Информационная безопасность, или о чем нужно знать родителям!

В период времени с 20 ноября по 20 декабря 2020 года на территории района проводится межведомственное мероприятие «Месяц безопасности в сети Интернет», направленное на профилактику правонарушений несовершеннолетних, предотвращение преступлений, совершаемых в отношении детей посредством Интернет – технологий, а также повышение правовой грамотности, как несовершеннолетних, так и их законных представителей.

В настоящее время, интернет и новые технологии прочно вошли в нашу жизнь. Число пользователей интернета стремительно растет, причем доля молодежи и совсем юной аудитории среди пользователей Всемирной паутины очень велика. К сожалению, в интернет-пространстве можно не только найти полезную информацию, но и столкнуться с рядом угроз. Часто объектом этих угроз в силу своего незнания правил безопасного поведения в интернете становятся дети.

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, группы смерти, секты, мошенники). При этом далеко не всегда дети, сталкиваясь с неприятностями, рассказывают об этом родителям.

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 ПО, посещают порнографические сайты. И в том, и в другом случае ребенок может решить скрыть свои действия от родителей, большинство которых, даже если и догадываются о том, что ребенок рассказывает им не все, не знают наверняка о том, с какими конкретно угрозами ребенок сталкивается.

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.

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 поджидает ребенка в интернете, – возможность доступа к **противоправному контенту**.

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.

Полностью предупредить кибербуллинг может быть трудно, однако не стоит пренебрегать несложным 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 IT-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 – совершить 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 **«вписка**м**»** - 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.

Многие родители видят главную угрозу детской безопасности в интернете в **развитии зависимости**. До того, как у 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.

Есть несколько признаков, на которые стоит обратить внимание, если вам кажется, что у вашего сына или дочери развивается интернет-зависимость:

- 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;

Есть и факторы, которые характеризуют лично ваше отношение ко времени, проводимому ребенком за компьютером. **Прислушайтесь к себе!**

- ваше чувство, когда вы видите ребенка за компьютером: не чувство облегчения («ну, слава богу, ему есть, чем заняться, а я пока отдохну»), а, напротив, злость, раздражение, недоумение, ощущение, что, кроме компьютера, ребенок вообще ничем не занимается;

- вы боитесь вызвать гнев ребенка, поэтому подбираете слова, когда просите его заканчивать, или для собственного спокойствия просто разрешаете ему сидеть за компьютером и дальше.

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.

Другим большим блоком противоправных действий является разного рода мошенничество по отношению к ребенку. Существуют целые **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 обыкновенными казино: 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 рассылать его друзьям сообщения с просьбой срочно положить денег на телефон или перевести незначительную сумму. Поговорите с вашим ребенком о таких ситуациях, чтобы он не попал в неприятности.

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 вашему 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. Обязательно поговорите с вашим ребенком о недопустимости подобного «заработка».

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.

Помните главные правила безопасного поведения в интернете и требуйте их соблюдения вашими 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 ваш ребенок. Для этого в браузере нажмите кнопку «журнал» или «история браузера». Однако помните, что ребенок может удалять историю посещений. Поэтому рекомендуется использовать более совершенные технические средства.

Если у ребенка наблюдается интернет-зависимость, то вам необходимо спокойно и без осуждения поговорить с ним об этой проблеме. Существует простая техника разговора с ребенком:

Шаг 1. Перед разговором подумайте о цели разговора – чего вы хотите? Чтобы ребенок меньше времени проводил за компьютером и телефоном? Наверное, вы переживаете, что он сильно отошел от реальности? Не знаете, что происходит в его жизни? Об этом, конкретном, и надо говорить…

Шаг 2. Выберите время для разговора. Нет смысла подходить к ребенку, когда он в интернете, скорее всего, вы не добьетесь отклика. Дождитесь подходящего момента – перерыва.

Шаг 3. Разговор без обвинения. Искренний, от вашего лица, с фразами от себя: «Дорогой, я все чаще и чаще вижу тебя за компьютером и реже говорю с тобой. Вижу, что тебе интересно там, но, так как это в компьютере, я не понимаю, что это. Не подумай, что я хочу контролировать тебя, мне действительно интересно, что ты делаешь». И вам должно быть интересно, либо не заходите к ребенку с таким разговором. Не обвиняйте интернет,

поскольку он ни при чем. Не нападайте на этого «друга»: вы автоматически попадете в немилость.

Шаг 4. Привлеките ребенка. Предложите совместную деятельность или помощь вам, чтобы ребенок почувствовал свою значимость и нужность.

Помните, **если ваш ребенок стал жертвой противоправных действий или вы подозреваете, что ему что-то угрожает**, при построении разговора существует главное правило: не занимать обвинительную позицию. Необходимо дать понять ребенку, что вы в любом случае на его стороне, — это самое главное. Крайне важно сохранять полное самообладание и не подавать признаков тревоги или волнения, так как дети ориентируются на эмоции взрослых. Если ваши опасения подтвердились, обратитесь к психологу, а также в правоохранительные органы. Помните, что пережитое, даже если для вас это кажется незначительным, – большой стресс для ребенка, которому нужна квалифицированная помощь и ваша поддержка.

Начальник отделения
по делам несовершеннолетних
МО МВД России «Павловский»
К.В. Пермякова

* Материал подготовлен с использованием методических рекомендаций предоставленных Главным Управлением Министерства внутренних дел России по Алтайскому краю