



Кибердипломатия в условиях обострения великодержавной конкуренции

Е.С. Зиновьева^{1,2}

¹ Московский государственный институт международных отношений (университет) МИД России

² Национальный исследовательский университет «Высшая школа экономики»

Фрагментация интернета, пришедшая на смену информационной глобализации, становится новой реальностью. Цифровые технологии и интернет превращается в поле новых геополитических противоречий и борьбы за лидерство между великими державами. Кибердипломатия, которая включает в себя спектр вопросов использования ИКТ для достижения внешнеполитических целей государства, а также новые проблемные и предметные области международных отношений, возникающие в связи с цифровизацией, является важнейшим инструментом межгосударственной конкуренции и конфликтов, а также средством ведения информационных войн.

На международном уровне отсутствуют международно признанные нормы, регламентирующие развитие и использование цифровых инструментов в рамках внешней политики, межгосударственной конкуренции или противоборства. Становится особенно важной выработка правил ответственного поведения государств в глобальном информационном пространстве.

Методологически статья построена на теории жизненного цикла норм. Согласно данному подходу, нормы представляют собой социальные стандарты, регулирующие поведение государств в определённой области международных отношений. Была исследована эволюция дискурса о нормах, регулирующих цифровую дипломатию и глобальное цифровое пространство. В настоящее время произошёл отказ от продвигаемых США норм глобального интернета, свободного от государственных границ. Сформировался набор норм в области ответственного поведения государств в ИКТ-среде, закреплённых в документах ООН, региональных организаций и иных международных форумов. Однако направления их развития и практического применения остаются предметом межгосударственной дискуссии, ввиду высокой значимости данной проблемы и различий в интересах и подходах государств.

Ключевые слова: цифровая дипломатия, кибердипломатия, фрагментация интернета, правила ответственного поведения, Россия, США

УДК: 327.8

Поступила в редакцию: 07.10.2022 г.

Принята к публикации: 02.12.2022 г.

Цифровые технологии широко использовались в дипломатической практике начиная с середины 2000-х гг. (Цветкова 2013). Первоначально, акцент в прикладном использовании и осмыслении цифровизации дипломатической практики был сделан на использование социальных сетей в публичной дипломатии (Цветкова 2013; Зиновьева 2013). Особое внимание к цифровой дипломатии было привлечено после событий «арабской весны» (Подберезкин 2016).

Однако по мере развития цифровых технологий менялось и их значение в международной политике и дипломатической практике. На сегодняшний день наметилась возрастающая значимость цифровых технологий и глобального информационного пространства, которые становятся важнейшим ресурсом влияния в современных международных отношениях и полем острейших геополитических противоречий, характеризующихся новым витком борьбы за глобальное лидерство в XXI в. между технологически развитыми державами (Danilin 2020; Allison 2021). Цифровые инструменты и социальные сети становятся каналом для формирования внешнеполитических нарративов и полем информационного противоборства (Nye 2021). В условиях, когда цифровое пространство милитаризируется, и использование цифровых инструментов становится важнейшим элементом межгосударственного противоборства, для дипломатов и дипломатических ведомств становится важным не столько использовать социальные сети для донесения информации до широкой международной аудитории, сколько формировать правила, управляющие цифровым пространством как таковым.

Фокус в исследованиях влияния цифровизации на дипломатию смещается с вопросов использования цифровых инструментов в публичной дипломатии на более широкий круг проблем управления глобальным цифровым пространством, выработки норм ответственного поведения государств в ИКТ-среде (Riordan 2019; Attatfa, Renaud, De Paoli 2020). Прежде всего, выработка норм осуществляется для обеспечения безопасного развития цифровой сферы и снижения напряженности в межгосударственных отношениях в данной области (Крутских 2022).

В настоящей статье кибердипломатия исследована с позиций теории жизненного цикла норм (Finnemore, Sikkink 2019). Проблематика применимости норм к управлению цифровым пространством и обеспечению его безопасности привлекает внимание российских и зарубежных исследователей уже достаточно давно (Finnemore, Hollis 2016; Rusinova 2022; Streltsov, Krutskikh 2020), однако – преимущественно с позиций применимости международного права к информационной сфере. Настоящая статья рассматривает нормы как социальные конструкты, которые могут изменяться по мере развития объекта управления и при этом отражают совпадающие ожидания акторов относительно объекта регулирования и одобряемых стандартов поведения. Цифровое пространство не отличается существенным образом от других объектов регулирования

с точки зрения этапов жизненного цикла норм и проблематики их практической имплементации (Finnemore, Hollis 2016).

В рамках данной статьи использован конструктивистский взгляд на международные нормы, которые представляют собой нематериальные факторы, влияющие на поведение субъектов международных отношений и международную структуру (Бакалова 2015). Согласно теории жизненного цикла норм, нормы проходят три этапа: зарождение норм, каскадное распространение норм, интернализация норм (Finnemore, Sikkink 1998: 895). На первом этапе нормы выдвигаются для обсуждения «нормативными антрепренёрами»; в случае если они нашли поддержку, нормы институционализируются на втором этапе каскадного распространения норм. На третьем этапе интернализации они воспринимаются как должное всеми членами международного сообщества. Как представляется, в настоящее время нормы в отношении цифрового пространства и цифровой дипломатии находятся на этапе обсуждения и зарождения. При этом, как отмечают исследователи (Rusinova 2022), выбор может быть сделан как в пользу правовой неопределённости, так и в пользу движения в сторону нормативного регулирования в данной области. Важным шагом на пути каскадного распространения норм в данной области видится принятие международного документа в рамках ООН, который мог бы придать данным нормам обязательную юридическую силу.

Фрагментация информационного пространства интернета как актуальная тенденция цифровых международных отношений

Протекционизм, пандемия, санкционные войны и нарастающая международная конфликтность способствуют сворачиванию процессов глобализации, как она формировалась и осмысливалась начиная с 1980-х гг.¹. Схожая динамика наблюдается и в информационном пространстве. Видение глобального интернета, в котором нет государственных границ, характерное для 1990-х – 2000-х гг., не оправдало себя. Государства и региональные организации проводят практику «огораживания» и выделения национальных и региональных сегментов глобальной сети. Особенно заметным является пример Китая, где с 1996 г. ведётся политика по укреплению цифрового суверенитета, символом и прикладным воплощением которой является Великий китайский файрвол. На уровне ЕС в последние годы также активизируются инициативы, направленные на формирование технологического и цифрового суверенитета на уровне региона².

¹ Толстухина А. Технологический суверенитет ЕС и его границы. *Валдайские записки*. №119. 07.10.2022. (дата обращения: 18.08.2024).

² Там же.

В России стоит задача обеспечения цифрового суверенитета и укрепления технологической независимости страны³.

Фрагментация интернета, однако, не носит абсолютного характера (Зинovieва 2022). Более того, многие государства заявляют о том, что суверенизация не означает закрытости. Как отмечает директор ДВП МИД России А.Ю. Дробинин, суверенизация возможна «при открытости к самому широкому взаимобогащающему равноправному международному сотрудничеству» (Дробинин 2022). Схожие подходы представлены и на уровне ЕС. Еврокомиссар по внутреннему рынку Т. Бретон отмечает, что стратегическая автономия и цифровой суверенитет ЕС «не предполагает протекционизма ... и самоизоляции»⁴.

Многие цепочки поставок на глобальном уровне сохраняют свою связность и играют важную роль в формировании не только глобальной инфраструктуры интернета, но и программного обеспечения и контента. Возрастают и объёмы трансгранично передаваемых данных. Таким образом, в современном цифровом пространстве сочетаются взаимозависимость на инфраструктурном и технологическом уровне с нарастающей фрагментацией и конфликтностью (Зинovieва 2022). Однако взаимозависимость становится и фактором конфронтации: цифровые технологии и, прежде всего, данные становятся новым полем для геополитических противоречий.

Растущая значимость цифровых технологий в сфере международной политики и конфликтов объясняется, прежде всего, их значимостью с точки зрения охвата по количеству пользователей, масштабам использования и степени проникновения во все сферы жизни общества и государства. Охват цифровых технологий беспрецедентен. На конец 2021 г. доступ к интернету имело порядка 66% населения планеты⁵. Существенно возросла популярность социальных сетей: 53,6% населения Земли или 4,2 млрд чел. имеют аккаунты в одной или нескольких социальных сетях, что больше показателей за 2020 г. на 13%. К концу 2021 г., в среднем люди проводили онлайн порядка семи часов в день на различных платформах и сервисах⁶. Социальные сети стали одним из важнейших источников новостей и информации. Их использование определяет то, как люди общаются, работают и совершают покупки и получают услуги. В среднем по миру люди проводят больше времени, просматривая новости в социальных сетях, чем передачи по телевидению⁷.

³ Цифровой суверенитет. Восточный экономический форум. *Росконгресс*. 2021. URL: <https://roscongress.org/sessions/eef-2021-tsifrovoy-suverenitet/translation/#> (дата обращения: 18.08.2024).

⁴ EU strategic autonomy 2013–2023: From concept to capacity. *European Parliament*. URL: [https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2022\)733589](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733589) (accessed 18.08.2024).

⁵ Internet usage and population statistics. URL: <https://www.internetworldstats.com/stats.htm>

⁶ Digital 2021: главная статистика по России и всему миру. *ExLibris*. URL: <https://exlibris.ru/news/digital-2021-glavnaya-statistika-po-rossii-i-vsemu-miru/> (дата обращения: 18.08.2024).

⁷ Digital 2021: global overview report. *Datareportal*. URL: <https://datareportal.com/reports/digital-2021-global-overview-report> (accessed 18.08.2024).

Однако цифровизация не ограничивается сферой общения и новых медиа. Цифровые технологии широко используются во всех сферах жизни общества и государства, в государственном управлении, финансовых институтах, в промышленности и др. Послы при ООН используют мессенджеры для координации голосования по различным вопросам на повестке дня организации, а пресс-атташе государств при международных организациях публикуют информацию о международных договорённости на своих страницах в социальных сетях и используют их для общения с журналистами (Manor 2019). Цифровая дипломатия применялась во время переговоров по ядерной сделке с Ираном в 2013–2015 гг. (Duncombe 2018), после воссоединения Крыма с Россией в 2014 г. (Bjola Pamment 2018), а затем во время пандемии COVID-19 (Bramsen, Nagemann 2021). Весной 2020 г. был проведён ряд виртуальных встреч на высшем уровне с использованием средств видео-конференц-связи лидеров «Группы двадцати», ООН, БРИКС.

В силу того, что цифровые технологии столь популярны и широко распространены, они всё чаще используются в противоправных целях, актуализируются угрозы информационной безопасности как на уровне государств, так и на международном уровне. Важнейшим вызовом цифровой сферы стал фактор фейковых новостей, под которым понимается широкое распространение недостоверной информации. В 2020 году ВОЗ даже предложила специальный термин «инфодемия», поскольку в социальных сетях распространяется очень много недостоверной информации о происхождении и лечении вируса. Среди пользователей социальных сетей утрачивается доверие к информации и размывается граница между правдой и ложью. Данный феномен получил название «постправды». Следствием становится феномен усталости от социальных сетей, когда пользователи сокращают время их использования и объём размещаемого контента⁸. В этих условиях снижается также и эффективность цифровой дипломатии, дипломаты вынуждены искать новые возможности и направления деятельности в данной сфере.

Нарастающая международная конфликтность способствует тому, что цифровые технологии становятся инструментом межгосударственного противоборства, а также широко используются транснациональными преступными и террористическими организациями. Интернет и социальные сети рассматриваются не как пространство сотрудничества, а как поле для международной конфликтности и конкуренции, важный стратегический ресурс и инструмент воздействия на противников и оппонентов. Данные тенденции находят отражение в официальных документах ведущих государств и научных работах.

⁸ Public diplomacy 3.0: mapping the next stages of tech disruption. 2022. *USC Center on Public Diplomacy*. URL: <https://uscpublicdiplomacy.org/event/public-diplomacy-30-mapping-next-stages-tech-disruption> (accessed 18.08.2024).

США⁹ и страны НАТО рассматривают ИКТ среду как новое поле боя, наряду с сушей, морским и воздушным пространствами и космосом¹⁰. В 2010 г. США объявили о создании кибервойск. Намети́лась милитаризация ИКТ-среды, и такого рода инструменты создаются в структурах вооружённых сил многих государств. В Стратегии национальной безопасности Российской Федерации от 2021 г. отмечается, что «информационное пространство активно осваивается как новая сфера ведения военных действий», при этом Россия ставит своей задачей мирное развитие глобальной ИКТ-среды.

Согласно докладу Совета по международным делам США от 2022 г., «американское видение интернета как открытой, надёжной и безопасной глобальной сети не реализовано и вряд ли когда-либо будет реализовано. Сегодня интернет менее свободен, более фрагментирован и менее безопасен» (Segal, Goldstein 2022: 8). «Балканизация интернета», «фрагментация интернета», «расколотый интернет» – такие термины используются в прессе и в академической литературе для обозначения нового качества международного информационного пространства.

Дипломатия адаптируется к изменяющейся геополитической реальности и к новому качеству информационного пространства, которое характеризуется фрагментацией и возросшей конфликтностью. Управление цифровой неопределённостью, выработка правил, регулирующих современную цифровую сферу становятся важнейшими задачами кибердипломатии Российской Федерации и всех современных государств, а также международных организаций. Кроме того, важнейшим направлением кибердипломатии остаётся использование социальных сетей для решения других внешнеполитических задач, в том числе в рамках цифровой публичной дипломатии и воздействия на глобальную информационную повестку.

От цифровой дипломатии к кибердипломатии: эволюция внешнеполитической практики и академического дискурса

Как правило, зарождение практики цифровой дипломатии связывают с опытом США. В 2006 г. в Государственном департаменте была создана специализированная структура Digital Outreach Team, которая занималась продвижением позитивного образа США в блогосфере и социальных сетях. Впоследствии аналогичные структуры стали создаваться во внешнеполитических ведомствах ряда государств. Россия существенно активизировала свои усилия на данном

⁹ US Department of Defense Cyber Strategy. 2018. *US Department of Defense*. URL: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF (accessed 18.08.2024).

¹⁰ Warsaw Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016. *NATO*. URL: https://www.nato.int/cps/en/natohq/official_texts_133169.htm (accessed 18.08.2024).

направлении в 2012 г., и сегодня по ряду показателей входит в число государств-лидеров (Зиновьева 2013).

Первоначальная популярность цифровых инструментов в дипломатической работе была обусловлена их диалоговым характером, что позволяло создавать и поддерживать долгосрочные интерактивные отношения с зарубежной аудиторией, получать обратную связь и корректировать внешнеполитические нарративы, отталкиваясь от предпочтений и особенностей целевой аудитории. Участники коммуникации не просто получали информацию, они её комментировали, редактировали и распространяли среди своих подписчиков, что существенно меняло традиционную практику дипломатии (Bjola, Zaiotti 2020).

В академической литературе начало исследований в области цифровой дипломатии приходится на начало 2010-х гг. В научных работах цифровая дипломатия понималась как использования социальных сетей для взаимодействия с зарубежной массовой аудиторией. Яркий пример успешной цифровой дипломатии, ориентированной на формирование диалога, работа российского посольства в Великобритании в конце 2010-х гг., которое активно использовало юмор, иронию и затрагивало вопросы, волнующие британское общество в своих аккаунтах в социальных сетях, что позволило получить широкую популярность и отклики среди аудитории в Великобритании и ЕС. В начале 2010-х гг. США на внешнеполитическом уровне активно продвигали дискурс о свободном интернете¹¹, выступая в роли нормативного антрепренёра в данной области.

По мере развития цифровой дипломатии подходы к исследованию данной проблематики эволюционировали. Первоначально исследовательское внимание было сфокусировано на особенностях адаптации МИДов к цифровым технологиям и социальным медиа (Manor 2015), а также к особенностям взаимодействия дипломатов и политических лидеров с широкой международной аудиторией посредством социальных сетей (Tsvetkova 2013). К. Бйола выделил два этапа цифровизации дипломатии: первый ориентирован на проблемы, а второй на нарративы (Bjola 2020). На первом этапе дипломаты открывали аккаунты в социальных сетях, а также освещали различные темы международной повестки в социальных медиа. На втором этапе дипломаты стремились выстроить долгосрочную стратегию использования социальных сетей не вокруг какой-то отдельной проблемы, но в целях долгосрочного цифрового влияния и формирования определённых нарративов (в США данный подход получил название «стратегической коммуникации»).

Научная мысль концентрировалась на том, как сформировать нужную информационную повестку в социальных медиа и вовлечь в неё целевую аудиторию

¹¹ См. напр.: International Strategy for CyberSpace US Department of State. *The White House. President Barack Obama*. May, 2011. URL: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (accessed 18.08.2024).

(Цветкова 2015). Так, например, Илон Манор выделяет две стратегии цифровой публичной дипломатии (Manor 2015):

1. Взаимодействие с лидерами мнений и иными заметными фигурами в глобальном цифровом пространстве.
2. Взаимодействие с «цифровыми привратниками» – крупными цифровыми информационными платформами.

В 2010-х также сложился ряд теоретических концепций, объясняющих тенденции и концептуализирующих опыт цифровизации дипломатии, в частности, отмечалась значимость цифровой дипломатии как инструмента «мягкой силы» (Манор, Захарна, Мелиссен 2015). При этом в российской академической литературе концептуализация цифровой дипломатии как «мягкой силы» никогда не пользовалась существенной популярностью (Цветкова 2013). Сама категория «мягкой силы» ориентирована на расширение аналитического поля реализма, что позволяет говорить о традиционных сферах сотрудничества в цифровой среде в терминах силы, свойственных анализу конфронтации. Именно через призму национальных интересов трактовалась роль цифровой дипломатии в «цветных революциях» и «арабская весна» 2011 г., использование США инструментов «мягкой силы» в социальных медиа в рамках информационного противоборства (Зиновьева 2013). Однако в западной академической литературе, в отличие от российской, видение интернета как открытого и свободного пространства практически не оспаривалось.

Во второй половине 2010-х гг. под влиянием событий «арабской весны» изменяется практика цифровой дипломатии и, как следствие исследовательская повестка. Появилось значительное количество публикаций, которые осмысливали цифровую дипломатию в терминах информационной войны и межгосударственного противоборства (Подберёзкин 2016). При этом также отмечалось растущее вовлечение негосударственных акторов, в том числе международных организаций, в практику цифровой дипломатии (Duncombe 2019). Исследователи фиксировали растущую конфликтность дискурса в социальных сетях (Tsvetkova 2020). Это предоставляется серьёзным вызовом национальной и международной безопасности в силу того, что цифровизация международных переговоров привела к тому, что общественное мнение стало оказывать большее влияние на ход международных переговоров. Для расширения аудитории дипломаты также вынуждены активно делиться информацией и раскрывать как можно больше подробностей о результатах и ходе международных переговоров. Так, например, Женевская конференция 2014 г. в режиме онлайн освещалась дипломатами, сидевшими за столом переговоров.

Растущую открытость переговорной практики оценивали неоднозначно, дискурс об открытости дипломатии не способствовал продвижению нормы об открытом интернете, свободном от государственных границ, поддерживаемой США. Рост внимания общественности к международным переговорам зачастую оказывает давление на дипломатов и не способствует выработке

взаимоприемлемых решений. Кроме того, публичность способствует конкуренции за внимание и, как следствие, может способствовать выбору весьма рискованных переговорных стратегий. Так, в 2018 г. Президент США Д. Трамп и глава Северной Кореи Ким Чен Ын в преддверии двусторонних переговоров о денуклеаризации Корейского полуострова публично обменялись угрозами и оскорблениями в своих аккаунтах в сети Twitter. Фактически оба президента заявили о возможности применения ядерного оружия. Угрозы не были приведены в действие, но эта ситуация создала опасный прецедент эскалации конфликта между ядерными державами вследствие неосторожных и резких высказываний в социальных сетях.

Визуальное представление и эмоциональное повествование, несомненно, занимают центральное место в возможностях, предоставляемых цифровизацией публичной дипломатии (Bramsen, Hagemann 2021). Важным фактором коммуникации становится характерная для современной цифровой культуры эмоциональная коммодификация – то есть преднамеренное усиление эмоционального содержания в онлайн-дискурсе. Специфика коммуникации в социальных сетях способствует поляризации и радикализации мнений, что в свою очередь сужает пространство для манёвра в ходе международных переговоров и не способствует поиску компромиссов. Цифровая поляризация (термин был предложен Д. Санстейном в 2000 г.) – это результат политики платформ по выявлению предпочтений пользователей с тем, чтобы в их аккаунтах в социальных сетях для них была видна та информация, которая поддерживает их предпочтения или убеждения, а не противоречит им. Подобная политика получила название «пузыря фильтров» и в результате формируются т. н. «эхо-камеры» (Manor 2019).

Таким образом, практика цифровой дипломатии способствует трансформации традиционной дипломатической культуры, которая сочетает традиционные элементы, такие как приверженность протоколу и этикету, церемониальность (в частности, чётко регламентированные процедуры представительства и коммуникации) с новыми цифровыми элементами, для которых характерна существенно большая открытость и динамизм. При этом в контексте международной политики и дипломатии трансформация переговорной культуры без выработки должных правил регулирования чревата снижением эффективности дипломатических усилий. Вкупе с нарастающей конфликтностью цифровой сферы данные тенденции ставили под вопрос продвигаемые во внешней политике США и западном академическом дискурсе идеи о необходимости поддержания открытости и доступности интернета, свободного от государственных границ.

Современными авторами цифровая дипломатия воспринимается не только как инструмент сотрудничества и вовлечения, но и как инструмент давления на оппонентов. Это находит отражение в теориях, в частности, в концепции «острой власти» (Nye 2021) и в работах о диалоговой пропаганде (Цветкова 2020). Важным водоразделом в практике и исследованиях в области цифровой дипломатии стала коронавирусная инфекция. Масштабная цифровизация

вкуче с вынужденной самоизоляцией способствовала ускоренному вовлечению цифровых инструментов в дипломатическую работу и усилила значимость цифровой среды как фактора международной политики. Так, например, в 2020 г. появляется новый термин «зум-дипломатия» для обозначения использования технологий видеосвязи для проведения дипломатических переговоров – программы, которые имитируют реальное общение с пользователем. Они стали востребованы в 2020 г., когда большинство учреждений были перегружены, в том числе международных организаций, а люди нуждались в точной и своевременной информации о характере вируса и ответных мерах.

Однако наиболее значимым фактором стало широкое распространение дипломатии данных, а именно использование технологий аналитики больших данных в рамках дипломатической активности и переговорной практики, в том числе для анализа общественного мнения (Boyd 2020; Цветкова 2020). Этот инструмент активно применяется в арсенале внешней политики разных стран, включая США, Россию, страны Европы, Китай, Иран и др. для фильтрации аудитории, построения информационных кампаний и поиска источников недружественной информации. Кроме того, в современных условиях данные становятся не только инструментом для внешней политики, но и ресурсом в борьбе с остерейшими геополитическими противоречиями, что актуализирует выработку правил управления трансграничными потоками данных на международном уровне (Allison 2021). Кроме того, в цифровую дипломатию привносятся практики, связанные с освоением вновь возникающих цифровых технологий, такие как технологии дополненной реальности, которые дают возможность взаимодействовать с аудиторией не только с помощью текста, но и с помощью визуальных и виртуальных средств коммуникации.

Однако помимо трансформаций на уровне технологий существенные изменения происходят на уровне практики и политических решений в сфере дипломатии, что находит отражение в новой концепции кибердипломатии.

В современных условиях, когда дискурс в социальных сетях становится частью информационного противоборства, наметилась усталость пользователей от социальных сетей: они реже добавляют новый контент, стараются сократить время, проводимое в социальных сетях. Единственным исключением в 2022 г. стали сети «ТикТок» и «Телеграмм», которые позволяют гибко настраивать контент в зависимости от предпочтений пользователей и формировать относительно закрытые сообщества. Однако в целом исследователи отмечают, что эффективность цифровой дипломатии как инструмента воздействия на общественное мнение начинает снижаться, что также подталкивает дипломатов и политиков искать новые форматы использования цифровых инструментов в дипломатической практике. К их числу следует отнести практику кибердипломатии, которая стала также водоразделом не только в академическом дискурсе, но и в выборе нормативного регулирования информационного пространства.

Кибердипломатия в практике современных международных отношений

Фрагментация интернета и растущая конфликтность цифрового пространства оказала влияние на практику цифровой дипломатии и кибердипломатии. Фрагментация подразумевает, что каждая группа или сообщество потребляет информацию в рамках заданных ценностных ориентиров и навязанной повестки. Государства столкнулись с необходимостью обращаться не ко всей аудитории национального государства, а к каждому отдельному сообществу, например, к защитникам прав человека, или патриотам, или противникам вакцинации и проч., причём с разными оценочными суждениями (Цветкова 2022).

Кроме того, в условиях фрагментации и растущей конфликтности глобального цифрового пространства перед дипломатией стоит задача не только выработки и распространения нарративов и смыслов в рамках новых медиа, но и управления цифровым пространством и решения глобальных проблем, порождённых процессами цифровизации. В академической литературе новые подходы к дипломатии получили название кибердипломатии. В самом широком смысле кибердипломатия предполагает использование дипломатических инструментов и мышления для решения проблем, возникающих в связи с международным использованием киберпространства. Риордан (Riordan 2019) разъясняет различие между кибер- и цифровой дипломатией, объясняя, что цифровая дипломатия относится к использованию цифровых инструментов и методов для ведения дипломатии, в то время как кибердипломатия относится к использованию дипломатических инструментов и дипломатического мышления для решения проблем, возникающих в киберпространстве.

Термин «кибердипломатия», предполагает продвижение интересов государства в глобальной ИКТ-среде и включает в себя цифровую дипломатию как составную часть. Однако главный акцент всё же сделан на выработку норм и правил, управляющих цифровым пространством и социальными сетями как одной из его составных частей. Показательно, что в апреле 2022 г. в Государственном департаменте США было создано бюро Цифровой политики и киберпространства, в задачи которого входит координация внешней политики США в области киберпространства и цифровой дипломатии, чтобы поощрять ответственное поведение государств в киберпространстве, защищать целостность и безопасность инфраструктуры интернета, продвигать интересы США¹². В МИД России в 2020 г. был создан Департамент международной информационной безопасности, в задачи которого входит участие в международном сотрудничестве в области выработки правил ответственного поведения государств в глобаль-

¹² Bureau of Cyberspace and Digital Policy. *USA Department of State*. URL: <https://www.state.gov/bureaus-offices/deputy-secretary-of-state/bureau-of-cyberspace-and-digital-policy/> (accessed 18.08.2024).

ном информационном пространстве¹³. При этом вопросами использования социальных медиа в целях продвижения внешнеполитических нарративов занимается Департамент информации и печати МИД России¹⁴.

В самом широком смысле кибердипломатия концептуализируется как двигатель и результат процессов масштабной цифровизации, и поэтому она включает в себя все возможные аспекты, в рамках которых цифровизация пересекается с дипломатической практикой (Pouliot, Cornut 2015). Подобный подход позволяет сместить фокус исследовательского внимания с вопросов эффективности инструментов цифровой дипломатии и востребованных навыков в дипломатической работе в область направления эволюции дипломатической практики в условиях современной цифровой трансформации. Востребованность кибердипломатии обусловлена растущим количеством угроз информационной безопасности. При этом на сегодняшний день на международном уровне отсутствуют международно признанные нормы, регламентирующие развитие и использование цифровых инструментов в рамках внешней политики, межгосударственной конкуренции или противоборства. Именно выработка этих инструментов становится важнейшей задачей современной кибердипломатии, наряду с использованием цифровых инструментов в рамках публичной дипломатии. Таким образом, начался новый цикл норм, и в настоящее время различные государства и негосударственные акторы выступают в роли нормативных антрепренёров, предлагая собственное видение будущих подходов к регулированию фрагментированного интернета.

Нормы необходимы для управления информационным пространством, которое становится всё более конфликтным и фрагментированным. Согласно конструктивистскому взгляду на теорию международных отношений, дискурс и диалог играют важнейшую роль в социальном конструировании мира (Алексеева 2014: 4), в том числе в цифровом пространстве (Finnemore, Hollis 2016). Именно дискурсивную природу международных норм подчёркивают представители данного подхода, причём дискурсивно разрабатываемые нормы управляют поведением акторов, они формируют ожидания относительно приемлемого поведения, таким образом структурируя и упорядочивая международную политику (Finnemore, Sikkink 1998: 894). При этом одной из важных областей исследования остаётся вопрос практической имплементации норм в конструктивизме (Виньо 2020). В российской академической литературе вопросам нормативного регулирования в цифровом пространстве уделяется значительное внимание, в том числе в контексте международно-правовой регламентации глобального цифрового пространства (Русинова 2022).

¹³ В МИД России появился новый департамент по информационной безопасности. 29.10.2019. РБК. URL: <https://www.rbc.ru/rbcfreenews/5e0803f39a79470b8bb249ac> (дата обращения: 18.08.2024).

¹⁴ Департамент информации и печати МИД России. URL: https://www.mid.ru/ru/press_service/dip/ (дата обращения: 18.08.2024).

Россия с 1998 г. выступает с инициативами, направленными на выработку правил ответственного поведения государств в глобальном информационном пространстве. Достижением российской дипломатии стало инициирование и поддержание переговорного процесса под эгидой ООН (сначала в рамках Группы правительственных экспертов (ГПЭ), включавшей в разное время от 15 до 25 государств, затем в рамках Рабочей группы открытого состава (РГОС), объединившей все 193 государства – члена ООН), укрепление диалога по мерам укрепления доверия в ОБСЕ, а также запуск переговоров по линии ШОС, БРИКС, СНГ, АСЕАН, со странами Африканского союза, арабского мира и Латинской Америки.

Во многом благодаря усилиям России и Китая норма уважения государственного суверенитета в ИКТ-среде получила закрепление в ряде документов ООН (Бойко 2021). Важным вкладом в развитие нормативных оснований международной информационной безопасности стало принятие в 2018 г. резолюции ГА ООН «Достижения в сфере информатизации и телекоммуникаций», в которой нашёл закрепление набор из 11 норм и принципов ответственного поведения государств, в том числе «суверенное равенство; разрешение международных споров мирными средствами таким образом, чтобы не подвергать угрозе международный мир и безопасность и справедливость; отказ в международных отношениях от угрозы силой или её применения как против территориальной неприкосновенности или политической независимости любого государства, так и каким-либо другим образом, несовместимым с целями Организации Объединённых Наций; уважение прав человека и основных свобод; невмешательство во внутренние дела других государств»¹⁵. На основании данной резолюции была сформирована Рабочая группа открытого состава ООН по безопасному использованию ИКТ и самих ИКТ, которая приняла итоговый доклад в 2021 г. и продолжила свою работу в формате второго созыва.

Помимо обеспечения международной информационной безопасности (Seagal 2017), дипломаты КНР активно продвигают на международном уровне вопросы управления большими данными.

В свою очередь ЕС также выступает с собственным видением нормативного регулирования в цифровой сфере, которое затрагивает, во-первых, проблемы защиты персональных данных (речь идёт прежде всего, о Регламенте ЕС по защите персональных данных 2016 г., который получил широкое распространение как модельный инструмент для выработки национального законодательства в области защиты персональных данных многих стран мира).

В 2021 г. ООН выступила с инициативой Глобального цифрового договора, который также призван упрочить лидерство западных ИТ-гигантов, подменяя

¹⁵ A/RES/73/27 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Генеральная ассамблея ООН. 2018.

выработку правил ответственного поведения государств правилами для ИТ-бизнеса, не предполагающими возможностей контроля исполнения. В этих условиях российские инициативы, направленные на мирное развитие информационного пространства, уважение государственного суверенитета, недопущения использования силы или угрозы силой в цифровой среде, представляются чрезвычайно востребованными. Если не будет сформирован режим международной информационной безопасности, высока вероятность эскалации киберпротиворечий и столкновения с применением кинетического оружия или оружия массового поражения. В этих условиях важно сохранять возможности для диалога, создавать условия для сотрудничества на взаимовыгодных и взаимоприемлемых условиях со всеми странами мира.

В 2022 г. диалог по проблемам международной информационной безопасности на площадке ООН сталкивался с определёнными сложностями. В ходе работы Генеральной Ассамблеи ООН в 2022 г. были приняты две резолюции по проблемам международной информационной безопасности.

Российская Федерация при поддержке дружественных стран внесла резолюцию «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», развивающую более ранние инициативы России и ориентированную на поддержку РГОС как основного механизма в рамках ООН по выработке правил ответственного поведения государств в глобальном информационном пространстве. Универсальный инклюзивный и демократичный характер РГОС обуславливает поддержку данного механизма со стороны международного сообщества. США в свою очередь присоединились к инициативе Франции о создании в ООН Программы действий по поощрению ответственного поведения государств в киберпространстве, которая также была поддержана Генеральной Ассамблеей ООН. Программа действий по поощрению ответственного поведения государств в киберпространстве изначально была предложена Францией и Египтом в 2018 г., однако в то время не получила поддержки. Согласно принятой в 2022 г. резолюции, данная Программа действий должна начать работу с 2025 г. и стать постоянно действующим переговорным механизмом, направленным на практическое воплощение в жизнь правил ответственного поведения государств, согласованных в рамках РГОС.

При этом в странах Запада приходит понимание того, что нормы действуют только в отношении союзников, как отмечается в докладе Совета по международным делам от 2022 г., в условиях, когда США становятся более уязвимыми, а соперники, прежде всего, Китай (Danilin 2022) и Россия (Бойко 2021) бросают вызов лидирующему положению США в глобальном информационном пространстве, необходимо распространять действия норм только на союзников, при этом активно проводить политику сдерживания, односторонних ограничительных мер (санкций) и упреждающих киберопераций в отношении противников, распространяя на них действие только норм, определяющих допустимые пределы военно-политического использования ИКТ (Seagal 2022). Именно с этим

связано стремление закрепить практику политической атрибуции кибератак как норму в цифровом пространстве (Finnemore, Hollis 2020). Россия же настаивает на необходимости юридической атрибуции кибератак и недопустимости огульных обвинений, в частности с тем, чтобы повысить доверие между государствами в глобальном информационном пространстве¹⁶.

В апреле 2022 г. администрация Байдена вместе с 61 страной выпустила Декларацию будущего интернета. Её цель – поддержание интернета открытым, свободным, взаимозависимым, безопасным и надёжным. При этом, в числе угроз безопасности интернета обозначена информационная политика так называемых авторитарных государств, которые запрещают доступ к глобальным онлайн платформам и цифровым инструментам. Нельзя не принять во внимание и незначительное число сторонников данного документа США, их менее трети всех государств – членов ООН. Следует отметить, что это лишь одна из последних, но единственная инициатива, ориентированная на распространение западных ценностей на глобальное цифровое пространство. В их числе Парижский призыв к доверию и безопасности в киберпространстве от 2018 г.¹⁷, Программа действий по продвижению ответственного поведения государств в киберпространстве, предложенная Францией и Египтом в 2020 г.¹⁸ и ряд других инициатив, в том числе исходящих от частного сектора. При этом следует отметить, что частные инициативы и инициативы НКО, как правило, идут «в фарватере» государственных и нацелены на продвижение схожих по содержанию нормативных оснований для регулирования глобального цифрового пространства¹⁹.

Дальнейшие перспективы переговорного процесса остаются открытыми. Российская Федерация выступает в поддержку согласования международного договора или конвенции по информационной безопасности. США, в свою очередь, предпочитают проводить политику «выбора удобных норм» и «выбора удобных институтов», поддерживая выработку норм в числе союзников.

Международные отношения как система всё больше становятся цифровыми. При этом цифровые международные отношения уже вошли в эпоху, когда угрозы международной безопасности становятся столь значимыми, что их необходимо регулировать для обеспечения международной безопасности в целом. Как представляется, выработка подобных правил должна быть основана

¹⁶ См. напр.: Число опасных кибератак на объекты в РФ выросло в 11 раз за три года. Интервью с О.В. Храмовым. *Российская газета*. 14.08.2019. URL: <https://rg.ru/2019/08/14/chislo-opasnyh-kiberatak-na-obekty-v-rf-vyroslo-v-11-raz-zatrigoda.html> (дата обращения: 18.08.2024).

¹⁷ Paris call for trust and security in cyberspace. 2018. URL: <https://pariscall.international/en/> (accessed 18.08.2024).

¹⁸ Program of Action for Trust and Security in Cyberspace. 2020. *Front.un-arm.org*. URL: <https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-future-of-cyber-discussions-at-un-10-08-2020.pdf> (accessed 18.08.2024).

¹⁹ См. напр.: A Digital Geneva Convention to protect cyberspace. Microsoft, policy papers. 2015. *Microsoft*. URL: <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH> (accessed 18.08.2024).

на принципах и нормах международного права, зафиксированных в Уставе ООН²⁰ и Декларации о принципах международного права²¹, прежде всего, равноправии государств и уважении государственного суверенитета. Однако усилий России без поддержки международного сообщества в выработке норм ответственного поведения недостаточно, для этого необходима согласованное видение на уровне ООН и других международных организаций.

Отталкиваясь от теории жизненного цикла норм, можно сделать вывод, что на современном этапе основные нормы уже сформулированы и представлены в докладах ГПЭ ООН²² и резолюциях ГА ООН. Данные нормы проистекают из Устава ООН и основополагающих норм и принципов современного международного права. Однако, государства придерживаются различных взглядов относительно перспектив развития, уточнения и имплементации норм. Действительно, нормы представляют собой гибкие социальные конструкторы (Алексеева 2022) и способны адаптироваться к изменениям международной политики. Российская дипломатия ориентируется на то, что в будущем, исходя из специфики ИКТ может потребоваться выработка новых норм, что нашло отражение в итоговых докладах групп правительственных экспертов и Рабочей группы ООН по международной информационной безопасности²³.

Однако отсутствие правового закрепления и институционализации норм, что может быть осознанным выбором государств, создаёт небезопасную ситуацию. Во многом сложившаяся ситуация обусловлена расхождением в позициях и взглядах государств, охарактеризованных выше, на области применения и сферу действия норм ответственного поведения государств в ИКТ-среде. При этом важно, чтобы существующие нормы, особенно востребованные в условиях масштабной трансформации международного порядка, способствовали укреплению международной безопасности в цифровом мире. Решение можно найти в поэтапном переходе от нормотворческого к правотворческому пути. Уже выработанные нормы, правила и принципы ответственного государственного поведения позволяют осуществить этот сдвиг (Rusinova 2022: 62). Для достижения данной задачи необходимо законодательное закрепление данных норм и принятие Конвенции ООН по международной информационной безопасности, впервые предложенной Россией в 2011 г. (Бойко 2021) и представленной

²⁰ Устав ООН. Вступил в силу 24 октября 1945 г. ООН. URL: <https://www.un.org/ru/about-us/un-charter/full-text> (дата обращения: 18.08.2024).

²¹ Декларация о принципах международного права, касающихся дружественных отношений и сотрудничества между государствами в соответствии с Уставом Организации Объединённых Наций Принята резолюцией 2625 (XXV) Генеральной Ассамблеи ООН от 24 октября 1970 г. ООН. URL: https://www.un.org/ru/documents/decl_conv/declarations/intlaw_principles.shtml (дата обращения: 18.08.2024).

²² См. напр.: A/70/174 Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2015 г. и др.

²³ A/76/135 Доклад Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности 2021 г.;

A/70/174 Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2015 г. и др.

в обновлённом варианте в 2021 г. Учитывая гибкую и адаптивную природу норм, вероятно, что в будущем они будут уточняться и развиваться с тем, чтобы в большей мере соответствовать направлениям эволюции и развития ИКТ, в том числе в вопросах управления данными и обеспечения цифрового суверенитета.

Об авторе:

Елена Сергеевна Зиновьева – доктор политических наук, профессор кафедры мировых политических процессов, заместитель директора Центра международной информационной безопасности МГИМО МИД России, 119454 Москва, проспект Вернадского, 76; профессор Департамента международных отношений НИУ ВШЭ, 117437 Москва, ул. Мясницкая, 20. Email: elena.zinovjeva@gmail.com

Конфликт интересов:

Автор заявляет об отсутствии конфликта интересов.

Благодарности:

Исследование выполнено в рамках проекта «Посткризисное мироустройство: вызовы и технологии, конкуренция и сотрудничество» по гранту Министерства науки и высшего образования РФ на проведение крупных научных проектов по приоритетным направлениям научно-технологического развития (Соглашение No 075-15-2020-783).

UDC: 327.8
Received: October 07, 2022
Accepted: December 02, 2022

Cyber Diplomacy under Increased Competition Between the Great Powers

E.S. Zinovieva^{1, 2}
[DOI 10.24833/2071-8160-2022-olf5](https://doi.org/10.24833/2071-8160-2022-olf5)

¹ MGIMO – University

² HSE University

Abstract: The fragmentation of the Internet, which has replaced information globalization, is becoming a new reality. Digital technologies and the Internet are becoming a field of new geopolitical contradictions and a struggle for leadership between the great powers. Cyber diplomacy, which includes a range of issues of using ICT to achieve the foreign policy goals of the state, as well as new problematic and subject areas of international relations arising in connection with digitalization, is the most important tool for interstate competition and conflicts, as well as a means of conducting information wars.

At the international level, there are no internationally recognized norms governing the development and use of digital tools in the framework of foreign policy, interstate competition or confrontation. It becomes especially important to develop rules for the responsible behavior of states in the global information space.

Methodologically, the article is based on the theory of the life cycle of norms. According to this approach, norms are social standards that regulate the behavior of states in a certain area of international relations. At present, there has been a rejection of the norms of the global Internet, which has been promoted by the United States for a long time, free from state borders. A set of norms has been formed in the field of responsible behavior of states in the ICT environment, enshrined in the documents of the UN, regional organizations and other international forums. However, the directions of their development and practical application remain the subject of interstate discussions, in view of the high significance of this problem and the differences in the interests and approaches of states.

Key words: digital diplomacy, cyber diplomacy, Internet fragmentation, rules of responsible behavior, Russia, USA

About the author:

Elena S. Zinovieva – Doctor of Political Science, Professor of the Department of World Political Processes, Deputy Director of the Center for International Information Security, MGIMO-University, 119454 Moscow, Prospekt Vernadskogo, 76; Professor, Department of International Relations, National Research University Higher School of Economics, 117437 Moscow, st. Myasnitskaya, 20. Email: elena.zinovieva@gmail.com

Conflict of interests:

The author declares the absence of conflicts of interests.

Acknowledgements:

The study was carried out within the framework of the project “Post-crisis world order: challenges and technologies, competition and cooperation” under a grant from the Ministry of Science and Higher Education of the Russian Federation to conduct large research projects in priority areas of scientific and technological development (Agreement No. 075-15-2020-783).

References:

- Allison G. et al. 2021. *The Great Tech Rivalry: China vs. the US*. Belfer Center.
- Attatfa A., Renaud K., De Paoli S. 2020. Cyber Diplomacy: A Systematic Literature Review. *Procedia computer science*. Vol. 176. P. 60–69. DOI:10.1016/j.procs.2020.08.007
- Bjola C. 2015. Introduction: Making Sense of Digital Diplomacy. *Digital Diplomacy*. Routledge. P. 15–24.
- Bjola C., Pamment J. 2018. Introduction: the ‘Dark Side’ of Digital Diplomacy. *Countering Online Propaganda and Extremism*. Routledge. P. 1–10.
- Bjola C., Zaiotti R. 2020. Going Digital: Choices and Challenges for International Organisations. *Digital Diplomacy and International Organisations*. Routledge. P. 1–18.
- Boyd A. et al. 2019. Data Diplomacy. *Science & diplomacy*. 8(1).
- Bramsen I., Hagemann A. 2021. The Missing Sense of Peace: Diplomatic Rapprochement and Virtualization During the COVID-19 Lockdown. *International Affairs*. 97(2). P. 539–560. DOI: 10.1093/ia/iaa229
- Creemers R. 2020. China’s Conception of Cyber Sovereignty. *Governing cyberspace: Behavior, power and diplomacy*. P. 107–145.
- Creemers R. 2022. China’s Emerging Data Protection Framework. *Journal of Cybersecurity*. 8(1).
- Danilin I. V. 2022. The US-China Tech War: A Dawn of New Geopolitics? *Technological Innovation and Security: The Impact on the Strategic Environment in East Asia*.

- Duncombe C. 2018. Twitter and the Challenges of Digital Diplomacy. *SAIS Review of International Affairs*. 38(2). P. 91–100. DOI:10.1353/SAIS.2018.0019
- Finnemore M., Hollis D. 2020. B. Beyond Naming and Shaming: Accusations and International Law in Cybersecurity. *European Journal of International Law*. 31(3). P. 969–1003. DOI:10.1093/ejil/chaa056
- Finnemore M., Hollis D.B. 2016. Constructing Norms for Global Cybersecurity. *American Journal of International Law*. 110(3). P. 425–479. DOI:10.1017/S0002930000016894
- Finnemore M., Sikkink K. 1998. International Norm Dynamics and Political Change. *International organization*. 52(4). P. 887–917.
- Krutsikh A.V., Streltsov A.A., Tikk E. 2020. International Information Security: Problems and Ways of Solving Them. *Routledge Handbook of International Cybersecurity*. Routledge. P. 260–268.
- Manor I. 2019. *The Digitalization of Public Diplomacy*. New York: Springer International Publishing.
- Melissen J., Hocking B. 2015. *Digital Diplomacy in the Digital Age*. Netherlands Institute of International Relations Clingendael. URL: https://www.researchgate.net/publication/309012711_Digital_Diplomacy_in_the_Digital_Age
- Nye J. S. 2021. Soft Power: the Evolution of a Concept. *Journal of political power*. 14(1). P. 196–208. DOI: 10.1080/2158379X.2021.1879572
- Pouliot V., Cornut J. 2015. Practice Theory and the Study of Diplomacy: A Research Agenda. *Cooperation and conflict*. 50(3). P. 297–315.
- Riordan S. 2019. *Cyber Diplomacy: Managing Security and Governance Online*. NY: John Wiley & Sons.
- Rusinova V.N. 2022. Standard-setting and Normativity in International Governance of Interstate Relations in the Information and Communication Technologies. *Context Legal Issues in the Digital Age*. 3(1). P. 61–80. DOI: 10.17323/2713-2749.2022.1.61.80
- Segal A. 2017. Chinese Cyber Diplomacy in a New Era of Uncertainty. *Hoover Institution, Aegis Paper Series*. Vol. 1703. P. 1–23.
- Segal A., Goldstein G.M. 2022. Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet. *Council on Foreign Relations*. URL: <https://www.cfr.org/report/confronting-reality-in-cyberspace>
- Taillat S. 2017. L'impact du numérique sur les relations stratégiques internationales. *Stratégique*. №117. P. 137–153. (In French)
- Thakur R., Cooper A.F., Heiner J. et al. 2013. Introduction: the challenges of 21st-century diplomacy. *The Oxford handbook of modern diplomacy*. Oxford University Press.
- Tsvetkova N. 2020. Russian Digital Diplomacy: A Rising Cyber Soft Power? *Russia's Public Diplomacy*. Palgrave Macmillan, Cham. P. 103–117. DOI: 10.21638/spbu06.2022.204
- Alekseeva T.A. 2014. Myslit' konstruktivistski: otkryvaja mnogogolosyj mir [Constructivists Analysis: Discovering a Polyphonic World]. *Sravnitel'naja politika*. 1(14). P. 4–21. DOI: 10.18611/2221-3279-2014-5-1(14)-4-21 (In Russian)
- Alekseeva T.A. 2022. Agent-strukturnye otnoshenija: metodologija konstruktivizma [Agent Structure Relationship: Methodology of Constructivism] *Polis: Politicheskie issledovanija*. №4. DOI: 10.17976/jpps/2022.04.07 (In Russian)
- Bakalova E.V. 2015. Konstruktivizm v issledovanii mezhdunarodnyh norm zashchity prav cheloveka ot genezisa, priznaniya i sobljudenija k narusheniju, osparivaniju i jerozii [Constructivists Analysis of the International Human Rights Norms: Genesis, Admission and Implementation, Contestation and Erosion] *Mezhdunarodnye processy*. 13(1). P. 48–67. (In Russian)

Bojko S.M. 2021. Politiko-pravovye predposylki sistemy mezhdunarodnoj informacionnoj bezopasnosti [Legal and Political Foundation of the International Information Security System] *Mezhdunarodnye processy*. 4(67). P. 6–25. (In Russian)

Drobinin A. Ju. 2022. Uroki istorii i obraz budushhego: razmyshleniya o vneshnej politike Rossii [History Lessons and the Image of the Future: Reflections on the Foreign Policy of Russia]. *Mezhdunarodnaja zhizn'*. №8. P. 1–15. (In Russian)

Krutskih A. V. 2022. Mezhdunarodnaja informacionnaja bezopasnost': v poiskah konsolidirovannyh podhodov [International Information Security: In Search of the Consolidated Approaches]. *Vestnik Rossijskogo universiteta družby narodov. Serija: Mezhdunarodnye otnosheniya*. 22(2). P. 342–351. (In Russian)

Podberjzkin A. I. 2016. Voennaja sila i politika novoj publichnoj diplomatii [Military Power and New Public Diplomacy] *Nauchno-analiticheskij zhurnal Obozrevatel'-Observer*. 12(323). P. 15–25. (In Russian)

Rusinova V. 2014. Teorii sootnosheniya norm mezhdunarodnogo gumanitarnogo prava i mezhdunarodnogo prava prav cheloveka [Theories of Relationship between the Norms of International Humanitarian Law and International Human Rights Law]. *Pravo. Zhurnal Vysshey shkoly ekonomiki*. №1. P. 43–56 (in Russian)

Tsvetkova N. 2015. Publichnaja diplomatija SShA [USA Public Diplomacy]. *Mezhdunarodnye processy*. 13(3). P. 121–133. (In Russian)

Tsvetkova N.A., Jarygin G.O. 2013. Politizacija «cifrovoj diplomatii»: publichnaja diplomatija Germanii, Irana, SShA i Rossii v social'nyh setjah [Politization of Digital Diplomacy: Public Diplomacy of Germany, Iran, Russia and USA] *Vestnik Sankt-Peterburgskogo universiteta. Politologiya. Mezhdunarodnye otnosheniya*. №1. (In Russian)

Vin'o A. 2020. Vnedrenie norm: ahillesova pjata konstruktivizma? [Norms Implementation: Achilles' Heel of Constructivism?] *MGIMO Review of International Relations*. 13(4). P. 199–215. (In Russian).

Zinov'eva E. S. 2013. Cifrovaja diplomatija SShA: vozmozhnosti i ugrozy dlja mezhdunarodnoj bezopasnosti [USA Digital Diplomacy: Possibilities and Threats for International Security] *Indeks bezopasnosti*. 19(1). P. 213–228. (In Russian)

Zinov'eva E. S. 2022. Formirovanie cifrovyyh granic i informacionnaja globalizacija: analiz s pozicij kriticheskoj geografii [Digital Borders and Information Globalization: Analysis from the Standpoint of Critical Geography]. *Polis: Journal of Political Studies*. №2. DOI: 10.17976/jpps/2022.02.02 (In Russian)

Список литературы на русском языке:

Алексеева Т.А. 2014. Мыслить конструктивистски: открывая многоголосый мир Сравнительная политика. 1(14). С. 4–21. DOI: 10.18611/2221-3279-2014-5-1(14)-4-21

Алексеева Т.А. 2022. Агент-структурные отношения: методология конструктивизма. *Полис: Политические исследования*. №4. DOI: 10.17976/jpps/2022.04.07

Бакалова Е.В. 2015. Конструктивизм в исследовании международных норм защиты прав человека от генезиса, признания и соблюдения к нарушению, оспариванию и эрозии. *Международные процессы*. 13(1). С. 48–67. DOI: 10.17994/IT.2015.13.40.4

Бойко С.М. 2021. Политико-правовые предпосылки системы международной информационно-безопасности *Международные процессы*. 4(67). С. 6–25.

Виньо А. 2020. Внедрение норм: ахиллесова пята конструктивизма? *Вестник МГИМО-Университета*. 13(4). С. 199–215. DOI: 10.24833/2071-8160-2020-4-73-199-215

Дробинин А.Ю. 2022. Уроки истории и образ будущего: размышления о внешней политике России. *Международная жизнь*. №8. С. 1–15.

Зиновьева Е.С. 2013. Цифровая дипломатия США: возможности и угрозы для международной безопасности. *Индекс безопасности*. 19(1). С. 213–228.

Зиновьева Е. С. 2022. Формирование цифровых границ и информационная глобализация: анализ с позиций критической географии. *Полис. Политические исследования*. №2. DOI: 10.22363/2313-0660-2022-22-2-352-371

Крутских А.В. 2022. Международная информационная безопасность: в поисках консолидированных подходов *Вестник Российского университета дружбы народов. Серия: Международные отношения*. 22(2). С. 342–351. DOI: 10.22363/2313-0660-2022-22-2-342-351

Подберёзкин А.И. 2016. Военная сила и политика новой публичной дипломатии. *Научно-аналитический журнал «Обозреватель-Observer»*. 12(323). С. 15–25.

Цветкова Н.А. 2015. Публичная дипломатия США. *Международные процессы*. 13(3). С. 121–133. DOI: 10.17994/T.2015.13.2.42.8

Цветкова Н.А., Ярыгин Г.О. 2013. Политизация «цифровой дипломатии»: публичная дипломатия Германии, Ирана, США и России в социальных сетях. *Вестник Санкт-Петербургского университета. Политология. Международные отношения*. №1.