1927

Информационная безопасность детей в Интернете

Лебедева Л.Г.,
заместитель директора по ИКТ

2022

ГБОУ лицей № 384 Кировского района Санкт-Петербурга

Общие сведения

По последним данным, в России: средний возраст начала самостоятельной работы в Сети - 10 лет и сегодня наблюдается тенденция к снижению возраста до 9 лет;

30% несовершеннолетних проводят в Сети более 3 часов в день (при норме 2 часа в неделю!)

Согласно ст. 5 ФЗ от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», к информации, запрещенной для распространения среди детей, относится информация:

1) побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;

2) способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;

3) обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия ;

4) отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;

5) оправдывающая противоправное поведение;

6) содержащая нецензурную брань;

7) содержащая информацию порнографического характера

Что смотрят и слушают наши дети

Источник: Концепция информационной безопасности детей

В России происходит процесс **вестернизации медиапотребления** среди детей и подростков из-за недостатка качественного отечественного контента

По данным анализа медиапотребления детей и подростков

«**Более трети** детей 9-16 лет сталкивались в сети с материалами **сексуального характера**»

«**Каждый второй** ребёнок 11-16 лет сталкивался в интернете с **угрозами** физическому здоровью, пропагандой **насилия** и расовой **ненависти**»

«**Треть** российских школьников **получали лично** сообщения сексуального характера в Интернете, >15% - раз в месяц и чаще»

«**Каждый десятый** ребёнок подвергался **кибербуллингу** (виртуальной травле, опасной агрессии киберсреды)»

Что смотрят и слушают наши дети

Больше половины пользователей сети в возрасте до 14 лет просматривают сайты с нежелательным содержимым.

39% детей посещают порносайты,

19% наблюдают сцены насилия,

16% увлекаются азартными играми.

14% детей интересуются наркотическими веществами и алкоголем,

11% посещают экстремистские и националистические ресурсы

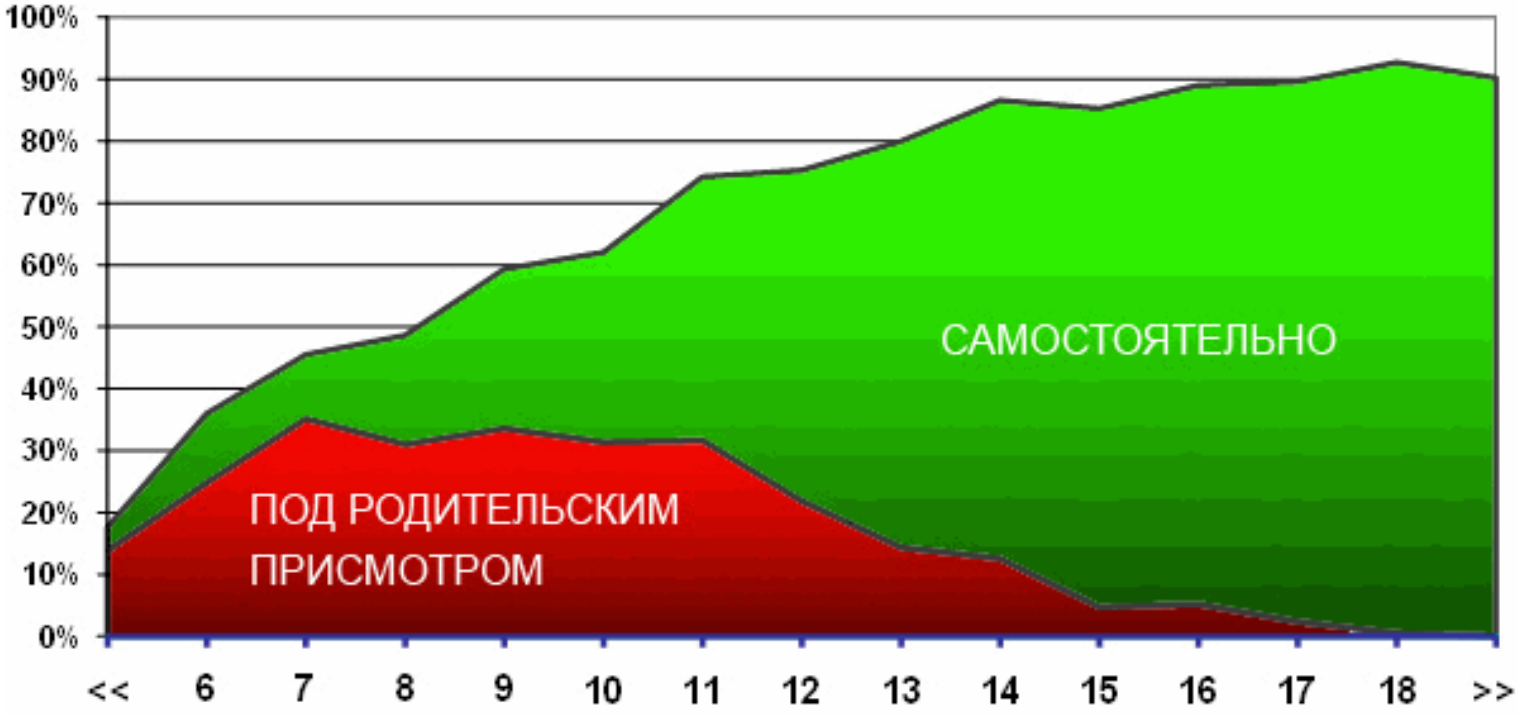
Что смотрят и слушают наши дети

Исследования показали:
90% детей сталкивались в сети с порнографией;
65% искали ее целенаправленно;
44% несовершеннолетних пользователей Интернета хотя бы раз подвергались в сети сексуальным домогательствам.

Что смотрят и слушают наши дети

Среди несовершеннолетних популярны следующие виды и формы онлайн-развлечений:

- ✓ социальных сетей;
- ✓ сетевые игры;
- ✓ просмотр и скачивание фильмов, клипов, аудиофайлов, программ;
- ✓ обмен файлами.



По результатам социологических исследований:
88% 4-летних детей выходят в сеть вместе с родителями.
В **8-9-летнем** возрасте дети всё чаще выходят в сеть самостоятельно.
К **14 годам** совместное, семейное пользование сетью сохраняется лишь для **7%** подростков.

Классификация Интернет-угроз

Электронная безопасность

Риски, этого типа относятся к различной кибердеятельности, которая включает в себя: разглашение персональной информации, выход в сеть с домашнего компьютера с низким уровнем защиты (риск подвергнуться вирусной атаке), онлайн-мошенничество и спам.

Вредоносные программы

Программы, негативно воздействующие на работу компьютера. К ним относятся вирусы, программы-шпионы, нежелательное рекламное программное обеспечение и различные формы вредоносных кодов.

Спам

Нежелательные электронные письма, содержащие рекламные материалы. Спам дорого обходится, так как пользователь тратит на получение большего количества писем свое время и оплаченный интернет-трафик. Также нежелательная почта может содержать вредоносные программы.

Классификация Интернет-угроз

Кибермошенничество

Один из видов киберпреступлений. Хищение конфиденциальных данных позволяет преступнику использовать личную информацию пользователя с целью получить материальную прибыль. Есть несколько видов кибермошенничества: нигерийские письма, фишинг, вишинг и фарминг.

Контентные риски

Контентные риски связаны с потреблением информации, которая публикуется в интернете и включает в себя незаконный и непредназначенный для детей контент. Неподобающий контент включает в себя материалы, содержащие: насилие, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр и наркотических веществ.

Классификация Интернет-угроз

Коммуникационные риски

Связаны с межличностными отношениями интернет-пользователей и включают в себя контакты педофилов с детьми и киберпреследования.

Незаконный контакт

Незаконный контакт - это общение между взрослым и ребенком, при котором взрослый пытается установить более близкие отношения для сексуальной эксплуатации ребенка.

Киберпреследование

Преследование человека сообщениями, содержащими оскорбления, агрессию, сексуальные домогательства с помощью интернет-коммуникаций. Также, может принимать такие формы, как обмен информацией, контактами или изображениями, запугивание, подражание, хулиганство (интернет-троллинг) и социальное бойкотирование.

Последствия бесконтрольного доступа в Интернет

Отказываться от благ Интернета бессмысленно, но бесконтрольный доступ детей к Интернету может привести к:

- Киберзависимости
- Заражению вредоносными программами при скачивании файлов
- Нарушению нормального развития ребенка
- Неправильному формированию нравственных ценностей
- Знакомству с человеком с недобрыми намерениями

Как защитить ребенка от нежелательного контента в Интернет

- ✓ Приучите ребенка советоваться со взрослыми и немедленно сообщать о появлении нежелательной информации подобного рода;
- ✓ Объясните детям, что далеко не все, что они могут прочесть или увидеть в Интернете – правда. Приучите их спрашивать о том, в чем они не уверены;
- ✓ Старайтесь спрашивать ребенка об увиденном в Интернете. Зачастую, открыв один сайт, ребенок захочет познакомиться и с другими подобными ресурсами.

Как научить ребенка быть осторожным при знакомстве с новыми людьми в Интернете

Общение в Интернете может повлечь за собой **коммуникационные риски**, такие как незаконные контакты (например, груминг), киберпреследования, кибербуллинг и др.

Злоумышленники обманом заставляют детей выдать личные данные, такие как домашний адрес, телефон, пароли к персональным страницам в Интернете и др. В других случаях они могут оказаться преступниками в поисках жертвы.

Специалисты используют специальный термин «груминг», обозначающий установление дружеских отношений с ребенком с целью вступления в сексуальный контакт. Знакомство чаще всего происходит в чате, на форуме или в социальной сети от имени ровесника ребенка. Общаясь лично («в привате»), злоумышленник входит в доверие к ребенку, пытается узнать личную информацию и договориться о встрече.

Как научить ребенка быть осторожным при знакомстве с новыми людьми в Интернете

Предупреждение груминга:

- Будьте в курсе, с кем контактирует в Интернете ваш ребенок, старайтесь регулярно проверять список контактов своих детей, чтобы убедиться, что они лично знают всех, с кем они общаются;
- Объясните ребенку, что нельзя разглашать в Интернете информацию личного характера (номер телефона, домашний адрес, название/номер школы и т.д.), а также пересылать интернет-знакомым свои фотографии;
- Если ребенок интересуется контактами с людьми намного старше его, следует провести разъяснительную беседу;
- Не позволяйте Вашему ребенку встречаться с онлайн-знакомыми без Вашего разрешения или в отсутствии взрослого человека. Если ребенок желает встретиться с новым интернет-другом, следует настоять на сопровождении ребенка на эту встречу;
- Интересуйтесь тем, куда и с кем ходит ваш ребенок.

Как избежать кибербуллинга

Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

Предупреждение кибербуллинга:

- 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;
- Научите детей правильно реагировать на обидные слова или действия других пользователей;
- Объясните детям, что нельзя использовать Сеть для хулиганства, распространения сплетен или угроз;
- Старайтесь следить за тем, что Ваш ребенок делает в Интернете, а также следите за его настроением после пользования Сетью.

Признаки в поведении, свидетельствующие, что ребенок стал жертвой кибербуллинга

- **Беспокойное поведение**

Депрессия и нежелание идти в школу – самые явные признаки того, что ребенок подвергается агрессии.

- **Неприязнь к Интернету**

Если ребенок любил проводить время в Интернете и внезапно перестал это делать, следует выяснить причину. В большинстве случаев внезапное нежелание пользоваться Интернетом связано с проблемами в виртуальном мире.

- **Нервозность при получении новых сообщений**

Негативная реакция ребенка на звук письма на электронную почту должна насторожить родителя.

Как научить ребенка не стать жертвой интернет-мошенников

Кибермошенничество — один из видов киберпреступления, целью которого является обман пользователей: незаконное получение доступа либо хищение личной информации (номера банковских счетов, паспортные данные, коды, пароли и др.), с целью причинить материальный или иной ущерб

Предупреждение кибермошенничества:

- Проинформируйте ребенка о самых распространенных методах мошенничества и научите его советоваться со взрослыми перед тем, как воспользоваться теми или иными услугами в Интернете;
- Установите на свои компьютеры антивирус или, например, персональный брандмауэр. Эти приложения наблюдают за трафиком и могут быть использованы для выполнения множества действий на зараженных системах, наиболее частым из которых является кража конфиденциальных данных.

Безопасное совершение покупок в Интернет-магазинах

- Прежде чем совершить покупку в интернет-магазине, удостоверьтесь в его надежности;
- Необходимо вместе с ребенком познакомиться с отзывами покупателей;
- 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, выдает ли магазин кассовый чек
- Сравните цены в разных интернет-магазинах
- Позвоните в справочную магазина
- Обратите внимание на правила интернет-магазина
- Выясните, сколько точно вам придется заплатить

Как распознать интернет-и игровую зависимость

Сегодня в России все более актуальны проблемы так называемой «интернет-зависимости».

Согласно исследованиям Кимберли Янг, предвестниками интернет-зависимости являются:

навязчивое стремление постоянно проверять электронную почту;

предвкушение следующего сеанса онлайн;

увеличение времени, проводимого онлайн;

увеличение количества денег, расходуемых онлайн.

Если Вы считаете, что Ваши близкие, в том числе дети, страдают от чрезмерной увлеченности компьютером, это наносит вред их здоровью, учебе, отношениям в обществе, приводит к сильным конфликтам в семье, то Вы можете обратиться к специалистам, занимающимся этой проблемой.

Пять правил безопасного пользования электронной почтой:

- Никогда не открывайте подозрительные сообщения или вложения электронной почты, полученные от незнакомых людей. Вместо этого сразу удалите их, выбрав команду в меню сообщений.
- Никогда не отвечайте на спам.
- Применяйте фильтр спама поставщика услуг Интернета или программы работы с электронной почтой (при наличии подключения к Интернету).
- Создайте новый или используйте семейный адрес электронной почты для Интернет-запросов, дискуссионных форумов и т.д.
- Никогда не пересылайте «письма счастья». Вместо этого сразу удаляйте их.

Общие рекомендации по обеспечению безопасности детей и подростков в Интернете

Расположите компьютер вашего ребенка в месте общей доступности: столовой или гостиной. Так вам будет проще уследить за тем, что делают дети в Интернете.

Следите, какие сайты посещают ваши дети. Если у вас маленькие дети, знакомьтесь с Интернетом вместе. Если у вас дети постарше, поговорите с ними о сайтах, которые они посещают, и обсудите, что допустимо, а что недопустимо в вашей семье. Список сайтов, которые посещает ваш ребенок, можно найти в истории браузера. Кроме того, вы можете воспользоваться инструментами блокировки нежелательного контента.

Общие рекомендации по обеспечению безопасности детей и подростков в Интернете

Расскажите детям о безопасности в Интернете. Вы не сможете все время следить за тем, что ваши дети делают в Сети. Им необходимо научиться самостоятельно пользоваться Интернетом безопасным и ответственным образом.

Установите защиту от вирусов. Используйте и регулярно обновляйте антивирусное ПО. Научите детей не загружать файлы с файлообменных сайтов, а также не принимать файлы и не загружать вложения, содержащиеся в электронных письмах от незнакомых людей.

Общие рекомендации по обеспечению безопасности детей и подростков в Интернете

Научите детей ответственному поведению в Интернете.

Помните золотое правило: то, что вы не сказали бы человеку в лицо, не стоит отправлять ему по электронной почте, чате или размещать в комментариях на его странице в Сети.

Оценивайте интернет-контент критически. То, что содержится в Интернете, не всегда правда. Дети должны научиться отличать надежные источники информации от ненадежных и проверять информацию, которую они находят в Интернете. Также объясните детям, что копирование и вставка содержания с чужих веб-сайтов могут быть признаны плагиатом.

Общие рекомендации по обеспечению безопасности детей и подростков в Интернете

Если Вы нуждаетесь в консультации специалиста по вопросам безопасного использования Интернета или если Ваш ребенок уже столкнулся с рисками в Сети, обратитесь на линию помощи "Дети Онлайн" (detionline.com), по телефону: 8 800 250 00 15 (звонок по России бесплатный).

Страница на сайте лицея № 384, посвященная информационной безопасности
http://sc384.kirov.spb.ru/spisok-vsekh-kategorij/2-uncategorised/72-informatsionnaya-bezopasnost