Международные процессы, Том 21, № 4 (75), сс. 104–132
DOI 10.17994/IT.2023.21.4.75.2

БРИКС В ГЛОБАЛЬНОМ РЕЖИМЕ ИКТ-БЕЗОПАСНОСТИ

ЕЛЕНА ЗИНОВЬЕВА
МГИМО МИД России, Москва, Россия

АЛЕКСАНДР ИГНАТОВ
МГИМО МИД России, Москва, Россия
РАНХиГС, Москва, Россия

Резюме

Глобальное управление в сфере ИКТ-безопасности представляет собой режимный комплекс, который включает в себя совокупность институтов и режимов, регулирующих проблематику безопасности цифровых сетей и технологий, противодействия преступному использованию информационных технологий, военно-политическим угрозам в цифровом пространстве и др. Сосуществование и конкуренция различных режимов позволяют отдельным странам и негосударственным игрокам манипулировать выбором удобных институтов и создают угрозу эскалации межгосударственных противоречий. Для того чтобы избежать подобного сценария, Россия выступает за формирование консолидированного режима информационной безопасности на глобальном уровне. При этом важная роль отводится региональным и макрорегиональным площадкам, в том числе БРИКС. Настоящая статья ставит задачей оценить влияние БРИКС на эволюцию режимного комплекса в сфере ИКТ-безопасности и формирование универсального режима в данной области.

Была исследована повестка БРИКС в области ИКТ-безопасности и определены заявленные обязательства. Для оценки потенциала имплементации достигнутых соглашений были проанализированы документы стратегического планирования стран БРИКС на предмет выявления в них приоритетов в сфере ИКТ-безопасности, которые затем были соотнесены с зафиксированными в официальных документах БРИКС обязательствами и обозначенными перспективными направлениями сотрудничества. Приоритетным направлением сотрудничества БРИКС в сфере ИКТ-безопасности является выработка общей внешнеполитической позиции относительно норм и принципов международного режима ИКТ-безопасности и их продвижение на уровне ООН. Важным преимуществом БРИКС на данном направлении является возможность агрегации интересов и позиций развивающихся стран. Однако в настоящее время в условиях нарастающей международной конфликтности формирование универсального режима представляется практически невероятным. В этом контексте взаимодействие на уровне БРИКС фокусируется на более узких проблемных областях. Наибольшим потенциалом институционализации обладает сотрудничество БРИКС в сфере противодействия терроризму и экстремизму в цифровой среде. Вместе с тем заинтересованность стран БРИКС в развитии и институционализации противодействия

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 № 075-15-2020-783).

Дата поступления рукописи в редакцию: 21.11.2022
Дата принятия к публикации: 07.11.2023

Для связи с авторами / Corresponding author:
Email: zinovjeva@mail.ru

ИКТ-угрозам неоднородна. Россия, Китай и Индия выступают в роли локомотивов сотрудничества, в то время как Бразилия и ЮАР проявляют в нём меньшую заинтересованность.

Ключевые слова:

БРИКС; информационная безопасность; ИКТ-безопасность; цифровая экономика; глобальное управление

Цифровые технологии, среди которых ключевая роль отводится Интернету, проникли во все сферы жизни общества. Интернет, выступая в качестве инфраструктурной основы растущей цифровой экономики [Бухт, Хикс 2018], одновременно является источником угроз безопасности личности и государства [Крутских 2007; Крутских, Стрельцов 2014; Безкоровайный, Татузов 2014; Згоба и др. 2014; Карпова 2014; Малахин, Малахина 2018, Ромашкина 2020].

Важность борьбы с информационными угрозами была зафиксирована в Стратегии национальной безопасности Российской Федерации и в Доктрине информационной безопасности Российской Федерации[1]. Она также фигурирует в схожих по назначению документах ведущих в отношении развитости цифровой экономики международных игроков[2]. В частности, в странах–партнёрах России по БРИКС: Бразилии, Индии, Китае и ЮАР – были приняты документы, закрепившие важность проблематики ИКТ-безопасности на национальном и глобальном уровнях[3].

Значимой темой международной повестки становятся вопросы выработки правил регулирования ИКТ-пространства, обеспечения его безопасного развития. Данной проблематикой занимается ООН[4], однако в 2020-х годах со стороны США и

[1] Указ Президента Российской Федерации от 02.07.2021 №400 «О Стратегии национальной безопасности Российской Федерации». URL: http://www.kremlin.ru/acts/bank/47046 (дата обращения: 11.09.2022); Указ Президента Российской Федерации от 05.12.2016 №646 «Об утверждении Доктрины информационной безопасности Российской Федерации». URL: http://kremlin.ru/acts/bank/41460 (дата обращения: 11.09.2022).

[2] См., например: The EU's Cybersecurity Strategy for the Digital Decade 2020. URL: https://digitalstrategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 (дата обращения: 04.08.2022); White House Interim National Security Strategic Guidance March 2021. URL: https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf (дата обращения: 27.01.2022).

[3] См., например: Política Nacional de Segurança da Informação Brazil 2019. URL: https://www.gov.br/governodigital/pt-br/estrategias-e-politicas-digitais/politica-nacional-de-seguranca-da-informacao (дата обращения: 11.09.2022); National Digital Communications Policy India 2018. URL: https://dot.gov.in/sites/default/files/EnglishPolicy-NDCP.pdf (дата обращения: 11.09.2022); India's National Security Strategy 2019. URL: https://manifesto.inc.in/pdf/national_security_strategy_gen_hooda.pdf (accessed: 11.09.2022); The National Cybersecurity Policy Framework South Africa 2019. URL: https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf (accessed: 11.09.2022); International Strategy of Cooperation on Cyberspace China, 2017. URL: https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/201703/t20170301_599869.html#:~:text=The%20strategic%20goal%20of%20China's,peace%2C%20security%20and%20stability%20in (дата обращения: 11.09.2022); Global Initiative on Data Security, China 2020. URL: https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/202009/t20200908_679637.html (accessed: 18.05.2023).

[4] См., например: Доклад Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности A/68/98 от 24 июня 2013 г. URL: https://namib.online/wp-content/uploads/2020/04/Report-of-the-UN-Group-of-Governmental-Experts-on-Developments-in-the-Field-of-Information-of-24-June-2013.pdf (дата обращения: 11.09.2022); Резолюция ГА ООН 73/27 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» от 5 декабря 2018 г. URL: https://namib.online/wp-content/uploads/2020/04/Developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-UN-GA-Resolution-A7327-on-5-December-2018.pdf (дата обращения: 11.09.2022) и др.

союзников был представлен ряд инициатив, ориентированных на формирование альтернативных режимов вне рамок ООН – в их числе Парижский призыв к доверию в киберпространстве[5], Декларация за будущее Интернета[6]. В сфере противодействия киберпреступности США и их партнёры по НАТО продвигают принятую ещё в 2001 г. Будапештскую конвенцию[7].

Подобные проекты подрывают инклюзивные переговоры по соответствующим темам под эгидой ООН[8]. На глобальном уровне наметилась конкуренция подходов к выработке норм и правил, лежащих в основе регулирования ИКТ-безопасности. Международное сотрудничество в исследуемой области представляет собой режимный комплекс, включающий в себя множество глобальных, региональных, функциональных и транснациональных режимов, зачастую пересекающихся, а в ряде случаев противоречащих друг другу. В отсутствие единых согласованных на международном уровне правил игры мы наблюдаем попытки со стороны ряда государств переложить ответственность за киберинциденты на соперников[9], а также активизацию политического и военного использования ИКТ, что негативно сказывается на международной безопасности. Наличие конкурирующих режимов открывает возможность манипулирования выбором удобных институтов, а также затрудняет возможности контроля взятых на себя государствами обязательств.

Трудности, с которыми сталкивается ООН на современном этапе, обусловливают рост авторитета трансрегиональных институтов управления, к числу которых можно отнести «группу двадцати» и БРИКС [Лебедева, Кузнецов 2019]. Возможность выработки решений по такой комплексной проблематике, как обеспечение ИКТ-безопасности на альтернативных площадках, является востребованной темой для исследования. БРИКС имеет положительное портфолио успешно согласованных решений, сформулированных и реализованных вопреки имеющимся разногласиям между участниками (например, совместными усилиями был учреждён Новый банк развития БРИКС) [Кузнецов 2020]. Изначально созданный как объединение быстрорастущих экономик, современный БРИКС занимается широким кругом вопросов, и его повестка продолжает расширяться [Ларионова и др. 2020]. Отечественный исследователь В. Панова отмечала, что БРИКС делает уверенные шаги в интенсификации взаимодействия в сфере безопасности [2015: 121]. В первую очередь БРИКС обеспечивает координацию внешнеполитических позиций государств по вопросам, связанным с обеспечением международной безопасности. При этом инициативы по формированию институтов к настоящему времени менее успешны [Abdenur 2017: 73].

Страны БРИКС заявляют о принципиальном несовпадении позиций со страна-

[5] Paris Call for Trust and Security in Cyberspace – URL: https://pariscall.international/en/call (accessed: 11.09.2022).

[6] Declaration for the Future of the Internet – URL: https://www.state.gov/declaration-for-the-future-of-the-internet (accessed: 18.05.2023).

[7] The Budapest Convention (ETS No. 185) and its Protocols. URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention (accessed: 18.05.2023).

[8] Выступление Министра иностранных дел России в Совете Безопасности ООН. 20.04.2023. URL: https://www.mid.ru/ru/press_service/video/view/1865243/?TSPD_101_R0=08765fb817ab2000019f48a794223f3ad630c5f6c18894fc02a2a55893b58e8859b2bc1adf9f1fba4089f16b658143000c5ddcd0cd3f040911f2e005d76f69b49bfa9c1626a778f40566660464437cc8a2f04a9708c92f97451d80ad99e4fcc7c (дата обращения: 17.12.2023).

[9] Подразумевается политизация процесса атрибуции киберинцидентов и возможность необоснованных и неподтверждённых обвинений. См., например: США обвинили Россию в кибератаках на украинские банки. URL: https://www.interfax.ru/world/823034 (дата обращения: 29.08.2022); Тайвань обвинил Китай в целенаправленной подготовке вторжения на остров. URL: https://www.mk.ru/politics/2022/08/09/tayvan-obvinil-kitay-v-celenapravlennoy-podgotovke-vtorzheniya-na-ostrov.html (дата обращения: 29.08.2022).

ми Запада по ряду вопросов глобального управления, в том числе и в цифровом пространстве. Объединение в данном контексте может рассматриваться как некая лаборатория для апробации внешнеполитических инициатив группы стран, претендующих на лидерство в глобальном нормотворчестве. Настоящая статья призвана ответить на вопрос о том, какую роль может сыграть БРИКС в формировании глобального режима информационной безопасности в рамках ООН.

Структурно работа состоит из трёх разделов. Мы начинаем с определения базового понятия для рассматриваемой темы – *ИКТ-безопасность*. Рассмотрев сложившиеся подходы к определению предметной области международной информационной безопасности, мы выдвигаем скорректированное определение этого концепта, которое точнее отражает различия между *кибербезопасностью* и *информационной безопасностью*. Оно также соответствует подходу стран БРИКС в данной области. После этого представлены теоретико-методологические основания исследования, а именно: *теория международных режимов* и разработанный исследователями Университета Торонто методологический аппарат, применяемый для выделения, мониторинга и экспертной оценки эффективности выполнения обязательств неформальных институтов глобального управления. Далее мы переходим к исследованию приоритетов стран БРИКС в области ИКТ-безопасности. Мы определяем приоритеты стран–участниц объединения в изучаемой области, сопоставляем их и приходим к выводам относительно их совместимости. Затем мы анализируем многосторонние решения БРИКС. Применяя методологию выделения политически обязательных решений и результаты последующего мониторинга и оценки исполнения коллективных обязательств БРИКС, а также сопоставляя их с выводами второго раздела исследования, мы приходим к заключению о реальных перспективах выработки многосторонних решений в области ИКТ-безопасности в рамках БРИКС и о характере влияния «пятёрки» на формирование глобального режима информационной безопасности.

Понятия «международная информационная безопасность», «кибербезопасность» и «ИКТ-безопасность»

Для исследования роли БРИКС в формировании и эволюции режима ИКТ-безопасности необходимо определиться с терминами, то есть обозначить подход к предмету регулирования исследуемого международного режима. При этом вопросы терминологии в рассматриваемой области – предмет острых международных дискуссий [Зиновьева, Мищишина 2022].

В Основах государственной политики в области международной информационной безопасности Российской Федерации от 2021 г.[10] даётся следующее определение: «Международная информационная безопасность представляет собой такое состояние глобального информационного пространства, при котором на основе общепризнанных норм и принципов международного права и на условиях равноправного партнёрства обеспечивается поддержание международного мира, безопасности и стабильности». Россия исходит из широкой трактовки угроз международной информационной безопасности, куда входят вопросы защиты сетей, систем и данных (информационно-техническая безопасность) и более широкий спектр вопросов контроля контента информационных сетей (политико-идеологическая безопасность). Большинство российских авторов придерживаются схожего подхода к определению угроз и содержания понятия «международная информационная безопасность» [Бойко 2019; Крутских 2022; Зиновьева 2022; Ромашкина 2022].

[10] Указ Президента РФ от 12.04.2021 г. № 213. Основы государственной политики в области международной информационной безопасности. URL: http://www.scrf.gov.ru/security/information/document114/ (дата обращения: 17.12.2023).

Между тем обнаруживается ряд трудностей, связанных с разграничением понятий *информационной безопасности* и *кибербезопасности*[11] – в отдельных отечественных исследованиях они[12] полностью смешиваются и употребляются произвольно, без уточнения методологических различий [Карцхия 2014; Малюк, Полянская 2016; Хабриева, Руйпин 2017; Ромашкина 2020]. Среди российских специалистов только формируется консенсус относительно соотношения предметных областей двух понятий – *кибербезопасность* рассматривается как смысловое подпространство *информационной безопасности* [Кадулин, Клочкова 2017: 7–8]. Большая часть авторов трактует *информационную безопасность* как более широкое понятие по сравнению с кибербезопасностью в полном соответствии с официальной позицией.

Зарубежные исследователи разграничивают рассматриваемые понятия. При этом предметная область *кибербезопасности* в зарубежных работах представляется более широкой по сравнению с *информационной безопасностью*. Работа [von Solms, Niekerk 2013] указывает на общий родовой корень понятий – *безопасность* чего-либо, уточняя, что *кибербезопасность* охватывает более широкий перечень угроз, уязвимостей и активов, являющихся предметом действий по обеспечению безопасности. *Информация* выступает в качестве ключевого охраняемого актива, что подразумевает схожий перечень угроз и уязвимостей, которые в той или иной степени воздействуют на конфиденциальность, целостность и доступность информации. В то же время *кибербезопасность* может затрагивать вопросы охраны личности от целенаправленного вредного воздействия (кибербуллинг), физические активы в распоряжении лица, которые могут пострадать вследствие нарушения *информационной безопасности* (например, выход из строя умной бытовой техники), *критической инфраструктуры* от действий террористов или условного противника [von Solms, Niekerk 2013: 3–4]. Вместе с тем за рамками внимания западных исследователей остаются вопросы безопасности общества и государства в цифровую эпоху, которые формируют важный пласт российской академической литературы на данном направлении.

Международные переговоры по созданию механизма регулирования отношений в ИКТ-среде были предприняты в рамках шести Групп правительственных экспертов ООН по МИБ (далее – ГПЭ) и двух созывов Рабочей группы открытого состава по МИБ ООН (далее – РГОС). Эти наиболее авторитетные площадки согласования многосторонних решений в рассматриваемой области пока не в полной мере оправдали возложенные на них в рамках мандата обязательства – на уровне ООН не было подписано глобального юридически обязательного документа по вопросам обеспечения информационной безопасности, хотя и был сформирован перечень правил ответственного поведения государств в формате «мягкого права». На уровне РГОС и ГПЭ используется компромиссный термин «*безопасность в сфере использования ИКТ и самих ИКТ*» или же более краткая версия, используемая в настоящей работе «*ИКТ-безопасность*». Данная терминология в целом схожа с официальной позицией России и исходит из широкой трактовки угроз безопасности, которые включают как политико-идеологические, так и информационно-технические аспекты. При этом с точки зрения предметных областей безопасности в неё включены вопросы противодействия военно-политическим угрозам (выработка правил ответственного поведения государств в ИКТ-среде), противодействие преступным угрозам, терроризму и экстремизму в цифровом пространстве. В силу того что в российской академиче-

[11] В частности, на это указывает [Массель et al. 2016] при рассмотрении вопросов энергетической безопасности России.

[12] Здесь также следует упомянуть пересечение понятий «информационное оружие» / «кибероружие», «информационное воздействие» / «кибервоздействие» и др.

ской литературе и в официальной позиции значительный акцент сделан на проблемах обеспечения суверенитета в ИКТ-среде и управления цифровым пространством в целом, в проблемное поле ИКТ-безопасности зачастую включаются также вопросы управления Интернетом на международном уровне [Зиновьева 2021; Крутских 2022]. В настоящей работе используется данный термин как компромиссный между различными подходами.

Несмотря на важность рассматриваемой проблематики, мы имеем сравнительно небольшую выборку работ, посвящённых вопросу о выработке решений в области ИКТ-безопасности на площадке БРИКС. Имеющиеся работы зачастую не разделяют понятия *кибербезопасность* и *информационная безопасность*, в результате чего повестка БРИКС в интересующей области представляется излишне обширной. Например, в сферу кибербезопасности, помимо противодействия вирусной угрозе и шпионажу с применением ИКТ [Хабриева, Руйпин 2017: 132], отнесены проблемы культурного взаимодействия между странами–членами объединения и информационного сопровождения государственной политики в международном измерении [Михалевич 2017]. Целесообразнее в сферу ИКТ-безопасности включать только вопросы, напрямую связанные с обеспечением безопасности от угроз в соответствующей области, сохраняя, однако, данную область широкой и включая в неё и вопросы технической безопасности, и вопросы контроля контента, и обеспечения цифрового суверенитета, а также проблематику интернационализации управления Интернетом и противодействия преступному использованию ИКТ.

Таким образом, мы обнаружили ряд проблем, связанных с принятием решений по вопросам ИКТ-безопасности, сразу на нескольких уровнях – от определения предметной области до взаимодействия на уровне многосторонних институтов глобального управления. Ответ на ключевой вопрос исследования – какую роль играет БРИКС в рамках формирования международного режима ИКТ-безопасности и каковы перспективы дальнейшей работы объединения в рассматриваемой области – непосредственно связан с определением предметной области ИКТ-безопасности.

Глобальное управление ИКТ-безопасностью как режимный комплекс

Настоящая работа опирается на теорию международных режимов. Ключевым понятием является *международный режим* как таковой. Наиболее распространённое определение было сформулировано С. Краснером: «Международный режим – это набор явных или неявных принципов, норм, правил и процедур принятия решений, в отношении которых сходятся ожидания тех или иных игроков» [Krasner 1983: 1].

Следует отметить ряд важных моментов. *Во-первых*, участники режимов, к числу которых относятся в первую очередь государства, могут договариваться в условиях международной анархии, и их взаимодействие необязательно должно иметь характер «игры с нулевой суммой». *Во-вторых*, сложившийся и функционирующий международный режим не является статичным явлением. Динамическому изменению могут быть подвержены как интересы сторон, так и состав участников и их восприятие проблемы. *В-третьих*, несмотря на выраженную приоритизацию роли государства в формировании и поддержании международного режима, негосударственные игроки принимаются во внимание.

Р. Кохейн отмечал, что в мировой политике имеется постоянное поле возможностей для формирования международного режима, который может устанавливать ответственность за те или иные противоправные действия, содействовать распространению более достоверной и полной информации или снижать сопутствующие издержки международного взаимодействия [Keohane 1982: 338].

В этом контексте формирование универсального международного режима может быть рассмотрено как важное условие стабильного развития ИКТ. Россия на

официальном уровне выступает в поддержку формирования международного режима информационной безопасности в рамках ООН, который включал бы в себя не только вопросы обеспечения ответственного поведения государств в глобальной ИКТ-среде, но и проблематику международного управления Интернетом и противодействие преступному использованию ИКТ[13].

В условиях роста числа международных организаций и институтов исследователи пишут о формировании не только самостоятельных режимов, но и режимных комплексов. Описывая актуальные тенденции в области регулирования *киберпространства*, Дж. Най определял данное понятие как совокупность множества международных режимов [Nye 2014]. Важным следствием из работы Ная является включение в список игроков *глобальных групп* «группы семи / восьми» и «группы двадцати». Следовательно, БРИКС как аналогичный институт также может рассматриваться как полноценный участник процесса формирования международных режимов[14]. В научной литературе понятие «режимный комплекс» становится весьма распространённым [Drezner 2013]. Режимный комплекс предполагает наличие множества различных режимов, которые пересекаются, дополняют друг друга, а в отдельных случаях конкурируют между собой. Подобная ситуация снижает эффективность глобального управления в силу конкуренции между различными институтами, возможности манипуляции выбором удобных институтов со стороны отдельных игроков, а также сложностей контроля исполнения обязательств, принятых в рамках отдельных режимов [Drezner 2013].

Именно эту тенденцию мы наблюдаем в сфере ИКТ-безопасности, где наметилась конкуренция нормативных подходов и институтов. Режимный комплекс ИКТ-безопасности включает в себя ряд предметных областей, в число которых входят выработка норм ответственного поведения государств в ИКТ-среде, противодействие преступному использованию ИКТ и интернационализация управления Интернетом, а также защита прав человека в цифровой среде. При этом международное сотрудничество в данной области представляет собой совокупность связанных и пересекающихся режимов, которые находятся в состоянии динамического развития [Зиновьева 2019].

В условиях фрагментации Интернета [Fick, Miscik 2022] усиливается конкуренция между различными подходами к управлению Интернетом. В результате наметилось формирование конкурирующих режимов в рамках единого режимного комплекса. Режимы разнятся по составу участников (например, в Парижском призыве акцент делался на участии бизнеса и негосударственных игроков, в то время как БРИКС и ШОС ориентированы в большей степени на межгосударственное сотрудничество), по охвату предметных областей (так, например, в рамках Крайстчерского призыва обсуждались исключительно вопросы противодействия цифровому терроризму и экстремизму, на уровне Международного союза электросвязи – технические аспекты безопасности, в рамках ООН, ШОС, БРИКС рассматривался широкий круг вопросов в сфере ИКТ-безопасности).

Вместе с тем наиболее серьёзные противоречия касаются норм и принципов, лежащих в основе режимов ИКТ-безопасности. США продвигают принцип свободы передачи информации, в том числе поверх государственных границ. Россия, Китай и партнёры разделяют видение режима ИКТ-безопасности, основанного на принципе уважения государственного суверенитета, то есть переносят принципы Вестфальского

[13] Указ Президента Российской Федерации от 12.04.2021 №213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности». URL: http://static.kremlin.ru/media/events/files/ru/RR5NtCWkkZPTuc5TrdHURpA4vpN5UTwM.pdf (дата обращения: 11.09.2022).

[14] В силу того что статья была написана в 2014 году, а БРИКС начал активную работу на данном направлении с 2015 года, Дж. Най не упоминает данную организацию в своём анализе.

миропорядка в цифровую сферу. США стремятся сформировать односторонний имперский порядок в цифровой среде, размывая принцип суверенитета. Формирование многополярности сопровождается нарастающей международной конфликтностью, поэтому конкуренция между различными площадками глобального управления в ИКТ-среде, в том числе БРИКС, обостряется.

Таким образом, к середине 2020-х годов произошло складывание режимного комплекса в области ИКТ-безопасности. Сложившаяся ситуация открывает возможность манипулирования выбором удобных институтов в рамках режимного комплекса, что может подрывать международную стабильность в ИКТ-среде. Россия выступает за формирование универсального режима в данной области под эгидой ООН, при этом важная роль в достижении данной цели отводится региональным и макрорегиональным площадкам, в их числе БРИКС.

Методология анализа приоритетов БРИКС в сфере ИКТ-безопасности

Для анализа особенностей повестки БРИКС в области ИКТ-безопасности будет использован исследовательский аппарат, разработанный специалистами Университета Торонто и применяемый для выделения, мониторинга и экспертной оценки эффективности выполнения обязательств неформальных институтов глобального управления – «группы семи/восьми», «группы двадцати» и БРИКС. Данный подход заслужил широкое признание и применяется в течение многих лет [Лесаж 2014; Ванг 2022; Kirton, Wang 2022].

Он позволяет установить и обосновать причинно-следственные связи между декларируемыми членами институтов глобального управления приоритетами и согласуемыми коммюнике, декларациями, иными типами документов. Авторы методологии поставили задачей оценить, насколько заявления лидеров по итогам саммитов заслуживают доверия и следует ли вообще уделять внимание документам (коммюнике и декларациям), которые принимаются по итогам встреч на высшем уровне.

Ключевым понятием в данном контексте выступает «обязательство», под которым понимается *обособленное, конкретизированное, политически обязывающее и выраженное публично заявление о намерениях*. Каждое обязательство обладает свойствами дискретности (указания на коллективную цель и / или инструмент выполнения поставленной цели), *конкретности* (в качестве цели не принимается достижение неких абстрактных результатов, например укрепление международного мира и согласие), *политической обязательности* (имеется выражение коллективного намерения, например «мы обязуемся ...»), *ориентированностью на будущее* (реализация поставленной цели произойдёт в период после принятия документа, содержащего обязательство) и *коллективности* (акторами-исполнителями принятого решения являются сами страны–участницы института; встречающиеся в тексте обращения к международным организациям и площадкам не считаются обязательствами). Пример обязательства даёт намерение стран–участниц БРИКС развивать многостороннее сотрудничество для расширения всеобщего доступа к средствам цифровой связи, принятое на саммите в Уфе в 2015 году[15].

Исследование обязательств в области ИКТ-безопасности БРИКС и их имплементации опирается на три группы источ-

[15] «Мы обязуемся сосредоточить наши усилия на расширении всеобщего доступа ко всем средствам цифровой связи и на повышении информированности людей в этой области» (Коммюнике министров связи стран БРИКС по итогам встречи «Расширение сотрудничества в сфере телекоммуникаций и информационно-коммуникационных технологий». URL: https://www.ranepa.ru/images/media/brics/ruspresidency2/Communique_BRICS_ICT_ministers.pdf (дата обращения: 11.09.2022). Более подробно процесс мониторинга, особенности отбора фактов, процедура верификации и вынесение итоговой оценки описаны в специальном руководстве. См.: [Global Governance Program 2020].

ников. Первая группа представлена документами стратегического характера стран БРИКС, которые были изучены на предмет выделения приоритетов, касающихся отдельных аспектов обеспечения ИКТ-безопасности. Вторая группа источников включает документы, согласованные на уровне лидеров БРИКС в ходе ежегодных саммитов, начиная со встречи в Уфе в 2015 г. до саммита в Нью-Дели в сентябре 2021 г. включительно[16]. Третья группа источников – это резолюции и иные официальные документы ООН, отражающие актуальные тенденции международного сотрудничества в исследуемой области на глобальном уровне, которая позволила вписать инициативы БРИКС в глобальный контекст, сопоставить его с актуальными тенденциями глобального режима ИКТ-безопасности.

В качестве начальной точки исследования был выбран 2015 год. Хотя вопросы информационной безопасности включались в повестку и итоговые документы БРИКС и до этого (впервые они были упомянуты в Плане действий по итогам саммита БРИКС в Дурбане в 2013 году), именно 2015 г. был выбран в качестве отправной точки исследования. Как отмечает исследователь из Бразилии Л. Белли, «Уфимская декларация БРИКС 2015 г. может рассматриваться как документ, который стал началом кристаллизации консенсуса БРИКС по вопросу о необходимости выработки общей политики в области цифровых технологий и кибербезопасности» [Belli 2021].

Таким образом, в рамках проведённого исследования при помощи методологии анализа имплементации обязательств Университета Торонто были изучены документы БРИКС начиная с 2015 года, что позволило оценить взаимозависимость между декларируемыми приоритетами сотрудничества и реально принимаемыми решениями, координацией политик стран БРИКС в рамках ООН и потенциал институционализации сотрудничества в исследуемой области.

Проблематика ИКТ-безопасности в решениях БРИКС

Среди стран БРИКС нет консенсуса относительно содержательного наполнения понятия *ИКТ-безопасность*. Россия, Китай и Индия относят к данной области не только техническую сторону обеспечения безопасности информации, но и её содержание, в то время как Бразилия[17] и ЮАР[18] делают акцент на технических аспектах безопасности, не исключая и политической составляющей угрозы. Компромиссным выступает признание значимости противодействия угрозам в области использования ИКТ в экстремистских и террористических целях на уровне контента и на широком спектре технических угроз в исследуемой области.

Проблематика обеспечения ИКТ-безопасности была введена в повестку БРИКС практически одновременно с обособлением более обширной повестки содействия развитию цифровой экономики от вопросов научно-технического сотрудничества. Проблемы развития ИКТ в странах–участницах объединения оформились в виде самостоятельной сферы к 2015 году. Выделение ИКТ-безопасности в самостоятельную область международного сотрудничества было закреплено в ходе российского председательства, когда по инициативе принимающей стороны в Москве состоялась первая встреча министров

[16] Ограничение временного периода исследования повестки БРИКС 2015 г. обусловлено фактическим обособлением повестки развития информационных и коммуникационных технологий, куда в широком смысле входят вопросы обеспечения кибербезопасности, от повестки научно-технического развития в рамках БРИКС, см.: [Ларионова и др. 2020].

[17] Política Nacional de Segurança da Informação, The Government of Brazil, 2019. URL: https://www.gov.br/governodigital/pt-br/estrategias-e-politicas-digitais/politica-nacional-de-seguranca-da-informacao (дата обращения: 15.12.2023).

[18] The National Cybersecurity Policy Framework. South African Republic, 2015. URL: https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf (accessed: 14.12.2023).

связи стран-партнёров. Стороны согласовали совместное коммюнике «Расширение сотрудничества в сфере телекоммуникаций и информационно-коммуникационных технологий»[19]. Основные итоги министерской встречи были включены в итоговую декларацию Уфимского саммита БРИКС[20].

В 2015 г. в Уфе лидеры стран БРИКС приняли 12 обязательств по вопросам цифрового развития, из которых четыре решения касаются вопросов обеспечения ИКТ-безопасности. В частности, лидеры объединения выделили в числе приоритетных направлений цифрового сотрудничества: а) *взаимодействие и сотрудничество в области реагирования в случае чрезвычайных ситуаций, связанных с вопросами информационной безопасности*; б) *проведение совместных исследований в области новых технологий и услуг, связанных с информационной безопасностью*; в) *содействие обеспечению мирного, безопасного, открытого, основанного на доверии и сотрудничестве характера цифрового и интернет-пространства*; а также: г) *продвижение использования инновационного телекоммуникационного оборудования, разработку и внедрение новых стандартов и технологий связи в целях развития информационного/цифрового общества и противостояния киберугрозам*[21].

Инициативы российского председательства 2015 г. в сфере ИКТ-безопасности встретили поддержку среди стран–партнёров по объединению. В частности, данные начинания поддержал Китай. Например, в 2017 г. в Сямэне, КНР, лидеры пяти стран заявили о поддержке выработки признанных на международном уровне и приемлемых для всех заинтересованных сторон правил в области безопасности инфраструктуры ИКТ, защиты данных и Интернета, а также обязались совместно строить надёжную и безопасную сеть[22]. В 2017 г. была принята Дорожная карта БРИКС, которая постулирует необходимость коллективного согласования норм и принципов, которые должны лечь в основу глобального режима ИКТ-безопасности[23].

В годы председательства Индии в БРИКС в 2016 и 2021 годах, ЮАР в 2018 г. и Бразилии в 2019 г. решения в области развития ИКТ также принимались, но на них делался меньший акцент по сравнению с годами, когда повестку обсуждений формировали Россия и КНР. В 2020 году, согласно установленному порядку ротации, председательство в объединении в очередной раз перешло к России. В число приоритетов она включила *продолжение диалога по вопросам обеспечения международной информационной безопасности и противодействия информационной преступности* (наряду с *развитием сотрудничества стран БРИКС в противодействии терроризму и экстремизму*). Особенностью российского председательства 2020 г. в контексте развития повестки БРИКС по вопросам информационной безопасности стало фактическое совмещение двух треков, то есть перевод обширной повестки ИКТ-безопасности в более узкую область противодействия терроризму и экстремизму. При этом был сохранён упор на координацию внешней политики в исследуемой области на уровне ООН – выра-

[19] Коммюнике министров связи стран БРИКС по итогам встречи «Расширение сотрудничества в сфере телекоммуникаций и информационно-коммуникационных технологий». 2015 г. URL: https://www.ranepa.ru/images/media/brics/ruspresidency2/Communique_BRICS_ICT_ministers.pdf (дата обращения: 15.12.2023).

[20] VII саммит БРИКС. Уфимская декларация 9 июля 2015 года. URL: https://www.ranepa.ru/images/News_ciir/Project/BRICS_new_downloadings/Ufa_Declaration.pdf (дата обращения: 15.12.2023).

[21] Там же.

[22] Сямэньская декларация руководителей стран БРИКС 4 сентября 2017 г. URL: https://www.ranepa.ru/images/media/brics/2017/Siamenskaia_deklaratsiia_rukovoditelei_stran_BRIKS_ff.pdf (дата обращения: 11.09.2022).

[23] Там же.

ботку всеобъемлющего соглашения по международной информационной безопасности и принятие конвенции о противодействии преступному использованию ИКТ.

По итогам саммита БРИКС в Москве была принята Антитеррористическая стратегия объединения, куда были включены согласованные коллективные решения в области безопасности в сфере использования ИКТ и самих ИКТ, в частности: а) *противодействовать распространению экстремистских идей, ведущих к терроризму, а также использованию террористами Интернета и социальных сетей в целях вербовки, радикализации и подстрекательства, а также для предоставления террористам материально-финансовой поддержки*; а также б) *укреплять взаимодействие в борьбе с использованием информационно-коммуникационных технологий в террористических и иных преступных целях*[24].

Проведённый анализ решений БРИКС в области ИКТ-безопасности позволяет сделать несколько важных выводов. *Во-первых*, ведущая роль в определении направлений развития повестки объединения в целом[25] и в области международной информационной безопасности в частности принадлежит России и Китаю, на периоды председательства которых приходится наибольшее количество принимаемых решений по рассматриваемому вопросу и наиболее субстантивные из них. При этом Москва делает больший акцент на политической составляющей проблематики, в то время как Пекин – на экономической и вопросах развития сетевой инфраструктуры и безопасности данных.

Во-вторых, исходя из результатов анализа содержания согласованных коллективных решений мы приходим к выводу о постепенном сужении широкой повестки обеспечения ИКТ-безопасности и её переводу во взаимоприемлемую для членов БРИКС плоскость противодействия экстремизму и терроризму как институционально оформленного взаимодействия[26]. На уровне координации внешнеполитических инициатив страны поддерживают формирование международного режима в области информационной безопасности под эгидой ООН.

В-третьих, нельзя не отметить меньшую активность других членов БРИКС, помимо России и Китая, в сфере международной информационной безопасности. Так, председательство Бразилии в БРИКС в 2019 году, Индии в 2016 и 2021 годах и ЮАР в 2018 году не отметились значимыми решениями в рассматриваемой области и сконцентрировались на выражении общей поддержки предлагаемой партнёрами повестки[27].

Принятые обязательства и направления международного сотрудничества могут быть классифицированы согласно модифицированной методологии Университета Торонто, рассмотренной ранее, на предмет соответствия базовым предъявляемым критериям (табл. 1).

Для анализа эффективности имплементации достигнутых соглашений представляется важным провести анализ приорите-

[24] Антитеррористическая стратегия БРИКС 2020. URL: https://www.ranepa.ru/ciir/briks/predsedatelstva/briks-rossijskoe-predsedatelstvo-2020/BRICS%20COUNTER-TERRORISM%20STRATEGY%20(rus).pdf (дата обращения: 11.09.2022).

[25] См. более подробно анализ повестки БРИКС в области управления Интернетом в: [Игнатов 2022].

[26] См., например: Антитеррористическая стратегия БРИКС 2020. URL: https://www.ranepa.ru/ciir/briks/predsedatelstva/briks-rossijskoe-predsedatelstvo-2020/BRICS%20COUNTER-TERRORISM%20STRATEGY%20(rus).pdf (дата обращения: 11.09.2022).

[27] Например, в 2021 г. в принятой на саммите в Нью-Дели, Индия, декларации страны БРИКС согласились «укрепить потенциал как самих государств, так и международных организаций для более эффективного реагирования на новые и возникающие, традиционные и нетрадиционные вызовы, в том числе связанные с «киберпространством», а также приветствовали «успешное завершение работы Межправительственной группы по киберпреступности». См.: [БРИКС 2021].

Таблица 1

Решения и направления сотрудничества БРИКС в области международной информационной безопасности

Направления сотрудничества	Конкретность	Политическая обязательность	Ориентированность на будущее	Коллективность
Поддержка выработки норм и правил ответственного поведения государств в ИКТ-среде (в рамках РГОС)	+	+	+	-
Поддержка выработки Конвенции по противодействию преступному использованию ИКТ на уровне ООН	+	+	+	-
Наличие двусторонних договоренностей по МИБ	+	+	+	+
Принятие конвенции БРИКС по МИБ	+	+	+	+
Противодействие терроризму и экстремизму в ИКТ-среде	+	+	+	+

Источник: составлено авторами.

тов и подходов стран БРИКС в сфере ИКТ-безопасности, а также принимаемых ими решений в данной области на международном уровне.

Приоритеты стран–участниц БРИКС в области ИКТ-безопасности

Бразилия

Бразилия заняла 66-е место по уровню развития ИКТ согласно индексу МСЭ 2017 г.[28] Это одна из наиболее развитых стран Латинской Америки, и, по экспертным оценкам, Бразилия является одной из наиболее перспективных стран в области развития цифровых технологий[29]. Такое положение обуславливает её заинтересованность в сотрудничестве по вопросам информационной безопасности в БРИКС. При этом для Бразилии основным приоритетом являются вопросы наращивания потенциала и получения помощи в развитии ИКТ-сектора, в том числе в сфере прорывных технологий [Перминов 2019: 1520]. Кроме того, страна сталкивается со значительным ущербом от ИКТ-преступности[30], что повышает заинтересованность в международном сотрудничестве именно на этом направлении.

Базовая национальная Стратегия обеспечения кибербезопасности Бразилии была принята в 2020 г. Стратегия объединила ключевые положения нескольких документов, определявших национальные приоритеты в области кибербезопасности – актуальные на тот момент Стратегию национальной безопасности (обновлённую в 2012 году)[31] и Национальную политику в области информационной безопасности 2019 года[32], а также Стратегию цифровой

[28] Measuring the Information Society Report 2017. Volume 1. International Telecommunication Union. URL: https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2017/MISR2017_Volume1.pdf (accessed: 18.12.2023).

[29] См., например: Digital trends in the Americas region 2021. International Telecommunications Union. URL: https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-DIG_TRENDS_AMS.01-2021-PDF-E.pdf (accessed: 15.12.2023).

[30] Там же.

[31] National strategy of defense. The government Brazil, 2008 (updated 2012). URL: https://www.files.ethz.ch/isn/154868/Brazil_English2008.pdf (accessed: 18.12.2023).

[32] Política Nacional de Segurança da Informação The Government of Brazil, 2019. URL: https://www.gov.br/governodigital/pt-br/estrategias-e-politicas-digitais/politica-nacional-de-seguranca-da-informacao (дата обращения: 11.09.2022).

трансформации Бразилии от 2018 года[33] [Hurel, Lobato 2021]. Среди первоочередных задач бразильское руководство выделило адаптацию национального законодательства к меняющимся условиям, в частности разработку новой классификации киберпреступлений и требований к обеспечению кибербезопасности в условиях удалённой работы, а также разработку проекта нового закона о кибербезопасности. Кроме того, были запланированы создание централизованной системы управления киберугрозами, разработка общенациональных требований к обеспечению кибербезопасности на уровне отдельных пользователей / устройств ввода информации для государственных организаций, внедрение соответствующих требований в системы управления цепочками поставок и государственных закупок и др.

Среди итогов саммита БРИКС в Бразилии в 2019 г. следует выделить инициативу Бразилии о разработке двусторонних соглашений между странами БРИКС по указанной тематике. При этом в документе выражается поддержка инициатив РГОС и ГПЭ, запущенных в 2019 году, а также подчёркивается важность работы ООН в области противодействия преступному использованию ИКТ[34].

В международном измерении Бразилия выдвигает на передний план развитие сотрудничества в Латинской Америке наряду с другими характерными для документов такого уровня направлениями, такими как участие в многосторонних дискуссиях и заключение соответствующих международных соглашений. Поставленная на национальном уровне цель создания централизованной системы управления киберугрозами открыто соотносится с моделями, принятыми в ряде зарубежных стран, в частности в Великобритании, где создан специальный Национальный центр кибербезопасности, координирующий усилия различных ведомств, а также частного бизнеса в данной области[35].

На практике деятельность Бразилии в отношении международных переговоров по обеспечению кибербезопасности направлена «вне БРИКС» и не во всём согласуется с российской позицией. В 2018 г. во время голосования по проекту резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», предложенной Россией для преодоления застоя в переговорах по линии ГПЭ и предполагавшей создание РГОС, Бразилия воздержалась от голосования. Она мотивировала свою позицию тем, что в дублировании работы ГПЭ нет необходимости [Стадник, Цветкова 2021: 75]. Для Бразилии характерно стремление оставаться равноудалённой от различных участников переговорного процесса, эксперты также называют её кибердипломатию «колеблющейся» [Hurel 2022]. При этом смена курса Бразилии и её поддержка Будапештской конвенции отчасти были связаны с приходом к власти политика правой ориентации Ж. Болсонару.

Представители Бразилии принимали участие в переговорах как в ГПЭ, так и в обоих созывах РГОС. Несмотря на то что официально Бразилия не поддержала Парижский призыв к доверию и безопасности в киберпространстве на федеральном уровне, представленный Францией в ноябре 2018 года[36], о поддержке инициа-

[33] Brazilian Digital Transformation Strategy. 2018. URL: https://www.gov.br/mcti/pt-br/centrais-de-conteudo/comunicados-mcti/estrategia-digital-brasileira/digitalstrategy.pdf (accessed: 11.12.2023).

[34] Декларация Бразилиа по итогам XI саммита государств–участников БРИКС. 2019. URL: https://www.ranepa.ru/images/News_ciir/Project/BRICS_new_downloadings/2019/11th_BRICS_Summit_rus.pdf (дата обращения: 18.05.2023).

[35] *Hurel L.M.* Cybersecurity in Brazil: an analisys if the national strategy. Ingrape institutr strategic paper 51. April 2021. ULR: https://igarape.org.br/wp-content/uploads/2021/04/SP-54_Cybersecurity-in-Brazil.pdf (дата обращения: 15.12.2023).

[36] Paris Call for Trust and Security in Cyberspace – URL: https://pariscall.international/en/call (accessed: 11.09.2022).

тивы заявили штат Сан-Паулу и не менее десятка бразильских частных компаний и организаций гражданского общества. Что касается инициатив Программы действий по продвижению ответственного поведения государств в киберпространстве, предложенной изначально Францией и Египтом в 2020 году[37], а затем получившей развитие в 2022 году[38] и ориентированной на замену РГОС институциональным механизмом Программы действий, Бразилия к ней не присоединилась.

Бразилия поддерживает работу над Конвенцией ООН по противодействию преступному использованию ИКТ, однако она также присоединилась и к Будапештской конвенции Совета Европы, которую Россия, Китай и ЮАР рассматривают как вступающую в противоречие с принципом соблюдения государственного суверенитета. Таким образом, ИКТ-безопасность нельзя отнести к числу основных внешнеполитических приоритетов государства, что объясняет меньшую по сравнению с другими участниками БРИКС заинтересованность в развитии и институциональном углублении взаимодействия в данной области и несколько переменчивую внешнеполитическую линию. Бразилия более всего заинтересована в противодействии ИКТ-преступности на международном уровне.

Россия

Россия является государством с развитой цифровой экономикой. Согласно индексу ИКТ развития МСЭ от 2017 года, Россия занимала 45-е место и характеризовалась высоким уровнем проникновения сетей связи[39]. К 2023 г. Россия сохранила высокий цифровой потенциал, несмотря на санкционное давление со стороны Запада. Во внешней политике Россия делает акцент на обеспечении международной информационной безопасности[40] и укреплении цифрового суверенитета. Россия сталкивается со значительным числом атак в киберпространстве, что обуславливает внимание к данной проблематике[41]. Россия является лидером в продвижении темы информационной безопасности в рамках ООН и БРИКС [Бойко 2021; Крутских 2022].

Российская позиция по вопросам ИКТ-безопасности представлена в широком перечне документов стратегического характера, среди которых Стратегия национальной безопасности[42], Доктрина информационной безопасности[43], Концепция внешней политики[44], Основы государственной

[37] Programme of Action (PoA) for advancing responsible state behaviour in cyberspace. 2020. 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: 15.12.2023).

[38] Programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security. A/C.1/77/L.73. URL: https://digitallibrary.un.org/record/3991743?ln=ru (accessed: 15.12.2023).

[39] Measuring the Information Society Report 2017. Volume 1. International Telecommunication Union. URL: https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2017/MISR2017_Volume1.pdf (accessed: 18.12.2023).

[40] Указ Президента России №229 «Об утверждении Концепции внешней политики Российской Федерации». URL: http://static.kremlin.ru/media/events/files/ru/udpjZePcMAycLXOGGAgmVHQDIoFCN2Ae.pdf (дата обращения: 18.05.2023).

[41] Интервью заместителя Секретаря Совета Безопасности России О. Храмова. 2022. URL: http://www.scrf.gov.ru/news/allnews/3217/ (дата обращения: 19.12.2023).

[42] Указ Президента Российской Федерации от 02.07.2021 №400 «О Стратегии национальной безопасности Российской Федерации». URL: http://www.kremlin.ru/acts/bank/47046 (дата обращения: 11.09.2022).

[43] Указ Президента Российской Федерации от 05.12.2016 №646 «Об утверждении Доктрины информационной безопасности Российской Федерации». URL: http://kremlin.ru/acts/bank/41460 (дата обращения: 11.09.2022).

[44] Указ Президента России №229 «Об утверждении Концепции внешней политики Российской Федерации». URL: http://static.kremlin.ru/media/events/files/ru/udpjZePcMAycLXOGGAgmVHQDIoFCN2Ae.pdf (дата обращения: 18.05.2023).

политики в области международной информационной безопасности[45] а также Стратегия развития информационного общества в Российской Федерации на 2017 – 2030 годы[46].

В международном измерении в качестве ключевой задачи рассматривается формирование системы международной информационной безопасности в интересах эффективного противодействия попыткам использования ИКТ в военных и иных целях, противоречащих международному праву, прежде всего путем создания соответствующих международно-правовых механизмов. Стратегия национальной безопасности Российской Федерации ставит во главу угла установление международно-правового режима обеспечения безопасности в сфере использования ИКТ. Концепция внешней политики указывает на то, что возможности информационно-коммуникационных технологий всё чаще используются для решения внешнеполитических задач, в том числе в военно-политическом измерении[47]. Наконец, Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы содержит несколько важных моментов, касающихся деятельности России в области ИКТ-безопасности на международной арене. Данная Стратегия акцентируется на создании международных механизмов обеспечения доверия в сети Интернет[48]. Таким образом, проблематика ИКТ-безопасности является важнейшим направлением внешней политики России, долгосрочной целью является формирование международно-правового режима в данной области.

Среди стран БРИКС Россия является наиболее последовательным и активным сторонником выработки универсальной регуляторной рамки в области ИКТ-безопасности. Именно Москва в 1998 г. инициировала обсуждение данной проблематики в ООН[49], а в период стагнации переговоров в формате ГПЭ предложила инициативу по созыву РГОС. Проработка вопроса о содержании резолюции по вопросам кибербезопасности велась усилиями России не только в ООН, но и в ШОС, что способствовало достижению международного консенсуса относительно учреждения дополнительного переговорного формата[50].

В Концепции участия Российской Федерации в объединении БРИКС, утвержденной Президентом Российской Федерации в феврале 2013 года[51], в числе основных целей России в области сотрудничества со странами–участницами БРИКС по вопросам международной безопасности заявлены сотрудничество в интересах обеспечения международной информационной безопасности, использование возможно-

[45] Указ Президента Российской Федерации от 12.04.2021 №213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности». URL: http://static.kremlin.ru/media/events/files/ru/RR5NtCWkkZPTuc5TrdHURpA4vpN5UTwM.pdf (дата обращения: 11.09.2022).

[46] Указ Президента Российской Федерации от 09.05.2017 №203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы». URL: https://base.garant.ru/71670570/ (дата обращения: 11.09.2022).

[47] Указ Президента России №229 «Об утверждении Концепции внешней политики Российской Федерации». URL: http://static.kremlin.ru/media/events/files/ru/udpjZePcMAycLXOGGAgmVHQDIoFCN2Ae.pdf (дата обращения: 18.05.2023).

[48] Указ Президента Российской Федерации от 09.05.2017 №203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы». URL: https://base.garant.ru/71670570/ (дата обращения: 11.09.2022).

[49] Резолюция Генеральной Ассамблеи ООН A/RES/53/70 от 4 декабря 1998 г. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». URL:https://digitallibrary.un.org/record/ 265311?ln=ru (дата обращения: 15.12.2023).

[50] РФ вместе со странами ШОС представит проект резолюции ГА ООН по кибербезопасности. URL: https://tass.ru/politika/4811804 (дата обращения: 11.09.2022).

[51] Концепция участия Российской Федерации в БРИКС. Утв. Президентом России в 2013 г. URL: http://static.kremlin.ru/media/events/files/41d452a8a232b2f6f8a5.pdf (дата обращения: 15.12.2023).

стей БРИКС для продвижения инициатив в этом направлении в рамках различных международных форумов и организаций, прежде всего ООН, и укрепление в формате БРИКС сотрудничества в области противодействия использованию ИКТ в военно-политических, террористических и криминальных целях, а также в целях, противоречащих обеспечению международного мира, стабильности и безопасности. Таким образом, Россия придает важное значение развитию и углублению сотрудничества на уровне БРИКС по вопросам международной информационной безопасности.

В конце 2021 г. Россия и США совместно выдвинули проект резолюции по вопросам кибербезопасности, которая была одобрена Генеральной Ассамблеей без голосования[52]. Резолюция закрепила возможность выработки дополнительных обязательных правил поведения государств в киберпространстве с поправкой «при необходимости». Руководствуясь соображениями о необходимости создания широких форматов регулирования отношений в киберпространстве против узких «коалиций желающих», к формированию которых может привести упомянутая ранее инициатива Франции, Россия не вошла в число сторонников Парижского призыва [Чихачев 2022], но несколько крупных отечественных ИТ-компаний заявили о его поддержке.

В 2022 г. в ходе 77-й сессии ГА ООН Россия вынесла на обсуждение проект резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»[53], ориентированной на продолжение работы РГОС ООН после 2023 года; среди стран–членов БРИКС только Китай выступил в роли со-спонсора документа[54].

Россия является лидером международного сотрудничества на уровне БРИКС по вопросам международной информационной безопасности, при этом в данную область Россия включает широкий круг вопросов – противодействие военно-политическим угрозам, ИКТ-преступности и экстремизму в сети, защиту цифрового суверенитета от внешнего вмешательства, а также вопросы управления Интернетом. В долгосрочной перспективе Россия ориентирует международное сообщество и БРИКС на заключение юридически обязательных соглашений в сфере ИКТ-безопасности на глобальном и региональном уровнях.

Индия

Несмотря на то что Индия – один из крупнейших в мире поставщиков информационно-коммуникационных услуг, степень разработанности системы приоритетов и планов действий в области ИКТ-безопасности остается достаточно низкой. Это объясняется тем, что до недавнего времени индийское руководство не придавало значения рискам противостояния в цифровом пространстве [Куприянов 2019]. Фактически, полноценное развитие системы противостояния возникающим угрозам началось только в 2018 году, в результате чего к настоящему моменту для анализа мы можем отобрать только два документа – актуальную версию Стратегии национальной безопасности Индии и Национальную политику в области цифровых коммуникаций.

Стратегия национальной безопасности Индии[55] содержит небольшой перечень

[52] Генассамблея ООН приняла резолюцию России и США по киберсфере. URL: https://tass.ru/mezhdunarodnaya-panorama/13127057?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com (дата обращения: 11.09.2022).

[53] Генассамблея ООН приняла несколько российских резолюций по безопасности и разоружению. URL: https://tass.ru/mezhdunarodnaya-panorama/16533015 (дата обращения: 18.05.2023).

[54] Манхэттенские проекты. Как Россия и западные страны продвигают в ООН конкурирующие резолюции по кибербезопасности. URL: https://www.kommersant.ru/doc/5651792 (дата обращения: 18.05.2023).

[55] India's National Security Strategy. The Government of India, 2019. URL: https://manifesto.inc.in/pdf/national_security_strategy_gen_hooda.pdf (accessed: 11.09.2022).

угроз и предполагаемых направлений действий в контексте ИКТ-безопасности. Среди угроз авторы Стратегии выделяют киберпреступность, возможность применения кибероружия против элементов критической инфраструктуры страны, использование социальных медиа для воздействия на население с целью «разобщения людей, распространения пропаганды и ослабления веры в правительство»[56]. Незащищённость персональных данных рассматривается как предпосылка к распространению персонифицированной недостоверной информации. В связи с этим в числе ключевых задач заявляется реализация требований о локализации пользовательских данных наряду с более детализированным перечнем шагов по противодействию использованию кибервооружений, в частности создание единого центра принятия решений (киберкомандования) и наращивание потенциала в деле выявления источника кибератак, которые следует рассматривать как недружественные акты и нарушение государственного суверенитета.

Приоритет защиты государственного «цифрового суверенитета» подчеркивается в Национальной политике в области цифровых коммуникаций[57], в которой сделан акцент на экономическом потенциале ИКТ. Данное направление включает в себя, в первую очередь, принятие шагов для защиты пользовательских данных от несанкционированного доступа, поддержку местных поставщиков услуг и продукции, повышение эффективности органов, осуществляющих надзор в сфере лицензирования коммуникационной продукции, продвижение национальных интересов в контексте формулирования международных отраслевых стандартов. Таким образом, на данном направлении политика Индии представляется схожей с позицией КНР по вопросам безопасности данных, а акцент на цифровом суверенитете сближает позицию Индии с позицией России.

Индия поддерживает включение вопросов ИКТ-безопасности в повестку ООН и БРИКС. Показательно, что в 2021 г. саммит БРИКС в Индии с подачи председательствующей стороны был озаглавлен как «Партнёрство БРИКС во имя глобальной стабильности, безопасности и процветания». При этом упор Индия сделала на вопросы антитеррористического сотрудничества. В документе также отмечается значимость сотрудничества в области ИКТ-безопасности и утверждается, что необходима «разработка межправительственного соглашения БРИКС о сотрудничестве в области обеспечения безопасности в сфере использования ИКТ и двусторонних соглашений между государствами объединения»[58]. Отдельный акцент сделан на центральной роли ООН на данном направлении и поддержке работы в области разработки в рамках ООН всеобъемлющей конвенции о противодействии использованию ИКТ в преступных целях[59]. При этом Индия поддерживает также и форматы сотрудничества, предлагаемые странами Запада, в том числе ГПЭ последнего созыва. Индия официально не присоединилась к числу стран, поддержавших Парижский призыв[60], но более 50 индийских частных компаний и организаций гражданского общества выразили свою поддержку данному своду необязательных принципов. Это наибольший показатель среди стран БРИКС. Индия наряду с Китаем

[56] Оригинальный текст: «to sow discord amongst people, spread propaganda and weaken faith in the government» (India's National Security Strategy. The Government of India, 2019. URL: https://manifesto.inc.in/pdf/national_security_strategy_gen_hooda.pdf (accessed: 11.09.2022).

[57] National Digital Communications Policy. The Government of India 2018. URL: https://dot.gov.in/sites/default/files/EnglishPolicy-NDCP.pdf (accessed: 11.09.2022).

[58] Нью-Делийская декларация XIII саммита БРИКС от 2021 г. URL: https://www.ranepa.ru/ciir/briks/predsedatelstva/briks-indiyskoe-predsedatelstvo-2021-g/New%20Delhi%20Declaration%202021%20RUS.pdf (дата обращения: 11.09.2022).

[59] Там же.

[60] Paris call for trust and security in cyberspace. 2018. URL: https://pariscall.international/en/ (accessed: 15.12.2023).

не вошла в число спонсоров российско-американской резолюции 2021 г. При этом Индия не поддержала и предложенную Францией в 2020 г. Программу действий в области ответственного поведения в ИКТ-среде[61], а также и Декларацию за будущее Интернета 2022 года, предложенную США[62]. Тем не менее в 2022 г. Индия проголосовала в поддержку предложенной Францией резолюции 77-й ГА ООН «Программа действий по поощрению ответственного поведения государств при использовании информационно-коммуникационных технологий в контексте международной безопасности»[63], которая предлагает создать Программу действий как альтернативу предложенной Россией РГОС [Зиновьева 2023].

Индия рассматривает ИКТ как важнейший двигатель экономического роста и развития, поэтому заинтересована в сотрудничестве в сфере ИКТ-безопасности, в том числе формировании международно-правового режима под эгидой ООН, основанного на принципах уважения цифрового суверенитета, а также заключения формальной договоренности по ИКТ-безопасности в рамках БРИКС. Важным приоритетом также является противодействие преступному использованию ИКТ и цифровому терроризму. Несмотря на то что Индия вынуждена учитывать позицию стран Запада, продвигающих альтернативное видение режима кибербезопасности, по многим параметрам ее приоритеты в сфере ИКТ-безопасности близки к позиции России и КНР, что повышает ее заинтересованность в институционализации взаимодействия и способствует активному участию в сотрудничестве на уровне БРИКС в сфере ИКТ-безопасности.

Китай

Китай известен как один из лидеров в области регулирования киберпространства, притом китайский подход можно охарактеризовать как один из самых жёстких с точки зрения обеспечения цифрового суверенитета. Китай наряду с США является лидером в развитии прорывных цифровых технологий[64], в том числе больших данных, интернета вещей и машинного обучения. Китай реализует инициативу «Один пояс – один путь», которая включает компонент «Цифрового шёлкового пути», ориентированный на построение цифровой инфраструктуры в развивающихся странах[65]. Таким образом, для Китая приоритетны экономические аспекты цифрового развития, однако для их реализации необходимо обеспечить высокий уровень безопасности.

Формирование нормативной базы политики Китая в рассматриваемой области берёт начало в момент учреждения Национальной координационной группы по кибербезопасности и информационной безопасности, итогом работы которой стала первая версия специализированной национальной стратегии [Ромашкина, Задремайлова 2020: 124]. Действующая версия Стратегии была принята в 2016 году[66]. В рамках

[61] Program of Action for advancing responsible states bahaviour in cyberspace. 2020. 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: 15.12.2023).

[62] Declaration for the future of Internet. White House, 2022. https://www.whitehouse.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet_Launch-Event-Signing-Version_FINAL.pdf

[63] Programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security. A/C.1/77/L.73 2022. URL: https://digitallibrary.un.org/record/3991743?ln=ru (accessed: 15.12.2023).

[64] UNCTAD Digital Economy Report. 2021. URL: https://unctad.org/publication/digital-economy-report-2021 (accessed: 15.12.2023).

[65] Action plan on the belt and road initiative. People Republic of China, 2015. URL: https://english.www.gov.cn/archive/publications/2015/03/30/content_281475080249035.htm (accessed: 15.12.2023).

[66] Неофициальный перевод с китайского на английский язык представлен здесь: National Cyberspace Security Strategy. URL: https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/ (дата обращения: 11.09.2022).

упомянутой Стратегии киберугрозы рассматриваются в числе основных препятствий экономическому росту, политической и экономической безопасности; среди возможных последствий применения возможностей ИКТ для противоправных и враждебных действий упоминаются нарушение работы критической инфраструктуры, в частности транспортной и энергетической инфраструктуры, распространение недостоверной информации, гражданские беспорядки, свержение действующих политических режимов. В качестве меры противодействия реализуется политика контроля онлайн-активности в интересах пресечения противоправной деятельности, в особенности призывов к гражданскому неповиновению и сепаратизму, закрепление социалистических ценностей как неотъемлемого элемента онлайн-культуры, развития кадрового резерва и национальной технологической базы. Правовую базу заявленных действий формируют Закон о противодействии терроризму (2015)[67], Закон о кибербезопасности (2016)[68] и Постановление о защите безопасности критической информационной инфраструктуры (2021)[69].

В июне 2021 г. Пекин принял новый Закон о безопасности данных, который определяет более строгие требования к обработке важных данных, основных данных о состоянии и конфиденциальных данных и распространяет на всю автоматизированную обработку данных требование соблюдать Многоуровневую схему защиты, предусмотренную Законом о кибербезопасности, расширяет обязательства по локализации данных на вышеупомянутые важные данные[70].

Приоритеты внешней политики Китая в области ИКТ-безопасности более подробно раскрываются в Стратегии международного сотрудничества в киберпространстве, принятой в 2017 году[71]. Стратегия закрепляет принцип отказа от стремления к гегемонии на пространстве Интернета, недопущение вмешательства во внутренние дела при помощи возможностей ИКТ и приоритетность реализации государственного суверенитета в информационном пространстве [Ромашкина, Задремайлова 2021: 130]. Авторы Стратегии выступают за создание системы регулирования отношений в киберпространстве на основе согласованных правил и норм, выработанных на базе равного участия и недискриминации.

В 2020 г. Китай представил Глобальную инициативу в области безопасности данных[72], в которой постулируется значимость суверенитета в цифровом пространстве и центральная роль ООН в области управления данными и обеспечении международной информационной безопасности.

В то же время Китай не выступил в качестве ко-спонсора российско-американской резолюции 2021 года, но не поддержал и прозападные инициативы в данной

[67] Counterterrorism Law of the People's Republic of China (Order No. 36 of the President of the PRC). URL: https://www.ilo.org/dyn/natlex/natlex4.detail?p_lang=en&p_isn=103954&p_country=CHN&p_count=1189 (accessed: 11.09.2022).

[68] Неофициальный перевод с китайского на английский язык представлен здесь: China Cybersecurity Law. URL: https://d-russia.ru/wp-content/uploads/2017/04/China-Cybersecurity-Law.pdf (accessed: 11.09.2022).

[69] *Gong J., Yue C.* China Released Regulation on Critical Information Infrastructure. Bird & Bird. 2021. [Электронный ресурс]. – Режим доступа: https://www.twobirds.com/en/insights/2021/china/china-released-regulation-on-critical-information-infrastructure (accessed: 04.08.2022).

[70] Data Security Law of China. 2021. URL: https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/ (accessed: 15.12.2023).

[71] International Strategy of Cooperation on Cyberspace. China, 2017. URL: https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/201703/t20170301_599869.html#:~:text=The%20strategic%20goal%20of%20China's,peace%2C%20security%20and%20stability%20in (accessed: 11.09.2022).

[72] Global Initiative on Data Security. The Government of China, 2020. URL: https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/202009/t20200908_679637.html (accessed: 18.05.2023).

области. Например Китай, как и другие страны БРИКС, официально не поддержал Парижский призыв на государственном уровне. Среди представителей частного сектора и организаций гражданского общества только одна компания заявила о поддержке данной инициативы. Что касается инициатив США и стран Запада с сильным политическим компонентом, таких как Декларация о будущем Интернета[73] и Программа действий в области поощрения ответственного поведения государств в киберпространстве[74], Китай выступил однозначно против.

В ходе саммита БРИКС в Пекине в 2022 г. акцент был сделан на вопросах обеспечения информационной безопасности. В частности, в Пекинской декларации подчеркивалась «необходимость развития практического сотрудничества в рамках БРИКС посредством осуществления "дорожной карты" в обеспечении безопасности в сфере использования ИКТ и в рамках деятельности Рабочей группы БРИКС по вопросам безопасности в сфере использования ИКТ»[75]. В документе отмечается также прогресс, достигнутый в рамках Специального комитета ООН по разработке всеобъемлющей международной конвенции о противодействии использованию ИКТ в преступных целях[76].

Таким образом, позиции России и Китая относительно основных параметров международного сотрудничества в сфере ИКТ-безопасности характеризуются наибольшей близостью – обе страны выступают за формирование международного режима в данной области, основанного на вестфальских принципах уважения суверенитета, противопоставляя его продвигаемым США и их союзниками инициативам. Важными акцентами в позиции Китая является также противодействие ИКТ-преступности и ИКТ-терроризму и защита данных, которые рассматриваются как важнейший ресурс технологического и экономического развития.

ЮАР

Несмотря на то что Южно-Африканская Республика входит в число лидеров цифрового развития Африканского региона [Панцерев 2018: 14], вопрос обеспечения кибербезопасности с учетом всего многообразия существующих угроз разработан в официальных документах и стратегиях ЮАР сравнительно неглубоко. Рамочная программа по обеспечению кибербезопасности ЮАР была принята в 2015 году. При этом к тому моменту ЮАР уже вошла в мировой антирейтинг по числу случаев онлайн-мошенничества и других криминальных инцидентов[77]. В числе основных угроз кибербезопасности авторы Рамочной программы указали необходимость импорта важного для обеспечения надлежащего уровня защиты оборудования и технологий, слабость кадровой базы на фоне увеличения количества киберинцидентов последних лет. Было предложено наладить эффективную координацию действий государственных органов и учредить специализированный координирующий орган. Основные координирующие функции были возложены на Хаб кибербезопасности (Cybersecurity Hub), ответственный также за выработку документов стратегического характера.

Достаточно длительное время занял процесс адаптации национального законодательства ЮАР к реалиям распространяющейся киберпреступности. Первый

[73] Declaration for the Future of the Internet. White House, 2022. URL: https://www.state.gov/declaration-for-the-future-of-the-internet (accessed: 18.05.2023).

[74] General Assembly official records, 77th session : 46th plenary meeting, Wednesday, 7 December 2022, New York. URL: https://digitallibrary.un.org/record/4009684?ln=en (accessed: 18.05.2023).

[75] Пекинская декларация XIV саммита БРИКС от 23 июня 2022 года. URL: http://www.kremlin.ru/supplement/5819 (дата обращения: 15.12.2023).

[76] Там же.

[77] The National Cybersecurity Policy Framework. South African Republic, 2015. URL:: https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf (дата обращения: 11.09.2022).

проект Закона о киберпреступлениях был представлен в августе 2015 года; процесс доработки занял около полутора лет, в результате чего на рассмотрение парламента он был направлен только в начале 2017 года. Принятие закона в его исходной форме активно поддерживалось сторонниками экс-президента Джейкоба Зумы, но встретило сильное сопротивление оппозиции – согласно распространенной оценке, в своей исходной редакции Закон «не проводит различий между шпионажем и работой журналистов» и может послужить в качестве инструмента давления на медиа на фоне участившихся скандалов с участием представителей администрации Зумы[78]. Уже после отставки Зумы и выдвижения обвинений в коррупции[79] Закон дважды прошел общественное обсуждение в 2018 и 2019 годах; в конце 2020 г. его поддержали обе палаты парламента ЮАР. Президент Рамапоса подписал Закон в мае 2021 г. с условием вступления в силу с 1 декабря 2021 года[80]. До принятия Закона о киберпреступлениях компетентные органы ЮАР руководствовались положениями Уголовно-процессуального кодекса, что вкупе с отсутствием четких определений затрудняло расследование преступлений, совершенных в киберпространстве[81].

Руководство ЮАР последовательно занимает скептическую позицию в отношении международных соглашений, касающихся ИКТ-безопасности, несмотря на заявленный в рамках Рамочной программы приоритет развития международного сотрудничества. В этом контексте показателен пример Конвенции Африканского союза (АС) по вопросам кибербезопасности и защиты данных[82] [Orji 2018], в отношении которой ЮАР заняла позицию «афроскептика», отказавшись от её ратификации.

Как и другие партнеры по БРИКС, ЮАР не вошла в число стран, поддержавших Парижский призыв, а общее количество поддержавших Призыв южноафриканских частных компаний и организаций гражданского общества не превышает двадцати. При этом ЮАР поддержала проект российско-американской резолюции 2021 года, но не присоединилась к Программе действий по продвижению правил ответственного поведения государств в киберпространстве. В 2022 г. в ходе 77-й сессии ГА ООН ЮАР выступила в поддержку российского проекта резолюции по международной информационной безопасности. Вместе с тем ЮАР присоединилась к Будапештской конвенции Совета Европы от 2001 года, что не препятствует её участию в переговорном процессе ООН по выработке Конвенции по противодействию преступному использованию ИКТ и поддержке данной инициативы на уровне БРИКС. В рамках второй Йоханнесбургской декларации БРИКС отмечалась приверженность продолжению работы «по выработке Конвенции по противодействию ИКТ-преступности в ООН, а также формирования нормативно-правовых рамок БРИКС по

[78] Raymond Joseph: South Africa's Cybercrimes and Cybersecurity Bill is deeply flawed. URL: https://www.indexoncensorship.org/2016/01/raymond-joseph-south-africa-cybercrimes-and-cybersecurity-bill/ (accessed: 11.09.2022).

[79] Zuma in the dock: South Africa's ex-president faces corruption charges. URL: https://www.theguardian.com/world/2018/apr/06/south-africa-jacob-zuma-court-corruption-charges (accessed: 11.09.2022).

[80] South Africa's newly enacted sections of the Cybercrimes Act 19 of 2020 and what you need to know to be compliant. URL: https://www.dentons.com/en/insights/articles/2021/december/6/newly-enacted-sections-of-the-cybercrimes-act-19-of-2020-and-what-you-need-to-know-to-be-compliant (accessed: 11.09.2022).

[81] South Africa lays down the law on cybercrime. URL: https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime (accessed: 11.09.2022).

[82] African Union Convention on Cyber Security and Personal Data Protection. 2014. URL: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (accessed: 11.09.2022).

вопросам обеспечения безопасности в сфере использования ИКТ»[83].

Таким образом, ЮАР демонстрирует меньшую по сравнению с другими членами БРИКС заинтересованность в развитии взаимодействия в данной области, однако поддерживает инициативы БРИКС на данном направлении на площадке ООН, а также подписание межправительственного соглашения в БРИКС.

Анализ стратегий и других важных в контексте национальной политики в области ИКТ-безопасности стран БРИКС документов позволяет сделать следующие выводы. *Во-первых*, внутри объединения степень проработанности данной категории вопросов находится на разных уровнях – Россия и Китай в настоящий момент обладают наиболее конкретизированной системой приоритетов и задач в области кибербезопасности и, следовательно, дальше остальных партнёров ушли в отношении законодательного подкрепления обсуждаемых действий на национальном и международном уровнях. Именно Москва и Пекин наиболее активно из числа участников БРИКС участвуют в международной дискуссии по исследуемому вопросу, а внутри дуэта инициатива чаще всего исходит от России. Тройка Бразилия–Индия–ЮАР заметно отстаёт в данном отношении, что в целом коррелирует с оценочным уровнем цифровой развитости государств БРИКС [Игнатов 2020]. *Во-вторых*, характер выдвигаемых приоритетов в области кибербезопасности различается между партнёрами по объединению. Россия, Китай и Индия склонны прямо или косвенно включать в сферу международной информационной безопасности работу с информацией, распространяемой посредством сетей цифровой связи, что значительно расширяет сферу предполагаемых угроз. Подход Бразилии и ЮАР носит более прикладной характер и предполагает работу, в первую очередь, с традиционными вызовами кибербезопасности (в частности, с потенциалом использования ИКТ как средства осуществления киберпреступлений). Разбивка на тройку Россия–Китай–Индия и двойку Бразилия–ЮАР в целом соответствует рассмотренной в [Игнатов 2022] концепции *слабого* (ограниченное вмешательство государства в обеспечение кибербезопасности, инициатива на стороне частных компаний) и *сильного цифрового суверенитета* (вопросы кибербезопасности поднимаются до уровня проблемы национальной безопасности и подкрепляются соответствующими действиями). Несмотря на то что в академической литературе данные страны относят к «ястребам суверенитета» [Панова 2015], в действительности трактовка наполнения цифрового суверенитета со стороны государств несколько различается. Акцент на значимости цифрового суверенитета обуславливает незначительное внимание к координации деятельности негосударственных игроков БРИКС в рамках режима ИКТ-безопасности, так как приоритетом является межгосударственная координация.

* * *

В рамках представленной работы было решено несколько исследовательских задач. Авторы предложили уточнённое определение понятия *ИКТ-безопасность*, которое затем было использовано при исследовании национальных приоритетов стран–членов БРИКС и решений, принятых в рамках объединения по интересующему вопросу.

Анализ документов стратегического планирования пяти стран показал, что все они привержены нормам уважения государственного суверенитета в ИКТ-среде и видят её как основу международного режима в данной области. Проведённый анализ позволил разделить страны БРИКС на две группы. В первую группу были включены Россия, Китай и Индия, которые деклари-

[83] Вторая Йоханнесбургская декларация стран БРИКС. 24 августа 2023 года. URL: http://static.kremlin.ru/media/events/files/ru/ls471x8ogLBhjRQx05ufVB2uzMFo1kWs.pdf (дата обращения: 15.12.2023).

руют и реализуют подход к обеспечению ИКТ-безопасности, ориентированный на включение в её предметную область вопросов регулирования содержания контента глобального Интернета и её технической безопасности (данный подход отражает используемая терминология – международная информационная безопасность [Зиновьева, Мищишина 2022]), а также уделяющий значительное внимание проблематике информационной безопасности. Ко второй группе были отнесены Бразилия и ЮАР, позиция которых фокусируется на наращивании потенциала и преодолении цифрового разрыва. В меньшей степени они ориентированы на регулирование цифрового контента. Все государства поддерживают необходимость международного сотрудничества в области противодействия преступному использованию ИКТ в рамках специального комитета ГА ООН на основании уважения принципа государственного суверенитета. При этом Индия проявляет бóльшую активность в области развития сотрудничества БРИКС в сфере ИКТ-безопасности по сравнению с Бразилией и ЮАР. Во всех странах–участницах БРИКС можно отметить растущее внимание к вопросам обеспечения безопасности данных.

Россия и Китай определяют направление многосторонней дискуссии внутри БРИКС по исследуемому вопросу. На глобальном уровне в рамках ООН именно Россия продвигает проблематику международной информационной безопасности, в то время как Китай в большей степени ориентирован на вопросы развития цифровых технологий и поддержку проекта цифрового «Пояса и пути». Наибольшее соответствие позиции лидеров демонстрирует Индия, которая также склонна включать в проблематику кибербезопасности аспект регулирования оборота информации в цифровой среде и, что немаловажно, контроль над её содержанием. Бразилия и ЮАР не заявляют подобные задачи в числе приоритетных, они в большей степени ориентированы на проблему преодоления цифрового разрыва и наращивание потенциала в сфере цифровых технологий. Кроме того, Россия и Китай существенно опережают партнёров в отношении постановки стратегических ориентиров и адаптации национального законодательства к меняющейся международной конъюнктуре.

БРИКС вносит существенный вклад в процесс формирования международного режима обеспечения кибербезопасности в части формулирования основных норм и принципов сотрудничества, которые поддерживают все страны в рамках ООН. Общность подходов государств БРИКС к формированию системы международной информационной безопасности особенно наглядно подтвердилась в ходе принятия 73-й сессией Генеральной Ассамблеи ООН российских проектов резолюций «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», а также «Противодействие использованию информационно-коммуникационных технологий в преступных целях». Таким образом, наибольшую эффективность взаимодействие в рамках БРИКС демонстрирует в области координации внешнеполитических курсов и поддержки инициатив на уровне ООН.

Ниже в табличной форме представлены результаты голосования и участия стран БРИКС в формировании международного режима ИКТ-безопасности (табл. 2). Данные в таблице демонстрируют высокую степень координации внешних политик государств в рамках ООН по вопросам формирования глобального режима ИКТ-безопасности. Вместе с тем в условиях нарастающей международной конфликтности принятие международных договорённостей в рамках ООН в настоящее время представляется маловероятным. В этом контексте представляется уместным сужение повестки БРИКС в исследуемой области.

Сужение повестки БРИКС в области ИКТ-безопасности до взаимоприемлемых тем для обсуждения, например до противодействия экстремизму и терроризму в сети во всех их проявлениях, будет способствовать углублению институционального сотрудничества в рамках объединения. Общим приоритетом также является про-

Таблица 2
Результаты голосования по основным проектам и участие стран БРИКС в формировании международного режима ИКТ-безопасности

	Бразилия	Россия	Индия	Китай	ЮАР
Поддержка выработки всеобъемлющего договора по МИБ (в рамках инициированной Россией РГОС)	+	+	+	+	+
Поддержка выработки Конвенции по противодействию преступному использованию ИКТ	+	+	+	+	+
Наличие двусторонних договорённостей с Россией по МИБ	+	+	+	+	+
Поддержка резолюции России 2022 г. ГА ООН (о продлении мандата РГОС после 2025 года)	+	+	+	+	+
Поддержка резолюции Франции 2022 года (PoA)	+	–	+	–	+
Поддержка Парижского призыва, Декларации о будущем Интернета	–	–	–	–	–
Участие в Будапештской конвенции 2001 г.	+	–	–	–	+

Источник: составлено авторами.

тиводействие ИКТ-преступности, однако сотрудничество на данном направлении весьма успешно реализуется на площадке ООН, поэтому углубление взаимодействия в БРИКС представляется нецелесообразным, поскольку может отвлечь ресурсы и внимание от ооновского процесса. Сохранение Россией и Китаем своих позиций относительно вопросов обеспечения ИКТ-безопасности, требующих обсуждения и принятия многосторонних решений в рамках БРИКС, позволит в будущем разрешить ряд вопросов прикладного характера, например наладить более широкий обмен информацией относительно противодействия распространению экстремистских материалов.

В рамках предстоящих председательств, в частности российского председательства БРИКС в 2024 году, целесообразным представляется направить переговоры в русло более детальной проработки вопросов, связанных с обеспечением международной информационной безопасности. Приоритетными могут стать вопросы о принципах сотрудничества и мерах доверия при определении источников ИКТ-угроз, о функционировании механизмов обеспечения доверия и верификации действий в ИКТ-пространстве. Важным пунктом также является определение согласованной позиции по инициативе А. Гуттериша – принятие ООН Глобального цифрового договора , в рамках которого также предполагается перехват повестки инициированной Россией РГОС ООН. Следование данному подходу может облегчить дальнейшее продвижение согласованной позиции БРИКС в рамках более крупных площадок, в частности ООН.

В настоящий момент достаточно сложно со всей определённостью говорить о перспективах сближения позиций с новыми членами БРИКС по вопросам ИКТ-безопасности. Некоторые из них, например Аргентина и Саудовская Аравия, имеют опыт участия в многосторонних инициативах «Группы двадцати» вместе со странами–членами БРИКС, в то время как Египет, Иран, Эфиопия и ОАЭ не обладают подобными компетенциями. В то же время можно предположить, что Иран, в последние годы активно наращивающий собственный киберпотенциал [Хегатуров 2019], может выступить в поддержку подхода России и Китая, основанного на максимизации цифрового суверенитета государства. Перспективы дальнейшего сближения расширенного БРИКС по вопросам обеспечения ИКТ-безопасности будут во многом зависеть от эффективности согласования позиций в ходе предстоящего председательства России в БРИКС в 2024 году.

Список литературы

Алпеев А.С. Терминология безопасности: кибербезопасность, информационная безопасность // Вопросы кибербезопасности. 2014. №5 (8). С. 39–42.

Бойко С.М. Проблематика международной информационной безопасности на площадках ШОС и БРИКС // Международная жизнь. 2019. №. 1. С. 1–22.

Бойко С.М. Международная информационная безопасность: новые вызовы и угрозы // Международная жизнь. 2021. [Электронный ресурс]. – Режим доступа: https://interaffairs.ru/jauthor/material/2738 (дата обращения: 18.05.2023).

Безкоровайный М.М., Татузов А.Л. Кибербезопасность – подходы к определению понятия // Вопросы кибербезопасности. 2014. №1(2). С. 22–27.

Бухт Р., Хикс Р. Определение, концепция и измерение цифровой экономики // Вестник международных организаций. 2018. Т. 13. №2. С. 143–172. DOI: 10.17323/1996-7845-2018-02-07

Ванг А.С. Модель лидерства Китая в БРИКС // Вестник международных организаций. 2022. Т.17. № 2. С. 50–85. DOI: 10.17323/1996-7845-2022-02-03

Згоба А.И., Маркелов Д.В., Смирнов П.И. Кибербезопасность: угрозы, вызовы, решения // Вопросы кибербезопасности. 2014. №5 (8). С. 30–38.

Зиновьева Е.С. Международное сотрудничество по обеспечению информационной безопасности: субъекты и тенденции эволюции: Дисс. ... д-ра полит. наук. МГИМО МИД России. М., 2019. 362 с.

Зиновьева Е.С. Международная информационная безопасность в двусторонних отношениях России и США [Электронный ресурс]. Российский совет по международным делам. 2023. – Режим доступа: https://russiancouncil.ru/analytics-and-comments/analytics/mezhdunarodnaya-informatsionnaya-bezopasnost-v-dvustoronnikh-otnosheniyakh-rossii-i-ssha/?sphrase_id=98721820 (дата обращения: 18.05.2023).

Зиновьева Е.С., Мищишина Е.Е. Формирование универсальной терминологии в сфере МИБ: политические аспекты. Российский совет по международным делам. 2022. [Электронный ресурс]. – Режим доступа: https://russiancouncil.ru/analytics-and-comments/analytics/formirovanie-universalnoy-terminologii-v-sfere-mib-politicheskie-aspekty/ (дата обращения: 16.05.2023).

Игнатов А.А. Цифровая экономика в БРИКС: Перспективы международного сотрудничества // Вестник международных организаций. 2020. Т. 15. №1. С. 31–62. DOI: 10.17323/1996-7845-2020-01-02

Игнатов А.А. Управление Интернетом в повестке БРИКС // Вестник международных организаций. 2022. Т. 17. № 2. С. 86–109.

Карпова Д.Н. Киберпреступность: глобальная проблема и её решение // Власть. 2014. №8. С. 46–50.

Карцхия А.А. Кибербезопасность и интеллектуальная собственность. Ч. 1 // Вопросы кибербезопасности. 2014. №1 (2). С. 61–66.

Кадулин В.Е., Клочкова Е.Н. Соотношение понятий «информационная безопасность» и «кибербезопасность» в современном правовом поле // Вопросы кибербезопасности. 2017. №2 (20). С. 7–10.

Киберпространство БРИКС: правовое измерение / Под ред. Т.Я. Хабриева, Д. Руйпин. М.: Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации, 2017. 336 с.

Кузнецов Д.А. Сетевая текстура мировой политики: трансрегионализм БРИКС // Мировая экономика и международные отношения. 2020. Т. 64. №11. С. 124–131.

Куприянов А.В. Индия в эпоху кибервойн. Российский совет по международным делам. 2019. [Электронный ресурс]. – Режим доступа: https://russiancouncil.ru/analytics-and-comments/analytics/indiya-v-epokhu-kibervoyn/ (дата обращения: 04.08.2022).

Крутских А.В. К политико-правовым основаниям глобальной информационной безопасности // Международные процессы. 2007. Т. 5. №1(13). С. 28–37.

Крутских А.В. Международная информационная безопасность: в поисках консолидированных подходов // Вестник РУДН. Серия: Международные отношения. 2022. Т. 22. №2. С. 342–351.

Крутских А.В., Стрельцов А.А. Международное право и проблема обеспечения международной информационной безопасности // Международная жизнь. 2014. № 11. С. 20– 34.

Ларионова М.В., Игнатов А.А., Попова И.М., Сахаров А.Г., Шелепов А.В. Десять лет БРИКС: что дальше? М.: Дело; РАНХиГС, 2020. 73 с.

Лебедева М.М., Кузнецов Д.А. Трансрегионализм – новый феномен мировой политики // Полис. Политические исследования. 2019. №5. С. 71–84.

Лесаж Д. Текущая программа действий «Группы двадцати» в сфере налогообложения: исполнение обязательств, отчётность и легитимность // Вестник международных организаций. 2014. Т. 9. №4. С. 40–54.

Малюк А.А., Полянская О.Ю. Зарубежный опыт формирования в обществе культуры информационной безопасности // Безопасность информационных технологий. 2016. Т. 23. №4. С. 25–37.

Массель Л.В., Воропай Н.И., Сендеров С.М., Массель А.Г. Киберопасность как одна из стратегических угроз энергетической безопасности России // Вопросы кибербезопасности. 2016. №4 (17). С. 1–10.

Михалевич Е.А. Российско-китайское взаимодействие по обеспечению безопасности в киберпространстве в рамках БРИКС // Свободная мысль. 2017. №6 (1684). С. 155–160.

Панова В.В. Проблемы безопасности и перспективы саммита БРИКС в Уфе // Вестник международных организаций. 2015. Т. 10. № 2. С. 119–139.

Перминов В.А. Сектор информационно-коммуникационных технологий Бразилии: история, современное положение и тенденции развития // Экономические отношения. 2019. Т. 9. №3. С. 1519–1532.

Ромашкина Н.П. Проблема международной информационной безопасности в ООН // Мировая экономика и международные отношения. 2020. Т. 64. №12. С. 25–32.

Ромашкина Н.П., Задремайлова В.Г. Эволюция политики КНР в области информационной безопасности // Путь к миру и безопасности. 2020. №1 (58) С. 122–138. DOI: 10.20542/2307-1494-2020-1-122-138

Стадник И.Т., Цветкова Н.А. Место и роль стран Латинской Америки в системе международной и региональной кибербезопасности // Латинская Америка. 2021. №4. С. 69– 84.

Хегатуров А. Кибермощь Ирана. Российский совет по международным делам. 2019. [Электронный ресурс]. — Режим доступа: https://russiancouncil.ru/activity/digest/longreads/kibermoshch-irana/ (дата обращения: 19.12.2023).

Чихачёв А.Ю. Российско-французские отношения при президенте Эмманюэле Макроне: достижения и противоречия // Вестник СПбГУ. Международные отношения. 2022. Т. 15. С. 86–104.

Abdenur A. Can BRICS Cooperate in International Security? // Вестник международных организаций. 2017. Т.12. № 3. С. 73–95.

CyberBRICS: Cybersecurity Regulations in the BRICS Countries / ed. by L. Belli. Springer Nature, 2021. 280 p.

Fick N., Miscik J. Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet. Council on Foreign Relations. 2022. [Электронный ресурс]. — Режим доступа: https://www.cfr.org/task-force-report/confronting-reality-in-cyberspace (дата обращения: 16.05.2023).

Global Governance Program. Compliance Coding Manual for International Institutional Commitments. 2020. [Электронный ресурс]. — Режим доступа: http://www.g7.utoronto.ca/compliance/Compliance_Coding_Manual_2020.pdf (дата обращения: 11.09.2022).

Hurel L.M., Lobato L.C. Cyber security in Brazil: keeping silos or building bridges? // Routledge Companion to Global Cyber-security Strategy / ed. by S. N. Romaniuk, M. Manjikian. London: Routledge, 2020. 656 p.

Krasner S. Regimes and the limits of realism: Regimes as autonomous variables // International Organization. 1982. Vol. 36. No. 2. P. 497–510.

Kirton J., Wang, A.X. China's Complex Leadership in G20 and Global Governance: From Hangzhou 2016 to Kunming 2021 // Chinese Political Science Review. 2022. DOI: https://doi.org/10.1007/s41111-022-00213-9

Nye J.S. The Regime Complex for Managing Global Cyber Activities. Global Commission on Internet Governance. 2014. [Электронный ресурс]. — Режим доступа: https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf (дата обращения: 11.09.2022).

Orji U.J. The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability? // Masaryk University Journal of Law and Technology. 2018. Vol. 12. No. 2. P. 91–130. DOI: https://doi.org/10.5817/MUJLT2018-2-1

THE ROLE OF BRICS IN THE INTERNATIONAL ICT SECURITY REGIME

ELENA ZINOVIEVA
MGIMO University, Moscow, 119454, Russia

ALEXANDER IGNATOV
MGIMO University, Moscow, 119454, Russia
Russian Presidential Academy of National Economy and Public Administration, Moscow, 119571, Russia

Abstract

The ubiquitous implementation of information and communication technologies (ICTs) is giving rise to cross-border security threats that require joint international responses. Fragmentation and growing conflict in the global information space complicates international cooperation within the UN to form a comprehensive global information security regime. Western countries actively support the formation of a cyber security regime based on Western values and promoted as a general initiative of the international community without taking into account the position of developing countries. An alternative approach focused on securing digital sovereignty is being promoted by many non-Western negotiating platforms, among which the BRICS occupies an important place. This article aims to assess the potential of BRICS influence in the framework of the international ICT security regime and the main directions of the BRICS activities in this area. In this paper, the BRICS agenda in the field of ICT security is studied on the basis of official documents of the annual summits and the main commitment made by the BRICS. The discourse analysis of the strategic planning documents of the BRICS countries allows to identify their priorities in the area under consideration, and to assess the potential for the implementation of the achieved obligations at the BRICS level. All the BRICS countries focus on ensuring sovereignty in the field of ICT. However, Russia, India and China consider digital development and ICT security as the most important direction of state policy and international cooperation; at the same time, they are more advanced in the field of digital technologies compared to other countries of the five and, as a result, are more vulnerable. In turn, Brazil and South Africa do not consider this area as a priority, placing more emphasis on ICT development and being more interested in access to technology and bridging the digital divide. However, all five countries are interested in solving the problem of extremism and terrorism in the digital sphere, which is also a promising area for the BRICS multilateral cooperation. A study of the voting of the BRICS countries in the UN and an analysis of their participation in alternative initiatives in the field of forming a cyber security regime promoted by Western countries showed the high efficiency of BRICS as a negotiating platform - the main contribution is made by developing a common position on the norms and principles of the international information security regime and their support at the UN level. Thus, BRICS can make a constructive contribution to the formation of the norms and principles of the international ICT security regime based on the principles of respect for state sovereignty, internationalization of the Internet governance, and counteraction to the criminal use of ICTs. An important advantage of BRICS in this area is the possibility of aggregating the interests and positions of developing countries.

Keywords:

BRICS; discourse analysis; ICT security; digital economy; global governance

References

Alpeev A.S. (2014). Terminologiya bezopasnosti: kiberbezopasnost', informacionnaja bezopasnost' [Terminology of Security: Cybersecurity, Information Security]. *Voprosy kiberbezopasnosti*. No. 5 (8). P. 39–42.

Abdenur, A. (2017). Can BRICS Cooperate in International Security? *Vestnik mezhdunarodnykh organizatsij*. Vol. 12. No. 3. P. 73–95.

Bezkorovajnyj M.M., Tatuzov A.L. (2014). Kiberbezopasnost' – podhody k opredeleniju ponjatija [Cybersecurity: Approaches to the Definition]. *Voprosy kiberbezopasnosti*. No. 1 (2). P. 22–27.

Belli L. (ed.) (2021). CyberBRICS: Cybersecurity Regulations in the BRICS Countries. Cham: Springer Nature. 280 p.

Bojko S.M. (2019). Problematika mezhdunarodnoj informatsionnoj bezopasnosti na ploshhadkakh ShOS i BRIKS [Problems of International Information Security at the SCO and BRICS Platforms] *Mezhdunarodnaya zhizn'*. No.1. P. 1–22.

Bojko S.M. (2022). *Mezhdunarodnaja informatsionnaja bezopasnost': novye vyzovy i ugrozy* [International Information Security: New Challenges and Threats]. *Mezhdunarodnaya zhizn'*. URL: https://interaffairs.ru/jauthor/material/2738 (accessed: 18.05.2023).

Bukht R., Hiks R. (2018). Opredelenie, konceptsiya i izmerenie tsifrovoj jekonomiki [Defining, Conceptualising and Measuring the Digital Economy]. *Vestnik mezhdunarodnyh organizacij*. Vol. 13. No.2. P. 143–172. DOI: 10.17323/1996-7845-2018-02-07

Chikhachev A.Yu. (2022). Rossijsko-francuzskie otnoshenija pri prezidente Jemmanjujele Makrone: dostizhenija i protivorechija [Russia-France Relations During E. Macrons's Term: Achievements and Challenges]. *Vestnik SPbGU. Mezhdunarodnye otnoshenija*. Vol. 15. P. 86–104.

Fick N., Miscik J. (2022). *Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet*. URL: https://www.cfr.org/task-force-report/confronting-reality-in-cyberspace (accessed: 16.05.2023).

Global Governance Program (2020). *Compliance Coding Manual for International Institutional Commitments*. URL: http://www.g7.utoronto.ca/compliance/Compliance_Coding_Manual_2020.pdf (accessed: 11.09.2022).

Hurel L.M., Lobato L. C. (2020). Cyber security in Brazil: keeping silos or building bridges? In: Romaniuk S.N., Manjikian M. (eds.) *Routledge Companion to Global Cyber-security Strategy*. London, Routledge. 656 p.

Ignatov A.A. (2020). Tsifrovaya jekonomika v BRIKS: Perspektivy mezhdunarodnogo sotrudnichestva [The Digital Economy of BRICS: Prospects for Multilateral Cooperation]. *Vestnik mezhdunarodnyh organizatsij*. Vol. 15. No.1. P. 31–62. DOI: 10.17323/1996-7845-2020-01-02

Ignatov A.A. (2022). Upravlenie Internetom v povestke BRIKS [The BRICS Agenda on the Internet Governance]. *Vestnik mezhdunarodnyh organizatsij*. Vol. 17. No 2. P. 86–109. DOI: 10.17323/1996-7845-2022-02-04

Kadulin V.E., Klochkova E.N. (2017). Sootnoshenie ponjatij "informacionnaya bezopasnost'" i "kiberbezopasnost'" v sovremennom pravovom pole [Correlation of Terms "Information Security" and "Cybersecurity" in Modern International Law]. *Voprosy kiberbezopasnosti*. No. 2 (20). P. 7–10.

Karchija A.A. (2014). Kiberbezopasnost' i intellektual'naja sobstvennost'. Chast' 1 [Cybersecurity and Intellectual Property. Part 1]. *Voprosy kiberbezopasnosti*. No.1 (2). P. 61–66.

Karpova D.N. (2014). Kiberprestupnost': global'naja problema i ee reshenie [Cybersecurity: Global Problem and Solution]. *Vlast'*. No. 8. P. 46–50.

KHabrieva T.Ya, Rujpin D. (Eds.) (2017). *Kiberprostranstvo BRIKS: pravovoe izmerenie* [BRICS Cyberdomain: Legislative Framework]. M.: Institut zakonodatel'stva i sravnitel'nogo pravovedenija pri Pravitel'stve Rossijskoj Federacii. 336 p.

KHegaturov A. (2019). *Kibermoshh' Irana* [Iran's Cyberpower]. Rossijskij sovet po mezhdunarodnym delam. URL: https://russiancouncil.ru/activity/digest/longreads/kibermoshch-irana/ (accessed: 19.12.2023).

Kirton J., Wang A.X. (2022). China's Complex Leadership in G20 and Global Governance: From Hangzhou 2016 to Kunming 2021. *Chinese Political Science Review*. P. 331–380. DOI: https://doi.org/10.1007/s41111-022-00213-9

Krasner S. (1982). Regimes and the limits of realism: Regimes as autonomous variables. *International Organization*. Vol. 36 (2). P . 497–510.

Krutskikh A.V. (2007). K politiko-pravovym osnovanijam global'noj informacionnoj bezopasnosti [On Political and Normative Foundations of Global Information Security]. *Mezhdunarodnye processy*. Vol. 5. No. 1(13). P. 28–37.

Krutskikh A.V. (2022). Mezhdunarodnaja informacionnaja bezopasnost': v poiskah konsolidirovannyh podhodov [International Information Security: In Search for Consolidated Approaches]. Vestnik RUDN. Serija: *Mezhdunarodnye otnoshenija*. Vol. 22. No. 2. P. 342–351.

Krutskikh A.V., Streltsov A.A. (2014). Mezhdunarodnoe pravo i problema obespechenija mezhdunarodnoj informacionnoj bezopasnosti [International Law and Issue of International Information Security Provision]. *Mezhdunarodnaja zhizn'*. No. 11. P. 20–34.

Kupriyanov A.V. (2019). Indija v jepokhu kibervojn [India in Times of Cyberwars]. URL: https://russiancouncil.ru/analytics-and-comments/analytics/indiya-v-epokhu-kibervoyn/ (accessed: 04.08.2022).

Kuznetsov D.A. (2020). Setevaja tekstura mirovoj politiki: transregionalizm BRIKS [Network Texture of World Politics: Transregionalism of BRICS]. *Mirovaja jekonomika i mezhdunarodnye otnosheniya*. Vol. 64. No. 11. P. 124–131.

Larionova M.V., Ignatov A.A., Popova I.M., Saharov A.G., Shelepov A.V. (2020). *Desjat' let BRIKS: chto dal'she?* [BRICS at Ten: The Way Forward]. M.: Delo, RANHiGS. 73 p.

Lebedeva M.M., Kuznetsov D.A. (2019). Transregionalizm – novyj fenomen mirovoj politiki // Polis [Transregional Integration as a New Phenomenon of World Politics: Nature and Prospects]. *Polis. Politicheskie issledovaniya*. No. 5. P. 71–84. DOI: 10.17976/jpps/2019.05.06

Lesazh, D. (2014). Tekushhaja programma dejstvij «Gruppy dvadcati» v sfere nalogooblozhenija: ispolnenie objazatel'stv, otchetnost' i legitimnost' [The Current G20 Taxation Agenda: Compliance, Accountability and Legitimacy]. *Vestnik mezhdunarodnyh organizatsij*. Vol. 9. No. 4. P. 40–54.

Massel' L.V., Voropaj N.I., Senderov S.M., Massel' A.G. (2016). Kiberopasnost' kak odna iz strategicheskih ugroz jenergeticheskoj bezopasnosti Rossii [Cybersecurity as One of Strategic Threats to Russia's Energy Security]. *Voprosy kiberbezopasnosti*. No. 4 (17). P. 1–10.

Malyuk A.A., Polyanskaya O.Ju. (2016). Zarubezhnyj opyt formirovanija v obshhestve kul'tury informacionnoj bezopasnosti [Fostering Information Security Culture: International Experience]. *Bezopasnost' informacionnyh tehnologij*. Vol. 23. No. 4. P. 25–37.

Mikhalevich E.A. (2017). Rossijsko-kitajskoe vzaimodejstvie po obespecheniju bezopasnosti v kiberprostranstve v ramkah BRIKS [Russia-China Cooperation in Cybersecurity Provision within BRICS]. *Svobodnaja mysl'*. No. 6 (1684). P. 155–160.

Panova V.V. (2015). Problemy bezopasnosti i perspektivy sammita BRIKS v Ufe [The BRICS Security Agenda and Prospects for the BRICS Ufa Summit]. *Vestnik mezhdunarodnyh organizacij*. Vol. 10. No. 2. P. 119–139.

Perminov V.A. (2019). Sektor informacionno-kommunikacionnyh tehnologij Brazilii: istorija, sovremennoe polozhenie i tendencii razvitija [Information and Communication Technologies Sector in Brazil: Histroty, Current State of Affairs, and Development Prospects]. *Jekonomicheskie otnoshenija*. Vol. 9. No. 3. P. 1519–1532.

Romashkina N.P. (2020). Problema mezhdunarodnoj informacionnoj bezopasnosti v OON [International Information Security Issue at the UN]. *Mirovaja jekonomika i mezhdunarodnye otnoshenija*. Vol. 64. No.12. P. 25–32.

Romashkina N.P., Zadremajlova V.G. (2020). Jevoljutsija politiki KNR v oblasti informacionnoj bezopasnosti [China's Information Security Policy Evolution]. *Put' k miru i bezopasnosti*. No.1 (58). P. 122–138. DOI: 10.20542/2307-1494-2020-1-122-138

Stadnik I.T., Tsvetkova N.A. (2021). Mesto i rol' stran Latinskoj Ameriki v sisteme mezhdunarodnoj i regional'noj kiberbezopasnosti [Latin American Countries Position Within Regional and Global Cybersecurity Systems]. *Latinskaya Amerika*. No. 4. P. 69–84.

Nye J.S. (2014). *The Regime Complex for Managing Global Cyber Activities*. URL: https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf (accessed: 11.09.2022).

Orji U. J. (2018). The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability? *Masaryk University Journal of Law and Technology*. Vol. 12. No. 2. P. 91–130. DOI: https://doi.org/10.5817/MUJLT2018-2-1

Vang A.S. (2022). Model' liderstva Kitaja v BRIKS [China's Leadership in BRICS Governance]. *Vestnik mezhdunarodnykh organizatsij*. Vol.17. No. 2. P. 50–85. DOI: 10.17323/1996-7845-2022-02-03

Zgoba A.I., Markelov D.V., Smirnov P.I. (2014). Kiberbezopasnost': ugrozy, vyzovy, reshenija [Cybersecurity: Threats, Challenges, Solutions]. *Voprosy kiberbezopasnosti*. No.5 (8). P. 30–38.

Zinovieva E.S. (2019). *Mezhdunarodnoe sotrudnichestvo po obespecheniju informacionnoj bezopasnosti: subjekty i tendentsii jevolyutsii*. [International Cooperation on Information Security Provision: Subjects and Evolution Tendencies] Diss. Na soiskanie uch.step. doktora nauk. M.: MGIMO. 362 p.

Zinovieva E.S. (2023). *Mezhdunarodnaja informatsionnaya bezopasnost' v dvustoronnikh otnosheniyakh Rossii i SShA* [International Information Security in Russia-USA Bilateral Relations]. Rossijskij sovet po mezhdunarodnym delam. URL: https://russiancouncil.ru/analytics-and-comments/analytics/mezhdunarodnaya-informatsionnaya-bezopasnost-v-dvustoronnikh-otnosheniyakh-rossii-i-ssha/?sphrase_id=98721820 (accessed: 18.05.2023).

Zinovieva E.S., Mishhishina E.E. (2022). *Formirovanie universal'noj terminologii v sfere MIB: politicheskie aspekty* [Formation of Universal Methodology in the Sphere of International Information Security: Political Aspects]. Rossijskij sovet po mezhdunarodnym delam. URL: https://russiancouncil.ru/analytics-and-comments/analytics/formirovanie-universalnoy-terminologii-v-sfere-mib-politicheskie-aspekty/ (accessed: 16.05.2023).