**Министерство образования и науки Республики Дагестан**

**Дагестанский институт развития образования**

**«Безопасность детей в Интернете. Рекомендации родителям»**

**Махачкала, 2020**

Автор-составитель:Пашаев К.И, зав.кафедрой социогуманитарного образования ГБОУ ДПО «Дагестанский институт развития образования»

Стремительное вхождение в жизнь информационных технологий, связанных с использованием компьютера, породило как спектр новых технологических возможностей, так и спектр новых факторов воздействия на психическую организацию современного человека.

Современные школьники существенно отличаются от детей и подростков, обучавшихся в школах 10 -15 лет назад. Сегодня они в дополнение к домашнему компьютеру пользуются различными гаджетами – мобильниками, смартфонами, айподами. Интернет становится важным инструментом социализации подрастающего поколения. Жить в цифровой среде считается престижным. Поэтому дети и подростки усердно постигают азы компьютерной грамотности, а некоторые из ребят в техническом смысле становятся искушенными пользователями. Они уверенно чувствуют себя в киберпространстве, стараются освоить новые технологии практически одновременно с их появлением. Вырастает новое цифровое поколение, вооружённое разнообразными гаджетами и чувствующее себя естественно и непринужденно не только в Рунете, но и в глобальной Сети в целом.

Число пользователей Интернета неуклонно растет с каждым днем, а самыми активными среди них являются молодые люди,подростки и дети. Дополнительными факторами вовлечения молодежи в Интернет стали снижение цены на электронные устройства и тарифы доступа в Интернет. Тенденции к развитию общения в социальных сетях, облачных технологий стирают границу между локальным и сетевым использованием вычислительной техники.

Интернет для детей, рано и интенсивно начинающих им пользоваться, выступает новым инструментом, опосредующим формирование у них высших психических процессов. До начала эпохи новых информационных технологий высшие психические процессыразвивались в непосредственном социальном взаимодействии взрослого человека и ребенка, детей между собой. Сегодня Интернет в значительной степени опосредует такое взаимодействие.У детей, активно пользующихся поисковыми системами Интернета, совсем по-другому начинает функционировать память. В первую очередь запоминается не содержание какого – либо источника информации в Сети, а место, где эта информация находится и способ, как до нее добираться.

Доступность практически любой информации в любое время, с раннего возраста, меняет структуру мнемонических процессов. Память становится не только «неглубокой», но и «короткой» («клиповое мышление»). У детей и подростков формируются другое запоминание, другая память, другие механизмы удержания информации.

Средняя продолжительность концентрации внимания по сравнению с той, что была 10 – 15 лет назад,уменьшилась в десятки раз. Если прежде ребенок на уроке мог удержать внимание в течение 40 минут, и это считалось нормой,то сейчас так сосредоточиться способны буквально единицы.

Особенности внимания, а также процессов восприятия тесно связаны с широко обсуждаемым феноменом «клипового мышления». Оно построено, скорее, на визуальных образах, чем на логике и текстовых ассоциациях, и предполагает переработку информации короткими порциями. Некоторые исследователи рассматривают «клиповое мышление» в качестве защитной реакция на информационную перегрузку учащихся.

В жизни цифрового поколения есть немало преимуществ, обретенных благодаря эпохе Интернета. Взрослым нередко приходится наблюдатьза тем как ребенок, сидя за компьютером, одновременно общается в чате, занимается поиском в Сети, скачивает музыку, отслеживаетобновления, периодически разговаривает по скайпу, пытается делать домашнее задание и при этом пьет сок и жует бутерброд. Такой режим деятельности характерен не только для работы за домашним компьютером – это происходит и на уроках в школе.В современныхусловияхучащимся необходимо приспособиться к более интенсивному темпу жизни. Пользователю необходимо успеть увидеть, совершить иотреагировать на многое. Педагогам и родителям учащихся следует понять суть происходящего и это позволит предупредить возникновение конфликтов.

Глобальная сеть несет и новые риски.Исследователиобычно выделяют четыре вида рисков:

*Контентные риски* возникают в процессе использования находящихся в Сети материалов, содержащих противозаконную, неэтичную и вредоносную информацию.

*Коммуникационные риски* возникают в процессе общения и межличностного взаимодействия пользователей в Сети. Примерами таких рисков могут быть кибербуллинг, незаконные контакты (сексуальные домогательства), знакомства в Сети и последующие встречи с интернет – знакомыми в реальной жизни. С коммуникационными рисками можно столкнуться при общении в чатах,социальных сетях, сайтах знакомств, форумах, блогах.

*Потребительские риски* возникают в процессе приобретения товаров и услуг черезИнтернет. Они включают риск приобретения товара низкого качества, контрафактной и фальсифицированной продукции, риск потери денежных средств без приобретения товара или услуг, хищения финансовой информациис целью мошенничества.

*Технические риски* определяются возможностями повреждения программного обеспечения компьютера, хранящейся на нем информации, нарушения ее конфиденциальности или взлома посредством вредоносных программ.

Ребенок, захваченный безграничными возможностями современных технологий, зачастую не может разглядеть этих рисков в Сети и в результате оказывается среди наиболее уязвимых её пользователей. Сталкиваясь с опасностью при использовании Интернета или мобильной связи, дети часто не знают, как поступить и к кому обратится в такой ситуации, а потому вынуждены действовать методом проб и ошибок. Такая ситуация сформировала понятие об интернет – угрозах, необходимость их распознавать и им противостоять.

Понятие "информационно-психологическая безопасность" определяется как состояние защищенности индивидуальной, групповой и общественной психологии, различных социальных субъектов от воздействия информационных факторов, вызывающих дисфункциональные социальные процессы.

Значительная часть социальной активности современных людей реализуется в рамках взаимодействия в интернет-сообществах и, прежде всего, в социальных сетях. Социальные сети подразумевают общение с людьми, с которыми уже установлены отношения в реальной жизни и предоставляют возможность создания своей реальной личности, размещения подлинной информации о себе. Такое общение предоставляет неограниченные возможности самопрезентации, возможность экспериментирования с собственной идентичностью и перспективы преодоления коммуникативного дефицита и расширения круга общения. Но, в то же время, общение в социальных сетях может угрожать психологическому благополучию пользователей сети Интернет. Прежде всего, следует отметить такие проявления как интернет – аддикция, синдром интернет – зависимости (навязчивое желание выйти в Интернет, находясь off-line, и неспособность выйти из Интернета, будучи on-line).

Аддиктивный потенциал Интернета высок, опасен. Этим опасностям Интернета подвергаются особенно несовершеннолетние. В подростковом возрасте увлечение сайтами с деструктивным содержанием, сетевыми играми с насилием, жестокостью повышают агрессивность, имеют негативные последствия. У подростков проявляется расстройство сна, недомогание, физическая усталость, пренебрежение и невыполнение домашних дел с тем, чтобы больше времени побыть в Интернете, конфликтность. Развитие компьютерных технологий в современном мире способствует распространению компьютерных игр, что оказывает значительное влияние на психическое здоровье и формирование воспитательного пространства подростков. Сегодня игры, помимо компьютера, присутствуют в беспроводных приставках, телефонах, планшетах, гаджетах, приобретая популярность в подростковой среде. Подростки в процессе компьютерной игровой деятельности удовлетворяют потребности в самоутверждении, получая эмоции, от положительных до отрицательных, при минимальных физических затратах.

Обратите внимание на поведение вашего ребенка. Если он проявляет следующие признаки, то стоит задуматься над тем, чтобы проверить его на наличие компьютерной (игровой или интернет) зависимости.

1. Ребёнок уже с утра начинает просить мультики или компьютер. Играет в планшет или с телефоном во время обеда, подготовки домашнего задания.

2. Ребёнок приходит со школы и первым делом садится за компьютер или берёт планшет. Не знает чем себя занять, если нет возможности выйти в Сеть, поиграть на компьютере или планшете.

3. Все свое свободное время ребёнок стремится провести за компьютером, теряет интерес к другим занятиям, игнорирует все дела и свои обязанности.

4. Начинает страдать учеба из-за времени, которое ребенок проводит в Сети. Ребёнок становится более небрежным и рассеянным, в школе жалуются на неуспеваемость, домашние задания остаются не выполненными.

5. Ребенок заводит всё новые знакомства в Интернете и все меньше стремится к общению с другими или общение становиться поверхностным.

6. Общению с близкими и друзьями ребенок начинает предпочитать Интернет, а общение с другими детьми начинают сводиться только к компьютерным играм и общению в Сети.

7. Если у ребенка забирают компьютер, то он выходит в Интернет через телефон. Если нет доступа к Интернету, ребенок становится раздражительным и даже агрессивным.

8. На любые ограничения, связанные с компьютером, планшетом или телефоном, реагирует нервно, сильно переживает, злится, грубит, плачет. Забрать ноутбук или планшет у ребенка удается только со скандалом.

9. Происходит постепенная утрата контакта с родителями, начинает формально отвечать на вопросы, избегать доверительных разговоров.

10. Ребенок скрывает, сколько на самом деле времени провёл за компьютером, начинает обманывать, стремится любыми способами заполучить желаемое.

В период возрастного развития подросткам свойственно стремление к интимно-личностному общению со сверстниками. Неудовлетворенная потребность подростка в эмоциональном общении, являющемся ведущей деятельностью в этот возрастной период, может компенсироваться активным виртуальным общением, нередко перерастающим в патологическое пристрастие.

Подросткам свойственна потребность переживания риска. Склонность к риску связана с возрастными особенностями – импульсивностью, эмоциональной неустойчивостью, экстраверсией, стремлением практически проверять границы дозволенного. В некоторых случаях повышенная склонность к риску объясняется неблагополучием эмоциональной сферы- отражением тревожности и стремлением к агрессивным способам разрешения проблем. Выбирая деструктивную форму деятельности, подросток погружается в мир виртуальной реальности, где у него есть возможности удовлетворения своей потребности к риску.

Важнейшим процессом, происходящим в подростковый период, является развитие самосознания, самооценки. Интерес к себе, качествам своей личности, потребность сравнивать себя с другими, оценивать себя, разобраться в своих чувствах и переживаниях свойственно этому возрасту. Недостаточное признание собственных заслуг в значимой подростковой среде, низкая внешняя оценка в случае незрелости «Я» порождает низкую самооценку и повышает возможность повысить свою самооценку за счет успехов в виртуальной реальности, затратив при этом гораздо меньше ресурсов чем в реальной жизни.

В этойсвязи основной акцент в профилактической работе необходимо ставить на сохранение и развитие условий, которые способствуют сохранению физического, личностного и социального здоровья подростка.

Профилактика Интернет –аддикции подростков является многогранным процессом, требует учета возрастных и личностных особенностей учащихся, социальных условий их жизнедеятельности.

Эффективность работы по профилактике подростковой интернет-аддикции в формировании новых ценностей и социальных отношений зависит от взаимодействия школы и семьи при активном, мотивированном участии подростков в организуемой творческой, учебно-познавательной и воспитательной деятельности.

Также в Сети можно столкнуться с кибербуллингом. Под кибербуллингом обычно понимается неоднократное умышленное агрессивное поведение в Сети как физическое, так и вербальное, направленное против кого-то, кто по каким-либо причинам считается слабее, с целью унижения его достоинства. Это поведение всегда присутствует в подростковой среде.Несмотря на то, что события при интернет-буллинге развиваются в виртуальном мире, отпечаток они накладывают вполне реальный. Влияние травмирующих факторов порой бывает даже сильнее, чем при травле в обычной жизни. Неприятные сообщения, комментарии и публикации постоянно будут давить на жертву. Особенно опасен этот момент для чувствительных людей, склонных мысленно прокручивать одни и те же события, многократно пересматривая травмирующие материалы.

Наиболее популярные формы кибербуллинга в России:

– исключение из общения или групп (носит характер бойкота человека в Интернете);  
– домогательства, при которых одним человеком или группой формируются угрозы и преследование;

– аутинг (от англ. outing – предание гласности), то есть публикация персональных данных без согласия человека;  
– киберсталкинг – одна из самых опасных форм буллинга, когда преследование человека переходит из виртуального мира в реальный, а сбор информации в Интернете используется для запугивания или домогательств;  
– поддельные профили, на основе открытых данных о человеке, создается фейковый (поддельный) аккаунт, и от его имени рассылается ложная, негативная и компрометирующая информация;

– троллинг– намеренная социальная провокация или издевательства в Сети.  
Для многих родителей Интернет представляется безобидным местом, где их ребенок просто развлекается. Многие родители не имеют представления о том, что их ребенок делает в Интернете, какие сайты посещает и какими ресурсами интересуется. Вместе с тем, кибербуллинг в школе встречается чаще других ситуаций для давления на кого-либо. С кибертравлей может столкнуться любой ребенок независимо от возраста, самые сложные случаи приводят к психическому расстройству и даже суициду. В реальном мире иногда сложно травить, потому что жертва может дать отпор. А в Интернете можно относительно соблюдать анонимность и посягать практически на любого.Подростки-недоброжелатели могутзайти с фейковых аккаунтов и рассылать злобные сообщения жертве. Другой вариант, когда дети коллективно создают специальный аккаунт на сверстника, чтобы его травить. Весь класс выкладывает туда неприглядные фото и кажущиеся им смешные истории, которые на самом деле являются очень обидными для конкретного ребенка.В итоге к травле могут присоединиться даже те, кто не знает жертву. Подросткам смешно и весело наблюдать за тем, как кого-то сфотографировали в неприглядной ситуации или нелепой позе, и они с радостью присоединяются к злобному "мейнстриму".Вариантов травли – десятки: от банальных рассылок в WhatsApp в группе, до анонимных угроз и звонков с оскорблениями.

Проблема тех, кто сталкивается с кибербуллингом, заключается в попытке отвечать на вызовы и провокационные вопросы от недоброжелателей.Именно этой реакции ждет инициатор буллинга. Любой ответ и попытка оправдаться вызывают только большее желание написать еще, потому что недоброжелатель видит в этом слабость человека.

Лучшее решение проблемы – не реагировать и игнорировать подобные вызовы и сообщения. Если взрослый человек способен понять это самостоятельно, то ребенку необходима помощь. Эксперты по детской онлайн-безопасности рекомендуют в первую очередь завести аккаунт и "подружиться" в соцсети со своими детьми. Важно посмотреть, какие сообщения появляются у ребенка на стене, какие группы он посещает. Но ни в коем случае не в формате слежки (у ребенка тоже есть право на личную жизнь), а чтобы знать его интересы, потребности и темы, которыми он увлекается.Также сегодня существуют специализированные программы родительского контроля, которые позволяют не только ограничивать детей от потенциально опасных ресурсов, но и фиксировать факты большого количества сообщений и постов ребенка в соцсети. Таким образом, взрослый может со своего телефона видеть объем поступивших ребенку сообщений, не видя их содержимое (соблюдаются права гражданина на тайну переписки). И если наблюдается резкое увеличениеколичества сообщений, то стоит поговорить об этом с ребенком. Важно уделить ему в общении особое внимание.Необходимо выстраивать общение со своими детьми так, чтобы они могли в любой момент к вам обратиться. Что бы ребенку ни писали в соцсети, он должен знать, что у него есть человек, способный его защитить. Тот, кто обладает авторитетом. Это может быть как один из родителей, так и старший брат, сестра или учителя. Психологически комфортная атмосфера в семье должна быть всегда, это вопрос доверия между ребенком и родителем, чтобы в случае опасной ситуации они могли рассказать все друг другу.

Если вы заметили, что ребенок стал тревожным, возбудимым, или, наоборот, замкнулся в себе, у него нарушился сон, аппетит или появились проблемы с мочеиспусканием, обратитесь к доктору. Давление со стороны сверстников может привести как к нервным тикам, так и к глубоким депрессивным состояниям. Психиатры сегодня способны убрать психологические последствия кибербуллинга у детей, научив их аутогенной тренировке или, по-другому, психическому закаливанию. Ребенок должен научиться таким образом ерестраивать свое взаимоотношение с миром, чтобы происходящее вокруг его не травмировало.

Отсутствие доверия и страх наказания – основные причины умалчивания травли, что порой приводит к непоправимым последствиям. Поэтому в защите ребенка от кибербуллинга огромное внимание должно отводиться построению искренних, поддерживающих и близких отношений. Также обязательно проработать с детьми две важных темы:

1.Реальная жизнь интереснее, чем виртуальная. Не игнорируйте постоянное пребывание ребенка в Сети. Такой образ жизни чреват не только повышенными рисками стать объектом травли. Он также опасен формированием тяжелых зависимостей, влекущих за собой ряд серьезных психологических расстройств личности.

2.Только личная встреча позволит составить впечатление о человеке, близкое к истинному положению дел. На примерах донесите ребенку, как легко в сети произвести необходимое впечатление и завладеть доверием в корыстных целях.

Чтобы защитить детей от кибербуллинга в их школьной жизни, как минимум, необходимо разобраться в следующих вопросах:

- деликатно выяснить, какие отношения у ребенка со сверстниками;

- узнать какая работа проводится в школе по профилактикекибербуллинга.

Существует ряд правил взаимодействия с жертвами травли в интернете, знание которых не помешает родителю ребенка:

1.Нельзя давить на человека, заставляя немедленно открыться в своей ситуации и выпытывая подробности произошедшего.

2.Не стоит комментировать чувства, которыми пострадавший с вами поделился, или давать им оценку.

3.Важно проявить принятие и готовность подождать, пока у человека появятся силы изложить все подробности.

4.Важно помочь человеку [избавиться от чувства вины](https://lifemotivation.ru/samopoznanie/chuvstvo-viny) или стыда, которые способны сильно усугубить его состояние.

Взаимодействие в сети Интернет привело к появлению множества «виртуальных миров», субъектами которых являются реальные виртуальные личности, группы и общности. Причиной выхода в Интернет в качестве реальной личности может быть социальная ригидность, самодостаточность. Интенцией к созданию виртуальной личности может служить неудовлетворенность реальной жизнью, пресыщенность реальной жизнью, желание получить новые ощущения, потребность в конструировании иной символической реальности для творческого самовыражения.

В сети Интернет существует проблема «опасного» контента - материалы, которые содержат сцены насилия (фильмы, музыка, изображения) и порнографию. В этой связи упоминаются агрессивные высказывания, комментарии, выражение ненависти, детская порнография а также контент, который может быть определен как оскорбительный.

Также исследователи выделяют такие угрозы, как недостоверная и навязчивая информация, нарушение прав человека, проблема изоляции, утраты «Я» и формирование идентичности, девальвация нравственности, снижение культурного уровня, вытеснение и ограничение традиционных форм общения, негативные социальные влияния.

Информационные потоки, поступающие из СМИ и сети Интернет, носят агрессивный характер и провоцируют разного рода защиты – от ответной, прямой агрессии до рационализаций и сублимаций. Процесс выработки психологических защит у современного человека чаще всего ограничен из-за эмоциональной незрелости, колеблющейся самооценки, разного уровня тревожности которые усиливают либо агрессивные паттерны поведения, либо стремление скрыться, избежать, не участвовать.

Политическая реальность нашей жизни такова, что любые информационно-психологические воздействия, осуществляемые через каналы СМИ или межличностного общения (например, слухи), являются манипулятивными по сути дела, а нередко – и инструментами провокации. И если к манипулятивной природе воздействия электронных СМИ большинство населения привыкло, признает их цивилизованными средствами политико-психологической борьбы, и к ним уже выработан политический иммунитет и приемы личностной психологической защиты, то с анонимными сообщениями, запущенными по Интернету, дело обстоит сложнее.

Серьезную опасность представляет также информация, оскорбляющая общественную нравственность, содержащая недобросовестную рекламу, мошеннические операции и т.п.

Интернет служит весьма удобной площадкой для подготовки и осуществления информационно-террористических и информационно-криминальных действий. В нем могут распространяться пропагандистские материалы преступных организаций, рецепты изготовления взрывчатых и ядовитых веществ, оружия, наркотических и психотропных средств, наконец, изощренных алгоритмов вскрытия шифров. Вся эта информация легко маскируется под научно-техническую информацию. Отсутствие географических границ, трудно определимая национальная принадлежность объектов Сети, возможность анонимного доступа к ее ресурсам – все это делает уязвимым системы общественной и личной безопасности.

**Памятка родителям по обеспечениюбезопасности школьников в сети Интернет**

*Советы по безопасности работе в общедоступных сетях Wi-fi:*

- не передавать личную информацию через общедоступные Wi-Fi сети, работая в них, желательно не вводить пароли доступа, логины и какие-то номера;

- использовать и систематически обновлять антивирусные программы;

- при использованииWi-Fi отключить функцию «Общий доступ к файлам и принтерам»;

- использовать только защищенное соединение; при наборе веб-адреса вводи «https://».

*Основные советы по безопасности в социальных сетях:*

- ограничить список друзей; он не должен включать случайных и незнакомых людей;

- защитить свою частную жизнь; не указывать пароли, телефоны, адреса и другую личную информацию;

- защитить свою репутацию;подумай, прежде чем что-то опубликовать, написать и загрузить;

- старайся не разглашать свое реальное имя и другую личную информацию в разговоре с незнакомыми людьми;

- избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;

- используй сложные пароли при регистрации в социальной сети;

- используй различные пароли для социальной сети, почты и других сайтов и в этом случае возможные злоумышленники получат доступ только к одной информации, а не ко всем сразу.

*Основные советы по безопасной работе с электронной почтой:*

- выбери правильный почтовый сервис;

- не указывай в личной почте информацию о себе;

- выбери сложный, надежный, устойчивый пароль для каждого почтового ящика;

- используй несколько почтовых ящиков и первый среди них для частной переписки с адресатами, которым ты доверяешь (этот адрес не стоит использовать при регистрации на форумах и сайтах);

- не открывай неизвестные файлы, уточни у друзей отправку писем к вам.

*Основные советы для безопасности мобильного телефона:*

- будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги;

- подумай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?

- не загружай приложения от неизвестного источника, они могут содержать вредоносное программное обеспечение;

- сообщай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь;

- bluetooth должен быть выключен, когда ты им не пользуешься.

*Основные советы по борьбе с фишингом (интернет-мошенничеством, главная цель которого состоит в получении конфиденциальных данных пользователей — логинов и паролей).*

- cледи за своим аккаунтом, если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;

- используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;

- используй сложные и разные пароли. Таким образом, если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в Сети, а не ко всем;

- если тебя взломали, то необходимо предупредить всех своих знакомых, которых ты добавил в друзья, о том, что тебя взломали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты;

- не открывай файлы и другие вложения в письмах даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы.

*Основные советы по защите цифровой репутации:*

– Цифровая репутация - это негативная или позитивная информация в Сети о тебе. Компрометирующая информация размещенная в Интернете может серьезным образом отразиться на твоей реальной жизни. Твое место жительства, учебы, твое финансовое положение, особенности характера и рассказы о близких – все это накапливается в Сети. Комментарии, размещение твоих фотографий и другие действия могут не исчезнуть даже после того, как ты их удалишь. Ты не знаешь, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли она, а главное: что подумают о тебе окружающее люди, которые найдут и увидят это.

- подумай, прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети;

- в настройках профиля установи ограничения на просмотр твоего профиля и его содержимого, сделай его только «для друзей»;

- не размещай и не указывай информацию, которая может кого-либо оскорблять или обижать.