

Как защитить детей от контентных рисков

Контентные риски

К контентным рискам относятся материалы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие противозаконную, неэтичную и вредоносную информацию. В первую очередь, с таким контентом можно столкнуться на сайтах социальных сетей, в блогах, на торрентах. Но сегодня практически весь интернет - это виртуальное пространство риска. *Противозаконный контент - распространение наркотических веществ через интернет, порнографические материалы с участием несовершеннолетних, призывы к разжиганию национальной розни и экстремистским действиям.

*Вредоносный (опасный) контент - контент, способный нанести прямой вред психическому и физическому здоровью детей и подростков.

*Неэтичный контент - контент, который не запрещен к распространению, но может содержать информацию, способную оскорбить пользователей. Подобное содержимое может распространяться ограниченно (например, "только для взрослых").

Особо опасны сайты, на которых обсуждаются способы причинения боли и вреда, способы чрезмерного похудения, способы самоубийства, сайты, посвященные наркотикам, сайты, на которых размещены полные ненависти сообщения, направленные против отдельных групп или лиц. Столкновения с контентными рисками могут иметь негативные последствия для эмоциональной сферы, психологического развития, социализации, а также физического здоровья детей и подростков.

Основные правила безопасности:

1. Прежде, чем позволить ребенку пользоваться Интернетом, расскажите ему о возможных опасностях Сети (вредоносные программы, небезопасные сайты, интернет-мошенники и др.) и их последствиях.
2. Четко определите время, которое Ваш ребенок может проводить в Интернете, и сайты, которые он может посещать.
3. Убедитесь, что на компьютерах установлены и правильно настроены антивирусные программы, средства фильтрации контента и нежелательных сообщений.
4. Контролируйте деятельность ребенка в Интернете с помощью специального программного обеспечения.
5. Спрашивайте ребенка о том, что он видел и делал в Интернете.
6. Объясните ребенку, что при общении в Интернете (чаты, форумы, сервисы мгновенного обмена сообщениями, онлайн-игры) и других ситуациях, требующих регистрации, нельзя использовать реальное имя. Помогите ему выбрать регистрационное имя, не содержащее никакой личной информации.

7. Объясните ребенку, что нельзя разглашать в Интернете информацию личного характера (номер телефона, домашний адрес, название/номер школы и т.д.), а также "показывать" свои фотографии.

8. Помогите ребенку понять, что далеко не все, что он может прочесть или увидеть в Интернете — правда. Приучите его спрашивать то, в чем он не уверен.

9. Объясните ребенку, что нельзя открывать файлы, полученные от неизвестных пользователей, так как они могут содержать вирусы или фото/видео с негативным содержанием.

10. Приучите ребенка советоваться со взрослыми и немедленно сообщать о появлении нежелательной информации.

11. Не позволяйте Вашему ребенку встречаться с онлайн-знакомыми без Вашего разрешения или в отсутствие взрослого человека.

12. Постараться регулярно проверять список контактов своих детей, чтобы убедиться, что они знают всех, с кем они общаются;

13. Объясните детям, что при общении в Интернете, они должны быть дружелюбными с другими пользователями, ни в коем случае не писать грубых слов — читать грубости также неприятно, как и слышать;

14. Если ребенок пользуется общим компьютером, для каждого члена семьи создайте свою учетную запись на компьютере. Ваша учетная запись должна иметь надежный пароль и обладать правами администратора, чтобы ребенок не мог менять установленные вами настройки и программы;

15. Проверяйте актуальность уже установленных правил. Следите за тем, чтобы Ваши правила соответствовали возрасту и развитию Вашего ребенка.

Важно помнить, что невозможно всегда находиться рядом с детьми и постоянно их контролировать. Доверительные отношения с детьми, открытый и доброжелательный диалог зачастую могут выступать более эффективными средствами для обеспечения безопасности вашего ребенка, чем постоянное отслеживание посещаемых сайтов и блокировка всевозможного контента.