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.

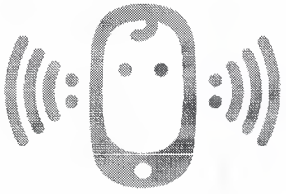
Электронные риски

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

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.

Рекомендации по предотвращению кибербуллинга

1. Объясните детям, что при общении в интернете они должны быть дружелюбными с другими пользователями. Ни в коем случае не стоит писать резкие и оскорбительные слова – читать грубости так же неприятно, как и слышать.
2. Научите детей правильно реагировать на обидные слова или действия других пользователей. Не стоит общаться с агрессором, и тем более пытаться ответить ему тем же. Возможно стоит вообще покинуть данный ресурс и удалить оттуда свою личную информацию, если не получается решить проблему мирным путем. Лучший способ испортить хулигану его выходку – отвечать ему полным игнорированием.
3. Обратите внимание на психологические особенности вашего ребенка. Специалисты выделяют характерные черты, типичные для жертв буллинга, они часто бывают:
   - пугливы, чувствительны, замкнуты и застенчивы
   - тревожны, неуверены в себе, несчастны
   - склонны к депрессии и чаще своих ровесников думают о самоубийстве
   - не имеют ни одного близкого друга и успешнее общаются с взрослыми, нежели со сверстниками.
   - если это мальчики, они могут быть физически слабее своих ровесников.
4. Если у вас есть информация, что кто-то из друзей или знакомых вашего ребенка подвергается буллингу или кибербуллингу, то сообщите об этом классному руководителю или школьному психологу – необходимо принять меры по защите ребенка.
5. Объясните детям, что личная информация, которую они выкладывают в интернете (домашний адрес, номер мобильного или домашнего телефона, адрес электронной почты, личные фотографии) может быть использована агрессорами против них.
6. Помогите ребенку найти выход из ситуации – практически на всех форумах и сайтах есть возможность заблокировать обидчика, написать жалобу модератору или администрации сайта, потребовать удаление странички.
7. Поддерживайте доверительные отношения с вашим ребенком, чтобы вовремя заметить, если в его адрес начнет поступать агрессия или угрозы. Наблюдайте за его настроением во время и после общения с кем-либо в интернете.
8. Убедитесь, что оскорбления (буллинг) из сети не перешли в реальную жизнь. Если поступающие угрозы являются достаточно серьезными, касаются жизни или здоровья ребенка, а также членов вашей семьи, то вы имеете право на защиту со стороны правоохранительных органов, а действия обидчиков могут попадать под статьи действия уголовного и административного кодексов о правонарушениях

Коммуникационные риски

Связаны с общением и межличностными отношениями интернет-пользователей. Примерами таких рисков могут быть: кибербуллинг, незаконные контакты (например, груминг), знакомства в сети и встречи с интернет-знакомыми и др.

С коммуникационными рисками можно столкнуться при общении в чатах, онлайн-мессенджерах (ICQ, Skype, MSN и др.), социальных сетях, на сайтах знакомств, форумах, блогах и т.д.

Кибербуллинг

Агрессивное, умышленное действие, совершаемое группой лиц или одним лицом с использованием электронных форм контакта, повторяющееся неоднократно и продолжительное во времени в отношении жертвы, которой трудно защитить себя.

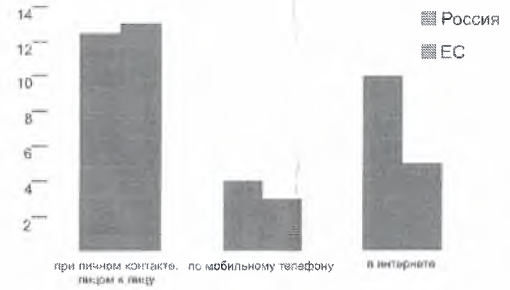
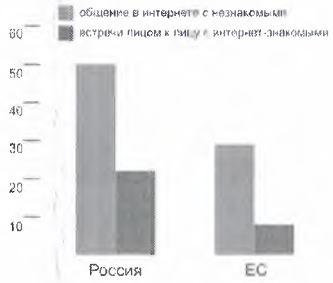


Рис.1. Где дети становятся жертвами буллинга?*

Знакомства в интернете и встречи с незнакомцами

Общаясь в сети, дети могут знакомиться, общаться и добавлять в «друзья» совершенно неизвестных им в реальной жизни людей. В таких ситуациях есть опасность разглашения ребенком личной информации о себе и своей семье. Также юный пользователь рискует подвергнуться оскорблениям, запугиванию и домогательствам.

Особенно опасным может стать груминг – установление дружеских отношений с ребенком с целью личной встречи, вступления с ним в сексуальные отношения, шантажа и эксплуатации.



* результаты исследования "Дети России онлайн"

Рекомендации по предупреждению встреч с незнакомцами и груминга

1. Поддерживайте доверительные отношения с вашим ребенком, чтобы всегда быть в курсе, с кем ребенок общается в сети. Обратите внимание, кого ребенок добавляет к себе «в друзья», с кем предпочитает общаться в сети – с ровесниками или людьми старше себя.
2. Объясните ребенку, что нельзя разглашать в интернете информацию личного характера (номер телефона, домашний адрес, название/номер школы и т.д.), а также пересылать виртуальным знакомым свои фотографии или видео.
3. Объясните ребенку, что нельзя ставить на аватарку или размещать в сети фотографии, по которым можно судить о материальном благополучии семьи, а также нехорошо ставить на аватарку фотографии других людей без их разрешения.
4. Объясните ребенку, что при общении на ресурсах, требующих регистрации (в чатах, на форумах, через сервисы мгновенного обмена сообщениями, в онлайн-играх), лучше не использовать реальное имя. Помогите ему выбрать ник, не содержащий никакой личной информации.
5. Объясните ребенку опасность встречи с незнакомыми людьми из интернета. В сети человек может представиться кем угодно, поэтому на реальную встречу с интернет-другом надо обязательно ходить в сопровождении взрослых.
6. Детский познавательный интерес к теме сексуальных отношений между мужчиной и женщиной может активно эксплуатироваться злоумышленниками в интернете. Постарайтесь сами поговорить с ребенком на эту тему. Объясните ему, что нормальные отношения между людьми связаны с доверием, ответственностью и заботой, но в интернете тема любви часто представляется в неправильной, вульгарной форме. Важно, чтобы ребенок был вовлечен в любимое дело, увлекался занятиями, соответствующими его возрасту, которым он может посвящать свободное время

дети онлайн

8 800 25 000 15

Мессенджеры

Мессенджер (IM = Instant **Messenger**) - **это** программа, мобильное приложение или веб-сервис для мгновенного обмена сообщениями

Мессенджер Вотсап (WhatsApp).

Мессенджер Вотсап позволяет людям связываться на расстоянии, причем абсолютно бесплатно (трафик интернета, в случае подключения через мобильную сеть, оплачивается согласно тарифу, никаких наценок). Возможно ведение переписок, отправление голосовых сообщений, мультимедийной информации, а также вызовы, в том числе и видеосвязь. Сообщения в чате можно украсить с помощью смайликов, дополнить геолокацией или аудиопояснением.

Для установки приложения необходимо зайти в App Store или Play Market, набрать в поиске WhatsApp и загрузить нужный элемент.

Мессенджер Вайбер (Viber)

Вайбер – это уникальное приложение, которое позволяет поддерживать связь с родными и друзьями. Приложение является бесплатным. Единственным условием является наличие интернета и установленной программы на телефоне или компьютере. Передача трафика происходит при помощи GPRS. Если подключиться к интернету по Wi-Fi, то платить ни за что не придётся.

Установку Вайбер можно произвести в магазине приложений на вашем смартфоне. Также скачать программу можно с официального сайта. После того, как приложение скачается, оно автоматически запустится.

При желании вы можете использовать **Вайбер на компьютере**. Вначале приложение устанавливается на смартфоне, а уже после на компьютере. Для того чтобы использовать программу на ПК, необходимо ввести зарегистрированный в системе номер телефона, а после активировать его с помощью кода подтверждения, который приходит на смартфон.

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)

ЕДИНЫЙ РЕЕСТР доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено http://zapret-info.gov.ru.

Сайт обеспечивает: получение ответа, находится ли запрошенный сайт либо какие-либо страницы сайта в реестре; подачу сообщения о сайте, содержащем запрещённую информацию, для последующего включения ресурса в реестр.

Рекомендации родителям по защите детей от информации, причиняющей вред их здоровью и развитию, в сети Интернет

Интернет – это мир интересных и полезных возможностей, но в то же время это источник информации наносящей вред здоровью, нравственному и духовному развитию, особенно для ребенка. Агрессия, преследования, мошенничество, психологическое давление, общение с онлайн незнакомцами – это лишь некоторый перечень угроз, которые поджидают ребенка в глобальной сети каждый день.

Россия вошла в зону повышенного риска по обеспечению безопасности детей в глобальной сети. Это обуславливается высокой пользовательской Интернет-активностью российских школьников и высоким уровнем ее бесконтрольности, а также низкими знаниями родителей об опасностях Интернет-среды.

Как же оградить от них ребенка?

- Самый главный совет для родителей – будьте осведомлены о деятельности ребенка.

- Говорите с ним об Интернете: спрашивайте, что он сегодня делал, с кем познакомился, что интересного узнал.

- Старайтесь регулярно просматривать ресурсы, которые посещает Ваш ребенок, и проверяйте список его контактов, чтобы убедиться, что он и Вы знаете всех, с кем общается.

- Попросите ребенка сообщать Вам или близким людям о любых угрозах или тревогах, связанных с Интернет, и не ругайте за неприятные случаи, иначе он все будет скрывать.

- Второе важное правило – станьте проводником ребенка в Интернет.

- Научите ребенка правильно искать нужную информацию, сформируйте список полезных, интересных, безопасных для детей ресурсов и посоветуйте правильно их использовать.

- С самого начала объясните ребенку, почему ни в коем случае не стоит выдавать данные о себе и своей семье, публиковать фотографии, где изображен сам ребенок, семья, школа и прочие данные.

- Научите вашего ребенка уважению и этикету в Интернете.

- По статистике, более 80% российских детей имеют профиль в социальных сетях, а 23% сталкиваются в Сети с агрессией и унижением. Попросите ребенка не провоцировать конфликтные ситуации и относиться к другим так же, как он хотел бы, чтобы относились к нему самому.

- Объясните, что ни при каких обстоятельствах не стоит размещать провокационный материал и не распространять по чьей-либо просьбе информационные и агрессивно-настроенные сообщения.

- Информация, выложенная в Интернет – доступна всем и может быть использована в любых, в том числе, мошеннических целях.

- Предупредите ребенка, что не стоит добавлять «в друзья» незнакомых людей - они могут быть не теми, за кого себя выдают.

- Ни в коем случае не соглашался на «живые» встречи с Интернет-незнакомцами, прежде чем не поставит в курс вас или близких родственников.

- Посоветуйте ему общаться в Интернете с теми, с кем он лично знаком.

- Предостерегите от скачивания платной информации, особенно через sms.

- Используйте технические возможности Вашего компьютера и Оператора.

- Для предотвращения нежелательного контента и вирусов необходимо установить антивирус, настроить антиспам фильтры в почте.

- С помощью средств Родительского контроля или соответствующих услуг Оператора можно создавать «белый» список Интернет-сайтов, ограничить время пребывания ребенка в Интернет, настроить возрастной фильтр.

Что делать, если ребенок уже столкнулся с какой-либо интернет-угрозой

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, но ни в коем случае не наказать.

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.

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.

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.

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.

Горячие телефоны

В России действует бесплатная всероссийская служба телефонного и онлайн консультирования для детей и взрослых по проблемам безопасного использования интернета и мобильной связи:

Линия помощи "Дети онлайн" (8-800-25-000-15)

Центр безопасного интернета 8-800-200-24-00