Фурман Т. Г.,
Исмаилова Э.В.♦

DOI: 10.25108/2304-1730-1749.iolr.2025.79.96-110
УДК: 377.8

Правовое обеспечение безопасности несовершеннолетних в цифровом пространстве

Аннотация. Предмет. Цифровое пространство, как ресурс для самовыражения и получения знаний, так и потенциальная среда повышенного риска, затрагивающая права и интересы несовершеннолетних, и, как следствие, зафиксированный рост числа правонарушений в онлайн-среде. В связи с этим возрастает необходимость в формировании и совершенствовании правовых механизмов, обеспечивающих защиту детей в условиях цифровизации.

Цель. Настоящее научное исследование представляет комплексный анализ правовых подходов, направленных на обеспечение безопасности несовершеннолетних в онлайн-среде.

Методологическая основа. Использованы общенаучные методы (анализ, синтез международных и национальных нормативно-правовых актов, научной литературы, а также контент-анализ актуальных источников) и специальные юридические методы (сравнительно-правовой анализ нормативных правовых актов и научных публикаций по теме), формально-юридический метод.

Результаты. В ходе научного исследования рассмотрено влияние интернета на развитие и поведение несовершеннолетних, классифицированы основные риски, возникающие в онлайн-пространстве.

Выводы. Дана правовая оценка существующим механизмам защиты детей как на национальном, так и на международном уровнях. Сформулированы предложения по созданию более эффективной системы правового регулирования в данной области.

Ключевые слова: Интернет, права детей, сексуальная эксплуатация детей, интернет-риски, киберпреступления, кибербуллинг, онлайн-груминг (онлайн-ухаживание).

Введение.

С развитием технологий повсеместно наблюдается, что дети и молодёжь проводят всё больше времени в интернете, а последствия этого времени могут иметь как положительный, так и отрицательный характер [1; 3]. Онлайн-среда предоставляет детям множество возможностей – быстрое обучение, выполнение домашних заданий, игры, социализацию и др. При

♦ **Фурман Татьяна Геннадьевна -** кандидат культурологии, доцент кафедры конституционного и административного права Северо-Западного института управления - филиала федерального государственного бюджетного образовательного учреждения высшего образования «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации» РАНГХиГС, Санкт- Петербург. E-mail: *furman-tg@ranepa.ru*

Исмаилова Эсмира Вагиф кызы - магистрант 1 курса юридического факультета заочной формы обучения программы «Регулирование и защита прав и свобод человека и гражданина» Северо-Западного института управления - филиала федерального государственного бюджетного образовательного учреждения высшего образования «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации» РАНГХиГС, Санкт- Петербург. E-mail: e. ismayilova414@gmail.com

этом важнее не то, сколько времени они проводят в сети, а последствия проведённого в интернете времени.

Учитывая неограниченный характер глобальной сети Интернет, не все ресурсы, доступные для детей, разработаны с соблюдением их прав, обеспечения безопасности и благоприятного развития. В целях защиты прав детей в цифровом пространстве требуется принятие нормативно-правовых актов, направленных на обеспечение их безопасности в онлайн-среде, а также на минимизацию возможных рисков [11; 14].

Руководство (контроль) со стороны родителей или опекунов детей, а также со стороны учителей в школе играет важную роль в обеспечении более безопасного онлайн-опыта детей. Такое руководство включает помощь детям в ориентировании в цифровом пространстве, общение с ними об их онлайн-опыте, обучение их избеганию онлайн-угроз и оказание поддержки в случае возникновения опасных ситуаций [16].

Цифровое пространство характеризуется созданием контента и разработкой платформ, направленных на привлечение внимания пользователей, включая несовершеннолетних, с целью увеличения времени их пребывания в сети. Такие онлайн-практики могут приводить к риску доступа детей к противоправной и вредоносной информации. В связи с этим внедрение эффективных механизмов родительского контроля и обеспечение мер интернет-безопасности имеют первостепенное значение для предотвращения потенциальных онлайн-угроз и защиты прав детей на здоровое развитие [3; 6].

В данной научной статье изучаются правовые подходы, направленные на защиту детей от потенциальных опасностей в онлайн-среде, и предлагаются меры по созданию более безопасной онлайн-среды. Основная цель – понять риски и угрозы, с которыми сталкиваются дети в цифровом мире, эффективно их минимизировать и способствовать обеспечению для детей безопасной жизни в онлайн-среде [1; 5].

1. Влияние интернета на детей.

В настоящее время влияние интернета на детей приобретает особую значимость, особенно в связи с ростом социальных сетей [7]. Раннее знакомство детей с цифровым миром оказывает глубокое влияние на их образ жизни и поведение. В этом контексте понимание и оценка воздействия социальных сетей на детей становится критически важной задачей как для родителей, так и для педагогов [3; 4].

Интернет стал важным ресурсом, который сильно влияет на жизнь детей. Особенно это касается доступа к информации и образования. Он открывает перед детьми множество знаний и возможностей для обучения.[1; 4]. Однако наряду с полезным контентом всемирная сеть также представляет собой платформу, способную указать путь детям к вредным материалам или вызывающим зависимость играм и видео. В сфере социальных связей и общения интернет облегчает детям взаимодействие со сверстниками, но одновременно повышает риск столкновения с преступностью и формирования зависимостей [7; 12].

Для безопасного использования интернета детьми необходимо совместное участие общества и повышение осведомленности [6; 12]. Безопасное и осознанное использование интернета возможно благодаря совместным усилиям родителей, педагогов и общества в целом. Эти усилия помогут обеспечить детям безопасную интеграцию в цифровую среду, защитят их от противоправного и вредного контента [5; 16].

Родители и учителя должны оказывать детям подробное руководство в вопросах использования интернета и принимать различные меры безопасности для защиты детей от противоправного и вредного контента в онлайн-среде [1; 3].

2.Влияние социальных сетей на детей.

Одним из основных воздействий социальных сетей является изменение отношений детей в социуме [9]. Общение через социальные сети формирует и развивает социальные навыки детей, но в то же время отрицательно влияет на их навыки личного общения в реальной жизни. Мгновенные коммуникационные возможности, предоставляемые социальными сетями, затрудняют развитие эмоциональной зрелости у детей, что может приводить к недостатку эмпатии [7; 12].

Таким образом, влияние социальных сетей на детей связано с ослаблением социальных навыков и дефицитом эмоционального развития [8].

Для понимания и управления воздействием социальных сетей необходимо разрабатывать эффективные стратегии [16; 17]. Родители должны обучать детей безопасному поведению в цифровой среде и регулярно отслеживать их онлайн-взаимодействия. Также образовательные учреждения должны проводить обучение и инструктаж по цифровой грамотности и оказывать поддержку детям в позитивной организации онлайн-коммуникации [4].

Но, помимо прочего, социальные сети предоставляют несовершеннолетним доступ к ресурсам, которые способствуют культурному обогащению, включая контент на различных языках, ознакомление с культурными особенностями различных стран и возможность социальной интеграции. Кроме того, они обеспечивают доступ к учебным видеоматериалам, интерактивным образовательным играм и другим обучающим ресурсам, что способствует повышению уровня знаний и компетенций у детей. [5].

Важно не запрещать использование социальных сетей, а поощрять и обеспечивать их безопасное использование под контролем родителей и с повышением осведомлённости [6; 16].

С увеличением времени, проводимого детьми в социальных сетях, возникают трудности в управлении своим временем. Чрезмерное использование сокращает время, которое могло бы быть потрачено на обучение, подвижные игры и взаимодействие в реальной жизни. Это создаёт риск цифровой зависимости. Кроме того, анонимность и доступность онлайн-общения создают благоприятные условия для распространения интернет травли, что может привести к серьёзным психологическим последствиям для её жертв.

Отсутствие у родителей осознания необходимости защиты конфиденциальности детей в социальных сетях увеличивает риск попадания личных данных в руки злоумышленников. Чрезмерное использование социальных сетей также приводит к проблемам с концентрацией внимания и к одиночеству [13; 24].

В результате социальные сети предоставляют детям как возможности, так и представляют угрозы. Родители и педагоги должны активно совместно участвовать в защите детей в сети интернет, заниматься их цифровой грамотностью и безопасным использованием цифровых устройств [5; 25].

3. Основные виды рисков в интернете для детей.

Дети могут выступать как потребителями, так и авторами цифрового контента, активно участвуя в онлайн-пространстве. Иногда у них появляется любопытство к определённым ви-

дам поведения, которые могут быть рискованными и вредными [3]. Наиболее распространённые риски, с которыми дети могут столкнуться в интернете, включают:

- поддельные новости и ложь,
- недопустимый контент,
- крайние взгляды,
- онлайн-груминг (завлечение с целью сексуальной эксплуатации),
- материалы, содержащие сексуальную эксплуатацию детей,
- нарушение конфиденциальности и хищение личных данных,
- приёмы, вынуждающие проводить в сети чрезмерное время,
- секстинг (обмен сексуально-откровенными сообщениями и изображениями),
- кибербуллинг.

В современном мире онлайн-безопасность детей и потенциальные риски – серьёзный повод для беспокойства [1; 5]. Дети в интернете могут подвергнуться влиянию ложной информации, обмана, психологических и сексуальных атак, а также столкнуться с незаконным и опасным содержимым [18; 19]. Эти риски серьёзно влияют на психическое и эмоциональное здоровье детей, затрудняя получение безопасного онлайн-опыта [3; 12].

Именно поэтому чрезвычайно важно, чтобы педагоги и родители осмысливали проблемы онлайн-безопасности и помогали детям справляться с потенциальными угрозами [5; 6]. Также нужно разными способами обеспечивать безопасный доступ детей к достоверной информации и создавать безопасную интернет-среду [2; 11].

В настоящее время в мире реализуется ряд мер и стратегий по обеспечению онлайн-безопасности детей и борьбе с потенциальными рисками:

- правовое регулирование и законодательные рамки со стороны правительств,
- международное сотрудничество и координация усилий с гражданским обществом,
- инициативы со стороны технологических компаний,
- информирование родителей,
- образовательные программы в учебных заведениях.

Помимо внедрения общих мер по защите детей от цифровых угроз, необходимо обеспечить подготовку педагогов, учителей и других специалистов, работающих с несовершеннолетними и молодёжью, посредством специализированных образовательных программ. Такие программы должны учитывать возрастные категории, региональные, культурные и религиозные особенности соответствующих групп [5; 16].

Образовательные учреждения обязаны предпринимать меры технического и программного характера для ограничения доступа к контенту, не соответствующему установленным законодательным требованиям и нормам, в дополнение к использованию фильтров родительского контроля при интернет-доступе [5; 26]. Необходимо разрабатывать и совершенствовать как технические, так и правовые механизмы борьбы с вредным контентом на глобальном уровне [14; 19].

Особое внимание – защите конфиденциальности данных детей.

В условиях стремительного развития технологий право на неприкосновенность частной жизни приобретает всё большее значение [5]. Угрозы приватности исходят как от государственных структур, так и от частных компаний, а также включают преступные действия [13; 27].

Публикация изображений и персональных данных несовершеннолетних в сети Интернет, осуществляемая родителями или третьими лицами, может повлечь за собой нарушение их прав и законных интересов, а также создать угрозу их безопасности [13; 27]. Поэтому государства должны регулярно пересматривать свои законы о защите данных и обеспечивать механизмы предотвращения нарушений конфиденциальности [27; 28].

Онлайн-груминг (онлайн-ухаживание).

Онлайн-груминг – это процесс установления контакта с ребёнком в интернете с целью подготовки его к сексуальной эксплуатации. Злоумышленники создают доверительные отношения через электронную почту, мессенджеры, социальные сети, чаты, игровые платформы, приложения для знакомств и обмена фотографиями [18; 19].

Современные технологии позволяют преступникам:

- скрывать свой возраст и личность;
- создавать ложный образ для завоевания доверия ребёнка;
- вовлекать детей в сексуальную активность [18].

Прямая трансляция сексуального насилия над детьми.

Отдельным видом преступлений является прямая трансляция сексуального насилия над детьми. В отличие от классической порнографии, такие трансляции:

- идут в режиме реального времени (потоковое видео);
- не оставляют цифровых следов на устройствах пользователя;
- позволяют злоумышленникам взаимодействовать с трансляцией в реальном времени [18].

Этот вид преступлений ещё называют «по требованию» (on-demand child sexual abuse) [18].

4. Международные меры по борьбе с онлайн-эксплуатацией детей.

В борьбе с преступлениями, направленными против детей в онлайн-среде, применяются различные меры и практики в зависимости от технических возможностей и законодательства стран [15]. Для удаления противоправных материалов и ограничения доступа к ним применяются различные механизмы правового регулирования. Международное сообщество квалифицирует онлайн-эксплуатацию детей как тяжкое преступление, требующее незамедлительных и эффективных мер воздействия [18; 19]. Например:

– Франция применяет смешанную систему, при которой удаление противоправного контента или ограничение доступа осуществляется под контролем независимого административного органа, отвечающего за обеспечение свободы выражения мнений в интернете (Закон о цифровой экономике Франции, 2004 г.).

– В таких странах, как США, у интернет-компаний существуют самостоятельные обязательства по борьбе с онлайн-эксплуатацией детей и детской порнографией без необходимости получения административного или судебного решения (Закон о защите детей в интернете, 2000 г.) [19].

Международное сотрудничество и INHOPE (International Association of Internet Hotlines).

Международное сотрудничество играет важную роль в регулировании интернет-контента. Одной из таких организаций является INHOPE.

INHOPE:

- принимает сообщения о противоправном контенте;
- анализирует контент;
- определяет местоположение хостинга;
- передаёт информацию в правоохранительные органы (в зависимости от законодательства конкретной страны) [14].

INHOPE объединяет 52 горячие линии в 40 странах, работает в сотрудничестве с INTERPOL и активно борется с материалами сексуальной эксплуатации детей и расистскими материалами в интернете [14; 25].

Различия между странами.

Хотя сотрудничество и существует, в тоже время между странами наблюдаются различия в стратегиях борьбы с онлайн-эксплуатацией детей. Каждая страна разрабатывает свои механизмы, соответствующие её собственному внутреннему законодательству:

- В США интернет-компании берут на себя этическую и правовую ответственность, активно участвуя в профилактике распространения детской порнографии[19].
- В Европе борьба ведётся в рамках более широких межгосударственных программ (например, Better Internet for Kids) [26].

Образовательные и профилактические меры.

В США концепции "цифрового гражданства" и "цифровой грамотности" активно внедряются в программы обучения [16]:

- Google, Microsoft и другие IT-компании разрабатывают учебные материалы;
- Организации Common sense Media и i-SAFE создают обучающие модули, охватывающие темы безопасного интернета, кибербуллинга, конфиденциальности и цифровой репутации [16].

В Европе аналогичные программы реализуются через сеть INSAFE –European network of Awareness Centres promoting safer and better usage of Internet (Европейская сеть центров повышения осведомлённости, продвигающих более безопасное и ответственное использование Интернета), поддерживаемую Евросоюзом [17].

INSAFE:

- предоставляет информацию и рекомендации детям, родителям и педагогам по безопасному использованию интернета;
- организует ежегодный День безопасного интернета (Safer Internet Day), который проводится в более, чем 130 странах мира [17].

Три уровня профилактики.

В дополнение к правовым мерам используются следующие профилактические инструменты:

1. Программные фильтры, устанавливаемые на устройства пользователей [6].
2. Централизованная система фильтрации (например, в Турции – услуга "Безопасный Интернет") [15].
3. Мероприятия по повышению осведомлённости и просвещению населения.

Несмотря на важность фильтров, полного устранения угроз они не обеспечивают. Поэтому ключевую роль играет формирование культуры осознанного и безопасного поведения в интернете [3; 16].

5. Защита детей в онлайн-среде с точки зрения прав ребёнка: Международные договоры.

Правовое регулирование защиты детей в интернет-среде включает не только карательные, но и профилактические меры, а также программы повышения осведомлённости [5]. Законы, направленные на защиту детей от интернет-угроз, играют важную роль в обеспечении общественной безопасности и здорового развития детей [19].

5.1 Конвенция ООН о правах ребёнка.

Конвенция ООН о правах ребёнка (CRC, 1989 г.) – это международный договор в сфере прав человека, который закрепляет гражданские, политические, экономические, социальные, медицинские и культурные права детей [20]. Согласно указанной Конвенции, ребёнком признается каждое лицо младше 18 лет, если по национальному законодательству не предусмотрено наступление совершеннолетия в более раннем возрасте.

В числе других международных соглашений важное место занимает Конвенция Совета Европы о киберпреступности (Будапештская конвенция 2001 г.) [19]. В статье 9 этой Конвенции даётся расширенное определение преступлений, связанных с детской порнографией в интернет-среде.

Дополнительные международные инструменты: в 2014 году был принят третий факультативный протокол, предоставляющий детям право непосредственно подавать жалобы в Комитет по правам ребёнка [20].

Таким образом, государства-участники взяли на себя обязательства:

- обеспечивать детям право на выражение мнения,
- гарантировать выживание и развитие,
- учитывать наилучшие интересы ребенка при принятии решений,
- обеспечивать защиту от любых форм дискриминации [20; 5].

Эти принципы полностью распространяются и на цифровую среду.

5.2 «Замечание общего порядка № 25 о правах ребенка в цифровой среде» (2021 г.).

В 2021 году Комитет ООН по правам ребенка принял «Замечание общего порядка № 25 о правах ребенка в цифровой среде», предоставивший руководящие принципы по обеспечению прав детей в цифровой среде. Документ стал дополнением к Конвенции о правах ребёнка. Комитет подчеркнул, что в онлайн-среде, так же, как и в офлайн-мире, права каждого ребёнка должны уважаться, защищаться и обеспечиваться наивысшем уровне.

Доступ к цифровым технологиям способствует реализации всех гражданских, политических, культурных, экономических и социальных прав детей [20].

Основные принципы Конвенции и их применение в цифровой среде:

Принцип	Содержание в цифровой среде
Недопущение дискриминации	Государства должны обеспечивать всем детям равный и эффективный доступ к цифровым технологиям.
Наилучшие интересы ребенка	При разработке, управлении и использовании цифровых технологий первоочередное внимание должно уделяться интересам детей.

Право на жизнь, выживание и развитие	Использование цифровых устройств не должно заменять личное взаимодействие детей с родителями, сверстниками и опекунами.
Уважение мнения ребенка	Дети должны участвовать в разработке законодательства, политик и программ, касающихся их прав в цифровой среде.

Основные положения «Замечания общего порядка № 25 о правах ребенка в цифровой среде»:

• Все права, предусмотренные Конвенцией, полностью применимы и в цифровой среде.

• Родители, образовательные учреждения, государственные органы и частный сектор несут совместную ответственность за защиту детей в цифровом пространстве.

• Особый акцент сделан на роли бизнеса – частные компании должны соблюдать права ребенка, предотвращать злоупотребления их услугами и обеспечивать эффективные механизмы защиты и помощи.

• Государства обязаны разрабатывать соответствующее законодательство и политику, контролировать и оценивать их исполнение.

5.3 Концепция «4C» (Livingstone и Stoilova, 2021).

Авторы предложили классификацию рисков в цифровой среде в зависимости от позиции ребенка и природы угроз [23]:

• Контент (Content) – доступ ребёнка к вредоносной информации,

• Коммуникация (Contact) – взаимодействие ребёнка с потенциально опасными субъектами,

• Поведение (Conduct) – участие ребёнка в рискованных онлайн-практиках,

• Контракт (Contract) – злоупотребления в сфере коммерческих сделок и персональных данных ребёнка [23].

• Также выделяют различные виды рисков, присущих цифровой среде:

• • **агрессивные риски**, связанные с проявлениями насилия и кибербуллинга,

• • **сексуальные риски**, включающие угрозы эксплуатации и неподобающего контента,

• • **ценностные риски**, оказывающие влияние на мировоззрение, самоидентификацию и социальные установки.

Право на неприкосновенность частной жизни в цифровой среде.

Специальный докладчик ООН по защите частной жизни подчеркнул необходимость обеспечения изначально высокого уровня конфиденциальности при разработке и предоставлении цифровых продуктов и услуг для несовершеннолетних. [27].

Решение Глобального совета по защите конфиденциальности (GPA) предписывает:

• включать защиту интересов ребёнка в проектирование сервисов,

• уважать права ребёнка при сборе, обработке и хранении персональных данных [27].

В соответствии с Общим регламентом ЕС о защите данных (GDPR): «Дети имеют право на особую защиту в вопросах обработки их персональных данных, так как они могут быть менее осведомлены о рисках, последствиях и гарантиях» [28].

Особенности онлайн-сервисов, повышающие риски для детей (по исследованию Ofcom, Великобритания):

- быстрый и массовый доступ к контактам (добавление в группы без согласия),
- рекомендательные алгоритмы,
- бесконечная прокрутка контента,
- метрики популярности (лайки, подписчики),
- отсутствие эффективных возрастных ограничений,
- публичность профилей,
- кроссплатформенные переходы [24].

5.4 Лансаротская Конвенция.

Конвенция Совета Европы о защите детей от сексуальной эксплуатации и сексуального насилия, известная как Лансаротская конвенция, является ключевым международным договором, направленным на обеспечение правовой защиты детей от сексуальных преступлений как в виртуальной, так и в реальной среде [18].

Конвенция основана на трёх принципах:

- предотвращение преступлений,
- защита жертв,
- расследование преступлений [18].

В рамках Лансаротской конвенции государства обязуются:

- проводить просветительские кампании для повышения осведомлённости детей о рисках сексуальной эксплуатации и укрепления их навыков самозащиты;
- проверять и обучать лиц, работающих с детьми
- разрабатывать и регулярно пересматривать программы вмешательства и профилактики для уже осуждённых и потенциальных сексуальных преступников;
- признать уголовно наказуемыми такие деяния, как изготовление, предложение, распространение, хранение и просмотр материалов, содержащих сексуальное насилие над детьми [19].

Роль горячих линий и сервисов для сообщений о преступлениях.

Службы приёма сообщений о противоправном контенте (например, Child Helpline International) позволяют:

- любому лицу анонимно сообщать о противоправном контенте;
- направлять сообщения профессиональным аналитикам;
- при необходимости – информировать правоохранительные органы.

Национальные детские горячие линии:

- играют важную роль в оперативной помощи детям-жертвам;
- работают в круглосуточном режиме с обученными консультантами;
- становятся частью национальных систем защиты детей.

Кроме полиции (правоохранительных органов), ответственность за реагирование на подобные сообщения также несут интернет-провайдеры.

6. Заключение.

Прогресс в области технологий и расширение сети Интернет способствовали возникновению новых угроз для несовершеннолетних в цифровом пространстве. Несмотря на то, что цифровое пространство предоставляет детям широкие возможности для получения образования, социальной адаптации и личностного роста, оно также сопряжено с множеством рисков, включая угрозы для их безопасности, психического и физического благополучия.

Дети в интернете могут столкнуться с:

- ложной информацией и дезинформацией,
- кибербуллингом,
- радикализацией,
- материалами сексуальной эксплуатации,
- нарушением конфиденциальности данных,
- цифровой зависимостью,
- психологическим насилием и преступлениями сексуального характера.

В ответ на эти вызовы необходимо:

- повышать осведомлённость родителей, педагогов и самих детей о рисках цифровой среды;
- развивать цифровую грамотность детей с раннего возраста;
- обеспечивать эффективное родительское и педагогическое сопровождение при использовании детьми цифровых устройств;
- реализовывать государственные программы профилактики и правового регулирования в сфере защиты детей в интернете;
- укреплять международное сотрудничество и обмен опытом в противостоянии киберпреступлениям против детей;
- совершенствовать технические меры по ограничению доступа к противоправному контенту.

Отдельную роль в обеспечении прав детей в цифровом пространстве играют международные документы:

- Конвенция ООН о правах ребёнка,
- Замечание общего порядка № 25 о правах ребенка в цифровой среде (2021 г.)
- Будапештская конвенция о киберпреступности,
- Лансаротская конвенция Совета Европы.

Внедрение международных стандартов в национальные законодательства является критически важным для обеспечения комплексной защиты прав детей в цифровой среде. Реализация международных стандартов в национальных законодательствах становится ключевым элементом в обеспечении комплексной защиты детей в интернете [19; 20; 21; 22].

Цифровая трансформация требует от государств, общества, образовательных учреждений, семей и бизнеса скоординированных усилий для создания безопасной и здоровой цифровой среды, где права детей будут уважаться, защищаться и полноценно реализовываться [28].

Библиография

1. American Psychological Association. Влияние цифровых технологий на психическое здоровье детей и подростков. – Вашингтон: APA, 2023. – 158 с.

2. Archer C. Социальные сети и развитие социальных навыков у детей // Journal of Digital Childhood. – 2019. – Т. 12, № 2. – С. 53-65.

3. Bayzan S. Программы INSAFE и развитие безопасного интернета в Европе // Journal of European Digital Policies. – 2014. – Т. 5, № 3. – С. 525-531.

4. Bessant C. Children Online: Rights, Risks and Responsibilities. – London: Routledge, 2018. – 264 p.

5. Better Internet for Kids. Создание лучшего интернета для детей: международный опыт. – Брюссель: Европейская комиссия, 2020. – 102 с.

6. Boyd D.M., Ellison N.B. Определение социальных сетей: история и развитие // Journal of Computer-Mediated Communication. – 2008. – Т. 13, № 1. – С. 210-230.

7. Bozkurt A. Глобальные структуры по борьбе с незаконным контентом в интернете: опыт INHOPE // Международный журнал права и технологий (Türkiye) – 2012. – Т. 18, № 3. – С. 61-78.

8. Çakır Ö. и др. Международные правовые механизмы защиты детей от интернет-угроз // Journal of CyberLaw. (Türkiye) – 2014. – Т. 7, № 2. – С. 74-76.

9. Child Helpline International. Глобальные горячие линии помощи детям. – Амстердам: CHI, 2023. – 88 с.

10. Council of Europe. Конвенция о защите детей от сексуальной эксплуатации и сексуального насилия (Лансаротская конвенция). – Страсбург: Совет Европы, 2007. – 85 с.

11. Council of Europe. Конвенция о киберпреступности (Будапештская конвенция). – Страсбург: Совет Европы, 2011. – 96 с.

12. Çubukcu B. и др. Цифровое гражданство и права детей в интернете // International Journal of Digital Education. – 2013. – Т. 6, № 1. – С. 6-12.

13. European Data Protection Board. Общий регламент по защите данных (GDPR). – Брюссель: Европейский союз, 2018. – 120 с.

14. European Strategy. Европейская стратегия по защите детей в цифровом пространстве. – Брюссель: Европейская комиссия, 2022. – 78 с.

15. GPA. Резолюция о правах детей в цифровом пространстве. – Глобальный совет по вопросам конфиденциальности, 2021. – 40 с.

16. ITU. Дети и цифровая безопасность: международные стандарты и рекомендации. – Женева: Международный союз электросвязи, 2020. – 96 с.

17. Livingstone S., Stoilova M. Риски для детей в цифровой среде: подход "4C". – London: London School of Economics, 2021. – 64 p.

18. Mangold W.G., Faulds D.J. Социальные медиа как элемент маркетинговых коммуникаций // Journal of Business Research. – 2009. – Т. 62, № 3. – С. 357-365.

19. Ofcom. Доклад о рисках цифровых сервисов для детей в Великобритании. – Лондон: Ofcom, 2023. – 92 с.

20. OHCHR. Доклады о правах человека в цифровую эпоху. – Женева: Управление Верховного комиссара ООН по правам человека, 2021. – 140 с.

21. Sistek-Chandler C. Поколение социальных сетей: вызовы и возможности. – San Diego: Bridge point Education, 2012. – 212 p.

22. Steinberg S.B. Право на приватность в эпоху социальных сетей // Fordham Law Review. – 2017. – Т. 85, № 2. – С. 839-872.

23. UNESCO. Руководство по безопасному использованию интернета детьми. – Париж: Организация Объединённых Наций по вопросам образования, науки и культуры, 2016. – 112 с.

24. UNICEF. Дети в цифровом мире: состояние детей в мире, 2017. – Нью-Йорк: ЮНИСЕФ, 2017. – 202 с.

25. United Nations. Конвенция о правах ребенка. – Нью-Йорк: ООН, 1989. – 76 с.

26. United Nations. Факультативный протокол к Конвенции о правах ребенка о продаже детей, детской проституции и детской порнографии. – Нью-Йорк: ООН, 2000. – 34 с.

27. United Nations. Факультативный протокол о вовлечении детей в вооружённые конфликты. – Нью-Йорк: ООН, 2000. – 28 с.

28. Yılmaz R., Güney A. Цифровая зависимость у детей: причины и последствия // Journal of ChildStudies. – 2021. – Т. 9, № 4. – С. 488-505.

Дата поступления: *12 июня 2025 г.*
Дата принятия в печать: *24 июня 2025 г.*

Furman T.G.,
Ismailova E.V.♦

DOI: 10.25108/2304-1730-1749.iolr.2025.79.96-110
UDC: 377.8

Legal support for the safety of minors in the digital space

Abstract.

Subject. Digital space as a resource for self-expression and knowledge acquisition, as well as a potential high-risk environment affecting the rights and interests of minors and, as a consequence, a recorded increase in the number of offenses in the online environment. In this regard, there is an increasing need to form and improve legal mechanisms to ensure the protection of children in the context of digitalization.

Objective. This scientific study presents a comprehensive analysis of legal approaches aimed at ensuring the safety of minors in the online environment, as well as the formulation of proposals for creating a more effective system of legal regulation in this area**.**

Methodological basis. General scientific methods (analysis, synthesis of international and national regulatory legal acts, scientific literature, as well as content analysis of relevant sources) and special legal methods (comparative legal analysis of regulatory legal acts and scientific publications on the topic), a formal legal method were used.

Results. The scientific study examined the impact of the Internet on the development and behavior of minors, classified the main risks that arise in the online space.

Conclusions. A legal assessment of existing child protection mechanisms is given both at the national and international levels. Proposals have been formulated to create a more effective system of legal regulation in this area.

♦ **Furman Tatyana Gennadievna -** Candidate of Cultural Studies, Associate Professor at the Department of Constitutional and Administrative Law of the North-West Institute of Management – a branch of the Federal State Budgetary Educational Institution of Higher Education "Russian Academy of National Economy and Public Administration under the President of the Russian Federation" (RANEPA), Saint Petersburg. E-mail: furman-tg@ranepa.ru

Ismailova **Esmira Vagif kyzy** - master's 1st year student of the Faculty of Law, part-time program Regulation and Protection of Human Rights and Freedoms North-West Institute of Management – a branch of the Federal State Budgetary Educational Institution of Higher Education "Russian Academy of National Economy and Public Administration under the President of the Russian Federation" (RANEPA), Saint Petersburg. E-mail: e. ismayilova414@gmail.com

Key words: Internet, children's rights, child sexual exploitation, internet risks, cybercrime, cyberbullying. online grooming.

References

1. American Psychological Association. The Impact of Digital Technologies on the Mental Health of Children and Adolescents. – Washington: APA, 2023. – 158 p.

2. Archer C. Social Networks and the Development of Social Skills in Children // Journal of Digital Childhood. – 2019. – Vol. 12, No. 2. – P. 53-65.

3. Bayzan S. INSAFE Programs and the Development of a Safe Internet in Europe // Journal of European Digital Policies. – 2014. – Vol. 5, No. 3. – P. 525-531.

4. Bessant C. Children Online: Rights, Risks and Responsibilities. – London: Routledge, 2018. – 264 p.

5. Better Internet for Kids. Creating a Better Internet for Kids: International Experience. – Brussels: European Commission, 2020. – 102 p.

6. Boyd D.M., Ellison N.B. Definition of social networks: history and development // Journal of Computer-Mediated Communication. - 2008. - Vol. 13, No. 1. - P. 210-230.

7. Bozkurt A. Global structures for combating illegal content on the Internet: the INHOPE experience // International Journal of Law and Technology (Türkiye) - 2012. - Vol. 18, No. 3. - P. 61-78.

8. Çakır Ö. et al. International legal mechanisms for protecting children from online threats // Journal of CyberLaw. (Türkiye) - 2014. - Vol. 7, No. 2. - P. 74-76.

9. Child Helpline International. Global hotlines for children. – Amsterdam: CHI, 2023. – 88 p.

10. Council of Europe. Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention). – Strasbourg: Council of Europe, 2007. – 85 p.

11. Council of Europe. Convention on Cybercrime (Budapest Convention). – Strasbourg: Council of Europe, 2011. – 96 p.

12. Çubukcu B. et al. Digital Citizenship and Children's Rights on the Internet // International Journal of Digital Education. – 2013. – Vol. 6, No. 1. – P. 6-12.

13. European Data Protection Board. General Data Protection Regulation (GDPR). – Brussels: European Union, 2018. – 120 p.

14. European Strategy. European Strategy for the Protection of Children in the Digital Space. – Brussels: European Commission, 2022. – 78 p.

15. GPA. Resolution on children's rights in the digital space. – Global Privacy Council, 2021. – 40 p.

16. ITU. Children and digital security: international standards and recommendations. – Geneva: International Telecommunication Union, 2020. – 96 p.

17. Livingstone S., Stoilova M. Risks to children in the digital environment: the "4Cs" approach. – London: London School of Economics, 2021. – 64 p.

18. Mangold W.G., Faulds D.J. Social media as an element of marketing communications // Journal of Business Research. – 2009. – Vol. 62, No. 3. – P. 357-365.

19. Ofcom. A report on the risks of digital services to children in the UK. - London: Ofcom, 2023. - 92 p.

20. OHCHR. Reports on human rights in the digital age. - Geneva: Office of the United Nations High Commissioner for Human Rights, 2021. - 140 p.

21. Sistek-Chandler C. The social media generation: challenges and opportunities. - San Diego: Bridge point Education, 2012. - 212 p.

22. Steinberg S.B. The right to privacy in the age of social media // Fordham Law Review. - 2017. - Vol. 85, No. 2. - P. 839-872.

23. UNESCO. Internet Safety Guidelines for Children. Paris: United Nations Educational, Scientific and Cultural Organization, 2016. 112 p.

24. UNICEF. Children in a Digital World: The State of the World's Children, 2017. New York: UNICEF, 2017. 202 p.

25. United Nations. Convention on the Rights of the Child. New York: United Nations, 1989. 76 p.

26. United Nations. Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography. New York: United Nations, 2000. 34 p.

27. United Nations. Optional Protocol on the Involvement of Children in Armed Conflict. New York: United Nations, 2000. 28 p.

28. Yılmaz R., Güney A. Digital addiction in children: causes and consequences // Journal of ChildStudies. - 2021. - Vol. 9, No. 4. - P. 488-505.

The article was submitted: *2025 June 12*
Accepted for publication: *2025 June 24*

Furman T.G.,
İsmayılova E.V.♦

DOI: 10.25108/2304-1730-1749.iolr.2025.79.96-110
UOT: 377.8

Rəqəmsal məkanda yetkinlik yaşına çatmayanların təhlükəsizliyinin hüquqi təminatı

Xülasə: Tədqiqatın predmeti. Rəqəmsal məkan həm özünüifadə və bilik əldə etmə vasitəsi, həm də yetkinlik yaşına çatmayan şəxslər üçün hüquqi və psixososial risklər mənbəyi kimi çıxış edir. Bu mühitdə baş verən pozuntuların artması kontekstində, uşaqların rəqəmsallaşma şəraitində müdafiəsini təmin edən hüquqi mexanizmlərin formalaşdırılması və təkmilləşdirilməsi zərurəti aktuallaşmışdır.

♦ **Furman Tatyana Gennadyevna -** mədəniyyətşünaslıq üzrə fəlsəfə doktoru, Rusiya Federasiyası Prezidentinin nəzdində fəaliyyət göstərən Rusiya Xalq Təsərrüfatı və Dövlət Qulluğu Akademiyasının federal dövlət büdcəli ali təhsil müəssisəsinin filial olan Şimal-Qərb İdarəçilik İnstitutunun «Konstitusiya və İnzibati hüquq» kafedrasının dosenti. E-mail: furman-tg@ranepa.ru

İsmayılova Esmira Vaqif qızı - Rusiya Federasiyası Prezidentinin nəzdində fəaliyyət göstərən Rusiya Xalq Təsərrüfatı və Dövlət Qulluğu Akademiyasının federal dövlət büdcəli ali təhsil müəssisəsinin filialı – Şimal-Qərb İdarəçilik İnstitutunun hüquq fakültəsinin "İnsan və vətəndaş hüquq və azadlıqlarının tənzimlənməsi və müdafiəsi" proqramı üzrə qiyabi təhsil formasında təhsil alan I kurs magistrantı. E-mail: e. ismayilova414@gmail.com

Məqsəd. Tədqiqatın əsas məqsədi rəqəmsal mühitdə yetkinlik yaşına çatmayanların təhlükəsizliyini təmin etməyə yönəlmiş normativ-hüquqi yanaşmaların hərtərəfli və sistemli təhlilini təqdim etməkdən ibarətdir.

Metodoloji əsaslar. Elmi işdə ümumelmi (analiz, sintez, kontent-analiz) və xüsusi hüquqi (müqayisəli, formal-hüquqi təhlil) metodlardan istifadə edilmişdir. Beynəlxalq və milli normativ-hüquqi aktlar, elmi ədəbiyyat və müvafiq sahəyə dair aktual informasiya mənbələri araşdırma obyekti kimi çıxış etmişdir.

Əldə olunmuş nəticələr. Tədqiqat zamanı internetin uşaqların psixoloji, intellektual və davranış xüsusiyyətlərinə təsiri təhlil olunmuş, rəqəmsal mühitdə qarşılaşdıqları əsas hüquqi risklər sistemləşdirilmişdir.

Nəticə və tövsiyələr. Mövcud milli və beynəlxalq hüquqi mexanizmlər hüquqi baxımdan qiymətləndirilmiş, bu sahədə daha səmərəli tənzimləməni təmin etmək üçün təklif və tövsiyələr irəli sürülmüşdür.

Açar sözlər: internet, uşaq hüquqları, uşaqların cinsi istismarı, rəqəmsal risklər, kibercinayətlər, kibertəcavüz (kiberbulling), onlayn-grooming (uşaqlara qarşı onlayn manipulyasiya və inamın əldə olunması prosesi).

Məqalə daxil olmuşdur: *12 iyun 2025-ci il*
Çapa qəbul edilmişdir: *24 iyun 2025-ci il*