БОЛАНИНГ РАҚАМЛИ МУҲИТДА ХАВФСИЗЛИККА БЎЛГАН ҲУҚУҚИ
(ЁКИ БОЛАЛАРНИ КИБЕРБУЛЛИНГ, ОНЛАЙН ЗЎРАВОНЛИК ВА ЖИНСИЙ ЭКСПЛУАТАЦИЯДАН ҲИМОЯ ҚИЛИШ)

Хамдамова Фируза Уразалиевна,
Жаҳон иқтисодиети ва дипломатия университети, доцент в.б.
Юридик фанлар доктори (DS),
E-mail: fxamdamova@uwed.uz

Аннотация

Мақолада жамиятнинг рақамли трансформацияси шароитида бола ҳуқуқининг хавфсизликка бўлган ҳуқуқи тадқиқ этилади. Ушбу ҳуқуқ мазмунининг рақамли технологиялар таъсирида ўзгариши, яъни бир томондан болалар ривожланиши учун имкониятларни кенгайтириши, иккинчи томондан эса уларнинг турли хавф-хатарларга дучор бўлишини кучайтириши таҳлил қилинади. Бола ҳуқуқларини ҳимоя қилиш бўйича халқаро ҳуқуқий стандартлар ҳамда “юмшоқ ҳуқуқ” ҳужжатлари кўриб чиқилади. Кибербуллинг, онлайн зўравонлик, жинсий эксплуатация ва бошқа ноқонуний рақамли таҳдидлар алоҳида ёритилади. Рақамли муҳит анонимлик, трансчегаравийлик ва ахборотнинг тез тарқалиши билан тавсифланиши таъкидланади. Давлатлар, халқаро ташкилотлар, технология платформалари ва фуқаролик жамияти ўртасида комплекс ҳамкорлик зарурлиги асосланади. Самарали ҳимоя ҳуқуқий, институционал ва технологик механизмларнинг уйғунлигини талаб этиши хулоса қилинади.

Калит сўзлар: бола ҳуқуқлари, рақамли муҳит, кибербуллинг, онлайн зўравонлик, жинсий эксплуатация, халқаро ҳуқуқ, болалар хавфсизлиги.

THE CHILD’S RIGHT TO SAFETY IN THE DIGITAL ENVIRONMENT

(OR PROTECTION OF CHILDREN FROM CYBERBULLYING, ONLINE VIOLENCE, AND SEXUAL EXPLOITATION)

Khamdamova Firuza Urazalievna,
University of world economy and diplomacy,
Associate Professor,
Doctor of Science in Law (DS),
E-mail: fxamdamova@uwed.uz

Abstract

The article examines the child's right to safety in the context of the digital transformation of modern society. It analyzes the changing content of this right under the influence of digital technologies, which both expand opportunities for children's development and increase their exposure to risks. International legal standards on child protection, enshrined in universal and regional instruments as well as soft law documents, are considered. Particular attention is given to contemporary digital threats, including cyberbullying, online violence, sexual exploitation, and other forms of unlawful conduct in the Internet environment. It is emphasized that the digital space is characterized by anonymity, transnationality, and rapid information dissemination, which complicates child protection. The study highlights the need for comprehensive cooperation between states, international organizations, technology platforms, and civil society, concluding that effective protection requires a combination of legal, institutional, and technological mechanisms.

Keywords: children's rights, digital environment, cyberbullying, online violence, sexual exploitation, international law, child safety.

ПРАВО РЕБЁНКА НА БЕЗОПАСНОСТЬ В ЦИФРОВОЙ СРЕДЕ

(или ЗАЩИТА ДЕТЕЙ ОТ КИБЕРБУЛЛИНГА, ОНЛАЙН-НАСИЛИЯ И СЕКСУАЛЬНОЙ ЭКСПЛУАТАЦИИ)

Хамдамова Фируза Уразалиевна,
Университет мирово й экономики и дипломатии, и.о. доцента,

Доктор юридических наук (DS),
E-mail: fxamdamova@uwed.uz

Аннотация

В статье исследуется право ребёнка на безопасность в условиях цифровой трансформации современного общества. Рассматривается изменение содержания данного права под влиянием цифровых технологий, которые одновременно расширяют возможности развития детей и усиливают риски их уязвимости. Анализируются международно-правовые стандарты защиты прав ребёнка, закреплённые в универсальных и региональных документах, а также в актах «мягкого права». Особое внимание уделяется современным цифровым угрозам, включая кибербуллинг, онлайн-насилие, сексуальную эксплуатацию и другие формы противоправного воздействия в сети Интернет. Подчёркивается, что цифровая среда характеризуется анонимностью, трансграничностью и высокой скоростью распространения информации, что усложняет обеспечение безопасности несовершеннолетних. Обосновывается необходимость комплексного взаимодействия государств, международных организаций, технологических платформ и гражданского общества. Делается вывод, что эффективная защита права ребёнка на безопасность возможна только при сочетании правовых, институциональных и технологических механизмов в цифровой среде.

Ключевые слова: права ребёнка, цифровая среда, кибербуллинг, онлайн-насилие, сексуальная эксплуатация, международное право, безопасность детей.

Введение

Конвенция о правах ребёнка 1989 года закрепляет принцип наилучшего обеспечения интересов ребёнка (статья 3). Статьи 19 и 34 устанавливают обязанность государств защищать детей от всех форм насилия, злоупотреблений и сексуальной эксплуатации. В совокупности данные

положения формируют международно-правовую основу права ребёнка на безопасность, включая его защиту от посягательств различного характера.

В условиях цифровизации общества право ребенка на безопасность приобретает качественно новое содержание. Его объём существенно расширяется за счёт включения цифрового измерения: если традиционно право на безопасность рассматривалось преимущественно как гарантия физической неприкосновенности, то в современных условиях оно охватывает также защиту от информационно-психологического воздействия, цифрового насилия и эксплуатации в онлайн-среде. При этом, в отличие от офлайн-пространства, вред в цифровой среде может носить длительный и кумулятивный характер, поскольку однажды размещённая информация способна сохраняться, копироваться и распространяться практически без ограничения [1].

Актуальность данной проблемы усиливается масштабами вовлечённости несовершеннолетних в цифровую среду. Так, молодые люди в возрасте от 15 до 24 лет традиционно являются наиболее активными пользователями Интернета; при этом цифровой разрыв между поколениями постепенно сокращается. Согласно пересмотренным оценкам, в 2025 году Интернетом пользовались около 82% лиц в возрасте от 15 до 24 лет, что свидетельствует о высокой степени цифровой интеграции данной возрастной группы [2].

На этом фоне киберпреступность в отношении несовершеннолетних выступает одной из ключевых цифровых угроз современности, непосредственно затрагивающих право ребёнка на безопасность в цифровой среде. В международно-правовой доктрине она рассматривается как совокупность противоправных деяний, совершаемых с использованием информационно-коммуникационных технологий и посягающих на права, свободы и безопасность несовершеннолетних. Таким образом, обеспечение защиты детей от онлайн-угроз становится приоритетным направлением как

государственной политики, так и международного сотрудничества в сфере защиты прав ребёнка.

В развитие указанных положений Комитетом ООН по правам ребёнка принято Замечание общего порядка № 25 о правах ребёнка в цифровой среде [3]. В данном документе подчёркивается, что государства несут прямую ответственность за осуществление регулятивного надзора в отношении цифровой среды, в которой находятся дети, а также обязаны обеспечивать соблюдение их прав в Интернете со стороны частного сектора. Особое внимание в Замечании уделяется вопросам обеспечения безопасности ребёнка в цифровом пространстве как одному из ключевых элементов реализации его прав.

ОСНОВНЫЕ ФОРМЫ КИБЕРПРЕСТУПНОСТИ ПРОТИВ ДЕТЕЙ

1. Кибербуллинг как форма нарушения права на безопасность

Защита детей от цифрового насилия (кибернасилия) является одной из приоритетных задач в сфере обеспечения и защиты прав ребёнка, поскольку данное явление непосредственно затрагивает его право на безопасность в цифровой среде. При этом цифровое насилие характеризуется высокой степенью латентности, что существенно затрудняет его выявление, фиксацию и правовую квалификацию [1].

Одной из наиболее распространённых форм цифрового насилия **выступает кибербуллинг,** представляющий собой систематическое агрессивное поведение, осуществляемое с использованием информационно-коммуникационных технологий. Статистические данные свидетельствуют о масштабности проблемы: дети до 18 лет составляют около трети всех пользователей Интернета в мире, при этом более трети молодых людей в 30 странах сообщают о фактах кибертравли, а каждый пятый из них пропускает занятия в школе вследствие её последствий [4].

В отличие от традиционных форм буллинга, кибербуллинг может происходить в любое время и в любом месте, что затрудняет его предотвращение. *Кибербуллинг часто выражается через травлю в социальных сетях, мессенджерах и других онлайн-платформах.* Анонимность, которую предоставляет интернет, делает агрессоров более смелыми, и жертвы могут столкнуться с агрессией, не зная, кто стоит за нападками. Тактика кибербуллинга может варьироваться от оскорблений и угроз до распространения ложной информации и персональных данных, что может серьезно подорвать самооценку и психическое здоровье жертвы.

Ключевая особенность кибербуллинга заключается в его перманентности и публичности. В отличие от традиционного буллинга, он не ограничен физическим пространством и временем, что усиливает психологическое давление на ребёнка. Жертвы кибербуллинга чувствуют себя беспомощными, испытывают стресс, унижение, беспокойство, гнев, потерю уверенности в себе. Такие дети нередко становятся изгоями в классе, что в дальнейшем может спровоцировать их на агрессию, месть [1].

Проблема кибербуллинга дополнительно осложняется низким уровнем обращаемости за помощью: несовершеннолетние часто испытывают страх, стыд или недоверие к взрослым и институциональным механизмам защиты, считая, что их переживания будут недооценены. В результате значительная часть жертв остаётся без поддержки, что повышает риск развития депрессивных состояний, тревожных расстройств и в отдельных случаях — суицидальных мыслей, что подчёркивает необходимость комплексного подхода к профилактике и противодействию цифровому насилию [5].

2. Онлайн-насилие и сексуальная эксплуатация несовершеннолетних

Особую категорию угроз составляют формы онлайн-насилия и сексуальной эксплуатации детей. Специальный докладчик ООН по вопросам торговли детьми, их сексуальной эксплуатации и сексуальном

насилии над ними заявила, что «*случаи сексуального насилия и эксплуатации детей участились в цифровой среде: по оценкам, более 300 миллионов детей в год становятся жертвами подобного рода преступлений в интернете*». [6]. Около 80 % детей в 25 странах сообщают, что опасаются сексуальных злоупотреблений и сексуальной эксплуатации в интернете[4].

К основным формам относятся:

- ***онлайн-груминг*** *(установление доверительных отношений с целью последующей эксплуатации);*
- *распространение материалов сексуального характера с участием детей;*
- ***сексторшн*** *(сексуальное шантажирование с использованием цифровых данных);*
- *вовлечение детей в противоправную деятельность через интернет-платформы.*

Данные явления характеризуются высокой степенью латентности и транснациональностью, что значительно осложняет их выявление и пресечение. В этой связи особую актуальность приобретает развитие международного сотрудничества в сфере кибербезопасности и защиты детей.

Важным аспектом является то, что жертвы не всегда осознают серьезность происходящего. Некоторые могут принять домогательства за шутку или недоразумение, что усугубляет проблему. Это приводит к тому, что подростки замыкаются в себе, испытывая чувство стыда и страха. Чаще всего они не рассказывают родителям или друзьям об инцидентах, что исключает возможность получить поддержку и защиту [5].

МЕЖДУНАРОДНО-ПРАВОВЫЕ И НАЦИОНАЛЬЛЬНЫЕ МЕХАНИЗМЫ ЗАЩИТЫ ДЕТЕЙ В ЦИФРОВОЙ СРЕДЕ

Международные объединения, органы государственной власти, общественные организации и родительское сообщество заинтересованы в создании условий для формирования у детей навыков самостоятельного,

осознанного и ответственного использования информационной продукции, защиты несовершеннолетних от внешнего деструктивного информационно-психологического воздействия [1].

Международные организации, включая UNICEF и структуры ООН, подчёркивают необходимость комплексного подхода к защите детей в цифровой среде. Такой подход включает три ключевых компонента:

1. **Нормативный** — разработка и гармонизация международных стандартов;
2. **Институциональный** — создание специализированных органов и механизмов мониторинга;
3. **Технологический** — внедрение цифровых инструментов раннего выявления угроз.

Важно отметить, недостаточность исключительно правовых средств в сфере защиты детей в цифровой среде обусловлена тем, что традиционные нормативно-правовые механизмы объективно не успевают адаптироваться к динамике развития цифровых технологий и трансграничному характеру онлайн-пространства. ограничением правовых средств выступает высокая скорость эволюции цифровых угроз: новые формы кибербуллинга, онлайн-груминга, алгоритмического воздействия и эксплуатации несовершеннолетних возникают быстрее, чем успевают формироваться соответствующие правовые нормы и международные стандарты. В результате возникает нормативный разрыв между фактическими угрозами и уровнем их правового регулирования. В этой связи правовые механизмы, несмотря на их фундаментальное значение, не способны самостоятельно обеспечить комплексную защиту ребёнка в цифровой среде без поддержки технологических и институциональных инструментов. Эффективная система защиты требует их интеграции с цифровыми средствами мониторинга, алгоритмами раннего выявления рисков и механизмами оперативного

реагирования, что позволяет компенсировать ограниченную гибкость и скорость правового регулирования

С учетом вышеизложенного, технологический компонент становится ключевым элементом современной модели защиты детей в цифровой среде, особенно для предупрждения цифрового насилия в отношении детей. Особое значение имеет именно превентивная функция технологических решений, поскольку она позволяет минимизировать сам факт причинения вреда ребёнку, а не только устранять его последствия. В отличие от традиционных правовых и институциональных механизмов, которые, как правило, включаются уже после факта нарушения, цифровые технологии позволяют выявлять потенциально опасное поведение и контент на ранних стадиях его возникновения.

В целом защита прав человека в цифровой среде сегодня во многом зависит от технологических решений, поскольку именно они определяют уровень безопасности пользователей в онлайн-пространстве. Одних только правовых норм недостаточно, так как реальные риски формируются и реализуются внутри цифровых платформ и алгоритмов. современная модель защиты прав человека в цифровой среде предполагает, что ответственность за безопасность должна закладываться не только через законодательство, но и через саму технологическую конструкцию цифровых сервисов.

Тем не менее это не умаляет значения правовых механизмов. Технологические решения, какими бы эффективными они ни были, не могут существовать автономно от правового регулирования, поскольку их разработка, внедрение и применение требуют нормативного закрепления стандартов, принципов и требований безопасности. Правовые нормы определяют ответственность за нарушения, создают механизмы контроля и надзора, а также обеспечивают возможность принудительного исполнения установленных требований. Без правового регулирования технологические

инструменты могут носить фрагментарный характер и не обеспечивать единообразного стандарта защиты на международном уровне.

Именно поэтому на универсальном уровне последовательно формируется система международных документов, направленных на регулирование и стандартизацию защиты детей в цифровой среде. Особо следует отметить **Руководящие указания для директивных органов по защите ребенка в онлайновой среде, принятые Международным союзом электросвязи в 2020 году [7].**

Создан Глобальный альянс WeProtect. Global Alliance WeProtect действует на основе единой и неизменной миссии — **защиты детей от распространённых угроз сексуальной эксплуатации и сексуального насилия в цифровой среде**. Альянс исходит из того, что каждый ребёнок имеет право пользоваться цифровым пространством безопасно и уверенно, находясь под защитой эффективных превентивных мер и коллективных международных усилий. Организация объединяет правительства государств, частный сектор, институты гражданского общества и международные организации с целью разработки совместных механизмов противодействия онлайн-эксплуатации детей и достижения практических результатов в данной сфере. Основная идея деятельности Альянса заключается в консолидации усилий различных государств и отраслей для решения проблем, которые невозможно эффективно преодолеть силами одной организации или отдельного государства [8].

Возможно, следует рассмотреть вопрос о принятии **Дополнительного протокола к Конвенции о правах ребенка о защите ребенка в цифровой среде.**

Данные меры следует подкреплять мерами на региональном и национальном уровне. Говоря о мерах, принимаемых на региональном уровне, особо следует упомянуть принятие в 2007 году **Конвенции Совета Европы о защите детей от сексуальной эксплуатации и сексуальных**

злоупотреблений (Лансаротская конвенция) [9]. Конвенция закрепила комплексный подход к предупреждению сексуальной эксплуатации детей, криминализации соответствующих деяний, защите и реабилитации потерпевших, а также развитию международного сотрудничества государств в данной сфере. Особую значимость документ приобретает в условиях цифровизации, поскольку его положения распространяются в том числе на преступления, совершаемые с использованием информационно-коммуникационных технологий и сети Интернет.

Отметим также, что Стратегия Совета Европы по правам ребёнка на 2022–2027 годы включает отдельное направление, посвящённое правам детей в цифровой среде. Данное направление дополнительно укрепляется **Рекомендацией CM/Rec (2018)7 Комитета министров государствам-членам о руководящих принципах по соблюдению, защите и обеспечению прав ребёнка в цифровой среде [10]**.

Отдельное значение имеет **доклад Совета Европы «Два шага вперёд и один шаг назад» («Two clicks forward and one click back»),** посвящённый положению детей с инвалидностью в цифровой среде. Документ содержит рекомендации по обеспечению прав детей с интеллектуальными, физическими, слуховыми и зрительными нарушениями в условиях цифровизации [11]. Аналогичные инициативы нужны и в других регионах, включая регион Центральной Азии.

На национальном уровне необходимо принимать комплексные меры. Как отмечает Комитет ООН по правам ребенка, “*защита детей в Интернете должна быть интегрирована в национальную политику защиты детей. Государствам-участникам следует осуществлять меры по защите детей от рисков, включая кибераггрессию и сексуальную эксплуатацию детей и сексуальные посягательства с использованием цифровых технологий и в Интернете, обеспечить расследование таких преступлений и предоставлять средства правовой защиты и поддержку пострадавшим*

детям. Им следует также удовлетворять потребности детей, находящихся в неблагоприятном или уязвимом положении, в том числе путем предоставления адаптированной для детей информации, при необходимости с переводом на соответствующие языки меньшинств" [3].

С учетом вышеизложенного целесообразным представляется принятие отдельной **Национальной концепции информационной безопасности детей,** которая дополняла бы общую Концепцию информационной безопасности и учитывала бы специфику уязвимости несовершеннолетних в цифровой среде. Такая концепция должна носить комплексный характер и включать правовые, институциональные, образовательные и технологические меры защиты. В её рамках необходимо определить приоритетные направления государственной политики по предотвращению киберугроз, развитию цифровой грамотности детей и родителей, а также усилению ответственности цифровых платформ. Концепция должна предусматривать систему межведомственного взаимодействия и международного сотрудничества, что позволит обеспечить более эффективную и устойчивую защиту прав ребёнка в условиях глобальной цифровизации.

Заключение

Право ребёнка на безопасность в цифровой среде представляет собой сложный и динамично развивающийся институт международного права, который формируется под влиянием стремительной цифровизации общественных отношений. Его содержание выходит за рамки традиционного понимания безопасности как защиты от физического насилия и включает также цифровые, информационные и технологические аспекты, связанные с функционированием онлайн-пространства.

Современные угрозы для детей в цифровой среде становятся всё более разнообразными и трансграничными. К числу наиболее значимых относятся кибербуллинг, онлайн-насилие, груминг, сексуальная эксплуатация, незаконное распространение персональных данных, а также манипулятивное

воздействие через цифровые платформы и социальные сети. Указанные формы угроз характеризуются высокой латентностью, анонимностью субъектов и возможностью мгновенного и массового распространения вредоносного контента, что значительно усложняет их выявление и предотвращение.

В этих условиях формирование эффективной системы защиты требует многоуровневого подхода, основанного на взаимодействии государства, международных организаций, технологических компаний и институтов гражданского общества. Особое значение приобретает интеграция правовых, институциональных и технологических механизмов регулирования, направленных не только на реагирование на уже совершённые нарушения, но и на их предупреждение.

Эффективная реализация права ребёнка на безопасность возможна лишь при условии постоянной адаптации правовых норм к быстро меняющейся цифровой реальности, а также внедрения превентивных механизмов защиты.

Сноски/Иктибослар/References:

1. Подустова О.Л., Чурочкина А.А. Правовыеаспекты защиты прав детей в цифровом пространстве// Вопросы безопасности. 2025. № 2. DOI: 10.25136/2409-7543.2025.2.74098 EDN:NLUAPO URL: https://nbpublish.com/library_read_article.php?id=74098

2. Безопасность детей и молодежи в Интернете. URL: https://www.un.org/ru/global-issues/child-and-youth-safety-online

3. Комитет по правам ребенка. Замечание общего порядка № 25 (2021) о правах детей в связи с цифровой средой// https://www.refworld.org/ru/policy/concobservations/crc/2021/ru/146359

4. Аналитическая записка МСЭ. Обеспечение безопасности детей в цифровой среде: Важность защиты и расширения прав и возможностей. 2021.

URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/COP/21-00821_COP-Policy-Brief-R.pdf

5. Армашова А.В. Предупреждение киберпреступности в отношении несовершеннолетних: проблемы и пути их решения // Право и государство: теория и практика. 2025. № 2. С. 409-411. http://doi.org/10.47643/1815-1337_2025_2_409

1. Спецдокладчик ООН: дети подвергаются повышенному риску сексуального насилия в интернете //Официальный сайт ООН. URL: https://news.un.org/ru/story/2024/10/1457276, 10.04.2025

2. Руководящие указания для директивных органов по защите ребенка в онлайновой среде, принятые Международным союзом электросвязи (МСЭ) в 2020 году. Текст документа доступен на https://8a8e3fff-ace4-4a3a-a495-4ea51c5b4a3c.filesusr.com/ugd/24bbaa_b5fec426d50d4a21b721489099b5781f.pdf

3. Глобальный альянс WeProtect Более подробная информация о деятельности Альянса доступна https://www.weprotect.org/about-us/strategy-and-impact/

4. Конвенция Совета Европы о защите детей от сексуальной эксплуатации и сексуальных злоупотреблений (Лансаротская конвенция). Текст документа доступен на https://rm.coe.int/09000016808b79f7

5. Рекомендация CM/Rec (2018)7 Комитета министров государствам-членам о руководящих принципах по соблюдению, защите и обеспечению прав ребёнка в цифровой среде

6. The digital environment. https://www.coe.int/en/web/children/the-digital-environment