АНАЛИТИЧЕСКАЯ ЗАПИСКА

54 / 2024

Расширение БРИКС и перспективы сотрудничества стран объединения в вопросах развития цифровой экономики

Александр Игнатов

РСМД
Российский совет по международным делам

РОССИЙСКИЙ СОВЕТ ПО МЕЖДУНАРОДНЫМ ДЕЛАМ

Автор:
канд. полит. наук **А.А. Игнатов**

Редакторская группа:
канд. ист. наук **С.М. Гаврилова** (ответственный редактор), **К.К. Суховерхов**,
Д.О. Растегаев (выпускающий редактор)

Российский совет по международным делам (РСМД) — некоммерческая организация, ориентированная на проведение исследований в области международных отношений, выработку практических рекомендаций в интересах российских органов государственной власти, бизнеса, НКО и иных организаций, нацеленных на внешнеполитическую деятельность. Совет создан решением учредителей в соответствии с распоряжением Президента Российской Федерации от 2 февраля 2010 года № 59-рп «О создании некоммерческого партнерства "Российский совет по международным делам"».

РСМД — один из ведущих аналитических центров страны, осуществляющий работу по более чем 20 исследовательским направлениям. Экспертная деятельность Совета востребована российскими профильными ведомствами, академическим сообществом, российским и зарубежным бизнесом.

Председатель Попечительского совета РСМД — министр иностранных дел Российской Федерации Сергей Лавров. Президент РСМД, член-корреспондент РАН Игорь Иванов занимал пост министра иностранных дел России в 1998–2004 гг. и секретаря Совета Безопасности Российской Федерации в 2004–2007 гг. Генеральный директор Совета — Иван Тимофеев. Научным руководителем Совета является Андрей Кортунов.

УЧРЕДИТЕЛИ

Министерство иностранных дел Российской Федерации

Министерство образования и науки Российской Федерации

Российская академия наук

Российский союз промышленников и предпринимателей

Информационное агентство «Интерфакс»

Высказанные в аналитической записке мнения отражают исключительно личные взгляды и исследовательские позиции автора и могут не совпадать с точкой зрения Некоммерческого партнерства «Российский совет по международным делам».

Полный текст аналитической записки опубликован на интернет-портале НП РСМД.

Источник фото на обложке: РИА Новости / Алексей Майшев

Расширение БРИКС и перспективы сотрудничества стран объединения в вопросах развития цифровой экономики

Введение

Развитие цифровых технологий трансформирует структуру мировой политики и коренным образом меняет расклад сил на международной арене. Традиционные компоненты мощи государства: его вооруженные силы, экономический, научный и демографический потенциал, и, как результат, способность устанавливать приемлемую модель поведения других акторов международной политики и др. — претерпевают изменения. Сложно представить современный вооруженный конфликт без использования возможностей цифровых технологий для нанесения ущерба противнику, в том числе в рамках информационно-психологической борьбы. Целые отрасли экономики, в особенности реальное производство, перенимают новые веяния и внедряют передовые решения в области «интернета вещей», «больших данных» и технологий искусственного интеллекта. Цифровая революция соединила мир в единое информационное поле и сделала контакты между людьми и обществами по всей планете проще и эффективнее. В глазах технооптимистов ключ к решению глобальных проблем человечества: голода, неравенства, бедности, адаптации к изменению климата, предотвращению новых пандемий и т.п. — лежит в развитии цифровой экономики[1].

Однако блага растущей цифровой экономики неизбежно связаны с новыми угрозами. Информационная глобализация не только сблизила континенты и народы, но и стала катализатором развития международной киберпреступности, привела к небывалому распространению террористических и экстремистских идей и нарративов, а список угроз международной безопасности пополнился средствами кибернападения, способными нанести ущерб, сопоставимый с последствиями применения оружия массового поражения.

Другая характерная черта современности — существование правил и норм, способных сгладить растущие противоречия и сделать поведение акторов международной политики более предсказуемым. Эти правила формируются с опозданием, не успевая за трансформацией угроз. Несмотря на то, что в условиях существования глобальных вызовов под угрозой находятся все государства, наиболее уязвимыми являются страны т.н. мирового большинства. Вопреки позитивным изменениям последних десятилетий, существенная часть населения Земли и представляющих их суверенных государств (как в одиночку, так и в составе объединений) по-прежнему оказывает сравнительно небольшое или вовсе незначительное влияние на процесс формирования новых правил и структур глобального управления цифровой экономикой.

Всякий вызов создает предпосылки для принятия контрмер. В контексте глобализации эффективный ответ может быть сформулирован только коллективными усилиями. То, насколько этот ответ будет соответствовать критерию справедливости и насколько реально будут учитываться интересы всех вовлеченных сторон, непосредственно зависит от их активности на международной арене. В отсутствие возможности конструктивного участия в международных переговорах у многих государств незападного мира[2] объединение БРИКС стремится стать представителем их ин-

ОБ АВТОРЕ

Игнатов Александр Александрович *— канд. полит. наук, старший научный сотрудник Центра исследований международных институтов Института прикладной экономической политики РАНХиГС.*

[1] См., например: Lechman E., Popowska M. Harnessing digital technologies for poverty reduction. Evidence for low-income and lower-middle income countries. *Telecommunications Policy.* 2022. Vol. 6. No. 6.; Neto O.L., Wyl V.V. Digital Transformation of Public Health for Noncommunicable Diseases: Narrative Viewpoint of Challenges and Opportunities. *JMIR Public Health Surveill.* 2024. Vol. 10; Whitelaw S. et al. Applications of digital technology in COVID-19 pandemic planning and response. *The Lancet Digital Health.* 2020. Vol. 2. No. 8. P. 435-440.

[2] См., например, исследование причин низкой активности государств Африканского континента в переговорах на платформе ВТО: The E-Commerce Negotiations in the WTO. Understanding non-participation // National board of trade Sweden. URL: https://www.kommerskollegium.se/globalassets/publikationer/rapporter/2023/the-e-commerce-negotiations-in-the-wto.pdf

тересов, заявляя это в качестве одной из своих стратегических задач.

БРИКС успешно выполняет возложенную на него роль международной переговорной платформы — за более чем десятилетие работы государства-члены приняли сотни решений по ключевым вопросам повестки дня[3], а самый общий перечень обсуждаемых в рамках объединения вопросов включает десятки наименований от макроэкономической политики до противодействия экстремизму и терроризму, а также развитие ИКТ и цифровой экономики. В рамках БРИКС создано множество механизмов многостороннего сотрудничества, создан и функционирует Новый банк развития БРИКС, развивается взаимодействие в области безопасности и гуманитарных обменов. Десятки заявлений о желании вступить в БРИКС доказывают востребованность объединения и продвигаемой им международной повестки[4].

Радикальное расширение состава членов — стресс-тест для любого международного института[5], грозящий утратой сформировавшейся идентичности и внутренней синергии, особенно важных в вопросе совместного продвижения многосторонних инициатив. В рамках представленного исследования мы ответим на вопрос о том, какие возможности и вызовы создает расширение БРИКС в контексте реализации потенциала объединения в управлении развитием цифровой экономики.

БРИК(С) от Екатеринбурга до Йоханнесбурга: достигнутый прогресс

До момента расширения основные успехи БРИКС в деле многостороннего управления развитием цифровой экономики состоялись во многом благодаря лидерству России и Китая, чьи инициативы по большинству направлений пользуются поддержкой со стороны Бразилии, Индии и ЮАР. Именно с российского председательства в объединении БРИКС в 2015 г. повестка развития ИКТ оформляется как самостоятельное направление сотрудничества. Ранее эта проблематика обсуждалась на полях встреч министров по вопросам науки. Символическим началом этого процесса стала встреча министров связи БРИКС в Москве, где была принята первая совместная декларация о сотрудничестве[6].

Особенностью сотрудничества БРИКС по вопросам цифрового роста является разность условий развития национальной цифровой экономики, а значит, и позиционирования приоритетных вопросов для многостороннего обсуждения. С точки зрения основных показателей — доли населения, активно пользующегося интернетом, доли домохозяйств, имеющих персональный компьютер, распространения цифровых навыков, а также оценок в отношении размера цифрового рынка и адекватности мер противодействия киберугрозам и т.п. — лидерами в «старом» БРИКС являются Россия и Китай[7]. Общим для стран «пятерки» приоритетом взаимодействия остается развитие цифровой инфраструктуры, однако в деталях подходы стран отличаются. В случае Китая, Индии, ЮАР и Бразилии на передний план выходит развитие цифровой инфраструктуры отстающих в экономическом плане регионов, для которых также характерен сравнительно невысокий уровень доходов местного населения. Россия принимает во внимание развитие инфраструктуры регионов, однако здесь речь идет скорее об отдаленных и малонаселенных территориях без отягчающего фактора в виде низкого уровня доходов населения[8].

Даже несмотря на то, что угроза монополизации национального рынка платформенных услуг крупными зарубежными компаниями

[3] См. более подробно обзор достижений первых десяти лет работы БРИКС: Ларионова М.В. и др. Десять лет БРИКС. Что дальше? М.: Издательский дом «Дело», 2020. — 98 с.

[4] Более 40 стран хотят вступить в БРИКС, 6 стран уже получили официальное приглашение // Российская газета. 22.09.2023. URL: https://rg.ru/2023/09/22/strategicheskij-prioritet.html

[5] См., например, случай расширения Шанхайской организации сотрудничества: Муратбекова А. Кризис идентичности Шанхайской организации сотрудничества: что будет дальше? // Вестник международных организаций. 2019. Т. 14. № 4. С. 138-160.

[6] Communique of BRICS Ministers of Communications on the outcomes of the meeting "Expansion of Cooperation in the Field of Communications and ICTs" // BRICS. URL: http://en.brics2015.ru/load/637860

[7] См. информацию по ряду показателей: BRICS Joint Statistical Publication 2023 // Росстат. URL: https://rosstat.gov.ru/storage/document/document_statistic_collection/2024-01/15/BRICS%20Joint%20Statistical%20Publication-2023(1).pdf. См. также: Игнатов А.А. Цифровая экономика в БРИКС: перспективы многостороннего сотрудничества // Вестник международных организаций. 2020. Т. 15. № 1. С. 31-62.

[8] См.: Игнатов А.А. БРИКС в системе управления интернетом. М.: Инфра-М, 2024. С. 104-108.

признается во всех странах БРИКС, сопоставимый масштабу угрозы ответ в виде контрмер, предпринимаемых местными регуляторами с опорой на соответствующие правовые нормы, реализуется только в России и Китае. В России принята Концепция государственного регулирования цифровых платформ и экосистем[9], опубликованы отраслевые стандарты, регулирующие отдельные аспекты взаимодействия участников цифрового рынка[10]. В 2020–2021 гг. в Китае было разработано и принято Руководство по антимонопольному регулированию в сфере платформенной экономики[11], в Закон о противодействии монополиям были внесены специальные положения, касающиеся ситуации на рынке цифровых платформенных услуг, а также опубликовано Руководство по классификации онлайн-платформ[12].

В Бразилии, Индии и ЮАР аналогичный процесс находится на начальной стадии, т.е. на этапе обсуждения требований о локализации пользовательских данных, модерации распространяемого контента, информирования о готовящихся слияниях и поглощениях и т.д., либо попыток применения действующего законодательства для регулирования рыночной ситуации на практике. В бразильском парламенте с 2022 г. идет обсуждение Законопроекта №2.768 о регулировании онлайн-платформ, действие которого будет охватывать только крупные платформы преимущественно иностранного происхождения[13]. В Индии проект Закона о цифровой конкуренции был представлен для обсуждения в 2023 г.[14] Законопроект предполагает установление новых правил регулирования нескольких крупных цифровых платформ — «системно значимых цифровых предприятий», определяемых на основании данных о получаемом доходе. Содержательно Законопроект представляет попытку ввести регулирование *ex ante*, что соответствует передовому международному опыту, однако, по мнению правительственных экспертов, эта практика может оказаться контрпродуктивной в Индии как развивающейся экономике. В правовой системе ЮАР нет специального закона, который регулировал бы деятельность онлайн-платформ, что в сочетании с несовершенной институциональной структурой приводит к фрагментации системы регулирования и снижению эффективности принимаемых мер, корректирующих ситуацию в сфере рыночной конкуренции. Так, например, Комиссия по вопросам конкуренции ЮАР добилась выполнения поставленных перед компаниями — операторами онлайн платформ требований в части улучшения конкурентной ситуации на рынке всего в нескольких случаях из всего перечня выявленных в результате рыночного исследования проблем[15].

Таким образом, попытки использовать передовой международный опыт — например, модель Общего регламента по защите данных ЕС[16] — не всегда отвечают сложившимся на национальном уровне условиям, а БРИКС как объединению еще только предстоит обсуждение общей позиции в этой области.

Разнятся подходы стран «старой пятерки» и к обеспечению международной информационной безопасности[17]. Россия и Китай демонстрируют лидерство в отношении защиты национального информационного пространства. Политика этих стран отталкивается от приоритета «цифрового суверенитета» — обеспечения независимости государства в

[9] Концепция государственного регулирования цифровых платформ и экосистем // Министерство экономического развития РФ. URL: https://www.economy.gov.ru/material/departments/d31/koncepciya_gos_regulirovaniya_cifrovyh_platform_i_ekosistem/

[10] См., например: Стандарты по взаимодействию маркетплейсов с продавцами товаров (редакция № 3) // Ассоциация компаний интернет-торговли. 2024. URL: https://admin.akit.ru/wp-content/uploads/2024/08/240816-Standarty_MP_i_prodavtsy_redaktsiya_-_3.pdf; Стандарты по взаимодействию маркетплейсов с владельцами пунктов выдачи заказов // Контур Норматив. URL: https://normativ.kontur.ru/document?moduleId=1&documentId=458483

[11] Anti-monopoly regulation of digital platforms in China // CeCo. URL: https://centrocompetencia.com/anti-monopoly-regulation-of-digital-platforms-in-china/

[12] China's new platform guidelines // Data protection and digital competition. URL: https://www.ianbrown.tech/2021/11/01/chinas-new-platform-guidelines/

[13] Chiarini T. et al. Regulation of markets mediated by digital platforms in Brazil // Center for Research on Science, Technology and Society. 2023. URL: https://www.ipea.gov.br/cts/en/all-contents/articles/articles/381-regulation-of-markets-mediated-by-digital-platforms-in-brazil-an-open-discussion

[14] MCA invites public comments on Report of Committee on Digital Competition Law and Draft Bill on Digital Competition Law // Press Information Bureau. URL: https://pib.gov.in/PressReleasePage.aspx?PRID=2013947

[15] См.: Игнатов А.А. Регулирование цифровых платформ в БРИКС: приоритеты и опыт ЮАР // Вестник международных организаций. 2024. Т. 19. № 2. С. 161-182; а также исследование экспертов Всемирного банка: Al-Dahdah E. et al. South Africa — Digital Economy Diagnostic // World Bank Group. 2024. URL: https://documents.worldbank.org/en/publication/documents-reports/documentdetail/464421589343923215/south-africa-digitaleconomy-diagnostic

[16] Общий регламент защиты персональных данных (GDPR) Европейского союза // GDPR Text. URL: https://gdpr-text.com/ru/

[17] См.: Зиновьева Е.С., Шитьков С.В. БРИКС на пути обретения цифрового суверенитета? // Проблемы национальной стратегии. 2024. № 2 (83). С. 144-183.

цифровой сфере и поддержания способности к самостоятельной реализации информационной политики внутри страны и на международной арене[18], что объясняет жесткость в требованиях к локализации пользовательских данных, изъятию из оборота нежелательных материалов, содержащих преимущественно экстремистские и террористические нарративы. Самое важное, что наряду с юридическим аппаратом Россия[19] и Китай[20] обладают, вероятно, наибольшим опытом имплементации этих положений в повседневную практику. Например, компетентное российское ведомство — Роскомнадзор — обеспечило блокировку тысяч онлайн-страниц, содержащих экстремистскую пропаганду запрещенной в России группировки ИГИЛ[21]. Ежегодно Роскомнадзор принимает решения о блокировке тысяч интернет-ресурсов, распространяющих противоправную информацию[22]. Относительно масштабов блокировок нежелательных материалов в Китае существуют разные оценки. Так, согласно исследованию, проведенному в 2021 г., для интернет-адресов на территории Китая недоступны порядка 350 тыс. интернет-ресурсов, однако, возможно, это количество существенно больше, нежели было подтверждено в ходе проведенного тестирования[23]. Следует отметить, что до момента расширения из всех стран БРИКС только Россия и Китай рассматривались как страны с высоким потенциалом применения возможностей цифровых технологий в качестве средства нападения.

Ближе всех из числа стран-партнеров к «дуэту» России и Китая с точки зрения декларируемых приоритетов находится Индия, которая предпринимает меры по исключению из оборота контента определенного содержания, например, о деятельности групп сепаратистов. Имеется сообщение о том, что в период с 2015 по 2023 гг. в Индии были заблокированы более 55 тыс. сайтов, преимущественно независимых новостных порталов. Около половины случаев связаны с положениями Закона об информационных технологиях. Отличительной особенностью модели поведения индийских властей является отсутствие предварительного уведомления с требованием удалить нежелательный контент. Сообщается, что решение о блокировке практически невозможно оспорить поскольку распоряжения компетентных органов (если таковые имеют место, что напрямую не утверждается в тексте расследования) не объявляются открыто. В качестве недавнего примера упоминается происшествие с сайтом *Kashmirwalla*, который освещал ситуацию в штате Джамму и Кашмир и который одномоментно перестал быть доступным на территории Индии[24].

Бразилия и ЮАР отличаются от партнеров по объединению как с точки зрения декларируемых приоритетов, так и сложившейся практики реализации цифрового суверенитета. Эти государства можно отнести к сторонникам «мягкой концепции» цифрового суверенитета, что на практике означает, что в вопросах цифровой безопасности подход этих стран не ставит на передний план регулирование содержания распространяемого в сети контента, что характерно для позиций России, Китая и Индии[25].

Трансформация содержания дискуссии в рамках БРИКС по вопросам информационной безопасности, наблюдаемая в течение последних пяти-семи лет, происходит под влиянием России и поддерживающего ее предложения Китая. Москва, ставшая первопроходцем

[18] См.: Зиновьева Е.С., Игнатов А.А. «Цифровой суверенитет» в повестке объединения БРИКС // РСМД. 24.01.2024. URL: https://russiancouncil.ru/analytics-and-comments/analytics/tsifrovoy-suverenitet-v-povestke-obedineniya-briks/

[19] См.: Федеральный закон №139-ФЗ от 28 июля 2012 г. «О внесении изменений в Федеральный закон "О защите детей от информации, причиняющей вред их здоровью и развитию" и отдельные законодательные акты Российской Федерации по вопросу ограничения доступа к противоправной информации в сети Интернет» // Консультант Плюс. URL: https://www.consultant.ru/document/cons_doc_LAW_133282/

[20] См.: Provisions on the Governance of the Online Information Content Ecosystem // China Law Translate. URL: https://www.chinalawtranslate.com/en/provisions-on-the-governance-of-the-online-information-content-ecosystem/; а также: 2016 Cybersecurity Law // China Law Translate. URL: https://chinalawtranslate.com/en/2016-cybersecurity-law/

[21] Роскомнадзор заблокировал более 23 тысяч страниц на русском за пропаганду ИГИЛ // Интерфакс. 24.03.2017. URL: https://www.interfax.ru/russia/555127

[22] Роскомнадзор в 2024 году заблокировал более 170 тыс. страниц с запрещенным контентом // ТАСС. 17.04.2024. URL: https://tass.ru/obschestvo/20568701

[23] См.: Cimpanu C. China's Great Firewall is blocking around 311k domains, 41k by accident // The Record. 2021. URL: https://therecord.media/chinas-great-firewall-is-blocking-around-311k-domains-41k-by-accident; Hoang N.P. et al. How Great is the Great Firewall? Measuring China's DNS Censorship // ArXiv. 2021. URL: https://arxiv.org/abs/2106.02167

[24] Website blocking in India: One arrow for all // Advox. URL: https://advox.globalvoices.org/2024/08/19/website-blocking-in-india-one-arrow-for-all/

[25] См. более подробно: Зиновьева Е.С., Игнатов А.А. БРИКС в глобальном режиме ИКТ-безопасности // Международные процессы. 2023. Т. 21. № 4 (75). С. 104-132.

международной дискуссии по вопросам информационной безопасности на платформе ООН, добилась расширения многостороннего диалога в БРИКС в области цифровой безопасности на вопросы противодействия терроризму и экстремизму, что было зафиксировано в Антитеррористической стратегии БРИКС 2020 г.[26] и Плане по ее реализации 2021 г.[27] Российские инициативы получают поддержку со стороны Китая как в рамках БРИКС, так и на международной арене. Сближающим моментом является также общее членство в Шанхайской организации сотрудничества, в которую из «старой пятерки» также входит Индия, а повестка сотрудничества в области безопасности, в том числе в цифровом пространстве, развивается уже много лет[28]. Другие партнеры по объединению поддерживают предлагаемые инициативы, однако сами не выдвигают новые решения.

Иными словами, даже с учетом очевидных успехов многосторонней дипломатии нельзя не отметить, что сотрудничество в БРИКС по вопросам цифрового развития, хотя номинально и распространяется на широкий круг вопросов, реальную эффективность показывает либо там, где интересы стран-участниц сходятся без выраженных противоречий (инфраструктурное развитие), либо в областях, где у одной или нескольких стран имеется выраженный лидерский потенциал, достаточный для преодоления вероятных разногласий (позиция России в вопросах международной информационной безопасности). Эффективному сотрудничеству по другим направлениям — например, в вопросах регулирования деятельности цифровых платформ — препятствует выраженная разность в зрелости местных рынков.

БРИКС + 5: возможность или вызов?

Невозможно игнорировать комплексность вызова, который представляет из себя расширение состава постоянных членов объединения БРИКС. Необходима интеграция новых участников в устоявшиеся в рамках объединения переговорные практики, обеспечение их деятельного участия в работе уже запущенных механизмов. Вопрос о приоритетах новых стран в рассматриваемой области требует дополнительного разъяснения.

Пять новых стран — участниц БРИКС имеют еще больше различий в оценках цифровой развитости и положении в формирующейся системе управления развитием цифровой экономики (Табл. 1).

Таблица 1. Некоторые показатели цифровой развитости новых стран — участниц БРИКС

	Пользователи интернета, % населения	**Имеют мобильный телефон, % населения**	**Покрытие сетями сотовой связи 3G / 4G, % населения**	**Стоимость широкополосного подключения к интернету, % ВНД на душу населения**	**Объем передаваемого трафика посредством мобильных сетей, ГБ (внутри территории страны)**
Эфиопия	19,4 (2022 г.)	58,3 (2016 г.)	98,5 / 33 (2022 г.)	12,1 (2023 г.)	19,8 (2022 г.)
Египет	72,2 (2022 г.)	97,4 (2022 г.)	99,8 / 98 (2023 г.)	2,4 (2023 г.)	52,9 (2023 г.)
Иран	81,7 (2022 г.)	72,4 (2021 г.)	92 / 91 (2023 г.)	0,17 (2023 г.)	129 (2023 г.)
Саудовская Аравия	100 (2023 г.)	100 (2023 г.)	100 / 100 (2023 г.)	2,99 (2023 г.)	531 (2023 г.)
ОАЭ	100 (2023 г.)	100 (2023 г.)	99,8 / 98,5 (2023 г.)	0,44 (2023 г.)	172 (2023 г.)

Источник: ITU DataHub[29]

[26] Антитеррористическая стратегия БРИКС // Официальный сайт председательства Российской Федерации в БРИКС. URL: https://brics-russia2020.ru/images/114/81/1148163.pdf

[27] BRICS Counter terrorism Action Plan // BRICS India 2021. URL: https://brics2021.gov.in/brics/public/uploads/docpdf/getdocu-52.pdf

[28] Себекин С.А. Роль Шанхайской организации сотрудничества и БРИКС в обеспечении международной информационной безопасности в условиях продолжающегося конфликта на Украине // Российско-китайские исследования. 2022. Т. 6. № 4. С. 279-281.

[29] ITU DataHub. URL: https://datahub.itu.int/

Например, существенно отличается положение Саудовской Аравии, Объединенных Арабских Эмиратов и Эфиопии. Первые две страны представляют уже состоявшиеся и развитые рынки цифровых товаров и услуг, где государство может выбрать из постоянно расширяющегося пула международных регуляторных практик, имплементация которых на локальном уровне с большой вероятностью позволит достигнуть ожидаемых положительных эффектов. В свою очередь для Эфиопии первостепенным является вопрос развития базовой инфраструктуры[30], распространения основных цифровых навыков и защиты от лавинообразного роста цифровых уязвимостей, в том числе связанных с низкой цифровой грамотностью потребителей услуг финансовых онлайн-посредников. На фоне остальных выделяется положение Ирана — страна в течение многих лет развивается в условиях санкционного давления, ограничивающего присутствие на местном рынке крупных иностранных платформ. Не в каждом случае предлагаемые национальные аналоги пользуются активным спросом со стороны потребителей. Египет является одним из крупнейших в регионе цифровых рынков и в целом открыто позиционирует себя в международных делах, однако на национальном уровне режимы регулирования деятельности участников цифрового рынка и оборота пользовательских данных требуют качественного пересмотра для адаптации к современным реалиям.

Рассмотрим упомянутые выше и другие особенности позиционирования пяти новых членов объединения БРИКС более подробно.

Эфиопия проходит стадию интенсивного цифрового роста. В стране постепенно увеличивается доля людей, пользующихся интернетом и цифровыми технологиями в широком смысле на постоянной основе — в Эфиопии этот показатель оценивается на уровне 19,4%, что ниже среднего показателя стран Африки (37%)[31]. Свойственным этому этапу развития является быстрое распространение киберпреступности — совсем недавно Эфиопия вошла в пятерку стран мира, где риск столкнуться со случаем злонамеренного использования внутренних уязвимостей популярного программного обеспечения был наиболее велик[32]. По собственным оценкам, в 2022–2023 гг. потенциальный ущерб только отраженных кибератак мог составить около 330 млн долл., а общее количество зафиксированных случаев превысило к концу 2023 г. 18 тыс. — это обозначило четырехкратный рост по сравнению с предыдущим периодом (4 тыс. в конце 2022 г.)[33]. Международный союз электросвязи в своем рейтинге кибербезопасности поместил Эфиопию на 115 место из 182 оцененных государств[34].

В контексте Эфиопии определенную трудность представляет оценка размера внутреннего рынка цифровых товаров и услуг, а следовательно, и обоснованные выводы относительно ситуации в сфере конкуренции в этом сегменте. Доступные оценки с осторожностью говорят о доле связанных с ИКТ секторов в ВВП страны на уровне 2%[35], что ниже среднего показателя стран Восточной Африки. В других экспертных заключениях говорится о том, что весь цифровой сегмент экономики страны представляет из себя совокупность нескольких сотен (до 600) небольших ИТ-компаний[36]. Самые крупные представители местного цифрового бизнеса, преимущественно онлайн-маркетплейсы, такие как *Qefira*, *Engocha* и *Jiji*, характеризуются охватом 50–150 тыс. уникальных посетителей в месяц, при этом основной доход от рекламы и пользовательских интеракций забирает корпорация *Google*[37]. Сообщается, что местный аналог поисковика *Google* — *Yahoonoo*, отличительной особенностью которого была более качественная работа с семантикой

[30] См., например, стратегию цифрового развития страны: Digital Ethiopia 2025: Empowering the nation in the digital economy // Resilient. 11.04.2024. URL: https://resilient.digital-africa.co/en/blog/2024/04/11/digital-ethiopia-2025-empowering-the-nation-in-the-digital-economy/

[31] Africa's Internet use doubles in decade despite high costs (report) // Ecofin Agency. 27.02.2024. URL: https://www.ecofinagency.com/telecom/2702-45230-africas-internet-use-doubles-in-decade-despite-high-costs-report

[32] Microsoft Security Intelligence Report // Microsoft. URL: https://info.microsoft.com/SIRv24Report.html

[33] INSA saves 19 billion birrs in 9 months // INSA Ethiopia. URL: https://insa.gov.et/sv/web/en/w/insa-saves-19-billion-birrs-in-9-months

[34] Global Cybersecurity Index 2020 // ITU. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

[35] Ethiopia's digital economy is blooming, but needs investment // ECDPM. 21.11.2022. URL: https://ecdpm.org/work/ethiopias-digital-economy-blooming-needs-investment

[36] Review — Ethiopia's Digital Economy Report // Shega. URL: https://shega.co/post/review-ethiopias-digital-economy-report/

[37] Review of the Top 3 Online Marketplaces in Ethiopia: Engocha // Shega. URL: https://shega.co/post/review-of-the-top-3-online-marketplaces-in-ethiopia-engocha/

амхарского языка, — в настоящий момент не функционирует. Система регулирования деятельности онлайн-платформ в Эфиопии представляется фрагментированной, предоставляющей недостаточный уровень защиты конкуренции для местных бизнесов, обладающих слишком малым ресурсом, чтобы составить зарубежным компаниям полноценную конкуренцию.

Несколько иная ситуация сложилась в другом важном аспекте цифрового развития — управлении пользовательскими данными. Эфиопия заимствовала опыт европейского Общего регламента по защите данных (*GDPR*), с которым действующее с апреля 2024 г. Постановление о защите данных[38] разделяет используемые определения, перечни прав и обязанностей субъектов и операторов данных, а также положения о трансграничной передаче данных. Эксперты[39] выделяют разницу в реализации положений эфиопского Постановления и европейского *GDPR* в части обязанности уничтожать по запросу субъектов данных собранные личные данные. Считается, что *GDPR* напрямую не требует от контролеров данных обеспечить стирание данных обработчиками данных, что непосредственно указано в положениях Постановления.

Эфиопия не относится к активным акторам формирующихся механизмов управления цифровой экономикой. Во многом это обусловлено общим для большинства стран Африки набором проблем — в частности, недостатком компетенций и ресурсов для непрерывного участия в многосторонней дискуссии. Это проявляется в переговорах по вопросу регулирования цифровой торговли в рамках ВТО. Эфиопия вместе с другими государствами Африки действует в составе т.н. Африканской группы, что позволяет стране номинально заявлять о своих интересах на международном уровне, но одновременно «растворяет» ее местные особенности в усредненной коллективной позиции. Двусторонние договоренности Эфиопии с американским бизнесом[40], правительствами Китая[41], Индии[42] и Великобритании[43], а также с ЕС[44] напрямую не касаются проблематики цифрового роста и чаще всего нацелены на решение базовых проблем развития. Реализация этих проектов, вероятно, окажет каталитическое воздействие и на цифровой рост за счет повышения благосостояния местного населения, и, как следствие, на рост спроса на цифровые продукты и услуги, создавая стимул для развития цифровых отраслей.

Среди стран Африки ***Египет*** обладает одним из крупнейших цифровых рынков, характеризующимся достаточно высокими по сравнению с другими развивающимися странами показателями доступа к цифровой инфраструктуре и в городских, и в сельских регионах. Согласно статистике, в Египте более 70% населения регулярно пользуются интернетом, персональным компьютером обладают не менее 70% домохозяйств. Инфраструктура широкополосной связи позволяет достигать показателей средней скорости обмена данными на отметке 10 Мбит/сек[45].

Для развития национальной правовой рамки управления пользовательскими данными Египет перенял опыт европейского Общего регламента по защите данных. Египетский Закон о защите данных 2020 г.[46] использует схожие с *GDPR* определения, действие Закона имеет экстерриториальный характер, а трансграничная передача пользовательских данных требует разрешение от компетентного органа

[38] Personal Data Protection Proclamation 1321/2024 // BonelliErede. 07.05.2024. URL: https://www.belex.com/en/case_study/personal-data-protection-proclamation-1321-2024/

[39] Ethiopia: General overview of Ethiopia's first personal data protection proclamation in light of the EU GDPR // DataGuidance. URL: https://www.dataguidance.com/opinion/ethiopia-general-overview-ethiopias-first-personal

[40] Microsoft Chooses Ethiopia As One of Africa New Digital Development Programme // Fana BC. URL: https://www.fanabc.com/english/microsoft-chooses-ethiopia-as-one-of-africa-new-digital-development-programme

[41] См.: Interview: BRI cooperation with China transforms Ethiopian lives for better // Belt and road portal. 26.03.2024. URL: https://eng.yidaiyilu.gov.cn/p/0SAV3Q82.html ; а также: Chinese investment hailed as essential driver of Ethiopia's economic development // Xinhua. 23.06.2024. URL: https://english.news.cn/africa/20240623/f12d2b70246f41d3baac0a315bd5f0c8/c.html

[42] Цуканов Л.В. Технологический ренессанс в Африке южнее Сахары: вызовы и возможности для России // ПИР-Центр. 2024. URL: https://pircenter.org/editions/37-2024-tehnologicheskij-renessans-v-afrike-juzhnee-sahary-vyzovy-i-vozmozhnosti-dlja-rossii/

[43] UK — Ethiopia development partnership summary, July 2023 // UK Government. 17.07.2023. URL: https://www.gov.uk/government/publications/uk-ethiopia-development-partnership-summary/uk-ethiopia-development-partnership-summary-july-2023#key-programmes

[44] EU, OACPS and UNCDF to Launch a New Programme on Digital Finance in Ethiopia // UNCDF. URL: https://www.uncdf.org/article/6852/eu-oacps-and-uncdf-to-launch-a-new-programme-on-digital-finance-services-in-ethiopia

[45] Digital Development Dashboard // ITU. URL: https://www.itu.int/en/ITU-D/Statistics/Dashboards/Pages/Digital-Development.aspx

[46] Egypt — Data Protection Overview // DataGuidance. URL: https://www.dataguidance.com/notes/egypt-data-protection-overview

и допускается только в юрисдикциях, статус которых определяется национальным регулятором как надежный.

На фоне распространения доступа в интернет в Египте наблюдается массированный рост количества фиксируемых киберинцидентов. Особенно быстрый рост наблюдается в сфере финансовых технологий: в 2022–2023 гг. количество попыток получения несанкционированного доступа в банковские системы возросло на 186%; за то же время число инцидентов с кражей пользовательских данных при помощи фишинговых ссылок выросло почти на 50%[47]. В своей региональной группе Египет занимает 4-е место по уровню готовности к цифровым вызовам, уступая Саудовской Аравии, ОАЭ и Оману[48].

Египет реализует достаточно жесткий подход к регулированию деятельности сетевых медиа. Согласно положениям Закона о регулировании СМИ и прессы 2018 г.[49], все сетевые информационные платформы с аудиторией более 5 тыс. пользователей относятся к категории СМИ и обязаны выполнять требования по противодействию распространению фейков и недостоверной информации. Запуск страницы в египетском домене интернета требует получения специальной государственной лицензии. Закон о противодействии киберпреступлениям и неправомерному использованию ИКТ 2018 г.[50] обязывает телекоммуникационные компании сохранять данные пользователей в течение 180 дней и обеспечивать правоохранительным органам доступ к ним в интересах противодействия экстремистской и террористической пропаганде среди молодежи. Блокировки интернет-ресурсов по подозрению в распространении запрещенной информации могут проходить в досудебном порядке. МИДу Египта поручено заключать с иностранными государствами соглашения о блокировке интернет-ресурсов, распространяющих неправомерную информацию. Египет, Саудовская Аравия и США стали учредителями Глобального центра по противодействию экстремистской идеологии «Этидаль»[51].

На цифровом рынке Египта широко представлены иностранные компании и платформы, которые занимают лидирующее положение во многих сегментах: поисковых систем, социальных сетей, доставки еды. К настоящему моменту не удалось обнаружить сообщения о проведенных или проводимых местным регулятором масштабных исследований состояния рыночной конкуренции. В отсутствии специализированного закона о деятельности цифровых платформ управление угрозами монополизации рынка иностранными компаниями происходит в соответствии с Законом о конкуренции 2005 г.[52] Эксперты ЮНКТАД утверждают, что местный регулятор испытывает определенные трудности с определением рыночного положения цифровых компаний, а также рекомендуют внести в действующий закон множество поправок, которые позволят бороться со злоупотреблениями рыночным положением, в частности, отказами от поддержания интероперабельности платформ и неравномерным доступом пользователей к информации[53].

Египет достаточно активно проявляет себя на международной арене. Представители Египта участвовали в работе Группы правительственных экспертов ООН по вопросам международной информационной безопасности с 2012 по 2017 гг., а также внесли на рассмотрение ряд замечаний, касающихся полномочий, структуры и содержания работы обсуждаемого Механизма регулярного межинституци-

[47] 49% increase in phishing attacks in Egypt during 1Q 2023: Kaspersky // Daily News Egypt. 07.05.2023. URL: https://www.dailynewsegypt.com/2023/05/07/49-increase-in-phishing-attacks-in-egypt-during-1q-2023-kaspersky/

[48] Global Cybersecurity Index 2020 // ITU. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

[49] Law No. 180 of 2018 on Press, Media and the Supreme Council for Media Regulation, Egypt // WIPO Lex. URL: https://www.wipo.int/wipolex/en/legislation/details/19960/. См. также: Egypt targets social media with new law // Reuters. 18.07.2018. URL: https://www.reuters.com/article/world/egypt-targets-social-media-with-new-law-idUSKBN1K720I/

[50] Law No. 175 of 2018 on Anti-Cyber and Information Technology Crimes, Egypt // WIPO Lex. URL: https://www.wipo.int/wipolex/en/legislation/details/19959

[51] Etidal and Telegram Combat Extremist Propaganda by Removing 18 Million Extremist Content for the Second Quarter of 2024 // Etidal. 02.07.2024. URL: https://etidal.org/en/etidal-and-telegram-combat-extremist-propaganda-by-removing-18-million-extremist-content-for-the-second-quarter-of-2024/

[52] Law No. 3 of 2005 Promulgating the Law on the Protection of Competition and the Prohibition of Monopolistic Practices // WIPO Lex. URL: https://www.wipo.int/wipolex/en/legislation/details/7409

[53] Voluntary peer review of competition law and policy of Egypt: Overview // UNCTAD. URL: https://unctad.org/system/files/official-document/ciclpd75_en.pdf

онального диалога по вопросам безопасности в использовании ИКТ[54]. Египет участвует в переговорах на платформе ВТО по вопросам регулирования электронной торговли и поддерживает рабочую программу 1998 г.[55] По предложению Египта в рабочую повестку Африканского союза были внесены положения, касающиеся управления развитием искусственного интеллекта[56].

Иран достиг достаточно высоких показателей цифрового развития в сравнении с группой стран схожего уровня благосостояния. Доля пользующегося интернетом населения оценивается в 80%; около 92% населения проживает в районах, охваченных сетями беспроводной связи четвертого поколения (*4G*)[57]. Основной интернет-трафик передается посредством мобильных подключений. По объемам передачи данных по широкополосным сетям Иран уступает странам с сопоставимым уровнем развития. Размер цифрового рынка страны оценивается в 24,6 млрд долл. с перспективой роста до 29 млрд долл. к 2029 г. Высокая доля молодого населения (до 35 лет) создает предпосылки для развития цифровых секторов благодаря ожидаемому росту спроса[58].

Иран реализует политику наращивания потенциала использования киберпространства для проведения специальных операций. В то же время сам Иран испытывает трудности в противодействии киберугрозам: согласно статистике, в 2023 г. в Иране в результате утечек данных пострадали порядка 150 млн пользователей электронных товаров и услуг, что говорит о том, что каждый активный пользователь интернет-услуг в Иране мог стать жертвой утечки данных минимум дважды в течение года[59].

В регулировании оборота пользовательских данных и работы онлайн-платформ Иран руководствуется действующими законами[60], которые пока что не содержат специальных положений, отражающих, например, особые условия конкуренции на цифровом рынке. Это оставляет отдельные категории пользовательских данных незащищенными, то есть получение к ним несанкционированного доступа может не рассматриваться в качестве состава преступления. Даже в условиях отсутствия на рынке крупных зарубежных игроков, существует угроза монополизации и злоупотребления лидирующим положением на рынке со стороны национальных компаний.

Достаточно хорошо известна жесткая позиция руководства Ирана относительно регулирования цифрового контента. Компетентные органы блокируют доступ ко многим популярным приложениям и платформам, а также демонстрируют высокий потенциал в отношении ограничения интернет-трафика — например, на фоне протестов 2019 г. в течение недели интернет-трафик не превышал 4–5% от нормальных показателей[61]. Имеется обширный перечень материалов[62], запрещенных к распространению в Иране, включая как призывающие к противоправным действиям, так и порочащие образ почитаемых в исламе святых и препятствующие проведению парламентских выборов. Все государственные учреждения подключены к «особому интернету», доступ к которому закрыт для интернет-адресов, расположенных за пределами страны.

---

[54] См.: Концептуальный документ Российской Федерации по организации под эгидой Организации Объединенных Наций регулярного институционального диалога с участием всех государств-членов ООН по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий // ООН. URL: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/RUS_Regular_institutional__dialogue_Proposal_of_the_Russian_Federation.pdf

[55] См.: Wunsch-Vincent S. WTO, E-commerce, and Information Technologies // Markle Foundation. URL: https://metacept.com/wp-content/uploads/2019/10/Chapter-1.1.pdf

[56] African Bodies: AU AI Working Group holds first session // DataGuidance. URL: https://www.dataguidance.com/news/african-bodies-au-ai-working-group-holds-first-session

[57] Iran // ITU Data Hub. URL: https://datahub.itu.int/data/?e=IRN

[58] Iran ICT Market Size & Share Analysis — Growth Trends & Forecasts (2024–2029) // Mordor Intelligence. URL: https://www.mordorintelligence.com/industry-reports/iran-ict-market

[59] Some Critical Data Breach Statistics and Facts for People To Be Well Prepared To Fight Against Cybercrime // Enterprise Apps Today. 05.03.2024. URL: https://www.enterpriseappstoday.com/stats/data-breach-statistics.html

[60] См., например, Закон о конкуренции: Islamic Republic of Iran "Law on Implementation of General Policies of Principle (44) of the constitution" // ФАС России. URL: https://fas.gov.ru/upload/other/ISLAMIC%20REPUBLIC%20OF%20IRAN%20LAW.pptx. В силу ограниченности доступа к интернет-ресурсам внутри страны для пользователей за пределами Ирана, информация о содержании проекта Закона о защите данных может быть получена только из косвенных источников. См.: Iran. Summary // DataProtection. URL: https://www.dataguidance.com/jurisdiction/iran

[61] Internet disrupted in Iran amid fuel protests in multiple cities // NetBlocks. 15.11.2019. URL: https://netblocks.org/reports/internet-disrupted-in-iran-amid-fuel-protests-in-multiple-cities-pA25L18b

[62] Hashemzadegan A., Gholami A. Internet Censorship in Iran: An Inside Look. *Journal of Cyberspace Studies*. 2022. Vol. 6(2). P. 183-204.

На международной арене Иран занимает бескомпромиссную антизападную позицию, однако влияние страны на принимаемые решения в рамках ключевых институтов представляется ограниченным. Иран активен на двустороннем уровне в вопросах цифрового сотрудничества. Ряд соглашений в области цифровой безопасности действуют между Ираном и Россией, Ираном и Китаем. Укреплению связей между странами способствует общее членство в Шанхайской организации сотрудничества, а теперь и в объединении БРИКС.

Королевство Саудовская Аравия (КСА) и ***Объединенные Арабские Эмираты (ОАЭ)*** являются не только географическими соседями, но и близкими партнерами в вопросах цифрового развития. Оба государства, владея значительными запасами углеводородов, достигли высочайших показателей в отношении развитости цифровой инфраструктуры и обеспечения доступности цифровых услуг для населения. Достигнуты 100% доли населения, пользующегося интернетом, а также 100% охват населения сетями связи пятого поколения[63]. Успехи в области цифровизации объясняются не только высоким уровнем благосостояния, обеспеченного экспортом нефти, но и компактностью проживания населения при его относительно небольшой численности, чем особенно показателен кейс ОАЭ, где большая часть 10-миллионного населения страны проживает в двух крупнейших эмиратах Абу-Даби и Дубай. Практически все население КСА и ОАЭ активно пользуется социальными сетями, а объем передаваемых данных в расчете на пользователя в год многократно превышает среднемировой показатель[64].

Саудовская Аравия и ОАЭ создали общий режим регулирования оборота пользовательских данных, который действует на территории двух государств с 2023 г. и опирается на положения специального Закона о защите данных[65]. Эксперты считают, что в его основу лег опыт европейского *GDPR*.[66] Разделяя ключевые определения и концепции европейской модели, действующий в КСА и ОАЭ закон отличается некоторыми деталями, что продиктовано культурными особенностями двух стран — так, например, согласно *GDPR* ребенком считается лицо, не достигшее 16 лет, тогда как в КСА и ОАЭ этот порог снижен до 13 лет. Трансграничная передача данных по умолчанию осуществляется только в надежные юрисдикции и не допускается без соответствующего разрешения компетентных органов. Действуют положения о локализации пользовательских данных.

Общими для двух стран являются основные характеристики цифрового рынка. В этих странах широко представлены международные зарубежные цифровые платформы, которые занимают лидирующее положение в сегментах социальных сетей, мессенджеров и торговых площадок, однако в сегментах доставки еды, организации перевозок и размещении туристов местные компании успешно конкурируют с иностранными. Среди действующих законов в КСА и ОАЭ нет специальных законов, регулирующих деятельность участников цифрового рынка для противодействия угрозы монополизации, однако в целом уровень рыночной концентрации в обеих странах оценивается как низкий[67].

Быстрое развитие цифровой экономики в КСА и ОАЭ сопряжено с ростом цифровых уязвимостей, однако такие оценки Международного союза электросвязи говорят о том, что реализуемая в этих странах политика позволяет обеспечить эффективное противодействие киберугрозам[68]. Многие виды правонарушений, совершаемых при помощи ИКТ, криминализированы и караются тюремным заключением на срок до 10 лет и штрафами более 1 млн долл. Общим «слабым местом» политики кибербезопасности в этих странах является дефицит квалифицированных кадров, что обозначено одним из основных вызовов в со-

[63] См., например: Saudi Arabia // ITU Data Hub. URL: https://datahub.itu.int/data/?e=SAU, а также United Arab Emirates // ITU Data Hub. URL: https://datahub.itu.int/data/?e=ARE

[64] Среднемировой показатель равен 134 ГБ (см. сноску 45).

[65] Personal Data Protection Law // Saudi Data & AI Authority. URL: https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf

[66] Sanjana S., Keyhani N. How does the new UAE Federal Decree Law on Personal Data Protection compare against the GDPR? // Bird & Bird. URL: https://www.twobirds.com/en/insights/2021/uae/how-does-the-new-uae-federal-decree-law-on-personal-data-protection-compare-against-the-gdpr

[67] Saudi Arabia ecommerce Market Size (2024–2029) // Mordor Intelligence. URL: https://www.mordorintelligence.com/industry-reports/saudi-arabia-ecommerce-market/market-size

[68] См.: Глобальный индекс кибербезопасности МСЭ 2020 год // ITU. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-R.pdf

ответствующих стратегических документах[69]. КСА и ОАЭ реализуют политику привлечения иностранных специалистов, а также внедряют требования по развитию необходимых компетенций в рамках образовательных программ.

КСА более активно проявляет себя на международной арене, хотя в целом подход Саудовской Аравии и ОАЭ можно охарактеризовать как осторожный и взвешенный. КСА пользуется своим положением члена «Группы двадцати», однако фокус ее политики в «двадцатке» в данный момент в основном направлен на вопросы справедливого энергетического перехода, на фоне которых проблемы цифрового развития отходят на второй план. КСА и ОАЭ неохотно принимают на себя новые международные обязательства и чаще всего присоединяются к уже заявленным инициативам, вокруг которых сложился устойчивый круг поддерживающих стран. Так, например, представители КСА участвовали в заседаниях РГОС ООН в 2019–2021 гг., но ни разу не заявляли собственные инициативы. Оба государства поддержали недавно представленный проект текста Соглашения о регулировании электронной торговли ВТО (*E-Commerce Joint Initiative*)[70]. Всего о поддержке инициативы заявили 80 государств-членов ВТО.

Заключение

Расширение БРИКС приводит за стол переговоров неформального объединения очень разные в отношении цифровой политики страны. Без сомнения, это отвечает духу БРИКС и его нацеленности на представление интересов мирового большинства во всем его разнообразии. Однако нельзя игнорировать и вероятное воздействие выявленных различий на переговорный процесс.

Наиболее перспективным направлением многостороннего сотрудничества в расширенном БРИКС в цифровой сфере остается обеспечение цифровой безопасности. Четыре из пяти новых стран-участниц (Иран, Египет, ОАЭ, Саудовская Аравия) на концептуальном уровне разделяют жесткий подход лидеров объединения — России и Китая — к реализации цифрового суверенитета. Это обстоятельство, а также (отчасти) перекрестное членство России, Китая, Ирана и Индии в ШОС позволят добиться большей идейной консолидации внутри объединения по вопросам международной информационной безопасности и создадут предпосылки для более активного практического сотрудничества — например, в деле исключения из цифрового пространства нежелательных нарративов и обмена информацией о произошедших или прогнозируемых киберинцидентах на условиях доверия. Идейное сближение позволит более эффективно продвигать разделяемые интересы и ценности в рамках ключевых глобальных институтов, в особенности, на платформе ООН.

Обеспечить сохранение и рост доверия между странами — участницами объединения крайне важно, особенно на фоне сохраняющихся двусторонних противоречий. Еще недавно Саудовская Аравия и Иран не имели полноценных дипломатических отношений, а Египет и Эфиопия еще не достигли компромисса в пользовании доступных водных ресурсов региона. БРИКС также должен сохранить свой глобальный, межцивилизационный характер, избежать проблем, характерных для институтов, поддерживаемых странами глобального Севера, и не допустить переключения фокуса работы объединения преимущественно на проблемы одного региона в свете существенного усиления представительства государств Африки и Ближнего Востока.

Потребность в развитии цифровой инфраструктуры и кадрового потенциала в новых странах — участницах БРИКС создает спрос на инвестиции, квалифицированные кадры и обмен наилучшими практиками. На этом фоне можно ожидать оживления внутренних механизмов многостороннего сотрудничества БРИКС, а также формирования новых инициатив и проектов. В этом процессе важно сохранить баланс между желанием создавать

[69] См.: (Saudi Arabia) National Cybersecurity Strategy // National Competitiveness Center. URL: https://www.ncc.gov.sa/en/Aboutus/Pages/Cybersecurity.aspx ; а также (UAE) National Cybersecurity Strategy // The United Arab Emirates' Government Portal. URL: https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/strategies-plans-and-visions-untill-2021/national-cybersecurity-strategy-2019

[70] Singh M. Saudi Arabia joins global e-commerce agreement // Gulf Business. 29.07.2024. URL: https://gulfbusiness.com/saudi-arabia-global-e-commerce-agreement

новые платформы и механизмы и растущей вместе с этим внутрисистемной нагрузкой в интересах поддержания достигнутого качества многостороннего взаимодействия в рамках объединения[71].

По некоторым вопросам включение новых членов в объединение БРИКС означает необходимость постановки новых задач. Например, крайне важно и желательно добиться консолидации позиций членов БРИКС по вопросам регулирования электронной торговли, а также запустить процесс согласования общих подходов к защите конкуренции на цифровых рынках. Этому может эффективно способствовать проведение совместных многосторонних консультаций на постоянной основе, а также формирование пула наилучших регуляторных практик, сформировавшихся на пространстве БРИКС.

[71] В развитии БРИКС ранее обнаруживались тревожные тенденции. См.: Игнатов А.А. Саммит БРИКС в Йоханнесбурге: больше механизмов и меньше конкретных решений // Вестник Российского Университета Дружбы Народов. Серия: Международные отношения. 2019. Т. 19. № 1. С. 89-99.

Тел.: +7 (495) 225 6283

Факс: +7 (495) 225 6284

welcome@russiancouncil.ru

russiancouncil.ru