Журнал международного права и международных отношений. 2023. № 2 (105). С. 10—16.
Journal of International Law and International Relations. 2023. N 2 (105). P. 10—16.
УДК 341+172.4 DOI: 10.33581/2072-0513-2023-2-10-16

МОРАЛЬНО-ПОЛИТИЧЕСКИЕ ОБЯЗАТЕЛЬСТВА ГОСУДАРСТВ В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Наталия Мороз

В настоящее время вопросы обеспечения информационной безопасности приобрели особую актуальность. При этом ориентиры должного поведения государств в киберпространстве задаются нормами международной морали. В статье рассматриваются морально-политические обязательства государств, вытекающие как из правовых, так и из норм рекомендательного характера. Указывается, что доклады Групп правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, а также доклад Группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности представляют собой своеобразный Кодекс ответственного поведения государств в киберпространстве. Автор приходит к выводу, что морально-политические обязательства государств в сфере обеспечения информационной безопасности следует рассматривать в узком и широком значении. Морально-политические обязательства государств в сфере поддержания информационной безопасности охватывают довольно широкий спектр международных отношений, ряд из которых не может регулироваться исключительно нормами международной морали и требует принятия необходимого международно-правового регулирования.

Ключевые слова: информационная безопасность; кибербезопасность; морально-политические обязательства; ответственное поведение государств в киберпространстве.

«Moral and Political Obligations of States in the Field of Ensuring Information Security» (Nataliya Maroz)

The issues of ensuring information security are relevant as ever. At the same time, the rules for appropriate state behaviour in cyberspace are regulated by the norms of international morality. The article addresses moral and political obligations of states arising from both legal and recommendatory norms. The article indicates that the reports of the Groups of Governmental Experts on Advances in the Sphere of Informatisation and Telecommunications in the Context of International Security, as well as the report of the Open-Ended Group on Advances in the Sphere of Informatisation and Telecommunications in the Context of International Security, constitute a peculiar kind of Code of Responsible Behaviour of States in Cyberspace. The author comes to the conclusion that the moral and political obligations of states in the field of information security should be considered in a narrow and broad sense. The moral and political obligations of states in the field of maintaining information security cover a fairly wide range of international relations, some of which cannot be regulated solely by the norms of international morality and require the adoption of the necessary international legal regulation.

Keywords: cybersecurity; information security; moral and political obligations; responsible behaviour of states in cyberspace.

Вопросы обеспечения информационной безопасности как никогда актуальны в настоящее время. Так, за последние три года существенно увеличилось количество инцидентов, связанных с оказанием неправомерного воздействия на функционирование информационно-телекоммуникационных систем и сетей. В 2020 г. число кибератак с использованием вредоносных программ возросло на 358 % по сравнению с 2019 г., в 2021 г. — на 125 % [42] и в 2022 г. — на 38 % [52]. При этом ущерб от таких кибератак стал рассматриваться как угроза не только национальной, но и международной безопасности [23]. Несмотря на тот факт, что международное сотрудничество в области обеспечения информационной безопас-

Автор:
Мороз Наталия Олеговна — кандидат юридических наук, доцент кафедры государственного управления юридического факультета Белорусского государственного университета, *e-mail: nataliya.maroz@gmail.com*
Белорусский государственный университет. Адрес: 4, пр. Независимости, Минск, 220030, БЕЛАРУСЬ

Author:
Maroz Nataliya — Candidate of Law, Associate Professor of the Department of State Management of the Faculty of Law, Belarusian State University, *e-mail: nataliya.maroz@gmail.com*
Belarusian State University. Address: 4, Nezavisimosti ave., Minsk, 220030, BELARUS

ности имеет значительную специфику, международно-правовое регулирование указанной сферы международных отношений на универсальном уровне по-прежнему осуществляется на основе международных договоров общего характера (Устава ООН 1945 г. [37], Международного пакта о гражданских и политических правах 1966 г. [21], Женевских конвенций о защите жертв войны 1949 г. [11—14] и Дополнительных протоколов 1977 г. к ним [8; 9] и др.). При этом ориентиры должного поведения государств в киберпространстве задаются нормами международной морали [23, с. 138—140].

Республика Беларусь выступает за разработку правил ответственного поведения в виртуальном пространстве в целях уменьшения конфронтации и восстановления доверия, активно принимает участие в Группе правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (далее — ГПЭ) [2], Рабочей группе открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (далее — РГОС) [18], а также в рамках своего членства в Организации Договора о коллективной безопасности и Содружестве Независимых Государств (далее — СНГ). Необходимость достижения целей обеспечения международной информационной безопасности в контексте поддержки и продвижения соответствующих инициатив, отвечающих национальным интересам Республики Беларусь в информационной сфере, подчеркивалась в Концепции информационной безопасности Республики Беларусь 2019 г. [26]. Указанное выше предопределяет значение данной статьи.

Правила ответственного поведения государств в киберпространстве, разработанные ГПЭ и РГОС, вносят весомый вклад в формирование нормативной основы для обеспечения международной информационной безопасности, поскольку не только определяют, как существующее международное право применимо к отношениям государств по вопросам безопасности в сфере использования информационно-коммуникационных технологий (далее — ИКТ), но и содержат рекомендации по укреплению доверия, а также наращиванию потенциала государств в области обеспечения безопасности в сфере использования ИКТ [47, p. 347—350]. Таким образом, положения, содержащиеся в докладах ГПЭ и РГОС, ориентированы на предупреждение международных споров, а также ситуаций, в том числе угрожающих международному миру и безопасности.

Более того, такие нормы «мягкого права» в дальнейшем способны стать основой кодификации норм международного права в рассматриваемой области, что подчеркивает важность и своевременность выявления специфики морально-политических обязательств в сфере обеспечения информационной безопасности. В частности, рекомендации, содержащиеся в резолюциях Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» и докладах ГПЭ и РГОС, были положены в основу Обновленной концепции Конвенции ООН об обеспечении международной информационной безопасности, подготовленной Российской Федерацией при участии Республики Беларусь, Корейской Народно-Демократической Республики, Республики Никарагуа и Сирийской Арабской Республики, представленной на имя Генерального секретаря ООН 15 мая 2023 г. [25].

Таким образом, целью данной статьи является определение особенностей морально-политических обязательств государств в сфере обеспечения информационной безопасности.

Следует отметить, что источники и содержание морально-политических обязательств государств в области обеспечения информационной безопасности, хотя частично исследовались в доктрине, но все же не стали самостоятельным предметом комплексного научного изучения. В научных работах, как правило, указанные обязательства рассматривались в комплексе с юридическими [1; 17; 24] либо с учетом выявления роли конкретной международной организации или конференции в сфере обеспечения информационной безопасности [4; 10; 29], либо в контексте оценки необходимости разработки международно-правовых норм для регулирования конкретных вопросов [43].

В доктрине международного права сложилось мнение, что источником морально-политических обязательств государств являются нормы «мягкого права» [35, с. 157—158]. В сфере обеспечения информационной безопасности основными из них являются доклады ГПЭ (A/65/201, 2009/2010; A/68/98, 2012/2013; A/70/174, 2014/2015; A/76/135, 2021), а также доклад РГОС (A/AC.290/2021/CRP.2, 2021), представляющие собой своеобразный Кодекс ответственного поведения государств в киберпространстве [43, p. 53—55]. Кроме того, указанные аспекты в той или иной степени регламентируются рядом актов Генеральной Ассамблеи ООН (резолюции 55/45, 57/239, 58/199, 62/17, 63/37, 64/25, 65/41, 66/24, 67/27, 68/243, 69/28, 70/237, 71/28, 73/266, 74/29, 74/247, 75/240, 76/19 и др. [31]), а также актами органов региональных международных организаций (решение Совета глав правительств СНГ о Стратегии обеспечения информационной безопасности государств — участников СНГ от 25 октября 2019 г. [28], Стратегия кибербезопасности Европейского союза от 16 декабря 2020 г., принятая совместным коммюнике Европейской комиссии и Верховного представителя ЕС по внешней политике и по-

литике безопасности [51], Стратегия АСЕАН по сотрудничеству в области кибербезопасности на 2021—2025 г. [41], решение Совета Министров ОБСЕ № 5/16 «Усилия ОБСЕ по сокращению рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий» [36] и др.).

В то же время не вполне корректно сводить все формы выражения морально-политических обязательств исключительно к источникам мягкого права.

Полагаем, что ряд международных договоров, применимых к регулированию международных отношений по поводу использования ИКТ, являются одновременно источниками как юридических, так и морально-политических обязательств в области обеспечения информационной безопасности. Тот факт, что международное право закрепляет в своих положениях последовательную систему гуманистических моральных норм и ценностей, в настоящее время в доктрине не оспаривается [38, с. 187]. Как справедливо отмечает российский ученый М. В. Шугуров, «в результате несоблюдение международного права со стороны его субъекта одновременно может рассматриваться как безнравственный акт» [38, с. 188]. В Декларации по случаю пятидесятой годовщины ООН, принятой резолюцией 50/6 Генеральной Ассамблеи от 24 октября 1995 г., указывается, что «Устав является выражением общих ценностей и чаяний человечества» [3]. Как отмечал российский ученый-правовед И. И. Лукашук, основные принципы международного права, закрепленные в Уставе ООН, обладают «высшим политическим, моральным и юридическим авторитетом» [16, с. 296]. Основные принципы международного права в полной мере применимы и к правоотношениям в сфере обеспечения информационной безопасности [40].

По мнению американского исследователя М. Дж. Перри, права человека, закрепленные в международных договорах, являются не только юридическими, но и моральными правами [49, p. 435]. Таким образом, международные договоры по правам человека в этом плане содержат одновременно и юридические, и моральные обязательства. В контексте обеспечения информационной безопасности они охватывают запрет пропаганды войны, а также выступлений в пользу национальной, расовой или религиозной ненависти, представляющих собой подстрекательство к дискриминации, вражде или насилию (ст. 20 Международного пакта о гражданских и политических правах 1966 г. [21]), запрет прямого публичного подстрекательства к совершению геноцида (п. *c* ст. III Конвенции о предупреждении преступления геноцида и наказании за него 1948 г. [15]), всякое распространение идей, основанных на расовом превосходстве или ненависти, подстрекательство к расовой дискриминации и актам насилия, направленным против любой расы или группы лиц другого цвета кожи или этнического происхождения, организованную и всякую другую пропагандистскую деятельность, которая поощряет расовую дискриминацию и подстрекают к ней (пп. *a*, *b* ст. 4 Международной конвенции о ликвидации всех форм расовой дискриминации 1965 г. [19]), подстрекательство к апартеиду (п. *a* ст. III Международной конвенции о пресечении преступления апартеида и наказании за него 1973 г. [20]), подстрекательство к совершению актов терроризма [30] и др.

Особого внимания заслуживают моральные ценности, воплощенные в нормах Женевских конвенций о защите жертв войны 1949 г. и Дополнительных протоколов к ним 1977 г. [46, с. 350]. Юридические запреты совершения определенных действий в ходе вооруженных конфликтов имеют и серьезные моральные основания (например, умышленные нападения на гражданское население, гражданские объекты, объекты, необходимые для выживания гражданского населения, установки и сооружения, содержащие опасные силы, и др.). Нормы международного гуманитарного права такого рода применимы и к деяниям, совершаемым с использованием ИКТ [50, p. 422, 434, 529].

Кроме того, полагаем, что региональные договоры по вопросам информационной безопасности также содержат важные ценностные установки в области регулирования сотрудничества государств в рассматриваемой сфере, характерные для конкретного региона, и воплощают морально-политические ориентиры государств-участников (преамбулы Соглашения о сотрудничестве государств — участников СНГ в области обеспечения информационной безопасности от 20 ноября 2013 г. (далее — Соглашение СНГ) — признание важного значения информационной безопасности для реализации основных прав и свобод человека и гражданина [27], Соглашения о сотрудничестве государств — членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности от 30 ноября 2017 г. (далее — Соглашение ОДКБ) — неприемлемость деструктивного информационного воздействия с использованием информационной инфраструктуры, использование информационных технологий для вмешательства во внутренние дела, провоцирование угроз информационной безопасности, признание, что доверие и безопасность в использовании ИКТ относятся к фундаментальным основам информационного общества, основанность культуры информационной безопасности на уважении прав и свобод человека, приоритете сохранения политической, социальной и экономической стабильности, необходимость соблюдения баланса между основными правами и свободами

человека и эффективным противодействием угрозам информационной безопасности и др. [33], Соглашения между правительствами государств — членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 г. (далее — Соглашение ШОС) — признание важной роли информационной безопасности в обеспечении прав и основных свобод человека и гражданина, указание на необходимость углубления доверия и развитие взаимодействия сторон в вопросах обеспечения международной информационной безопасности [32], Конвенции Африканского союза о кибербезопасности и защите персональных данных от 27 июня 2014 г. — необходимость мобилизации усилий всех государственных и частных субъектов для продвижения кибербезопасности, указание на необходимость обеспечения баланса между защитой персональных данных и обеспечением безопасности ИКТ [39] и др.).

Таким образом, источники морально-политических обязательств государств в сфере поддержания информационной безопасности можно рассматривать в узком и широком смысле. В широком смысле такие источники включают также источники права, в которых воплощены определенные моральные нормы. К ним, прежде всего, относится Устав ООН, иные международные договоры, применимые для регулирования обеспечения информационной безопасности, резолюции Совета Безопасности ООН, а также источники «мягкого права». В узком смысле источниками морально-политических обязательств государств в сфере поддержания информационной безопасности выступают исключительно документы, содержащие правила ответственного поведения государств в сфере поддержания информационной безопасности, которые нельзя отнести к источникам международного права. При этом основным источником морально-политических обязательств государств в рассматриваемой сфере является так называемый Кодекс ответственного поведения государств в киберпространстве.

Морально-политические обязательства, сформулированные в докладах ГПЭ и РГОС, изложены достаточно аффирмативно («государства не должны осуществлять или заведомо поддерживать...» [5, п. 13 *k)*; 6, с. 20], «государства должны принимать надлежащие меры для защиты...» [5, п. 13 *k)*; 6, с. 16], «все государства должны принимать участие в деятельности по повышению безопасности киберпространства» [5, с. 5], «государства не должны осуществлять или сознательно поддерживать деятельность в области ИКТ, противоречащую их обязательствам по международному праву...» [48, para. 31]), что отличает их от положений, сформулированных как рекомендации («Группа рекомендует государствам рассмотреть следующие добровольные меры укрепления доверия» [5, п. 16], «рекомендовать... принятие мер по укреплению доверия...» [7, п. 18 *ii*)]). Полагаем, что положения докладов ГПЭ и РГОС, не сформулированные аффирмативно, т. е. по сути являющиеся положениями-рекомендациями, не создают морально-политических обязательств для государств в области обеспечения информационной безопасности, поскольку «устанавливают желательную, целесообразную модель поведения, но не обязывают следовать ей» [16, с. 152].

Учитывая характер формулировок морально-политических обязательств в сфере обеспечения информационной безопасности («государства не должны осуществлять...», «государства должны принимать надлежащие меры»), можно также прийти к выводу, что морально-политические обязательства в сфере обеспечения информационной безопасности разделяются на позитивные и негативные.

По своему содержанию морально-политические обязательства государств в сфере обеспечения информационной безопасности, содержащиеся в источниках «мягкого права», шире установленных в международных договорах [5]. Как уже было указано выше, на универсальном уровне вопросы обеспечения информационной безопасности не стали предметом специального международно-правового регулирования и регламентированы фрагментарно в международных договорах общего характера. Региональные соглашения в сфере информационной безопасности в основном ориентированы на организацию взаимодействия и сотрудничества государств-участников по определенным в них основным направлениям (например, ст. 3 Соглашения СНГ [27], ст. 3 Соглашения ШОС [32]), взаимодействия сторон в интересах обеспечения информационной безопасности (ст. 1 Соглашения ОДКБ [33]). Иными словами, данные международные соглашения практически не закрепляют конкретные негативные обязательства в сфере использования ИКТ в отношении как друг друга, так и третьих государств, а также позитивные обязательства такого рода в отношении третьих государств. Единственным региональным международным соглашением, указывающим на запрет совершения определенных действий с использованием ИКТ в отношении других государств — участников данного соглашения, является Соглашение ШОС. При этом перечень таких действий довольно узок. Так, в данном международном договоре указывается лишь на защиту информационных ресурсов и критически важных структур своего государства от недопустимого неправомерного использования и несанкционированного вмешательства, в том числе от информационных атак, а также оказание содействие другим сторонам в реализации указанных действий (п. 3 ст. 4) [32].

В то же время, например, в докладах ГПЭ и РГОС как негативные, так и позитивные обязательства в отношении третьих государств регламентируются. В частности, они включают недопустимость заведомого использования территории государств для совершения международно-противоправных деяний с использованием ИКТ [5, п. 13 *c*)]; недопустимость нанесения ущерба информационным системам групп экстренной готовности к компьютерным инцидентам других государств или же использования таких групп для участия в злонамеренной международной деятельности [5, п. 13 *k*)]; удовлетворение просьб об оказании помощи, поступающих от других государств, критически важная инфраструктура которых становится объектом злонамеренных действий в сфере ИКТ [5, п. 13 *h*)]; принятие разумных мер для обеспечения неприкосновенности каналов поставок и предупреждения распространения злонамеренных программных средств в сфере ИКТ, технических средств или пагубных скрытых функций [5, п. 13 *i*)]; обеспечение трансформации цифрового разрыва в цифровые возможности через принятие мер в области наращивания потенциала [48, para. 58] и др.

Таким образом, можно заключить, что морально-политические обязательства государств в сфере поддержания информационной безопасности носят как негативный (воздерживаться от совершения действий, которые могут квалифицироваться как угроза или нарушение международного мира и безопасности), так и позитивный характер (принимать комплекс мер, направленных на предупреждение, недопущение ухудшения ситуации, а также пресечение угрозы и (или) нарушения международного мира и безопасности, совершаемых с использованием ИКТ, восстановление положения, существовавшего до нарушения, и недопущение повторения подобной ситуации в будущем; оказывать помощь государству, пострадавшему от злонамеренной деятельности в сфере ИКТ; сотрудничать в разработке и осуществлении мер по укреплению стабильности и безопасности в использовании ИКТ, в том числе в контексте права на развитие).

В то же время ряд международных отношений не может регулироваться исключительно нормами международной морали и требует принятия правовых норм. К вопросам, требующим специального международно-правового регулирования, в доктрине ранее относили международное сотрудничество государств в борьбе с киберпреступностью [45]. Вместе с тем с учетом содержания ряда резолюций Совета Безопасности ООН, из которых следует, что ИКТ могут использоваться в террористических целях, создавать угрозу международному миру и безопасности (резолюции 2395 и 2396 от 21 декабря 2017 г., 2462 от 28 марта 2019 г., 2535 от 14 июля 2020 г. и др. [31]), полагаем, что указанные аспекты требуют также адекватного регулирования комплексного характера. Кроме того, учитывая разрушительный характер результата, который может быть достигнут в случае кибератак на критически важную инфраструктуру государств или иной злонамеренной деятельности с использованием ИКТ против таких объектов [44], правила сотрудничества государств по пресечению, а также иным аспектам преодоления негативных последствий подобного рода деяний требуют именно правовой регламентации. Необходимо также определение минимального перечня объектов, в отношении которых такие правила будут применимы, поскольку отнесение той или иной инфраструктуры к категории «важнейшей» входит в исключительную компетенцию государств [34], что фактически приводит к отсутствию единого подхода к установлению перечня критически важных инфраструктур и неопределенности списка объектов, которые не могут подвергаться кибератакам в мирное время.

На основании изложенного можно сделать следующие выводы.

1. Установлено, что источники морально-политических обязательств государств в сфере поддержания информационной безопасности можно рассматривать в узком и широком смысле. В широком смысле такие источники включают, прежде всего, Устав ООН, международные договоры, посвященные вопросам регулирования обеспечения информационной безопасности, а также источники «мягкого права», применимые к рассматриваемой области. В узком смысле источниками морально-политических обязательств государств в сфере поддержания информационной безопасности выступают исключительно документы, содержащие правила ответственного поведения государств в сфере поддержания информационной безопасности, которые нельзя отнести к источникам международного права. К основным из них относятся резолюции Генеральной Ассамблеи ООН, доклады ГПЭ и РГОС.

2. Выявлено, что морально-политические обязательства государств в сфере поддержания информационной безопасности носят как негативный (воздерживаться от совершения действий, которые могут квалифицироваться как угроза или нарушение международного мира и безопасности), так и позитивный характер (принимать комплекс мер, направленных на предупреждение, недопущение ухудшения ситуации, пресечение угрозы и (или) нарушения международного мира и безопасности, совершаемых с использованием ИКТ, а также восстановление положения, существовавшего до нарушения, и недопущение повторения подобной ситуации в будущем, оказывать помощь государству, пострадавшему от злонамеренной деятельности в сфере ИКТ, сотрудничать в разработке и осуществлении мер по укреплению стабильности и безопасности в использовании ИКТ, в том числе в контексте права на разви-

тие). Таким образом, сфера позитивных морально-политических обязательств государств в сфере поддержания информационной безопасности шире, чем сфера юридических обязательств в данной области.

3. Установлено, что морально-политические обязательства государств в сфере поддержания информационной безопасности охватывают довольно широкий спектр международных отношений, ряд из которых не может регулироваться исключительно нормами международной морали и требует принятия необходимого международно-правового регулирования. К вопросам, требующим специального международно-правового регулирования, относятся: а) международное сотрудничество в борьбе с террористическим или иным преступным использованием информационно-коммуникационных технологий; б) правила взаимодействия государств в случае, если критически важная инфраструктура одного из них становится объектом злонамеренных действий в сфере ИКТ.

Список использованных источников

1. Арчаков, В. Ю. О теоретико-методологических подходах к обеспечению международной информационной безопасности / В. Ю. Арчаков // Журн. междунар. права и междунар. отношений. — 2019. — № 3-4 (90-91). — С. 3—11.
2. Бойко, С. Группа правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности: взгляд из прошлого в будущее / С. Бойко [Электронный ресурс] // Фонд НОРАВАНК. — 19.12.2016. — Режим доступа: <http://www.noravank.am/rus/articles/security/detail.php?ELEMENT_ID=15284>. — Дата доступа: 10.03.2023.
3. Декларация по случаю пятидесятой годовщины Организации Объединенных Наций: док. ООН A/RES/50/6 [Электронный ресурс] // Система официальной документации ООН. — Режим доступа: <https://undocs.org/ru/A/RES/50/6>. — Дата доступа: 20.06.2023.
4. Довгань, Е. Ф. ОДКБ и информационная безопасность / Е. Ф. Довгань, Н. О. Мороз // Организация Договора о коллективной безопасности и планирование на случай чрезвычайных обстоятельств после 2014 г. / Е. Ф. Довгань [и др.]; под ред. Е. Ф. Довгань, А. В. Русаковича. — Женева; Минск, 2015. — С. 207—236.
5. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности: док. ООН A/70/174 [Электронный ресурс] // Система официальной документации ООН. — Режим доступа: <https://undocs.org/ru/A/70/174>. — Дата доступа: 12.11.2022.
6. Доклад Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности: док. ООН A/76/135 [Электронный ресурс] // Система официальной документации ООН. — Режим доступа: <https://undocs.org/ru/A/76/135>. — Дата доступа: 12.11.2022.
7. Доклад правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности: док. ООН A/65/201 [Электронный ресурс] // Система официальной документации ООН. — Режим доступа: <https://undocs.org/ru/A/65/201>. — Дата доступа: 12.11.2022.
8. Дополнительный протокол к Женевским конвенциям от 12 августа 1949 года, касающийся защиты жертв международных вооруженных конфликтов (Протокол I). Женева, 8 июня 1977 г. [Электронный ресурс] // Международный комитет Красного Креста. — Режим доступа: <https://www.icrc.org/ru/doc/resources/documents/misc/treaties-additional-protocol-1.htm>. — Дата доступа: 09.06.2023.
9. Дополнительный протокол к Женевским конвенциям от 12 августа 1949 года, касающийся защиты жертв немеждународных вооруженных конфликтов (Протокол II). Женева, 8 июня 1977 г. [Электронный ресурс] // Международный комитет Красного Креста. — Режим доступа: <https://www.icrc.org/ru/doc/resources/documents/misc/6lkb3l.htm>. — Дата доступа: 09.06.2023.
10. Ефремов, А. А. Развитие регулирования информационной или «цифровой» безопасности в документах международных организаций / А. А. Ефремов // Междунар. право и междунар. организации. — 2017. — № 1. — С. 48—55. (https://doi.org/10.7256/2226-6305.2017.1.20710)
11. Конвенция (I) об улучшении участи раненых и больных в действующих армиях. Женева, 12 авг. 1949 г. [Электронный ресурс] // Международный комитет Красного Креста. — Режим доступа: <https://www.icrc.org/ru/doc/resources/documents/misc/geneva-conventon-1.htm>. — Дата доступа: 09.06.2023.
12. Конвенция (II) об улучшении участи раненых, больных и лиц, потерпевших кораблекрушение, из состава вооруженных сил на море. Женева, 12 авг. 1949 г. [Электронный ресурс] // Международный комитет Красного Креста. — Режим доступа: <https://www.icrc.org/ru/doc/resources/documents/misc/geneva-conventon-2.htm>. — Дата доступа: 09.06.2023.
13. Конвенция (III) об обращении с военнопленными. Женева, 12 авг. 1949 г. [Электронный ресурс] // Международный комитет Красного Креста. — Режим доступа: <https://www.icrc.org/ru/doc/resources/documents/misc/geneva-conventon-3.htm>. — Дата доступа: 09.06.2023.
14. Конвенция (IV) о защите гражданского населения во время войны. Женева, 12 авг. 1949 г. [Электронный ресурс] // Международный комитет Красного Креста. — Режим доступа: <https://www.icrc.org/ru/doc/resources/documents/misc/geneva-convention-4.htm>. — Дата доступа: 09.06.2023.
15. Конвенция о предупреждении преступления геноцида и наказании за него: [принята резолюцией 260 (III) Генеральной Ассамблеи ООН от 9 дек. 1948 г.] [Электронный ресурс] // Организация Объединенных Наций. — Режим доступа: <https://www.un.org/ru/documents/decl_conv/conventions/genocide.shtml>. — Дата доступа: 12.06.2023.
16. Лукашук, И. И. Международное право. Общая часть: учеб. для студентов юрид. фак. и вузов. Изд. 3-е, перераб. и доп. / И. И. Лукашук; Рос. акад. наук, Ин-т государства и права, Акад. правовой ун-т. — М.: Волтерс Клувер, 2008. — 432 с.
17. Макаров, О. С. Актуальные аспекты обеспечения информационной безопасности государств — участников СНГ / О. С. Макаров. — Минск: Ин-т нац. безопасности Респ. Беларусь, 2013. — 270 с.
18. Международная информационная безопасность [Электронный ресурс] // Министерство иностранных дел Республики Беларусь. — Режим доступа: <https://mfa.gov.by/mulateral/global_issues/inform/>. — Дата доступа: 10.03.2023.
19. Международная конвенция о ликвидации всех форм расовой дискриминации: [принята резолюцией 2106 (XX) Генеральной Ассамблеи от 21 дек. 1965 г.] [Электронный ресурс] // Организация Объединенных Наций. — Режим доступа: <https://www.un.org/ru/documents/decl_conv/conventions/raceconv.shtml>. — Дата доступа: 22.05.2023.
20. Международная конвенция о пресечении преступления апартеида и наказании за него: [принята резолюцией 3068 (XXVIII) Генеральной Ассамблеи ООН от 30 нояб. 1973 г.] [Электронный ресурс] // Организация Объединенных Наций. — Режим доступа: <https://www.un.org/ru/documents/decl_conv/conventions/apartheid1973.shtml>. — Дата доступа: 23.06.2023.
21. Международный пакт о гражданских и политических правах: [принят резолюцией 2200 A (XXI) Генеральной Ассамблеи от 16 сент. 1966 г.] [Электронный ресурс] // Организация Объединенных Наций. — Режим доступа: <https://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml>. — Дата доступа: 23.06.2023.
22. Мороз, Н. О. Информационный суверенитет Республики Беларусь в контексте современного международного права / Н. О. Мороз // Право.by. — 2022. — № 2 (76). — С. 111—116.
23. Мороз, Н. О. Международно-правовое регулирование поддержания информационной безопасности / Н. О. Мороз // Там же. — № 6 (80). — С. 138—144.

24. Мороз, Н. О. Международно-правовые основы обеспечения международной информационной безопасности / Н. О. Мороз // Труд. Профсоюзы. Общество. — 2016. — № 1 (51). — С. 77—81.
25. Обновленная концепция Конвенции Организации Объединенных Наций об обеспечении международной информационной безопасности: приложение к письму постоянных представителей Беларуси, Корейской Народно-Демократической Республики, Никарагуа, Российской Федерации и Сирийской Арабской Республики при Организации Объединенных Наций от 15 мая 2023 г. на имя Генерального секретаря: док. ООН A/77/894 [Электронный ресурс] // Система официальной документации ООН. — Режим доступа: <https://undocs.org/ru/A/77/894>. — Дата доступа: 26.05.2023.
26. О Концепции информационной безопасности Республики Беларусь: постановление Совета Безопасности Респ. Беларусь от 18 марта 2019 г. № 1 [Электронный ресурс] // Национальный правовой Интернет-портал Республики Беларусь. — Режим доступа: <https://pravo.by/document/?guid=12551&p0=P219s0001&p1=1>. — Дата доступа: 12.06.2023.
27. О ратификации Соглашения о сотрудничестве государств — участников Содружества Независимых Государств в области обеспечения информационной безопасности: Закон Респ. Беларусь от 14 июля 2014 г. № 179-З [Электронный ресурс] // Национальный правовой Интернет-портал Республики Беларусь. — Режим доступа: <https://pravo.by/document/?guid=12551&p0=H11400179&p1=1&p5=0>. — Дата доступа: 12.06.2023.
28. О Стратегии обеспечения информационной безопасности государств — участников СНГ: решение Совета глав правительств СНГ от 25 окт. 2019 г. [Электронный ресурс] // Исполнительный комитет Содружества Независимых Государств. — Режим доступа: <http://www.cis.minsk.by/reestrv2/doc/6162#text>. — Дата доступа: 15.06.2023.
29. Полякова, Т. А. Проблемы формирования системы международной информационной безопасности в условиях трансформации права и новых вызовов и угроз / Т. А. Полякова, Г. Г. Шинкарецкая // Право и государство: теория и практика. — 2020. — № 10 (190). — С. 138—142.
30. Резолюция 1624 (2005), принятая Советом Безопасности на его 5261-м заседании 14 сентября 2005 года: док. ООН S/RES/1624(2005) [Электронный ресурс] // Система официальной документации ООН. — Режим доступа: <https://undocs.org/ru/S/RES/1624(2005)>. — Дата доступа: 26.05.2023.
31. Система официальной документации ООН [Электронный ресурс]. — Режим доступа: <https://documents.un.org/>. — Дата доступа: 22.06.2023.
32. Соглашение между правительствами государств — членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности: [закл. в г. Екатеринбурге 16 июня 2009 г.] [Электронный ресурс] // Президентская библиотека им. Б. Н. Ельцина. — Режим доступа: <https://www.prlib.ru/item/1283353>. — Дата доступа: 20.06.2023.
33. Соглашение о сотрудничестве государств — членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности: [закл. в г. Минске 30 нояб. 2017 г.] [Электронный ресурс] // Национальный правовой Интернет-портал Республики Беларусь. — Режим доступа: <https://pravo.by/document/?guid=12551&p0=E01700001>. — Дата доступа: 20.06.2023.
34. Создание глобальной культуры кибербезопасности и защита важнейших информационных инфраструктур: резолюция Генеральной Ассамблеи ООН: док. A/RES/58/199 [Электронный ресурс] // Система официальной документации ООН. — Режим доступа: <https://undocs.org/ru/A/RES/58/199>. — Дата доступа: 12.11.2022.
35. Толстых, В. Л. Курс международного права: учеб. / В. Л. Толстых. — М.: Проспект, 2018. — 736 с.
36. Усилия ОБСЕ по сокращению рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий: док. ОБСЕ MC.DEC/5/16/Corr.1 [Электронный ресурс] // Организация по безопасности и сотрудничеству в Европе. — Режим доступа: <https://www.osce.org/files/f/documents/8/9/290396.pdf>. — Дата доступа: 17.06.2023.
37. Устав Организации Объединенных Наций от 26 июня 1945 г. // Антология мировой политической мысли. В 5 т. Т. 5: Политические документы / ред.-науч. совет: Г. Ю. Семигин (пред.) [и др.]. — М.: Мысль, 1997. — С. 343—392.
38. Шугуров, М. В. Динамика соотношения международного права и международной морали: теоретический и методологический аспекты / М. В. Шугуров // Рос. журн. правовых исследований. — 2017. — Т. 4, № 1. — С. 183—191. (https://doi.org/10.17816/RJLS18254)
39. African Union convention on cyber security and personal data protection: [adopted 27th June 2014] [Electronic resource] // African Union. — Mode of access: <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>. — Date of access: 12.06.2023.
40. Applicability of international law [Electronic resource] // The Cyber Law Toolkit. — Mode of access: <https://cyberlaw.ccdcoe.org/wiki/Applicability_of_international_law>. — Date of access: 22.06.2023.
41. ASEAN Cybersecurity Cooperation Strategy (2021—2025) [Electronic resource] // ASEAN. — Mode of access: <https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf>. — Date of access: 25.06.2023.
42. De Pasquale, F. Terrifying Cyber Security Statistics from 2022 / F. De Pasquale [Electronic resource] // TekSpace. — 20.01.2023. — Mode of access: <https://www.tekspace.com.au/blog/cyber-security-stats-2022/>. — Date of access: 10.03.2023.
43. Heinl, C. Cyber Dynamics and World Order: Enhancing International Cyber Stability / C. Heinl // Irish Studies in International Affairs. — 2018. — Vol. 29. — P. 53—72. (https://doi.org/10.3318/isia.2018.29.18)
44. Kerner, M. S. Colonial Pipeline hack explained: Everything you need to know / M. S. Kerner [Electronic resource] // TechTarget. — 26.04.2022. — Mode of access: <https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know>. — Date of access: 24.06.2023.
45. Maroz, N. A Critical Analysis of the Need for a Stronger International Legal Framework for Cyber Ethics in Times of Pandemic / N. Maroz // Revista Etică şi Deontologie. — 2021. — Vol. 1, N 1. — P. 60—73. (https://doi.org/10.52744/RED.2021.01.08)
46. Meron, T. The Geneva Conventions as Customary Law / T. Meron // The American Journal of International Law. — 1987. — Vol. 81, N 2. — P. 348—370. (https://doi.org/10.2307/2202407)
47. Meyer, P. Norms of Responsible State Behaviour in Cyberspace / P. Meyer // The Ethics of Cybersecurity: the International Library of Ethics, Law and Technology (ELTE. Vol. 21) / ed. by M. Christen, B. Gorjin, M. Loi. — Springer, 2020. — P. 347—360.
48. Open-ended working group on developments in the field of information and telecommunications in the context of international security: final Substantive Report: UN Doc. A/AC.290/2021/CRP.2 [Electronic resource] // Digital Watch. — Mode of access: <https://dig.watch/wp-content/uploads/2022/08/OEWG-Report.pdf>. — Date of access: 17.06.2023.
49. Perry, M. J. The Morality of Human Rights / M. J. Perry // Human Rights Quarterly. — 2020. — Vol. 42, N 2. — P. 434—478. (https://doi.org/10.1353/hrq.2020.0023)
50. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / ed. M. N. Schmitt. — Cambridge: Cambridge University Press, 2017. — 598 p.
51. The EU's Cybersecurity Strategy for the Digital Decade: Joint Communication to the European Parliament and the Council, 16 Dec. 2020, JOIN(2020) 18 final [Electronic resource] // European Commission. — Mode of access: <https://ec.europa.eu/newsroom/dae/redirection/document/72164>. — Date of access: 23.06.2023.
52. The Latest 2023 Cyber Crime Statistics (updated March 2023) [Electronic resource] // AAG. — Mode of access: <https://aag-it.com/the-latest-cyber-crime-statistics/>. — Date of access: 10.03.2023.

Статья поступила в редакцию в марте 2023 г., доработана в июне 2023 г.

Исследование выполнено в рамках ГПНИ № ГР 20212197