РЕКОМЕНДАЦИИ РОДИТЕЛЯМ

О ЗАЩИТЕ ДЕТЕЙ ОТ ИНТЕРНЕТ УГРОЗ И НЕГАТИВНОЙ ИНФОРМАЦИИ В ИНТЕРНЕТЕ

Оглавление

Введение

В настоящее время во всем мире, в том числе и в Российской федерации, проблема защиты детей в киберпространстве привлекает все больше и больше внимания. С приходом в нашу жизнь высоких технологий мы не только получили ряд благ, но и приобрели определенные риски, в том числе и риск деструктивного воздействия на нравственное, духовное, психическое развитие детей.

На территории Российской Федерации политика государства в сфере защиты детей от негативной информации отражена в следующих нормативно-правовых актах: Федеральный закон от 29 декабря 2010 г. №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью»; нормативно-правовые акты Минкомсвязи.

О том, какие угрозы таит в себе интернет и как защитить детей в информационном пространстве, пойдет речь в данной рекомендации.

Основные виды угроз и негативной информации в Интернете

В Интернете, как и в обычном мире, детей поджидает ряд угроз, основными из которых являются:

- мошенники;
- похитители;
- ресурсы, призывающие к расовой нетерпимости;
- ресурсы для взрослых;
- ресурсы, содержащие сцены насилия;
- ресурсы, призывающие к суициду;
- ресурсы экстремистского содержания;

- ресурсы, пропагандирующие, реализующие наркотические вещества;
- ресурсы, пропагандирующие алкоголь;
- ресурсы, отрицающие семейные ценности;
- ресурсы, содержащие ненормативную лексику;
- ресурсы, посвященные азартным играм;
- ресурсы религиозных сект.

Отдельно среди угроз можно выделить социальные сети (далее соцсети).

Соцсети уже достаточно давно вошли в нашу жизнь, но они не безобидны, как это кажется на первый взгляд. По своей сути соцсети представляют собой Интернет в Интернете, на страницах соцсетей зачастую размещаются посты (статьи) экстремистского, суицидного, порнографического содержания, а также посты, пропагандирующие употребление наркотических, психотропных веществ, аморальный образ жизни, гомосексуализм и т.д.

Кроме того, к глубочайшему сожалению, дети, зарегистрированные в соцсетях, чаще становятся жертвами похитителей, педофилов, вербовщиков экстремистских, запрещенных организаций.

2. Как защитить детей от негативной информации

Защита детей от негативной информации в Интернете дома и на мобильном устройстве - обязанность каждого родителя.

Защита детей в интернете - это не просто установка родительского контроля и пароля. Дети намного умнее и «продвинутее», чем вы думаете, и даже самую идеальную и надежную защиту они могут обойти. Для того, чтобы ваша защита возымела эффект, необходим комплекс мер:

1. Необходимо договориться с ребенком, когда и в какое время он может пользоваться Интернетом. Объяснить, что ни при каких условиях он не должен размещать в интернете и никому не сообщать сведения о себе, в том числе: школу, класс, домашний адрес, ф.и.о., материальное положение родителей и так далее.
2. Объяснить, какие угрозы подстерегают в Интернете, объяснить, что люди на самом деле могут быть не теми, за кого себя выдают, а также не знакомиться с ними и не соглашаться на встречи в реальном мире.
3. Создать на домашнем компьютере отдельную учетную запись для ребенка и установить родительский контроль.
4. Ввести оговоренное с ребенком ограничение использования компьютером, выбрать программы и игры, доступные ребенку.

5. Применить защиту через DNS. Компьютеры между собой оперируют цифрами, и адреса сайтов для компьютеров тоже числа, а человеку проще и лучше оперировать осмысленным текстом. DNS - это преобразователь "текста" для людей (типа rambler.ru) в "адреса-числа" (типа 81.19.70.1) и наоборот. Первый этап защиты детей от нежелательного контента будет основан на том, что есть DNS сервера, которые во время "преобразования" могут ещё и фильтровать. Другими словами, если ребёнок оказывается в браузере на сайте yandex.ru, то этот хороший сайт в DNS будет преобразован в его компьютерный-числовой-адрес (IP адрес). Но если ребёнок вольно или невольно попадает на sex.com, то такой адрес будет преобразован НЕ в его компьютерный-числовой-адрес (IP адрес), а в адрес, где будет предупреждение о недопустимости его открытия или сообщение, что такой сайт отсутствует в сети.

6. Установить защиту поисковой выдачи. Данный этап защитит ребёнка во время поиска информации. Можно воспользоваться Семейным поиском Яндекс, который фильтрирует поисковые запросы и не выдаёт результаты, не предназначенные ребёнку. Защита основана на том, что по умолчанию все новые открытые вкладки в браузере используют в качестве домашней страницы поисковую систему Яндекс с Семейным фильтром. Вероятнее всего, что ребёнок не будет переходить на другие поисковые системы, а воспользуется уже предложенным с фильтрацией.

7. Установить дополнительные бесплатные или платные контент фильтры. Среди бесплатных программ можно выделить:

- Интернет-цензор
- Веб-фильтр для родителей, предлагаемый лигой безопасного Интернета

Среди платных программ можно выделить:

- Kaspersky safe kids
- Kindergate

8. Для ограничения доступа детей к негативному контенту, в том числе и с мобильных устройств, можно обратиться к вашему провайдеру. Крупные поставщики услуг, такие как МТС, Билайн, Мегафон, Ростелеком, предоставляют услуги детского Интернета.

Список ресурсов, которые помогут защитить детей в Интернете:

http://www.ligainternet.ru/

http://detionline.com/