



Научная статья

УДК 32

<https://doi.org/10.22394/2079-1690-2024-1-4-215-222>

EDN JICUX

Проблемы регулирования информационно-коммуникативных технологий в условиях кризиса мирового порядка

Екатерина Ильинична Хубулури

Ростовский государственный университет путей сообщения, Ростов-на-Дону, Россия,
ehubuluri@yandex.ru

Аннотация. В условиях кризисного характера формирования мирового порядка актуализируется проблематика глобального регулирования. Развитие информационно-коммуникативных технологий (ИКТ), будучи одним из мегатрендов мирового развития, не является исключением. В настоящее время регулирование глобального информационно-коммуникационного пространства затруднено ввиду ряда различных причин, таких как его секьюритизация государствами, отсутствие аккомодации между великими державами и гомогенности в определении угроз, существенных терминов, идей и подходов. В статье рассматривается роль ИКТ как ресурса атрибутивной и релятивной силы, подходы России, США и КНР к глобальному регулированию развития ИКТ и информационно-коммуникационного пространства, а также основные проблемы на этом пути.

На современном этапе технологического развития важнейшее значение приобретает суверенитет в области цифровых технологий. Внимание к цифровому суверенитету обусловлено радикальной трансформацией экономического и технологического укладов, общественных отношений и политической жизни, вызванной глобальной цифровой трансформацией. Эти изменения проявились и в сфере международных отношений – цифровое пространство стало полем геополитических противоречий, а уровень цифровизации становится важным фактором, определяющим положение страны на международной арене и спектр доступных ей внешнеполитических возможностей.

Исследования в области цифрового суверенитета тесно связаны с анализом технологического суверенитета, под которым понимается обеспечение независимости в научных разработках, определении стандартов, безопасности физической инфраструктуры связи.

Также рассматривается взаимосвязь с исследованиями в области технологических укладов, которые проводятся в сфере экономических наук и подчеркивают экономический потенциал цифровых технологий в рамках перехода к Четвертой промышленной революции.

В заключение делается вывод о необходимых шагах в этом направлении, которые следует предпринять России для достижения лидерства в этом функциональном «досье».

Ключевые слова: кибербезопасность, глобальное управление, сдерживание, информационно-коммуникационные технологии (ИКТ), великие державы, мегатренды, нормативный активизм, суверенитет

Для цитирования: Хубулури Е. И. Проблемы регулирования информационно-коммуникативных технологий в условиях кризиса мирового порядка // Государственное и муниципальное управление. Ученые записки. 2024. № 4. С. 215–222. <https://doi.org/10.22394/2079-1690-2024-1-4-215-222>. EDN JICUX

Problems of regulation of information and communication technologies in the context of the crisis of the world order

Ekaterina I. Hubuluri

Rostov State Transport University, Rostov-on-Don, Russia, ehubuluri@yandex.ru

Abstract. In the context of the crisis nature of the formation of the world order, the problems of global regulation are being actualized. The development of information and communication technologies (ICT), being one of the megatrends of global development, is no exception. Currently, the regulation of the global information and communication space is difficult due to a number of different reasons, such as its securitization by States, lack of accommodation between great powers and homogeneity in defining threats, essential terms, ideas and approaches. The article examines the role of ICT as a resource of attributive and relational power, the approaches of Russia, the United States and China to global regulation of the development of ICT and information and communication space, as well as the main problems along this path. At the present stage of technological development, sovereignty in the field of digital technologies is of crucial importance. Attention to digital sovereignty is conditioned by the radical transformation of economic and technological structures, public relations and political life caused by the global digital transformation. These changes have also manifested themselves in the sphere of international relations – the digital space has become a field of geopolitical contradictions, and the level of digitalization is becoming an important factor determining the country's position in the international arena and the range of foreign policy opportunities available to it.

Research in the field of digital sovereignty is closely related to the analysis of technological sovereignty, which means ensuring independence in scientific research, defining standards, and the security of physical communications infrastructure. It also examines the relationship with research in the field of technological structures, which are conducted in the field of economic sciences and emphasize the economic potential of digital technologies as part of the transition to the Fourth Industrial Revolution. In conclusion, the conclusion is made about the necessary steps in this direction that Russia should take to achieve leadership in this functional "dossier".

Keywords: information and communication technologies, cybersecurity, global governance, constraint, great powers, megatrends, normative activism, sovereignty

For citation: Hubuluri E. I. Problems of regulation of information and communication technologies in the context of the crisis of the world order. *State and Municipal Management. Scholar Notes*. 2024;(4):215–222 (In Russ.). <https://doi.org/10.22394/2079-1690-2024-1-4-215-222>. EDN JIICUX

Введение

В настоящее время происходит формирование современного мирового порядка [1, с.7]. На фоне этого актуализируются нормативный и коммуникационный аспекты взаимодействия между субъектами, а также вопрос о механизмах принятия решений на глобальном уровне [2, с. 25]. Несмотря на то, что черты нового мирового порядка до конца еще не оформились, вполне можно констатировать недостаточную степень аккомодации в отношениях между великими державами, размывание международных режимов и несоблюдение норм, а также кризис институтов глобального регулирования. Сегодня мир можно описать либо как «осыпавшийся»¹, либо как «опять разделенный», в котором выделяются три центра силы, отождествленные тремя великими державами - Россией, США и КНР [3, с.10].

¹ Мир осыпался: что дальше? Четвёртый день ежегодного заседания клуба «Валдай». - Международный дискуссионный клуб «Валдай». 28.10.2022. Доступ: <https://ru.valdaiclub.com/events/posts/articles/mir-osypalsya-clito-dalshe/>.

ИКТ: от инструмента «коммуникации во благо» до ресурса «войн будущего»

С развитием информационно-коммуникационных и цифровых технологий (ИКТ) изменилось само пространство международных отношений: из трехмерного (суша, вода и воздух) оно трансформировалось в четырехмерное (киберпространство/информационная сфера¹). И если в начале его активного освоения (1990-е гг.) оно рассматривалось как неподконтрольное государствам, то уже в нулевых годах постепенно стало приходить понимание, что оно имеет свои политические границы, отражающие существующую карту мира [4, с. 112]. Глобальное регулирование этого пространства становится прерогативой национальных государств, поскольку информационные технологии рассматриваются как проблема обеспечения их национальной безопасности.

Если на заре развития ИКТ и становления понимания информационного пространства как «коммуникационного» виделась возможность междержавной кооперации в информационной среде для достижения общего блага, то в дальнейшем данная среда стала рассматриваться как потенциально конфликтная, включенная в пространство войны [5, с. 105; 6, с. 186], в которой возникают и развиваются различные типы кибер-/ кибернетических/кибернетизированных (cybered) конфликтов как внутри национальных государств (в т.ч. в результате вмешательства извне), так и между ними. Складывается дихотомия, в рамках которой ИКТ рассматриваются как обоюдоострый меч: усиливая то или иное государство и позволяя ему стать лидером, они одновременно становятся орудием для нанесения ему вреда со стороны тех, кто стремится его разрушить. Эти технологии также рассматриваются с точки зрения их возможного двойного и военного назначения, в т.ч. как инструмент ведения гибридных войн [7, с. 57], и одной из особенностей природы и методов ведения «войн будущего» [8, с. 12]. Более того, угрозы и вызовы в информационном и киберпространстве стали восприниматься через призму обеспечения безопасности ядерного комплекса государств [9, с. 148]. Закономерным итогом стала милитаризация глобального информационного пространства [10, с. 55], а информационно-коммуникационные и цифровые технологии стали ресурсом как атрибутивной, так и релятивной силы.

Причины кризиса глобального регулирования информационно-коммуникационного пространства

В настоящее время эффективное глобальное регулирование информационно-коммуникационного пространства отсутствует по нескольким причинам.

Во-первых, как уже упоминалось выше, в настоящее время наблюдается недостаточная степень аккомодации между тремя ключевыми великими державами. Во-вторых, каждая из великих держав стремится предложить свое видение будущего мирового устройства и глобального регулирования. Такие попытки нередко направлены на обретение статуса лидера/гегемона, сдерживание других держав, программирование системы международных отношений на междержавную конкуренцию. Особенно это характерно для внешнеполитической деятельности США [11, с. 13]. В-третьих, по-прежнему сохраняется дискурс относительно того, стоит ли передавать больше полномочий на уровень глобальных институтов или идти по пути укрепления роли национальных государств в различных сферах [12, с. 15]. Для современного состояния системы международных отношений характерны опасения государств относительно углубления взаимозависимости, которая воспринимается как средство вмешательства во внутренние дела, а также «суверенизация повесток», являющаяся как инструментом обретения собственных выгод, так и средством конкуренции с другими игроками, в результате чего подрывается доверие между ними, и достижение баланса сил и гомогенизация идей становятся невозможными [13, с. 66–67].

Видение глобального регулирования информационно-коммуникационного пространства отличается у трех держав. ИКТ обретают еще одну грань – они становятся ресурсом нормативной силы государств.

¹ National Security Strategy. - Historical Office. Office of the Secretary of Defense. May 2010. P. 24. URL: <https://historydefense.gov/Portals/70/Documents/nss/NSS2010.pdf?ver=Zt7IeSPX2uNQ0t07wq6Hg%3D%3D>.

Подходы великих держав

Россия подразумевает под таким пространством «информационную среду/ пространство» (отсюда термин «информационная безопасность»)¹, а США – «киберпространство» («кибербезопасность»)². Понимание пространства Китая можно описать как «сетевое пространство» [14, с. 384] («сетевая безопасность»)³. В то же время достаточно распространенным термином в китайских документах остается «информационная среда» [15, с. 175] и «информационная безопасность»⁴. Также встречаются термины «цифровая сфера» и «кибербезопасность». Отличаются и подходы государств к глобальному регулированию информационного пространства.

Россия выступает с позиции необходимости институционализации информационной сферы, признания всеми игроками существования национальных сегментов информационного пространства и принципа суверенитета национальных государств над своей частью пространства, означающего невмешательство при помощи ИКТ во внутренние дела суверенных государств. Более того, российский подход не только затрагивает проблематику безопасности компьютерных систем и иных средств связи, но также рассматривает политико-идеологические аспекты безопасности и направлен на обеспечение безопасности социально-гуманитарного развития общества. По мнению России, интернационализированное глобальное регулирование информационного пространства – ключ к кооперационной модели существования государств. Россия в 2004 г. выступила инициатором создания Группы правительственных экспертов ООН (ГПЭ), на базе которой в 2018 г. вновь по предложению России была создана Рабочая группа открытого состава (РГОС). Создание РГОС было обусловлено возникновением во второй половине 2010-х гг. серьезных противоречий между членами ГПЭ [16] по вопросу применения международного права относительно действий держав в информационном/киберпространстве. Но несмотря на принятие в 2021 г. доклада РГОС, ставшего символом «триумфального успеха российской дипломатии»⁵, и упразднение параллельно возрожденного США формата ГПЭ, по-прежнему затруднено внедрение принятых предложений и норм в реальную практику. На это есть как минимум две принципиальные причины. Во-первых, между странами по-прежнему отсутствует единая позиция относительно механизмов применения международного права в информационном/киберпространстве. Во-вторых, ООН не является инструментом глобального регулирования (необходимыми атрибутами обладает лишь Совет Безопасности) [17, с. 62, 63].

Китай выступает с позиции многосторонней централизованной модели [18, с. 21], суть которой заключается в распространении суверенитета⁶ государства в вопросах, относящихся к глобальному регулированию информационного/интернет-пространства [19, с. 55] (роль негосударственных акторов сводится лишь к консультативной функции). Китай в своей внешнеполитической стратегии рассматривает «традиционные международные институты», например, систему ООН, как структуру, в которой он не может достичь лидирующей роли и конструктивного сотрудничества с другими державами, считая, что его интересы не будут удовлетворены в результате ограничительных действий других влиятельных игроков. Это объясняется тем, что они создавались в то время, когда Китай еще не был одним из системообразующих акторов. Следовательно, в них он видит свою роль в качестве «участника», действия которого лишь направлены на поддержку этих институтов. Это, впрочем, вовсе не означает, что его роль в них в качестве «участника» выработки глобальных норм и создания

¹ Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». Доступ: <http://krenilm.ra/acts/barLk/41460>.

² National Cybersecurity Strategy. - The White House. March 2023. URL: <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>.

³ China's Positions on Global Digital Governance (Contribution for the Global Digital Compact). - Ministry of Foreign Affairs of the People's Republic of China. 25.05.2023. URL: https://www.fmprc.gov.cn/eng/wjw663304/zjzg663340/jks665232/kjlc665236/qtwt_665250/202305/t20230525_11083607.html // Text China%20supports%20thc%20lcading%L0zzjg_663340/jks_665232/kjlc_665236/qtwt665250/201703Д20170301_599869.html.

⁴The Internet in China. - Information Office of the State Council of the People's Republic of China. 08.06.2010. URL: http://iq.china-embassy.gov.cn/ara/zt/zgzfbps/201206/t20120621_2518854.htm.

⁵ В РФ заявили, что рабочая группа ООН по информационной проблематике начнет работу в июне. - ТАСС. 13.03.2021. Доступ: <https://tass.ru/politika/10895625>.

⁶ Global Initiative on Data Security. - Ministry of Foreign Affairs of the People's Republic of China. 08.09.2020. URL: https://www.fmprc.gov.cn/nTfa_eng/wjdt_665385/2649_665393/202009/t20200908_679637.html.

международных режимов не будет активной. Напротив, в «модифицированных», или «улучшенных», а тем более в «инновационных» международных институтах (ШОС+, БРИКС+), созданных, когда Пекин уже стал одной из ключевых глобальных держав, влияющей на систему международных отношений, он видит свою роль в качестве «созидателя», «лидера» и «направляющего» [20, с. 17, 18]. Поэтому предполагается, что именно эти институты Китай будет рассматривать как перспективные для своей нормативной деятельности и активизации сотрудничества в области глобального регулирования развития ИКТ и информационно-коммуникационного пространства.

США рассматривают глобальное регулирование киберпространства как децентрализованную модель [18, с. 21], основную роль в которой играют частные структуры (на которые, впрочем, могут оказывать влияние американские власти, т.е. речь идет о государственно-частном режиме управления, или принципе мультистейкхолдерности). Что касается категории суверенитета, то она по-прежнему не употребляется в американских документах, предназначенных для глобального уровня. Это может интерпретироваться как «желание распространить нормы и практики внутренней политики США на своих союзников» [21, с. 47]. Это вовсе, однако, не означает, что США не секьюритизируют эту проблематику (например, они вводят рестриктивные меры в отношении иностранных цифровых платформ). США заинтересованы в экстратерриториальном глобальном регулировании, т.е. расширении собственной юрисдикции «на международный уровень системы Интернета в целом», что позволит им ограничить суверенитет других держав и укрепить свой статус гегемона-лидера [22, с. 14]. Таким образом, для них неприемлем российский и китайский подходы, поскольку они видят в них укрепление примата государственного контроля над киберсредой. В области обеспечения кибербезопасности Вашингтон институционализирует сотрудничество со странами НАТО. США продвигают Группу независимых экспертов под эгидой НАТО, ключевым проектом которой является Таллинское руководство, целью которого стало регулирование киберпространства с точки зрения международного гуманитарного права. На сегодняшний день Руководство уже охватывает два принципиальных вопроса, давая понять, что США рассматривают киберпространство как настоящий театр военных действий. Более того, США в своих стратегических документах отмечают, что на кибератаки они будут «реагировать всеми соответствующими инструментами национальной мощи». В целом, стратегия США в киберсреде направлена на сдерживание России и Китая [23], что не только мешает конструктивному диалогу между великими державами, но и «обостряет дилемму безопасности» [22, с. 59].

В рамках глобального регулирования в области информационно-коммуникационных и цифровых технологий заметны те же тенденции, которые характерны для многих других сфер: постепенное смещение акцента на «два конкурирующих мирорегулирующих блока («глобальное НАТО» и «ШОС+»)» [17, с. 63], а также повышение статуса БРИКС+. В настоящее время отсутствие международного режима со своими работающими институтами во многом является следствием нежелания США лишать себя особого положения в этом функциональном «досье». Все это не ведет к снижению конфликтности между игроками на международной арене и элиминации глобальных угроз в информационной и цифровой среде.

Заключение

На этом фоне возможным положительным сценарием для России может стать углубление взаимодействия в рамках данной проблематики с Китаем, а также с Индией, Бразилией и другими заинтересованными державами в рамках ООН, ШОС+, БРИКС+, ОДКБ и других глобальных и региональных форматов, альтернативных западным институтам. Иными словами, России крайне важно сохранить гибкость, рационализм и инклюзивность своего подхода по формированию всеобъемлющего и универсального международно-правового режима регулирования информационно-коммуникационного пространства. Для этого России необходимо продолжать активно выступать на международной арене в качестве нормативного актора, манифестируя свои намерения в рамках глобального публичного пространства.

Помимо дискурсивных практик, не менее важным для России является онтологическое наполнение ее цифрового суверенитета. В существующих реалиях экономического давления западных стран и их попыток сдержать ее технологическое развитие добиться этого становится весьма нетривиальной задачей. Однако достижение ощутимых результатов в рамках этой деятельности, на наш взгляд, будет являться стратегической целью для России, поскольку от этого будет зависеть ее развитие и ее мощь.

Цифровой и технологический суверенитет России позволит ей помешать складыванию американо-китайской дуополии в информационном/сетевом/ киберпространстве. Заключение двусторонних и многосторонних договоров в области обеспечения региональной и глобальной информационной безопасности позволит ей не допустить своей изоляции и сдерживания со стороны какой-либо державы.

Активная и самостоятельная политика России на этом направлении будет встречать критику и, возможно, даже неприятие со стороны стран Запада. В то же время именно независимость внешней политики России и стремление развивать глобальное регулирование в области информационно-коммуникационных и цифровых технологий в логике кооперации с другими государствами с целью построения инклюзивного (справедливого) и равноправного для национальных государств и суверенного для каждого из них коммуникационного пространства будет укреплять роль Москвы как ответственной великой державы, позволяя ей продвигаться на пути лидерства как минимум в этом функциональном «досье» глобального регулирования, оказывающего влияние на формирование нового мирового порядка.

Список источников

1. Шаклеина Т.А. Переломный момент в мировом развитии. Сохранит ли Запад преобладающее влияние на формирование мирового порядка XXI века? // Международные процессы. Т. 20. 2022. № 4(71). С. 6-22. DOI: 10.17994/IT.2022.20.4.71.2. EDN: IGCAUV.
2. Лебедева М.М. Новый мировой порядок: параметры и возможные контуры // Полис. Политические исследования. 2020. № 4. С. 24-35. DOI: 10.17976/jpps/2020.04.03. EDN: DNORYR.
3. Богатуров А.Д. Введение. Попытка построения «однополярной безопасности» и современная трехполюсная система / Системная история международных отношений. Опять разделенный мир. 1980-2018: учебное пособие для вузов. 3-е изд., перераб. и доп. М.: Юрайт. 2020. С. 10-17. EDN: WFDKWR.
4. Зиновьева Е.С. Глобальное управление Интернетом: российский подход и международная практика // Вестник МГИМО Университета. 2015. № 4(43). С. 111-118. DOI: 10.24833/2071-8160-2015-4-43-111-118. EDN: UDUNML.
5. Истомин И.А. Войны будущего в свете опыта прошлого // Мировая экономика и международные отношения. 2022. Т. 66. № 11. С. 101-114. DOI: 10.20542/0131-2227-2022-66-11-101-114. EDN: IRAVWZ.
6. Коньшев В.Н. Изучая природу войны: взгляд из России и Европы // Полис. Политические исследования. 2022. № 6. С. 182-188. DOI: 10.17976/jpps/2022.06.13. EDN: MIYBGV.
7. Коньшев В.Н., Парфенов Р.В. 2019. Гибридные войны: между мифом и реальностью // Мировая экономика и международные отношения. Т. 63. № 12. С. 56-66. DOI: 10.20542/0131-2227-2019-63-12-56-66. EDN: NQTLHW.
8. Сучков М.А., Тэк С. Будущее войны: доклад международного дискуссионного клуба «Валдай». - МДК«Валдай». 2019. 24 с. EDN: JZOFUG.
9. Футтер Э. Ядерное оружие в век информационных технологий // Россия в глобальной политике. 2016. Т. 14. № 6. С. 146-159. EDN: XAELEN.
10. Зиновьева Е.С. Киберсдерживание и цифровая дилемма безопасности в американском экспертном дискурсе // Международные процессы. 2019. Т. 17. № 3(58). С. 51-65. DOI: 10.17994/IT.2019.17.3.58.4. EDN: LVKPIA.
11. Шаклеина Т.А. Политика США в отношении России: конкуренция, сдерживание и управление // Вестник РГГУ. Сер. Политология. История. Международные отношения. 2020. № 4. С. 10-26. DOI: 10.28995/2073-6339-2020-4- 10-26. EDN: FOEVRX.
12. Сафранчук И.А., Лукьянов Ф.А. Современный мировой порядок: адаптация акторов к структурным реалиям // Полис. Политические исследования. 2021. № 4. С. 14-25. DOI: 10.17976/jpps/2021.04.03. EDN: JVPZJB.
13. Сафранчук И.А., Лукьянов Ф.А. Современный мировой порядок: структурные реалии и соперничество великих держав // Полис. Политические исследования. 2021. № 3. С. 57-76. DOI: 10.17976/jpps/2021.03.05. EDN: XOYUIZ.

14. Понька Т.И., Рамич М.С., У Ю. Информационная политика и информационная безопасность КНР: развитие, подходы и реализация. // Вестник Российского университета дружбы народов. Сер. Международные отношения. 2020. Т. 20. № 2. С. 382-394. DOI: 10.22363/2313-0660-2020-20-2-382-394. EDN: UANODL.
15. Creemers R. The Chinese Conception of Cybersecurity: A Conceptual, Institutional, and Regulatory Genealogy. - Journal of Contemporary China. 2024. Vol. 33. Is. 146. P. 173-188. DOI: 10.1080/10670564.2023.2196508.
16. Шакиров О.И. Широкий киберконсенсус. - Российский совет по международным делам. 23.03.2021. Доступ: https://russiancouncil.ru/analyt-ics-and-comments/analytics/shirokiy-kiberkonsensus/?sphrase_id=13172130
17. Худайкулова А.В. К вопросу о глобальном управлении в XXI в.: подходы РФ, КНР и США. - Социальные и гуманитарные знания. Т. 8. 2022. № 1(29). С. 56-69. DOI: 10.18255/2412-6519-2022-1-56-69. EDN: CYFJSX.
18. Дегтерев Д.А., Рамич М.С., Пискунов Д.А. Подходы США и КНР к глобальному управлению киберпространством: «новая биполярность» в «сетевом обществе» // Вестник международных организаций: образование, наука, новая экономика. Т. 16. 2021. № 3. С. 7-33. DOI: 10.17323/1996-7845-2021-03-01. EDN: RHBSFR.
19. Ребро О.И., Гладышева А., Сучков М.А., Сушенцов А.А. Категория «Цифрового суверенитета» в современной мировой политике: вызовы и возможности для России // Международные процессы. Т. 19. 2021. № 4(67). С. 47-67. DOI: 10.17994/1X2021.19.4.67.6. EDN: QRXXVU.
20. Грачиков Е.Н., Сюй Х. КНР и международная система: формирование собственной модели мироустройства // Вестник международных организаций: образование, наука, новая экономика. Т. 17. 2022. № 1. С. 7-24. DOI: 10.17323/1996-7845-2022-01-01. EDN: ZDZJNP.
21. Зиновьева Е.С., Шитьков С.В. Цифровой суверенитет в практике международных отношений // Международная жизнь. 2023. № 3. С. 38-51. EDN: HBTQYT.
22. Зиновьева Е.С. Формирование цифровых границ и информационная глобализация: анализ с позиций критической географии // Полис. Политические исследования. 2022. №2. С. 8-21. DOI: 10.17976/jpps/2022.02.02. EDN: AJDIQL.
23. Себекин С.А. Система международной информационной безопасности в условиях политической турбулентности // Вестник Санкт-Петербургского университета. Международные отношения. Т. 16. 2023. № 2. С. 170-190. DOI: 10.21638/spbu06.2023.205. EDN: JQHKPU.

References

1. Shakleina T.A. A turning point in world development. Will the West retain its predominant influence on shaping the world order of the 21st century? *International processes*. Vol. 20. 2022;4(71):6-22. (In Russ.). DOI: 10.17994/IT.2022.20.4.71.2. EDN: IGCAUV.
2. Lebedeva M.M. The New World Order: parameters and possible contours. *The policy. Political research*. 2020;(4):24-35. (In Russ.). DOI: 10.17976/jpps/2020.04.03. EDN: DNORYR.
3. Bogaturov A.D. *Introduction. An attempt to build a "unipolar security" and a modern three-pole system. - A systematic history of international relations. A divided world again. 1980-2018: textbook for universities*. 3rd ed., reprint. and additional. (In Russ.). Moscow: Yurait; 2020:10-17. EDN: WFDKWR.
4. Zinovieva E.S. Global Internet governance: the Russian approach and international practice. *Bulletin of MGIMO University*. 2015;4(43):111-118. (In Russ.). DOI: 10.24833/2071-8160-2015-4-43-111-118. EDN: UDUNML.
5. Istomin I.A. Wars of the future in the light of the experience of the past. *World economy and international relations*. 2022;66(11):101-114. (In Russ.). DOI: 10.20542/0131-2227-2022-66-11-101-114. EDN: IRAVWZ.
6. Konyshov V.N. Studying the nature of war: a view from Russia and Europe. *The policy. Political research*. 2022;(6):182-188. (In Russ.). DOI: 10.17976/jpps/2022.06.13. EDN: MIYBGV.
7. Konyshov V.N., Parfenov R.V. Hybrid Wars: Between myth and reality. *World Economy and International Relations*. 2019;63(12):56-66. (In Russ.). DOI: 10.20542/0131-2227-2019-63-12-56-66. EDN: NQTLHW.
8. Suchkov M.A., Tek S. *The future of war: report of the Valdai International Discussion Club*. - MDK "Valdai". 2019. 24 p. (In Russ.). EDN: JZOFUG.

9. Futter E. Nuclear weapons in the age of information technology. *Russia in global politics*. (In Russ.). 2016;14(6);146–159. EDN: XAELEH.
10. Zinovieva E.S. Cyber support and the digital security dilemma in American expert discourse. *International processes*. 2019;(17(3(58))):51-65. (In Russ.). DOI 10.17994/IT.2019.17.3.58.4. EDN: LVKPIA.
11. Shakleina T.A. U.S. policy towards Russia: competition, deterrence and governance. *Bulletin of the Russian State University. Ser. Political science. History. International relations*. 2020;(4):10-26. (In Russ.). DOI: 10.28995/2073-6339-2020-4- 10-26. EDN: FOEVRX.
12. Safranchuk I.A., Lukyanov F.A. Modern world order: adaptation of actors to structural realities. *The policy. Political research*. 2021;(4):14-25. (In Russ.). DOI: 10.17976/jpps/2021.04.03. EDN: JVPZJB.
13. Safranchuk I.A., Lukyanov F.A. Modern world order: structural realities and rivalry of great powers. *The policy. Political research*. 2021;(3):57-76. (In Russ.). DOI: 10.17976/jpps/2021.03.05. EDN: XOYUIZ.
14. Ponka T.I., Ramich M.S., U. Yu. Information policy and Information Security of the People's Republic of China: development, approaches and implementation. *Bulletin of the Peoples' Friendship University of Russia. Ser. International Relations*. 2020; 20(2):382–394. (In Russ.). DOI: 10.22363/2313-0660-2020-20-2-382-394. EDN: UANODL.
15. Creemers R. The Chinese Conception of Cybersecurity: A Conceptual, Institutional, and Regulatory Genealogy. *Journal of Contemporary China*. 2024;33(146):173-188. DOI: 10.1080/10670564.2023.2196508.
16. Shakirov O.I. Broad cyberconsensus. *The Russian Council for International Affairs*. 23.03.2021. (In Russ.). Access: https://russiancouncil.ru/analyt-ics-and-comments/analytics/shirokiy-kiberkonsensus/?sphrase_id=13172130.
17. Khudaikulova A.V. On the issue of global governance in the XXI century: approaches of the Russian Federation, China and the USA. *Social and humanitarian knowledge*. 2022;8(1(29)):56-69. (In Russ.). DOI: 10.18255/2412-6519-2022-1-56-69. EDN: CYFJSX.
18. Degterev D.A., Ramich M.S., Piskunov D.A. Approaches of the USA and China to global cyberspace management: “new bipolarity” in the “network society”. *Bulletin of International Organizations: Education, Science, New Economy*. 2021;16(3):7–33. (In Russ.). DOI: 10.17323/1996-7845-2021-03-01. EDN: RHBSFR.
19. Rebro O.I., Gladysheva A., Suchkov M.A., Sushentsov A.A. The category of “Digital sovereignty” in modern world politics: challenges and opportunities for Russia. *International processes*. 2021;19(4(67));47–67. (In Russ.). DOI: 10.17994/1X2021.19.4.67.6. EDN: QPXXVU.
20. Grachikov E.N., Xu H. China and the international system: the formation of its own model of the world order. *Bulletin of International Organizations: Education, Science, New Economy*. 2022;17(1);7–24. (In Russ.). DOI: 10.17323/1996- 7845-2022-01-01. EDN: ZDZJNP.
21. Zinovieva E.S., Shitkov S.V. Digital sovereignty in the practice of international relations. *International life*. 2023;(3);38–51. (In Russ.). EDN: HBTQYT.
22. Zinovieva E.S. The formation of digital borders and information globalization: an analysis from the standpoint of critical geography. *The policy. Political research*. 2022;(2):8-21. (In Russ.). DOI: 10.17976/jpps/2022.02.02. EDN: AJDIQL.
23. Sobekin S.A. The system of international information security in conditions of political turbulence. *Bulletin of St. Petersburg University. International Relations*. 2023;16(2):170-190. (In Russ.). DOI: 10.21638/spbu06.2023.205. EDN: JQHKPU.

Информация об авторе

Е. И. Хубулури – доцент, доктор политических наук, профессор кафедры «Государственное и муниципальное управление» гуманитарного факультета Ростовского государственного университета путей сообщения.

Information about the author

E. I. Khubuluri – Associate Professor, Dr. Sci. (Polit.), Professor of the Department of State and Municipal Administration, Faculty of Humanities, Rostov State University of Railway Engineering.

Автор заявляет об отсутствии конфликта интересов.
The author declares that there is no conflict of interest.

Статья поступила в редакцию 27.10.2024; одобрена после рецензирования 28.11.2024; принята к публикации 29.11.2024.

The article was submitted 27.10.2024; approved after reviewing 28.11.2024; accepted for publication 29.11.2024.