Глобальная сеть: правила пользования

Как защитить ребенка от столкновения с вредоносной информацией в сети?
Как научить его справляться с последствиями таких встреч?
Рекомендации для родителей

Контентные риски

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 и др. - фактически все, что сейчас существует в сети интернет – это виртуальное пространство риска.

Такой контент может быть:

- **противозаконным** – например, распространение наркотических веществ через интернет, порнографические материалы с участием несовершеннолетних, призывы к разжиганию национальной розни и экстремистским действиям;
- **неэтичным** – данный контент не запрещен к распространению, но может содержать информацию, способную оскорбить пользователей. Подобное содержимое может распространяться ограниченно (например, «только для взрослых»);
- **вредоносным** – такой контент может нанести прямой вред психическому и физическому здоровью детей и подростков;

В интернете дети и подростки могут столкнуться с шокирующей информацией. Это могут быть сайты, на которых люди обсуждают **способы причинения себе боли или вреда, способы чрезмерного похудения, сайты, посвященные наркотикам, и даже сайты, на которых описываются способы самоубийства**.

Более 40% детей в России сталкиваются с **изображениями сексуального характера** в интернете или других источниках. И каждый шестой из этих детей видит сексуальные изображения ежедневно или почти ежедневно, каждый пятый – систематически: 1-2 раза в неделю.

На вопрос, что может расстроить их сверстников в сети, многие дети называли 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.**

Около 35% опрошенных детей в возрасте 11-16 лет сталкивались 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.

В то же время данные исследования показывают, что около половины детей не умеют оценивать сайты с точки зрения достоверности информации, чуть меньше половины не умеют удалять историю своих действий на компьютере и блокировать спам.

Рекомендации для родителей по предупреждению контентных рисков:

1. Установите на компьютер специальные программные фильтры, которые могут блокировать всплывающие окна и сайты с определенной тематикой. Почти каждый интернет-браузер обладает настройками безопасности: какой контент должен быть заблокирован, а какой можно загружать на компьютер. Настройки браузера устанавливаются бесплатно. На сайте каждого разработчика можно найти подобную информацию в разделе «Безопасность». Специальные программы, называемые системами родительского контроля, позволяют родителям самим решать, какое содержимое в интернете могут просматривать их дети, отсекать «плохие» сайты в соответствии с введенными настройками. Такие программы позволяют смотреть отчеты о том, какие сайты посещал ребенок, сколько времени пользовался интернетом, устанавливать ограничения пользования компьютером и интернетом по времени.
2. Создайте на компьютере несколько учетных записей, когда каждый пользователь сможет входить в систему независимо и иметь собственный уникальный профиль. Учетная запись администратора позволяет контролировать системные настройки и устанавливать новое программное обеспечение, ограничивая в таких правах других пользователей компьютера. Создавайте для работы надежные и защищенные пароли.
3. 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 с большой вероятностью из любопытства захочет познакомиться и с другими подобными ресурсами. Важно заметить это как можно раньше и объяснить, ребенку, чем именно ему грозит

просмотр подобных сайтов, а также обновить настройки безопасности браузера или программного фильтра.

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. Помните, что невозможно всегда находиться рядом с детьми и постоянно их контролировать. Доверительные отношения с детьми, открытый и доброжелательный диалог зачастую может быть гораздо конструктивнее, чем постоянное отслеживания посещаемых сайтов и блокировка всевозможного контента.

Коммуникационные риски

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. Английское слово буллинг (bullying, от bully – драчун, задира, грубиян, насильник) обозначает запугивание, унижение, травлю, физический или психологический террор, направленный на то, чтобы вызвать у другого страх и тем самым подчинить его себе. По данным, полученным в исследовании «Дети России онлайн», в среднем по РФ 23% детей, которые пользуются интернетом, являются жертвой буллинга онлайн или офлайн

Новые инфокоммуникационные технологии предоставляют дополнительные возможности для буллинга, и российские дети этим пользуются. Если сравнить виртуальность и реальность, то российские дети подвергаются буллингу в интернете так же часто, как и в реальной жизни. Оскорбления в чатах, на форумах, в блогах и в комментариях к ним, поддельные страницы или видеоролики, на которых над кем-то издеваются или даже избивают уже давно стали привычной частью Рунета – каждый десятый ребенок 9-16 лет становился жертвой кибербуллинга.

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.

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. Такие знакомства чаще всего происходят в чате, на форуме или в социальной сети. Общаясь лично («в привате»), злоумышленник, чаще всего представляясь сверстником, входит в доверие к ребенку, а затем пытается узнать личную информацию (адрес, телефон и др.) и договориться о встрече. Иногда такие люди выманивают у детей информацию, которой потом могут шантажировать ребенка, например, просят прислать личные фотографии или провоцируют на непристойные действия перед веб-камерой.

В целом в России за последний год 28% подростков 11-16 лет получали или просматривали сообщения сексуального характера, причем более 10% - раз в месяц и чаще. Эти сообщения могли быть разного характера: подростки могли сами обмениваться неприличными картинками и видео, а некоторые могли подвергаться сексуальному домогательству (грумингу).

Рекомендации по предупреждению встречи 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.

Электронные риски

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. Подобные программы чаще всего снижают скорость обмена данными с интернетом, а также могут использовать ваш компьютер для распространения своих копий на другие компьютеры, рассылать от вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети. Вредоносное программное обеспечение использует множество методов для распространения и проникновения в компьютеры, не только через внешние носители информации (компакт-диски, флешки и т.д.), но и через электронную почту посредством спама или скачанных из интернета файлов.

Заражение компьютера в интернете вирусом – одна из наиболее частых жалоб: с данной проблемой сталкивалась в течение года почти половина (48%)

опрошенных детей 11-16 лет. Она актуальна для всех детей, вне зависимости от пола или возраста. Ситуации, когда личные данные ребенка используются другими людьми, когда ребенок становится жертвой мошенничества в сети, когда другие люди неправомерно используют личную информацию о нем или кто-то использует его пароль, в России происходят значительно чаще, чем в Европе (рис.13).

Рекомендации по предупреждение столкновения с вредоносными программами:

1. Установите на все домашние компьютеры антивирусные программы и специальные почтовые фильтры для предотвращения заражения компьютера и потери ваших данных. Подобные программы наблюдают за трафиком и могут остановить как прямые атаки злоумышленников, так и атаки, использующие вредоносные приложения.
2. Используйте только лицензионные программы и данные, полученные из надежных источников. Чаще всего вирусами бывают заражены пиратские копии программ, особенно компьютерные игры.
3. Никогда не открывайте вложения, присланные с подозрительных и неизвестных вам адресов.
4. Следите за тем, чтобы ваш антивирус регулярно обновлялся, и раз в неделю проверяйте компьютер на вирусы.
5. Регулярно делайте резервную копию важных данных, а также научите это делать ваших детей.
6. Старайтесь периодически менять пароли (например, от электронной почты, от профилей в социальных сетях), но не используйте слишком простые пароли, которые можно легко взломать (даты рождения, номера телефонов и т.п).
7. Расскажите ребенку, что нельзя рассказывать никакие пароли своим друзьям и знакомым. Если пароль стал кому-либо известен, то его необходимо срочно поменять.
8. Расскажите ребенку, что если он пользуется интернетом с помощью чужого устройства, он должен не забывать выходить из своего аккаунта в социальной сети, в почте и на других сайтах после завершения работы. Никогда не следует сохранять на чужом компьютере свои пароли, личные файлы, историю переписки – по этой информации злоумышленники могут многое узнать о вашем ребенке.

Потребительские риски

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 и др. **Кибермошенничество** – один из видов киберпреступлений, целью которого является причинение материального или иного ущерба путем хищения личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.).

Основной процент обращений на Линию помощи «Дети онлайн» по потребительским рискам составляют неудачные покупки, когда пользователь при заказе через интернет приобретает некачественный товар или не получает его вообще. На втором месте – обращения по поводу потери денежных средств при использовании интернета для перевода денег или оплаты счетов. Часть обращений связаны с нарушением авторских прав пользователей (размещение материалов в интернете без согласия автора). (см. Рис. 7)

Рекомендации по предупреждение кибермошенничества:

1. Проинформируйте ребенка о самых распространенных методах мошенничества в сети. Всегда совместно принимайте решение о том, стоит ли воспользоваться теми или иными услугами, предлагаемыми в интернете.
2. Не оставляйте в свободном для ребенка доступе банковские карты и платежные данные, воспользовавшись которыми ребенок может самостоятельно совершать покупки.
3. Не отправляйте о себе слишком много информации при совершении интернет-покупок: данные счетов, пароли, домашние адреса и телефоны. Помните, что никогда администратор или модератор сайта не потребует полные данные вашего счета, пароли и пин-коды. Если кто-то запрашивает подобные данные, будьте бдительны – скорее всего, это мошенники.
4. Установите на свои компьютеры антивирус или персональный брандмауэр. Подобные приложения наблюдают за трафиком и могут предотвратить кражу конфиденциальных данных или другие подобные действия.
5. Убедитесь в безопасности сайта, на котором Вы или Ваш ребенок планируете совершить покупку:
    - Ознакомьтесь с отзывами покупателей.
    - Избегайте предоплаты.

- Проверьте реквизиты и название юридического лица – владельца магазина.
- Уточните, как долго существует магазин. Посмотреть можно в поисковике или по дате регистрации домена (сервис Whois).
- Поинтересуйтесь возможностью получения кассового чека и других документов за покупку.
- Сравните цены в различных интернет-магазинах.
- Позвоните в справочную магазина.
- Обратите внимание на правила интернет-магазина.
- Выясните, сколько точно вам придется заплатить.

Интернет-зависимость

Интернет-зависимость – навязчивое желание войти в интернет, находясь офлайн и неспособность выйти из интернета, будучи онлайн. (Гриффит В., 1996). По своим проявлениям она схожа с уже известными формами аддиктивного поведения (например, в результате употребления алкоголя или наркотиков), но относится к типу нехимических зависимостей, то есть не приводящих непосредственно к разрушению организма. По своим симптомам интернет-зависимость ближе к зависимости от азартных игр; для этого состояния характерны следующие признаки: потеря ощущения времени, невозможность остановиться, отрыв от реальности, эйфория при нахождении за компьютером, досада и раздражение при невозможности выйти в интернет.

В случае интернет-зависимости выделяют следующие типы онлайн-активности:

✓ Навязчивый веб-серфинг – бесконечные путешествия по всемирной паутине, поиск информации

✓ Пристрастие к виртуальному общению и виртуальным знакомствам (большие объемы переписки, постоянное участие в чатах, веб-форумах, избыточность знакомых и друзей в сети)

✓ Игровая зависимость – навязчивое увлечение компьютерными играми по сети

✓ Навязчивое желание потратить деньги – игра по сети в азартные игры, ненужные покупки в интернет-магазинах или постоянное участие в интернет-аукционах

✓ Пристрастие к просмотру фильмов через интернет

✓ Киберсексуальная зависимость – навязчивое влечение к посещению порносайтов и занятию киберсексом

Исследователи отмечают, что большая часть Интернет-зависимых (91 %) пользуется сервисами Интернета, связанными с общением. Другую часть зависимых (9%) привлекают информационные сервисы сети.

Рекомендации по предупреждению интернет-зависимости

В первую очередь необходимо обратить внимание на возможные признаки интернет-зависимости у вашего ребенка.

1. Оцените, сколько времени ваш ребенок проводит в сети, не пренебрегает ли он из-за работы за компьютером своими домашними обязанностями, выполнением уроков, сном, полноценным питанием, прогулками.
2. Поговорите с ребенком о том, чем он занимается в интернете. Социальные сети создают иллюзию полной занятости – чем больше ребенок общается, тем больше у него друзей, тем больший объем информации ему нужно охватить – ответить на все сообщения, проследить за всеми событиями, показать себя. Выясните, поддерживается ли интерес вашего ребенка реальными увлечениями, или же он просто старается ничего не пропустить и следит за обновлениями ради самого процесса. Постарайтесь узнать, насколько важно для ребенка общение в сети и не заменяет ли оно реальное общение с друзьями.
3. Понаблюдайте за сменой настроения и поведения вашего ребенка после выхода из интернета. Возможно проявление таких психических симптомов как подавленность, раздражительность, беспокойство, нежелание общаться. Из числа физических симптомов можно выделить: головные боли, боли в спине, расстройства сна, снижение физической активности, потеря аппетита и другие.
4. Поговорите со школьным психологом и классным руководителем о поведении вашего ребенка, его успеваемости и отношениях с другими учениками. Настораживающими факторами являются замкнутость, скрытность, нежелание идти на контакт. Узнайте, нет ли у вашего ребенка навязчивого стремления выйти в интернет с помощью телефона или иных мобильных устройств во время урока.

Если вы обнаружили возможные симптомы интернет-зависимости у своего ребенка, необходимо придерживаться следующего алгоритма действий:

1. Постарайтесь наладить контакт с ребенком. Узнайте, что ему интересно, что его беспокоит и т.д.

2. Не запрещайте ребенку пользоваться интернетом, но постарайтесь установить регламент пользования (количество времени, которые ребенок может проводить онлайн, запрет на сеть до выполнения домашних уроков и пр.). Для этого можно использовать специальные программы родительского контроля, ограничивающие время в сети.

3. Ограничьте возможность доступа к интернету только своим компьютером или компьютером, находящимся в общей комнате – это позволит легче контролировать деятельность ребенка в сети. Следите за тем, какие сайты посещает Ваш ребенок.

4. Попросите ребенка в течение недели подробно записывать, на что тратится время, проводимое в интернете. Это поможет наглядно увидеть и осознать проблему, а также избавиться от некоторых навязчивых действий – например, от бездумного обновления странички в ожидании новых сообщений.

5. Предложите своему ребенку заняться чем-то вместе, постарайтесь его чем-то увлечь. Попробуйте перенести кибердеятельность в реальную жизнь. Например, для многих компьютерных игр существуют аналогичные настольные игры, в которые можно играть всей семьей или с друзьями – при этом общаясь друг с другом «вживую». Важно, чтобы у ребенка были не связанные с интернетом увлечения, которым он мог бы посвящать свое свободное время.

6. Дети с интернет-зависимостью субъективно ощущают невозможность обходиться без сети. Постарайтесь тактично поговорить об этом с ребенком. При случае обсудите с ним ситуацию, когда в силу каких-то причин он был вынужден обходиться без интернета. Важно, чтобы ребенок понял – ничего не произойдет, если он на некоторое время «выпадет» из жизни интернет-сообщества.

7. В случае серьезных проблем обратитесь за помощью к специалисту.

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, но ни в коем случае не наказать.

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.