Международное право
Правильная ссылка на статью:
Родионов А.Е. Современное международно-правовое регулирование кибербуллинга в отношении защиты прав детей // Международное право. 2025. № 1. DOI: 10.25136/2644-5514.2025.1.72807 EDN: XDBUQD URL: https://nbpublish.com/library_read_article.php?id=72807

Современное международно-правовое регулирование кибербуллинга в отношении защиты прав детей

Родионов Алексей Евгеньевич

ORCID: 0009-0002-5146-473X

аспирант; кафедра Международное право; Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации» (ИЗиСП)
Юрист; Адвокатское Бюро "Дубровская; Кузнецова и партнеры г. Москвы

117218, Россия, г. Москва, ул. Большая Черемушкинская, 34

alex.kreativ@mail.ru

Статья из рубрики "Развитие отдельных отраслей международного публичного права"

DOI:

10.25136/2644-5514.2025.1.72807

EDN:

XDBUQD

Дата направления статьи в редакцию:

22-12-2024

Дата публикации:

25-01-2025

Аннотация: Статья посвящена анализу современного международно-правового регулирования кибербуллинга и его влияния на защиту прав детей. Актуальность исследования обусловлена возрастающей распространенностью кибербуллинга, особенно среди детей, и его усилением в условиях гибридных вооруженных конфликтов. Это явление требует всестороннего изучения существующей международно-правовой базы для выявления ее сильных и слабых сторон в обеспечении защиты прав ребенка в цифровом пространстве. Объектом исследования является международно-правовая база, регулирующая кибербуллинг и защиту прав ребенка. Предметом исследования выступают нормы международного права, регулирующие общественные отношения в сфере защиты несовершеннолетних от буллинга в сети Интернет. Цель исследования –

критически оценить эффективность существующих международных договоров, конвенций и деклараций в противодействии кибербуллингу и защите детей от насилия в сети «Интернет». Методами исследования выступили анализ, абстрагирование, индукция, дедукция, гипотеза, аналогия, синтез, типология, классификация, систематизация и обобщение, а также формально-логический; историко-правовой; сравнительно-правовой; статистический; социологический; метод анализа конкретных правовых ситуаций. Статья сосредоточена на выявлении пробелов и недостатков в современном международном праве, включая его ограниченность в эффективном реагировании на различные цифровые вызовы, в том числе создаваемые кибербуллингом в условиях гибридных войн. В работе исследованы сущностные аспекты правовых основ и значения международного сотрудничества по борьбе с кибербуллингом, уделено внимание различным подходам противодействия как со стороны основных органов ООН, так и региональных международных организаций, в условиях новых вызовов и угроз в отношении детей. Приведены основные международные акты, регламентирующие рассматриваемый вопрос и аргументирована позиция относительно современного состояния международных актов по преодолению проблемы. Отражена значимость совершенствования международно-правового регулирования с целью обеспечения защиты прав ребенка в условиях гибридных вооружённых конфликтов. Уделено внимание пробелам и недостаткам существующих норм, а также перспективам развития международного права в указанной области.

Ключевые слова:

вооруженные конфликты, гибридная война, защита прав детей, интернет, кибербуллинг, международное право, международные акты, международно-правовое регулирование, международные организации, международное взаимодействие

Введение

Информационно-телекоммуникационная сеть Интернет стала неотъемлемой частью мировой экономики, коммуникации и права [5, 6, 22, 40]. Развитие Интернета привело к появлению новых правовых вызовов – защиты персональных данных, кибербезопасности и международного регулирования цифровой среды [41], а также невозможно исключить влияние Интернета как основного средства достижения целей гибридной войны [25, с. 6].

Интернет перешел из статуса исследовательского проекта в глобальное коммерческое и общественное явление, поскольку в 1989 году Тим Бернерс-Ли предложил концепцию Всемирной паутины (World Wide Web), которая включала гипертекстовые документы, доступные через браузеры [52]. Указанная технология сделала Сеть доступной для массового использования, что привело к ее стремительному росту в современном виде.

Следует отметить, что угрозы информационной безопасности являются неотъемлемым аспектом развития и использования информационных технологий [18, с. 129]. Отсутствие в международном праве точных правовых норм, регламентирующих противодействие кибератакам, усугубляется, вместе с тем, и отсутствием единого определения понятию «кибератака» [18, 39].

Компьютерные преступления, или киберпреступления, – это широкий круг деяний,

включающий в себя посягательства разной степени опасности на различные общественные ценности: неприкосновенность частной жизни, собственность, доступ к информации [5, с. 167–171]. По мнению Г.Г. Шинкарецкой, в принятых определениях не проводится различия между киберпреступностью, кибератакой и кибервойной, поэтому эти термины могут применяться повсеместно и широко [35].

Для обозначения травли в образовательных организациях используется термин «буллинг». Слово «буллинг» как лексическая единица современного языкового поля происходит от голландского *boel «любовник, брат»* и средненемецкого уменьшительного *buole «брат»*. В течение XVII века в европейских языках оно применялось в значениях о т *«славного парня»*, *«хвастуна»* до *«преследователя слабых»*. В качестве глагола *«запугивать»* слово *bully* впервые употребляется в английском языке не ранее 1710 года [19, с. 112–115].

В указанной связи следует отметить, что кибербуллинг является отдельным видом сетевой (онлайн) агрессии, которая отличается от природы интернет-атак [5, с. 1–2; 6], и как современное правовое явление определение «жертвы кибербуллинга» у многих авторов отсутствует [5, с. 1]. В отечественной и зарубежной литературе традиционно ограничиваются толкованием «киберзапугивания», не разъясняя понятие пострадавших от него лиц [4; 13; 46].

Проблематика кибербуллинга является предметом активных исследований как в зарубежной, так и в отечественной науке.

Работы таких зарубежных ученых, как Йувонен и Е.Ф. Гросс, Ц. Кыриацоу и А. Зуин, а также К. Алонсо, Э. Ромеро и К. Кумар, в значительной степени способствовали развитию теоретических основ данного явления. В их исследованиях кибербуллинг рассматривается с различных точек зрения – психологической, социальной, культурной и правовой. Они уделяют внимание психологическим эффектам, которые испытывают жертвы, а также анализируют особенности агрессивных действий в онлайн-среде.

Отечественные исследователи – такие, как Д.В. Завьялова, А.Ю. Гусев, Д.В. Жмуров, Л.В. Бондаренко, О.Н. Ведерникова, Э. Верхелст и др., также внесли значительный вклад в изучение проблемы. Работы этих авторов посвящены различным аспектам кибербуллинга, включая его правовую классификацию, социальные последствия и меры противодействия. Д.В. Завьялова и А.Ю. Гусев акцентируют внимание на характеристиках и формах кибербуллинга в российском контексте, а Д.В. Жмуров и Л.В. Бондаренко рассматривают психологические и социальные факторы, влияющие на возникновение этого явления.

Конкретизация понятия кибербуллинга осуществлена в работах Й. Йувонен и Е.Ф. Гросс, где под кибербуллингом предложено понимать воздействие на физическое лицо или преследование физического лица с применением информационно-коммуникационных технологий. Кибербуллинг осуществляется для распространения клеветы и оскорблений, унижения жертвы, доведения жертвы до самоубийства [11, 42].

В то же время, Ц. Кыриацоу, А. Зуин понимают под кибербуллингом и разглашение конфиденциальной информации как самостоятельную категорию преступных деяний, включающих в себя размещение в информационной среде материалов, составляющих личную или семейную тайну [11, 44].

Категорию пострадавших нередко описывают как лиц с относительно высокими

показателями доброжелательности, нейротизма и экстраверсии, открытых опыту [38].

В указанных определениях можно отметить несколько спорных моментов. Во-первых, при ограничении кибербуллинга исключительно воздействием через информационно-коммуникационные технологии (Йувонен и Гросс) не учитывается роль других факторов – таких, как контекст социальной сети или конкретные формы онлайн-агрессии. Во-вторых, разглашение конфиденциальной информации (Кыриацоу и Зуин) может быть слишком обширным и охватывать действия, которые не всегда можно классифицировать как кибербуллинг, например, в случае случайных утечек данных или неумышленного распространения личной информации.

Современные русские правоведы дают следующие определения кибербуллинга. Д.В. Завьялова: «Кибербуллинг, в отличие от классической травли, осуществляется в киберпространстве: в социальных сетях, мессенджерах, на форумах, на игровых площадках и в других коммуникационных сетевых пространствах» [6]. А.Ю. Гусев дает обтекаемую формулировку: кибербуллинг – травля, издевательство, носящие систематический характер, с использованием информационно-телекоммуникационной сети Интернет [15]. Д.В. Жмуров утверждает: «Традиционно под этим явлением понимается агрессивное взаимодействие с использованием электронных средств коммуникации» [13].

При анализе определений кибербуллинга, предложенных отечественными авторами, можно сделать несколько ключевых замечаний. Д.В. Завьялова ограничивает кибербуллинг исключительно киберпространством, не учитывая, что агрессия может проявляться и в других формах коммуникации – таких, как онлайн-игры или электронная почта. А.Ю. Гусев указывает на «систематический характер», но не уточняет критерии, по которым можно определить систематичность травли, что затрудняет практическое применение определения данного автора в юридической или социальной практике. Определение Д.В. Жмурова, характеризующее кибербуллинг как «агрессивное взаимодействие», является слишком обобщённым и не отражает специфических психологических и социальных аспектов этого явления – таких, как намеренное унижение и психологическое воздействие на жертву.

Представляется возможным в рамках настоящей работы дать собственное определение данному деянию: кибербуллинг – это систематические целенаправленные действия, совершаемые с использованием информационно-коммуникационных технологий (включая, но не ограничиваясь Интернетом, мобильными телефонами, социальными сетями и другими электронными средствами связи), направленные на унижение, запугивание, оскорбление, преследование или причинение иного вреда (физического, психологического, репутационного) другому лицу; эти действия включают угрозы, распространение ложной или компрометирующей информации, публикацию оскорбительных материалов, использование уничижительных изображений или сообщений, а также другие формы онлайн-агрессии, которые приводят к значительным и долгосрочным негативным последствиям для психоэмоционального состояния, социальной репутации или физического благополучия жертвы.

У Р. Бадинтера есть формулировка: «Права человека не даны нам в откровение, у них есть своя история» («Les droits de l'homme ne nous ont pas été révélés, mais ont une histoire») [39, с. 1], что отражает длительное становление таких прав. В условиях стремительного развития цифровых технологий и расширения виртуального пространства кибербуллинг становится глобальной проблемой, затрагивающей права человека в

целом, а также права детей, включая право на защиту от насилия, психическое и физическое здоровье, неприкосновенность частной жизни в условиях новой угрозы.

Между тем, развитие информационных технологий внесло существенные коррективы в военные доктрины, планы и стратегии боевых действий. К примеру, в военных подразделениях стран Североатлантического альянса созданы кибервойска с функциями, не ограниченными одной лишь защитой собственных коммуникаций [34, с. 2]. Они активно занимаются шпионажем с помощью сети Интернет, а также распространением порочащих сведений и формированием нужного общественного мнения в социальных сетях [25, с. 6]. В условиях гибридного противостояния государств дети являются самой уязвимой группой.

Взаимосвязь между кибербуллингом в отношении несовершеннолетних и гибридными (информационными) войнами обуславливается использованием информационно-телекоммуникационной сети Интернет в качестве инструмента целенаправленного информационного воздействия. Кибербуллинг, являющийся одной из форм незаконного информационного влияния, предполагает психологическое давление, угрозы, распространение порочащих сведений и манипуляцию данными, что приводит к существенному нарушению прав и свобод несовершеннолетних, гарантированных международным и национальным правом. Эти методы могут быть интегрированы в стратегии гибридных войн, направленные на подрыв устойчивости гражданских институтов, разжигание социальной напряженности и деморализацию уязвимых групп населения, включая несовершеннолетних [16; 21].

Кроме того, подходы, используемые в кибербуллинге, по своей сути схожи с методами, применяемыми в рамках гибридных войн, включая распространение дезинформации, информационные манипуляции и пропагандистское давление. Разница заключается в масштабе воздействия: если кибербуллинг ограничивается воздействием на индивидов, то гибридные войны охватывают более широкий круг субъектов, включая несовершеннолетних как наиболее уязвимую аудиторию [26].

Кибербуллинг может рассматриваться не только как самостоятельное противоправное явление, но и как элемент стратегии гибридных войн, использующий схожие механизмы информационного воздействия в целях нарушения общественного порядка, дестабилизации и достижения иных противоправных целей [27].

Ввиду актуальности проблемы противодействия кибербуллингу в контексте защиты прав детей представляется возможным исследовать международно-правовые регуляторы, направленные на предупреждение и пресечение кибербуллинга, и рассмотреть эффективность применяемых международным сообществом мер. Особого внимания требует рассмотрение роли универсальных и региональных международных договоров, а также деятельности специализированных международных организаций.

Материалы и методы

Объектом исследования является международно-правовая база, регулирующая кибербуллинг и защиту прав ребенка. Предметом исследования выступают нормы международного права, регулирующие общественные отношения в сфере защиты несовершеннолетних от буллинга в сети Интернет. Цель исследования — критически оценить эффективность существующих международных договоров, конвенций и деклараций в противодействии кибербуллингу и защите детей от насилия в сети Интернет.

Для проведения исследования и комплексного раскрытия его предмета в статье применены системный и комплексный подходы, сравнительно-правовой и доктринальный принципы исследования.

Основная часть

В силу ч. 3 ст. 1 «Устава Организация Объединенных Наций», ООН преследует цель осуществлять международное сотрудничество в разрешении международных проблем экономического, социального, культурного и гуманитарного характера, а также поощрять и развивать уважение к правам человека и основным свободам для всех людей без различия расы, пола, языка и религии.

На любой основной орган ООН налагается обязанность через «Устав ООН» содействовать международному сотрудничеству в вышеуказанных областях (п. «b» ч. 1 ст. 13, ч. «c» ст. 55, ч. 2 ст. 62, ч. «c» ст. 76 «Устава ООН»).

Реализация международного взаимодействия зафиксирована в «Декларации о принципах международного права», касающихся дружественных отношений и сотрудничества между государствами в соответствии с «Уставом Организации Объединенных Наций», «Резолюцией 2625 (XXV) Генеральной Ассамблеи ООН» от 24.10.1970.

Основополагающие положения свободы убеждений и их свободного выражения были определены в ст. 19 «Всеобщей декларации прав человека» (принята Генеральной Ассамблеей ООН 10.12.1948), в ст. ст. 2–27 «Международного пакта о гражданских и политических правах» (принят 16.12.1966 «Резолюцией 2200 (XXI)» на 1496-м Пленарном заседании Генеральной Ассамблеи ООН), в ст. ст. 12–14 «Конвенции о правах ребенка» (одобрена Генеральной Ассамблеей ООН 20.11.1989), в ч. 6 ст. 1 «Декларации тысячелетия Организации Объединенных Наций» (принята «Резолюцией 55/2 Генеральной Ассамблеи» от 08.09.2000) и многих других документах.

В контексте кибербуллинга необходимо отметить «Конвенцию о правах ребенка» 1989 года, которая закрепляет общие принципы защиты прав ребенка, применимые к деятельности по защите детей от преступлений в сети Интернет и обязывающие государства защищать ребенка от информации и материалов, наносящих вред его благополучию (п. «e» ст. 17) [7, с. 2].

Значимость имеет также «Конвенция Совета Европы о защите физических лиц в отношении автоматизированной обработки персональных данных» (1981 года), которая создала основы для защиты частной жизни в условиях цифровизации, косвенно затрагивая возможные угрозы кибербуллинга, связанные с неправомерным использованием данных. В ст. 1 данной Конвенции закреплено, что ее целью является обеспечение на территории каждой стороны для каждого физического лица, независимо от его гражданства или местожительства, уважения его прав и основных свобод, и в частности его права на неприкосновенность частной жизни в отношении автоматизированной обработки касающихся его персональных данных («защита данных»). В ст. 2 указанной Конвенции прямо закрепляется понятие «персональные данные», однако из смысла всей Конвенции вытекает, что в действительности ставится вопрос о защите не конкретного физического лица от посягательства (ст. 10 Конвенции), а именно самих персональных данных. Первичные персональные данные также являются объектом посягательства при кибербуллинге, а следовательно, указанные нормы гарантируют безопасность и защиту передачи данных.

Важным международным инструментом в области регулирования поведения в цифровом пространстве стала «Конвенция Совета Европы по киберпреступлениям» (Будапештская конвенция), принятая 23.11.2001. Это первый и до сих пор ключевой международный договор, направленный на борьбу с преступлениями, совершаемыми с использованием компьютерных систем. Основной целью данной Конвенции, закрепленной в ее преамбуле, является разработка совместной политики уголовного права, которая способствовала бы защите общества от киберпреступности, в том числе путем принятия соответствующих законодательных мер и создания эффективного международного сотрудничества. Рассматриваемая Конвенция вводит правовые и процедурные стандарты для предотвращения и преследования киберпреступлений, включая такие явления, как кибербуллинг, в тех случаях, когда он сопряжен с нарушением уголовного законодательства [48].

В ст. 2–6 Будапештской Конвенции перечислены составы преступлений, которые государства-участники обязаны инкорпорировать в свое национальное законодательство, включая неправомерный доступ к компьютерным системам, вмешательство в данные или системы, а также неправомерное использование устройств. Эти положения косвенно охватывают случаи кибербуллинга, связанные с использованием взломанных или поддельных учетных записей, размещением вредоносного контента или незаконным доступом к персональным данным.

Особое внимание в «Конвенции СЕ по киберпреступлениям» уделено вопросам сбора электронных доказательств и обеспечения защиты пострадавших. Глава II данного правого документа устанавливает процессуальные меры для эффективного расследования киберпреступлений. В частности, ст. 16 и 18 вводят обязательства по обеспечению быстрого доступа к данным о трафике и идентификации пользователей, что особенно важно в делах о кибербуллинге, где правонарушители часто используют анонимность Интернета для уклонения от ответственности.

Не менее значимым является положение ст. 15 Будапештской Конвенции, которое требует от государств-участников предусмотреть гарантии защиты прав и свобод личности при реализации процедурных норм, включая защиту данных, что сближает ее с положениями «Конвенции о защите физических лиц в отношении автоматизированной обработки персональных данных» (1981 г.). Данное требование обеспечивает баланс между необходимостью борьбы с преступлениями и защитой частной жизни пользователей, создавая правовые рамки для пресечения незаконных действий без чрезмерного вмешательства в права человека.

Кроме того, «Конвенция СЕ по киберпреступлениям» предусматривает механизмы международного сотрудничества (глава III), включая оперативный обмен информацией между компетентными органами государств-участников, что особенно важно для расследования трансграничных случаев кибербуллинга. Так, ст. 35 данной Конвенции вводит институт круглосуточных контактных точек, которые могут быть использованы для быстрого обмена данными о преступлениях, совершаемых в Интернете. 7 ноября 2002 года Комитетом министров СЕ был принят, а 20 января 2003 года открыт «Дополнительный протокол к Конвенции о киберпреступности, касающийся криминализации актов расистского и ксенофобского характера, совершаемых через компьютерные системы», который прямо направлен на предотвращение дискриминационного и унижающего достоинство поведения в Интернете, включая случаи, сопряженные с кибербуллингом.

Недостатком Будапештской Конвенции является отсутствие прямой статьи, посвященной

травле в цифровой среде, однако ее положения создают основу для привлечения к ответственности за смежные правонарушения – такие, как угрозы (ст. 4) и неправомерное использование данных (ст. 6). Конвенция о киберпреступности, хотя и является прогрессивным документом своего времени, требует модернизации в свете новых вызовов цифровой эпохи [49]. Вызовы включают распространение явлений – таких, как массовые кибератаки, анонимность, шифровку подключения, систематические онлайн-нападки с помощью платформ, которые охватывают большую аудиторию онлайн-посетителей и другие, выходящие за рамки первоначальных формулировок Конвенции [45].

Между тем, интерес представляет «Рекомендация CM/Rec(2014)6 Комитета министров государствам-членам Совета Европы к Руководству по правам человека для интернет-пользователей» (принята 16.04.2014 г. на 1197-м заседании постоянных представителей министров), в которой подчеркивается необходимость разработки национальных стратегий, направленных на защиту детей от насилия, включая кибербуллинг, а также на продвижение цифровой грамотности.

В ч. 1 «Рекомендации CM/Rec(2014)6…»закреплено, что: «Государства-члены Совета Европы обязаны обеспечить каждому, находящемуся под их юрисдикцией, права и основные свободы, закрепленные в "Европейской конвенции о защите прав человека" (СЕД № 5, Конвенция). Это обязательство также действует и в отношении использования сети Интернет. Здесь также применяются и другие конвенции и документы Совета Европы, касающиеся защиты свободы выражения мнения, доступа к информации, свободы собраний, защиты от киберпреступности и права на частную жизнь и на защиту персональных данных».

В разделе «Дети и молодежь» ч. 5 «Рекомендации CM/Rec(2014)6…»прямо указано, что кибербуллинг должен пресекаться и не допускаться: «Вам должна быть предоставлена особая защита от нарушения вашего физического, психического и нравственного благополучия, в частности, защита от сексуальной эксплуатации и оскорблений в Интернете и других форм киберпреступности. В частности, у вас есть право на образование, призванное защитить вас от таких угроз».

Совет Европы закрепил необходимость пресечения и недопущения кибербуллинга, рассматривая его как угрозу физическому, психическому и нравственному благополучию детей, сопоставимую с сексуальной эксплуатацией и другими формами киберпреступности.

Исходя из этого, кибербуллинг юридически признается противоправным деянием, требующим принятия всех возможных мер для его искоренения. Государства, являющиеся членами Совета Европы, обязаны обеспечивать право детей на защиту от подобных угроз, включая создание образовательных программ, направленных на профилактику и противодействие кибербуллингу. Кроме того, особое значение уделяется свободе выражения мнения, праву на частную жизнь, праву на образование, правам ребенка и защите от киберпреступности (ч. 9 «История вопроса и контекст»).

Более того, Совет Европы, не отменяя, а развивая положения «Рекомендации CM/Rec(2009)5 Комитета министров государствам-членам о мерах по защите детей от вредоносного контента и поведения и по поощрению их активного участия в новой информационной и коммуникационной среде», перенес эти принципы и цели в новую Рекомендацию, тем самым отразив преемственность и актуальность поднятых вопросов и подчеркнув, что государства-участники должны организовать своевременный ответ на

жалобы на кибериздевательства или киберухаживания, которые влекут за собой негативные последствия.

На рост кибертравли в обществе, в частности в отношении детей в Интернете и цифровом пространстве, обратили недавно внимание и в ООН.

П. 16 «Резолюции ООН № 74/133» от 2019 г. «решительно осуждает все формы насилия в отношении детей, совершаемого при любых обстоятельствах, включая физическое, психологическое и сексуальное насилие, (…) сексуальную эксплуатацию детей в Интернете и вне его, травлю, включая кибертравлю, и настоятельно призывает государства к тому, чтобы они активизировали усилия для предотвращения всех форм такого насилия и защиты детей от него посредством применения всеобъемлющего, учитывающего гендерные аспекты и возраст подхода, выработали инклюзивный, многофункциональный и систематизированный комплекс мер для эффективного реагирования на насилие в отношении детей и для обеспечения безопасных и учитывающих интересы детей механизмов консультирования, рассмотрения жалоб и представления сообщений и гарантий прав пострадавших детей и интегрировали этот комплекс мер в национальные процессы планирования».

Резолюция Генеральной Ассамблеи ООН № 75/166 «Защита детей от издевательств» от 16.12.2020 зафиксировала, что ежегодно, начиная с 2020 года, в первый четверг ноября отмечается Международный день борьбы с насилием и издевательствами в школе, включая киберзапугивание [7, с. 5].

ООН разработаны различные иные рекомендации – например, «Защита детей в Интернете (COP)», которая представляет собой многостороннюю сеть, созданную Международным союзом электросвязи (МСЭ) для защиты детей в Интернете с всеобъемлющим набором рекомендаций для всех заинтересованных сторон о том, как способствовать созданию безопасной и расширяющей возможности онлайн-среды для детей и молодёжи.

В 2019 г. ЮНИСЕФ опубликовал дискуссионный документ под заголовком*Child Rights and Online Gaming: Opportunities & Challenges for Children and the Industry* («Права ребенка и онлайновые игры: возможности и сложности для детей и отрасли»), чтобы обсудить возможности и сложности, возникающие перед детьми в одной из наиболее быстро растущих отраслей развлечений. В документе рассматриваются следующие темы: 1) право детей на игру и свободу выражения (время, проводимое за игрой, и последствия для здоровья); 2) отсутствие дискриминации, участие и защита от насилия (социальное взаимодействие и полноправное включение, токсичная среда, возрастные ограничения и их проверка, защита от груминга и сексуальных злоупотреблений); 3) право на конфиденциальность и свободу от экономической эксплуатации (бизнес-модели предоставления доступа за данные, бесплатные игры и монетизация, отсутствие прозрачности в коммерческом контенте).

Основой международного права является государственный суверенитет, который, однако, с трудом вписывается в реальность киберпространства [53]. Несмотря на достигнутый консенсус относительно реализации государственного суверенитета в киберпространстве, ни одно из существующих государств не может претендовать на суверенитет, который бы охватывал все киберпространство [47] ввиду того фактора, что многие элементы инфраструктуры, на базе которых существует киберпространство, находятся в пределах разных суверенных территорий и, следовательно, согласно международному праву, относятся к разным юрисдикциям [8].

Тем не менее, Дж. Трахтмэн справедливо отмечает, что деление юрисдикций не должно быть основанием для отказа от регулирования всего киберпространства: в конце концов, действия в киберпространстве всё равно осуществляются на конкретной территории, равно как и их последствия ощущаются в конкретной области [51]. И то обстоятельство, что отдельные проблемы выходят за рамки конкретных юрисдикций, не является чем-то новым для международного права [8].

Исходя из вышеуказанного, следует констатировать, что мировое сообщество в целом начало процедуру признания через нормы международного права проблематики кибербуллинга как новой формы киберпреступности, представляющей угрозу, сопоставимую по наносимому вреду с традиционными формами насилия в отношении детей.

Вопрос профилактики кибербуллинга как одной из форм насилия в цифровом пространстве стал приоритетным направлением деятельности многих региональных международных организаций. Их подходы к решению данной проблемы формируют правовые рамки и создают платформы для сотрудничества между государствами.

Рассмотрим ключевые документы и инициативы таких организаций, как Европейский Союз (ЕС), Организация американских государств (ОАГ), Ассоциация государств Юго-Восточной Азии (АСЕАН), Евразийский экономический союз (ЕАЭС) и Содружество Независимых Государств (СНГ) [7, с. 1–2].

Европейский Союз активно занимается вопросами регулирования поведения в цифровой среде, уделяя особое внимание защите персональных данных и борьбе с незаконным контентом. Ведущим документом ЕС в данном контексте является «Общий регламент по защите данных (GDPR) 2016/679», который вступил в силу в 2018 г. «Общий регламент… (GDPR) 2016/679» устанавливает строгие требования к обработке персональных данных, что, в свою очередь, создает барьеры для неправомерного использования информации, типичного для кибербуллинга (например, публикации личных данных без согласия).

В 2022 г. Европейский парламент и Совет ЕС приняли «Акт о цифровых услугах (Digital Services Act)», который регулирует деятельность цифровых платформ, обязывая их оперативно реагировать на жалобы о противоправном контенте, включая случаи кибербуллинга. В ст. 12 Акта DSA предусматриваются обязательства платформ обеспечивать безопасное онлайн-пространство, что прямо касается профилактики цифрового насилия.

Как подчеркивает Г. Винер, меры ЕС демонстрируют комплексный подход к обеспечению цифровой безопасности, сочетая уголовно-правовые, гражданско-правовые и административные механизмы [54].

Межамериканская комиссия по правам человека в 2015 г. опубликовала доклад «Кибербуллинг и цифровая безопасность в Америке» и призвала государства-члены разработать национальные программы по предотвращению насилия в Интернете, особенно среди детей и подростков в социальных сетях, поскольку, когда виктимизация происходит в Интернете, существует большая вероятность того, что она охватит широкую аудиторию. Контроль над содержанием и распространением публикаций находится вне контроля жертвы, и публикация может мгновенно стать вирусной. Это усугубляется тем фактом, что контент хранится в сети Интернет дольше, чем при личном общении, что делает его доступным на неопределённый срок, если только он не будет удалён. Однако

удаление чего-либо на одном сайте не означает, что это будет недоступно на других сайтах и легко не распространится на сотни, если не тысячи, других сайтов [48].

В рамках АСЕАН разработан «План действий по обеспечению кибербезопасности 2021–2025 гг.», который включает меры по защите пользователей от киберугроз, включая кибербуллинг. В документе подчеркивается необходимость развития регионального сотрудничества в области предотвращения и расследования цифровых преступлений [50].

В ЕАЭС осознают необходимость совместных усилий для борьбы с киберпреступностью и кибербуллингом и принимают серьезные меры, направленные на обеспечение информационной безопасности. Так, в 2013 г. в Санкт-Петербурге было заключено «Соглашение о сотрудничестве государств – участников Содружества Независимых государств в области обеспечения информационной безопасности». Указанный нормативно-правовой акт является основным в области борьбы с киберпреступностью, и страны – участницы ЕАЭС всё еще руководствуются им при составлении новых актов в области кибербезопасности [14, с. 3–4].

29.05.2014 в г. Астане подписан «Протокол об информационно-коммуникационных технологиях и информационном взаимодействии в рамках Евразийского Экономического Союза» (Приложение № 3 к «Договору о Евразийском экономическом союзе») [14, с. 4–5].

По мнению Г.И. Тункина, еще в 1970 г. сфера прав человека, которая ранее была исключительно внутренним делом государств, долгое время оставалась закрытой для международного вмешательства. Однако за последние 60 лет в этой области международного права произошло беспрецедентное развитие. Это развитие охватывает широкий спектр норм – от общепризнанных стандартов до положений, касающихся международных механизмов с обязательной юрисдикцией для защиты нарушенных прав. Это развитие можно рассматривать как значительное достижение, свидетельствующее о расширении влияния международного права на защиту прав человека [23, с. 93]; за последующие 40 лет международное сообщество смогло увеличить указанный спектр [12].

Тем не менее, самым главным остается следующий аспект любого международного правового предложения – выгода всем участникам потенциального процесса. Если договор не является компромиссным, то возможность его подписания маловероятна. Это обусловлено «волей государств» в международном праве [31].

Отметим, что правовую позицию по «согласованной воли» государства в международном праве разделяют такие правоведы современности, как В.Р. Авхадеев [1], Б.М. Ашавский [2, 3, 33], А.И. Ковлер [10], И.В. Холиков [25–29, 43], а также правоведы прошлого: Г.И. Тункин [23], И.И. Лукашук [31], Ф.Ф. Мартенс [32] и другие.

«Согласованная воля, во-первых, находит выражение в содержании нормы, во-вторых, она обязывает субъектов соблюдать эту норму. От воли субъектов зависит характер обязательной силы нормы. Они могут придать ей юридическую или морально-политическую обязательную силу по своему усмотрению. Непосредственно субъекты достигают соглашения о содержании нормы и о придании ей соответствующей обязательной силы» [31, с. 17].

Существующие международные правовые акты, хотя и затрагивают отдельные аспекты

защиты прав детей в цифровом пространстве, не всегда содержат исчерпывающие нормы, регулирующие кибербуллинг, поскольку разногласия возникают по вопросам определения самого понятия кибербуллинга, установления юрисдикции в трансграничных случаях, а также определения мер ответственности за совершение данного деяния [24].

Традиционные международно-гуманитарные механизмы, ориентированные на физические формы насилия [9], оказываются недостаточно эффективными для противодействия кибербуллингу, который может причинять существенный вред психическому и эмоциональному здоровью детей, усугубляя гуманитарный кризис в условиях вооружённых конфликтов [16].

Применение кибербуллинга в качестве инструмента гибридной войны представляет собой новую угрозу правам ребенка [16, с. 3], требующую правового ответа [14, 7, 16, 17], а разработка и внедрение универсальных международно-правовых основ требует необходимости достижения консенсуса между государствами с различными правовыми системами, культурными традициями и уровнями технологического развития [20, с. 5–6].

Заключение

Таким образом, новые международные акты должны учитывать специфику киберпреступности в условиях вооруженных конфликтов, включая определение ответственности за организацию и проведение кибератак, направленных на детей [15], установление юрисдикции в отношении трансграничных преступлений [21, 30], а также разработку механизмов предотвращения и расследования подобных деяний [36-37]. В условиях гибридной войны ключевыми факторами являются идентификация субъектов, ответственных за кибербуллинг (государства, негосударственные вооруженные формирования, частные лица), и установление ответственности за действия, совершаемые под прикрытием анонимности.

Кибербуллинг, направленный на несовершеннолетних, представляет собой не только отдельное противоправное деяние, но и элемент информационного воздействия, применяемого в рамках гибридных войн. Сходство методов и целей данных явлений – таких, как дезинформация, манипуляция общественным сознанием и психологическое давление, подтверждает необходимость их комплексного анализа в условиях вооруженных конфликтов. Современное международное право демонстрирует на настоящий момент недостаточную степень регламентации указанных вопросов, поскольку отсутствие унифицированного понятия кибербуллинга, пробелы в определении трансграничной юрисдикции и недостаточная разработка механизмов привлечения к ответственности создают правовую неопределенность. Указанные факторы усложняют предотвращение и расследование преступлений, связанных с кибербуллингом и его использованием в рамках гибридных войн.

С учетом вышеизложенного, в числе приоритетных направлений совершенствования международно-правового регулирования кибербуллинга остается необходимость развития унифицированного понятия на основании опыта региональных международных организаций с целью обеспечения единообразного применения норм в различных юрисдикциях.

Кроме того, следует рассмотреть разработку концепции «цифрового нейтралитета» – принципа, запрещающего использование киберпространства для ведения

информационных атак и манипуляции в сторону детей и использование методов гибридной войны, с обязательством государств принимать меры по предотвращению таких действий для защиты детей.

Указанные меры должны быть основаны на базовых принципах международного права, включая принцип суверенного равенства государств, ненападения, мирного разрешения споров и сотрудничества между государствами. Особое внимание должно быть уделено необходимости выполнения обязательств, вытекающих из «Устава ООН». Принятие таких мер укрепит международный правопорядок и обеспечит стабильность в условиях цифровых вызовов современности.

Библиография

1. Авхадеев В.Р.: Оптимизация международного сотрудничества в Арктике в целях предотвращения основных вызовов и угроз национальной безопасности и устойчивому развитию Российской Федерации // Российский ежегодник международного права. 2022. Санкт-Петербург: ООО «Контраст», 2023. С. 169 – 181.
2. Ашавский, Б. М. Принципы невмешательства во внутренние дела государств и уважения прав и свобод человека как компоненты системы основных принципов международного права / Б. М. Ашавский // Образование и право. – 2016. – № 11. – С. 68-74. – EDN XEIFOF.
3. Ашавский Б.М. Обязанность защищать: путем гуманитарных интервенций или в соответствии с международным правом? // Право и культура: Материалы международной научной конференции / Отв. ред. Т.А. Сошникова. М.: Изд-во Моск. Гуманит. Ун-та, 2012.
4. Бажанова, А. С. Инновационные технологии в образовательном пространстве современной школы в условиях внедрения ФГОС / А. С. Бажанова, А. Г. Костина // СОВРЕМЕННАЯ НАУКА и ОБРАЗОВАНИЕ: АКТУАЛЬНЫЕ ВОПРОСЫ ТЕОРИИ и практики : сборник статей II Международной научно-практической конференции, Пенза, 10 марта 2023 года. – Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2023. – С. 109-111. – EDN XAHMKB.
5. Бондаренко, Л. В. Кибербуллинг в современных условиях: правовые аспекты противодействия / Л. В. Бондаренко // Перспективы развития институтов права и государства: Сборник научных статей 5-й Международной научной конференции, Курск, 12 мая 2022 года / Редколлегия: А.Н. Пенькова (отв. ред.). – Курск: Юго-Западный государственный университет, 2022. – С. 167.
6. Василевская Л.Ю., Иванов А.А., Харитонова Ю.С., Калятин В.О., Новикова М.А., Завьялова Д.В. Обзор круглого стола «Социальные сети и гражданское право» // Закон. 2023. № 3. С. 90-113.
7. Ведерникова, О.Н. Международно-правовые основы противодействия преступлениям против детей в сети Интернет / О.Н. Ведерникова // Международное уголовное право и международная юстиция. – 2022. – № 2.
8. Верхелст, Э. Глобальное управление в сфере кибербезопасности: взгляд с позиции международного права и права ЕС / Э. Верхелст, Я. Ваутерс // Вестник международных организаций: образование, наука, новая экономика. – 2020. – Т. 15, № 2. – С. 141-172. – DOI 10.17323/1996-7845-2020-02-07. – EDN QPNOSY.
9. Гаврилов С.О., Глебов И.Н., Чукин С.Г. Право в точке бифуркации: обсуждение концептуального исследования военных проблем международного права (Дискуссия в формате «круглого стола» по материалам гл. 6 «Военные проблемы международного права» т. III монографии «Военное право») // Государство и право. 2022. № 12. С. 59—67.
10. Европейская Конвенция в международной системе защиты прав человека: монография / А. И. Ковлер. — М.: Институт законодательства и сравнительного

правоведения при Правительстве Российской Федерации: Норма: ИНФРА М, 2019. — 304 с.
11. Елин, В. М. Уголовно-правовые инструменты борьбы с кибербуллингом в США / В. М. Елин // Международное уголовное право и международная юстиция. – 2022. – № 1. – С. 22-25. – DOI 10.18572/2071-1190-2022-1-22-25. – EDN AADVJZ.
12. Епифанов, А. Е. К вопросу о влиянии международного права на формирование механизмов защиты прав и свобод человека (вопросы теории и истории) / А. Е. Епифанов // Вестник Южно-Уральского государственного университета. Серия: Право. – 2015. – Т. 15, № 2. – С. 14-20. – EDN TVTJKB.
13. Жмуров, Д. В. Жертвы кибербуллинга: состояние проблемы / Д. В. Жмуров // Российский следователь. – 2023. – № 1. – С. 45-50. – DOI 10.18572/1812-3783-2023-1-45-50. – EDN ALMEIV.
14. Клюканова Т. М., Виниченко А. Т., Христинченко К. Ю. Анализ законодательства стран ЕАЭС в области борьбы с киберпреступностью // Евразийская интеграция: экономика, право, политика. 2024. Т. 18. № 3. С. 83–90.
15. Ответственность за травлю (буллинг) А.Ю. ГУСЕВ в редакции НИУ «Высшая школа экономики» подготовлен для системы КонсультантПлюс, 2024 – ст. 16.
16. Плакса В.Н., Холиков И.В. Международно-правовая защита гражданского населения и гражданской инфраструктуры при использовании военного киберпотенциала // Военное право. 2020. № 5(63). С. 200-213.
17. Преступность в XXI веке. Приоритетные направления противодействия / Ю. М. Батурин, В. Е. Батюкова, С. Д. Белоцерковский [и др.]; Институт государства и права РАН. Москва: Общество с ограниченной ответственностью «Издательство «Юнити-Дана», 2020. 559 с.
18. Прончев Г.Б., Лонцов В.В., Монахов Д.Н., Монахова Г.А. Проблемы безопасности информационного общества современной России: Монография.-М.: Экон-Информ, 2014.-215 с.
19. Ращектаева И.С.: «Работа педагога по формированию цифровой кибербезопасности младшего школьника»-с. 112-115. Современная наука и образование: актуальные вопросы теории и практики: сборник статей II Международной научно-практической конференции. – Пенза: МЦНС «Наука и Просвещение». – 2023. – 176 с.
20. Родионов А.Е., Иванов А.М.: Историко-правовые взгляды на международные проблемы взаимоотношений государств и наций С. 312. В книге Война и мир: уроки истории, вызовы времени. Международная научно-практическая конференция / Авторы-составители: Е.А. Ульяненкова, А.М. Иванов, канд. ист. наук / Под общей ред. Е.А. Ивановой, канд. ист. наук. — Смоленск, 2022.— 440 с., 65 ил.
21. Рябцева Т.Т., Холиков И.В. Правовое регулирование информационной безопасности в современных условиях // Военное право. 2024. № 3(85). С. 17-28.
22. Современное международное право: вызовы, угрозы и тенденции / Государство и право XX1 века: современные тенденции и новые вызовы. Сборник материалов международной научно-практической конференции. Отв. ред. Т.А. Сошникова. М. Изд-во Московского гуманитарного университета. 2020.-346 с.
23. Тункин, Г.И. Теория международного права / Г. И. Тункин. – М., 1970. – 511 с.
24. Уголовно-правовые гарантии суверенитета государства (сравнительно-правовое исследование): Научно-практическое пособие / В. Ю. Артемов, А. М. Белялова, Х. И. Гаджиев [и др.]. Москва: Издательство Проспект, 2022. 352 с.
25. Холиков И.В. Гибридная война как многовекторная угроза национальной безопасности России в условиях кризиса системы мирового правопорядка // Право в Вооруженных Силах – Военно-правовое обозрение. 2022. № 11(304). С. 30–38.
26. Холиков И.В., Милованович А., Наумов П.Ю.: Динамика функционирования

международного права в условиях трансформации современного миропорядка: постнеклассический подход // Журнал российского права. 2022. Т. 26. № 11. С. 132—148.
27. Холиков И.В., Сазонова К.Л. Проблемные вопросы реализации международной ответственности международных организаций за нарушения норм международного гуманитарного права // Право в Вооруженных Силах – Военно-правовое обозрение. 2022. № 4(297). С. 102–111.
28. Холиков И. В. Актуальные вопросы правового обеспечения сил и средств обороны и безопасности России в условиях современных вызовов и угроз // Право в Вооруженных Силах-Военно-правовое обозрение. 2021. № 12(293). С. 116-120.
29. Холиков И. В. Теоретико-правовая характеристика современных глобальных вызовов и угроз в сфере здравоохранения // Актуальные проблемы государства и права. 2022. Т. 6, № 4(24). С. 547-555. DOI 10.20310/2587-9340-2022-6-4-547-555.
30. Киберпреступления в банковской сфере (Батюкова В.Е.) («Банковское право», 2021, № 2) – С.57-63.
31. Лукашук И.И.: Международное право. Общая часть: учеб. для студентов юрид. фак. и вузов; Изд-во 3-е, перераб. и доп. / И.И. Лукашук.-М.: Волтерс Клувер, 2005.-432 с.
32. Мартенс Ф.Ф. Современное международное право цивилизованных народов. В 2 т. / Ф.Ф. Мартенс; под ред. В. А. Томсинова.-М.: Зерцало, 2008.-Т. 1. – 251 с.
33. Международное право: учебник / Б.М. Ашавский, М.М. Бирюков, В.Д. Бордунов и др.; отв. ред. С.А. Егоров. 5-е изд., перераб. и доп. М.: Статут, 2014.
34. Цыбаков Д.Л. Развертывание политико-информационных коммуникаций НАТО и Евросоюза в прибалтийском регионе // ГосРег: государственное регулирование общественных отношений. 2021. № 3. С. 212 – 219.
35. Шинкарецкая, Г. Г. Проблема выработки определения кибератаки / Г. Г. Шинкарецкая // Международное право. – 2023. – № 2. – С. 10-21. – DOI 10.25136/2644-5514.2023.2.40051. – EDN NYDJJZ.
36. Электронное голосование в России и за рубежом (Худолей Д.М., Худолей К.М.) («Вестник Пермского университета. Юридические науки», 2022, № 3) – С. 476-503.
37. Юсупов М.Ю. Фишинг как угроза конфиденциальности в сети / М.Ю. Юсупов, А.О. Путилов // E-Scio. 2021. № 10 (61). С. 223-232.
38. Alonso C., Romero E. Aggressors and victims in bullying and cyberbullying: a study of personality profiles using the five-factor model // The Spanish Journal of Psychology. 2017. Vol. 20. e76. P.1-14.
39. Badinter R. L'universalité des droits de l'homme dans un monde pluraliste // Revue universelle des droits de l'homme. 1989. Т. 1. P. 204
40. Carr, J., Mechanisms for collective action to prevent and combat online child sexual exploitation and abuse, Council of Europe, 2019. P. 1-36.
41. JACK GOLDSMITH & TIM WU, WHO CONTROLS THE Internet? ILLUSIONS OF A BORDERLESS WORLD (Oxford University Press, Inc., 2006). PP. 226.
42. Juvonen J., Gross E.F. Extending the school grounds?-Bullying experiences in cyberspace // Journal of school Health. 2008. Vol. 78 (9). P. 496 – 505;
43. Kholikov I. Ethical and Legal Basis for the Standards of Triage Used in the Russian Military Medical Service // Resource Scarcity in Austere Environments. An Ethical Examination of Triage and Medical Rules of Eligibility. Cham: Springer Nature Switzerland AG, 2023. P. 77-87. DOI 10.1007/978-3-031-29059-6_5.
44. Kyriacou C., Zuin A: Cyberbullying of teachers by students on YouTube: challenging the image of teacher authority in the digital age // Res. Pap. 2015. Educ. 1522 (October). P. 1-19.;
45. Kumar, C. (2024). Cybercrime and the Law: Challenges in Prosecuting Digital Offenses.

Indian Journal of Law, 2(5), P. 20-25.
46. Murphy C., Understanding cybercrime, EPRS, March 2024. P. 1-9.
47. Schmitt M. et al. (2017) Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press P. 184.
48. Shahidullah S., Coates C. and Kersha-Aerga D. (eds), Global Cybercrime and Cybersecurity Laws and Regulations: Issues and Challenges in the 21st Century, Nova Science Publishers Inc., 2022. P.362.
49. Svantesson, D. J. B. Solving the Cybercrime Jurisdiction Puzzle: International Jurisdiction Strategies for a Digitally Connected World. Oxford University Press, 2021.p. 254.
50. Teunissen, C. and Napie, S., Child sexual abuse material and end-to-end encryption on social media platforms: An overview, Australian Government, 2022. P. 1-19.
51. Trachtman J. (2013) Cyberspace and Cybersecurity. The Future of International Law: Global Government / J. Trachtman (ed.). Cambridge: Cambridge University Press. P. 88.
52. Tim Berners-Lee and Mark Fischetti, Harper: Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by Its Inventor. San Francisco, 1999 Publisher: Harper Business; 1st edition (November 7, 2000) PP. 246.
53. Vergne J., Duran R. (2014) Cyberespace et Organisations "Virtuelles": L' état Souverain a-t-Il Encore un Avenir? [Cyberspace and "Virtual" Organizations: Does the Sovereign State Still Have a Future?] // Regards Croisés sur L'Économie. Vol. 1. No. 14. P. 126–139.
54. Wiener G. European Digital Policy: Combating Online Harassment and Cyberbullying // European Journal of Law, 2022). P. 12

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

Предмет исследования. В рецензируемой статье «Современное международно-правовое регулирование кибербуллинга в отношении защиты прав детей» исходя из ее названия предметом исследования должны быть нормы международного права, регулирующие общественные отношения в сфере защиты несовершеннолетних от буллинга в сети Интернет.
Методология исследования. Методологический аппарат составили следующие диалектические приемы и способы научного познания: анализ, абстрагирование, индукция, дедукция, гипотеза, аналогия, синтез, типология, классификация, систематизация и обобщение. Отмечается применение современных научных методов (таких как, формально-логический; историко-правовой; сравнительно-правовой; статистический; социологический; метод анализа конкретных правовых ситуаций и др.).
Актуальность исследования. Актуальность темы рецензируемой статьи не вызывает сомнения. Можно согласиться с автором, что «информационно-телекоммуникационная сеть «Интернет», стала неотъемлемой частью мировой экономики, коммуникации и права... Развитие интернета привело к появлению новых правовых вызовов: защиты персональных данных, кибербезопасности и международного регулирования цифровой среды...». Автор правильно отмечает, что «ввиду актуальности проблемы противодействия кибербуллингу в контексте защиты прав детей, представляется возможным исследовать международно-правовые регуляторы, направленных на предупреждение и пресечение кибербуллинга, и рассмотреть эффективность применимых мер международным сообществом». Данные обстоятельства обуславливают необходимость доктринальных разработок по данной проблематике в целях совершенствования правового регулирования в сфере защиты несовершеннолетних от

буллинга в сети Интернет.
Научная новизна. Не подвергая сомнению важность проведенных ранее научных исследований, послуживших теоретической базой для данной работы, тем не менее, можно отметить, что в этой статье не сформулированы положения, отличающиеся научной новизной. Статья изобилует ссылками на источники, но отсутствует собственная аргументированная позиция автора по заявленной проблематике.
Стиль, структура, содержание. Нельзя сказать, что тема статьи раскрыта, не все содержание статьи соответствует ее названию. Отдельные фрагменты статьи выходят за рамки заявленной тематики, и на взгляд рецензента, нуждаются в корректировке (например, «... также невозможно исключить влияние «Сети» как основного средства достижения целей гибридной войны...») Материал изложен не всегда последовательно и ясно. Автор смешивает понятия «буллинг в сети Интернет в отношении несовершеннолетних» и «гибридные (информационные) войны». Если по мнению автора эти понятия связаны, то следует это аргументировать. Соблюдены автором требования по объему материала. Статья написана научным стилем, использована специальная юридическая терминология. Встречаются опечатки «современноq». Предпринята автором попытка структурировать статью. Заключение (как обязательная часть научной статьи) должна содержать итоги исследования, собственные выводы автора. Ссылки на других ученых в заключении неуместны.
Библиография. Автором использовано достаточное количество доктринальных источников. Ссылки на источники оформлены с соблюдением требований библиографического ГОСТа. Вместе с тем, представляется, что список библиографии следует актуализировать, а именно исключить те источники, которые автор не использовал в своей работе.
Апелляция к оппонентам. По спорным вопросам заявленной тематики представлена научная дискуссия, обращения к оппонентам корректные, заимствования оформлены ссылками на автора и источник опубликования.
Выводы, интерес читательской аудитории. Статья «Современное международно-правовое регулирование кибербуллинга в отношении защиты прав детей» не может быть рекомендована к опубликованию. Статья нуждается в тщательной доработке. Хотя статья соответствует тематике журнала «Международное право» и написана на актуальную тему, но не отличается научной новизной. Данная статья могла бы представлять интерес для широкой читательской аудитории, прежде всего, специалистов в области международного права, информационного права, ювенального права, а также, была бы полезна для преподавателей и обучающихся юридических вузов и факультетов.

Результаты процедуры повторного рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

Предметом исследования в представленной на рецензирование статье является, как это следует из ее наименования, современное международно-правовое регулирование кибербуллинга в отношении защиты прав детей. Заявленные границы исследования соблюдены ученым.
Методология исследования раскрыта: "Для проведения исследования и комплексного раскрытия его предмета в статье применены системный и комплексный подходы, сравнительно-правовой и доктринальный принципы исследования, а также актуальные разработки в области современной защиты прав детей от кибербуллинга".
Актуальность избранной автором темы исследования несомненна и обосновывается им

следующим образом: "Информационно-телекоммуникационная сеть «Интернет», стала неотъемлемой частью мировой экономики, коммуникации и права [5, 6, 22, 40]. Развитие интернета привело к появлению новых правовых вызовов: защиты персональных данных, кибербезопасности и международного регулирования цифровой среды [41], а также невозможно исключить влияние интернета как основного средства достижения целей гибридной войны [25, с. 6]. Интернет перешел из статуса исследовательского проекта в глобальное коммерческое и общественное явление, ввиду того обстоятельства, что в 1989 году Тим Бернерс-Ли предложил концепцию Всемирной паутины (World Wide Web), которая включала гипертекстовые документы, доступные через браузеры [52]. Указанная технология сделала «Сеть» доступным для массового использования, что привело к ее стремительному росту в современном ее виде. Следует отметить, что угрозы информационной безопасности являются неотъемлемым аспектом развития и использования информационных технологий [18, с. 129]. Отсутствие в международном праве точных правовых норм, регламентирующих противодействие кибератакам, усугубляется вместе с тем и отсутствием единого определения понятию «кибератака» [18, 39]" и др.; "Для обозначения травли в образовательных организациях используют термин «буллинг». ... В указанной связи, нужно отметить, что кибербуллинг является отдельным видом сетевой (онлайн) агрессии, которая отличается от природы интернет-атак [5, с. 1-2; 6], и как современное правовое явление определение «жертвы кибербуллинга» у многих авторов отсутствует [5, с. 1]. В отечественной и зарубежной литературе традиционно ограничиваются толкованием «киберзапугивания», не разъясняя понятие пострадавших от него лиц [4; 13; 46]"; "Р. Бадинтера есть формулировка: «Права человека не даны нам в откровение, у них есть своя история» («Les droits de l’homme ne nous ont pas été révélés, mais ont une histoire») [39, с. 1], что отражает длительное становление таких прав, а в условиях стремительного развития цифровых технологий и расширения виртуального пространства кибербуллинг становится глобальной проблемой, затрагивающей права человека в целом, и права детей, включая право на защиту от насилия, психического и физического здоровья, неприкосновенность частной жизни в условиях новой угрозы". Дополнительно ученому необходимо перечислить фамилии ведущих специалистов, занимавшихся исследованием поднимаемых в статье проблем, а также раскрыть степень их изученности.

Научная новизна работы проявляется в некоторых заключениях автора, к примеру: "Современное международное право демонстрирует на настоящий момент недостаточную степень регламентации указанных вопросов, поскольку отсутствие унифицированного понятия кибербуллинга, пробелы в определении трансграничной юрисдикции и недостаточная разработка механизмов привлечения к ответственности создают правовую неопределенность. Указанные факторы усложняют предотвращение и расследование преступлений, связанных с кибербуллингом и его использованием в рамках гибридных войн. С учетом вышеизложенного, в числе приоритетных направлений совершенствования международно-правового регулирования кибербуллинга, остается необходимость развития унифицированного понятия, на основании опыта региональных международных организаций с целью обеспечения единообразного применения норм в различных юрисдикциях. И кроме того, рассмотреть разработку концепции «цифрового нейтралитета», принципа, запрещающего использование киберпространства для ведения информационных атак и манипуляции в сторону детей, используя методы гибридной войны, с обязательством государств принимать меры по предотвращению таких действий для защиты детей. Указанные меры должны быть основаны на основополагающих принципах международного права, включая принцип суверенного равенства государств, ненападения, мирного разрешения споров и сотрудничества между государствами. Особое внимание должно быть уделено необходимости

выполнения обязательств, вытекающих из Устава ООН. Принятие таких мер укрепит международный правопорядок и обеспечит стабильность в условиях цифровых вызовов современности", однако в целом статья носит реферативный характер, представляя собой компиляцию ряда использованных при ее написании источников. Таким образом, исследование нуждается в доработке, о чем более подробно будет сказано ниже.

Научный стиль исследования выдержан автором в полной мере.

Структура работы логична. Во вводной части статьи ученый обосновывает актуальность избранной им темы исследования. В основной части работы автор исследует эффективность существующих международных договоров, конвенций и деклараций в сфере противодействия кибербуллингу и защиты детей от насилия в сети «Интернет». В заключительной части работы содержатся выводы по результатам проведенного исследования.

Содержание статьи соответствует ее наименованию, но не лишено недостатков.

Так, автор пишет: "Информационно-телекоммуникационная сеть «Интернет», стала неотъемлемой частью мировой экономики, коммуникации и права [5, 6, 22, 40]" - первая запятая является лишней.

Ученый отмечает: "Указанная технология сделала «Сеть» доступным для массового использования, что привело к ее стремительному росту в современном ее виде" - "доступной".

Автор указывает: "По мнению Г. Г. Шинкарецкой в отраженных определениях не проводится различия между киберпреступностью, кибератакой и кибервойной, поэтому они могут применяться повсеместно и широко [35]" - "По мнению Г. Г. Шинкарецкой, в отраженных определениях не проводится различия между киберпреступностью, кибератакой и кибервойной, поэтому они могут применяться повсеместно и широко [35]".

Таким образом, статья нуждается в дополнительном вычитывании - в ней встречаются множественные опечатки, орфографические, пунктуационные и стилистические ошибки (приведенный в рецензии перечень опечаток и ошибок не является исчерпывающим!).

Автору следует избегать сплошного цитирования. Его необходимо разбавлять критическими замечаниями, высказыванием своей позиции по спорному вопросу и т.п.

Ученый не предлагает оригинальной дефиниции понятия "кибербуллинг", не разрабатывает концепций определения трансграничной юрисдикции и механизмов привлечения правонарушителей к юридической ответственности.

Библиография исследования представлена 54 источниками (монографиями, научными статьями, учебниками), в том числе на английском языке. С формальной точки зрения этого достаточно, однако работа не отличается высокой степенью самостоятельности.

Апелляция к оппонентам имеется, но носит общий характер. В научную дискуссию с конкретными учеными автор не вступает, ссылаясь на ряд теоретических источников исключительно в обоснование своих суждений либо для иллюстрирования отдельных положений работы.

Выводы по результатам проведенного исследования имеются ("Кибербуллинг, направленный на несовершеннолетних, представляет собой не только отдельное противоправное деяние, но и элемент информационного воздействия, применяемого в рамках гибридных войн. Сходство методов и целей данных явлений, таких как дезинформация, манипуляция общественным сознанием и психологическое давление, подтверждает необходимость их комплексного анализа в условиях вооруженных конфликтов. Современное международное право демонстрирует на настоящий момент недостаточную степень регламентации указанных вопросов, поскольку отсутствие унифицированного понятия кибербуллинга, пробелы в определении трансграничной юрисдикции и недостаточная разработка механизмов привлечения к ответственности создают правовую неопределенность. Указанные факторы усложняют предотвращение и

расследование преступлений, связанных с кибербуллингом и его использованием в рамках гибридных войн. С учетом вышеизложенного, в числе приоритетных направлений совершенствования международно-правового регулирования кибербуллинга, остается необходимость развития унифицированного понятия, на основании опыта региональных международных организаций с целью обеспечения единообразного применения норм в различных юрисдикциях. И кроме того, рассмотреть разработку концепции «цифрового нейтралитета», принципа, запрещающего использование киберпространства для ведения информационных атак и манипуляции в сторону детей, используя методы гибридной войны, с обязательством государств принимать меры по предотвращению таких действий для защиты детей. Указанные меры должны быть основаны на основополагающих принципах международного права, включая принцип суверенного равенства государств, ненападения, мирного разрешения споров и сотрудничества между государствами. Особое внимание должно быть уделено необходимости выполнения обязательств, вытекающих из Устава ООН. Принятие таких мер укрепит международный правопорядок и обеспечит стабильность в условиях цифровых вызовов современности"), обладают свойствами достоверности, обоснованности и, несомненно, заслуживают внимания научного сообщества.

Интерес читательской аудитории к представленной на рецензирование статье может быть проявлен прежде всего со стороны специалистов в сфере международного права при условии ее доработки: дополнительном обосновании актуальности избранной автором темы исследования (в рамках сделанного замечания), введении дополнительных элементов научной новизны и дискуссионности, уточнении и углублении отдельных положений работы, устранении многочисленных нарушений в оформлении статьи.

Результаты процедуры окончательного рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.

Со списком рецензентов издательства можно ознакомиться здесь.

РЕЦЕНЗИЯ

на статью на тему «Современное международно-правовое регулирование кибербуллинга в отношении защиты прав детей».

Предмет исследования.

Предложенная на рецензирование статья посвящена актуальным вопросам международно-правового регулирования кибербуллинга. Как указано в статье, «Объектом исследования является международно-правовая база, регулирующая кибербуллинг и защиту прав ребенка. Предметом исследования выступают нормы международного права, регулирующие общественные отношения в сфере защиты несовершеннолетних от буллинга в сети Интернет». Автором выявляются проблемы на международно-правовом уровне в рассматриваемой сфере, делаются выводы по поводу того, как можно минимизировать данные проблемы, как можно найти решение в заявленных сферах.

Методология исследования.

Цель исследования прямо в статье заявлена: «Цель исследования — критически оценить эффективность существующих международных договоров, конвенций и деклараций в противодействии кибербуллингу и защите детей от насилия в сети Интернет». Исходя из поставленных цели и задач, автором выбрана методологическая основа исследования. В самой статье отмечается, что «Для проведения исследования и комплексного

раскрытия его предмета в статье применены системный и комплексный подходы, сравнительно-правовой и доктринальный принципы исследования».

В частности, автором используется совокупность общенаучных методов познания: анализ, синтез, аналогия, дедукция, индукция, другие. В частности, методы анализа и синтеза позволили обобщить и разделить выводы различных научных подходов к предложенной тематике, а также сделать конкретные выводы из материалов практики.

Наибольшую роль сыграли специально-юридические методы. В частности, автором активно применялся формально-юридический метод, который позволил провести анализ и осуществить толкование положений международно-правовых актов. Например, следующий вывод автора: «На рост кибертравли в обществе, в частности в отношении детей в Интернете и цифровом пространстве, обратили недавно внимание и в ООН. П. 16 «Резолюции ООН № 74/133» от 2019 г. «решительно осуждает все формы насилия в отношении детей, совершаемого при любых обстоятельствах, включая физическое, психологическое и сексуальное насилие, (…) сексуальную эксплуатацию детей в Интернете и вне его, травлю, включая кибертравлю, и настоятельно призывает государства к тому, чтобы они активизировали усилия для предотвращения всех форм такого насилия и защиты детей от него посредством применения всеобъемлющего, учитывающего гендерные аспекты и возраст подхода, выработали инклюзивный, многофункциональный и систематизированный комплекс мер для эффективного реагирования на насилие в отношении детей и для обеспечения безопасных и учитывающих интересы детей механизмов консультирования, рассмотрения жалоб и представления сообщений и гарантий прав пострадавших детей и интегрировали этот комплекс мер в национальные процессы планирования»»»

Таким образом, выбранная автором методология в полной мере адекватна цели исследования, позволяет изучить все аспекты темы в ее совокупности.

Актуальность.

Актуальность заявленной проблематики не вызывает сомнений. Имеется как теоретический, так и практический аспекты значимости предложенной темы. С точки зрения теории международно-правовое регулирование кибербуллинга сложна и неоднозначна. От решения задачи противодействия кибербуллингу зависит вопрос нравственного здоровья детей. При этом ввиду наднационального характера интернета решение задачи лишь на внутригосударственном уровне не может явиться перспективным. Сложно спорить с автором в том, что «Информационно-телекоммуникационная сеть Интернет стала неотъемлемой частью мировой экономики, коммуникации и права [5, 6, 22, 40]. Развитие Интернета привело к появлению новых правовых вызовов – защиты персональных данных, кибербезопасности и международного регулирования цифровой среды [41], а также невозможно исключить влияние Интернета как основного средства достижения целей гибридной войны [25, с. 6]. Интернет перешел из статуса исследовательского проекта в глобальное коммерческое и общественное явление, поскольку в 1989 году Тим Бернерс-Ли предложил концепцию Всемирной паутины (World Wide Web), которая включала гипертекстовые документы, доступные через браузеры [52]. Указанная технология сделала Сеть доступной для массового использования, что привело к ее стремительному росту в современном виде. Следует отметить, что угрозы информационной безопасности являются неотъемлемым аспектом развития и использования информационных технологий [18, с. 129]. Отсутствие в международном праве точных правовых норм, регламентирующих противодействие кибератакам, усугубляется, вместе с тем, и отсутствием единого определения понятию «кибератака» [18, 39]».

Тем самым, научные изыскания в предложенной области стоит только поприветствовать.

Научная новизна.

Научная новизна предложенной статьи не вызывает сомнений. Во-первых, она выражается в конкретных выводах автора. Среди них, например, такой вывод:
«Кибербуллинг, направленный на несовершеннолетних, представляет собой не только отдельное противоправное деяние, но и элемент информационного воздействия, применяемого в рамках гибридных войн. Сходство методов и целей данных явлений – таких, как дезинформация, манипуляция общественным сознанием и психологическое давление, подтверждает необходимость их комплексного анализа в условиях вооруженных конфликтов. Современное международное право демонстрирует на настоящий момент недостаточную степень регламентации указанных вопросов, поскольку отсутствие унифицированного понятия кибербуллинга, пробелы в определении трансграничной юрисдикции и недостаточная разработка механизмов привлечения к ответственности создают правовую неопределенность. Указанные факторы усложняют предотвращение и расследование преступлений, связанных с кибербуллингом и его использованием в рамках гибридных войн».
Указанный и иные теоретические выводы могут быть использованы в дальнейших научных исследованиях.
Во-вторых, автором предложены идеи по совершенствованию норм международного права, что может быть полезным для специалистов в данной сфере и для правотворческой деятельности.
Таким образом, материалы статьи могут иметь определенных интерес для научного сообщества с точки зрения развития вклада в развитие науки.
Стиль, структура, содержание.
Тематика статьи соответствует специализации журнала «Международное право», так как она посвящена правовым проблемам, связанным с международно-правовым регулированием кибербуллинга.
Содержание статьи в полной мере соответствует названию, так как автор рассмотрел заявленные проблемы, в целом достиг поставленной цели исследования.
Качество представления исследования и его результатов следует признать в полной мере положительным. Из текста статьи прямо следуют предмет, задачи, методология и основные результаты исследования.
Оформление работы в целом соответствует требованиям, предъявляемым к подобного рода работам. Существенных нарушений данных требований не обнаружено.
Библиография.
Следует высоко оценить качество использованной литературы. Автором активно использована литература, представленная авторами из России и из-за рубежа (Василевская Л.Ю., Иванов А.А., Харитонова Ю.С., Калятин В.О., Гаврилов С.О., Глебов И.Н., Чукин С.Г., Vergne J., Duran R. и другие). Многие из цитируемых ученых являются признанными учеными в области регулирования отдельных отношений в цифровой среде.
Таким образом, труды приведенных авторов соответствуют теме исследования, обладают признаком достаточности, способствуют раскрытию различных аспектов темы.

Апелляция к оппонентам.
Автор провел серьезный анализ текущего состояния исследуемой проблемы. Все цитаты ученых сопровождаются авторскими комментариями. То есть автор показывает разные точки зрения на проблему и пытается аргументировать более правильную по его мнению.

Выводы, интерес читательской аудитории.
Выводы в полной мере являются логичными, так как они получены с использованием

общепризнанной методологии. Статья может быть интересна читательской аудитории в плане наличия в ней систематизированных позиций автора применительно к вопросам совершенствования международно-правового регулирования кибербуллинга.

На основании изложенного, суммируя все положительные и отрицательные стороны статьи
«Рекомендую опубликовать»