети Интернет.

Чтобы избежать этого следует обращать внимание на следующие моменты:

1. Насколько много времени и в каких сетях проводит ваш ребенок. Наиболее популярным каналом распространения информации для наркопреступников являются Telegram и соцсеть VK. Если у вашего ребенка установлен Telegram, то это повод обратить дополнительное внимание. Если нет возможности проверить телефон ребенка, то вы можете установить программу на свой и увидеть непосредственно в программе, подключен ли к ней телефон ребенка.

2. Если на компьютере установлен браузер TOR, то это повод заострить внимание на поведении и контактах ребенка, поскольку этот браузер часто используется для подключения к «даркнету» - сайтам, которые заблокированы в России. Если на компьютере установлен пароль, то можно попробовать войти, используя «Безопасный режим» работы Windows (зачастую в него можно войти без пароля, как администратор, а не пользователь): Перезагрузите компьютер. На экране входа удерживайте клавишу Shift, а затем выберите элементы – Выключение – Значок питания – Перезапуск. После перезагрузки компьютера, на экране Выберите параметр выберите элементы: Диагностика->Дополнительные параметры-> Параметры загрузки-> Перезапуск. После перезагрузки компьютера вы увидите список параметров. Нажмите клавишу 4 или F4, чтобы запустить компьютер в безопасном режиме. Если вам будет нужен Интернет, выберите клавиши 5 или F5, чтобы войти в Безопасный режим с загрузкой сетевых драйверов.

3. Обращайте внимание на использование ребенком режима «инкогнито» в браузерах и на историю заходов и поиска. Посмотрев историю можно понять какими сайтами интересуется ваш ребенок. Отсутствие же истории заходов в браузере, при условии, что ребенок «сидел в Интернете» - повод присмотреться.

4. Также обратите внимание на использование в браузере надстроек, обеспечивающих VPN-соединение.

5. Использование ребенком KIWI-кошелька или Bitcoin-кошелька также повод задуматься, поскольку ими очень часто пользуются в целях нелегальных покупок. Обратите внимание, что KIWI-кошелек можно пополнять просто с номера мобильного телефона, поэтому не лишним будет подключить для номера телефона ребенка отдельный «контентный счет» (делается в офисах операторов) и контролировать списание со счета телефона.

6. Наличие и использование автономных операционных систем, расположенных на съемных дисках или Flash-накопителях, например TAILS. Такие системы используются для анонимного доступа в Интернет и позволяют пользователю сохранить инкогнито. Чаще всего ими пользуются распространители наркотиков и экстремисты.

Но помните! Самое главное – это доверие вашего ребенка, ведь ни один из перечисленных индикаторов не может дать 100% уверенность, а возможности подрастающего поколения зачастую превышают возможности контроля со стороны родителей. Кроме того, высокий уровень доверия позволит вам вести более эффективный контроль за сетевой жизнью ребенка.