

Безопасность школьников в информационном обществе

Осенью прошла Всероссийский неделя кибербезопасности несовершеннолетних, на которой у меня была возможность учиться, этими материалами сегодня хочу поделиться с Вами.

Особенностью современного этапа развития информационной сферы является её распространение и объединение с помощью информационно-телекоммуникационных технологий в единое мировое (глобальное) информационное пространство, и, безопасности самого человека.

Несовершеннолетний ребёнок является активным участником информационных отношений.

Специалисты констатируют, что «дети и молодежь не просто идут в информационном фарватере, в недалеком будущем они станут его главными действующими лицами, будут прокладывать центральный курс развития человечества». Интернет-пространство является частью социальной среды ребёнка, который получает объём информации из открытых источников самостоятельно. Здесь важно подчеркнуть, что если в дошкольном и младшем школьном возрасте ребёнок контактирует с информационными ресурсами, в сопровождении взрослых, в связи с чем поступающая информация подвергается «родительскому фильтру», то уже в средней школе круг информационных ресурсов ребёнка значительно расширяется, что минимизирует родительский контроль за поступающей к ребёнку информацией. По данным сайта «Интернет-контроль: сайт для умных родителей», детская аудитория пользователей интернета сегодня составляет почти 9 млн детей в возрасте до 14 лет, 75% которых пользуются сетью без контроля со стороны взрослых¹. С одной стороны, несовершеннолетние с большей легкостью, чем их родители, адаптируются в информационном пространстве, с другой — результаты исследований последних лет позволяют утверждать, что, погружаясь в современное информационное пространство,

несовершеннолетний попадает в небезопасную для него среду, противостоять которой он не в состоянии в силу возрастных особенностей формирующейся личности.

Рассмотрим наиболее вероятные риски и угрозы безопасности несовершеннолетнего ребёнка, которые могут возникнуть в связи с его погружением в современную информационную среду.

Заслуживает внимания классификация интернет-рисков, или «онлайн-рисков», предложенная в 2012 году Организацией экономического сотрудничества и развития предложила классификацию интернет-рисков для школьников:

первая группа — *контентные риски*, возникающие в процессе использования находящихся в Сети материалов (текстов, картинок, аудио- и видеофайлов, ссылок на различные ресурсы), и содержащие «противозаконную, неэтичную и вредоносную информацию (насилие, агрессию, эротику или порнографию, ненавистнический контент, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр, наркотических веществ и т. д.)»;

вторая группа — *коммуникационные риски*, возникающие в процессе общения и межличностного взаимодействия пользователей в Сети (среди примеров ученые называют: кибербуллинг, незаконные контакты (например, онлайн-груминг- формирование доверительных отношений с ребенком с целью получить его интимные фото и видео, для вымогания дальнейших интимных встреч), знакомства в Сети и последующие встречи с интернет-знакомыми в реальной жизни);

третья группа — *потребительские риски*, возникающие в результате злоупотребления в интернете правами потребителя (риск приобретения товара низкого качества, различных подделок, контрафактной и фальсифицированной продукции; потерю денежных средств без

приобретения товара или услуги; хищение персональной информации с целью мошенничества);

четвертая группа — *технические риски*, которые определяются возможностями реализации угроз повреждения программного обеспечения компьютера, хранящейся на нем информации, нарушения ее конфиденциальности или хищения персональной информации посредством вредоносных программ (вирусы, «черви», «троянские кОни», шпионские программы, боты и др.);

пятая группа — *риски приобретения интернет-зависимости* или непреодолимой тяги к чрезмерному использованию Интернета, которая у несовершеннолетних проявляется в форме увлечения видеоиграми, навязчивой потребности в общении посредством мессенджеров, социальных сетей и форумов, онлайн-просмотре видео, фильмов и сериалов. Среди основных симптомов интернет-зависимости учеными выделяются: потеря контроля над временем, проводимым в сети (рекомендуют использовать таймер); синдром отмены («ломка»); замена реальности.

По результатам исследований фирмы «Лаборатория Касперского» основные риски, которые видят сами родители для их несовершеннолетних детей при использовании Интернета, можно разделить на несколько групп²: риск взаимодействия с порнографическим контентом, на втором месте — сцены насилия, и на третьем, с прошлого года — группы смерти; риск общения с незнакомыми людьми; риск негативного влияния интернета на здоровье (зрение, осанка); риск наступления интернет-зависимости и др. Это очень ограниченный перечень представлений родителей об интернет-угрозах.

Рассмотрим варианты возможных рисков и угроз для несовершеннолетнего ребёнка, связанные с бесконтрольным погружением в информационное коммуникационное пространство.

² URL: <http://www.pravmir.ru/deti-v-internete-4-glavnyihopasnosti-i-kak-ot-nih-zashhititsya> [Электронный ресурс]. (дата обращения: 21.03.2020)

Первая группа рисков связана с получением деструктивной информации, которая может негативно повлиять на психическое, духовное, нравственное здоровье³ и развитие несовершеннолетнего.

Полагаем, что деструктивная для несовершеннолетнего ребёнка информация представляет собой информацию (аудио-, видеоконтент), направленную на разрушение принятых в обществе нравственных ценностей и моральных установок, в т. ч. содержащая элементы жестокого обращения с человеком (или животным), сцен агрессии, насилия, причинения боли, страданий, а также информация, содержащая недостоверные сведения, способная ввести в заблуждение несовершеннолетнего.

Анализируя негативное влияние интернет-контента на нравственное воспитание несовершеннолетних, специалисты по детской интернет-безопасности отмечают, что в настоящее время «появляются тысячи сайтов, которые призывают причинить себе боль и вред», в том числе «каждый четвертый ребенок заходит на сайты о диетах, а учитывая, что это в основном девочки, то каждая вторая из них пытается это использовать, порой во вред своему здоровью» [21, с. 21]. Безусловно, при просмотре подобного информационного контента, в отсутствие рядом взрослого «проводника» (родителя, воспитателя, учителя и т. д.), способного грамотно преподнести несовершеннолетнему увиденные сюжеты, ребёнок может полагать, что увиденные модели поведения приемлемы и в реальной жизни.

В случае отсутствия фильтров несовершеннолетний ребёнок имеет доступ к неограниченному количеству информационных ресурсов.

Вторая группа — риски, связанные с вовлечением несовершеннолетнего в противоправную деятельность посредством сети Интернет.

С учетом возрастных особенностей ребёнок постепенно расширяет объем взаимодействия с информационной интернет-средой, к поисковым

³ В рамках данной публикации мы не рассматриваем группу рисков для физического здоровья несовершеннолетних, получившие достаточно широкое освещение в работах психологов, медиков, специалистов в сфере охраны здоровья несовершеннолетних (физическое переутомление, нервное напряжение, снижение работоспособности, снижение зрения, изменение осанки, увеличение массы тела и др.)

запросам информации добавляются возможности установления новых контактов с виртуальными собеседниками, в т. ч. посредством социальных сетей (ВКонтакте, Facebook и др.). Общение несовершеннолетних друг с другом и внешним миром происходит в виртуальной реальности. Психологи утверждают, что пространство социальных сетей для подростка одновременно связывается с автономностью от взрослых и с ощущением возможности проявления собственной активности и свободы в выборе содержания и форм общения [27, с. 5]. Тем самым Интернет представляет альтернативную коммуникационную площадку для несовершеннолетних, где, в отсутствии визуализации собеседника, они имеют возможность общаться, обмениваться информацией, выражать мнение, рассчитывать на поддержку виртуального сообщества (собеседника), в связи с чем чувствовать себя полноценно, уверенно и комфортно.

Само по себе общение не представляет опасности, если не нарушаются нормы дозволенного. С одной стороны, виртуальное общение удобно для самих несовершеннолетних. Особенности психики детей и подростков характеризуются наличием, в той или иной степени, определенных комплексов и фобий, низкой самооценки, неуверенности в собственных силах (внешности, знаниях, социальном положении и т. д.), что часто препятствует полноценному общению со сверстниками вне виртуального пространства; данная форма общения является предпочтительнее визуальной формы межличностного взаимодействия. По данным исследования «Дети России онлайн», почти треть опрошенных детей и подростков признались, что хотя бы раз представлялись в сети другим человеком, причем каждый шестой из опрошенных детей делал это достаточно часто [15]. Таким образом, несовершеннолетний отдает предпочтение виртуальной самореализации, нежели традиционным способам взаимодействия со сверстниками.

Виртуальное общение становится опасным в тех случаях, когда оно выходит за рамки обычного общения, содержит элементы агрессии,

незаконного давления (психического, эмоционального и т. д.) на несовершеннолетнего.

Бесконтрольное неограниченное нахождение в Сети оказывает на несовершеннолетнего психотравмирующее и порой растлевающее влияние, что в результате может привести к различным формам асоциального поведения.

Современное информационное пространство, имеющее большой охват аудитории, часто используется преступным сообществом для распространения криминальной субкультуры. Специалисты отмечают массовое вовлечение несовершеннолетних в противоправную деятельность экстремистских организаций, где подростки становятся доступной добычей взрослых манипуляторов, пропагандирующих насилие, возбуждение ненависти среди молодежи, растление малолетних [28]. Подобные организации культивируют в сети положительный образ экстремиста, террориста, преступника, что может вызвать у несовершеннолетнего желание подражать и быть одним из них.

По данным исследований, проведенных Фондом развития Интернет в 2018—2020 годах, выделяются следующие разновидности деструктивного поведения несовершеннолетних в цифровой среде:

- различные формы киберагрессии, в том числе кибер-буллинг;
- деятельность экстремистских сообществ;
- популяризация и распространение способов деструктивного поведения (А.У.Е., криминализация, алкогольная и наркотическая зависимость);
- пропаганда самоповреждающего (анорексия, селфхарм-самоповреждение, без суицидальных намерений) и суицидального поведения;
- целенаправленное распространение негативного поведения онлайн и призыв к асоциальному поведению офлайн⁴.

⁴ Комплексная программа профилактики деструктивного поведения в интернете у подростков и молодежи (2019 г.) [Электронный ресурс]. URL: <http://detonline.com/research/20172019> (дата обращения 20.03.2020).

Несколько лет назад большой популярностью среди подростковой аудитории России и Украины пользовались сюжеты, снятые самими несовершеннолетними и распространяемые в сети со сценами «трейнсерфинга» (поезда на крыше поезда), «зацепинга» (езда на поезде, на подножке, держась за поручень), «руфинга» (опасное нахождение на крыше высокого здания). Сами подростки в своих блогах пишут о том, что «Игра со смертью зачаровывает...»

Анализируя половозрастную характеристику аудиторий закрытых групп в социальных сетях (напр., ВКонтакте), а также контент, содержащийся в других информационных ресурсах, ученые приходят к выводу, что «с молодежью работают взрослые люди, имеющие представления о методах психологической работы с детьми в целях формирования у них необходимого отношения к (криминальной) субкультуре». Противоправная деятельность в социальных сетях осуществляется не только организованными преступными группировками, но и специальными службами иностранных государств. При этом несовершеннолетние являются «крайне привлекательной для такого взаимодействия целевой аудиторией», легкой к внушению и навязыванию чуждой ему информации. Посредством погружения в виртуальную реальность несовершеннолетний, сам того не подозревая, может быть вовлечен в противоправную деятельность (в т. ч. экстремистской, террористической, любой другой направленности), например, по распространению запрещенной информации, нарушению общественного порядка и общественной безопасности и т. д. Особую группу риска, составляют дети из неблагополучных семей, которые являются наиболее доступными для вовлечения в подобные сообщества.

Третья группа — риски для несовершеннолетнего самому стать жертвой правонарушений (преступлений).

Гораздо большую опасность для несовершеннолетних представляет возможность стать жертвой различных киберпреступлений, разновидность которых увеличивается с каждым годом, начиная со взломов аккаунта,

электронной почты, кибермошенничества и т. д. Несовершеннолетний не обладает специальными знаниями и достаточным опытом, чтобы противостоять этому. К наиболее распространенным проявлениям киберкачеств жертвы относят: беззаботность по отношению к защите своих персональных (личных) данных, в частности, паспортных данных, сведений банковской карты, паролей и др.; несоблюдение элементарных киберпрофилактических мер, к примеру, сообщение сведений о банковской карте посторонним лицам; отсутствие надлежащих средств защиты компьютерной системы; отсутствие критического мышления; незнание способов киберпреступлений и др. Большую часть из вышеперечисленных качеств потенциальной жертвы можно отнести к несовершеннолетнему. Например, беззаботность и беспечность по отношению к защите своих персональных данных (добровольная передача их третьим лицам), отсутствие средств защиты технических средств, отсутствие критического мышления, незнание своих прав и др.

Добровольно распространяя личную информацию о себе, своей семье, своих друзьях путем размещения фотографий из семейного архива несовершеннолетний может не осознавать, что после попадания снимков в сеть они становятся всеобщим достоянием и могут быть использованы недоброжелателями против него самого и его семьи. Например, несовершеннолетний предоставляет свои персональные данные по запросу системы при регистрации аккаунта в социальных сетях (напр., ВКонтакте, Instagram, Facebook), а также при общении в мессенджерах (Viber, Whatsapp и др.), не предполагая, что происходит вторжение в его личное пространство и он подвергается серьезным рискам стать жертвой мошенников и киберпреступников. Зачастую несовершеннолетний ребенок намерено пренебрегает возрастными ограничениями, рекомендуемыми администраторами социальных сетей для своих пользователей (например, 13+ для Instagram, Facebook).

В последние несколько лет одним из распространенных видов деструктивного поведения среди несовершеннолетних стало интернет-преследование сверстников с применением угроз, выражение других форм агрессии. Агрессивное поведение несовершеннолетних в отношении сверстников происходит в форме запугиваний, как правило, с использованием личной информации о жертве. В специальной литературе данное явление получило название «кибербуллинг», под которым понимается использование информационных технологий коммуникации с целью негативного воздействия на личность человека. Специалисты отмечают, что буллинг (кибербуллинг) предполагает использование силы или влияния, прямо или косвенно, в устной, письменной или физической форме, либо путем демонстрации или иного использования снимков, символов или чего-либо другого в целях запугивания, угроз, травли, преследования или смущения при помощи информационных технологий. Психологическое воздействие может происходить через электронную почту, сервисы мгновенных сообщений, в чатах, социальных сетях, на web-сайтах, а также посредством мобильной связи. Имеют место и особые стилевые типы сетевой агрессии, такие как, например, «троллинг» (социальная провокация, издевательство, эпатаж) или «хейтерство» (ненавистничество, склочничество).

Посредством сети Интернет несовершеннолетние могут вступать в неформальные интернет-сообщества, деятельность которых прямо или косвенно направлена на склонение несовершеннолетних к суицидам. Речь идет, например, о «группах смерти», которые организуют ритуальные игры для участников либо размещают информацию (изображения, аудио-, видеоматериалы), которая может пагубно отразиться на личностной направленности детей на суицидальное поведение, создать стереотипы о безысходности той или иной жизненной ситуации и единственном выходе из нее — смерти. Так, ученые обращают внимание, что в 2016—2018 гг. Россия и общество столкнулись с пропагандой суицидального поведения и призывами к самоубийствам, распространяемыми как посредством сети

Интернет, так и путем отправки СМС-сообщений и рассылок с помощью всевозможных мессенджеров (WhatsApp, Viber, Telegram и пр.) При этом несовершеннолетний практически лишен возможности покинуть данную группу; если он изъявляет такое желание, он подвергается психологическому давлению и угрозам его жизни (либо происходит запугивание насильственной смертью близких людей) [38, с. 50]. Не имея поддержки со стороны взрослых (родителей, лиц их заменяющих, учителей, психологов и др.), несовершеннолетний не в состоянии самостоятельно решить свои проблемы, не осознавая их реальный масштаб и уровень опасности, противостоять им, обратившись за помощью в правоохранительные органы.

Гиперинформированность современной информационной среды ставит вопрос о необходимости защиты несовершеннолетних от избыточной информации, негативной для восприятия и не предназначенной для детского возраста и психики. Новые формы и способы противоправного взаимодействия преступного сообщества с несовершеннолетними, которые реализуются посредством сети Интернет и при этом непрерывно «совершенствуются» и видоизменяются, требуют новых подходов к решению задачи обеспечения информационной безопасности несовершеннолетнего.

С 2010 года в России проводятся Форумы безопасного интернета, создаются порталы, например, Год Безопасного интернета, журналы «Дети в информационном обществе», социальные проекты «Не Допусти». Проект направлен на защиту детей от похищений, противоправной эксплуатации и жестокого обращения.

В 2012 году начал свою деятельность фонд «Разумный интернет», в его задачи входит развитие специальных интернет-ресурсов для детей и поддержка гуманитарных сетевых проектов. Одним из проектов фонда является создание доменной зоны «Дети», где развивается детский контент с гарантией отсутствия на его ресурсах информации, связанной с насилием, пропагандой наркотиков и прочими негативными последствиями.

В качестве одного из примеров просвещения родителей по проблемам кибербезопасности детей может служить проект «Родительский контроль: интернет территория безопасности», созданный при поддержке Магнитогорского государственного Университета в 2013 году. Участники проекта – родители подростков, которым преподают на специальных семинарах основы родительского контроля интернет-ресурсов.

Также в РФ разработан бесплатный интернет-фильтр для детей «Цензор», который создает учетные записи – на каких сайтах был ребенок, блокирует неизвестные контакты.

В России организовано общество «Журавлик», которое анонимно работает по вопросам буллинга с несовершеннолетними. Директор этого центра начинала работать только с буллингом детей с аутизмом, потом они поняли, что травить могут любого ребенка. Она говорит о том, что проблема не в данном ребенке, а в коллективе. Педагогическая проблема в том, что дети о травле обычно не рассказывают педагогам, а рассказывают родителям, те говорят – не тебя травят и ладно. В корне неверная позиция, т.к. сегодня это один ребенок, завтра другой. Дети нанимают хейтеров (склочник, ненавистник), они за денежное вознаграждение травят этого ребенка еще и круглосуточно в сети.

Также в России появилось интернет-сообщество «Сдай педофила», директор этого сообщества рассказала о том, что они за несколько лет существования помогли полиции задержать более 300 человек с педофилией, которые были осуждены по этой статье и отбывают срок. О том, что с детьми об этом в семье нужно говорить открыто, нельзя ругать, если ребенок попал в такую ситуацию, нельзя отбирать телефон, обязательно обращаться в следственный комитет, не стирать переписку, не удалять фото и видео. Помнить, что в насилии виноват только насильник. Дети огромное количество информации выкладывают в сеть. Люди с педофилией пользуются шантажом, указывая, что знают, где живут, как выглядят родители, братья и сестры, что они причинят им вред, если дети не будут отправлять фото и видео

эротического содержания. Она рассказывала о последнем деле -13 летней девочке, которой они помогли.

«Цифровые дети» требуют от нас, взрослых (родителей, специалистов, научного сообщества, общества в целом, государства) решения задач по обеспечению его безопасности в интернет-пространстве. Речь идет о необходимости формирования национальной модели информационной безопасности несовершеннолетнего, наиболее отвечающей вызовам и угрозам современного киберпространства, обеспечивающей оптимальные условия реализации прав и свобод несовершеннолетнего в условиях информационного общества.

В нашей школе каждый год Майя Реджепова проводит со школьниками беседы о безопасном поведении в интернете, на школьном сайте расположены памятки, полезные ссылки для сотрудников, детей и их родителей по данной теме, которые мы дополним после педагогического совета.

«Безопасный интернет сегодня — это необходимое условие счастливого детства для наших детей» Галина Солдатова, руководитель Фонда развития Интернет, доктор психологических наук, профессор МГУ.