

## Проблемы обеспечения защиты детей от противоправного контента в образовательной среде колледжа и дома

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 из 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 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 уроки. Многие даже не догадываются, что их сын в игре хватается топор и бежит рубить всех новичков, которые не могут дать ему отпор, и чем больше крови, тем лучше он себя чувствует.

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.

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.

– Социальные сети, сайты знакомств, форумы и мессенджеры, ведение блогов, каналы в ютубе сами по себе не несут угроз, опасность заключается в методах использования. Зависимость 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. Существуют особенности 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.

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 окружающие 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. 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 террористические 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 попадают на такое, особенно те, у кого сложности в жизни, критическая ситуация.

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](http://fid.ru).

– [Линия помощи «Дети Онлайн»](#)

[www.detionline.com](http://www.detionline.com)

– [Горячая линия Центра безопасного Интернета](#)

[rushotline.ru](http://rushotline.ru).

– [Горячая линия по приему сообщений о противоправном контенте в сети Интернет](#)

[hotline.friendlyrunet.ru](http://hotline.friendlyrunet.ru)

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

[www.google.ru/familysafety](http://www.google.ru/familysafety)

Заместитель директора по ВР Хасанова А.Х.