

Политика стран БРИКС по защите цифрового суверенитета в контексте преодоления вызовов цифрового неоколониализма

Н.В. СИДОРЕНКО*

МГИМО МИД России (Россия)

В.А. ДМИТРИЕВА**

МГИМО МИД России (Россия)

М.И. САВЧЕНКОВА***

МГИМО МИД России (Россия)

Аннотация

Статья посвящена анализу феномена цифрового неоколониализма и проблематике обеспечения цифрового суверенитета государств в условиях трансформации глобального цифрового пространства. Концепция цифрового суверенитета в последние годы набирает популярность в мировых общественно-политических кругах: так, вопросы цифрового суверенитета поднимаются на надгосударственном (ЕС, Всемирный экономический форум) и государственном (например, Канада) уровнях. Страны БРИКС не отстают от этой тенденции: в каждой стране на текущем этапе реализуются инициативы по усилению государственного цифрового суверенитета, закрепленные в государственном регулировании. Некоторые исследователи связывают это с возрастающим «колониализмом данных» транснациональных цифровых корпораций, использующих данные населения стран в обмен на услуги (в некоторых статьях феномен получил название цифрового неоколониализма). В рамках исследования ставятся следующие задачи: во-первых, конкретизировать понятия «цифровой суверенитет» на основе современных отечественных и зарубежных академических подходов; во-вторых, провести сравнительный анализ институциональных, нормативно-правовых и стратегических основ политики стран-членов объединения БРИКС в сфере защиты цифрового суверенитета; в-третьих, сформулировать и обосновать сценарий развития сотрудничества стран БРИКС по вопросам защиты цифрового суверенитета в контексте международных вызовов

* **Сидоренко Наталья Валерьевна** – кандидат политических наук, преподаватель кафедры мировых политических процессов, Факультет управления и политики, МГИМО МИД России, 119454, Москва, проспект Вернадского 76.

E-mail: nataly.sidorenko@bk.ru

** **Дмитриева Валентина Андреевна** – кандидат политических наук, МГИМО МИД России, 119454, Москва, проспект Вернадского 76.

E-mail: dmitrieva.v.a@my.mgimo.ru

*** **Савченкова Мария Игоревна** – аналитик Проектного офиса Минобрнауки России на базе МГИМО, магистрант, Управление магистерской подготовки, МГИМО МИД России 119454, Москва, проспект Вернадского 76.

E-mail: savchenkova.maria@mail.ru

цифрового неоколониализма. Цель настоящей статьи – определить современный политический курс стран БРИКС по защите цифрового суверенитета в связи с возникающими вызовами цифрового неоколониализма. Для этого представляется необходимым выявить черты цифрового суверенитета и дать определение цифрового неоколониализма, отметить общие шаги стран БРИКС в контексте защиты цифрового суверенитета, определить национальные модели защиты цифрового суверенитета (с учетом новых участников) и выявить ограничения для развития общего подхода стран БРИКС к цифровому суверенитету. Для реализации поставленной цели применяются методы кейс-стади, анализа документов, сравнительный метод и сценарный метод. Полученные выводы позволяют оценить потенциал и пределы кооперации стран БРИКС в сфере цифровой политики и определить возможные направления формирования согласованных подходов к защите цифрового суверенитета.

Ключевые слова

цифровой суверенитет, цифровой колониализм, неоколониализм, страны БРИКС, вопросы защиты, вестфальская система, цифровая среда, транспарентность

Для цитирования

Сидоренко Н.В., Дмитриева В.А., Савченкова М.И. (2026). Политика стран БРИКС по защите цифрового суверенитета в контексте преодоления вызовов цифрового неоколониализма. *Управление и политика*. 5(2). С. 51–69. DOI: 10.24833/2782-7062-2026-5-2-51-69

Конфликт интересов

авторы заявляют об отсутствии конфликтов интересов

Благодарности

Исследование выполнено за счет средств гранта №КМУ-16/02 «Политика стран БРИКС по защите цифрового суверенитета в контексте преодоления вызовов цифрового неоколониализма».

Авторы выражают признательность А.А. Игнатову и В.М. Жорнист за полезные замечания.

Понятия «цифровой суверенитет государства» и «цифровой неоколониализм», подобно многим категориям политической науки, демонстрируют различия в трактовках, обусловленные принадлежностью исследовательских традиций к различным школам.

В отечественном (российском) подходе цифровой суверенитет, как правило, рассматривается через призму безопасности, контроля над критической инфраструктурой.

В западном подходе акцент научных публикаций лежит в более прикладной плоскости: в центре большинства западных исследований лежит баланс между государственным регулированием и защитой

цифровых прав индивида. В западной школе изучения цифрового суверенитета выделяются направления исследований, фокусирующиеся на концепте «data governance», вопросах транспарентности работы платформ, обсуждении наднациональных регуляторных механизмов (например, в рамках ЕС). Ключевыми вопросами, связанными с понятием цифрового суверенитета западной традиции, являются управление цифровыми потоками и стандартами.

Однако при анализе терминов необходимо вернуться к истокам. Вопрос о цифровом суверенитете невозможно рассматривать изолированно от эволюции самого понятия суверенитета, укорененного в вестфальской политико-правовой традиции.

Несмотря на растущий интерес академического сообщества к вопросам цифрового суверенитета и цифрового неокOLONиализма, в научной литературе по-прежнему сохраняется фрагментарность понятийного аппарата и недостаточная сопоставимость национальных кейсов, особенно в отношении стран БРИКС. Это обуславливает необходимость конкретизации ключевых понятий, а также комплексного сравнительного анализа нормативно-правовой базы государств объединения в цифровой сфере.

Особое значение проблематика цифрового суверенитета приобретает для стран БРИКС, выступающих важными акторами формирующегося многополярного мирового порядка. Страны БРИКС демонстрируют различный уровень технологического развития, что влияет на многообразие подходов к регулированию цифрового пространства. В то же время объединение обладает значительным потенциалом для выработки альтернативных моделей цифрового развития и коллективного реагирования на вызовы цифрового неокOLONиализма.

Понятия «цифровой суверенитет государства» и «цифровой неокOLONиализм» в зарубежной и российской научной традиции

В рамках вестфальской парадигмы международного порядка суверенитет государства мыслится как абсолютная, неделимая и территориально закреплённая верховная власть, предполагающая исключительное право политического центра на регулирование процессов внутри собственной юрисдикции

и автономное осуществление внешнеполитических функций. Как отмечает профессор М.М. Лебедева, именно вестфальское понимание суверенитета сформировало устойчивую нормативно-институциональную основу мировой системы, в которой государство выступает первичным и самодостаточным носителем политической субъектности (Лебедева, 2008). Однако в условиях стремительной цифровизации международного пространства, формирования транснациональных инфраструктур данных и экспансии негосударственных технологических акторов традиционные параметры суверенитета оказываются концептуально размытыми, а сама возможность государства осуществлять верховное регулирование все более проблематизируется.

Данный принцип суверенности, основанный на идее неприкосновенности пространства и монополии государства на принятие политико-правовых решений, на протяжении нескольких столетий обеспечивал устойчивость мировой системы. Формирование глобальной цифровой среды, сетевой организации власти и возрастающая роль негосударственных акторов приводят к эрозии ключевых принципов вестфальской модели.

С этой позиции формирование понятия цифрового суверенитета выступает не только как адаптация вестфальского принципа к новым условиям развивающихся технологий, но и как реконфигурация самой логики суверенитета в сторону инфраструктурной и алгоритмической автономии¹.

Цифровой суверенитет интерпретируется как расширенная форма суверенной компетенции, включающая

¹ Niall Ferguson: 'Westerns don't understand how vulnerable freedom is' // The Guardian. 20.02.2011. URL: <https://www.theguardian.com/books/2011/feb/20/niall-ferguson-interview-civilization> (accessed: 20.11.2025).

способность государства осуществлять стратегический и регулятивный контроль над национальным цифровым контуром, над критически значимыми данными и над архитектурой сетевой инфраструктуры. Российский специалист А.А. Игнатов отмечает, что «определение понятия «цифровой суверенитет» еще не сложилось». Автор выделяет «среднюю» позицию, которая заключается в «утверждении суверенитета как способности государства осуществлять независимую цифровую политику» (Игнатов, 2025). Действительно, предложенная «средняя» позиция, понимающая суверенитет как способность государства проводить независимую цифровую политику, выглядит наиболее сбалансированной и аналитически продуманной, поскольку позволяет избежать как узко-технологического, так и чрезмерно политизированного объяснения данной категории.

Еще одно схожее определение дано С.С. Морозовой, которая описывает цифровой суверенитет как «право и способность контролировать инфраструктуру, данные и потоки информации в пределах своих границ, а также определять правила игры в цифровом пространстве» (Морозова, 2025).

В результате цифровой суверенитет можно рассматривать как ключевое направление трансформации вестфальской модели: он фиксирует переход от территориально-центричной логики к логике сетевой, инфраструктурной власти, в рамках которой суверенитет перестает быть исключительно территориальным феноменом и превращается в способность

государства контролировать цифровую среду на множестве уровней, определяющую динамику политического и социально-экономического развития.

Е.С. Зиновьева и С.В. Шитьков утверждают, что «суверенитет никогда не был статичной категорией, эволюционировал и включает в себя не только территориальный суверенитет, но и суверенитет в области территориальных вод, воздушного пространства государства, валютный суверенитет и ряд других компонентов» (Зиновьева, Шитьков, 2023). Данный подход позволяет рассматривать цифровой суверенитет как логическое продолжение и адаптацию традиционных принципов суверенитета к современным условиям.

В условиях, когда критические инфраструктуры, например от простых вычислений до алгоритмических систем, становятся объектами контроля транснациональных платформ (Ш. Зубофф описывает этот процесс как *surveillance capitalism* — «надзорный капитализм»²), возникает необходимость в переосмыслении категории суверенитета. Как отмечает Е. Морозов, цифровые платформы приобрели способность выполнять функции, ранее присущие только государству – распределять доступ к информации, формировать поведенческие стимулы, регулировать цифровые практики³.

В коллективной монографии *Digital Sovereignty in the BRICS Countries* (2025) подчеркивается, что исследования, посвященные цифровой сфере, преимущественно вписываются в парадигму изучения управления Интернетом и цифрового

² Zuboff S. 2029. *Surveillance capitalism and the challenge of collective action*. New Labor Forum. 22.01.2019. URL: <https://newlaborforum.cuny.edu/2019/01/22/surveillance-capitalism> (accessed: 20.11.2025).

³ Conversation: Yanis Varoufakis on Crypto & the Left, and Techno-Feudalism. the crypto syllabus. URL: <https://the-crypto-syllabus.com/yanis-varoufakis-on-techno-feudalism/> (accessed: 20.11.2025).

управления. Авторы отмечают, что значительная часть научных работ фокусируется на анализе институтов, механизмов и нормативных структур управления цифровым пространством, тогда как вопросы цифрового суверенитета нередко рассматриваются лишь косвенно, то есть через призму регулирования трансграничных потоков данных, стандартов Интернета и контроля над цифровой инфраструктурой (Schiffrin et al., 2025).

Особую значимость цифровой суверенитет приобретает в контексте дискуссий о *цифровом неокOLONIALИЗМЕ*. Доминирование глобальных технологических корпораций формирует асимметричные зависимости, сопоставимые по структурному воздействию с колониальными практиками прошлого, но реализуемые через механизмы контроля над данными, стандартами и алгоритмами.

В своей работе Ш. Зубофф, анализируя феномен «капитализма наблюдения/слежки», фактически подводит его под категорию, которую все чаще используют современные исследователи, — цифрового неокOLONIALИЗМА. По ее мнению, этот режим экономической власти представляет собой своеобразную мутацию, возникшую в Кремниевой долине и стремительно распространившуюся на различные отрасли экономики⁴. Его распространение стало возможным благодаря тому, что модели, основанные на систематическом наблюдении, сборе поведенческих данных и предсказательном анализе, оказались чрезвычайно успешными. В результате можно говорить о формировании нового экономического порядка,

построенного на тотальном мониторинге, который сегодня встроен в широкий спектр сервисов, влияя на как индивидов, так и на государства.

В свою очередь М.В. Харкевич обращается к проблеме глобального управления и отмечает цифровую слежку, рассматривая ее в контексте такой формы управления, как «правительственность». Автор отмечает, что данная форма властных практик начала складываться в странах Европы еще в XVII веке, постепенно расширяя инструменты наблюдения и контроля⁵. В дальнейшем она вышла на глобальный уровень, проявляясь в распространении международных рейтингов, развитии политических механизмов, усилении практик секьюритизации, а также внедрении цифровых технологий мониторинга. Можно сделать вывод, что в этом контексте цифровая слежка или цифровое наблюдение рассматривается как современное проявление «правительственности», усиливающее возможности надзора и управления в транснациональном масштабе.

По мнению Е.С. Зиновьевой и С.В. Шитькова, в развивающихся странах обеспечение цифрового суверенитета невозможно рассматривать в отрыве от процессов неокOLONIALИЗМА (Зиновьева, Шитьков 2023). Стоит отметить, что современные формы цифровой зависимости, включая контроль над данными, доминирование иностранных технологических корпораций и влияние транснациональных стандартов, создают новые асимметричные отношения, схожие по своему воздействию с историческими

⁴ Zuboff S. 2019. *Surveillance capitalism and the challenge of collective action*.

⁵ Харкевич М.В. 2023. Глобальное управление в эпоху обострения конкуренции между великими державами. Российский совет по международным делам. 05.12.2023. URL: <https://russiancouncil.ru/analytics-and-comments/analytics/globalnoe-upravlenie-v-epokhu-obostreniya-konkurentsii-mezhdu-velikimi-derzhavami/> (дата обращения: 30.11.2025).

колониальными практиками. Так, укрепление цифрового суверенитета становится не только технической и экономической задачей, но и политическим и технологическим инструментом, необходимым для снижения уязвимости государств и обеспечения равноправного участия в глобальном цифровом пространстве.

Можно сделать вывод, что разделение на отечественный и западный подходы отражает более глубокие различия между моделями политического регулирования: первая ориентирована на укрепление государственности, вторая – на институциональное регулирование цифровых систем при сохранении открытости и правовых гарантий.

В данном исследовании мы хотели бы предложить авторское понимание терминов «цифровой суверенитет» и «цифровой неоколониализм». На наш взгляд, цифровой колониализм – это система асимметричных властных отношений в глобальном цифровом пространстве, при которой транснациональные технологические корпорации и государства-лидеры цифрового развития устанавливают контроль над данными, цифровой инфраструктурой, алгоритмами и стандартами, тем самым формируя зависимость развивающихся стран от внешних центров технологической силы.

На основании статьи А.А. Игнатова (Игнатов, 2025) авторы доработали определение цифрового суверенитета, который рассматривается как способность государства к следующим действиям:

1. Определять цели, принципы, механизмы функционирования цифровой среды;
2. Контролировать критически важную инфраструктуру;
3. Обеспечивать независимость цифровой инфраструктуры;
4. Формировать свои решения вне зависимости от внешних акторов (стимулировать собственных национальных решений);
5. Контролировать ситуацию рынка цифровых платформенных услуг;
6. Контролировать содержание распространяемой информации;
7. Контролировать оборот данных;
8. Формировать устойчивость населения к киберугрозам (кибергигиену)⁶.

Сравнительный анализ институциональной, нормативно-правовой и стратегической основ политики стран-членов БРИКС по вопросам защиты цифрового суверенитета государства

Для формирования представления о политике цифрового суверенитета в странах БРИКС важным пунктом является изучение существующих национальных институциональных, нормативно-правовых и стратегических основ политики по вопросам защиты своего суверенитета. Необходимо отметить, что в концептуальных документах почти всех стран БРИКС этот термин найти не удастся: понятие «цифровой суверенитет» появляется в Национальном политическом курсе по цифровым коммуникациям Индии 2018 г.⁷,

⁶ Об этом пункте отчасти говорили страны БРИКС в своей декларации 2025 г., согласно которой они обязаны обеспечить безопасность населения от рисков использования искусственного интеллекта. Источник: BRICS Leaders' statement on the global governance of artificial intelligence. BRICS. 06.07.2025. URL: <https://brics.br/en/documents/presidency-documents> (accessed: 03.12.2025).

⁷ India's National Digital Communications Policy 2018. Department of Telecommunications India. 2018. URL <https://dot.gov.in/sites/default/files/EnglishPolicy-NDCP.pdf> (accessed: 30.11.2025).

а концепция «суверенитета в киберпространстве» находит отражение в Международной стратегии сотрудничества в киберпространстве Китая⁸. Однако такое понятие часто встречается в устной речи и выступлениях ряда политиков, например, в речи президента Индонезии Джоко Видодо⁹ и интервью заместителя руководителя администрации президента России С. Кириенко¹⁰.

Тем не менее представляется, что этот вопрос является для стран достаточно важным: это подтверждают высокие позиции стран в глобальном индексе кибербезопасности¹², проведенные исследования в академической сфере (Игнатов, 2025), совместные усилия (двусторонние и многосторонние) объединения в сфере кибербезопасности и информационно-коммуникационных технологий (ИКТ) (Zinovieva, Ignatov, 2024), а также нормативно-правовые и концептуальные документы, в которых использование ИКТ в целях нарушения безопасности отмечается как одна из угроз безопасности государства. При этом в соответствии с глобальным индексом кибербезопасности считается, что в странах БРИКС сложилась неравномерная ситуация с точки

зрения реализации стратегий кибербезопасности: так, есть абсолютные мировые лидеры (пять стран БРИКС — Бразилия, Египет, Индия, Индонезия, ОАЭ), относительно преуспевающие в реализации повестки (Китай, Россия и ЮАР), а также страны, которые пока устанавливают свою политику по кибербезопасности (Иран и Эфиопия)¹².

Проведено сравнение стран по семи критериям, выделенным в качестве описания феномена цифрового суверенитета (Таблица №1):

- 1) Контроль над критически важными технологиями и производственными цепочками;
- 2) Контроль над инфраструктурой связи и интернета;
- 3) Контроль над ситуацией на рынке цифровых платформенных услуг;
- 4) Контроль над содержанием распространяемой информации;
- 5) Контроль над оборотом данных;
- 6) Развитие собственных технологий для снижения зависимости от зарубежных технологий;
- 7) Обучение населения навыкам кибербезопасности.

⁸ China's International Strategy of Cooperation on Cyberspace. Xinhua. 01.03.2017. URL: http://www.xinhuanet.com/english/china/2017-03/01/c_136094371_2.htm (accessed: 30.11.2025).

⁹ Digital Transformation Realizes Digital Sovereignty and Independence, President Jokowi Says. Cabinet Secretariat of the Republic Indonesia. 26.02.2021. URL: <https://setkab.go.id/en/digital-transformation-realizes-digital-sovereignty-and-independence-president-jokowi-says/> (accessed: 30.11.2025).

¹⁰ Россия получила полный цифровой суверенитет в интернет-сфере, наряду с США и Китаем — Кириенко. Интерфакс. 24.09.2025. URL: <https://www.interfax-russia.ru/rossiya-i-mir/rossiya-poluchila-polnyy-cifrovoy-suverenitet-v-internet-sfere-naryadu-s-ssha-i-kitaem-kirienko> (дата обращения: 30.11.2025).

¹¹ Global Cybersecurity Index. ITU. 2024. URL: <https://www.itu.int/hub/publication/d-hdb-gci-01-2024/> (accessed: 30.11.2025).

¹² Global Cybersecurity Index.

Таблица №1.

Сравнение концептуальных, нормативно-правовых и институциональных основ стран БРИКС в сфере цифрового суверенитета

Table 1.

Comparison of the conceptual, regulatory, and institutional frameworks of BRICS countries in the area of digital sovereignty

Страна	Контроль над критически важной инфр-рой (КВИ)	Контроль над инфр-рой связи	Контроль над ситуацией на рынке цифровых платформенных услуг	Контроль над содержанием распространяемой информации	Контроль над оборотом данных	Развитие собственных технологий для снижения зависимости	Обучение населения навыкам кибербезопасности
Бразилия	КВИ: объекты информационной и цифровой безопасности. Угроза: киберугрозы	Уголовная ответственность за нарушение целостности компьютерных устройств, кражу и мошенничество с помощью электронных средств или через Интернет	Попытки контроля путем передачи функции контроля Национальному агентству по коммуникациям. Посредники признаны ответственными по размещаемому контенту	Провайдеры не контролируют информацию, фейковые новости и дезинформация могут быть удалены по решению суда	Угрозы: шпионаж, утечки информации. Намерение усилить безопасность данных между системами и цифровыми каналами	Стимулирование национальных технологий, минимальных стандартов кибербезопасности для снижения зависимости от зарубежных технологий	Повышение осведомленности населения о безопасном поведении, поддержке, борьбе с киберпреступлениями
Египет	Программа укрепления безопасности КВИ и продвижения национальных стандартов	Сертификация компаний, предоставляющих услуги по кибербезопасности	Законодательство по контролю на рынке	Закон о киберпреступлениях: контроль над распространяемой информацией и возможность блокировки сайтов	Контроль и наказания за нарушения, установление ответственных лиц за данные. Обработка и защита данных в соответствии с национальным законодательством	Не найдено направления	Обучение населения пошагово от простого к сложному, в том числе в части осведомленности о безопасном поведении
Индия	ИКТ не входят в КВИ, но планируется включить их в состав	Создание собственной устойчивой цифровой инфраструктуры, периодическое отключение сети	Установлены ограничения по регистрации компаний платформенных услуг	Контроль над контентом в соответствии с правом правительства по защите суверенитета страны	Контроль над данными, конфиденциальностью, некоторые типы данных могут храниться только на территории Индии. Планируется усиление защиты	Создание собственной цифровой инфраструктуры, стимулирование новых технологий	Обучение населения кибергигиене, включение обучения кибергигиене в школьное образование
Индонезия	Принята стратегия для защиты КВИ (в т.ч. ИКТ), ответственность возлагается на провайдера услуг	Периодическое отключение сети	Установлены ограничения для частных операторов электронных систем	Контроль над контентом, планируется ограничения социальных сетей	Контроль над персональными данными, передача данных за границу при соблюдении законодательства. Планируется ужесточение законодательства	Не найдено направления	Население обучают цифровой грамотности и цифровой безопасности
ОАЭ	Программа по защите КВИ (в т.ч. ИКТ) принята в 2025 г.	Создание устойчивой инфраструктуры по кибербезопасности	Национальная политика облачной безопасности, которая определяет требования к провайдерам облачных услуг	Осуществляется контроль над контентом путем борьбы с распространением фейковых новостей и слухов, а также соблюдения стандартов медиаконтента	Передача данных за границу разрешена на установленных законодательством условиях, требования по локализации данных для ряда отраслей. Проблема передачи данных между СЭЗ и остальной частью ОАЭ	Создание программы национальных наград для стимулирования развития кибербезопасности	Обучение населения для определения рисков и практики кибергигиены разных сегментов населения
Россия	Недопущение иностранного контроля над объектами КВИ	Намерение в недопущении иностранного контроля над национальным сегментом сети, противодействие вмешательству во внутренние дела	Усиливается контроль над цифровыми платформенными услугами с 2026 г.	Действует законодательство о запрете фейковых новостей, установлен контроль над распространяемым контентом	С 2025 г. запрещено хранение персональных данных россиян за рубежом (за исключением ряда случаев)	Обеспечение технологической независимости технологий, в т.ч. ОПК, и приоритетного использования российских ИКТ	Обучение населения кибергигиене

Китай	Защита КВИ — приоритет	Усиление контроля над сетью как приоритет развития законодательства	Есть контроль над операторами в отношении данных	Действует контроль над контентом с запретом фейковой информации	Персональные данные китайцев должны храниться на территории Китая	Законы о данных как стимул технологической индустрии и снижения зависимости от иностранных компаний	Обучение населения как приоритет правительства
ЮАР	Защита КВИ — приоритет	Есть контроль над сетью	Есть контроль над посредниками в вопросах удаления контента	Действует контроль над медиаконтентом, контроль над ложной информацией	Жесткие требования по локализации данных, письменное обоснование для передачи данных за рубеж	Не найдено направления	В процессе разработки, но не реализуется
Иран	Не найдено направления	Инtranet под контролем государства	Действует система выдачи лицензий платформам	Действует контроль над контентом, запрет отдельных платформ	Есть требования по хранению данных на территории Ирана	Блокировка зарубежных платформ и санкции стимулируют снижение зависимости	Обучение населения ограничено отдельными курсами для сотрудников
Эфиопия	Не найдено направления	Выключение интернета, инtranet под контролем государства	Не найдено направления	Контроль над контентом, выключение интернета, блокировка платформ, платформа проверки	Есть требования по хранению данных на территории Эфиопии	Не найдено направления	Не найдено направления

Источник: составлено авторами на основе академических статей (Chipangura, Gustave, 2022; Karimnia et al., 2022; Popova, 2024; Calandro, 2024; Cong, 2024; Krylov, 2025; Zinovieva, Ignatov, 2024; Vadiati, Mehran, 2025) и нормативно-правовых актов и концептуальных документов¹³, официальных публикаций, речей руководящего состава стран БРИКС, оценок специализированных агентств кибербезопасности, материалов СМИ¹⁴.

¹³ Decreto Nº 9.573 «Aprova a Política Nacional de Segurança de Infraestruturas Críticas». 22.11.2018. URL: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm (accessed: 30.11.2025); Decreto Nº 10.569 «Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas». 09.12.2020. URL: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10569.htm (accessed: 30.11.2025); Decreto Nº 11.200 «Aprova o Plano Nacional de Segurança de Infraestruturas Críticas». 15.09.2022. URL: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Decreto/D11200.htm (accessed: 30.11.2025); Legislação // Gabinete de Segurança Institucional. 24.11.2020. URL: <https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/legislacao> (accessed: 30.11.2025); Lei Nº 14.460 «Transforma a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial e transforma cargos comissionados». 25.10.2022. URL: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/l14460.htm (accessed: 30.11.2025); Lei Nº 14.155 «Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal)». 27.05.2021. URL: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm (accessed: 30.11.2025); Lei Nº 12.737 «Dispõe sobre a tipificação criminal de delitos informáticos...». 30.11.2012. URL: https://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm (accessed: 30.11.2025); E Ciber 2025 Inglês Digital. 2025. URL: <https://www.calameo.com/read/0075181912e2c2b6a7b92> (accessed: 30.11.2025); Question 3/2: Securing information and communication networks: Best practices for developing a culture of cybersecurity // ITU. 2025. URL: <https://www.itu.int/hub/publication/d-stg-sg02-03-2-2025/> (accessed: 30.11.2025); Decreto Nº 12.572 «Institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação no âmbito da administração pública federal». 04.08.2025. URL: <https://www2.camara.leg.br/legin/fed/decret/2025/decreto-12572-4-agosto-2025-797812-publicacaooriginal-176047-pe.html> (accessed: 30.11.2025); Lei Geral de Proteção de Dados Pessoais (LGPD). 2018. URL: <https://www.gov.br/esporte/pt-br/aceso-a-informacao/lgpd> (accessed: 30.11.2025); Política Nacional de Defesa. Ministério da Defesa. 02.09.2024. URL: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/politica-nacional-de-defesa (accessed: 30.11.2025); Livro Branco de Defesa Nacional (LBDN). Ministério da Defesa. 19.11.2025. URL: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/livro-branco-de-defesa-nacional-lbdn-1 (accessed: 30.11.2025); Decreto Nº 12.725 «Aprova a Política Nacional de Defesa, a Estratégia Nacional de Defesa e o Livro Branco de Defesa Nacional». 18.11.2025. URL: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/livro-branco-de-defesa-nacional-lbdn-1/arquivos/

livro-branco-de-defesa-nacional/decreto-no-12-725-de-18-de-novembro-de-2025-dou_lbdn.pdf (accessed: 30.11.2025); Brazil Supreme Court Ruling Redefines Framework for Platform Liability. TechPolicy.press. 20.11.2025. URL: <https://www.techpolicy.press/brazil-supreme-court-ruling-redefines-framework-for-platform-liability/> (accessed: 30.11.2025); Translation of Law No. 151 of 2020 «Issuance of the Personal Data Protection Law». Andersen. 03.06.2025. URL: <https://eg.andersen.com/wp-content/uploads/2025/06/Law-No.-151-OF-2020.pdf> (accessed: 30.11.2025); The National Cybersecurity Strategy of Egypt (2023-2027). DigWatch. 06.2023. URL: <https://dig.watch/resource/the-national-cybersecurity-strategy-of-egypt-2023-2027> (accessed: 30.11.2025); India's National Digital Communications Policy 2018; The Digital Personal Data Protection Act, 2023. 11.08.2023. URL: <https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf> (accessed: 30.11.2025); Indonesia's Fourth Industrial Revolution. Ministry of Industry Indonesia. 24.07.2018. URL: https://sea-vet.net/images/seb/initiatives/appendix_file/570/making-indonesia-40-bppi.pdf (accessed: 30.11.2025); Data Sovereignty in UAE. InCountry Staff. 29.04.2025. URL: <https://incountry.com/blog/data-sovereignty-in-the-uae/> (accessed: 30.11.2025); Cybersecurity Laws and Regulations Indonesia 2026. ICLG. 21.11.2025. URL: <https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/indonesia> (accessed: 30.11.2025); UAE National Cybersecurity Strategy. Telecommunications Regulatory Authority. URL: <https://tdra.gov.ae/userfiles/assets/Lw3seRUaIMd.pdf> (accessed: 30.11.2025); Critical Information Infrastructure Protection Policy. UAE. 07.05.2025. URL: <https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/policies/transport-and-infrastructure/critical-information-infrastructure-protection-policy> (accessed: 30.11.2025); National Cloud Security Policy. UAE. 23.10.2025. URL: <https://u.ae/en/about-the-uae/digital-uae/digital-transformation/strategies-policies-and-initiatives/National-Cloud-Security-Policy> (accessed: 30.11.2025); Концепция внешней политики Российской Федерации (утверждена Президентом Российской Федерации В.В.Путиным 31 марта 2023 г.). МИД России. 31.03.2023. URL: <https://www.mid.ru/ru/detail-material-page/1860586/> (дата обращения: 30.11.2025); Указ Президента Российской Федерации от 02.07.2021 г. № 400. Президент России. 02.07.2021. URL: <http://www.kremlin.ru/acts/bank/47046> (дата обращения: 30.11.2025); Доктрина информационной безопасности Российской Федерации. Совет Безопасности РФ. 05.12.2016. URL: <http://www.scrf.gov.ru/security/information/document5/> (дата обращения: 30.11.2025); Федеральный закон от 28.02.2025 № 23-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» и отдельные законодательные акты Российской Федерации» // Официальное опубликование правовых актов. 28.02.2025. URL: <http://publication.pravo.gov.ru/document/0001202502280034?index=1> (дата обращения: 30.11.2025); Федеральный закон «О внесении изменений в статью 15.3 Федерального закона «Об информации, информационных технологиях и о защите информации» от 18.03.2019 N 31-ФЗ // Консультант Плюс. 18.03.2019. URL: https://www.consultant.ru/document/cons_doc_LAW_320401/ (дата обращения: 30.11.2025); International Strategy of Cooperation on Cyberspace; India's Global Initiative on Data Security. UNODA. 03.2022. URL: <https://documents.unoda.org/wp-content/uploads/2022/03/Position-paper-Global-Initiative-on-Data-Security-submitted-by-China.pdf> (accessed: 30.11.2025); China's The Global Security Initiative Concept Paper. ChinaDiplomacy. URL: https://en.chinadiplomacy.org.cn/pdf/The_Global_Security_Initiative_Concept_Paper.pdf (accessed: 30.11.2025); China's National Cyberspace Security Strategy. China Copyright and Media. 27.12.2016. URL: <https://china-copyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/> (accessed: 30.11.2025); Data Security Law of the People's Republic of China. The National People's Congress of the People's Republic of China. 10.06.2021. URL: http://www.npc.gov.cn/englishnpc/c2759/c23934/202112/t20211209_385109.html (accessed: 30.11.2025); Personal Information Protection Law of the People's Republic of China. The National People's Congress of the People's Republic of China. 29.12.2021. URL: http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm (accessed: 30.11.2025); China's Digital Data Sovereignty Laws and Regulations. InCountry. 20.08.2024. URL: <https://incountry.com/blog/chinas-digital-data-sovereignty-laws-and-regulations/> (accessed: 30.11.2025); South Africa's Localization Regulation / ITIF. 09.06.2025. URL: <https://itif.org/publications/2025/06/09/south-africa-localization-regulation/> (accessed: 30.11.2025); Iran: Personal Data Protection and Safeguarding Draft Act. Article19. URL: <https://www.article19.org/wp-content/uploads/2019/06/Legal-Analysis-of-Draft-Data-Protection-Act.pdf> (accessed: 30.11.2025); Digital Ethiopia 2025. Ethiopia. 2025. 148 p. URL: https://www.lawethiopia.com/images/Policy_documents/Digital-Ethiopia-2025-Strategy-english.pdf (accessed: 30.11.2025).

- ¹⁴ A Review of Content Moderation Policies in Latin America. TechPolicy.press. 08.07.2024. URL: <https://www.techpolicy.press/a-review-of-content-moderation-policies-in-latin-america/> (accessed: 30.11.2025); The imperative of digital sovereignty. Ahramonline. 22.05.2025. URL: <https://english.ahram.org.eg/NewsContentP/4/546567/Opinion/The-imperative-of-digital-sovereignty>.

Лидеры в сфере мер кибербезопасности и их цифровой суверенитет

Как показывает сравнение, лидеры в сфере мер кибербезопасности стремятся

закрепить в своих нормативно-правовых актах почти все направления цифрового суверенитета. Исключение составляет направление собственных технологий,

aspx (accessed: 30.11.2025); Tsebee D., Adaramola V. Review of Ethiopia's Data Protection Act. Tech Hive Advisory. 18.11.2024. URL: <https://www.techhiveadvisory.africa/insights/review-of-ethiopia-s-data-protection-act> (accessed: 30.11.2025); Ethiopia. RSF. URL: <https://rsf.org/en/country/ethiopia> (accessed: 30.11.2025). South Africa. Policy and Regulations for Community Networks. URL: <https://policy.communitynetworks.group/country-profiles/south-africa> (accessed: 30.11.2025); South Africa challenges US tech giants. ET Insights. 03.03.2025. URL: <https://etedge-insights.com/featured-insights/geopolitics-and-strategy/south-africa-challenges-us-tech-giants/> (accessed: 30.11.2025); Cyber safety and digital security// UAE. 12.11.2025. URL: <https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security> (accessed: 30.11.2025); С 1 октября 2026 года в России вводится официальное регулирование деятельности платформ. Минэкономразвития России. 22.07.2025. URL: https://economy.gov.ru/material/news/s_1_oktyabrya_2026_goda_v_rossii_vvoditsya_oficialnoe_regulirovanie_deyatelnosti_platform.html (дата обращения: 30.11.2025); Iran unveils plan for tighter internet rules to promote local platforms. AlJazeera. 24.02.2024. URL: <https://www.aljazeera.com/news/2024/2/24/iran-unveils-plan-for-tighter-internet-rules-to-promote-local-platforms/> (accessed: 30.11.2025); India's Search for Digital Sovereignty. TechPolicy.press. 30.10.2025. URL: <https://www.techpolicy.press/indias-search-for-digital-sovereignty/> (accessed: 30.11.2025); Egypt Sets New Rules For Cybersecurity Firms: What To Know // Business monthly. 08.10.2025. URL: <https://businessmonthlyeg.com/egypt-sets-new-rules-for-cybersecurity-firms-what-to-know/> (accessed: 30.11.2025); Sharmraev R.A., Kurbatova T.A., Lindre Yu.A., Ignatiev A.G. Egypt as a Digital State: opportunities for cooperation // Center for global IT-cooperation. 18.11.2024. URL: <https://www.cgic.ru/en/media/egypt-as-a-digital-state-opportunities-for-cooperation/> (accessed: 30.11.2025); Authoritarian Diffusion in the Cyberspace: How Egypt Learns, Emulates, and Cooperates in Digital Authoritarianism. European Center for Populism Studies. 09.05.2025. URL: <https://www.populismstudies.org/authoritarian-diffusion-in-the-cyberspace-how-egypt-learns-emulates-and-cooperates-in-digital-authoritarianism/> (accessed: 30.11.2025); India expands censorship powers, lets lower officials demand takedowns. AlJazeera. 08.09.2025. URL: <https://www.aljazeera.com/features/2025/9/8/india-expands-censorship-powers-lets-lower-officials-demand-takedowns> (accessed: 30.11.2025); E-commerce regulation in India: what you need to know if you want to sell online. IndiaConnected. 07.11.2024. URL: <https://www.indiaconnected.co.uk/blog-articles/market-focus-e-commerce-in-india/> (accessed: 30.11.2025); Delhi schools promote digital safety awareness to prevent cybercrimes among students and staff // The Times Of India. 25.05.2025. URL: <https://timesofindia.indiatimes.com/city/delhi/delhi-schools-promote-digital-safety-awareness-to-prevent-cybercrimes-among-students-and-staff/articleshow/121394056.cms> (accessed: 30.11.2025); Digital Transformation Landscape in Indonesia // Digital Transformation Center Indonesia. 2023. URL: <https://cgd.abc-institute.id/wp-content/uploads/2024/10/DTLI-2023.pdf> (accessed: 30.11.2025); Towards Indonesia's ICS OT Cyber Security National Standard. Fedco International. URL: <https://fedco.co.id/towards-indonesias-ics-ot-cyber-security-national-standard/> (accessed: 30.11.2025); Indonesia's bid for social media control raises alarm about future of digital freedom. SCMP. 02.10.2025. URL: <https://www.scmp.com/week-asia/lifestyle-culture/article/3327538/indonesias-bid-social-media-control-raises-alarm-about-future-digital-freedom> (accessed: 30.11.2025); Indonesia applies blacklist model to control digital content: Ministry. The Indonesia.Co. 28.06.2024. URL: <https://www.theindonesia.co/news/2024/06/28/190000/indonesia-applies-blacklist-model-to-control-digital-content-ministry> (accessed: 30.11.2025); Data Protection in Indonesia. DLA Piper. 20.01.2025. URL: <https://www.dlapiperdataprotection.com/?t=law&c=ID> (accessed: 30.11.2025); Internet Shutdown in Indonesia: The New Normal Policy to Censor Information Online?. SAFEnet. URL: <https://safenet.or.id/2020/10/internet-shutdown-in-indonesia-the-new-normal-policy-to-censor-information-online/> (accessed: 30.11.2025); Silveira A.C.R.D., Camelo A.P., Schmitt Katano B.Y., Wagner F.R., de Perdigão Lana P., Gatto R.F. Internet Impact Brief. Proposals to Regulate Digital Platforms in Brazil: Potential Impacts for the Internet. São Paulo: CEPI FGV DIREITO SP; ISOC Brasil, 2024. 10 p. URL: <https://www.internetsociety.org/wp-content/uploads/2025/02/Brazil-IIB.pdf> (accessed: 30.11.2025); Egypt's Cybersecurity, Cybercrime, and Data Protection Laws: A Legal Overview // Ibrachy & Derkamar Law Firm. URL: <https://id.com.eg/egypts-cybersecurity-cybercrime-and-data-protection-laws-a-legal-overview/> (accessed: 30.11.2025).

которые не стимулирует ряд стран, хотя наблюдается проблема зависимости от зарубежных компаний (Ларионова, Шелепов 2024). Представляется, что это направление будет развиваться в последствии.

В *Бразилии* термин «цифровой суверенитет» используется представителями гражданского и научно-экспертного сообщества. Под суверенитетом подразумевается снижение зависимости от транснациональных цифровых компаний и защиты данных граждан Бразилии от использования в целях корпораций¹⁵, что является для Бразилии серьезной проблемой (Ларионова, Шелепов, 2024). Государство активно действует в вопросах цифрового суверенитета: к реализации вопросов привлечено большое количество институтов разных уровней, большой объем нормативно-правовых документов, продолжающих формироваться: например, все еще в процессе обсуждения законопроект о фейковых новостях (Законопроект 2630). В результате Бразилия стремится уделять внимание всем аспектам цифрового суверенитета, однако заметен явный перекос в сторону вопросов критически важной инфраструктуры как основного пункта деятельности. При этом реализация, согласно изучению практики, явно отстает от концептуальных и нормативно-правовых аспектов (Игнатов, 2025).

В *Египте* государство развивает стратегию по кибербезопасности, но при этом не все аспекты цифрового суверенитета внедряются на данном этапе (некоторые только планируются к внедрению).

Институциональная система уже создана (например, правительственный центр данных и облачных технологий, Верховный совет по кибербезопасности), но стратегическая и нормативно-правовая системы продолжают совершенствоваться и дорабатываться. Так планируется внедрение новых стандартов, а также обучение граждан Египта грамотности и информационным технологиям¹⁶.

В *Индии* цифровой суверенитет как термин определяется в нормативно-правовых документах и сочетает в себе конфиденциальность данных, выбор данных и безопасности граждан¹⁷. При этом сама нормативно-правовая система является достаточно молодой и начала формироваться только в 2018 г. (Zinovieva, Ignatov, 2024). Страна планирует переключаться на альтернативные сервисы западным сервисам технических гигантов (в страну активно проникают китайские технические корпорации (Ларионова, Шелепов, 2024)), а также прорабатывается вопрос создания собственного браузера, что говорит об усилении стремления к цифровому суверенитету¹⁸. Параллельно развивается институциональная структура: учреждена Коллегия по защите данных Индии¹⁹. Также в Индии действуют достаточно жесткие требования по локализации данных и модерации контента и периодически происходят отключения интернета (Thumfart, 2024).

В *Индонезии* используются понятия цифровой суверенитет и суверенитет данных²⁰. Отмечается нормативно-правовое и концептуальное оформление вопроса,

¹⁵ Carta Soberania Digital. Carta Soberania Digital. 2022. URL: <https://cartasoberaniadigital.lablivre.wiki.br/carta/> (accessed: 30.11.2025).

¹⁶ The National Cybersecurity Strategy of Egypt (2023-2027).

¹⁷ India's National Digital Communications Policy 2018.

¹⁸ India's Search for Digital Sovereignty

¹⁹ The Digital Personal Data Protection Act, 2023.

²⁰ Digital Transformation Landscape in Indonesia.

в 2020-х гг. приняты законы и стратегии по реализации цифровой трансформации и, следовательно, расширения цифрового суверенитета, проведено объединение законодательства по защите данных. При этом законодательство продолжает разрабатываться, как и институциональная система, состоящая на данный момент из государственных агентств.

В ОАЭ достаточно сложная ситуация с нормативно-правовой базой ввиду существования нескольких свободных экономических зон, однако ОАЭ в соответствии со своей стратегией кибербезопасности планируют создать правовые рамки для борьбы с киберпреступлениями и защиты технологий, уже приняли Политику защиты критически важной инфраструктуры (в эмирате Дубай принята своя стратегия кибербезопасности)²¹. При этом продолжает совершенствоваться институциональная структура ОАЭ, создан Совет по кибербезопасности ОАЭ, планируется создать новые институты, которые возьмут на себя функции, вводимые концептуальными и нормативно-правовыми документами²². Для снижения зависимости пока требуется дальнейшее развитие законодательства.

Относительно преуспевающие страны

В России достаточно много концептуальных и нормативно-правовых документов, регулирующих вопросы цифрового суверенитета (начиная от общих внешнеполитических и заканчивая специализированными документами, посвященными кибербезопасности). При этом

законодательство продолжает дорабатываться во всех сферах цифрового суверенитета, несмотря на комментарии правительства о том, что цифровой суверенитет был достигнут. Одним из наиболее важных вопросов является вопрос критической инфраструктуры, так, существует специальный институт, реагирующий на киберинциденты²³. Критикуется недостаточное вовлечение в восполнение производственных цепочек и собственное производство компонентов (Игнатов, 2025).

Китай, определяющий государство центральным (Морозова, 2025) в вопросах суверенитета в киберпространстве, свою концептуальную, институциональную и нормативно-правовую основы развивает целенаправленно и планомерно, что делает его своеобразным лидером в контексте развития документов. При этом Китай предлагает эту модель на экспорт через Цифровой Шелковый путь путем строительства цифровой инфраструктуры в других развивающихся странах²⁴. Важной чертой подхода к цифровому суверенитету является концептуальное закрепление экстерриториальности, которая позволяет использовать законодательство за пределами Китая и использовать персональные данные за пределами Китая в ряде случаев (Cong, 2024).

В ЮАР вопросы цифрового суверенитета пока не развиваются достаточно активно, однако в части кибербезопасности действуют нормативно-правовые акты и институты. Так, существует Информационный регулятор ЮАР, который занимается вопросами персональной

²¹ Cyber Safety and Digital Security.

²² National Cybersecurity Strategy.

²³ Global Cybersecurity Index

²⁴ How China Governs Its Internet and Plans to Export Its Model. TechPolicy.Press. 24.07.2025. URL: <https://www.techpolicy.press/how-china-governs-its-internet-and-plans-to-export-its-model/> (accessed: 30.11.2025).

информации²⁵. Также создан проект Национальной политики данных и облачных данных, согласно которой сейчас основные обладатели данных – иностранные компании и государства.

Страны, устанавливающие политику кибербезопасности

Будучи под санкциями, Иран усилил контроль над внутренней инфраструктурой (Vadiati, Mehran, 2025). На данный момент основным направлением является контроль не только над инфраструктурой, но и над распространяемым контентом (блокировка международных приложений, выключение интернета). Тем не менее, наблюдается пробел в концептуальных и нормативно-правовых документах в сфере контроля над критически важной инфраструктурой (Karimnia et al., 2022).

Эфиопия обладает достаточным потенциалом в реализации политики цифрового суверенитета: концептуальные и нормативно-правовые основы с институтами-регуляторами вносят в это свой вклад. Ситуацию осложняет низкое распространение интернета и недостаточно построенная инфраструктура (в т.ч. и оснащение электричеством, и зависимость от гидроресурсов), поэтому стремление к цифровизации страны отодвигает вопросы построения цифрового суверенитета на второй план²⁶.

Сценарий развития сотрудничества стран БРИКС по проблемам защиты цифрового суверенитета в контексте цифрового неоколониализма

Укрепление цифрового суверенитета государств БРИКС становится стратегической задачей объединения на фоне стремительного усложнения глобальной

технологической конкуренции. Для стран группы, значительная часть которых исторически сталкивалась с внешней зависимостью, цифровое пространство превращается в поле соперничества за контроль над данными, нормами, платформами и алгоритмами. В подобных условиях развитие сотрудничества БРИКС может двигаться по сценарию, в котором приоритетом становится формирование коллективной архитектуры устойчивости, способной снизить уязвимость государств перед структурной силой западных технологических центров и применяемыми ими практиками цифрового неоколониализма (Барандова, 2025).

Ключевым направлением будущего взаимодействия БРИКС выступает формирование собственной нормативной базы в сфере цифровых технологий и искусственного интеллекта. Страны объединения обладают разными моделями регулирования, однако их объединяет стремление избежать импорта западных стандартов, которые могут ограничивать национальные интересы. Создание согласованной рамки регулирования данных, алгоритмической ответственности, кибербезопасности и платформенной деятельности позволит БРИКС стать самостоятельным центром международного нормотворчества. В перспективе БРИКС получает шанс сформировать модель «суверенного цифрового развития», которая будет учитывать культурные, экономические и политические особенности стран Глобального Юга.

Другим системным элементом сценария является создание совместной цифровой инфраструктуры: распределённых центров обработки данных, безопасных каналов передачи информации, облачных

²⁵ Information Regulator (South Africa). URL: <https://inforegulator.org.za/> (accessed: 30.11.2025).

²⁶ A Digital Ethiopia 2025 Strategy.

платформ и коммуникационных систем. Развитие собственных каналов связи позволит минимизировать риски внешнего вмешательства, обеспечить безопасность государственных данных и создать условия для автономного развития цифровых экосистем.

Важным вектором кооперации станет совместное развитие и адаптация технологий ИИ, в том числе крупные языковые модели (LLM), системы компьютерного зрения, роботизированные комплексы и средства интеллектуального анализа данных. Страны БРИКС обладают разным уровнем технологической зрелости, однако в совокупности их научно-исследовательский потенциал способен конкурировать с ведущими западными центрами разработки ИИ. В перспективе возможно формирование консорциумов университетов и исследовательских центров БРИКС, направленных на создание открытых, но защищённых платформ коллективного обучения моделей, что позволит странам объединения избежать зависимости от иностранных технологических гигантов. Параллельно БРИКС может выстроить механизм «этического федерализма», в котором ценностные принципы использования ИИ будут определяться государствами самостоятельно, без навязывания западных подходов.

Особое значение в будущем приобретет сотрудничество стран БРИКС в сфере информационной и когнитивной безопасности. Учитывая высокую уязвимость государств БРИКС к когнитивным воздействиям, логичным развитием становится создание коллективной системы раннего предупреждения и взаимной поддержки при выявлении признаков внешнего вмешательства. Механизм, в частности, может включать координированные центры мониторинга информационных кампаний, обмен методиками анализа сетевой активности, совместную разработку

технологий выявления и нейтрализации когнитивных атак.

Экономический контекст также определяет необходимость совместных шагов. Доминирование западных цифровых корпораций на глобальном рынке создает угрозу вытеснения национальных компаний и утраты контроля над внутренними рынками данных. БРИКС способен развивать собственные транснациональные цифровые платформы, например, в сфере электронных платежей, торговли, финансовых услуг, логистики и образования. В перспективе страны группы становятся ядром альтернативной цифровой глобализации, в рамках которой обмен технологиями, инвестиции в инфраструктуру и стандартизация обеспечивают устойчивое развитие и минимизируют риски внешнего давления.

В ближайшем будущем сотрудничество БРИКС может перейти от кооперации к формированию полноценного цифрового пространства объединения, что может включать собственные стандарты, данные, инфраструктуру и модели регулирования. Центральной идеей становится формирование коллективного иммунитета против цифрового неокOLONиализма, который включает технологическую автономию, информационную устойчивость и нормативную субъектность.

Заключение

Проведенный анализ позволил авторам сделать вывод, что страны БРИКС структурно неравномерно готовы к реализации общего институционально оформленного подхода к защите цифрового суверенитета. Как показывает данное исследование, существенные различия в уровне технологического развития, масштабе цифровых рынков, готовности нормативно-правового регулирования и роли государства в цифровом

пространстве формируют асимметричные условия. В результате цифровой суверенитет для одних государств выступает как инструмент закрепления уже достигнутой технологической автономии, тогда как для других – долгосрочная цель, ориентированная на преодоление зависимости от внешних цифровых инфраструктур и платформ.

Анализ национальных стратегий показывает, что задачи защиты цифрового суверенитета в странах БРИКС в ряде случаев носят принципиально различный характер. Расхождение между государствами затрудняет выработку универсальных подходов и ограничивает возможности институционализации сотрудничества в цифровой среде.

В этом контексте особого внимания заслуживает вопрос роли Китая. С одной стороны, Китай объективно является тем государством, которое способно предложить альтернативные западным цифровые платформы, инфраструктурные решения и технологические стандарты, что позволяет рассматривать его как важный фактор снижения глобальной технологической монополизации. С другой стороны, масштаб и экспансия китайских цифровых экосистем позволяют поставить вопрос о потенциальном воспроизводстве элементов цифрового неокOLONиализма, однако в отличной от западной форме. Это создает внутреннее напряжение в рамках БРИКС, поскольку доминирование одного

участника в цифровой сфере может привести к асимметрии, что противоречит политике объединения.

Для России данная конфигурация имеет двойственный характер: сотрудничество с Китаем в цифровом пространстве отвечает интересам диверсификации технологических связей и снижению зависимости от западных платформ, но и избыточная ориентация на китайские технологии несет риски замещения одной формы цифровой зависимости другой. В данных условиях интересы России в рамках БРИКС требуют выстраивания более сбалансированной модели сотрудничества, предполагающей не только использование китайских технологических решений, но и развитие собственных цифровых компетенций.

В целом выявленные противоречия свидетельствуют о том, что для БРИКС как института проблема цифрового суверенитета становится не только внешним, но и внутренним вызовом. Без учета структурной неоднородности стран-участниц, потенциальных асимметрий внутри объединения и различий в национальных интересах БРИКС рискует сохранить преимущественно декларативный характер цифрового взаимодействия. В то же время признание этих вызовов создает основу для обеспечения конструктивного сотрудничества, соответствующего как философии объединения, так и национальным интересам его участников.

Received: January 26, 2026

Accepted: March 1, 2026

DOI: 10.24833/2782-7062-2026-5-2-51-69

UDC: 327

International Politics / Research article

DIGITAL SOVEREIGNTY IN BRICS COUNTRIES: POLICY RESPONSES TO THE CHALLENGES OF DIGITAL NEOCOLONIALISM

Natalia V. Sidorenko, PhD in Political Science, Lecturer,
Department of World Political Processes, Faculty of Governance and Politics, MGIMO University,
76 Vernadsky Prospect, Moscow, 119454, Russia.
E-mail: Nataly.sidorenko@bk.ru

Valentina A. Dmitrieva, PhD in Political Science, MGIMO University,
76 Vernadsky Prospect, Moscow, 119454, Russia.
E-mail: dmitrieva.v.a@my.mgimo.ru

Maria I. Savchenkova, Analyst, Project Office of the Ministry of Science
and Higher Education of the Russian Federation based at MGIMO University;
Master's Student, MGIMO University,
76 Vernadsky Prospect, Moscow, 119454, Russia.
E-mail: savchenkova.maria@mail.ru

Abstract: The article is devoted to the analysis of digital neocolonialism and the issues of ensuring state digital sovereignty amid the transformation of the global digital space. In recent years, the concept of digital sovereignty has been gaining prominence in global political and public discourse: issues related to digital sovereignty are raised at both supranational (the EU, the World Economic Forum) and national levels (for example, Canada). The BRICS countries are not lagging behind this trend: at the current stage, each member state is implementing initiatives aimed at strengthening state digital sovereignty, enshrined in national regulatory frameworks. Some scholars associate this trend with the growing «data colonialism» of transnational digital corporations that exploit population data in exchange for services – a phenomenon referred to in the literature as digital neocolonialism. The study sets the following objectives: first, to clarify the concept of «digital sovereignty» based on contemporary domestic and international academic approaches; second, to conduct a comparative analysis of the institutional, legal-regulatory, and strategic foundations of BRICS member states' policies on protecting digital sovereignty; third, to formulate and substantiate a scenario for the development of BRICS cooperation on digital sovereignty protection in the context of international challenges posed by digital neocolonialism. The purpose of this article is to identify the current political course of the BRICS countries in protecting digital sovereignty in response to emerging challenges of digital neocolonialism. To achieve this aim, the study seeks to identify the key features of digital sovereignty and to define digital neocolonialism; to outline common steps taken by BRICS countries in protecting digital sovereignty; to determine national models of digital sovereignty protection (including new members); and to identify constraints on the development of a common BRICS approach to digital sovereignty. The research employs case study methods, document analysis, the comparative method, and scenario method. The findings make it possible to assess the potential and limits of cooperation among BRICS countries in the field of digital policy and to identify possible directions for developing coordinated approaches to the protection of digital sovereignty.

Keywords: digital sovereignty, digital colonialism, neocolonialism, BRICS countries, protection, Westphalian system, digital environment, transparency

Conflicts of interest: the author has no conflicts of interest to declare

Список литературы / References:

Calandro, E. (2025). South African digital sovereignty at the crossroad of securitization and development. In: Schiffrin, A., Donahue, E. & Mancini, M. (eds.). *Digital Sovereignty in the BRICS Countries*. Cambridge: Cambridge University Press, 81–102.

Chipangura, B. & Gustave, D.-N. (2022). Securing the cybersafety of South African online high school learners beyond COVID-19. *The Journal for Transdisciplinary Research in Southern Africa*, 18 (1), Article a1256. DOI: 10.4102/td.v18i1.1256.

Cong, W. (2025). The spatial expansion of China's digital sovereignty. In: Schiffrin, A., Donahue, E. & Mancini, M. (eds.). *Digital Sovereignty in the BRICS Countries*. Cambridge: Cambridge University Press, 63–80.

Digital Sovereignty in the BRICS Countries. (2025). Schiffrin, A., Donahue, E. & Mancini, M. (eds.). Cambridge: Cambridge University Press.

Thumfart, J. (2025). Digital sovereignty in China, Russia, and India. In: Schiffrin, A., Donahue, E. & Mancini, M. (eds.). *Digital Sovereignty in the BRICS Countries*. Cambridge: Cambridge University Press, 41–62.

Vadiati, N. & Mehran, N. (2025). Smart mandate in Iranian cities: from digital sovereignty to the automated oppression of everyday life. *Dialogues on Digital Society*, 1 (3). DOI: 10.1177/29768640251375558.

Barandova, T.L. (2025). Tsifrovaya transformatsiya v stranakh BRIKS+: al'yansy i mezhdunarodstvennyye struktury koordinatsii (obzor zarubezhnogo opyta) [Digital transformation in the BRICS+ countries: alliances and interstate coordination structures (a review of foreign experience)]. *Rossiya v global'nom mire = Russia in the Global World*, 28 (3), 9–31. DOI: 10.48612/RG/RGW.28.3.1. (In Russian)

Ignatov, A.A. (2025). Sravnitel'noe issledovanie politiki po realizatsii tsifrovogo suvereniteta gosudarstva stranami-chlenami BRIKS [A comparative study of digital sovereignty implementation policies in BRICS member states]. *Vestnik mezhdunarodnykh organizatsij = International Organisations Research Journal*, 20 (3). DOI: 10.17323/1996-7845-2025-02-04. (In Russian)

Karimnia, R., Maennel, K. & Shahin, M. (2022). Culturally-sensitive cybersecurity awareness program design for Iranian high-school students. In: *Proceedings of the 8th International Conference on Information Systems Security and Privacy (ICISSP 2022)*, 121–132. DOI: 10.5220/0010824800003120.

Krylov, D. (2025). Digital transformation of the United Arab Emirates as a tool of national modernization and foreign policy strategy (2023–2025). *Russia and the Moslem World*, 3 (329), 55–66. DOI: 10.31249/rmw/2025.03.05.

Larionova, M.V. & Shelepov, A.V. (2024). Indiya: formirovanie regulirovaniya tekhnologicheskikh kompanij dlya rosta tsifrovoy ekonomiki [India: shaping the regulation of technology companies for the growth of the digital economy]. *Vestnik mezhdunarodnykh organizatsij: obrazovanie, nauka, novaya ekonomika = International Organisations Research Journal*, 19 (2), 127–144. DOI: 10.17323/1996-7845-2024-02-07. (In Russian)

Lebedeva, M.M. (2008). Politicheskaya sistema mira: proyavleniya «vnesistemnosti», ili novye aktory – starye pravila [The world political system: manifestations of “extra-systemicity”, or new actors – old rules]. In: *“Privatizatsiya” mirovoj politiki: lokal'nye dejstviya – global'nye rezul'taty* [“Privatization” of world politics: local actions – global outcomes]. Moscow: Golden Bee, 53–66. (In Russian)

Morozova, S.S. (2025). Tsifrovoy suverenitet i global'noe sotrudnichestvo: konkuriruyushchie modeli tsifrovogo gosudarstva v Rossii, Kitae, SShA i ES [Digital sovereignty and global cooperation: competing models of the digital state in Russia, China, the USA, and the EU]. *Sotsial'nye i gumanitarnye znaniya = Social and Humanitarian Knowledge*, 11 (3), 224–235. DOI: 10.18255/2412-6519-2025-3-224-235. (In Russian)

Popova, I. (2024). Digital platforms regulation in Brazil: the political context of new laws adoption. *International Organisations Research Journal*, 19 (2), 93–109. DOI: 10.17323/1996-7845-2024-02-05.

Zinovieva, E.S. & Ignatov, A.A. (2024). The role of BRICS in the international ICT security regime. *Russian Journal of World Politics and Law of Nations*, 3 (1), 54–82. DOI: 10.24833/RJW-PLN-2024-1-54-82.

Zinovieva, E.S. & Shitkov, S.V. (2023). Tsifrovoy suverenitet v praktike mezhdunarodnykh otnoshenij [Digital sovereignty in the practice of international relations]. *Mezhdunarodnaya zhizn' = International Affairs*, 3. URL: <https://interaffairs.ru/jauthor/material/2798> (In Russian)

Литература на русском языке:

Барандова Т.Л. (2025). Цифровая трансформация в странах БРИКС+: альянсы и межгосударственные структуры координации (обзор зарубежного опыта). *Россия в глобальном мире*. Т. 28. № 3. С. 9–31. DOI: 10.48612/RG/RGW.28.3.1

Зиновьева Е.С., Шитков С.В. (2023). Цифровой суверенитет в практике международных отношений. *Международная жизнь*. No 3. URL: <https://interaffairs.ru/jauthor/material/2798>

Игнатов А.А. (2025). Сравнительное исследование политики по реализации цифрового суверенитета государства странами-членами БРИКС. *Вестник международных организаций*. Т. 20. № 3. DOI: 10.17323/1996-7845-2025-02-04

Ларионова М.В., Шелепов А.В. (2024). Индия: формирование регулирования технологических компаний для роста цифровой экономики. *Вестник международных организаций: образование, наука, новая экономика*. Т. 19. № 2. С. 127–144. DOI: 10.17323/1996-7845-2024-02-07

Лебедева М.М. (2008). Политическая система мира: проявления «внесистемности»: или новые акторы – старые правила. В: «Приватизация» мировой политики: локальные действия – глобальные результаты / под ред. М.М. Лебедевой. М.: Голден Би. С. 53–66.

Морозова С.С. (2025). Цифровой суверенитет и глобальное сотрудничество: конкурирующие модели цифрового государства в России, Китае, США и ЕС. *Социальные и гуманитарные знания*. Т. 11. № 3. С. 224–235. DOI: 10.18255/2412-6519-2025-3-224-235

Krylov D. (2025). Digital Transformation of the United Arab Emirates as a Tool of National Modernization and Foreign Policy Strategy (2023–2025). *Russia and the Moslem World*. № 3 (329). P. 55–66. DOI: 10.31249/rmw/2025.03.05