# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ДЕТЕЙ:

# ВОЗМОЖНОСТИ БИБЛИОТЕКИ:

# ЧАСТЬ 1. ИНТЕРНЕТ РИСКИ

В условиях современного общества, когда происходит глобальная информатизация общества, в деятельности человека прочно закрепились средства электронного общения - глобальные компьютерные сети, прежде всего сеть Интернет. По данным кафедры психологии личности МГУ, количество детей, ежедневно пользующихся интернетом, за последние два года выросло до 95%. При этом 32% детей сидят в сети каждый день по 8 часов.

Что же таит в себе всемирная паутина? Какие интернет-риски подстерегают наших детей за светящимся экраном?

В первую очередь, это чрезмерная увлеченность Интернет пользованием, компьютерными играми, «серфингом», онлайн-казино. Психологи отмечают, что у некоторых детей интернет-зависимость формируется уже после полугода активного пользования. У части детей – через год.

Особенно опасна чрезмерная увлеченность для дошкольников, так как у дошкольников слабо развита тормозная система. Они быстро возбуждаются,  вовлекаются в процесс, а вот затормозить чувства и желания им сложно. Яркие картинки, динамичные игры – все это завораживает, увлекает. Ребенок становится заложником виртуальной реальности.

Интернет пространство, которое окружает ребенка, не может не сказываться на всей его жизни. Интернет-риски, которым подвержены современные дети, вносят свои коррективы в развитие детей. У ребенка  происходит нарушение в развитии познавательных способностей, наблюдаются отклонения в эмоциональной сфере, меняется в целом личность ребенка, пропадает интерес к учебе.

Все опасности интернет-среды специалисты объединяют в четыре крупные группы рисков:

# Контентные риски

Контентные риски — это материалы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие насилие, агрессию, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр, наркотических веществ и т.д. Столкнуться с ними можно практически везде. Это и сайты, и социальные сети, и блоги, и торренты, и видеохостинги, фактически все, что сейчас существует в Интернете. Зачастую подобный материал может прийти от незнакомца по почте в виде спама или сообщения.

Негативные контентные материалы можно условно разделить на:

* **Незаконные**, к которым могут относиться: детская порнография (включая изготовление, распространение и хранение); наркотические средства (изготовление, продажа, пропаганда употребления), все материалы, имеющие отношение к расовой или религиозной ненависти (экстремизм, терроризм, национализма и др.), а также ненависти или агрессивного поведения по отношению к группе людей, отдельной личности или животным), азартные игры и т.д.

Внутреннее законодательство каждой страны предусматривает различные виды наказания за распространение такой информации. В Российском законодательстве есть возможность в соответствии со статьями Уголовного кодекса РФ привлечь к административной и уголовной ответственности за распространение подобного негативного контента владельцев сайтов, а также авторов таких электронных текстов и видеопродукции.

* **Неэтичные**, противоречащие принятым в обществе нормам морали и социальным нормам.

Подобные материалы не попадают под действие уголовного кодекса, однако могут оказывать негативное влияние на психику столкнувшимися с ними человека, особенно ребенка. Примерами таких материалов могут служить широко распространенные в сети изображения сексуального характера, в том числе и порнография, агрессивные онлайн игры, азартные игры, пропаганда нездорового образа жизни (употребление наркотиков, алкоголя, табака, анорексии, булимии), принесения вреда здоровью и жизни (различных способов самоубийства, аудионаркотиков, курительных смесей), нецензурная брань, оскорбления, и др. Информация, относящаяся к категории неэтичной может быть также направлена на манипулирование сознанием и действиями различных групп людей.

Контентные риски связаны с другими типами рисков Сети. Например, просмотр тех или иных видео-материалов может привести к заражению компьютера вирусами и потере важных данных. Очень многие распространители подобного негативного контента преследуют цель заразить компьютер, чтобы в дальнейшем иметь возможность манипулировать данными и действиями зараженного компьютера. Пропаганда негативных материалов также может идти через социальные сети, блоги, различные форумы. В данном случае контентные риски пересекаются с коммуникационными.

# Коммуникационные риски

Коммуникационные риски связаны с межличностными отношениями интернет-пользователей и включают в себя риск подвергнуться оскорблениям и нападкам со стороны других. Примерами таких рисков могут быть: незаконные контакты (например, груминг), киберпреследования, кибербуллинг и др. Для подобных целей используются различные чаты, онлайн-мессенджеры , социальные сети, сайты знакомств, форумы, блоги и т.д.

Оказаться жертвой намного проще, чем кажется. Каждый участник той или иной социальной сети может признаться, что хотя бы один раз ему приходило непристойное предложение от неизвестного человека. Это беда не только социальных сетей. На любом популярном форуме, в блоговом сообществе и чате появляются такие участники, которые хамят и оскорбляют других участников.

Коммуникационные риски включают в себя «незаконный контакт» и «киберпреследование».

*Незаконный контакт* — это общение между взрослым и ребенком, при котором взрослый пытается установить более близкие отношения для сексуальной эксплуатации ребенка. Это понятие включает в себя такие интернет-преступления как домогательство и груминг.

*Домогательство* — причиняющее неудобство или вред поведение, нарушающее неприкосновенность частной жизни лица. Такое поведение может заключаться в прямых или косвенных словесных оскорблениях или угрозах, недоброжелательных замечаниях, грубых шутках или инсинуациях, нежелательных письмах или звонках, показе оскорбительных или унизительных фотографий, запугивании, похотливых жестах, ненужных прикосновениях, похлопываниях, щипках, ударах, физическом нападении или в других подобных действиях.

*Груминг* — установление дружеских отношений с ребенком с целью изнасилования.

Злоумышленник нередко общается в интернете с ребенком, выдавая себя за ровесника либо ребенка немного старше. Он знакомится в чате, на форуме или в социальной сети с жертвой, пытается установить с ним дружеские отношения и перейти на личную переписку. Общаясь лично («в привате»), он входит в доверие к ребенку, пытается узнать номер мобильного и договориться о встрече.

*Киберпреследование*) — это преследование пользователя сообщениями, содержащими оскорбления, агрессию, сексуальные домогательства с помощью различных интернет-сервисов.

Виды агрессии в интернете:

*Флейминг* – разжигание спора, публичные оскорбления и эмоциональный обмен репликами в интернете между участниками в равных позициях.

*Троллинг* – размещение в интернете провокационных сообщений с целью вызвать негативную эмоциональную реакцию или конфликты между участниками.

*Хейтинг* – негативные комментарии и сообщения, иррациональная критика в адрес конкретного человека или явления, часто без основания своей позиции.

*Киберсталкинг* – использование электронных средств для преследования жертвы через повторяющиеся сообщения, вызывающие тревогу и раздражение.

*Кибербуллинг* – агрессивные, умышленные, продолжительные во времени действия, совершаемые группой лиц или одним лицом с использованием электронных форм контакта и повторяющиеся неоднократно в отношении жертвы, которой трудно себя защитить.

Также, киберпреследование может принимать такие формы, как обмен информацией, контактами; запугивание; подражание; хулиганство (интернет-троллинг); социальное бойкотирование. По форме буллинг может быть не только словесным оскорблением. Это могут быть фотографии, изображения или видео жертвы, отредактированные так, чтобы быть более унизительными.

Подобный унизительный контент может исходить от одного человека или группы людей по одному или нескольким электронным контактам жертвы, на электронный ящик или в сообщениях онлайн-мессенджеров. Распространены также случаи преследования в социальных сетях или на подобных им ресурсах. При этом помимо рассылки оскорбительных сообщений и вывешивания унизительных материалов, изображений или видеозаписей, буллер может также взломать профиль или страницу жертвы и организовать спам-рассылку по всем контактам жертвы.

Основные характеристики буллинга и кибербуллинга:

– умышленность,

– регулярность,

– неравенство сил,

–групповой процесс (затягивается широкий круг участников).

– не заканчивается сам по себе,

– негативное психологическое воздействие ситуации на всех участников.

Особенности кибербуллинга:

– Анонимность и дистантность агрессора, агрессор чувствует себя менее уязвимым и ответственным;

– Не видна эмоциональная реакция жертвы;

– Возможность травли 24 часа, независимость от времени и места;

– Один источник (фото, пост и т.д.) может использоваться множество раз;

– Увеличение аудитории наблюдателей;

– Жертвой кибербуллинга может стать каждый вне зависимости от статуса;

– Не оставляет физических следов, незаметность для родителей, учителей;

– Жертва скрывает факт травли:

– Кибербуллингу нельзя противостоять в одиночку.

К сожалению, кибербуллинг — очень распространенное явление среди российских подростков. Каждый пятый ребенок может признать, что подвергался буллингу онлайн или в реальной жизни. И это беда не только России, она распространена во всем мире. Но в России дети становятся жертвами буллинга в интернете так же часто, как и в реальной жизни. Нередко кибербуллинг берет начало в отношениях с реальными людьми, и в этом случае, жертва знает своих оскорбителей. Когда же буллинг происходит в интернете, всегда важно удостовериться, чтобы он не перерос в реальное насилие над ребенком.

# Электронные риски

Электронные (кибер) риски — это возможность столкнуться с хищением персональной информации, риск подвергнуться вирусной атаке, онлайн-мошенничеству, спам-атаке, шпионским программам и т.д. Вредоносное ПО (Программное Обеспечение) использует широкий спектр методов для распространения и проникновения в компьютеры, не только через компакт-диски или другие носители, но и через электронную почту посредством спама или скачанных из Интернета файлов.

К вредоносным программам относятся вирусы, черви и «троянские кони» – это компьютерные программы, которые могут нанести вред вашему семейному компьютеру и хранящимся на нем данным. Они также могут снижать скорость обмена данными с Интернетом и даже использовать ваш компьютер для распространения своих копий на компьютеры ваших друзей, родственников, коллег и по всей остальной глобальной сети. Защита в социальных сетях — это задача, которая не так давно стала актуальна для их пользователей. Буквально несколько месяцев назад, взлом страниц в социальных сетях превратился в один из основных способов распространения спама в Интернете.

В частности, теперь вирусное ПО (программное обеспечение), которое рассылает спам в социальной сети, может быть установлено на ваш компьютер с любого сайта. И от вашего лица могут регулярно рассылаться абсолютно любые сообщения, избавиться от которых не поможет ни одна защита самого сайта. Хотя бы просто по той причине, что в этом случае потребуется не защита вашей страницы, а современное антивирусное программное обеспечение. Поэтому не забывайте обновлять свою антивирусную программу и следить за защитой своего компьютера.

К сожалению, вероятность наткнуться на подобные вредоносные программы очень велика. Помимо негативного воздействия на компьютер и мобильное устройство, можно стать жертвой еще одного вида кибер- преступления — кибер-мошенничества. В самом широком смысле мошенничество — это умышленный обман или злоупотребление доверием с целью получения какой-либо выгоды.

Мошенничество в сети Интернет (кибермошенничество) — один из видов киберпреступления, целью которого является обман пользователей. Хищение конфиденциальных данных может привести к тому, что хакер незаконно получает доступ и каким-либо образом использует личную информацию пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.), с целью причинить материальный и финансовый ущерб.

# Потребительские риски

Потребительские риски – злоупотребление в интернете правами потребителя. Включают в себя: риск приобретения товара низкого качества, различные поделки, контрафактная и фальсифицированная продукция, потеря денежных средств без приобретения товара или услуги, хищение персональной информации с целью кибер-мошенничества, и др.

Также дети, зачастую совершая онлайн покупки, могут растратить значительные суммы своих родителей, если каким-либо способом имели или получили к ним доступ.

Одним из самых распространенных видов данного типа рисков является мошенничество — это умышленный обман или злоупотребление доверием с целью получения какой-либо выгоды. Мошенничество, как правило, является преступлением.

Поскольку мошенничество в сети интернет совершается с помощью различных технических средств и разнообразного количества программ, то некоторые его виды могут быть отнесены и к группе электронных рисков, а часть к группе коммуникационных, поскольку включает в свою схему установления более близкого контакта с жертвой в течение какого-либо времени (например, с помощью электронных писем и смс, которые могут привести и к реальным встречам с мошенниками).

Дети и подростки, - группы риска

* употребляющие алкоголь, психоактивные вещества;
* с недостатками физического развития;
* совершившие серьезный проступок или жертвы уголовного преступления (в том числе, насилия);
* под влиянием опасных групп (в том числе, в соцсетях), религиозных сект или молодежных течений;
* в сложной семейной ситуации;
* остро переживающие несчастную любовь;
* в депрессивном состоянии;
* без реальных друзей;
* без устойчивых интересов, хобби;
* с серьезными проблемы в учебе;
* отличники, остро переживающие любые неудачи;
* с историей суицида.

Влияние Интернета на детей и информационная безопасность в XXI веке — тема огромная. Здесь представлены лишь основные, очевидные вызовы, стоящие перед родителями сегодня. Под угрозой психика ребенка, его образ мышления, его жизненные ценности. Более подробно узнать об интернет-рисках, правилах безопасности, ознакомиться с другими важными материалами, которые также помогут разобраться в теме безопасного использования сети интернет, можно на порталах:

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

[www.fid.su](http://www.fid.su),

<http://www.google.ru/familysafety>,

<http://safety.mts.ru>.

*Приложение 1*

**Рекомендации взрослым:**

Поощряйте детей делиться с вами их опытом в Интернете. Посещайте сеть вместе с детьми

научите детей: если их что-нибудь беспокоит, им следует сообщить вам об этом

Научите детей уважать других в Интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде – даже в виртуальном мире.

Если дети общаются в чатах, используют программы мгновенного обмена сообщениями, играют или занимаются чем-то другим, требующим регистрационного имени, помогите ребенку его выбрать и убедитесь, что оно не содержит никакой информации

настаивайте, чтобы дети уважали собственность других в Интернете. Объясните, что незаконное копирование чужой работы – музыки, компьютерных игр, программ – является кражей.

Объясните детям, что им никогда не следует встречаться с друзьями из Интернета. Объясните, что эти люди могут быть не теми, за кого себя выдают.

Объясните, что не все, что они видят или читают в Интернете, является правдой. Научите детей спрашивать вас, если им что-то непонятно, или они в чем-то не уверены.

Контролируйте деятельность детей в интернете с помощью ПО «Родительский контроль». Данные программы помогут отфильтровать вредное содержимое, выяснить какие сайты посещает ребенок и что он делает на них.

*Приложение 2*

**Правила по безопасному использованию интернета**

**(рекомендации для детей)**

Контентные риски

* Для того, чтобы избежать встречи с неприятной информацией в интернете, установи на свой браузер фильтр или попроси сделать это взрослых – тогда ты сможешь смело путешествовать по интересным тебе страницам.
* Всегда спрашивай родителей о незнакомых вещах в интернете. Они расскажут, что безопасно делать, а что нет.

Электронные риски

* Не скачивай и не открывай неизвестные тебе или присланные незнакомцами файлы из интернета. Чтобы избежать заражения компьютера вирусом, установи на него специальную программу – антивирус!
* Если твой компьютер заблокирован, то попроси взрослых разблокировать твой компьютер с помощью антивируса. Если твой компьютер заблокировался картинкой с требованием отправить смс, позвони на Линию помощи «Дети Онлайн» (8-800-25-000-15, бесплатно), и тебе помогут решить проблему!

Коммуникационные риски

* Прежде чем начать дружить с кем-то в интернете, спроси у родителей, как безопасно общаться в сети.
* Никогда не рассказывай о себе незнакомым людям: где ты живешь, учишься, свой номер телефона. Это должны знать только твои друзья и семья!
* Не отправляй свои фотографии, а также фотографии своей семьи и своих друзей незнакомым людям. Они могут использовать их так, что это навредит тебе или твоим близким.
* Не встречайся без родителей с людьми из интернета в реальной жизни. В интернете многие люди рассказывают о себе неправду.
* Общаясь в интернете, будь дружелюбен с другими. Не пиши грубых слов! Ты можешь нечаянно обидеть человека. Читать грубости также неприятно, как и слышать.
* Если тебя кто-то расстроил или обидел в интернете, обязательно расскажи об этом родителям.

Потребительские риски

* Если хочешь скачать картинку или мелодию, но тебя просят отправить смс – не спеши! Сначала проверь этот номер в интернете – безопасно ли отправлять на него смс, и не обманут ли тебя. Сделать это можно на специальных сайтах:

<http://smscost.ru>,

<http://smswm.ru>,

<http://smsnumbers.ru> .