ISSN 2500-4255

УДК 343.85
DOI 10.17150/2500-4255.2020.14(2).234-241

ЗАЩИТА ПРАВ И СВОБОД НЕСОВЕРШЕННОЛЕТНИХ В ЦИФРОВОМ ПРОСТРАНСТВЕ

С.М. Миронова, С.С. Симонова
Волгоградский институт управления — филиал Российской академии народного хозяйства и государственной службы, г. Волгоград, Российская Федерация

Информация о статье

Дата поступления
2 ноября 2018 г.

Дата принятия в печать
8 апреля 2020 г.

Дата онлайн-размещения
30 апреля 2020 г.

Ключевые слова
Информационная безопасность; несовершеннолетние; цифровое пространство; защита прав и свобод; защита в сети Интернет; безопасность в сети Интернет; виктимологическая профилактика; информация; Интернет; кибербуллинг

Финансирование
Работа выполнена при поддержке Волгоградского института управления — филиала РАНХиГС в рамках реализации научного проекта № 04-2018ВИУ «Актуальные проблемы защиты прав и свобод в цифровом пространстве»

Аннотация. Проблема обеспечения информационной безопасности в настоящее время является актуальной как для Российской Федерации, так и для всего мирового сообщества. С огромной скоростью возрастает количество киберугроз не только для граждан, но и для организаций, общества, государства. Особого внимания заслуживает такая проблема, как обеспечение информационной безопасности детей и подростков. Именно несовершеннолетние чаще подвергаются негативному воздействию в сети Интернет, они рискуют стать жертвами кибербуллинга, мошенничества и неправомерного доступа к личной информации. Среди распространенных угроз информационной безопасности несовершеннолетних также можно выделить постоянное увеличение количества интернет-сайтов с агрессивным или нелегальным контентом, в том числе призывающих к суициду и склоняющих к употреблению наркотических средств и психотропных веществ, а также осуществление посредством сети Интернет киберпреследований и виртуальных домогательств. Информационная безопасность несовершеннолетних в цифровом пространстве является комплексной проблемой, для успешного решения которой необходима консолидация правовых и информационных ресурсов. В статье проанализирован российский и зарубежный опыт обеспечения информационной безопасности несовершеннолетних. Обобщены различные научные подходы к решению проблемы обеспечения защиты несовершеннолетних в сети Интернет. Предложена классификация киберугроз, представляющих наибольшую опасность: программно-технические (умышленное распространение вирусов и троянских программ), экономические (хищение и продажа данных кредитных карт, фишинг-атаки, взломы платежных аккаунтов) и контентные (публичное размещение в сети Интернет любых материалов, в том числе незаконных). Рассмотрены правовые, социальные и технические меры обеспечения информационной безопасности несовершеннолетних. Предложены изменения в действующее законодательство, регулирующее вопросы обеспечения информационной безопасности несовершеннолетних, проанализированы конкретные способы решения данной задачи, сформулирован ряд мер, направленных на защиту прав и свобод несовершеннолетних в цифровом пространстве (проведение с несовершеннолетними тематических профилактических занятий, разработка специализированных программ по защите информации).

PROTECTION OF THE RIGHTS AND FREEDOMS OF MINORS IN THE DIGITAL SPACE

Svetlana M. Mironova, Svetlana S. Simonova
Volgograd Institute of Management — branch of the Russian Academy of National Economy and Public Administration, Volgograd, the Russian Federation

Article info

Received
2018 November 2

Accepted
2020 April 8

Available online
2020 April 30

Abstract. The problem of ensuring information security is currently urgent for the Russian Federation as well as for the whole world. The number of cyber-threats is increasing at a great speed, and they concern not only private citizens, but also organizations, the community and the state. Special attention should be paid to the information security of children and teenagers. Minors are most susceptible to negative influences on the Internet, they risk becoming victims of cyberbullying, fraud and illegal access to personal data. Common threats to the information security of minors include a constant increase in the number of sites with aggressive or illegal content, including those inciting to suicide or abuse of drugs and psychoactive substances, as well as cyber-stalking or virtual sexual harassment. The information security of minors in the digital space is a complex issue, whose successful solution requires a con-

Keywords
Information security; minors; digital space; protection of rights and freedoms; protection in the Internet; security in the Internet; victimological prevention; information; the Internet; cyberbullying

Acknowledgements
This work was supported by the Volgograd Institute of Management — RANEPA, in the framework of the research project No. 04-2018VIU «Actual Problems of the Protection of Rights and Freedoms in the Digital Space»

solidation of legal and information resources. The article analyzes Russian and foreign experience of ensuring the information security of minors. The authors summarize research approaches to solving the problem of protecting minors on the Internet. They present a classification of the most urgent cyber-threats: software-technical (intentional dissemination of viruses and Trojan software), economic (theft and sale of credit card details, phishing-attacks, hacking of payment accounts), and content (public dissemination of any materials, including illegal ones, on the Internet). The authors also examine legal, social and technical measures of ensuring the information security of minors and suggest changes to the current legislation which regulates the information security of minors. The authors also study specific methods of solving this task and outline a number of measures aimed at protecting the rights and freedoms of minors in the digital space (thematic prevention classes for minors, development of special information protection software).

Развитие информационного и цифрового пространства в современном мире требует усиления мер по защите информационной безопасности граждан. На государственном уровне принимаются специальные программы по обеспечению информационной безопасности, например Доктрина информационной безопасности Российской Федерации, утвержденная указом Президента РФ от 5 декабря 2016 г. № 646. Принятая в 2017 г. программа «Цифровая экономика Российской Федерации» (распоряжение Правительства РФ «Об утверждении программы «Цифровая экономика Российской Федерации» от 28 июля 2017 г. № 1632-р) в качестве одной из задач указывает обеспечение защиты прав, свобод и законных интересов личности в условиях цифровой экономики.

Особенно важной представляется защита информационной безопасности отдельных категорий граждан, которые в силу некоторых особенностей не в состоянии защитить свои права самостоятельно, к примеру несовершеннолетних. Обеспечение информационной безопасности детей в сегодняшних условиях является важной, актуальной задачей, нуждающейся во всестороннем рассмотрении в целях поиска эффективных методов защиты несовершеннолетних в цифровом пространстве.

Сам термин «информационная безопасность несовершеннолетних» трактуется современными исследователями по-разному. Так, Е.В. Никульченкова рассматривает информационную безопасность несовершеннолетних как составляющую личной неприкосновенности подростков. При этом личная неприкосновенность ребенка представляется как широкий комплекс его прав и свобод, а информационная безопасность выступает частью этого комплекса [1, с. 52]. Анализируя вопросы информационно-психологической безопасности несовершеннолетних, И.В. Тазин приходит к выводу, что психологическую основу концепции информационно-психологической безопасности личности образует теория деструктивности Э. Фромма [2, с. 221]. Но большинство исследователей приходят к обоснованному выводу о том, что информационная безопасность несовершеннолетних в первую очередь должна рассматриваться как часть национальной безопасности государства.

Традиционно выделяют трехуровневую систему субъектов обеспечения информационной безопасности:

– федеральные органы законодательной, исполнительной и судебной власти, исполнительные органы власти субъектов Российской Федерации, органы местного самоуправления;

– общественные объединения и организации;

– физические лица (граждане России, иностранные граждане и лица без гражданства), принимающие в соответствии с законодательством Российской Федерации участие в решении задач обеспечения информационной безопасности России [3, с. 40].

Начало XXI в. ознаменовалось практически повсеместным внедрением цифровых технологий в различные сферы жизнедеятельности человека. Распространение цифровых технологий в настоящее время происходит и в образовательной среде. Подтверждение этому — появление нового приоритетного проекта «Цифровая школа», реализация которого намечена на 2018–2025 гг. Одна из задач проекта заключается в формировании у школьников необходимых в современном мире навыков по обработке и

анализу данных, в изучении ими основных элементов программирования[1].

Интернет — уязвимая система, и этот аспект в сочетании с преимуществами, которые он предлагает (хранение, обработка и передача больших объемов данных, доступность, простота использования, дистанционная независимость, возможность применения в сфере бизнеса), превращает его также в благоприятную среду для криминальной деятельности, обусловливает возникновение нового криминального явления — киберпреступности [4, p. 53]. Виртуальный мир предоставляет людям, склонным к совершению преступлений, огромные возможности. Поскольку доступ киберпреступников к информации посредством сети Интернет упростился, угроза для интернет-пользователей стать жертвой преступления значительно возросла. При этом риск виктимизации среди детей и подростков гораздо выше, чем среди взрослых [5, p. 324].

Возможность использования информации, содержащейся в сети Интернет в открытом доступе, может крайне негативно повлиять на несовершеннолетних. Речь в первую очередь идет о преступлениях в отношении несовершеннолетних, совершаемых с использованием новейших информационных технологий.

Поскольку несовершеннолетние в силу возрастных и психологических особенностей развития, как правило, неспособны в полной мере осознавать все опасности, подстерегающие их в цифровом пространстве, необходимо принятие всесторонних мер виктимологической профилактики в сфере защиты прав и свобод несовершеннолетних в цифровом пространстве.

В век информационных технологий проблема защиты прав и свобод несовершеннолетних в цифровом пространстве является одной из приоритетных и требует внимательного изучения. Какие же угрозы подстерегают несовершеннолетних в цифровом пространстве? По данным социологических исследований, детская аудитория российского Интернета насчитывает 8–10 млн пользователей до 14 лет — это около половины всех детей, проживающих в Российской Федерации. При этом около 40 % детей, регулярно посещающих Сеть, просматривают интернет-сайты с агрессивным и нелегальным контентом, подвергаются киберпреследованиям и виртуальным домогательствам.

[1] Цифровые дети аналоговых родителей // Парламентская газета. 2018. 1 июня.

В целом киберугрозы традиционно подразделяются на три группы: программно-технические, к которым относится умышленное распространение вирусов и троянских программ; экономические, среди которых хищение и продажа данных кредитных карт, фишинг-атаки, взломы платежных аккаунтов; контентные, связанные с возможностью публичного, в том числе анонимного, размещения в сети Интернет любых материалов, включая незаконные, пропагандирующие, например, употребление наркотиков, призывающие к терроризму, экстремизму или суициду.

Именно третья группа киберугроз представляет особую опасность для подростков, поскольку контентные киберугрозы проявляются в том числе в пропаганде употребления наркотических средств, распространении детской порнографии, материалов террористического и экстремистского характера, а также другой информации девиантной направленности [6, с. 88].

Распространение детской порнографии посредством сети Интернет — проблема, характерная для большинства развитых стран, поэтому и меры борьбы с детской порнографией закреплены на международном уровне. Так, Конвенция о киберпреступности предусматривает уголовную ответственность за все деяния, связанные с созданием, производством, распространением и использованием любых детских порнографических изображений [7, p. 140].

Несовершеннолетние наиболее подвержены негативному влиянию извне. Иначе говоря, они обладают повышенной степенью виктимности. Поэтому проблема обеспечения информационной безопасности подростков может быть рассмотрена в двух аспектах: во-первых, как риск вовлечения несовершеннолетних в преступные сообщества посредством общения в социальных сетях; во-вторых, как риск совершения преступлений в отношении несовершеннолетних путем получения киберпреступниками персональных данных самих несовершеннолетних или их близких либо с помощью незаконного использования информационных технологий, либо в результате добровольного сообщения несовершеннолетними этих данных.

Не менее актуальной является угроза безопасности несовершеннолетних, связанная с суицидальными призывами к подросткам, осуществляемыми посредством сети Интернет. По количеству самоубийств среди несовершенно-

летних в возрасте от 15 до 19 лет Российская Федерация занимает первое место в Европе и одно из первых мест в мире. При этом каждый год более 200 малолетних и около 1,5 тыс. подростков совершает самоубийство [8, с. 13].

Коммуникативная активность несовершеннолетних связана с переносом определяющего влияния с родителей на ровесников. В связи с этим еще не до конца сформированная сфера ценностей и жизненных ориентиров у подростков претерпевает отрицательное и даже губительное влияние под воздействием негативной информации, содержащейся в социальных сетях [9, с. 211]. В частности, речь идет о публичных призывах к суициду, нивелировании отношения к жизни как к главной ценности.

Следующей не менее важной угрозой информационной безопасности несовершеннолетних является кибербуллинг — психологическое насилие по отношению к ним, осуществляемое посредством сети Интернет. В отличие от традиционного буллинга (травли), все действия, унижающие подростков, производятся в виртуальном пространстве с помощью информационных и коммуникационных технологий. И буллинг, и кибербуллинг несет двойную опасность, поскольку, с одной стороны, дети подвергаются травле, что негативно сказывается на их психологическом развитии, а иногда приводит к летальным последствиям. С другой стороны, травля подростков может подтолкнуть их самих на совершение противоправных действий, что, например, по мнению многих специалистов, и произошло со студентом колледжа в Керчи, расстрелявшим своих сверстников.

Полноценное развитие индивида возможно только в определенных условиях. Большое значение имеет качество межличностного общения и психологическая безопасность в образовательной среде. Проявление психологического насилия по отношению к несовершеннолетнему накладывает на его личность существенный отпечаток [10, с. 63]. Именно поэтому родителям, педагогам и психологам в школе важно своевременно выявлять подобные ситуации и пресекать их, важно проводить с детьми беседы с целью предупреждения травли. Однако если случаи буллинга еще можно выявить, поскольку они могут происходить на глазах других детей, а иногда и педагогов, то кибербуллинг выявить намного сложнее. Издевательства в Сети могут быть скрыты от посторонних глаз и быть известны только самому подростку, в отношении которого осуществляется травля. Именно поэтому так необходимо проводить профилактические мероприятия среди школьников, разъясняя, к каким последствиям это может привести.

Кибербуллинг представляет собой проблему международного уровня — травле в Интернете в настоящее время подвергаются подростки по всему миру. Изучение кибербуллинга следует осуществлять в контексте защиты прав несовершеннолетних, поскольку права ребенка должны пониматься широко, в том числе как право на уважительное отношение, на поддержку в обществе. Тем не менее во многих зарубежных исследованиях, посвященных кибербуллингу, вопрос о защите прав подростков отсутствует [11, p. 552].

Интересен тот факт, что родители в качестве основных угроз для их несовершеннолетних детей в цифровом пространстве видят интернет-зависимость и риски, связанные с экономической и технической безопасностью [12, с. 38].

Меры, направленные на защиту несовершеннолетних в сети Интернет, можно разделить на три группы: правовые, социальные и технические. Только их комплексное применение может иметь положительный результат [13, с. 53].

К *правовым* мерам относится законодательное регулирование вопросов информационной безопасности несовершеннолетних. В последние годы был принят ряд законодательных актов, закрепивших законодательные меры, касающиеся информационной безопасности несовершеннолетних, и в этом направлении наметились определенные позитивные сдвиги. Так, с 2006 г. в России действует федеральный закон «Об информации, информационных технологиях и о защите информации»[2], а в 2010 г. был принят федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию»[3]. Но при этом проблемы, связанные с созданием защищенной информационной среды, по-прежнему остаются актуальными, ведь законы зачастую не успевают за развитием информационных отношений, а законодатель не всегда может вовремя проследить ту или иную негативную тенденцию и, как следствие, не в состоянии оперативно противостоять новым рискам для подростков, появляющимся в Сети [14, с. 6].

[2] Российская газета. 2006. 29 июля.

[3] Там же. 2010. 31 дек.

Проблема обеспечения информационной безопасности несовершеннолетних осложняется тем, что Интернет является глобальной информационной средой, однако применяемые юридические механизмы обычно ограничены национальными рамками [15, с. 104]. В связи с этим представляется целесообразной консолидация усилий правоохранительных органов различных стран с целью обмена ресурсами для выявления, преследования и задержания киберпреступников [16, p. 84].

В этом аспекте интересен опыт Англии, где в 2016 г. был принят Закон о контрольных полномочиях, регламентирующий новые требования к хранению данных о поставщиках интернет-услуг, согласно которому необходимо хранить записи о подключении к Интернету в течение 12 месяцев, что обеспечивает возможность ретроспективно их исследовать [17, p. 112].

Социальные меры, направленные на защиту прав и свобод несовершеннолетних в цифровом пространстве, должны осуществляться целым рядом субъектов: родителями, педагогами, специально созданными организациями. К социальным мерам обеспечения информационной безопасности несовершеннолетних относятся создание и внедрение программ обучения детей и подростков правилам безопасного поведения в интернет-пространстве, профилактики интернет-зависимости, предупреждения рисков вовлечения в противоправную деятельность [18, с. 28]. Данная задача представляется актуальной прежде всего для образовательных учреждений. Большинство учебников по информатике базового уровня формирует у учащихся неполную базу личной информационной безопасности в современной информационной среде. Так, в них не рассматриваются вопросы, связанные с навыками фильтрации нежелательного контента в Интернете, противодействия деструктивным программам, фишингу, психологическим преследованиям в Сети, а также касающиеся профилактики интернет-зависимости у детей. Это может негативно повлиять на психологическое и нравственное здоровье школьников [19, с. 65].

Правовое просвещение детей и подростков по поводу опасностей и угроз, возникающих в сети Интернет, является приоритетной задачей профилактики правонарушений в Сети. В рамках решения данной задачи в 2008 г. был создан Национальный узел интернет-безопасности в России (в настоящее время является интернет-СМИ «Центр безопасного Интернета в России»)[4]. На сайте Центра действует горячая линия, на которую дети и подростки могут сообщить о противоправном контенте, а также линия помощи жертвам интернет-угроз.

В рамках проекта «Дети онлайн» разработаны материалы, посвященные безопасному поведению в Интернете. На сайте фонда «Дружественный Рунет» доступны рекомендации для детей, родителей и педагогов по предотвращению рисков, связанных с использованием несовершеннолетними сети Интернет.

Еще одной социальной мерой профилактики киберугроз для подростков является проведение единых уроков безопасности школьников в сети Интернет. Единый урок, впервые проведенный в 2014 г., а в 2016 г. прошедший более чем в 36 тыс. школ и в 350 библиотеках России, — это результат совместных усилий государства, общества и представителей IT-отрасли, направленных на то, чтобы сделать интернет-пространство безопасным для подростков[5].

С 2012 г. Координационным центром национальных доменов .RU и .РФ при поддержке ПАО «Ростелеком» реализуется социально-образовательный проект для школьников «Изучи Интернет — управляй им». Проект позволяет подросткам получить базовые знания об устройстве сети Интернет. Цель проекта заключается в повышении уровня цифровой грамотности несовершеннолетних пользователей Интернета в современной интерактивной форме[6].

Несмотря на ряд предпринимаемых мер, следует констатировать, что российские школьники пока в должной степени не вовлечены в просветительский процесс, направленный на обучение информационной безопасности в сети Интернет на постоянной основе. На уроках информатики не проводится каких-либо специальных мероприятий, посвященных информационной безопасности. В рамках иных школьных предметов такое обучение также отсутствует. Тема информационной безопасности, включая защиту от кибербуллинга, может затрагиваться в рамках классных часов, при этом данные занятия не носят системный характер, а проходят в связи с возникновением какой-либо ситуации в классе, школе, городе или стране. Причем учителя, которые проводят такие занятия, как правило, сами не владеют

[4] URL: http://www.saferunet.ru.

[5] Дети в информационном обществе. 2017. № 4 (26). (Спец. вып.: Единый урок безопасности).

достаточным уровнем правовых и информационных знаний, необходимым для ознакомления детей с темой. Следует констатировать, что многие современные подростки в сфере информационных технологий, включая информационную безопасность, знают много больше своих учителей информатики.

Выходов из сложившейся ситуации может быть несколько. В первую очередь необходимо проводить курсы повышения квалификации для самих учителей, повышая их уровень знаний и умений в сфере информационной безопасности в сети Интернет. Такие курсы могут проходить как в традиционной форме, так и онлайн. Сейчас их предлагается достаточно много.

Одним из способов повышения правовой и информационной грамотности детей в сфере информационной безопасности может стать проведение занятий по правовому просвещению, по информационной гигиене. Такие занятия могут организовывать, например, юридические клиники вузов в рамках программ правового просвещения. Так, Центр бесплатной правовой помощи (юридическая клиника) Волгоградского института управления — филиала РАНХиГС на регулярной основе проводит такие занятия на базе школ для учеников разных классов, а также на базе Волгоградской областной библиотеки для молодежи. В рамках занятий школьникам рассказывается о юридически грамотном поведении в сети Интернет, о необходимости соблюдения этических норм в киберпространстве, правовых последствиях кибербуллинга, иных форм нарушений, дети получают знания об информационной безопасности с точки зрения раскрытия персональных данных и пр. Несмотря на то что интернет-среда для подростков становится обычной, многие из них не задумываются о последствиях своих действий в Интернете. Очень важно, чтобы подобные занятия проводились не только в форме лекций, но и в практической форме, чтобы несовершеннолетние могли получить необходимые им навыки.

Повышение уровня технической грамотности детей и подростков и проведение соответствующих занятий могли бы взять на себя студенты технических вузов в рамках осуществления волонтерской деятельности.

Технические меры обеспечения защиты прав и свобод несовершеннолетних в сети Интернет имеют свою специфику. Борьба с некорректным поведением в цифровом пространстве (кибербуллинг, клевета, распространение персональных сведений) ведется по двум направлениям. В первую очередь это развитие технических приспособлений, ограничивающих нежелательный контент (настраиваемые пользователями фильтры, использование цензуры), возможность пожаловаться на оскорбительное поведение в социальных сетях и на веб-сайтах администрации данного ресурса (так называемые кнопки тревоги), а также возможность установить настройки конфиденциальности персональных аккаунтов. С другой стороны, осуществляется обучение пользователей Интернета основным правилам безопасности и корректного поведения по отношению к другим пользователям [20, с. 186–187].

Следует отметить, что названные выше способы не могут в полной мере защитить пользователей от некорректного поведения в цифровом пространстве. Нередки случаи, когда администрация ресурса применяет меры взыскания к нарушителям несвоевременно либо не реагирует на жалобы пользователей вовсе. Что касается самих нарушителей, они могут вместо заблокированных по жалобам других пользователей аккаунтов создавать новые, вымышленные, и продолжать свои действия против жертвы.

В последнее время в различных странах получила распространение обширная анонимная сеть — так называемая Deep Web («Глубокая паутина»), представляющая собой группу сайтов, которые находятся в зашифрованном сетевом пространстве и поэтому не могут быть обнаружены традиционными поисковыми механизмами. Основная цель анонимных веб-сайтов — хранить не предназначенную для широкой общественности информацию, часто используемую для преступной деятельности, связанной с торговлей наркотиками, мошенничеством в финансовой сфере, незаконным оборотом оружия, шпионажем, сексуальным надругательством над несовершеннолетними [21, p. 414]. Анонимные веб-сайты могут быть также использованы в преступных целях. Например, известны случаи онлайн-продажи наркотиков через анонимный сайт Silk Road. При этом данные сайты не в состоянии гарантировать полную защиту от хакерских атак.

Таким образом, в настоящее время существует ряд правовых, социальных и технических мер, призванных обеспечивать информационную безопасность несовершеннолетних. Тем не менее следует констатировать их недостаточ-

ISSN 2500-4255

ную эффективность в связи с отсутствием комплексного подхода, слаженной деятельности уполномоченных субъектов. С другой стороны, сама сфера защиты подростков от негативного воздействия в цифровом пространстве быстро меняется, обрастает все новыми угрозами со стороны киберпреступников.

Проблема защиты несовершеннолетних в цифровом пространстве является комплексной, поскольку для ее успешного решения необходима консолидация усилий целого ряда субъектов в лице как уполномоченных органов и учреждений, так и общественных объединений и граждан.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Никульченкова Е.В. Информационная безопасность несовершеннолетних как составляющая личной неприкосновенности / Е.В. Никульченкова // Криминология: вчера, сегодня, завтра. — 2016. — № 4 (43). — С. 52–56.

2. Тазин И.В. Правовое обеспечение информационно-психологической безопасности несовершеннолетних / И.В. Тазин // Вестник Томского государственного педагогического университета. — 2012. — № 6 (121). — С. 220–225.

3. Занина Т.М. Формирование государственной защиты несовершеннолетних от вредоносной информации в Российской Федерации / Т.М. Занина, Е.И. Лукина // Научный вестник Омской академии МВД России. — 2016. — № 3 (62). — С. 40–44.

4. Drăgan A.T. Child Pornography and Child Abuse in Cyberspace / A.T. Drăgan // Journal of Legal Studies. — 2018. — Vol. 21, iss. 35. — P. 52–60.

5. Ates E. Cybercrimes Against Children in Turkey / E. Ates, E. Bostanci, M. Guzel // 6th International Symposium on Digital Forensic and Security (ISDFS). — 2018. — P. 324–329.

6. Хохлова Н.И. Обеспечение детской безопасности в Интернете: российский опыт и зарубежные инициативы / Н.И. Хохлова // Пространство и время. — 2012. — № 1. — С. 87–92.

7. Jalil J. Combating Child Pornography in Digital Era: Is Malaysian Law Adequate to Meet the Digital Challenge? / J. Jalil // Pertanika Journal of Social Science and Humanities. — 2015. — Vol. 23. — P. 137–152.

8. Брылева Е.А. Информационная безопасность несовершеннолетних как часть национальной безопасности / Е.А. Брылева // Вестник Самарского юридического института. — 2014. — № 1 (12). — С. 12–14.

9. Сашенков С.А. Роль социальных сетей в формировании суицидального поведения у несовершеннолетних / С.А. Сашенков // Общество и право. — 2017. — № 1 (59). — С. 210–212.

10. Баранов А.А. Кибербуллинг — новая форма угрозы безопасности личности подростка / А.А. Баранов, С.В. Рожина // Вестник Балтийского федерального университета им. И. Канта. Сер.: Филология, педагогика, психология. — 2015. — Вып. 11. — С. 62–66.

11. Pare M. Taking Stock of Bullying and Cyberbullying Research and Introducing a Child Rights Perspective / M. Pare // United Nations Convention on the Rights of the Child: Taking Stock After 25 Years and Looking Ahead / ed. T. Liefaard, J. Sloth-Nielsen. — Boston : Brill, 2017. — P. 541–563.

12. Федяй Д.С. Обращение детей и подростков к возможностям Интернета в контексте комплексной безопасности личности / Д.С. Федяй // Вестник Саратовского областного института развития образования. — 2015. — № 1. — С. 34–43.

13. Букалерова Л.А. Правовые, организационные, технические меры противодействия призывам к самоубийствам несовершеннолетних в сети «Интернет» / Л.А. Букалерова, В.С. Лавелина, А.В. Остроушко // Ученые труды Российской академии адвокатуры и нотариата. — 2017. — № 3 (46). — С. 48–57.

14. Архирейская Т.Ю. Правовая защита детей от информации, причиняющей вред их здоровью и развитию / Т.Ю. Архирейская // Труды Оренбургского института (филиала) Московской государственной юридической академии. — 2018. — № 35. — С. 5–9.

15. Бородин К.В. Проблемы правового регулирования безопасности в интернет-среде / К.В. Бородин // Вестник ЮУрГУ. Сер.: Право. — 2013. — Т. 13, № 3. — С. 104–105.

16. Dubord P. Investigating Cybercrime / P. Dubord // Handbook of Digital and Multimedia Forensic Evidence / ed. J.J. Barbara. — Berlin : Springer, 2008. — P. 77–89.

17. Horsman G. Combatting those who Intentionally Access Images Depicting Child Sexual Abuse on the Internet: A Call for a New Offence in England and Wales / G. Horsman // Computer Law & Security Review. — 2018. — Vol. 34, iss. 1. — P. 111–124.

18. Кучма В.Р. Охрана здоровья детей и подростков в Национальной стратегии действий в интересах детей на 2012–2017 г. / В.Р. Кучма // Гигиена и санитария. — 2013. — № 6. — С. 26–30.

19. Проблемы обучения школьников безопасному использованию средств ИКТ / М.С. Анурьева, Н.Л. Королева, К.И. Остапчук [и др.] // Психолого-педагогический журнал «Гаудеамус». — 2017. — Т. 16, № 1. — С. 63–68.

20. Бочавер А.А. Кибербуллинг: травля в пространстве современных технологий / А.А. Бочавер, К.Д. Хломов // Психология. Журнал Высшей школы экономики. — 2014. — Т. 11, № 3. — С. 177–191.

21. Tomazic T. Ongoing Criminal Activities in Cyberspace: From the Protection of Minors to the Deep Web / T. Tomazic, N. Vilela // Revija za Kriminalistiko in Kriminologijo. — 2017. — Vol. 68, iss. 4. — P. 412–423.

REFERENCES

1. Nikulchenkova E.V. Information Security of the Juniors as a Component of Personal Inviolability. *Kriminologiya: vchera, segodnya, zavtra = Criminology: Yesterday, Today, Tomorrow,* 2016, no. 4 (43), pp. 52–56. (In Russian).

2. Tazin I.I. Legal Security for Information Psychological Safety of Minors. *Vestnik Tomskogo gosudarstvennogo pedagogicheskogo universiteta = Tomsk State Pedagogical University Bulletin*, 2012, no. 6 (121), pp. 220–225. (In Russian).

3. Zanina T.M., Lukina Ye.I. Building the National System of Juvenile Protection from Harmful Information in the Russian Federation. *Nauchnyi vestnik Omskoi akademii MVD Rossii = Scientific Bulletin of the Omsk Academy of the MIA of Russia,* 2016, no. 3 (62), pp. 40–44. (In Russian).

4. Drăgan A.T. Child Pornography and Child Abuse in Cyberspace. *Journal of Legal Studies,* 2018, vol. 21, iss. 35, pp. 52–60.

5. Ates E., Bostanci E., Guzel M. Cybercrimes Against Children in Turkey. *6th International Symposium on Digital Forensic and Security* (*ISDFS)*, 2018, pp. 324–329.

6. Khokhlova N.I. Providing the Safety of Children on the Internet: the Russian Experience and International Initiatives. *Prostranstvo i vremya = Space and Time,* 2012, no. 1, pp. 87–92. (In Russian).

7. Jalil J. Combating Child Pornography in Digital Era: Is Malaysian Law Adequate to Meet the Digital Challenge? *Pertanika Journal of Social Science and Humanities,* 2015, vol. 23, pp. 137–152.

8. Bryleva E.A. Information Security of Juvenile as Part of National Security. *Vestnik Samarskogo yuridicheskogo instituta = Bulletin of the Samara Law Institute,* 2014, no. 1 (12), pp. 12–14. (In Russian).

9. Sashenkov S.A. The Role of Social Networks in the Formation of Suicidal Behaviour among Minors. *Obshchestvo i pravo = Society and Law,* 2017, no. 1 (59), pp. 210–212. (In Russian).

10. Baranov A.A., Rozhina S.V. Cyberbullying, a New Threat to Adolescents' Personal Security. *Vestnik Baltiiskogo federal'nogo universiteta im. I. Kanta. Seriya: Filologiya, pedagogika, psikhologiya = Bulletin of Immanuel Kant Baltic Federal University. Series: Philology, Pedagogy, Psychology,* 2015, iss. 11, pp. 62–66. (In Russian).

11. Pare M. Taking Stock of Bullying and Cyberbullying Research and Introducing a Child Rights Perspective. In Liefaard T., Sloth-Nielsen J. (eds.). *United Nations Convention on the Rights of the Child: Taking Stock After 25 Years and Looking Ahead*. Boston, Brill, 2017, pp. 541–563.

12. Fedyai D.S. Children and Teenagers Reference to Internet: a Complex Safety of User's Person. *Vestnik Saratovskogo oblastnogo instituta razvitiya obrazovaniya = Bulletin of the Saratov Regional Institute of Education Development,* 2015, no. 1, pp. 34–43. (In Russian).

13. Bukalerova L.A., Laevelina V.S., Ostroushko A.V. Legal, Organizational, Technical Measures to Counter Appeals for Suicides of Minors in the Internet Network. *Uchenye trudy Rossiiskoi akademii advokatury i notariata = Scientific Works of the Russian Academy of Advocacy and Notary,* 2017, no. 3 (46), pp. 48–57. (In Russian).

14. Arkhireyskaia T.Yu. Legal Protection of Children from Information, Doing Harm to their Health and Development. *Trudy Orenburgskogo instituta (filiala) Moskovskoi gosudarstvennoi yuridicheskoi akademii = Proceedings of Orenburg Institute (Branch) of Moscow Juridical Academy,* 2018, no. 35, pp. 5–9. (In Russian).

15. Borodin K.V. Issues on Legal Regulation of Security in the Internet. *Vestnik Yuzhno-Ural'skogo gosudarstvennogo universiteta. Seriya: Pravo = Bulletin of South Ural State University. Series: Law,* 2013, vol. 13, no. 3, pp. 104–105. (In Russian).

16. Dubord P. Investigating Cybercrime. In Barbara J.J. (ed.). *Handbook of Digital and Multimedia Forensic Evidence*. Berlin, Springer, 2008, pp. 77–89.

17. Horsman G. Combatting those who Intentionally Access Images Depicting Child Sexual Abuse on the Internet: A Call for a New Offence in England and Wales. *Computer Law & Security Review,* 2018, vol. 34, iss. 1, pp. 111–124.

18. Kuchma V.R. National Strategy for Action for Children for 2012–2017 School Health and Objectives. *Gigiena i sanitariya = Hygiene and Sanitation*, 2013, no. 6, pp. 26–30. (In Russian).

19. Anuryeva M.S., Koroleva N.L., Ostapchuk K.I., Puzanova Ya.M., Lopatin D.V. Problems of Training of School Students to Safe Use of Means of ICT. *Psikhologo-pedagogicheskii zhurnal «Gaudeamus» = Psychological-Pedagogical Journal GAUDEAMUS,* 2017, vol. 16, no. 1, pp. 63–68. (In Russian).

20. Bochaver A.A., Khlomov K.D. Cyberbullying: Harassment in the Space of Modern Technologies. *Psikhologiya. Zhurnal Vysshei shkoly ekonomiki = Psycholocy journal of the Higher School of Economics,* 2014, vol. 11, no. 3, pp. 177–191. (In Russian).

21. Tomazic T., Vilela N. Ongoing Criminal Activities in Cyberspace: From the Protection of Minors to the Deep Web. *Revija za Kriminalistiko in Kriminologijo,* 2017, vol. 68, iss. 4, pp. 412–423.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Миронова Светлана Михайловна — директор Центра бесплатной правовой помощи (юридической клиники) Волгоградского института управления — филиала Российской академии народного хозяйства и государственной службы, кандидат юридических наук, доцент, г. Волгоград, Российская Федерация; e-mail: smironova2017@gmail.com.

Симонова Светлана Сергеевна — доцент кафедры уголовно-правовых дисциплин Волгоградского института управления — филиала Российской академии народного хозяйства и государственной службы, кандидат юридических наук, г. Волгоград, Российская Федерация; e-mail: simonova.ss@mail.ru.

ДЛЯ ЦИТИРОВАНИЯ

Миронова С.М. Защита прав и свобод несовершеннолетних в цифровом пространстве / С.М. Миронова, С.С. Симонова. — DOI: 10.17150/2500-4255.2020.14(2).234-241 // Всероссийский криминологический журнал. — 2020. — Т. 14, № 2. — С. 234–241.

INFORMATION ABOUT THE AUTHORS

Mironova, Svetlana M. — Director, Center for Free Legal Aid (Legal Clinic), Volgograd Institute of Management — branch of the Russian Academy of National Economy and Public Administration, Ph.D. in Law, Ass. Professor, Volgograd, the Russian Federation; e-mail: smironova2017@gmail.com.

Simonova, Svetlana S. — Ass. Professor, Chair of Criminal Law Disciplines, Volgograd Institute of Management — branch of the Russian Academy of National Economy and Public Administration, Ph.D. in Law, Volgograd, the Russian Federation; e-mail: simonova.ss@mail.ru.

FOR CITATION

Mironova S.M., Simonova S.S. Protection of the rights and freedoms of minors in the digital space. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2020, vol. 14, no. 2, pp. 234–241. DOI: 10.17150/2500-4255.2020.14(2).234-241. (In Russian).