## Классификация рисков

### Коммуникационные риски

Связаны с общением и межличностными отношениями интернет-пользователей. Примерами таких рисков могут быть: кибербуллинг, незаконные контакты (например, сексуальные домогательства), знакомства в сети и встречи с интернет-знакомым.
С коммуникационными рисками можно столкнуться при общении в чатах, онлайн-мессенджерах (ICQ, Skype, MSN), социальных сетях, на сайтах знакомств, форумах, блогах.

### Контентные риски

Это различные материалы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие противозаконную, неэтичную и вредоносную информацию.
Столкнуться с ними можно практически везде: социальные сети, блоги, торренты, персональные сайты, видеохостинги.

### Электронные риски

Вероятность столкнуться с хищением персональной информации или подвергнуться атаке вредоносных программ.Вредоносные программы – различное программное обеспечение (вирусы, черви, «троянские кони», шпионские программы, боты и др.), которое может нанести вред компьютеру и нарушить конфиденциальность хранящейся в нем информации.

### Потребительские риски

Злоупотребление в интернете правами потребителя. Включают в себя: риск приобретения товара низкого качества, различные подделки, контрафактную и фальсифицированную продукцию, потерю денежных средств без приобретения товара или услуги, хищение персональной информации с целью кибермошенничества.

# ГЛОБАЛЬНАЯ СЕТЬ: ПРАВИЛА ПОЛЬЗОВАНИЯ

дети онлайн

8 800 25 000 15

helpline@detionline.com

## РЕКОМЕНДАЦИИ ДЛЯ РОДИТЕЛЕЙ

## 2. КОНТЕНТНЫЕ РИСКИ

www.detionline.com

Факультет психологии МГУ

Фонд развития Интернет

ФИРО

Лига безопасного интернета

МТС

МГТС

## Как помочь ребенку, если он уже столкнулся с какой-либо интернет-угрозой?

1. Установите положительный эмоциональный контакт с ребенком, постарайтесь расположить его к разговору о том, что произошло. Расскажите о своей обеспокоенности тем, что с ним происходит. Ребенок должен вам доверять и понимать, что вы хотите разобраться в ситуации и помочь ему, а не наказать его.
2. Если ребенок расстроен чем-то увиденным (например, кто-то взломал его профиль в социальной сети) или он попал в неприятную ситуацию (потратил деньги в результате интернет-мошенничества и пр.), постарайтесь его успокоить и вместе разберитесь в ситуации. Выясните, что привело к данному результату – непосредственно действия самого ребенка, недостаточность вашего контроля или незнание ребенком правил безопасного поведения в интернете.
3. Если ситуация связана с насилием в интернете в отношении ребенка, то необходимо узнать информацию об обидчике, историю их взаимоотношений, выяснить, существует ли договоренность о встрече в реальной жизни и случались ли подобные встречи раньше, узнать о том, что известно обидчику о ребенке (реальное имя, фамилия, адрес, телефон, номер школы и т. п.). Объясните и обсудите, какой опасности может подвергнуться ребенок при встрече с незнакомцами, особенно без свидетелей.
4. Соберите наиболее полную информацию о происшествии – как со слов ребенка, так и с помощью технических средств. Зайдите на страницы сайта, где был ребенок, посмотрите список его друзей, прочтите сообщения. При необходимости скопируйте и сохраните эту информацию – в дальнейшем это может вам пригодиться для обращения в правоохранительные органы.
5. В случае, если вы не уверены в своей оценке того, насколько серьезно произошедшее с ребенком, или ребенок недостаточно откровенен с вами и не готов идти на контакт, обратитесь к специалисту (телефон доверия, горячая линия и др.), где вам дадут рекомендации и подскажут, куда и в какой форме обратиться по данной проблеме.

## Опыт столкновения школьников с контентными рисками*

- Среди рискованного контента, с которым сталкиваются пользователи, наиболее распространена информация сексуального характера. Каждый второй ребенок 9-16 лет (51%) сталкивался с сексуальными изображениями онлайн или офлайн. Большинство из них (41%) сталкивается с сексуальными изображениями в интернете. Это почти в три раза чаще, чем в Европе.
- Российские школьники в 6 раз чаще, чем европейские, сталкиваются с сексуальными изображениями во всплывающих окнах и значимо чаще - в социальных сетях.
- Каждый четвертый ребенок, столкнувшийся с неприятными сексуальными изображениями в интернете, был сильно или очень сильно расстроен этим. Особенно сильно переживают дети 9-10 лет: каждый второй был сильно расстроен.

| % | Возраст | | | Общий % |
|---|---|---|---|---|
| | 11-12 лет | 13-14 лет | 15-16 лет | |
| Способы причинения себе вреда и боли | 9 | 14 | 11 | 12 |
| Способы совершения самоубийства | 9 | 10 | 11 | 10 |
| Способы чрезмерного похудения | 16 | 26 | 30 | 25 |
| Наркотики, опыт их употребления | 4 | 13 | 13 | 11 |
| Сталкивался с чем-либо из перечисленного | 26 | 37 | 40 | 35 |

- Каждый третий ребенок в возрасте 11-16 лет сталкивался с сайтами, на которых люди обсуждают способы причинения себе боли или вреда, способы чрезмерного похудения, сайты, посвященные наркотикам, а также сайты, на которых описываются способы самоубийства.
- Дети считают, что их сверстников могут расстроить агрессивные видео и фото, сайты, на которых обсуждаются различные способы насилия по отношению к другим и к себе, пропагандируется нездоровый образ жизни, анорексия, наркотики.
- Каждый четвертый ребенок старше 11 лет (независимо от пола) указал, что сталкивался в интернете с сайтами, на которых размещены полные ненависти сообщения, направленные против отдельных групп или лиц.

* результаты исследования "Дети России онлайн"

# 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) контен** – 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 себе боли или вреда, способы чрезмерного похудения, способы самоубийства, сайты, посвященные наркотикам, сайты, на которых размещены полные ненависти сообщения, направленные против отдельных групп или лиц.**

Столкновение с контентными рисками может иметь негативные последствия для эмоциональной сферы, психологического развития, социализации, а также физического здоровья детей и подростков.

дети онлайн

8 800 25 000 15

## Рекомендации по предупреждению контентных рисков

1. Используйте специальные технические средства, чтобы ограничивать доступ ребенка к негативной информации – программы родительского контроля и контентной фильтрации, настройки безопасного поиска. Часто пакет функций родительского контроля уже есть в вашей антивирусной программе.

   Программы родительского контроля позволяют: установить запрет на посещение сайтов различного негативного содержания, сайтов онлайн-знакомств, сайтов с вредоносным содержимым; ограничить время доступа ребенка к интернету; производить мониторинг переписки в социальных сетях и онлайн мессенджерах (чатах); блокировать сомнительные поисковые запросы в поисковых системах; блокировать баннеры; а также отслеживать все действия ребенка в сети.
2. 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.
3. Регулярно следите за активностью вашего ребенка в сети. Просматривайте историю посещений сайтов, чтобы быть уверенным, что среди них нет опасных. При необходимости обновляйте настройки технических средств безопасности.
4. Объясните детям, что далеко не все, что они могут прочесть или увидеть в интернете – правда. Необходимо проверять информацию, увиденную в интернете. Для этого существуют определенные правила проверки достоверности информации. Признаки надежного сайта, информации которого можно доверять, включают: авторство сайта, контактные данные авторов, источники информации, аккуратность представления информации, цель создания сайта, актуальность данных. Расскажите об этих правилах вашим детям.
5. Поддерживайте доверительные отношения с вашим ребенком, чтобы всегда быть в курсе с какой информацией он сталкивается в сети. Попав случайно на какой-либо опасный, но интересный сайт, ребенок может продолжить поиск подобных ресурсов. Важно заметить это как можно раньше и объяснить, ребенку, чем именно ему грозит просмотр подобных сайтов.

**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.**