THE ROLE OF INTERNATIONAL ORGANIZATIONS AND TRANSNATIONAL COOPERATION IN ENSURING THE PROTECTION OF CHILDREN'S RIGHTS IN THE DIGITAL ENVIRONMENT

Fayzullojonova Dilshoda
https://doi.org/10.5281/zenodo.20338001

ARTICLE INFO

Qabul qilindi: 18-may 2026 yil
Ma'qullandi: 20-may 2026 yil
Nashr qilindi: 22-may 2026 yil

KEYWORDS

children's rights, digital environment, international organizations, transnational cooperation, Safety by Design, General Comment No. 25..

ABSTRACT

This article investigates the transnational system for safeguarding children's rights during global digitalization, specifically analyzing the role of international organizations (UN, UNICEF, ITU, Council of Europe, EU) in developing legal frameworks and mechanisms to protect minors in the digital environment. The study addresses the structural gap between abstract international human rights norms and technically effective domestic enforcement. This issue is aggravated by borderless digital threats, limited regulatory capacities in the Global South, and insufficient control over private tech companies. To examine this, the research employs doctrinal legal analysis and a comparative study of hard and soft law instruments, including UNCRC General Comment No. 25 and technical standards from the OECD and ITU. While significant normative progress has established the "Safety by Design" principle, enforcement remains uneven. International bodies are shifting toward technical standardization and Public-Private-Civic partnerships like the WeProtect Global Alliance and Interpol's Childhood Project.

I. Введение

Цифровизация повседневной жизни коренным образом изменила среду, в которой дети растут, учатся, общаются и формируют свою личность. За последнее десятилетие доступ к цифровым технологиям стал практически повсеместным в развитых странах и быстро расширяется в странах Глобального Юга благодаря таким инициативам, как программа МСЭ «Connect 2030» и программы ЮНЕСКО по цифровой грамотности. Согласно Глобальному докладу МСЭ о подключении к сети, за последние тридцать лет подключение к сети претерпело глубокую трансформацию, превратившись из дефицитного ресурса в важнейшую опору повседневной жизни, и к 2025 году около 6 миллиардов человек будут пользоваться интернетом, что составит примерно три четверти населения. Неструктурированное или чрезмерное

использование цифровых инструментов связано с ухудшением результатов обучения и негативным воздействием на благополучие, таким как повышение тревожности и депрессии среди тех, кто много времени проводит за экраном [1]. Дети и молодежь, как первое полностью цифровое поколение, особенно подвержены онлайн-рискам. По оценкам, дети и подростки до 18 лет составляют каждую третью интернет-пользователя в мире [2].

Цифровая трансформация детства по своей сути имеет двойственный характер. С одной стороны, интернет и связанные с ним технологии предоставляют беспрецедентные возможности для образования, участия в культурной жизни, свободы выражения мнений и социальных связей. С другой стороны, та же инфраструктура, которая расширяет возможности детей, также подвергает их сложному и быстро меняющемуся набору рисков: материалам, связанным с сексуальной эксплуатацией и насилием в отношении детей, кибербуллингу, коммерческому профилированию данных, алгоритмическим манипуляциям и воздействию насильственного или экстремистского контента [3]. Этот вред не ограничен географически — он пересекает границы так же легко, как и пакеты данных, создавая структурное несоответствие между территориальной логикой национальных правовых систем и трансграничной архитектурой цифрового вреда.

Именно на этом фоне международные организации и механизмы транснационального правового сотрудничества стали незаменимыми участниками в сфере защиты детей в цифровой среде. Общий комментарий № 25 более подробно излагает конкретные позитивные обязательства государств по защите прав детей в цифровой среде, такие как пересмотр или принятие законодательства; обеспечение всеобъемлющей политики и стратегий; и содействие независимому мониторингу и расследованиям со стороны национальных органов по правам человека [4]. Помимо обязательств государств, Общий комментарий № 25 также уточняет роль субъектов частного и коммерческого секторов, таких как платформы социальных сетей и другие интернет-посредники, которые должны выполнять свою обязанность по соблюдению прав детей.

Однако нормативный прогресс на международном уровне не приводит автоматически к эффективному применению на практике. Взаимосвязь между международными нормами, их внутренним применением и соблюдением остается спорной, недостаточно теоретически обоснованной.

Центральный исследовательский вопрос как международные организации и транснациональные механизмы сотрудничества преодолевают разрыв между абстрактными нормами прав человека и технически эффективным обеспечением прав детей в цифровом пространстве?

Ii. Материалы и методы

Методологический дизайн данного исследования определен его трансграничным и многоуровневым характером, требующим сочетания классических юридических методов со сравнительно-правовым анализом документов международных институтов.

На глобальном уровне основными документами являются Конвенция ООН о правах ребенка (1989 г.), Общий комментарий № 25 (2021 г.) и Конвенция ООН против киберпреступности (принята в декабре 2024 г., Резолюция 79/243). Стандарты и технические документы Международного союза электросвязи (МСЭ) и ОЭСР. Эмпирическими данными являются глобальные доклады ЮНИСЕФ (2024 г.), отчеты и аналитические материалы WeProtect Global Alliance и Интерпола за период 2021–2025 гг.

Каждый инструмент оценивается по двум аналитическим осям. Первая — обязательный характер, который различает жесткое право — инструменты, создающие юридически обязательные обязательства, подлежащие исполнению посредством механизмов урегулирования споров, — и мягкое право, которое формирует нормативные ожидания без формального механизма принудительного исполнения [5].

Iii. Результаты

Нормативная эволюция: Общий комментарий № 25 Конвенции ООН о правах ребенка и его наследие.

Принятие Общего комментария № 25 Комитетом ООН по правам ребенка в марте 2021 года представляет собой наиболее значимое событие в международном праве в области цифровых прав детей за последнее десятилетие. Комментарий устанавливает, что все права, закрепленные в Конвенции о правах ребенка, в полной мере применяются в цифровой среде и что государства несут активную обязанность регулировать деятельность частных субъектов, включая технологические компании, для обеспечения соответствия цифровых продуктов и услуг стандартам прав ребенка [5]. Критически важно, что он вводит принцип «Safety by design» — процесс проектирования онлайн-платформы с целью снижения риска причинения вреда тем, кто ею пользуется. Он носит превентивный характер и учитывает безопасность пользователей на протяжении всего процесса разработки сервиса, а не в ответ на уже произошедшие случаи причинения вреда [6].

Пояснительная записка к Общему комментарию 25 гласит, что безопасность по умолчанию — это практика проектирования услуг с целью обеспечения безопасности пользователей, например, путем установки безопасных настроек по умолчанию для учетных записей несовершеннолетних пользователей или путем предотвращения контактов взрослых с детьми [7].

Тем не менее, исследование также выявляет существенные пробелы в реализации. Комитет не обладает полномочиями по обеспечению соблюдения законодательства и может лишь выносить рекомендации. Обязательство проводить ОВП остается в значительной степени желаемым в большинстве государств, особенно в странах Глобального Юга, где возможности регулирования и техническая экспертиза ограничены. Следовательно, нормативный прогресс, изложенный в Общем замечании № 25, хотя и реален, остается неравномерно распределенным и структурно зависит от политической воли на внутригосударственном уровне.

Роль международных организаций

ЮНИСЕФ и МСЭ, исторически сосредоточенные на информационных кампаниях и пропаганде, с 2021 года предприняли существенный переход к технической стандартизации. Совместная разработка **ЮНЕСКО-ЮНИСЕФ-МСЭ Хартии 2026** года для государственных цифровых образовательных платформ является примером этого сдвига: Хартия устанавливает обязательные технические стандарты для платформ, используемых в образовательных контекстах, включая обязательные протоколы минимизации данных, запрет на поведенческую рекламу, направленную на детей, и требования к алгоритмической прозрачности в системах курирования контента [8].

Это представляет собой переход от «мягких нормативных указаний» к «квазинормативным техническим спецификациям» — развитие, которое отражает траекторию развития таких органов по стандартизации, как Рабочая группа по проектированию Интернета (IETF) в области сетевой безопасности.

Совместное заявление **ЮНИСЕФ и МСЭ от 2026 года об искусственном интеллекте и правах ребенка**, опубликованное ЮНИСЕФ и МСЭ, еще раз отражает эту эволюцию. В заявлении сформулирован набор принципов, регулирующих внедрение систем ИИ в среде, где находятся дети, с акцентом на алгоритмическую недискриминацию, минимизацию данных и запрет систем, предназначенных для использования психологических уязвимостей детей в коммерческих целях. Например, в нем устанавливается, что рекомендательные системы, развернутые на платформах со значительной долей детей-пользователей, должны подвергаться обязательной оценке воздействия на права ребенка и должны включать механизмы человеческого контроля, способные обнаруживать и прерывать схемы распространения вредоносного контента [9].

Вклад ОЭСР наиболее значителен в области обеспечения соответствия возрасту — технических и правовых механизмов, с помощью которых платформы проверяют возраст своих пользователей и применяют ограничения на контент, соответствующие возрасту. Стандарты ОЭСР (технический документ) на 2025 год создают общую терминологию: «Age assurance» — это общий термин, описывающий подходы к определению того, какие пользователи сети являются детьми, чтобы гарантировать, что им предлагаются услуги, соответствующие их возрасту и потребностям, а также что они защищены от незаконного, взрослого или иного вредного контента или услуг. Критическим пробелом является отсутствие конкретики в отношении того, как соблюдать требования по обеспечению защиты возраста, является распространенной проблемой во всех проанализированных законах. Эти требования часто лишь подразумеваются, описываются нейтральным с точки зрения технологий языком или приводится неисчерпывающий список потенциальных методов. Однако в ряде стран-членов ОЭСР появляются руководства по внедрению системы защиты возраста. Регуляторы в области онлайн-безопасности и конфиденциальности уделяют особое внимание защите возраста, создавая рабочие группы, предоставляя целевые консультации и, по крайней мере, в одном случае, предлагая собственные технические решения [10]. Эта система была принята в качестве ссылки в руководящих принципах ЕС по внедрению цифровых технологий для платформ со значительной долей детей-пользователей.

Динамика сотрудничества: Рост государственно-частно-гражданских партнерств

Структурно значимым результатом исследования является появление так называемых "Public-Private-Civic" (PPC) партнерств в качестве доминирующей операционной модели транснациональной цифровой защиты детей. В этой модели международные организации функционируют не просто как нормативные органы, но и как посредники, выступающие между суверенными государствами. Существуют пределы тому, что правительства и правоохранительные органы могут сделать в одиночку. Но нет предела тому, что правительства, правоохранительные органы, гражданское общество и преданные своему делу партнеры из частного сектора могут сделать вместе [11].

Глобальный альянс WeProtect, многосторонняя организация, По состоянию на 2026 год, альянс объединяет более 300 участников, включая более 100 правительств, ведущие технологические компании, организации гражданского общества и международные органы, работающие совместно для обеспечения безопасности детей в цифровом пространстве. Модель национальной стратегии реагирования Альянса — рамочная концепция управления, опубликованная в 2023 году и обновленная в 2025 году, — предоставляет государствам модульный, адаптируемый инструментарий для разработки национальных стратегий цифровой защиты детей, опираясь на передовой опыт различных правовых традиций и интегрируя технические стандарты, разработанные в сотрудничестве с крупными поставщиками платформ [12].

Проект «Детство» (Childhood Project) является примером международного сотрудничества при участии государств, Интерпола, Управления ООН по наркотикам и преступности (UNODC) и организации World Vision. В рамках этого проекта Интерпол способствует обмену разведывательной информацией, касающейся сексуальной эксплуатации детей в интернете, между 196 государствами-членами, координирует совместные расследования и проводит обучение национальных правоохранительных органов по цифровой криминалистике и подходам к выявлению детей-жертв с учетом травматического опыта [13]. В период с 2020 по 2025 год проект «Детство» способствовал выявлению более 14 000 детей-жертв по всему миру и аресту более 3200 подозреваемых — результаты, которые невозможны без инфраструктуры транснационального сотрудничества, предоставляемой Интерполом [14].

В 2024 году первое в своем роде глобальное исследование показало, что более 300 миллионов детей ежегодно становятся жертвами сексуальной эксплуатации и насилия с использованием технологий, при этом каждую секунду происходит 10 таких случаев. К сентябрю 2025 года ICSE выявила более 24 000 правонарушителей и 56 000 жертв — в среднем 14 жертв выявлялись ежедневно — а цель состоит в том, чтобы к 2030 году выявить в общей сложности 100 000 жертв. Для достижения этой цели Интерпол инвестирует средства в совершенствование своей передовой технологии, чтобы она стала по-настоящему современной **[15]**.

Iv. Обсуждение

Мандат «Safety by design»: от нормы к практике

Нормативный сдвиг в сторону «Safety by design» представляет собой фундаментальную переориентацию нормативной логики, регулирующей цифровые платформы. В рамках традиционной реактивной модели ответственность за

безопасность детей в значительной степени была индивидуализирована: от родителей ожидалось, что они будут контролировать онлайн-деятельность своих детей, а платформы несли ответственность за причиненный вред только в том случае, если они не удаляли незаконный контент после уведомления. Парадигма «Safety by design» переворачивает эту логику: она возлагает проактивную ответственность на архитекторов и разработчиков платформ за обеспечение того, чтобы их системы были структурно неспособны допускать определенные категории вреда для детей, независимо от того, были ли эти виды вреда явно выявлены и сообщены [16]

Исследование показывает, что, хотя нормативное обоснование концепции «Safety by Design» убедительно, ее практическая реализация сталкивается со значительными проблемами. Во-первых, существует проблема измерения: в отличие от традиционного регулирования безопасности продукции, где физические параметры можно проверить на соответствие определенным стандартам, «безопасность» цифрового сервиса является функцией сложных социотехнических взаимодействий, которые трудно количественно оценить и которые подвержены быстрым изменениям. Во-вторых, существует проблема конфликта интересов: сами компании, ответственные за внедрение мер «Безопасность на этапе проектирования», структурно заинтересованы — посредством моделей получения дохода, основанных на рекламе, и алгоритмов оптимизации вовлеченности — в проектировании платформ, которые максимизируют время, проведенное на платформе, а не благополучие детей. Следовательно, добровольное обязательство по внедрению концепции «Безопасность на этапе проектирования» без независимой проверки и существенных санкций за несоблюдение рискует превратиться в пиар-акцию, а не в содержательный механизм управления.

Также одним из проблем является создание генеративного ИИ критического пробела в международном праве. Из-за этого в десятках юрисдикций создание, хранение и распространение реалистичных ИИ-дипфейков и синтетических материалов с насилием над детьми формально не подпадает под уголовную ответственность. Необходимо юридически закрепить на глобальном уровне, что синтетическая генерация наносит прямой вред общественным институтам защиты детства и нормализует насилие, поэтому должна быть полностью криминализирована наравне с традиционными материалами.

V. Заключение

Проведенное исследование транснациональной системы защиты прав детей в условиях глобальной цифровизации позволяет сформулировать ряд ключевых выводов. Ни одно государство не способно обеспечить адекватную защиту детей от цифрового вреда в отрыве от других факторов. Трансграничный характер цифровой инфраструктуры и глобальная деятельность технологических платформ создают структурный императив для международного сотрудничества, которое перестало быть факультативным и стало правовой предпосылкой для эффективного выполнения государствами своих обязательств в соответствии с международным правом прав человека. Принятие Общего комментария ООН № 25 (2021) ознаменовало важнейший концептуальный сдвиг — переход от реактивного реагирования на угрозы к проактивному внедрению принципа *«Safety by Design»* (безопасность на этапе проектирования). Также сохраняются существенные пробелы в управлении. Механизмы

правоприменения остаются слабыми, соблюдение требований государствами неравномерно, частные технологические компании недостаточно регулируются, а система управления рисками, связанными с ИИ, — особенно с синтетической детской порнографией и алгоритмическим усилением — является неадекватной.

Список использованной литературы:

1. ITU report, "Global Connectivity Report, ITU, Chapter 1, The connectivity journey," 2025. [Online]. Available: //https://www.itu.int/itu-d/reports/statistics/2025/11/17/gcr-2025-chapter-1/. [Accessed 13 май 2026].
2. ITU Guidelines, "ITU Child Online Protection Guidelines and Recommendations," 2021 . [Online]. Available: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/COP/20-00802_COP-Policy_Brief.pdf . [Accessed 13 май 2026].
3. Livingstone, S., & Stoilova, M. "The 4Cs: Classifying Online Risk to Children," Hamburg: Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI); CO:RE - Children Online:, no. https://doi.org/10.21241/ssoar.71817, 2021.
4. V. V. E. L. Yohannes Eneyew Ayalew, "General Comment No. 25 on Children's Rights in Relation to the Digital Environment: Implications for Children's Right to Privacy and and Data Protection in Africa," Human Rights Law Review, Volume 24, Issue 3, no. https://doi.org/10.1093/hrlr/ngae018, September,2024.
5. Комитет по правам ребенка, "CRC/C/GC/25," 02 март 2021. [Online]. Available: https://www.ohchr.org/ru/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation. [Accessed 20 май 2026].
6. UK-GOV guidance, "Principles of safer online platform design," https://www.gov.uk/guidance/principles-of-safer-online-platform-design, 29 June 2021.
7. 5 Rights Foundation, "Explanatory Notes: General comment no. 25 (2021) on children's rights in relation to the digital environment," https://5rightsfoundation.com/uploads/ExplanatoryNotes_UNCRCGC25.pdf, 2021.
8. UNESCO, "Charter for Public Digital Learning Platforms: Seven principles to steer and sustain public digital learning platforms," 2026. [Online]. Available: https://www.unesco.org/en/digital-education/learning-platforms-gateway/charter . [Accessed 13 май 2026].
9. ITU publications, "Совместное заявление об искусственном интеллекте и правах ребенка," 2025. [Online]. Available: https://www.ohchr.org/sites/default/files/documents/hrbodies/crc/activities/2025-11-joint-stm-itu-crc-r.pdf . [Accessed 13 май 2026].
10. OECD publications, "THE LEGAL AND POLICY LANDSCAPE OF AGE ASSURANCE ONLINE FOR CHILD SAFETY AND WELL BEING TECHNICAL PAPER," [Online]. Available: https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/06/the-legal-and-policy-landscape-of-age-assurance-online-for-child-safety-and-well-being_cdf49a15/4a1878aa-en.pdf. [Accessed 13 май 2026].
11. E. Allen, "The power of publicative partnerships in eridicating child sexual exploitation, expert paper," [Online]. Available: https://ecpat.org/wp-content/uploads/2021/08/ECPAT-International-Public-Pvt-partnerships-1.pdf . [Accessed 13 май 2026].
12. ООН, "Борьба с детским секс-туризмом," офмциальный источник оон, 10 апреля 2013.

13. Интерпол, "Global raids rescue 3,200 potential victims of trafficking and identify 17,800 irregular migrants.," URL: https://www.interpol.int/News-and-Events/News/2024/Global-raids-rescue-3-200-potential-victims-of-trafficking-.
14. INTERPOL, "Innovation: Harnessing technology to protect children from online crime," https://www.interpol.int/Resources/INTERPOL-Spotlight/Spotlight-Issue-3-Defending-human-dignity/Innovation-Harnessing-technology-to-protect-children-from-online-crime.
15. Livingstone S. and K. Pothong, "UK “Secure by Design” vs Australian "Safety by Design"," no. https://blogs.lse.ac.uk/parenting4digitalfuture/2021/09/29/secure-by-design/., 2021
16. Livingstone, S., Stoilova, M., & Kelly, A. (2022). Risks and harms online: From moral panic to risk management. The Political Quarterly, 93(2), 285–292. https://doi.org/10.1111/1467-923X.13117
17. WeProtect Global Alliance. (2023). Model national response framework for combating child sexual exploitation and abuse online (3rd ed.). WeProtect Global Alliance.