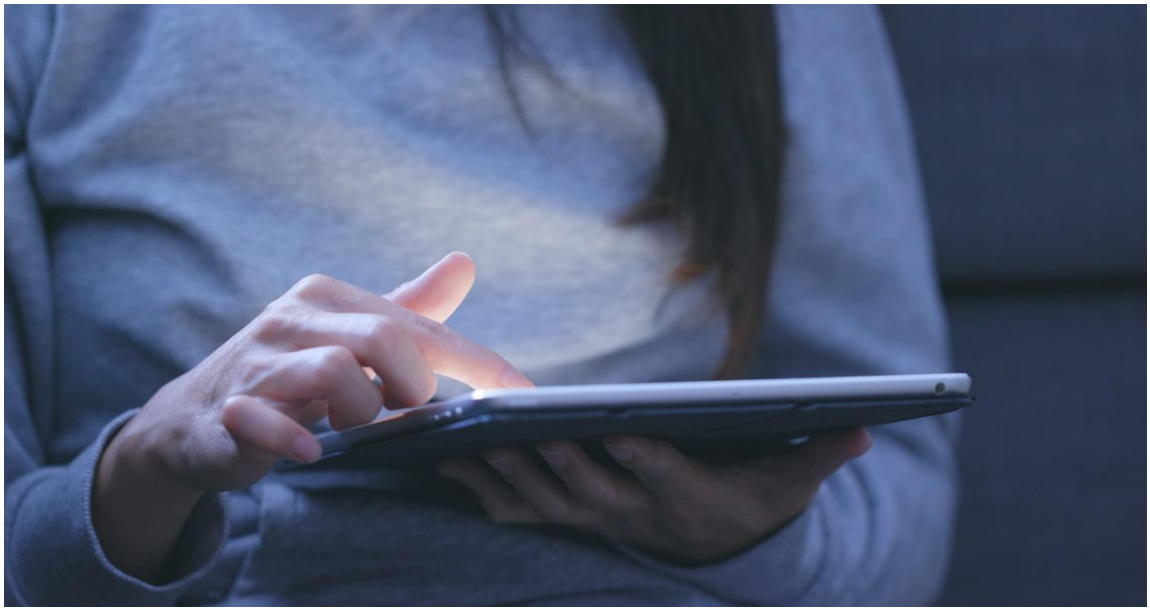
Информационная безопасность ребёнка: комплексный подход к проблеме

23.09.2020



Согласно отраслевому докладу «Детский Рунет 2019», большая часть родителей считает главной угрозой для детей в интернете порнографию и эротический контент. Также опасения взрослых вызывают суицидальный контент и публикации, содержащие жестокость и агрессию. При этом 79% родителей следят за тем, что их дети дел

Однако проблема информационной безопасности представляется современным исследователям шире, она включает в себя изучение интернет-зависимости, формирование критического мышления и даже вопросы дистанционного образования.

По просьбе АНО «ЦИСМ» ведущий эксперт в области информационной безопасности, доцент кафедры юридической психологии и права факультета юридической психологии МГППУ кандидат психологических наук Елена Шпагина ответила на вопросы, связанные с проблемой.

С разрешения автора публикуем эссе, которое может быть полезным широкому кругу читателей – от специалистов, занимающихся вопросами сетевых угроз, до родителей и педагогов, желающих получить глубокое представление об этом направлении.

– Как приучить ребёнка к соблюдению правил информационной безопасности?

– Чтобы родители или педагоги смогли помочь ребёнку выработать необходимые навыки, им самим нужно представлять, что такое «информационная безопасность» детей (или личности) в целом. Я подразумеваю под информационной безопасностью личности не только правила пользования цифровыми технологиями, но и потребление информации в целом. Запрет информации, направленной на развитие ребёнка – это тоже нарушение информационной безопасности. Важно научить детей получать, воспринимать, анализировать и выбирать информацию, нужную для развития, принятия решений, понимания причинно-следственных связей.

Для каждого возраста будет свой подход. Например, в дошкольном возрасте важно знакомство с окружающим миром через овладение предметной деятельностью и получением разнообразной информации именно таким образом: фактуры, формы, цвета и запахи и, конечно же, речь окружающих людей, эмоции. На это направлены такие методики, как школа Монтессори, Вальдорфская школа, об этом писал Л.С. Выготский. Конечно, проще включить мультфильм и пойти заниматься своими делами… Но тогда развитие будет неполным. Я не против мультфильмов. Это дополняет и развивает. Я против подмены общения родителя с ребёнком виртуальными формами в таком возрасте. Развитие должно проходить через реальный предметный мир с помощью взрослого. Абстрактное восприятие придёт, но чуть позже.

Я бы сравнила процесс обучения правилам информационной безопасности с процессом питания ребёнка. Если родитель хочет, чтобы ребёнок рос здоровым, он будет выбирать экологически чистые и непросроченные продукты, соблюдать режим питания, контролировать количество потребляемой пищи. Мы (взрослые и опытные) должны предостеречь ребёнка от употребления ядов: «Стоп! Это мухомор! Его есть нельзя». Так и с информацией. Научить выбирать, критически относиться, проверять информацию. И показать путь к прекрасному, полезному: науке, искусству, технологиям. В любом возрасте – это диалог ребёнка с родителем. Всё уже есть в педагогике, психологии: нужно только адаптировать эти знания к использованию в современных условиях, когда цифровые технологии так прочно вошли в повседневную жизнь, просто ускорив и упростив процессы получения, распространения информации.

– Как быть с детьми, у которых такого диалога нет (его либо никогда не было, либо он утрачен)?

– Такие функции должно взять на себя государство в системе просвещения и образования. Должны быть программы, проекты, направленные на развитие у детей навыков получения информации и продуктивного безопасного использования её. Такие программы на государственном уровне существуют во многих странах, где в образовательный процесс включены занятия, которые подразумевают как обучение продуктивному использованию цифровых технологий в повседневной жизни ребёнка, так и вопросы, связанные с рисками. В нашей стране такие проекты реализовывались (например, «Единый урок информационной безопасности»), но, к

сожалению, не на регулярной основе. Кроме того, такие моменты нужно включать в информационную продукцию для детей: фильмы, игры. Как, например, это делает «Лаборатория Касперского», выкладывая в сеть интересные ролики про безопасность в виде мультфильмов.

– В каком возрасте современные дети начинают осознанно пользоваться социальными сетями и интернетом?

– Осознанно – значит обдуманно, преднамеренно. Канадский педагог Билл Белси, президент и основатель организации Bullying.org, отмечает, что современные подростки и молодые люди должны быть «всегда на связи». Это иллюстрируют и недавние опросы. Выпускница нашего факультета делала исследование с использованием методики определения киберзависимости. Результаты показали, что больше 80% респондентов (*исследование проводилось среди школьников*) склонны к зависимости. Мы пришли к выводу, что методика 2000-х годов устарела, и те результаты тестирования, что раньше показывали зависимость, сейчас являются скорее нормой.

Здесь уместно сравнение с ездой на велосипеде… Вы сознательно на нём катаетесь? Нет, – это навык. Если что-то умеешь, то уже не задумываешься. Просто многие (и взрослые в том числе) вообще не представляют себе жизнь без телефона и интернета. Это просто уже часть тебя. Учёные (*например, Тхостов А.Ш., 2011*) называют это явление «инвалидизацией». Мы отдали часть функций техническому устройству: компьютеру или мобильному телефону. Во всяком случае память свою мы ему уже точно отдали. Я психолог и люблю наблюдать за людьми, например, в метро: у всех «глаза в смартфонах». А молодые люди всё время пишут – смотрят ответ, получают послание – пишут ответ… Не так давно я читала исследование ВШЭ (*Бочавер А. А., Докука С. В., Новикова М. А, Сивак Е.В., Смирнов И.Б., 2019*), где говорится о том, что современный школьник смотрит в смартфон на уроке каждые 6 минут. Так что это скорее навык, и этот навык приобретается всё раньше и раньше… А вот как будет использоваться технология – это вопрос осознанности. Многие программы в мировой практике по обучению детей информационной безопасности как раз и направлены на формирование у детей критического мышления по отношению к информации, получаемой из интернета, и навыкам самовыражения и самопрезентации в той же сети. Вопрос осознанности и понимания целей во взаимоотношениях человека и компьютера – это глобальный философский вопрос современности. А зачем эта цифровизация нам? А не поработят ли нас роботы? Здесь я согласна с теми, кто говорит, что это управляемый процесс и что мы сами заложим в технологии, то они и будут делать (*например, Ускова О.А., заведующая кафедрой инженерной кибернетики НИТУ МИСиС*). То есть цифровизацию нужно сочетать с гуманизацией.

Если обратиться с вопросом осознанности к юридической психологии детей и подростков, то способность к осознанной саморегуляции формируется у человека к концу подросткового периода, продолжающегося от 11-12 до 14-15 лет

(*Дозорцева Е.Г., 2004*). На этом основывается и обоснование возраста уголовной ответственности в нашей стране (с 16 лет, а за некоторые правонарушения с 14 лет).

– Насколько остро стоит проблема информационной безопасности детей в России и мире? Какие глобальные сетевые угрозы можно выделить?

– В Европе наиболее известные и крупномасштабные исследования проводились в рамках проекта Сони Ливингстон, Курсат Кагилтай и Кьяртан Олафссон. В рамках проекта «EU Kids Online» в 25 европейских странах были взяты интервью у детей и родителей об использовании интернета детьми: о деятельности и навыках; о рисках использования Сети, с которыми они столкнулись; об осведомлённости родителей об этих проблемах и стратегиях поведения по обеспечению безопасности. В каждой стране были отобраны репрезентативные по национальному признаку выборки исследований, в фокусе которых были дети в возрасте 9-16 лет вместе с одним из родителей (1000 пар «ребёнок/родитель» в стране). Вопросы были в основном закрытыми, с открытым (качественным) элементом и с деликатными вопросами, которые ребёнку задавали наедине.

Дизайн исследования опирался во многом на сравнение различных групп и параметров. Во-первых, сравнение выборки между странами для выявления национальных сходств и различий путём проверки ряда гипотез, полученных из обзора литературы (*Hasebrink, Livingstone, Haddon & Ólafsson, 2009*). Также опрос касался рисков, с которыми сталкиваются дети в интернете: вопросы, касающиеся запугивания, онлайн-порнографии, сексуальных сообщений («секстинг»), предложений об онлайн-контактах («опасный незнакомец»). Наконец, исследование носило сравнительный характер в стремлении выявить сходства и различия в зависимости от возраста, пола и социально-экономического положения ребёнка.

Вопросы касались возможностей использования, онлайн-активности и имеющихся у детей навыков, факторов риска и понимания их вреда, а также стратегий преодоления риска детьми и стратегий посредничества родителей.

Обобщённые результаты этого исследования переведены на русский язык в статье Михалевой Г.В. Выявлены следующие риски для детей, использующих интернет:

– небезопасное содержание того или иного сайта (небезопасный медиаконтент);

– потенциальная угроза неприемлемого контакта (виртуального или реального) юного пользователя с небезопасным медиаконтентом или виртуальным знакомым;

– угрозы, исходящие от других пользователей в интернете;

– угрозы, заложенные разработчиками вредоносных программ, кибератаки (кибертерроризм);– угрозы, связанные с причинением вреда здоровью пользователей, разные формы интернет-зависимости.

Данный проект позволил доказать, что пользователи с более высоким уровнем цифровой компетенции сталкиваются с бóльшим объёмом онлайн-рисков. Кроме того, они с вероятностью 30 – 45 % более подвержены риску столкнуться с

вышеперечисленными рисками (*Livingstone, 2013*). Дело в том, что цифровая грамотность и высокий уровень владения компьютерной грамотностью, и даже достаточный опыт работы в интернете не гарантируют защиту пользователя от потенциального риска и связанного с ним вреда, так как главный вопрос заключается не в том, как часто или как долго пользователь появляется в Сети, а каким образом он/она работает в интернете. Иначе говоря, речь идёт о медиакомпетентности личности, которая отличается от сугубо практической компьютерной/цифровой грамотности пользователя.

Говоря об информационной безопасности детей в России и мире, нужно обратиться к работам Галины Солдатовой, директора Фонда Развития Интернет, которая выделяет:

– *контентные риски,*
– *коммуникационные риски,*
– *технические риски,*
– *потребительские риски,*
– *интернет-зависимость.*

Статистика обращений на линию помощи «Дети Онлайн» по типу рисков за 8 лет работы (2009-2016 гг.) выделяет наиболее частые обращения по поводу коммуникационных рисков (41%) и технических (32%). И самая часто встречающаяся проблема – это агрессия в интернет-коммуникациях. Особенно стоит выделить кибербуллинг или травлю в интернете. Последствия кибербуллинга для подростка, ставшего жертвой: социальная изоляция, развитие форм асоциального поведения, тревожные расстройства, депрессивные состояния, психосоматические симптомы (нарушение сна, плохой аппетит, головная боль и т.д.), посттравматическое стрессовое расстройство, риск суицидального поведения. Каждый второй продолжает думать об опыте школьного буллинга во взрослой жизни (*Солдатова Г.В., 2017*). Также установлено, что различные виды кибербуллинга имеют значимые связи со склонностью к аддиктивному поведению, в меньшей степени к делинквентному поведению и склонности к преодолению норм и правил (*Дозорцева Е.Г., Кирюхина Д.В., 2020*). То есть некоторые виды насилия перешли в виртуальную форму и ранят не меньше, чем в реальности, и могут приводить к летальному исходу (например, суициду).

Также нужно обратить внимание на контент, который влияет на социализацию молодёжи. «Киберсоциализация» – термин, который уже прочно вошёл в работы учёных (*Плешаков В.А., 2012*). Это говорит о том, что современные подростки черпают информацию о правилах общественной жизни, взрослеют и формируют правосознание именно посредством сети Интернет. Поэтому государству очень важно контролировать эту сферу контентных рисков.

Ещё одна проблема, подсвеченная карантином в связи с пандемией, – это переход образования в цифровую среду или «цифровизация» образования. Важно понять, каково качество такого образования? С какого возраста оно эффективно и приемлемо? Пока, те психологи и психиатры, работы которых я читала, говорят, что

для взрослых использование IT-технологий – во многих случаях благо, а вот развитие детей нужно начинать через предметную деятельность и общение со взрослым. Конечно, мир меняется очень стремительно в связи с прогрессом и цифровизацией. Наличие цифровых навыков – это залог успешности в будущем и, как показал опыт этого года, и в настоящем. Этот вопрос очень остро стоит перед образованием: каким компетенциям отдать предпочтение: цифровым (опосредованным интернетом) или тем, что требуют непосредственного контакта с объектом будущего труда.

– Насколько современное образование готово к воспитанию детей в рамках глобальной цифровизации? Насколько учителя компетентны в сфере детской интернет-безопасности?

– Пандемия поставила все субъекты образовательного процесса (ученики, их родители и учителя) в ситуацию шокового освоения инноваций в области цифровых технологий. Конечно, уже были педагоги, которые активно и эффективно использовали цифровые технологии в своей работе как вспомогательное средство в обучении. Электронные учебные комплексы создаются в вузах уже давно. Существует много информационных образовательных ресурсов, которые используют родители, выбравшие для своих детей домашнее обучение (закон «Об образовании» позволяет это сделать), а также родители «особенных детей». Потребность в этом есть со стороны родительского сообщества. Но нужно сознаться, что в первые месяцы на карантине для многих образовательный процесс был сильным стрессом, особенно для родителей и детей младших классов, так как они не были готовы в таком объёме «переварить» информацию в цифровом виде. Многие из них не имели таких развитых навыков в этой области. Задания во многих случаях не соответствовали возрасту и ситуации, не были тщательно продуманы, и дети не могли усвоить тех знаний, которые им нужны, чтобы двигаться дальше в своём развитии. Препятствие на пути получения необходимой информации – это тоже угроза.

– Перейдём к воспитательному процессу. Насколько учителя осведомлены о рисках сети Интернет?

– Отвечу на этот вопрос с помощью результатов исследования своих коллег по МГППУ. Изучение представлений на тему информационной безопасности детей было проведено в нескольких работах учёных факультета юридической психологии МГППУ (*И.Б. Бовина, Н.В. Дворянчиков, С.В. Будыкин, С.Ю. Гаямова, А.В. Милёхин*), посвящённых изучению обыденных представлений родителей и учителей об информационной безопасности детей и подростков.

Исследование было выстроено вокруг следующих восьми категорий в области информационной безопасности детей, которые можно объединить в две большие (угрозы информационной безопасности и способы защиты): пути обеспечения безопасности; традиционные и новые медиа; угрожающая информация; безопасность информации; ответственность родителей и учителей; закон об информационной безопасности детей; защита персональных данных;

профилактические и образовательные программы по обеспечению информационной безопасности детей.

В результате проведённого исследования были получены следующие выводы о «наивных представлениях» родителей и учителей о категориях в отношении информационной безопасности детей:

– Родители и учителя сходным образом понимают такой конструкт как «угроза информационной безопасности детей и подростков». Иерархия угроз выглядит следующим образом: первое место – насилие; второе место – психоактивные вещества и их использование; третье место – информация сексуального характера; четвёртое место – информация о действиях, нарушающих нормы и правила.

– Родители и учителя сходным образом понимают последствия информационного воздействия негативной информации на детей, которые обобщаются в представлениях как: вред здоровью и развитию детей, возникновение травмы; возникновение изменений в поведении в результате подражания.

– Иерархия источников негативной и опасной информации в обеих группах: интернет, телевидение, сверстники (в отношении детей); интернет, сверстники, телевидение (в отношении подростков).

– Обе группы едины во мнении, что «основная ответственность по обеспечению информационной безопасности лежит на родителях».

– Родители «ожидают от учителей обучения школьников правилам безопасности и поведению при столкновении с опасной информацией».

– Учителя ожидают от родителей контроля за доступом к информации и ограничения этого доступа.

Интерес представляет и разработанная авторами методологическая стратегия скриптов, которая выражалась в том, что респондентам (родителям) предлагались ситуации, связанные со столкновением детей и подростков с угрожающей информацией трёх самых опасных направлений: наркотики, порнография, самоубийство. Респонденты должны были предложить стратегию обеспечения информационной безопасности детей и подростков в случае столкновения с угрожающей информацией.

Результаты исследования можно обобщить одной фразой: родители не имеют конструктивных стратегий на этот счёт. Например, «для объяснения угрозы той или иной информации (случай с употреблением наркотиков) родители предлагали продемонстрировать детям десятилетнего возраста видеоматериалы о смерти наркоманов»; «ситуация просмотра материалов порнографического характера подростками вызывает у родителей смущение и отсутствие коммуникативной стратегии обсуждения сложившейся ситуации»; в случае с обнаружением у подростка брошюры о совершении самоубийства «респонденты скорее отвергают саму ситуацию, чем демонстрируют определённый скрипт поведения в ней».

На следующем этапе исследования, направленном на изучение социальных представлений учителей в отношении обеспечения информационной безопасности детей, было выявлено, что «…в целом практически отсутствует сложное решение (многошаговое, продолжительное по своей форме реализации) проблемы, респонденты исходят из идеи того, что проблемная ситуация может быть решена в одно действие и не требует последующего контроля поведения ребёнка. Преобладание нормативных, предписывающих элементов над функциональными говорит в пользу того, что учителя едва ли имеют стратегию обеспечения информационной безопасности, которую они используют в повседневной жизни».

– Возможно ли обучить педагогов работе в современных реалиях? На чём в первую очередь нужно делать акцент?

– Учителя на самом деле – лучшие ученики! Я верю в потенциал учителя, все они искатели и новаторы в душе…

Любые новшества нужно начинать с просвещения и обучения, тогда это не будет восприниматься «как испытание новизной» и «психологические барьеры» по отношению к новому исчезнут. Учителя и сами понимают, что мир меняется и нужно меняться вместе с молодым поколением, своими учениками. Но меняться трудно, даже если хочется!

Я считаю, что небольшой курс по информационной безопасности детей должен включаться в образовательные программы при подготовке современных учителей. А для уже опытных учителей нужны курсы по переподготовке, повышению квалификации (тем более что законодательная база для повышения квалификации есть).

Приведу ниже результаты собственного исследования. Оно касалось пожеланий педагогов и психологов относительно вопросов, которые они хотели бы изучить в области информационной безопасности детей.

Наибольший интерес вызывают следующие вопросы обучения:

– построение доверительных детско-родительских отношений в вопросах информационной безопасности;

– профилактика и работа с кибербуллингом;

– проблема предостережения детей от опасных знакомств посредством сети Интернет;

– обучение детей работе с информацией СМИ;

– обучение критичному поиску и использованию информации;

– обучение детей самостоятельному контролю за обеспечением информационной безопасности;

– проблема кибераддикции: преодоление зависимости;

– влияние гаджетов на психику;

– методы просвещения педагогов и преподавателей в области информационной безопасности детей;

– юридическая грамотность и компетентность в области информационной безопасности детей;

– коррекционная работа с последствиями нарушений информационной безопасности;

– польза интернета, развитие интересов детей, показ новых возможностей.

Сама же я считаю, что подготовка учителей, педагогов и психологов в области информационной безопасности детей должна касаться трёх основных направлений:

– юридическая подготовка (вопросы обработки персональных данных; обоснование запретов и экспертизы информации, предназначенной для детей);

– организационно-техническая подготовка (элементарные навыки, связанные с техническими аспектами: например, средства родительского контроля или технологии блокировки нежелательного контента);

– психолого-педагогические методы обеспечения информационной безопасности детей.

Приоритет, конечно, следует отдать обучению психолого-педагогическим методам.