

Информационное сопровождение

Для современного ребенка интернет не менее значим и так же естественен, как для поколения их родителей электричество или вода в водопроводе. Исследования Лаборатории Касперского показали, что две трети детей не представляют своей жизни без смартфона, а 56% подростков говорят, что находятся в Сети постоянно. Это неудивительно, ведь и их родители то и дело проверяют мессенджеры и почту, выходят в социальные сети, смотрят видео.

Важно помнить о том, что интернет не является полностью безопасным пространством, здесь и взрослого, и ребенка поджидает множество угроз как технического (например, вирусы), так и социального характера (например, секты, мошенники). При этом далеко не всегда дети, сталкиваясь с неприятностями, рассказывают об этом родителям. Так, согласно опросам, только 10% родителей думают, что их дети видели взрослый контент в Сети, в то время как о посещении страниц с таким содержимым сообщает более половины всех опрошенных нами детей.

Некоторые опасные действия в Сети дети производят случайно – например, попадаются на уловки мошенников или заходят на сайты со взрослым содержимым по ссылке «Кликни сюда и увидишь симпатичных котят». Есть и те, кто намеренно совершает в Сети рискованные действия – например, общаются с незнакомыми людьми, скачивают пиратское программное обеспечение. И в том, и в другом случае ребенок может решить скрыть свои действия от родителей: 58% детей признались в ходе нашего опроса, что не рассказывают о таких активностях родителям. При этом 47% родителей твердо верят в то, что их дети ничего не скрывают, а 92%, даже если и догадываются о том, что ребенок рассказывает им не все, не знают наверняка о том, с какими конкретно угрозами ребенок сталкивается.

Чтобы скрыть свои действия в Сети, дети:

- 22%** используют анонимайзеры;
- 18%** выходят в Интернет, когда родителей нет рядом;
- 16%** детей защищают устройство паролем;
- 14%** применяют специальные программы, которые позволяют скрыть используемые приложения;
- 10%** удаляют историю поиска в браузере.

Дети же для сокрытия своих действий в Сети прибегают к самым разным ухищрениям – от вполне банального посещения интернета, когда родителей нет дома, до специальных программ, скрывающих другие приложения или действия в Сети.

В тоже время наши опросы показывают, что многие родители беспокоятся за своего ребенка, когда он использует гаджеты. Их страхи, однако, не всегда одинаково обоснованы, а иногда родители просто не понимают, какие действительно опасные ситуации могут произойти с ребенком в Сети. Так большинство родителей, почти 60%, боятся влияния работы с гаджетами на зрение и осанку.

54% родителей боятся развития у детей интернет - зависимости, причем многие взрослые принимают за зависимость желание ребенка всегда быть на связи, путая болезненное состояние с обычной современной тенденцией. Меньше половины родителей

опасаются общения своих детей с незнакомцами в Сети, а чуть больше трети волнуются, что такое общение может перерости в общение в реальной жизни.

Интересно, что, несмотря на волнения относительно детской online - активности, 20% взрослых не принимают никаких мер, чтобы защитить своего ребенка. 60% полагаются исключительно на воспитательные меры: общаются с ребенком, запрещают какие-то действия в Сети, иногда отбирают гаджеты. Лишь 20% родителей пришли к выводу, что полноценную защиту в технологической среде можно обеспечить, только применяя технологическое решение.



Чтобы понять, о каких опасностях в интернете идет речь, разберемся сначала в том, какие страницы дети чаще всего посещают в Сети. Почти 70% всей интернет - активности подростков приходится на социальные сети. Для современных школьников они практически заменили собой весь интернет. Второй по популярности темой страниц, которые посещают школьники, стала «Алкоголь, табак, наркотические вещества» – более 10% всех посещений веб-страниц детьми пришлись именно на такие ресурсы. На третьем месте страницы, посвященные видео-играм.

Возможно, родители бы более серьезно относились к технологическим средствам защиты, если бы четко осознавали, что интернет дает ребенку доступ к таким явлениям, от которых мы старательно оберегаем своих детей в реальной жизни.

Итак, первая опасность, которая поджидаст ребенка в интернете, – возможность доступа к **противоправному контенту**. Некоторые опасные действия в Сети дети производят случайно – например, заходят на сайты с взрослым содержимым. Есть и те, кто намеренно совершает в Сети рискованные действия – например, общаются с незнакомыми людьми, скачивают пиратское программное обеспечение, посещают порнографические сайты. И в том, и в другом случае ребенок может решить скрыть свои действия от родителей: 58% детей признались в ходе опросов, что не рассказывают о таких активностях родителям. В Сети

можно с легкостью найти сайты по продаже наркотических веществ и алкоголя, получить доступ к порнографическим материалам, кровавым снимкам с мест терактов, изображения казней и пыток, видео из лагерей джихадистов.

Кибербуллинг, или **кибертравля**, – это методичное и постоянное преследование и унижение человека в Сети. Пользователя оскорбляют, присылают ему неприятные сообщения, пишут гадости на стене, оскорбляют в сообществах, в которых он участвует, даже создают специальные группы, «посвящая» их жертве травли и размещая там неприятные посты об этом человеке. Кибертравлю обычно ведут люди, знакомые ребенку в реальности. В результате травли ребенок может получить серьезную психологическую травму, а особенно ранимые подростки даже совершают попытки самоубийства из-за действий агрессоров.

Формы кибербуллинга:

1. Исключение

Эта форма кибербуллинга аналогична бойкоту: жертву намеренно исключают из отношений и коммуникации. При этом возможны самые разнообразные проявления исключения:

- ребенка могут не допускать к играм, встречам или другим совместным занятиям с его друзьями;
- друзья ребенка могут не допускать его к совместным разговорам онлайн;
- иногда причинами к исключению может быть то, что у ребенка нет смартфона, или же то, что он не пользуется социальными сетями.

2. Домогательство

Домогательством называют постоянную и умышленную травлю при помощи оскорбительных или угрожающих сообщений, отправленных ребенку лично или как часть какой-либо группы.

Эта форма кибербуллинга крайне опасна и может привести к серьезным последствиям для ребенка. Эти злонамеренные сообщения могут устрашить ребенка и навредить ему, делая его неуверенным в себе. То, что такие сообщения будут посыпаться постоянно, означает, что ребенку не будет даваться никакой передышки от травли, что делает этот вид кибербуллинга особенно опасным.

3. Аутинг

Аутингом называется преднамеренная публикация личной информации ребенка с целью его унизить, при этом произведенная без его согласия. Аутинг может принимать разные формы, при этом опубликованная информация может быть, как серьезной, так и незначительной. Даже чтение сохраненных сообщений на телефоне ребенка можно считать аутингом. Личную информацию никогда нельзя разглашать.

4. Киберстalking

Киберстalking может привести к тому, что киберобидчик – человек, который производит саму травлю, – будет представлять реальную угрозу для безопасности и благополучия ребенка. В частности, этим термином могут называться попытки взрослых связаться с детьми и подростками через Интернет с целью личной встречи и дальнейшей сексуальной эксплуатации. Эта форма кибербуллинга крайне опасна и может иметь самые серьезные последствия, поэтому по обнаружению необходимо принимать все меры, чтобы

немедленно ее остановить.

5. Фрейпинг

Фрейпингом называют форму кибербуллинга, в которой обидчик каким-либо образом получает контроль над учетной записью ребенка в социальных сетях и публикует нежелательный контент от его имени.

Несмотря на то, что некоторые могут считать это занятие забавным и смешным, фрейпинг – серьезное преступление, которое может привести к серьезным последствиям. Так можно полностью разрушить репутацию жертвы – важно помнить, что Google никогда ничего не забывает. Если что-то было опубликовано в Сети, то в какой-то форме оно там останется навсегда.

6. Поддельные профили

Киберобидчики могут создавать поддельные профили – скрывать то, кем они на самом деле являются, чтобы травить ребенка. Также они могут использовать чужие телефонные номера и адреса электронной почты, чтобы заставить ребенка думать, что им угрожает не обидчик, а кто-то другой. Часто хулиганы используют поддельные профили, потому что боятся, что их личность станет известна. Такое обычно бывает, когда обидчик – кто-то, кого ребенок хорошо знает.

7. Диссинг

Диссингом называют передачу или публикацию порочащей информации о жертве онлайн. Это делается с целью испортить репутацию жертвы или навредить ее отношениям с другими людьми.

Информация может публиковаться в самых разных форматах – от текста до фото, скриншотов или видео. Обидчик всеми силами будет пытаться унизить ребенка, при этом привлекая максимум внимания к этому процессу. В этом случае обидчик чаще всего кто-то из знакомых ребенка, что может дополнительно усугубить ситуацию.

8. Обман

В этом случае киберхулиган обманом пытается завоевать доверие ребенка, чтобы тот рассказал ему какую-либо чувствительную информацию, которую обидчик затем публикует в Сети.

Обидчик сперва «подружится» с ребенком и обманом вызовет у него ложное чувство безопасности, а потом нарушит созданное доверие и отправит полученную информацию третьим лицам.

9. Троллинг

Троллингом называют намеренную провокацию при помощи оскорблений или некорректной лексики на интернет-форумах и в социальных сетях.

Тролли будут лично нападать на жертву и стараться унизить ее. Основная задача троллинга – разозлить жертву и заставить ее прибегнуть в манере самого тролля к оскорблению и некорректной лексике. Тролли могут тратить долгое время в поисках особенно уязвимой жертвы. Как правило, тролли получают положительные эмоции за счет унижения других.

10. Кетфишинг

Кетфишинг – форма кибербуллинга, в которой киберхулиган с целью обмана воссоздает профили жертвы в социальных сетях на основе украденных фотографий и других личных данных.

Важно обратить внимание не на конкретные разновидности кибербуллинга, а на само

явление в целом.

Чаще всего обидчики будут пытаться скрыть, кем они на самом деле являются. Они будут использовать информацию, которую ребенок уже разместил в социальных сетях, для создания поддельных личностей. Иногда они ограничиваются только фотографией ребенка и используют выдуманное имя, но иногда они могут использовать и всю доступную информацию. Часто бывает сложно понять, зачем обидчик занимается кетфишингом, но в любом случае важно понимать, что эта форма кибербуллинга может серьезно навредить репутации ребенка.

Полностью предупредить кибербуллинг может быть трудно, однако не стоит пренебрегать несложными мерами предосторожности, которые помогут защитить ваших детей от проблемы и ее последствий.

Например, отрегулировав настройки приватности в социальных сетях, взрослые помогут своим детям контролировать, кто может смотреть их публикации и писать им сообщения. Надежной защиты помогут добиться настройки родительского контроля, которые можно найти как в некоторых приложениях, так и в решениях для обеспечения ИТ-безопасности.

Онлайн-грумминг – это попытки незнакомого человека втереться в доверия к ребенку для дальнейшей сексуальной эксплуатации. Онлайн-груммеры могут пытаться вывести ребенка на личную встречу или получить от него интимные снимки или видео. Для получения такого материала злоумышленники прибегают к самым разным уловкам, чаще всего представляются сотрудниками модельных агентств. Таким лжеагентам, к сожалению, готовы отправить «красивые фотографии» девочки самого нежного возраста – известны случаи, когда это делали девятилетние школьницы. Получив от ребенка такие снимки, злоумышленник начинает шантажировать его, угрожая отправить их родителям или в школу. Целью шантажа являются все новые снимки и видео.

В последние месяцы очень много говорится о так называемых **группах смерти**. В указанных группах пользователю предлагается сыграть в «игру», на каждом этапе которой ему предстоит выполнять разные задания своего «куратора», а в конце – совер什ить самоубийство. Если пользователь хочет покинуть игру, куратор начинает угрожать игроку, что найдет его или его семью и навредит им тем или иным способом. Обычно информацию о семье кураторы получают из тех же социальных сетей. Стоит помнить, что детская психика очень восприимчива к угрозам, ребенок может замкнуться и следовать указаниям «куратора», чтобы не навредить своей семье.

Группы смерти также не являются единственным опасным видом групп в социальных сетях. Существуют также группы, посвященные так называемым **«впискам»** - вечеринкам с ночевкой на квартире у одного из участников сообщества. Участники этих групп приглашают «вписаться» к себе или же ищут себе вечеринку по вкусу. Среди участников таких групп огромное количество подростков, которые действительно ходят на тусовки к совершенно незнакомым людям, договорившись об этом через подобное сообщество. Хуже того, после проведенного веселья в той же группе размещаются снимки, сделанные на вписке. Никто не заботится о том, чтобы скрыть лица участников, которые зачастую изображены в сильно подвыпившем состоянии или даже без одежды, не говоря уже о том, что само нахождение ребенка в незнакомом месте с незнакомыми людьми, по меньшей мере, небезопасно.

Согласно исследованиям Лаборатории Касперского 52% родителей в России видят

главную угрозу детской безопасности в интернете в **развитии зависимости**. До того, как ребенка появится необходимость постоянно быть в Сети, у родителей есть возможность разными способами научить его ограничивать время, проводимое онлайн. Это можно делать «по наитию» или использовать ограничение времени работы устройства с помощью специального ПО. При этом психологи подчеркивают, что в этом вопросе очень важна последовательность действий, когда правило фиксируется, и у него нет исключений. С точки зрения развития зависимости самыми опасными являются массовые многопользовательские игры. Здесь нет оконченного сюжета, или он не является ключевым для игрового процесса, зато здесь есть социальные связи, крепче привязывающие ребенка к игре, и возможность вкладывать реальные деньги, что, с одной стороны, бьет по семейному бюджету, а с другой – является дополнительным стимулом продолжать игру, ведь в нее уже столько вложено. Психологи рекомендуют не допускать ребенка к таким играм до 11-12 лет и подтверждают, что такие игры привязывают ребенка в первую очередь отношениями.

Есть несколько пунктов, на которые стоит обратить внимание, если вам кажется, что у ребенка развивается интернет-зависимость, это:

- соотношение времени нахождения в интернете и времени, потраченного на другие занятия и обязанности (правда, с разумным учетом того, что почти все дети пытаются отлынивать от выполнения домашней работы или домашних обязанностей). Ребенок поглощен интернетом, не может остановиться и выйти из Сети;

- настроение ребенка: он успокаивается, радуется, когда в Сети, может ожидать следующего сеанса с приятным предвкушением, при этом раздражен, агрессивен, беспокоен, встревожен или чувствует пустоту и апатию, когда находится вне Сети;

- снижение школьной успеваемости: ребенок всегда хорошо учился, но в последнее время это изменилось, домашние занятия не выполняются или выполняются некачественно, хотя раньше ему было интересно;

- охлаждение отношений с реальными друзьями. Пренебрежение реальными отношениями в пользу интернета – очевидный признак появления зависимости, который может встречаться как у детей со сложностями в установлении отношений со сверстниками, так и у детей, которые легко заводят друзей;

- избыточная реакция ребенка на незначительные события в интернете (количество лайков на фото, комментарии). Ребенок начинает сильно переживать, отслеживать, контролировать процесс, происходящий в Сети: сильно радоваться, когда на его действия в Сети реагируют, или огорчаться, если ожидаемой реакции нет. Социальные сети создают иллюзию 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, проследить, сколько лайков поставили на его фото, а сколько у других;

- физические симптомы: головные боли, боли в спине, сухость в глазах, расстройства сна, снижение физической активности, вялость, бледность – все это более чем серьезные симптомы;

- пренебрежение базовыми потребностями: личная гигиена, сон, питание, потеря аппетита;

- антисоциальное поведение как признак сильной зависимости: ребенок может соврать, оскорбить, ударить человека, который мешает или препятствует его нахождению в интернете.

Помните, что наличие всего одного из перечисленных факторов (исключая разве что агрессию) не говорит о развитии зависимости. Если ребенок имеет несколько хобби и ведет о них блог, переживая за недостаток лайков в нем, это не говорит о том, что у него интернет-зависимость, скорее, он просто сильно вовлечен в свою деятельность. Отслеживать надо именно совокупность нескольких факторов.

Различные интернет-ресурсы являются платными. Более того, **платный доступ** может понадобиться для игры или просмотра фильма. В этом случае дети могут вводить данные банковских карт своих родителей или оплачивать доступ к сайтам через мобильный телефон. При этом некоторые ресурсы списывают деньги «за пользование контентом» не один раз, а ежемесячно или ежедневно. Обязательно проверяйте наличие (отсутствие) платных подписок у ребенка через своего оператора сотовой связи.

Другим большим блоком противоправных действий является разного рода мошенничество по отношению к ребенку. Существуют целевые **онлайн-казино для детей**. Детей «нагоняют» в эти казино популярные видеоблоггеры, чьей целевой аудиторией являются школьники: они прямо рекламируют такие сервисы или рассказывают о своем опыте игры. Принцип работы схож с обычными казинами: на сайтах таких игр есть и рулетки, и игры про открывание сундучков. Такие ресурсы, однако, не блокируются Роскомнадзором, поскольку игра в них идет не на деньги, а на предметы из популярных у подростков игр. Тем не менее эти предметы дети покупают за реальные деньги, а выигрыш можно вывести с помощью специальных сервисов. Чтобы иметь возможность делать высокие ставки в таких казино, некоторые подростки доходят до того, что начинают воровать деньги у родителей, оправдывая это тем, что обязательно вернут, отыгравшись.

Часто именно **дети становятся жертвами мошенников**, которые вымогают у них деньги под различными предлогами. Получив доступ к чужому аккаунту, злоумышленник начинает рассыпать его друзьям сообщения с просьбой срочно положить денег на телефон или перевести незначительную сумму.

Процветают в Сети и различные секты, **экстремистские, националистические и религиозные группы**, чьего влияния в реальной жизни мы также стараемся избежать и защитить от него детей. Участники таких объединений стремятся склонить как взрослых, так и детей к участию в религиозном объединении или, хуже того, к экстремистской деятельности. Такие люди постепенно втираются в доверие к ребенку, чтобы в момент, когда он наиболее уязвим (например, расстался с девушкой или поругался с родителями), попробовать предложить ему идеи, которые «могут помочь». В случае возникновения реальной угрозы ребенку незамедлительно обратитесь в правоохранительные органы.

Злоумышленники, играя на желании ребенка обрести финансовую независимость или помочь семье, могут вовлекать его в различные **незаконные способы заработка**. Как правило, это различные финансовые пирамиды и MLM продажи. Однако иногда ребенка вовлекают в кардинг, то есть снятие денежных средств с краденых банковских карт, за определенное вознаграждение. Другим способом «заработка» может стать подготовка закладок с наркотическими веществами. Подобные случаи уже известны СМИ.

Существуют различные технические средства защиты ребенка от негативной информации в интернете. Во-первых, необходимо установить антивирус, который нужен не только на компьютере, но и на **смартфонах и планшетах**.

Самым же простым способом защитить ребенка от социальных и контентных угроз (то есть тех, которые связаны с содержимым страниц) являются модули «Родительского

контроля» или специальные программы для безопасности детей в интернете.

На сегодня программы для обеспечения безопасности детей в интернете могут помочь родителям в самых разных аспектах онлайн-воспитания. Их можно использовать на **любом устройстве** ребенка.

Что же может такая программа?

1. Избавит детей от неподходящих их возрасту сайтов и приложений. Для этого родителям нужно просто выбрать, какие категории страниц и программ им можно видеть, а какие нельзя, и указать возраст ребенка.

2. Предупредит обо всех попытках ребенка перейти на запрещенный сайт или искать нежелательную информацию в интернете. Если вы пользуетесь специальной программой, вам не нужно учиться просматривать историю браузера и выискивать среди сотен страниц, посещенных ребенком, что-то подозрительное. Программа сама предупредит вас, если ребенок ищет или видит что-то непредназначенное для его возраста.

3. Сообщит, в какие недетские по содержанию группы ВКонтакте вступает ребенок. Интерес ребенка к запретной теме больше не ограничивается веб страницами и поисковиком, теперь дети могут получать ту или иную информацию из групп в социальных сетях.

4. Научит детей правильно распределять свое время и не жертвовать ради нескольких дополнительных минут в интернете сном или приемом пищи. Для этого нужно настроить ограничение времени работы устройства в определенные временные промежутки (например, запрещать работу на время школьных занятий) или на определенное количество часов в день.

5. Пришлет статистику звонков и SMS ребенка на устройстве Android, а также позволит отслеживать изменения количества друзей ребенка в социальных сетях и его публикации через удобный интерфейс. Это позволит предотвратить опасные связи.

Помните главные правила безопасного поведения в интернете и требуйте их соблюдения детьми: сообщать о себе минимум личной информации (настоящее имя, адрес, номер школы, фотографии) и не открывать никаких вложений, поступивших с электронным письмом, за исключением тех случаев, когда вы точно знаете содержимое такого файла.

Даже без установки дополнительного программного обеспечения вы можете посмотреть, какие сайты посещает ребенок. Для этого в браузере нажмите кнопку «журнал» или «история браузера». Также вы можете одновременно нажать комбинацию клавиш Ctrl + H и увидеть, какие сайты посещает ваш ребенок. Однако помните, что ребенок может удалять историю посещений. Поэтому рекомендуется использовать более совершенные технические средства.

Что делать, если ребенок столкнулся с онлайн-грумингом или секстингом?

Во-первых, об этом обязательно следует сообщить в правоохранительные органы: именно они должны заниматься раскрытием преступлений такого рода. Даже если вы считаете, что это не поможет, что преступника не найдут, отбросьте сомнения и подумайте о том, что если злодея не остановить, то могут пострадать и множество других детей.

Чтобы обезопасить ребенка от этой угрозы, мы рекомендуем придерживаться таких правил:

1. Объясните ребенку, что с незнакомцами нельзя говорить не только на улице, но и в Сети.
2. Лучше заранее обсудить с ребенком возможные угрозы и опасности от встреч и

онлайн-общения с незнакомцами и договориться о том, как он будет вести себя в той или иной ситуации.

3. Ребенок должен знать, что никому нельзя отправлять свои эротические фотографии, в т.ч. своим знакомым. Аккаунт друга, с которым вздумалось поделиться интимным снимком, может быть взломан и использоваться другим человеком. Сравнение с реальной жизнью в данной ситуации более чем уместно: ребенок должен понимать, что такие поступки сродни обнажению перед совершенно незнакомым человеком «в реале».

4. Родители должны добавить своего ребенка в друзья во всех социальных сетях, где он общается, чтобы иметь возможность видеть, с кем «дружит» ребенок. С помощью специальных программ можно отслеживать список друзей и сообщения в ленте ребенка, а также контакты, с которыми он общается с помощью телефонных звонков и SMS.

5. Помните: чем раньше вы введете эти правила для ребенка, тем лучше он их воспримет.

Если у ребенка наблюдается интернет-зависимость, то вам необходимо спокойно и без осуждения поговорить с ним об этой проблеме.