Безопасность несовершеннолетних в информационном обществе: анализ киберрисков и угроз

Рыбакова О. С.[*]

Ключевые слова: *обеспечение безопасности, информационная безопасность, информационный риск, кибербезопасность, права ребёнка, психологическое воздействие, деструктивная информация.*

Аннотация.

Цель: исследование факторов риска современного информационного общества и их влияния на здоровье и развитие личности несовершеннолетнего ребёнка.

Методология: в работе использован метод диалектики, на основе которого изучаются процессы тотальной информатизации общества и их возможные негативные последствия для здоровья и развития несовершеннолетних; общенаучный метод системного анализа, позволивший проанализировать общесоциальную проблему риска применительно к информационной безопасности несовершеннолетнего; сравнительно-правовой метод, позволивший автору обосновать и аргументировать дифференциацию и классификацию рисков.

Полученные результаты: на основе анализа и обобщения теоретических подходов учёных и мнений специалистов-практиков выявлено наличие общесоциальных, технологических, контентных, коммуникационных и др. рисков и угроз информационного пространства для развития несовершеннолетнего, предложено авторское понимание деструктивной для несовершеннолетнего информации. В результате проведенного исследования предлагается авторская классификация возможных рисков и угроз информационной среды для несовершеннолетнего.

DOI: 10.21681/2226-0692-2020-2-65-73

Особенностью современного этапа развития информационной сферы является её распространение и объединение с помощью информационно-телекоммуникационных технологий в единое мировое (глобальное) информационное пространство, детерминирующее состояние социальной среды современного общества, качество жизни человека, несущее в себе как определенные преимущества (условия взаимодействия между участниками: отдельными индивидами, человеком и обществом, человеком и государством), так и реальные риски безопасности информационных ресурсов, безопасности информации как объекта, и, что важно, риски безопасности самого человека как участника этих отношений. Исследуя теоретические основания «риска» как общенаучной категории, О.Ю. Рыбаков полагает, что технологические риски становятся социальными для современного информационного общества, «уже сегодня существует вероятность, что главным риском футурологического характера станет уход человека естественного в развитие человека частично искусственного» [1, с. 18—19], с чем сложно не согласиться.

Несовершеннолетний ребёнок не изолирован от информационного общества, он находится внутри него и является 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» [2, с. 17—19]. Современный ребёнок, в отличие от своих родителей знакомится с информационными технологиями уже в дошкольном возрасте (телевизор, игровые приставки, смарт-игры и т. д.) [3, с. 105]. Интернет-пространство является частью социальной среды ребёнка, который получает определенный объём информации из открытых источников самостоятельно. Здесь важно подчеркнуть, что если в дошкольном и младшем школьном возрасте ребёнок контактирует с информационными ресурсами, как правило, в сопровождении взрослых (родителей или лиц, их заменяющих), 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 ребенку информацией [4, с. 428]. По данным сайта «Интернет-контроль: сайт для умных родителей», детская аудитория пользователей интернета сегодня составляет почти 9 млн детей в возрасте до 14 лет, три четверти которых пользуются сетью без контро-

[*] ***Рыбакова Ольга Сергеевна,*** кандидат юридических наук, старший научный сотрудник отдела научно-исследовательской и образовательной деятельности ФБУ «Научный центр правовой информации при Министерстве юстиции Российской Федерации», г. Москва, Российская Федерация.

E-mail: orro21@yandex.ru

ля со стороны взрослых[1]. С одной стороны, несовершеннолетние с большей легкостью, чем их родители, адаптируются в информационном пространстве, осваивают его в различных целях, с другой — несовершеннолетние представляют собой наиболее уязвимую аудиторию для воздействия мощного информационного потока, что может негативно сказываться на их развитии, психическом и физическом здоровье. 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 [5; 6; 7; 8; 9; 10; 11].

В условиях современных больших вызовов и киберугроз, происходящих в глобальном информационном обществе, учеными актуализируется необходимость дополнительного изучения потенциальных кибервызовов и киберугроз информационно-коммуникационного пространства, которое не ограничивается территорией одного государства и имеет транснациональный характер [12, с. 10—13; 13; 14, с. 42]. Информационное пространство несовершеннолетнего представляет собой информационно-коммуникативное поле его взаимодействия с другими участниками информационного социума, которое постепенно расширяется по мере взросления ребёнка. Здесь следует говорить не только о взаимодействии несовершеннолетнего с различными источниками информации, но и о сложном процессе взаимодействия между всеми участниками (субъектами) информационных отношений, среди которых находится несовершеннолетний, что обуславливает необходимость изучения возможных рисков и угроз в данной сфере.

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

Определенный интерес представляет классификация информационных рисков, с которыми может столкнуться несовершеннолетний в интернет-пространстве, предложенная в 2012 году Организацией экономического сотрудничества и развития (ОЭСР)[2]:

1. *Технологические риски* (Internet technology risks), которые подразделяются на: *контент-риски* (content risks), предполагающие просмотр запрещенной информации (порнография, расизм, агрессия, ненависть, в т. ч. вредные советы (суицид)); *контакт-риски* (contact risks) — кибергруминг (cyber grooming), онлайн-беспокойство (online harassment), кибербуллинг (cyberbullying), предполагающие различные формы унижения в сети или по мобильному телефону, киберсталкинг (cyberstalking) (преследование или домогательство в сети Интернет).
2. *Потребительские риски* (consumer-related risks), подразделяющиеся на следующие подвиды: *риски онлайн-маркетинга* (online marketing), предполагающие приобретение несовершеннолетним нежелательных продуктов (услуг); *риски чрезмерных трат* (overspending risks), предполагающие чрезмерную трату средств либо трафика; *риск стать жертвой мошенников* (fraudulent transactions), предполагающие мошеннические действия со стороны третьих лиц в отношении несовершеннолетнего.
3. *Риски, связанные с нарушением прав несовершеннолетнего на частную жизнь и защиту информации о несовершеннолетнем* (information privacy and security risks).

Заслуживает внимания классификация интернет-рисков, или «онлайн-рисков», предложенная отечественными учеными в результате многолетних исследований особенностей использования современными российскими детьми и подростками инфокоммуникационных технологий [15, с. 91—92]:

- 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, сексуальные домогательства), знакомства в Сети и последующие встречи с интернет-знакомыми в реальной жизни);
- третья группа — *потребительские риски,* возникающие в результате злоупотребления в интернете правами потребителя (среди рисков данной группы ученые называют: 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; синдром отмены; замена реальности.

[1] URL: http://www.internet-kontrol.ru/stati/deti-v-internete.html (дата обращения: 26.01.2020).

[2] Recommendation on the OECD Council Report on risks faced on children online and policies to protect them. Pp. 24-30. [Электронный ресурс]. URL: http://www.oecd.org/sti/ieconomy/childrenonline_with_cover.pdf (дата обращения: 03.03.2020).

В юридической литературе можно встретить и другие классификации основных рисков и угроз, с которыми могут столкнуться несовершеннолетние в информационном пространстве. Например, А.А. Чесноков и Е.С. Акимышева предлагают классифицировать возможные риски исходя из вида получаемой информации:

1) информация, причиняющая вред здоровью (высокочастотное излучение, повышенный уровень шума и опасность возгорания, вред для зрения, артрит кистевых суставов и т. п.);
2) информация, пропагандирующая запрещенные в обществе идеи (терроризм, фашизм, расовая нетерпимость, сектантство, наркотики, жестокое отношение к людям и прочее);
3) информация, вызывающая сексуальные девиации (порнография, гомосексуализм, различного рода извращения);
4) игры, погружающие в виртуальный мир, пропагандирующие насилие, развивающие игроманию, не способствующие развитию интеллекта;
5) социальные сети, способствующие созданию компьютерной зависимости, риска доступа взрослых с криминальными намерениями, условий для приобретения запрещенных товаров (спайсы, иные наркотические и психотропные вещества, краденые вещи, оружие);
6) различного рода мошенничества, интернет-казино, воровство, склонение к приобретению дорогостоящих информационных продуктов [16, 140—141].

По результатам исследований фирмы «Лаборатория Касперского» основные риски, которые видят сами родители для их несовершеннолетних детей при использовании Интернета, можно разделить на несколько групп[3]: риск взаимодействия с нежелательным контентом (как правило, под таковым понимается порнографический контент), на втором месте — сцены насилия, и на третьем, с весны прошлого года — группы смерти; риск общения с незнакомыми людьми; риск негативного влияния интернета на здоровье (зрение, осанка); риск наступления интернет-зависимости и др.

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

Первая группа рисков связана с получением деструктивной информации, которая может негативно повлиять на психическое, духовное, нравственное здоровье[4] и развитие несовершеннолетнего.

Глобальное информационное пространство предоставляет возможность неограниченного доступа к широкому кругу информационных ресурсов, обеспечивая тем самым реализацию права человека на свободный доступ к информации. И.Л. Бачило предлагает рассматривать всю совокупность информации как «воспринимаемую и понимаемую человеком характеристику окружающего мира во всем его разнообразии, которая возникает в процессе познания последнего и позволяет на основе познания и измерения свойств предметов, явлений, процессов, фактов и отражения их в различных формах восприятия отличать их признаки, элементы, значения и устанавливать связи и зависимости всего многообразия проявления материального, духовного, идеологического мира»[5]. «Информация — это обусловленные бытием человека, сведения об окружающей действительности, изменяющиеся в процессе жизнедеятельности человека» [17, с. 72]. «Информация, с точки зрения её сущностной характеристики, — представляет собой отражение существующей действительности в сознании человека, выраженная в символьной форме с целью дальнейшей ориентации и адаптации в жизни»[6]. Отражая окружающий мир в своем сознании, пишет В.М. Сырых, человек одновременно познает его по преимуществу в форме чувственных образов, восприятий и представлений [18, с. 26]. В связи с этим заслуживает внимания психологический подход к пониманию информации, которая, по мнению ученых, представляет собой «совокупность сведений об окружающем мире, получаемая человеком из различных источников с помощью органов чувств, отражаемые в виде сигналов и знаков, которые являются объектом преобразования психических процессов (внимания, восприятия, памяти, мышления, воображения) и используются для выработки поведения»[7]. Приведенный подход основан на психических познавательных процессах человека при работе с информацией (восприятии, хранении, передаче и др.), которая выступает определяющим фактором его поведения.

Информация, которую получает несовершеннолетний ребёнок, таким образом, представляет собой всю совокупность сведений об окружающей его реальности, воспринимаемую сознанием ребёнка и принимаемую им в соответствии с его психическими и интеллектуальными способностями, которая в результате оказывает влияние на формирование его сознания, психическое состояние, дальнейшее развитие, а также детерминирует модели его поведения в обществе. В связи с этим большой риск причинения вреда психическому и нравственному здоровью несовершеннолетнего может быть сопряжен с содержанием получаемой информации. Далеко не всякая информация может способствовать формированию у ребёнка правильных морально-нравственных ориентиров и способствовать его развитию.

Полагаем, что *деструктивная для несовершеннолетнего ребёнка информация* представляет собой информацию (аудио-, видеоконтент), направленную на разру-

---

[3] URL: http://www.pravmir.ru/deti-v-internete-4-glavnyih-opasnosti-i-kak-ot-nih-zashhititsya [Электронный ресурс]. (дата обращения: 21.03.2020)

[4] 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.)

[5] Бачило И. Л. Информационное право : учебник для академического бакалавриата / И. Л. Бачило. 5-е изд., перераб. и доп. М. : Издательство Юрайт, 2016. 419 с. С. 25.

[6] Информационные технологии в юридической деятельности: учебник / П.У. Кузнецов [и др.] под общ. ред. П.У. Кузнецова. 3-е., перераб. и доп. М.: Юрайт, 2020. 325 с. С. 37.

[7] Превентивные технологии защиты детей от вредной информации: уч. пособие для вузов / С.В. Пазухина, С.А. Филиппова. 2-е изд. перераб и доп. М., Издательство: Юрайт, 2020. 194 с. С. 13.

шение 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.

В юридической науке под «вредной информацией» принято понимать информацию, «обуславливающую необходимость охраны и защиты прав и законных интересов личности, общества и государства в силу возможного вреда, который она может нанести этим субъектам в результате своего распространения (применения)» [19]. Учеными выделяется пять основных категорий «вредной информации», среди которых:

1) информация, направленная на разжигание вражды, ненависти и насилия;
2) ложная информация (в т. ч. недостоверная, заведомо ложная реклама);
3) информация, содержащая посягательства на доброе имя, честь и достоинство;
4) непристойная информация (в т. ч. порнография, неэтичная реклама и т. д.);
5) информация, оказывающая деструктивное воздействие на здоровье людей[8].

Интересным представляется понимание «вредоносной информации», предложенное К.Д. Рыдченко, под которой автор понимает «сведения, содержащие качества недостоверности, непристойности или деструктивности, негативное воздействие которых на индивидуальную психику и общественное сознание обуславливает необходимость ограничения или запрета их оборота» [20, с. 40]. Предложенный автором психологический подход к пониманию деструктивной информации, безусловно, заслуживает внимания и поддержки. Подобная информация оказывает всестороннее негативное воздействие на несовершеннолетнего в условиях формирования его личности: интеллектуальное, социальное, физическое, включая духовно-нравственную и эмоциональную сферы. «Вредная информация», пишут С.В. Пазухина и С.А. Филиппова, может стать для несовершеннолетнего ребёнка причиной психологической либо психической травмы, которая представляет собой нарушения нормального функционирования психики, в том числе познавательных процессов (памяти, внимания, мышления, речи), и сказывается на социальной адекватности несовершеннолетнего[9]. Сцены жестокости, насилия, порнографические изображения, информация экстремистского, террористического характера, другие противоправные деяния, распространяемые в сети, в том числе в компьютерных играх, ведут к неосознаваемому несовершеннолетним ребёнком желанию подражать увиденному.

Анализируя негативное влияние интернет-контента на нравственное воспитание несовершеннолетних, Э.И. Атагимова отмечает, 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. Результаты отечественных исследований подтверждают, что в 2010 г. до принятия Федерального закона от 29.12.2010 № 436-ФЗ «О защите детей от информации, приносящей вред их здоровью и развитию»[10] более 40% российских школьников сталкивались с изображениями сексуального характера онлайн [15]. Чаще всего несовершеннолетний ребёнок попадает на «вредные странички» случайно, посредством всплывающих окон, неверно истолкованных поисковиком запросов, всплывающих гиперссылок в социальных сетях и т. д. [7, с. 52; 21, с. 23]. Как отмечают специалисты, в гиперинформированном обществе под прессингом информационного воздействия у несовершеннолетнего происходит снижение критичности восприятия и оценки получаемой информации, присвоение социальной роли через идентификацию с виртуальными персонажами [7; 22; 23; 24]. Погружаясь в информационную среду, несовершеннолетний ребёнок воспринимает информацию через её отражение в своём сознании, дифференцирует полученную информацию на интересную (неинтересную), полезную (бесполезную), положительную (отрицательную) и т. д. в соответствии со своими интеллектуальными, морально-нравственными, психическими возможностями развития личности. В силу возрастных особенностей ребёнок не всегда способен правильно дифференцировать получаемую информацию.

Следует отметить: существует позиция специалистов [25; 26], что с целью нормальной социализации ребёнка и адекватного восприятия негативной информации несовершеннолетний в соответствии с возрастом и уровнем своего развития все же должен получать определенный объем «негативной информации» и тем самым быть осведомлённым о существовании негативных моделей поведения, которое не должно преподноситься как поощряемое, а напротив, необходимо при совместном просмотре выражать порицание такому поведению, говорить о нем как об отклоняющемся от нормы. В данном случае роль «проводника» в информационное пространство отведена родителям, учителям, воспитателям, которые призваны расставить правильные морально-нравственные ориентиры несовершеннолетнего, способствуя тем самым формированию положительной модели его восприятия получаемой инфор-

[8] Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право / Под ред. акад. РАН Б.Н. Топорнина. СПб. : Юридический центр Пресс, 2001. 789 с. С. 574.

[9] Подробнее об этом: Превентивные технологии защиты детей от вредной информации… С. 15—16.

[10] Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 01.05.2019) «О защите детей от информации, причиняющей вред их здоровью и развитию» (с изм. и доп., вступ. в силу с 29.10.2019) // Собрание законодательства РФ, 03.01.2011, № 1, ст. 48.

мации. В отсутствие грамотного сопровождения, в силу своих возрастных, психологических, физиологических особенностей развития личности, ребёнок не способен самостоятельно адаптироваться к современному информационно-коммуникативному социуму, что приводит к трансформации моральных и нравственных установок ребёнка и может в дальнейшем привести к формированию агрессивной модели поведения и, как следствие, росту числа детей с различными формами социальной дезадаптации и девиантного поведения.

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 запросам информации добавляются возможности установления новых контактов с виртуальными собеседниками, в т. ч. посредством социальных сетей (ВКонтакте, Одноклассники, 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. Вся сложность регулирования отношений в данной сфере, как в свое время справедливо отмечала И.Л. Бачило, объясняется тем, что в интернет-пространстве действует так называемый «виртуальный субъект», который «плохо осязаем» (его признаки и характеристики неустойчивы), но он способен к действию и участвует в отношениях наравне с другими»[11]. Данное высказывание актуально и сегодня. Анонимность участников социальных сетей осложняет процесс управляемости данной сферы правового регулирования. Новые формы взаимодействия и способы выстраивания отношений с виртуальным сообществом (собеседником) детерминируют появления коммуникативных навыков общения в сети, что в совокупности определяет правила, ценностные установки и, в конечном счете, субкультуру виртуального сообщества. В данном случае возникает риск отклонения от общепринятых в обществе морально-нравственных ценностных установок, появлению различных форм асоциального поведения несовершеннолетних в условиях виртуальной реальности.

С учетом того, что несовершеннолетним свойственна незрелость мышления как результата недостаточного опыта и знаний, склонность к подражанию, определенная податливость отрицательным влияниям микросреды[12], стремление к экстремальному образу поведения [27, с. 5—6], то, попадая в виртуальное интернет-пространство, ребёнок оказывается в зоне особого риска, которому трудно противостоять самостоятельно. Бесконтрольное неограниченное нахождение в Сети оказывает на несовершеннолетнего психотравмирующее и порой растлевающее влияние, что в результате может привести к различным формам асоциального поведения.

Современные 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 2017—2019 годах, выделяются следующие разновидности деструктивного поведения несовершеннолетних в цифровой среде:

- различные формы киберагрессии, в том числе кибербуллинг;
- деятельность экстремистских сообществ;
- популяризация и распространение способов деструктивного поведения (А.У.Е., криминализация, алкогольная и наркотическая зависимость);
- пропаганда самоповреждающего (анорексия, селфхарм) и суицидального поведения;

[11] Бачило И.Л. Информационное право… С. 141.

[12] Фельдштейн Д.И. Психология взросления: структурно-содержательные характеристики развития личности / Избранные труды: 2-е изд. М., 2004. 672 с. С. 129—132; Голубева Л.М. Причины правонарушений среди молодежи и меры по их устранению // Правонарушения среди молодежи и меры их предупреждения. Фрунзе, 1985. С. 43.

- целенаправленное распространение негативного поведения онлайн и призыв к асоциальному поведению офлайн[13].

Несколько лет назад большой популярностью среди подростковой аудитории пользовались сюжеты, снятые самими несовершеннолетними и распространяемые в сети со сценами «трейнсерфинга» (проезда на крыше поезда), «зацепинга», «руфинга» (опасное нахождение на крыше высокого здания).

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» [29, с. 181]. Как отмечает А.Н. Прокопенко, противоправная деятельность в социальных сетях осуществляется не только организованными преступными группировками, но и специальными службами иностранных государств [30, с. 157—158]. При этом несовершеннолетние являются «крайне привлекательной для такого взаимодействия целевой аудиторией» [31, с. 25], 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, по мнению А.А. Реана, составляют дети из неблагополучных семей, которые являются наиболее доступными для вовлечение в подобные сообщества, а «в случае, когда они попадают в «заботливые» руки взрослых и многоопытных «воспитателей» — зона риска молодежного экстремизма быстро может превратиться в трагическую реальность» [27, с. 6]. В данном случае, не имея положительного образа поведения в своей семье, несовершеннолетний невольно поддается авторитетному влиянию извне. Далеко не все дети в подростковом возрасте знают, что подобная деятельность наказуема, и наказание может быть применимо непосредственно к ним (законным представителям). Многие из несовершеннолетних полагают, что, «спрятавшись за ником», они могут остаться незамеченными и неидентифицированными в виртуальной реальности. Вместе с тем несовершеннолетние дети, сами того не подозревая, несут ответственность (административную и уголовную) начиная с установленного законом возраста.

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

Следует оговориться, что приведенный ниже перечень возможных незаконных действий в отношении несовершеннолетних не является исчерпывающим. Назовем наиболее распространенные случаи нарушения прав несовершеннолетних.

Несовершеннолетние являются активными пользователями различных поисковых систем, в том числе в образовательных целях в рамках учебных программ, реализуя свои познавательные навыки. На смену библиотечным системам современному школьнику и студентам порой приходит так называемое «яндекс-гугл образование», где без труда можно найти «нужную» информацию по ключевым запросам (словам). О том, насколько найденная информация достоверная, ребёнок не всегда задумывается. Получая «яндекс-гугл ответ» на заданный вопрос, несовершеннолетний не в состоянии критически оценить полученную информацию, он принимает её как истину. В данном случае, реализуя свое право на доступ к информации, несовершеннолетний не предполагает, что происходит нарушение другого, не менее важного права, — права на получение *достоверной информации*. В данном случае речь идет об информации как объекте потребления.

В силу своей неопытности несовершеннолетний ребёнок может столкнуться с другими видами нарушения его прав как потребителя различной продукции, товаров и услуг в случае предоставления их в низком качестве либо непредоставления их вообще после произведенной онлайн оплаты.

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 кибервиктимных качеств жертвы Е.А. Антонян и Е.Н. Клецина 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. [32, с. 6]. 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.

Неограниченный доступ к информации одновременно может формировать среду, облегчающую нарушение другого основополагающего права несовершеннолетнего — права на частную жизнь. Правовая категория «частная жизнь» неоднократно была предметом рассмотрения Конституционного Суда Российской Федерации. Так, в сформированной по данному вопросу позиции Конституционный Суд определил, что в понятие «частная жизнь» включается та область жизнедеятельности человека, которая относится к отдельному лицу,

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

касается только его и не подлежит контролю со стороны общества и государства, если она носит непротивоправный характер[14]. «Право на неприкосновенность частной жизни, личную и семейную тайну означает предоставленную человеку и гарантированную государством возможность контролировать информацию о самом себе, препятствовать разглашению сведений личного, интимного характера; в понятие «частная жизнь» включается та область жизнедеятельности человека, которая относится к отдельному лицу, касается только его и не подлежит контролю со стороны общества и государства, если носит непротивоправный характер. Соответственно, лишь само лицо вправе определить, какие именно сведения, имеющие отношение к его частной жизни, должны оставаться в тайне, а потому и сбор, хранение, использование и распространение такой информации, не доверенной никому, не допускается без согласия данного лица, как того требует Конституция Российской Федерации» (Определение Конституционного Суда РФ от 09.06.2005 № 248-О).

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 [33, с. 61; 34, с. 187; 35]. 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 [36, с. 29; 37]. 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) [27, с. 6].

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—2017 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.) [5, с. 363]. Одной из основных особенностей суицидальных интернет-ресурсов, по мнению специалистов, является постоянное их видоизменение, а также совершенствование работы так называемых кураторов с подростковой аудиторией; например, чтобы избежать преследования со стороны правоохранительных органов, «группы смерти» разбиваются на более мелкие подгруппы идейных участников, которые имеют более сложную систему конспирации [38, с. 49]. 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. В данной группе рисков находятся не только противоправные и аморальные действия, совершение которых сопряжено с непосредственным использованием информационных технологий. Серьезной угрозой для несовершеннолетнего может стать встреча с виртуальным преследователем (злоумышленником) в реальной жизни, которая может быть небезопасной для здоровья и жизни несовершеннолетнего.

Предложенная нами классификация информационных рисков, безусловно, не является исчерпывающей. 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

[14] См. определения Конституционного Суда РФ от 28.06.2012 № 1253-О, от 27.05.2010 № 644-О-О, от 09.06.2005 № 248-О; от 27.05.2010 № 644-О-О; от 09.06.2005 № 248-О и др.

сети Интернет и при этом непрерывно «совершенствуются» и видоизменяются, требуют новых подходов к решению задачи обеспечения информационной безопасности несовершеннолетнего. «Цифровой ребёнок» требует от нас, взрослых (родителей, специалистов, научного сообщества, общества в целом, государства) решения задач по обеспечению его безопасности в новой социокультурной среде — информационно-телекоммуникационном 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.

Литература

1. Риски финансовой безопасности: правовой формат : монография / отв. ред. И.И. Кучеров, Н.А. Поветкина. М. : ИзиСП: Норма: ИНФРА-М, 2018. 304 с.
2. Солдатова Г.У., Рассказова Е.И., Нестик Т.А. Цифровое поколение России: компетентность и безопасность. М. : Смысл, 2017. 375 с.
3. Ростова Ю.В. Интернет-пространство — основа современного российского информационного общества / В сб.: Общество, государство, личность: модернизация системы взаимоотношений в современных условиях / Материалы XVI Всероссийской научно-практической конференции (с международным участием): в 2 ч. 2016. С. 103—107.
4. Rybakov O.J., Rybakova O.S. Principles of information security of a child on the internet // Studies in Computational Intelligence. 2019. Т. 826. С. 427—433.
5. Филиппов В.М., Насонкин В.В., Папачараламбоус Ч. Права и интересы детей в информационной сфере: реформирование законодательства // Вестник Санкт-Петербургского университета. Право. 2019. Т. 10. № 2. С. 362—372.
6. Кобзева С.В. Защита прав несовершеннолетних от угроз в сети Интернет // Информационное право. 2017. № 2. С. 33—39.
7. Рыбакова О.С. Законодательное регулирование обеспечения безопасности ребенка в интернет-пространстве // Правовая информатика. 2017. № 4. С. 49—54.
8. Рыбаков О.Ю., Рыбакова О.С. Ребенок и интернет-пространство: вопросы правового обеспечения безопасности // Информационное право. 2018. № 1. С. 27—31.
9. Общество: пространство, риски, ценности / Устьянцев В.Б., Гобозов И.А., Пигров К.С. и [др] : монография / Под ред. А. Н. Чумакова. Саратов, 2012. 268 с.
10. Солдатова Г.У., Рассказова Е.И., Нестик Т.А. Цифровое поколение России: компетентность и безопасность. М. : Смысл, 2017. 375 с. С. 91—92.
11. Атагимова Э.И., Рамазанова И.М. Некоторые аспекты законодательного уровня обеспечения информационной безопасности в Российской Федерации // Правовая информатика. 2014. № 2. С. 14—19.
12. Полякова Т.А. Проблемы и вызовы цифровой трансформации и тенденции правового обеспечения информационной безопасности / В кн.: Проблемы и вызовы цифрового общества: тенденции развития правового регулирования цифровых трансформаций. Сборник научных трудов по материалам I Международной научно-практической конференции. Под редакцией Н.Н. Ковалевой. 2019. 184 с.
13. Карцхия А.А., Макаренко Г.И., Сергин М.Ю. Современные тренды киберугроз и трансформация понятия кибербезопасности в условиях цифровизации системы права // Вопросы кибербезопасности. 2019. № 3 (31). С. 18—23.
14. Полякова Т.А. Актуальные проблемы развития системы правового обеспечения информационной безопасности в цифровую эпоху и юридическое образование // Вестник Университета имени О.Е. Кутафина (МГЮА). 2019. № 12 (64). С. 37—44.
15. Солдатова Г., Рассказова Е., Зотова Е., Лебешева М., Роггендорф П. Дети России Онлайн: риски и безопасность. Результаты международного проекта EU Kids Online II в России. М., 2012. [Электронный ресурс]. URL: http://psypublic.com/assets/files/EU-Kids-Online-II-inRussia.pdf (дата обращения: 12.03.2020).
16. Чесноков А.А., Акимышева Е.С. Роль органов внутренних дел в механизме обеспечения информационной безопасности ребенка // Алтайский юридический вестник. 2015. № 11. С. 139—142.
17. Рыбаков О.Ю. Приоритеты развития информационного общества в России: правовое обеспечение // Мониторинг правоприменения. 2017. № 3 (24). С. 71—76.
18. Сырых В.М. Введение в теорию образовательного права. М. : «Готика», 2002. 400 с.
19. Лопатин В.Н. Информационная безопасность России: дис. ... д-ра юрид. наук: 12.00.01. СПб., 2000. 433 с.
20. Рыдченко К.Д. «Недетские» проблемы обеспечения информационной безопасности детей // Вестник Воронежского института МВД России. 2015. № 2. С. 40—45.
21. Атагимова Э.И. Проблемы отрицательного влияния интернета на нравственное воспитание подростков в информационном пространстве и пути решения // Правовая информатика. 2013. № 1. С. 21—24.
22. Батенова Ю.В., Волчегорская Е.Ю., Емельянова И.Е. Современная социальная ситуация развития и формирование информационной культуры дошкольника // Балтийский гуманитарный журнал. 2019. Т. 8. № 3 (28). С. 13—16.
23. Милушкина О.Ю., Скоблина Н.А., Маркелова С.В., Татаринчик А.А., Бокарева Н.А., Федотов Д.М. Оценка рисков здоровью школьников и студентов при воздействии обучающих и досуговых информационно-коммуникационных технологий // Анализ риска здоровью. 2019. № 3. С. 135—142.
24. Полянина А.К. Информационная безопасность детства в условиях новой медиареальности // Информационное общество. 2019. № 1-2. С. 108—115 и др.

25. Амбалова С.А. Психологические причины отклоняющегося поведения подростков: профилактика и коррекция // Азимут научных исследований: педагогика и психология. 2019. Т. 8. № 3 (28). С. 317—319.
26. Собкин В.С., Федотова А.В. Подростковая агрессия в социальных сетях: восприятие и личный опыт // Психологическая наука и образование. 2019. Т. 24. № 2. С. 5—18.
27. Реан А.А. Подростковая субкультура — зона потенциальных рисков // Психологическая наука и образование. 2012. № 4. С. 5—10.
28. Гехова Д.Х. О практике прокурорского надзора по защите прав детей в информационной среде // Безопасность информационного пространства для несовершеннолетних в Магаданской области (материалы круглого стола, г. Магадан, 12 ноября 2019 года). [Электронный ресурс]. URL: http://magoblduma.ru/common/upload/49/editor/file/Sbornik_2019__Bezopasnost_informatsionnogo_prostranstva_dlya_nesovershennoletnikh_v_Magadanskoy_oblasti.pdf.
29. Антонян Е.А., Борисов Е.А. К вопросу о популяризации криминальной субкультуры среди молодежи // Lex russica (Русский закон). 2017. № 12 (133). С. 180—186.
30. Прокопенко А.Н. Правовые проблемы противодействия противоправным деяниям в социальных сетях и мессенджерах / В кн. Формирование системы правового регулирования обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе. Вторые Бачиловские чтения. Сб. науч. трудов / Под ред. Т.А. Поляковой, В.Б. Наумова, А.В. Минбалеева. М. : ИГП РАН, 2019. 341 с. С. 157—158.
31. Гребеньков А.А., Гребенькова Л.А. Пропаганда социально-негативного поведения среди несовершеннолетних как общественно опасное явление // Проблемы правоохранительной деятельности. 2019. № 3. С. 24—28.
32. Антонян Е.А., Клещина Е.Н. Кибервиктимность // Вестник Пермского института ФСИН России. 2019. № 3 (34). С. 5—10.
33. Барышева К.А. Определение понятия общественно опасной природы кибersталкинга // Адвокат. 2016. № 10. С. 60—66.
34. Антонян Е.А. Детствосбережение и информационная безопасность детей // Проблемы экономики и юридической практики. 2019. Т. 15. № 6. С. 187—189.
35. Белицкий М.Э. Кибербуллинг как социально-психологическая проблема и правовые пути ее решения // Научно-образовательный потенциал молодежи в решении актуальных проблем XXI века. 2019. № 13. С. 333—337.
36. Кобец П.Н. Противодействие угрозам кибersталкинга — важнейшей проблеме, исследуемой в рамках совершенствования аспектов информационной безопасности регионов в условиях глобализации информационного пространства // Вестник Прикамского социального института. 2017. № 1 (76). С. 27—35.
37. Иванова К.А., Степанов А.А., Немчинова Е.В. Кибербуллинг как девиация права граждан на свободу мнения в сети Интернет // Актуальные проблемы российского права. 2019. № 1. С. 96—101.
38. Букалерова Л.А., Лавелина В.С., Остроушко А.В. Правовые, организационные, технические меры противодействия призывам к самоубийствам несовершеннолетних в сети «Интернет» // Ученые труды Российской академии адвокатуры и нотариата. 2017. № 3 (46). С. 48—57.

Рецензент: Антонян Елена Александровна, *доктор юридических наук, профессор кафедры криминологии и уголовно-исполнительного права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), г. Москва, Россия. E-mail: antonyaa@yandex.ru*