ГОСУДАРСТВО И ПРАВО, 2023, № 12, с. 139–149
STATE AND LAW, 2023, No. 12, pp. 139–149

ИНФОРМАЦИОННОЕ ПРАВО И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ



МЕЖДУНАРОДНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: УНИВЕРСАЛЬНОЕ ПРАВОВОЕ ИЗМЕРЕНИЕ

© 2023 г. Т. А. Полякова[1, *], Е. С. Зиновьева[2, **], А. А. Смирнов[1, 3, *]**

[1]Институт государства и права Российской академии наук, г. Москва
[2]Московский государственный институт международных отношений (университет) МИД России
[3]Всероссийский научно-исследовательский институт МВД России, г. Москва

**E-mail: polyakova_ta@mail.ru*
***E-mail: elena.zinovjeva@gmail.com*
****E-mail: smirnovsng@yandex.ru*

Поступила в редакцию 01.08.2023 г.

Аннотация. Статья посвящена вопросам развития системы правового обеспечения международной информационной безопасности. Проведено научное осмысление понятия международной информационной безопасности и основных угроз в данной сфере. Проанализированы стратегические задачи и основные направления государственной политики Российской Федерации в области международной информационной безопасности. Исследованы текущее состояние системы правового обеспечения международной информационной безопасности и основные проблемы в данной области. Проведен системный анализ различных подходов относительно вопросов применимости норм и принципов действующего международного права к ИКТ-среде, разработки и принятия новых правил, принципов и норм, касающихся обеспечения безопасности в ИКТ-среде.
Проведенное авторами исследование позволило с междисциплинарных позиций научно обосновать выводы относительно приоритетных векторов развития системы правового обеспечения международной информационной безопасности на универсальном, региональном и двустороннем уровнях в условиях геополитической конфронтации ведущих мировых держав.

Ключевые слова: международная информационная безопасность, информационно-коммуникационные технологии, информационные угрозы, международное право, правовое обеспечение, нормы ответственного поведения государств в ИКТ-среде, информационный суверенитет.

Цитирование: *Полякова Т.А., Зиновьева Е.С., Смирнов А.А.* Международная информационная безопасность: универсальное правовое измерение // Государство и право. 2023. № 12. С. 139–149.

Статья подготовлена в рамках выполнения Государственного задания № FMUZ-2021-0042 «Правовое регулирование цифровой экономики, искусственного интеллекта, информационной безопасности».

DOI: 10.31857/S102694520029294-4

INTERNATIONAL INFORMATION SECURITY: UNIVERSAL LEGAL DIMENSION

© 2023 T. A. Polyakova[1, *], E. S. Zinovieva[2, **], A. A. Smirnov[1, 3, *]**

[1]Institute of State and Law of the Russian Academy of Sciences, Moscow
[2]MGIMO University
[3]National Research Institute of the Ministry of Interior of the Russian Federation, Moscow

** E-mail: polyakova_ta@mail.ru*
*** E-mail: elena.zinovjeva@gmail.com*
**** E-mail: smirnovsng@yandex.ru*

Received 01.08.2023

Abstract. The article is devoted to the development of the system of legal support of international information security. A scientific understanding of the concept of international information security and the main threats in this area has been carried out. The strategic objectives and main directions of the state policy of the Russian Federation in the field of international information security are analyzed. The current state of the system of legal support of international information security and the main problems in this area are investigated. A systematic analysis of various approaches of states regarding the applicability of the norms and principles of current International Law to the ICT environment, the development and adoption of new rules, principles and norms related to security in the ICT environment. Of particular interest from the standpoint of International and national Law is the problem of voluntary and non-binding norms of responsible behavior of states in the ICT environment. The research conducted by the authors made it possible to scientifically substantiate conclusions from interdisciplinary positions regarding the priority vectors of the development of the system of legal support for international information security at the universal, regional and bilateral levels in the conditions of geopolitical confrontation of the leading world powers.

Key words: international information security, information and communication technologies, information threats, International Law, legal support, norms of responsible behavior of states in the ICT environment, information sovereignty.

For citation: *Polyakova, T.A., Zinovieva, E.S., Smirnov, A.A. (2023).* International information security: universal legal dimension // Gosudarstvo i pravo=State and Law, No. 12, pp. 139–149.

The article was prepared within the framework of the State assignment No. FMUZ-2021-0042 “Legal regulation of the digital economy, artificial intelligence, information security”.

Введение

В условиях бурного развития процессов цифровизации возрастают новые информационные вызовы, риски и угрозы, многие из которых носят трансграничный глобальный характер. Вызовы «цифровой революции» обусловливают и вызовы международному и национальному праву, что подтверждает необходимость проведения фундаментальных исследований правового обеспечения информационной безопасности и системной модернизации правового регулирования отношений в данной сфере[1].

Существенное влияние на динамику роста информационных угроз оказывает усиливающаяся геополитическая конфронтация ведущих государств. США и иные страны Запада, следуя логике глобального доминирования, все активнее применяют противоправные методы воздействия на информационную сферу. Особую тревогу вызывают подрывные информационные операции, направленные на вмешательство во внутренние дела государств, нарушение деятельности экономических институтов и работы объектов критической информационной инфраструктуры, разжигание социальной розни и вражды, продвижение чуждых ценностей. «Распространенной формой вмешательства во внутренние дела суверенных государств стало навязывание им деструктивных неолиберальных идеологических установок, противоречащих традиционным духовно-нравственным ценностям»[2].

Для поддержания устойчивости международных отношений очевидную опасность представляют попытки использования западными государствами своего технологического доминирования для сдерживания цифрового развития иных государств, усиления их технологической зависимости, а также для осуществления политически мотивированной цензуры в глобальном информационном пространстве. В этих условиях особое значение приобретает обеспечение цифрового и технологического суверенитета Российской Федерации[3].

[1] См.: Модели правового регулирования обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе / под общ. ред. Т.А. Поляковой. Саратов, 2020. С. 36.

[2] Концепция внешней политики России (утв. Указом Президента РФ от 31.03.2023 № 229) // СЗ РФ. 2023. № 14, ст. 2406.

[3] См.: *Капустин А.Я.* Суверенитет государства в киберпространстве: международно-правовое измерение // Журнал зарубежного законодательства и сравнительного правоведения. 2022. Т. 18. № 6. С. 99–108; *Виноградова Е.В., Полякова Т.А.* О месте информационного суверенитета в информационно-правовом пространстве современной России // Правовое государство: теория и практика. 2021. № 1 (63). С. 32–49; *Полякова Т.А., Минбалеев А.В., Кроткова Н.В.* Развитие науки

Цифровые технологии активно используются террористическими и экстремистскими организациями для пропаганды своих радикальных идей, вербовки новых участников, виртуального подстрекательства к совершению терактов и иных насильственных преступлений, координации действий своих сторонников, сбора финансовых средств, а также совершения кибератак на объекты критической информационной инфраструктуры[4]. Экстремисты активно применяют технологии дезинформации, включая распространение ложных предупреждений о готовящихся террористических актах[5].

ИКТ-среда прочно утвердилась в качестве области противоправной деятельности преступных элементов. Опасность возрастающей угрозы, исходящей от преступлений в сфере информационных технологий, подчеркивается в базовых документах стратегического планирования в области национальной безопасности Российской Федерации, включая Стратегию национальной безопасности Российской Федерации[6], Доктрину информационной безопасности[7], Основы государственной политики Российской Федерации в области международной информационной безопасности[8]. Как свидетельствует анализ статистических данных, в России доля преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, в общей структуре преступности уже составляет более четверти (26.5%)[9].

Наиболее массовыми видами преступлений с использованием ИКТ в Российской Федерации являются мошенничества и кражи денежных средств со счетов граждан и организаций. Экономические потери от преступлений в сфере информационных технологий возрастают с каждым годом и исчисляются уже десятками миллиардов рублей[10]. Вместе с тем в мировом масштабе по экспертным оценкам доходы от киберпреступности уже превышают доходы наркоторговцев[11].

Перечисленные вызовы составляют т.н. триаду основных угроз международной информационной безопасности, включающей использование ИКТ в военно-политических, террористических и криминальных целях[12]. Однако следует признать, что спектр рисков новой цифровой среды постоянно расширяется, к ним следует отнести применение цифровых технологий в экстремистских целях для проведения компьютерных атак на информационные ресурсы государств, в том числе на критическую информационную инфраструктуру, и др.

В этих условиях для противодействия актуальным информационным вызовам требуется сплочение усилий мирового сообщества и организация эффективного международного сотрудничества в области международной информационной безопасности. Как отмечает Министр иностранных дел РФ С.В. Лавров, Российская Федерация выступает последовательным сторонником консолидации действий государств для эффективного решения данной проблемы[13]. Именно Россия почти четверть века назад стала инициатором вынесения на уровень Организации Объединенных Наций темы противодействия угрозам в информационном пространстве и является последовательным приверженцем такой позиции и продвижения прогрессивных инициатив в этой сфере, включая и правовые.

Проблемы формирования системы правового регулирования международной информационной безопасности имеют междисциплинарный характер и включают в себя «блок теоретико-методологических правовых вопросов применения норм, правил и принципов ответственного поведения государств, призванных способствовать обеспечению открытой, безопасной, стабильной, доступной и мирной информационно-коммуникационной среды»[14]. Таким образом, природа угроз международной информационной безопасности обусловливают необходимость нормативного регулирования данной области на основании норм международного публичного права.

Особую роль в системе правового обеспечения международной информационной безопасности играют нормы международного информационного права[15]. Российские исследователи пишут о формировании новой отрасли международного публичного права – международного информационного права[16]. Настоящая статья ставит своей

информационного права и правового обеспечения информационной безопасности: формирование научной школы информационного права (прошлое и будущее) // Государство и право. 2021. № 12. С. 97–108; *Бойко С.* Основы государственной политики Российской Федерации в области международной информационной безопасности: регулирование и механизмы реализации // Междунар. жизнь. 2018. № 11. С. 24–35.

[4] См.: *Сундиев И.Ю., Смирнов А.А.* Использование информационных сетей в экстремистской и террористической деятельности // Научный портал МВД России. 2014. № 1. С. 84–91; *Их же.* Медиаресурсы в экстремистской и террористической деятельности: функциональный анализ // Свободная мысль. 2014. № 4. С. 55–72; *Сундиев И.Ю., Смирнов А.А., Андрюхин Н.Г.* Бесструктурные и бесконтактные способы вовлечения молодежи в террористическую и экстремистскую деятельность // Научный портал МВД России. 2018. № 2. С. 52–60.

[5] См.: *Смирнов А.А.* Правовые и организационные аспекты противодействия распространения фейковой информации террористическими и экстремистскими организациями // Аграрное и земельное право. 2023. № 1. С. 40–43.

[6] Утв. Указом Президента РФ 02.07.2021 г. № 400 (см.: СЗ РФ. 2021. № 27, ст. 5351).

[7] Утв. Указом Президента РФ от 05.12.2016 г. № 646 (см.: СЗ РФ. 2016. № 50, ст. 707).

[8] См.: Указ Президента РФ от 12.04.2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» // СЗ РФ. 2021. № 16, ст. 2746.

[9] См.: Состояние преступности в России за январь–декабрь 2022 года. ГИАЦ МВД России, 2023.

[10] Как отметил Министр внутренних дел РФ В.А. Колокольцев в ходе выступления на правительственном часе в Государственной Думе в октябре 2022 г., с начала года ущерб от преступлений в сфере IT увеличился на 20%, составив 65 млрд руб. (см.: Ущерб от IT-преступлений в России с начала года вырос на 20% // Коммерсантъ. 2022. 19 окт.).

[11] См.: Международная информационная безопасность: подходы России / рук. авт. кол. А.В. Крутских, Е.С. Зиновьева. М., 2021. С. 8.

[12] См.: *Зиновьева Е.С.* Международная информационная безопасность: проблемы многостороннего и двустороннего сотрудничества. М., 2021. С. 37.

[13] См.: Обращение к читателям Министра иностранных дел Российской Федерации С.В. Лаврова // Международная информационная безопасность: теория и практика: учеб. для вузов: в 3 т. / под общ. ред. А.В. Крутских. 2-е изд., доп. М., 2021. Т. 1. С. 13.

[14] *Полякова Т.А., Шинкарецкая Г.Г.* Проблемы формирования системы международной информационной безопасности в условиях трансформации права и новых вызовов и угроз // Право и государство: теория и практика. 2020. № 10 (290). С. 138.

[15] См.: *Полякова Т.А., Смирнов А.А.* Правовое обеспечение международной информационной безопасности: проблемы и перспективы // Росс. юрид. журнал. 2022. № 3. С. 8.

[16] См.: *Ясносокирский Ю.А.* Международное информационное право как регулятор международных отношений в сфере информационно-коммуникационных технологий // Междунар. жизнь. 2022. № 3. URL: https://interaffairs.ru/jauthor/material/2634

целью очертить основные нормы и принципы, лежащие в основе формирующейся отрасли международного публичного права – права информационной безопасности, а также охарактеризовать подход Российской Федерации к международно-правовой регламентации отношений, связанных с проблемами информационной безопасности.

Понятие международной информационной безопасности и стратегические задачи государственной политики Российской Федерации в данной области

В Основах государственной политики Российской Федерации в области международной информационной безопасности[17] (далее – Основы государственной политики в области МИБ) под международной информационной безопасностью понимается «такое состояние глобального информационного пространства, при котором на основе общепризнанных принципов и норм международного права и на условиях равноправного партнерства обеспечивается поддержание международного мира, безопасности и стабильности» (п. 6).

Как подчеркивают эксперты, «предложенный и продвигаемый Российской Федерацией термин МИБ подразумевает наличие не только технических, но и политико-идеологических угроз в данной области», что не коррелируется с западной концепцией кибербезопасности, акцентирующей внимание на технологическом измерении информационных угроз[18]. В Российской Федерации в основополагающих документах стратегического планирования в области национальной безопасности информационная безопасность рассматривается комплексно, как состояние защищенности от информационных угроз широкого спектра. Данные угрозы имеют как информационно-технические, так и информационно-психологические проявления.

Полагаем, что особенно четко данный подход зафиксирован в Стратегии национальной безопасности Российской Федерации 2021 года, где в содержание национальных интересов включена защита российского общества от деструктивного информационно-психологического воздействия[19].

Кроме того, российский подход подчеркивает существование военно-политического измерения угроз международной информационной безопасности, представляющего значительную опасность для международной стабильности. Однако США и ее союзники всячески сопротивлялись включению данного компонента в повестку обсуждения, не желая ограничивать свои возможности в развитии наступательных информационных потенциалов.

Представляется, что именно продвигаемое Российской Федерацией комплексное понимание международной информационной безопасности должно быть положено в основу архитектуры системы ее правового обеспечения на международном уровне в рамках складывающейся отрасли права – международного информационного права.

При этом Россия играет важную роль в развитии данного международно-правового направления. Основной целью российской государственной политики в области международной информационной безопасности является «содействие установлению международно-правового режима, при котором создаются условия для предотвращения (урегулирования) межгосударственных конфликтов в глобальном информационном пространстве, а также для формирования с учетом национальных интересов Российской Федерации системы обеспечения международной информационной безопасности» (п. 9 Основ государственной политики в области МИБ). Сходных позиций придерживается и Китайская Народная Республика. Так, согласно представленному в мае 2023 г. документу КНР[20] важнейшим элементом управления глобальным цифровым пространством является содействие развитию международного сотрудничества (как противовеса актуальной и широко обсуждаемой в западной научной литературе концепции «фрагментации интернета»[21]), необходимостью обеспечить защиту государственного суверенитета и уважения прав человека и основных свобод в интернете. Кроме того, отмечается значимость развития правовых основ регламентации деятельности крупных ИТ-компаний, а также регулирование новой и весьма перспективной области развития цифровых технологий искусственного интеллекта[22].

Таким образом, Российская Федерация и КНР, а также участники ШОС, БРИКС, ОДКБ и другие международные организации придерживаются схожей цели – формирования международно-правовых оснований обеспечения информационной безопасности. Для ее достижения необходимо развитие всестороннего международного сотрудничества на глобальном, региональном, многостороннем и двустороннем уровнях по вопросам формирования системы обеспечения международной информационной безопасности, безусловно, включая и правовые вопросы в целях противодействия основным угрозам международной информационной безопасности.

Исходя из анализа содержания п. 5 Основ государственной политики в области МИБ, можно выделить приоритетные задачи государственной политики Российской Федерации в рассматриваемой сфере, к числу которых относятся: 1) продвижение российских подходов к развитию системы обеспечения международной информационной безопасности на международной арене и российских инициатив в данной области; 2) содействие формированию международно-правовых механизмов предотвращения (урегулирования) конфликтов государств в глобальном информационном пространстве; 3) организация межведомственного взаимодействия при реализации государственной политики в области международной информационной безопасности.

В рамках реализации указанных задач в Основах государственной политики в области МИБ закреплены основные направления реализации государственной политики

---

[17] См.: Указ Президента Российской Федерации от 12 апреля 2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» // СЗ РФ. 2021. № 16, ст. 2746.

[18] См.: Международная информационная безопасность: подходы России / рук. авт. кол. А.В. Крутских, Е.С. Зиновьева. С. 6.

[19] См.: *Смирнов А.А.* Четвертый приоритет: правовое закрепление задач обеспечения информационной безопасности в новой Стратегии национальной безопасности Российской Федерации // Вестник Воронежского гос. ун-та. Сер.: Право. 2021. № 3 (46). С. 222–228.

[20] См.: China's Positions on Global Digital Governance (Contribution for the Global Digital Compact) // Ministry of Foreign Affairs of the Peoples' Republic of China. 25.05.2023. URL: https://www.fmprc.gov.cn/eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/202305/t20230525_11083607.html

[21] *Mueller M.* Will the internet fragment? Sovereignty, globalization and cyberspace. John Wiley & Sons, 2017.

[22] China's Positions on Global Digital Governance (Contribution for the Global Digital Compact) // Ministry of Foreign Affairs of the Peoples' Republic of China. 25.05.2023. URL: https://www.fmprc.gov.cn/eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/202305/t20230525_11083607.html

в данной сфере. Полагаем, что особую роль среди них играет развитие системы правового обеспечения международной информационной безопасности. В указанном документе стратегического планирования выделены такие ключевые направления развития, как: 1) содействие принятию странами – участницами ООН Конвенции об обеспечении международной информационной безопасности; 2) содействие выработке принципов и норм международного права, регламентирующих поведение государств в глобальном информационном пространстве; 3) заключение и реализация международно-правовых и иных договоренностей между Российской Федерацией и зарубежными государствами о сотрудничестве в сфере международной информационной безопасности.

Значимость заключения юридически обязывающего международного договора под эгидой ООН как основополагающего компонента режима в области информационной безопасности подчеркивается также в официальных документах, принятых по итогам саммитов БРИКС, ШОС и других международных организаций[23].

Ключевые проблемы и направления развития международного права в области международной информационной безопасности

Учитывая глобальный и трансграничный характер многих информационных угроз, нормы и принципы международного права играют, по сути, определяющую роль в обеспечении безопасности в ИКТ-среде. Хотя со стороны западных стран постоянно предпринимаются попытки подменить нормы международного права некими правилами, выработанными узкой группой государств и не выражающими интересы мирового сообщества. Россия неоднократно выступала с практическими разоруженческими и миротворческими инициативами. Фактически первый в истории международно-правовой документ, ограничивающий применение конкретных видов оружия, носит название Санкт-Петербургской декларации 1868 г., его принятие стало весомой заслугой российской дипломатии[24].

В период с 1998 г., когда по инициативе Российской Федерации Генеральной Ассамблеей ООН была принята первая резолюция «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности», международным сообществом, несмотря на противодействие целого ряда государств, проделана большая работа, направленная не только на осмысление ключевых информационных вызовов, стоящих перед государствами, но и выработку доктринальных подходов для противодействия им, обеспечения международной стабильности и безопасности. Важную роль в этом процессе в последующие годы сыграли институциональные механизмы группы правительственных экспертов ООН (далее – ГПЭ) и рабочей группы открытого состава (РГОС). Указанными группами была подготовлена серия экспертных докладов, аналитических материалов, содержащих и обосновывающих ключевые выводы и рекомендации по развитию международного сотрудничества по вопросам безопасности в области использования ИКТ, включая вопросы правового регулирования[25].

В фокусе внимания в целях развития системы правового обеспечения в международных экспертных дискуссиях находятся два исключительно важных вопроса: 1) о применимости норм и принципов действующего международного права к ИКТ-среде; 2) о разработке и принятии новых правил, принципов и норм, направленных на обеспечение безопасности в ИКТ-среде.

В отношении первого вопроса следует отметить, что доминирующей является позиция, включая и российских юристов, о применимости основополагающих принципов и норм международного права к ИКТ-среде. Так, в Докладе ГПЭ 2021 подтвержден вывод предыдущих групп правительственных экспертов о «применимости норм международного права, в частности положений Устава Организации Объединенных Наций, и их ключевого значения для поддержания мира и стабильности и для создания открытой, безопасной, стабильной, доступной и мирной информационно-коммуникационной среды». В связи с этим ГПЭ отметила, что соблюдение государствами международного права, в частности их обязательств по Уставу ООН, составляет «важнейшую основу действий государств при использовании ИКТ» (п. 69)[26].

Важно отметить, что в данном Докладе ГПЭ закреплена позиция о применимости положений о суверенитете государств и вытекающих из него международных норм и принципов к деятельности государств в ИКТ-среде и к их юрисдикции над инфраструктурой ИКТ, расположенной на их территории (п/п. “b” п. 71). При этом также в указанном Докладе подчеркнуто, что существующие обязательства государств по международному праву распространяются на их деятельность в ИКТ-среде (п/п. “b” п. 71).

Представляется, что особую остроту в условиях военной операции приобретает вопрос о применимости норм международного гуманитарного права к конфликтам в ИКТ-среде. Как известно, позиция западных экспертов по данному вопросу нашла отражение в одиозном Таллинском руководстве[27], которое предлагается его авторами рассматривать как свод из 95 правил, регламентирующих применимость международного гуманитарного права к киберконфликтам, а также содержит пространный комментарий по этим правилам. В 2015 г. было опубликовано «Таллинское руководство 2.0», содержащее расширенный перечень уже из 124 правил, регламентирующих применимость международного гуманитарного права к киберпространству.

В приведенном т.н. Таллинском руководстве обосновывается вывод о распространении действия норм международного гуманитарного права на конфликты в киберпространстве, включая и право на самооборону[28]. В связи с этим важно отметить, что, по мнению российских экспертов, Таллинское руководство следует рассматривать в качестве инструмента легитимации военного использования ИКТ[29]. При этом обращается внимание на то, что в кибер-

[23] См., напр.: Пекинская декларация БРИКС от 23.07.2022 г., Делийская декларация БРИКС от 09.09.2021 г. и др.

[24] См.: *Федоров А.В.* Информационная безопасность в мировом политическом процессе. М., 2006. С. 5.

[25] См.: Международная информационная безопасность: подходы России / рук. авт. кол. А.В. Крутских, Е.С. Зиновьева. С. 10–23.

[26] Доклад Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности от 14.07.2021 г. A/76/135.

[27] См.: *Schmitt, Michael N.* Tallinn Manual on the International Law Applicable to Cyber Warfare. New York, 2013.

[28] См.: *Гриняев С.* «Таллиннское руководство по применению юридических норм международного права к военным действиям в киберпространстве» в оценках западных экспертов // Обзор. НЦПТИ. 2013. № 3. С. 18–22.

[29] См.: Международная информационная безопасность: подходы России / рук. авт. кол. А.В. Крутских, Е.С. Зиновьева. С. 10–23.

пространстве весьма затруднительно провести атрибуцию источника кибератак. Кроме того, отмечается необходимость выработки критериев и порогового уровня киберинцидентов, которые бы позволяли идентифицировать их как применение силы, а также критериев пропорциональных мер самообороны.

Обращает внимание тот факт, что в 2021 г. Центром НАТО по сотрудничеству в сфере кибероборонны (CCDCOE) запущен новый проект «Таллинского руководства 3.0», рассчитанный сроком на пять лет. На наш взгляд, показательным является то обстоятельство, что к разработке и обсуждению данного проекта не были приглашены специалисты из Российской Федерации, КНР и государств – участников ШОС и БРИКС.

Исследования в области применения международного гуманитарного права свидетельствуют о том, что, несмотря на правомерность генерального вывода о распространении норм международного права на отношения в ИКТ-среде и применимости существующих обязательств государств по международному праву к их деятельности в данной среде, вопросы практического применения таких норм и обязательств к отдельным сферам и объектам ИКТ-среды требуют тщательной проработки и регламентации. Представляется, что это обусловлено спецификой ИКТ-среды, которая «не допускает простой экстраполяции уже существующих норм международного публичного права на информационное пространство»[30]. В этой связи заслуживает внимания вопрос о том, что международное право нуждается в существенной адаптации, в выработке новых международно-правовых норм, а также дополнении и уточнении уже существующих норм.

Поэтому вопросы применимости норм международного права к ИКТ-среде еще требуют обсуждения, на что прямо было обращено внимание в Докладе ГПЭ 2021: «Продолжение коллективного обсуждения и обмена мнениями между государствами в Организации Объединенных Наций о том, как конкретные нормы и принципы международного права применяются к использованию ИКТ государствами, имеет особое значение для углубления общего понимания во избежание недоразумений и повышения предсказуемости и стабильности» (п. 72).

Переходя ко второму вопросу, касающемуся развития международного права в рассматриваемой сфере, также отметим отсутствие единства позиций государств. Вместе с тем в общей части Доклада РГОС 2021[31] содержится общая рекомендация государствам «поддерживать дополнительные усилия по наращиванию потенциала в области международного права, национального законодательства и политики с тем, чтобы все государства могли способствовать достижению общего понимания того, как международное право применяется к использованию ИКТ государствами, и содействовать достижению консенсуса в международном сообществе» (п. 39).

Полагаем, что за размытостью такой формулировки кроются различия в подходах мировых держав, которые освещены в резюме Председателя РГОС (приложение II к Докладу РГОС 2021). По мнению одних государств, существующих норм международного права, дополненных добровольными и необязательными нормами и правилами поведения государств в ИКТ-среде (на них остановимся ниже), в настоящее время *вполне достаточно* для правовой регламентации рассматриваемой сферы. Поэтому сторонники такого подхода предлагают сосредоточить усилия на «операционализации» имеющихся нормативных рамок к информационной сфере[32].

Однако значительная часть государств не разделяет точку зрения о достаточности существующих норм международного права, дополненных добровольными и необязательными правилами ответственного поведения государств, и настаивает *на выработке согласованных на международном уровне и имеющих обязательную юридическую силу норм использования ИКТ*. Кроме того, Российская Федерация исходит из необходимости адаптации уже существующих норм международного права с учетом специфики ИКТ-технологий[33]. То есть современное международное публичное право, по сути, в полной мере применимо к регулированию правоотношений, возникающих в связи с развитием новых технологий, но по форме нуждается в дополнении и развитии.

Еще в 2011 г. в г. Екатеринбурге был представлен проект всеобъемлющего универсального международного соглашения в области международной информационной безопасности – *концепция Конвенции об обеспечении международной информационной безопасности*.

В мае 2023 г. Российская Федерация представила на рассмотрение ООН обновленный вариант проекта Конвенции об обеспечении международной информационной безопасности. В качестве соавторов по указанному проекту выступили Беларусь, КНДР, Никарагуа и Сирия. Данный проект признан официальным документом 77-й сессии ГА ООН. Концепция Конвенции базируется на основе принципов суверенного равенства государств и невмешательства в их внутренние дела. В числе ее задач указаны – предотвращение и урегулирование конфликтов, налаживание межгосударственного сотрудничества, в том числе в плане наращивания потенциала развивающихся стран в области информационной безопасности[34].

С точки зрения международного права следует отметить упоминание в данном документе значимости защиты прав человека в ИКТ-среде. Кроме того, важным элементом международного права, согласно документу, является защита интересов развивающихся государств и содействие наращиванию потенциала. Представляется важным, что документ отражает актуальную структуру международной системы, которая характеризуется формированием многополярного мира и ростом влияния незападных стран.

Однако США и иными западными государствами проект указанной Конвенции об обеспечении международной информационной безопасности поддержан не был. Представляется, что именно это есть главное препятствие для прогрессивного развития международного права в области

[30] Международная информационная безопасность: подходы России / рук. авт. кол. А.В. Крутских, Е.С. Зиновьева. С. 40.

[31] См.: Доклад Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности от 18.03.2021 г. A/75/816.

[32] Там же. Приложение II.

[33] См.: *Крутских А.В., Стрельцов А.А.* Международное право и проблема обеспечения международной информационной безопасности // Междунар. жизнь. 2014. № 11. URL: https://interaffairs.ru/jauthor/material/1167

[34] См.: Сообщение для СМИ. О Концепции Конвенции об обеспечении международной информационной безопасности // МИД России. Официальный сайт // https://mid.ru/ru/foreign_policy/news/1870609/?TSPD_101_R0=08765fb817ab20006c01cb974a2c15473d927adc1806f8c0ecaa9085c1723c30549f0148e3b49d2608ae102641143000f80145860eee2c86a2310340c8ccfbd95740e40c69a25a7adea865e6d2222dc64b87ec18a7deb7bc573b698eb5252e32

международной информационной безопасности. В Концепции внешней политики Российской Федерации отмечается стремление узкой группы государств подменить международно-правовую систему концепцией миропорядка, основанного на правилах (навязывание правил, стандартов и норм, при выработке которых не было обеспечено равноправное участие всех заинтересованных государств). Это «в значительной мере осложняет выработку коллективных ответов на транснациональные вызовы и угрозы, включая использование информационно-коммуникационных технологий в противоправных целях, приводит к деградации культуры диалога в международной сфере, снижению эффективности дипломатии как средства мирного урегулирования споров». Вследствие этого «остро ощущается дефицит доверия и предсказуемости в международных делах» (п. 9)[35].

Принятие базового универсального международного договора, который определит понятие, принципы и правовые механизмы обеспечения международной информационной безопасности, заложило бы фундамент системы правового обеспечения последней и придало бы мощный импульс развитию международно-правового регулирования противодействия отдельным информационным угрозам. В связи с этим продвижение и содействие принятию государствами – членами ООН Конвенции об обеспечении международной информационной безопасности по-прежнему остается одной из приоритетных задач государственной политики Российской Федерации в рассматриваемой сфере.

Вместе с тем нельзя отрицать, что имеются перспективы принятия значимого универсального международного договора, касающегося противодействия одной из ключевых угроз международной информационной безопасности – преступлений в сфере информационных технологий. В 2019 г. по инициативе Российской Федерации был учрежден Специальный комитет ООН в целях подготовки всеобъемлющей международной конвенции в данной области. В 2021 г. российская сторона внесла в данный Комитет *проект конвенции ООН о противодействии использованию информационно-коммуникационных технологий в преступных целях*[36]. По мнению Генеральной прокуратуры РФ, проект конвенции имеет целый ряд преимуществ: «он учитывает современные вызовы и угрозы в сфере международной информационной безопасности (в том числе криминальное использование криптовалюты), вводит новые составы преступлений, совершаемых с использованием ИКТ (распространение фальсифицированной медицинской продукции, оборот наркотиков, вовлечение несовершеннолетних в совершение противоправных деяний, опасных для их жизни и здоровья, и др.). Также проект расширяет сферу международного сотрудничества в вопросах выдачи и оказания правовой помощи по уголовным делам, включая выявление, арест, конфискацию и возврат активов»[37].

Несмотря на происходящие в мире процессы турбулентности, работа в рамках Специального межправительственного комитета ООН продолжается. 29 мая 2023 г. Председателем Специального комитета ООН представлен *проект Всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях* A/AC.291/22.

Характеризуя состояние международно-правового регулирования в области международной информационной безопасности, нельзя также не отметить наличие целого ряда международно-правовых актов универсального характера, направленных на противодействие отдельным угрозам международной безопасности, в том числе их проявлениям в информационном пространстве. К их числу, в частности, относятся Факультативный протокол к Конвенции о правах ребенка, касающийся торговли детьми, детской проституции и детской порнографии, от 25 мая 2000 г.[38], Глобальная контртеррористическая стратегия ООН от 8 сентября 2006 г.[39], Всеобъемлющая международная рамочная стратегия противодействия распространению террористических идей от 26 апреля 2017 г.[40] Однако большинство из них не носит обязательного характера.

Отдельно следует выделить *добровольные и необязательные нормы ответственного поведения государств в ИКТ-среде,* представляющие собой самостоятельный контур нормативного регулирования сферы международной информационной безопасности, дополняющий существующее международное право. Данные нормы закреплены в докладах ГПЭ 2015[41] и ГПЭ 2021 и рекомендованы для рассмотрения государствами Генеральной Ассамблеей ООН на 75-й сессии. По сути, в условиях отсутствия юридически обязательных соглашений указанные нормы стали неким промежуточным вариантом «мягкого регулирования», нацеленного на закрепление необходимых международных правил обеспечения безопасности ИКТ-среды.

Важно отметить, что в докладах ГПЭ и РГОС необязательные нормы рассматриваются как правовой механизм, который способен снизить риски международному миру и безопасности и повысить предсказуемость поведения государств. Несмотря на отсутствие обязательной (императивной) юридической силы, «нормы ответственного поведения государств в ИКТ-среде отражают ожидания международного сообщества, определяют стандарты ответственного поведения и позволяют международному сообществу давать оценку действиям и намерениям государств»[42].

Группой ведущих российских исследователей под эгидой Национальной ассоциации международной информационной безопасности (НАМИБ) было проведено фундаментальное научное исследование относительно

---

[35] См.: Концепция внешней политики Российской Федерации (утв. Указом Президента РФ от 31.03.2023 № 229) // СЗ РФ. 2023. № 14, ст. 2406.

[36] См.: О внесении в Спецкомитет ООН российского проекта универсальной международной конвенции по противодействию использованию информационно-коммуникационных технологий в преступных целях // МИД России. 28.07.2021. URL: https://archive.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/4831832 (дата обращения: 27.09.2021).

[37] Россия внесла в Специальный комитет ООН проект конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях // Генеральная прокуратура Российской Федерации. 27.07.2021 г. URL: https://epp.genproc.gov.ru/web/gprf/mass-media/news?item=63983506 (дата обращения: 21.06.2023).

[38] См.: Бюллетень международных договоров. 2014. № 6. С. 8–15.

[39] См.: Контртеррористическое управление ООН. URL: https://www.un.org/counterterrorism/ru/un-global-counter-terrorism-strategy (дата обращения: 05.06.2023).

[40] См.: Приложение к письму Председателя Комитета Совета Безопасности, учрежденного резолюцией 1373 (2001) о борьбе с терроризмом, от 26.04.2017 г. на имя Председателя Совета Безопасности S/2017/375 // Организация Объединенных Наций. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/120/85/PDF/N1712085.pdf? OpenElement (дата обращения: 05.06.2023).

[41] См.: Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности от 22.07.2015 г. A/70/174.

[42] Там же (п. 10).

применимости норм ответственного поведения государств в ИКТ-среде. Его результаты нашли отражение в реферате[43] и коллективной монографии[44].

В исследовании обращено внимание, что применение норм ответственного поведения государств в ИКТ-среде для регулирования отношений на международном и национальном уровнях сталкивается с рядом фундаментальных проблем, обусловленных отсутствием: а) общего понимания содержания международных обязательств государств в области применения ИКТ и использования ИКТ-среды; б) признанных международным сообществом границ зон ответственности государств в ИКТ-среде; в) правовых оснований для имплементации норм ответственного поведения государств в ИКТ-среде в национальное законодательство; г) правовых и иных нормативных оснований для применения некоторых норм ответственного поведения государств[45].

Для решения выявленных проблем предложено реализовать комплекс мер в рамках решения ключевых задач: 1) адаптации норм и принципов международного права к регулированию отношений в области применения ИКТ и функционирования глобальной информационной инфраструктуры в рамках ИКТ-среды как нового пространства международного сотрудничества; 2) развития на основе соглашений государств и международных организаций системы норм международного права, закрепляющих обязательства государств по вопросам применения норм ответственного поведения в ИКТ-среде, по процедуре их имплементации в национальное законодательство; 3) организации международного сотрудничества по вопросам развития системы технических стандартов, применение которых создает условия для сбора суверенными государствами информации об инцидентах в ИКТ-среде существования в этом вопросе различий[46].

При этом необходимо отметить, что цифровые технологии развиваются быстрыми темпами, появляются новые области, нуждающиеся в международно-правовом регулировании. В их числе международно-правовая регламентация использования технологий искусственного интеллекта, в том числе в военных целях, регулирование трансграничных потоков Больших данных и ряд других. Как представляется, данные проблемы нуждаются в решениях в рамках международного публичного права в силу трансграничной природы угроз, порождаемых развитием соответствующих технологий.

Формирование международно-правового регулирования международной информационной безопасности в региональных и двусторонних форматах

В связи с занятой коалицией западных государств недружественной позицией в отношении проекта конвенции об обеспечении международной информационной безопасности и дальнейшим ухудшением отношений данного блока с Российской Федерацией и КНР перспективы принятия универсальных международных соглашений в области международной информационной безопасности оцениваются как весьма низкие. Исключением здесь является проект всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях.

В этой связи на текущем этапе очевидна целесообразность усиления региональных и двусторонних треков международного сотрудничества России в области международной информационной безопасности. В Концепции внешней политики Российской Федерации в числе задач внешней политики указаны «развитие взаимовыгодного и равноправного сотрудничества с конструктивно настроенными иностранными государствами и их объединениями, раскрытие и укрепление потенциала многосторонних региональных объединений и интеграционных структур с участием России» (п. 17). В числе таких объединений и структур отмечены: БРИКС, Шанхайская организация сотрудничества (ШОС), Содружество Независимых Государств (СНГ), Евразийский экономический союз (ЕАЭС), Организация Договора о коллективной безопасности (ОДКБ), РИК (Россия, Индия, Китай) (п. 19).

В рамках перечисленных региональных организаций за последние двадцать лет был принят ряд значимых международно-правовых актов в области международной информационной безопасности, включая международные договоры. Среди них: Соглашение между правительствами государств – членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 г.[47], Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности от 20 ноября 2013 г.[48], Соглашение о сотрудничестве государств – членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности от 30 ноября 2017 г.[49]

Кроме того, принят ряд международных соглашений в области борьбы с отдельными угрозами международной информационной безопасности: Шанхайская конвенция о борьбе с терроризмом, сепаратизмом и экстремизмом от 15 июня 2001 г.[50], Конвенция Шанхайской организации сотрудничества по противодействию экстремизму от 9 июня 2017 г.[51], Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий[52] и др.

Наращивание усилий по развитию законодательства о сотрудничестве в области международной информационной безопасности в форматах региональных международных организаций и объединений есть одно из наиболее перспективных направлений в среднесрочной перспективе.

Требуется также дальнейшее развитие двустороннего сотрудничества Российской Федерации в рассматриваемой сфере с конструктивно настроенными иностранными

---

[43] См.: Применение норм ответственного поведения государств в ИКТ-среде и международное сотрудничество (реферат по результатам исследования). М., 2022.

[44] См.: Международная безопасность в среде информационно-коммуникационных технологий: коллективная монография по проблеме применения норм ответственного поведения государств в ИКТ-среде / под ред. А.А. Стрельцова, А.Я. Капустина, Т.А. Поляковой и др. М., 2023.

[45] Применение норм ответственного поведения государств в ИКТ-среде и международное сотрудничество (реферат по результатам исследования). С. 18.

[46] См.: Международная безопасность в среде информационно-коммуникационных технологий: коллективная монография по проблеме применения норм ответственного поведения государств в ИКТ-среде / под ред. А.А. Стрельцова, А.Я. Капустина, Т.А. Поляковой и др. С. 82, 83.

[47] См.: Бюллетень международных договоров. 2012. № 2.

[48] См.: Официальный портал правовой информации. 06.04.2015. http://publication.pravo.gov.ru/Document/View/0001201506040007 (дата обращения: 12.01.2023).

[49] См.: Официальный портал правовой информации. 26.04.2019. http://publication.pravo.gov.ru/Document/View/0001201904260001?index=1&rangeSize=1 (дата обращения: 12.01.2023).

[50] См.: Бюллетень международных договоров. 2004. № 1. С. 29–36.

[51] См.: Бюллетень международных договоров. 2020. № 4.

[52] См.: Бюллетень международных договоров. 2022. № 9.

государствами. У Российской Федерации на двустороннем уровне заключено более 30 межправительственных соглашений с Бразилией, Вьетнамом, Индией, КНР, Кубой, Туркменистаном и другими странами.

Особое значение в условиях гибридной войны коллективного Запада против России имеет сотрудничество с Республикой Беларусь. В 2021 г. в рамках заседания Совета министров Союзного государства были утверждены 28 союзных программ («дорожных карт»), направленных на реализацию масштабных задач по укреплению российско-белорусской интеграции, в которых уделено внимание и вопросам информационной безопасности. В частности, одна из программ нацелена на гармонизацию требований в области обеспечения информационной безопасности в финансовой сфере[53].

Важным шагом на пути сотрудничества государств в области международной информационной безопасности стало утверждение в 2023 г. *Концепции информационной безопасности Союзного государства Республики Беларусь и России*[54]. Концепция определяет основы для формирования согласованной государственной политики и развития общественных отношений в области обеспечения информационной безопасности, а также выработки мер по совершенствованию систем обеспечения информационной безопасности государств – участников Договора о создании Союзного государства. В документе определены основные угрозы информационной безопасности Союзного государства, общие принципы, цель и задачи обеспечения информационной безопасности Союзного государства. В частности, Концепция предусматривает, что меры обеспечения информационной безопасности Союзного государства реализуются в рамках: а) программ Союзного государства, государственных программ вооружения и государственных программ в области обеспечения национальной безопасности государств-участников; б) межгосударственных программ взаимодействия государств-участников по вопросам совместного обеспечения информационной безопасности; в) целевых и отраслевых программ и планов государственных органов и организаций, осуществляющих деятельность на территории государств-участников.

Важным шагом по развитию сотрудничества между Российской Федерацией и Республикой Беларусь в области международной информационной безопасности станет принятие Плана реализации основных направлений белорусско-российского сотрудничества в области обеспечения международной информационной безопасности на 2024–2026 гг. Решение о разработке такого плана было принято на встрече секретарей советов безопасности государств в июне 2023 г.[55]

Как представляется, сотрудничество на региональном уровне является важным элементом формирования международного права информационной безопасности. Заключаемые в рамках ШОС, БРИКС, ОДКБ и других международных организаций договоры становятся источниками международного права, органично вписываясь в глобальный режим международной информационной безопасности. В рамках двустороннего сотрудничества также формируются нормы и принципы международного режима информационной безопасности, причем важнейший из них – уважение государственного суверенитета и невмешательство во внутренние дела суверенных государств.

Заключение

В условиях тотальной цифровизации существенно расширился спектр вызовов и угроз, связанных с применением информационно-коммуникационных технологий в деструктивных целях. И этот процесс нарастает.

Мировым сообществом уделяется пристальное внимание угрозам ИКТ-среды и предпринимаются попытки выработки адекватного правового инструментария их сдерживания. С начала 2000-х годов под эгидой Организации Объединенных Наций проведена значительная экспертная работа, которая позволила выявить, проанализировать и обосновать ключевые проблемы обеспечения безопасности в ИКТ-среде, а также наметить основные пути деятельности международных институтов в данной области.

Однако это пока не привело к выработке и принятию базовых универсальных международных договоров в сфере международной информационной безопасности, поскольку подходы ведущих мировых держав существенно отличаются. Предложенный Российской Федерацией еще в 2011 г. проект конвенции об обеспечении международной информационной безопасности был изначально оценен скептически западными государствами. А в условиях усилившейся геополитической конфронтации шансы принятия данного документа не возрастают.

В результате проведенного анализа также были выявлены основные принципы, которые лежат в основе международного режима информационной безопасности: Принцип суверенного равенства государств; Принцип мирного разрешения международных споров; Принцип невмешательства во внутренние дела суверенных государств; Принцип уважения прав человека и основных свобод; Принцип неприменения силы и угрозы силой в ИКТ-среде; Принцип равноправия государств; Принцип недопустимости огульного обвинения государств в ИКТ-инцидентах.

При этом данные принципы могут быть уточнены и дополнены с учетом специфики ИКТ, направлений их дальнейшего развития, а также характера отношений в международной системе.

Консенсусная позиция государств о применимости общих принципов и норм международного права к ИКТ-среде не исчерпывает вопроса правовой регламентации рассматриваемой сферы, поскольку специфика ИКТ-среды не допускает экстраполяции уже существующих норм международного права на информационное пространство и требует решения комплекса сложных вопросов применения таких норм к отдельным сферам и объектам ИКТ-среды. К тому же многими государствами поддерживается необходимость прогрессивного развития международного права в сфере международной информационной безопасности, однако этому мешают принципиальные различия в подходах к данному вопросу у ключевых акторов мировой политики.

Вместе с тем определенные позитивные результаты в развитии международно-правового регулирования на универсальном уровне в последнее время достигнуты. Так, во-первых, были согласованы добровольные и необязательные нормы ответственного поведения государств в ИКТ-среде. Во-вторых, наметилась реальная перспектива разработки и принятия Всеобъемлющей международной конвенции о противодействии

[53] Опубликованы названия 28 «дорожных карт» интеграции России и Белоруссии // Эксперт. 10.09.2021 г. URL: https://expert.ru/2021/09/10/opublikovany-nazvaniya-28-dorozhnykh-kart-integratsii-rossii-i-belorussii/ (дата обращения: 21.06.2023).

[54] Утв. постановлением Высшего Государственного Совета Союзного государства от 22.02.2023 г. № 1. Официально опубликована не была.

[55] См.: Беларусь и Россия наращивают взаимодействие в сфере безопасности // Информационно-аналитический портал Союзного государства. 07.06.2023 г. URL: https://soyuz.by/bezopastnost/belarus-i-rossiya-narashchivayut-vzaimodeystvie-v-sfere-bezopasnosti (дата обращения: 15.07.2023).

использованию информационно-коммуникационных технологий в преступных целях.

В условиях весьма ограниченных перспектив развития международно-правового регулирования в области международной информационной безопасности на глобальном уровне интересам Российской Федерации отвечает наращивание взаимовыгодного и равноправного сотрудничества с конструктивно настроенными зарубежными государствами и их объединениями. Приоритетными для Российской Федерации являются форматы региональных международных организаций с участием России: СНГ, ОДКБ, ШОС, БРИКС, Союзное государство.

СПИСОК ЛИТЕРАТУРЫ

1. *Бойко С.* Основы государственной политики Российской Федерации в области международной информационной безопасности: регулирование и механизмы реализации // Междунар. жизнь. 2018. № 11. С. 24–35.
2. *Виноградова Е.В., Полякова Т.А.* О месте информационного суверенитета в информационно-правовом пространстве современной России // Правовое государство: теория и практика. 2021. № 1 (63). С. 32–49.
3. *Гриняев С.* «Таллиннское руководство по применению юридических норм международного права к военным действиям в киберпространстве» в оценках западных экспертов // Обзор. НЦПТИ. 2013. № 3. С. 18–22.
4. *Зиновьева Е.С.* Международная информационная безопасность: проблемы многостороннего и двустороннего сотрудничества. М., 2021. С. 37.
5. *Капустин А.Я.* Суверенитет государства в киберпространстве: международно-правовое измерение // Журнал зарубежного законодательства и сравнительного правоведения. 2022. Т. 18. № 6. С. 99–108.
6. *Крутских А.В., Стрельцов А.А.* Международное право и проблема обеспечения международной информационной безопасности // Междунар. жизнь. 2014. № 11. URL: https://interaffairs.ru/jauthor/material/1167
7. Международная безопасность в среде информационно-коммуникационных технологий: коллективная монография по проблеме применения норм ответственного поведения государств в ИКТ-среде / под ред. А.А. Стрельцова, А.Я. Капустина, Т.А. Поляковой и др. М., 2023. С. 82, 83.
8. Международная информационная безопасность: подходы России / рук. авт. кол. А.В. Крутских, Е.С. Зиновьева. М., 2021. С. 6, 8, 10–23, 40.
9. Модели правового регулирования обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе / под общ. ред. Т.А. Поляковой. Саратов, 2020. С. 36.
10. Обращение к читателям Министра иностранных дел Российской Федерации С.В. Лаврова // Международная информационная безопасность: теория и практика: учеб. для вузов: в 3 т. / под общ. ред. А.В. Крутских. 2-е изд., доп. М., 2021. Т. 1. С. 13.
11. *Полякова Т.А., Минбалеев А.В., Кроткова Н.В.* Развитие науки информационного права и правового обеспечения информационной безопасности: формирование научной школы информационного права (прошлое и будущее) // Государство и право. 2021. № 12. С. 97–108.
12. *Полякова Т.А., Смирнов А.А.* Правовое обеспечение международной информационной безопасности: проблемы и перспективы // Росс. юрид. журнал. 2022. № 3. С. 8.
13. *Полякова Т.А., Шинкарецкая Г.Г.* Проблемы формирования системы международной информационной безопасности в условиях трансформации права и новых вызовов и угроз // Право и государство: теория и практика. 2020. № 10 (290). С. 138.
14. Применение норм ответственного поведения государств в ИКТ-среде и международное сотрудничество (реферат по результатам исследования). М., 2022. С. 18.
15. *Смирнов А.А.* Правовые и организационные аспекты противодействия распространения фейковой информации террористическими и экстремистскими организациями // Аграрное и земельное право. 2023. № 1. С. 40–43.
16. *Смирнов А.А.* Четвертый приоритет: правовое закрепление задач обеспечения информационной безопасности в новой Стратегии национальной безопасности Российской Федерации // Вестник Воронежского гос. ун-та. Сер.: Право. 2021. № 3 (46). С. 222–228.
17. *Сундиев И.Ю., Смирнов А.А.* Использование информационных сетей в экстремистской и террористической деятельности // Научный портал МВД России. 2014. № 1. С. 84–91.
18. *Сундиев И.Ю., Смирнов А.А.* Медиаресурсы в экстремистской и террористической деятельности: функциональный анализ // Свободная мысль. 2014. № 4. С. 55–72.
19. *Сундиев И.Ю., Смирнов А.А., Андрюхин Н.Г.* Бесструктурные и бесконтактные способы вовлечения молодежи в террористическую и экстремистскую деятельность // Научный портал МВД России. 2018. № 2. С. 52–60.
20. *Федоров А.В.* Информационная безопасность в мировом политическом процессе. М., 2006. С. 5.
21. *Ясносокирский Ю.А.* Международное информационное право как регулятор международных отношений в сфере информационно-коммуникационных технологий // Междунар. жизнь. 2022. № 3. URL: https://interaffairs.ru/jauthor/material/2634
22. *Mueller M.* Will the internet fragment? Sovereignty, globalization and cyberspace. John Wiley & Sons, 2017.
23. *Schmitt, Michael N.* Tallinn Manual on the International Law Applicable to Cyber Warfare. New York, 2013.

REFERENCES

1. *Boyko S.* Fundamentals of the State policy of the Russian Federation in the field of international information security: regulation and implementation mechanisms // International life. 2018. No. 11. P. 24–35 (in Russ.).
2. *Vinogradova E.V., Polyakova T.A.* On the place of information sovereignty in the information and legal space of modern Russia // The Rule of Law: theory and practice. 2021. No. 1 (63). P. 32–49 (in Russ.).
3. *Grinyaev S.* "Tallinn Manual on the application of legal norms of International Law to military operations in cyberspace" in the assessments of Western experts // Review. NCPTI. 2013. No. 3. P. 18–22 (in Russ.).
4. *Zinovieva E.S.* International information security: problems of multilateral and bilateral cooperation. M., 2021. P. 37 (in Russ.).
5. *Kapustin A. Ya.* State sovereignty in cyberspace: an international legal dimension // Journal of Foreign Legislation and Comparative Jurisprudence. 2022. Vol. 18. No. 6. P. 99–108 (in Russ.).
6. *Krutskikh A.V., Streltsov A.A.* International Law and the problem of ensuring international information security // International life. 2014. No. 11. URL: https://interaffairs.ru/jauthor/material/1167 (in Russ.).
7. International security in the environment of information and communication technologies: a collective monograph on the problem of applying the norms of responsible behavior of states in the ICT environment / ed. by A.A. Streltsov, A. Ya. Kapustin, T.A. Polyakova et al. M., 2023. P. 82, 83 (in Russ.).
8. International information security: approaches of Russia / head authors col. A.V. Krutskikh, E.S. Zinovieva. M., 2021. P. 6, 8, 10–23, 40 (in Russ.).
9. Models of legal regulation of information security in the context of big challenges in the global information society / under the general editorship of T.A. Polyakova. Saratov, 2020. P. 36 (in Russ.).
10. Address to readers of the Minister of Foreign Affairs of the Russian Federation Sergey Lavrov // International information security: theory

and practice: textbook for universities: in 3 vols / under the general editorship of A.V. Krutskikh. 2nd ed., supplement. M., 2021. Vol. 1. P. 13 (in Russ.).

11. *Polyakova T.A., Minbaleev A.V., Krotkova N.V.* Development of the science of Information Law and legal provision of information security: formation of the scientific school of Information Law (past and future) // State and Law. 2021. No. 12. P. 97–108 (in Russ.).
12. *Polyakova T.A., Smirnov A.A.* Legal support of international information security: problems and prospects // Russ. legal journal. 2022. No. 3. P. 8 (in Russ.).
13. *Polyakova T.A., Shinkaretskaya G.G.* Problems of formation of the international information security system in the context of the transformation of law and new challenges and threats // Law and the State: Theory and Practice. 2020. No. 10 (290). P. 138 (in Russ.).
14. Application of norms of responsible behavior of states in the ICT environment and international cooperation (abstract based on the results of the study). M., 2022. P. 18 (in Russ.).
15. *Smirnov A.A.* Legal and organizational aspects of countering the spread of fake information by terrorist and extremist organizations // Agrarian and Land Law. 2023. No. 1. P. 40–43 (in Russ.).
16. *Smirnov A.A.* The fourth priority: the legal consolidation of the tasks of ensuring information security in the new National Security Strategy of the Russian Federation // Herald of the Voronezh State University. Ser.: Law. 2021. No. 3 (46). P. 222–228 (in Russ.).
17. *Sundiev I. Yu., Smirnov A.A.* The use of information networks in extremist and terrorist activities // Scientific portal of the Ministry of Internal Affairs of Russia. 2014. No. 1. P. 84–91 (in Russ.).
18. *Sundiev I. Yu., Smirnov A.A.* Media resources in extremist and terrorist activities: functional analysis // Free Thought. 2014. No. 4. P. 55–72 (in Russ.).
19. *Sundiev I. Yu., Smirnov A.A., Andryukhin N.G.* Structureless and contactless ways of involving youth in terrorist and extremist activities // Scientific portal of the Ministry of Internal Affairs of Russia. 2018. No. 2. P. 52–60 (in Russ.).
20. *Fedorov A.V.* Information security in the global political process. M., 2006. P. 5 (in Russ.).
21. *Yasnosokirsky Yu.A.* International Information Law as a regulator of international relations in the field of information and communication technologies // International life. 2022. No. 3. URL: https://interaffairs.ru/jauthor/material/2634 (in Russ.).
22. *Mueller M.* Will the internet fragment? Sovereignty, globalization and cyberspace. John Wiley & Sons, 2017.
23. *Schmitt, Michael N.* Tallinn Manual on the International Law Applicable to Cyber Warfare. New York, 2013.

Сведения об авторах

ПОЛЯКОВА Татьяна Анатольевна –
доктор юридических наук, профессор,
заслуженный юрист РФ,
главный научный сотрудник,
и.о. заведующей сектором
информационного права и международной
информационной безопасности
Института государства и права
Российской академии наук;
119019 г. Москва, ул. Знаменка, д. 10
ORCID: 0000-0003-3791-2903

ЗИНОВЬЕВА Елена Сергеевна –
доктор политических наук, доцент,
заместитель директора Центра международной
информационной безопасности
и научно-технологической политики МГИМО;
119454 г. Москва, проспект Вернадского, д. 76
ORCID: 0000-0002-5129-338X
Scopus Author ID: 57191565394

СМИРНОВ Александр Александрович –
доктор юридических наук, доцент,
ведущий научный сотрудник 3 отдела НИЦ № 4
ВНИИ МВД России; 121069 г. Москва,
ул. Поварская, д. 25, стр. 1;
старший научный сотрудник сектора
информационного права и международной
информационной безопасности
Института государства и права
Российской академии наук;
119019 г. Москва, ул. Знаменка, д. 10

Authors' information

POLYAKOVA Tatyana A. –
Doctor of Law, Professor,
Chief Researcher, Acting Head
of the Sector of Information Law
and International Information Security,
Institute of State and Law
of the Russian Academy of Sciences;
10 Znamenka str., 119019 Moscow, Russia

ZINOVIEVA Elena S. –
Doctor of Sciences (Politics), Associate Professor,
Deputy Director of the Center for International
Information Security and Scientific
and Technological Policy of MGIMO University;
76 Vernadskogo Ave., 119454 Moscow, Russia

SMIRNOV Aleksandr A. –
Doctor of Law, Associate Professor,
Leading Researcher
of the 3rd Department of SIC No. 4,
All-Russian Research Institute
of the Ministry of Internal Affairs
of the Russian Federation; 25, bld. 1 Povarskaya str.,
121069 Moscow, Russia;
Senior Researcher of the Sector of Information Law
and International Information Security,
Institute of State and Law
of the Russian Academy of Sciences;
10 Znamenka str., 119019 Moscow, Russia