Опасности при использовании сети Интернет бесконтрольно

Количество пользователей интернета в мире составляет 3,5 миллиарда человек. Ежегодно растет число пользователей, среди которых все больше – детей и подростков. В России восемьдесят пять процентов российских детей в возрасте от 10 до 17 лет активно пользуются Интернетом. По статистическим данным в Сети они проводят до 25 часов в неделю и, как правило, пользуются Интернетом бесконтрольно.

В современных условиях развития общества компьютер стал для ребенка и «другом», и «помощником», и даже «воспитателем», «учителем».

При этом развитие высоких технологий, открытость страны мировому сообществу привели к незащищенности детей от противоправного контента в информационно-телекоммуникационной сети «Интернет», усугубили проблемы, связанные с торговлей детьми, детской порнографией и проституцией.

По сведениям МВД России, **число сайтов, содержащих материалы с детской порнографией за последние несколько лет, увеличилось почти на треть, а количество самих интернет-материалов - в 25 раз**.

Значительное число **сайтов, посвященных суицидам**, доступно подросткам в любое время.

По информации Генеральной прокуратуры Российской Федерации в 2018 году более 93 тыс. детей стали жертвами преступлений. Проблема обеспечения информационной безопасности детей в информационно-телекоммуникационных сетях становится все более актуальной .

По данным различных исследований более 40% детей сталкиваются с сексуальными изображениями в интернете. Младшие школьники сталкиваются с сексуальными изображениями реже, чем старшие, но испытывают больший стресс. Прилежные дети в 2 раза чаще попадают на «плохие» сайты в силу природной любознательности. Более 20% детей становятся жертвами нападок со стороны сверстников. 90% школьников имеют аккаунты в социальных сетях. 70% в своих аккаунтах указывают свою фамилию, точный возраст и номер школы. 40% российских детей готовы продолжить он-лайн общение в реальной жизни. У 30% школьников данные аккаунта открыты всему миру. Более 28% опрошенных детей готовы переслать свои фотографии незнакомцам в Сети.

17% без колебаний соглашаются сообщить информацию о себе и своей семье – место жительства, профессия и график работы родителей, наличие в доме ценных вещей и

т. д. (о том, для чего посторонним может потребоваться такая информация, дети, как правило, не задумываются).

Виды интернет-угроз.

Итак, рассмотрим по порядку какие же бывают интернет-угрозы.

– Информация, пропагандирующая или описывающая запрещенные в обществе вещи и понятия. Сюда можно отнести сайты, на которых пропагандируют расовую нетерпимость, фашизм, сектантство, терроризм, жестокое отношение к людям или животным, наркотики, алкоголь, курение и прочее. Сложность отслеживания таких сайтов в том, что их часто тяжело определить идеологически, то есть не всегда сайт называется «О пользе героина и как скрыть его от родителей». Часто это могут быть вполне безобидные ресурсы под названием «Тусовка города Н», где на открытом форуме, кто-то мог организовать какой-то соответствующий раздел. Более того часто какие-то деструктивные вещи скрываются за благовидными заголовками, например, «Спасем души наших родителей» – не подкопаешься, а по сути там статья о деструктивной секте, которая предлагает уйти под землю и ждать очередного Конца Света. Или существует множество видеороликов, в которых показывают одно, например прохождение игры , а автор за кадром рассказывает как выпрыгнуть лучше с окна или моста для сведения счетов с жизнью;

– ***Сюда же можно отнести и контент, связанный с сексом. В интернете действительно очень много сайтов, пропагандирующих именно нездоровые сексуальные отношения***: педофилия, гомосексуальные связи, разного рода извращения, интим за деньги и т.д.

– *Игры.* ***Первое, о чем не всегда знают взрослые****, что большинство игр, в которые играют их милые дети, рассчитаны на возраст от 14-и, 16-и или 18-и лет. Ограничение вызвано множеством сцен насилия, крови, психотропным воздействием (например, мрачной атмосферой) и эротическими сценами*. Причем большинство современных игр относятся именно к такой опасной категории.

Второе, онлайн-игры предполагают большое количество участников, голосовой или текстовый чат и кто знает о том, кто скрывается под виртуальным собеседником. Хорошо, если это просто сверстник, а если это сорокалетний извращенец?

Третье, мир игр поглощает, заменяя реальную жизнь. Дети погружаются в него полностью, там интересней, там можно себе многое позволить. И совершенно не надо сильно напрягаться. Тебя любит противоположный пол, у тебя друзья, ты герой. А потом так тяжело выходить назад и делать тошнотворные уроки. И что

после этого стоит модель самолета, которую вы делали с сыном 3 месяца? Скажем, она может смотреться убого и весьма проигрывать американскому стелс F-22 на котором ваш сын уже несколько недель ведет ожесточенные бои в интернете. Многие даже не догадываются, что их милый сынишка в игре хватает топор и бежит рубить всех новичков, которые не могут дать ему отпор, и чем больше крови, тем лучше он себя чувствует. И я не сгущаю краски, так и есть.;

– Продолжая тему игр, стоит отдельно выделить сайты, которые предлагают азартные виртуальные развлечения за реальные деньги. Ребенку очень хочется откликнуться на множество вывесок типа «я стал в 15 лет богаче родителей всего за полдня» и прочего бреда. Видели подобные баннеры на сайтах?. А потом выясняется, что чадо тягает деньги и спускает их в лучшем случае на онлайн покер;

– ***Один из видов угроз - интернет-мошенничество или фишинг***, главная цель которого состоит в получении конфиденциальных данных пользователей — логинов и паролей. Среди разных способов и технологий подобного мошенничества выделяются следующие: вишинг, фарминг, смишинг и сам фишинг. Большинство методов фишинга сводится к созданию копий реальных сайтов и маскировке поддельных ссылок под ссылки сайтов настоящих организаций. Обычно злоумышленники используют доменные адреса с опечатками или субдомены. Таким образом, мошенники могут получить доступ к вашим аккаунтам, личным кабинетам, платежным системам, банковской карте.

– Переход в реальный мир. К счастью, физически добраться до вас и вашего ребенка через интернет невозможно. Но можно попытаться выманить куда-то подростка, способов сделать это существует множество. Самым банальным является назначение свидания. Преступник регистрируется как лицо противоположного пола, ставит себе привлекательную фотографию, втирается к подростку в доверие, а потом предлагает встретиться в кафе поесть мороженое. Думаю, катастрофические последствия такой встречи расписывать не стоит. И не нужно быть недальновидными и считать, что мой ребенок «не так-то глуп». Существует множество способов заманить ребенка в ловушку, например, преступник подойдет к подростку и скажет, что он папа его подружки, и она заболела и что он отвезет его к ней.

– Социальные сети, сайты знакомств, форумы и мессенджеры, ведение блогов, каналы в ютюбе сами по себе не несут угроз, как не несет угроз и просто телефон. Опасность заключается в методах использования. Я не буду рассказывать о зависимости от виртуального общения – это другая большая тема, но при этом все должны понимать, ***что когда подросток впадает в истерику, если ему не дали немедленно зайти пообщаться в социальную сеть – это уже плохой знак***. Я хочу рассказать о тех особенностях угроз из социальных сетей, о которых не каждый взрослый знает:

- ***Во- первых, есть такое понятие как цифровая репутация*** - это негативная или позитивная информация в сети о пользователе. Компрометирующая информация, размещенная в интернете может серьезным образом отразиться на реальной жизни человека.

«Цифровая репутация» - это имидж, который формируется из информации о пользователе в интернете. Место жительства, учебы, финансовое положение, особенности характера и рассказы о близких – все это накапливается в сети.

Комментарии, размещение фотографий и другие действия могут не исчезнуть даже после их удаления. Пользователь не знает, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли она, а главное: что подумают окружающее люди, которые найдут и увидят это. Найти информацию много лет спустя сможет любой – как из добрых побуждений, так и с намерением причинить вред. Это может быть кто угодно.

Многие сотрудники отдела кадров учитывают цифровую репутацию, решая, принять ли человека на работу.

– *Следующая угроза из соц. сетей - секстинг - пересылка личных фотографий, сообщений интимного содержания посредством современных средств связи:* сотовых телефонов, электронной почты, социальных интернет-сетей.

Подростки используя камеры, встроенные в мобильные телефоны, фотографируют себя в обнаженном или полуобнаженном виде и отправляют эти картинки своим друзьям, подругам или одноклассникам. Некоторые отправляют такие фотографии только одному человеку, а уже тот в свою очередь пересылает их другим людям.

Секстинг выглядит как забава или какая-то игра до тех пор, пока кто-нибудь не пострадает. Проблема секстинга заключается в том, что конфиденциальные фотографии могут быстро стать достоянием общественности. Смелая фотка, отправленная сегодня другу или подруге, завтра может начать бесконтрольно распространяться, в результате чего автор станет посмешищем в школе, на него выльется много грязи и сплетен. Когда фотография становится доступной в Интернете, то практически невозможно удалить все ее копии.

- ***Еще одна угроза в социальных сетях - Кибербуллинг или виртуальное издевательство.***

Первый случай кибербуллинга был зафиксирован в 2002 году. Американский подросток Жислен Раза ради развлечения снял видеоролик, в котором он, подобно герою фильма «Звездные войны», фехтовал бейсбольной битой вместо лазерного меча. Одноклассники разместили в сети это видео с целью позабавиться над

Жисленом. Эту запись посмотрели миллионы людей, через несколько дней был создан специальный сайт с исходным видео и пародиями на него. Насмешки сломали психику Жислена Раза и его родители были вынуждены обратиться к психиатру. Против одноклассников, разместивших исходное видео в интернете, был подан судебный иск.

Спектр целей кибер-преследователей широк, но всех объединяет стремление нанести жертве психологический ущерб. Это могут быть шутки, которые просто уязвят жертву, а может быть психологический террор, который приведет к суициду. Один из самых популярных случаев – это унижение или избиение человека в реальной жизни, заснятое на видео и выложенное в интернет. Подобные ситуации не редкость в новостях по телевизору.

- ***Ну и, пожалуй, самое основное – это так называемое зомбирование***. Это могут быть и группы смерти и террористичнские группировки, и секты, и пр. Но план действий у всех один и тот же. Как я уже говорила, не сложно узнать из соц. сети чем живет человек, что ему нравится, какие интересы. И, когда подросток вступает в контакт с незнакомцем, он не догадывается, что по ту сторону сидит тонкий психолог. Подростку кажется, что собеседник его понимает как никто другой, что они «на одной волне». Он доверяется ему, соглашается делать все, что от него требуется. Этот процесс происходит достаточно долго, поэтому сложно догадаться, что кто-то манипулирует тобой, это кажется крепкой дружбой. И это касается не только наивных детей и подростков. Очень многие взрослые попадаются на такое, особенно те, у кого сложности в жизни, критическая ситуация.

Информационная защита.

Теперь посмотрим, какая защита существует.

Согласно российскому законодательству информационная безопасность детей - это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию. Обеспечение государством информационной безопасности детей, защита их физического, умственного и нравственного развития во всех аудиовизуальных медиа-услугах и электронных СМИ - это требование международного права (Рекомендации Европейского Парламента и Совета ЕС от 20.12.2006 «О защите несовершеннолетних и их человеческого достоинства в Интернете»),

Значительные изменения внесены в Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Здесь впервые даётся определение интернет-сайта, интернет-страницы, доменного имени, сетевого адреса, владельца интернет-сайта, хостинг-провайдера. В закон

добавляется новая статья 15 и создаётся информационная система «Единый реестр доменных имен и (или) универсальных указателей страниц сайтов в сети Интернет и сетевых адресов сайтов в сети Интернет, содержащих информацию, запрещённую к распространению на территории Российской Федерации федеральными законами» (далее — Реестр). После решения федеральных органов, операторы Реестра вносят в него ссылки на интернет-страницы или доменные имена содержащие:

а) материалы с порнографическими изображениями несовершеннолетних и (или) объявления о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера;

б) информацию о местах приобретения, методах изготовления и использования наркотиков, психотропных веществ и их прекурсоров. Способах и местах культивирования наркосодержащих растений;

в) информацию о способах совершения самоубийства, а также призывов к совершению самоубийства;

г) (добавлено ФЗ 05.04.2013 № 50-ФЗ) информацию о несовершеннолетних, пострадавших в результате противоправных деяний.

д) любую иную информацию, запрещённую к распространению в России решениями судов.

Также ряд ведущих организаций российской Интернет-общественности, обеспокоенные возрастанием рисков и опасностей, подстерегающих детей и подростков в Интернете, объявили о своем объединении.

Появились различные центры, общества, фонды, ведущие борьбу с незаконным контентом и противоправными действиями в сети :

– Центр Безопасного Интернета в России

http://www.saferunet.ru

– Фонд «Дружественный Рунет»

http://www.friendlyrunet.ru/

– Также компания Microsoft разместила на своем интернет ресурсе много полезной информации по безопасности детей в интернете. http://www.microsoft.com

– Фонд Развития Интернет (проводит специальные исследования, которые посвящены изучению психологии цифрового поколения России.)

fid.ru.

– Линия помощи «Дети Онлайн»

www.detionline.com

– Горячая линия Центра безопасного Интернета

rushotline.ru.

– Горячая линия по приему сообщений о противоправном контенте в сети Интернет

hotline.friendlyrunet.ru

– Справочник по детской безопасности в Интернете от корпорации Google. (кстати, очень рекомендую почитать)

www.google.ru/familysafety

Правила безопасности в сети интернет.

Эти правила, как и правила пожарной безопасности, правила дорожного движения и др. мы должны знать наизусть. Причем, как и взрослые так и дети, и подростки.

1. Используйте надежный пароль, который содержит цифры, буквы латинского алфавита, знаки. Всего не менее чем из 8 символов. И не используйте в пароле личную информацию, такую как дата рождения, имя и фамилия и пр.
2. Пользуйтесь антивирусом.
3. Ничего не скачивайте с сомнительных сайтов, не переходите по сомнительным ссылкам. Программы лучше скачивать только с официальных сайтов разработчиков.
4. Если Вы работаете за компьютером, к которому имеют доступ другие люди (на роботе или в интернет кафе), не сохраняйте пароли в браузере. В противном случае, любой, кто имеет доступ к этому компьютеру, сможет зайти на сайт, используя Ваш пароль. (если в компьютерах в учительской посмотреть, там можно много паролей и логинов найти))
5. При вводе каких-либо данных на сайте, обращайте внимание на название сайта в адресной строке: протокол передачи данных https говорит о том, что вам будет обеспечена криптографическая защита, а в http – нет, т.е. ввод данных там не защищен.
6. Что касается социальных сетей, это

1. Будьте всегда на чеку, относитесь всегда с излишней осторожностью, когда с вами заводят беседу незнакомые люди, когда что-то предлагают.
2. Защищать свою частную жизнь. Не указывать пароли, телефоны, адреса, дату твоего рождения и другую личную информацию.
3. Защищать свою репутацию - держать ее в чистоте и задавать себе вопрос: хотел бы я, чтобы другие пользователи видели, что я загружаю? Нужно подумать, прежде чем что-то опубликовать, написать и загрузить;
4. При разговоре с людьми, которых не знаешь, не используйте свое реальное имя и другую личную информацию: имя, место жительства, место учебы, место работы и прочее;
5. Не храните в одном месте всю информацию. Например, взять телефон большинства людей – и это простор для хулиганов и мошенников. У большинства людей на телефоне есть личные фото и видео, установленные приложения сбербанк онлайн, установленные соц. сети и т.д. Многие в телефоне еще хранят пароли от электронных ящиков например. В лучшем случае, если этим воспользуется одноклассник, в худшем, когда телефон будет утерян и последствия будут очень плачевные. Кстати, про приложения. При скачивании приложений на телефон, следует обращать внимание на разрешения, требуемые разработчиком этого приложения. Зачастую, не читая соглашения и разрешая доступ к различным функциям телефона, люди сами себя подвергают опасности.

Все правила безопасности в сети Интернет очевидные, их соблюдать не сложно, главное быть бдительнее и внимательнее.

Что касается детей, существуют средства блокирования нежелательного контента с помощью спец. программ Родительского контроля.

Их достаточно много.

Платная программа KinderGate Родительский контроль, Бесплатный браузер детский интернет фильтр КиберПапа, Платная программа КиберМама, Бесплатный детский браузер Гогуль, NetKids, Платная программа KidsControl.

Также можно в настройках большинства поисковых систем включить функцию безопасного поиска. Она позволяет исключить неприемлемый контент (например, порнографию) из безопасного поиска.

Заключение.

Еще хочется немного добавить не о безопасности в сети, а о ложности информации.

Интернет содержит огромное количество информации и, к сожалению, большая ее часть является информационным мусором. То есть, чтобы повысить рейтинг сайта их владельцы создают мусорные страницы, тексты со ссылками на основной сайт. Иногда на одну страницу ведут тысячи мусорных страниц с других сайтов. Или информация копируется и разносится по разным сайтам и соцсетям, иной раз меняя даже смысл сказанного. Часто теряется ссылка на первоисточник, поэтому проверить достоверность информации крайне затруднительно.

А иногда заведомо ложная информация разносится с умыслом повлиять на общественное мнение (особенно это касается средств массовой информации), которые в своих корыстных целях манипулируют мнением людей.

Если информация из Интернета, это совсем не значит, что она достоверна.

Пользователю нужно уметь различать сайты по авторитетности, надежности, а информацию по достоверности.

Не верьте никому, кроме себя и своего здравого смысла;

Будьте критичны к любой информации;

Проверяйте информацию: делайте личные запросы, ищите источники и официальные документы;

Повышайте собственную грамотность.

Интернет сейчас используется везде. И чем больше спрос, тем больше предложение. Для того, чтобы избежать проблем, достаточно соблюдать несложные правила безопасности.