Non multa, sed multum

ИНДЕКС БЕЗОПАСНОСТИ №4 (51) I 2024

НАУЧНЫЕ ЗАПИСКИ

Леонид Цуканов

ОТ ЗАЛИВА ДО СУБСАХАРСКОЙ АФРИКИ: РАЗВИТИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ И ИНТЕРЕСЫ РОССИИ

МГИМО УНИВЕРСИТЕТ

ПИР-ЦЕНТР Non multa, sed multum 1994-2024

приоритет2030^ лидерами становятся

МОСКВА, 2024

Главный редактор: В.А. Орлов

Технический редактор: Е.Г. Чобанян

Рецензенты: В.Б. Козюлин, С.А. Себекин, В.А. Орлов

Цуканов Леонид Вячеславович. *От Залива до Субсахарской Африки*: развитие цифровых технологий и интересы России / Тех. ред. Е.Г. Чобанян. М.: ПИР-Пресс, 2024. – 23 с. – (*Индекс Безопасности* – Научные записки).

ISBN 978-5-6051623-8-4

Цифровые технологии играют все большую роль в мировой политике и экономике. По мере развития глобального сетевого общества потребность национальных государств в использовании высокотехнологичных инструментов для достижения внешне- и внутриполитических целей приобретает основополагающее значение, что обусловлено стремлением занять выгодные позиции в новом, высокотехнологичном мире. На примере государств Персидского залива и Субсахарской Африки автор выделяет ключевые аспекты сотрудничества, включая цифровую безопасность, использование цифровых технологий в экономике и государственном управлении, развитие искусственного интеллекта и разработку программного обеспечения. Отмечено, что несмотря на культурные и экономические различия, оба региона сталкиваются со схожими задачами в сфере цифровизации, что создает благоприятные условия для сотрудничества России с местными игроками.

Данная научная записка и другие материалы научной серии размещены на сайте:
https://nonproliferation.world/indeks-bezopasnosti

Данная научная записка подготовлена в рамках реализации совместного проекта ПИР-Центра и МГИМО МИД России *Глобальная безопасность, стратегическая стабильность и контроль над вооружениями* под эгидой Программы стратегического академического лидерства *Приоритет-2030*.

ISBN 978-5-6051623-8-4

9 785605 162384 >

Автор

ЦУКАНОВ Леонид Вячеславович

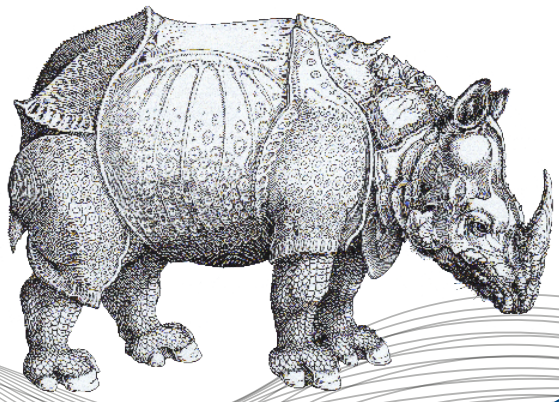
Кандидат политических наук, консультант программы *Глобальная и региональная безопасность: новые идеи для России*, журналист-международник.

Четвертьфиналист премии *Innovators in Global Affairs* в категории *Международное сотрудничество* (Open Network, 2021), полуфиналист Международной премии Насера бен Хамада в сфере молодежного творчества по треку *наука* (Бахрейн, 2021); Лауреат премии имени Г.М. Евстафьева для молодых специалистов в области международной безопасности и ядерного нераспространения (ПИР-Центр, 2022). Победитель конкурса молодых журналистов-международников в категории *лучшая аналитическая статья по международной проблематике* (РСМД/СЖР, 2023).

Прошел курсы повышения квалификации по проблемам региональной безопасности на Ближнем Востоке (Tel-Aviv University, МГИМО), и кибербезопасности (УрФУ им. Б.Н. Ельцина, Arab Academy for Science, Technology & Maritime Transport), а также по вопросам исследования проблем терроризма (Universiteit Leiden, Allameh Tabataba'i University).

Экспертиза: современные вызовы и угрозы международной безопасности, вопросы безопасности на Ближнем Востоке, кибербезопасность (с углубленной специализацией на киберсистемах государств Ближнего Востока), противодействие терроризму.

Эл. почта: leon.tsukanov@mail.ru



Оглавление

Главное

- Масштабы *цифрового разрыва* в АЮС и Персидском заливе варьируются от страны к стране даже в рамках одного региона, а совместные подходы к обеспечению безопасности и политико-экономической кооперации в цифровом пространстве пока не прошли проверку временем и имеют в основном реактивный характер.

- Помимо *позднего старта* подавляющего большинства рассмотренных держав в цифровом мире, общими вызовами для стран АЮС и Залива являются инертность законодательной сферы, сохранение устаревшей системы государственных институтов с дублирующим функционалом, дисбалансы в диалоге между государством и бизнес-сектором.

- Опыт России – как одного из активных акторов глобального цифрового пространства – интересен и востребован как со стороны АЮС, так и Персидского залива.

- Кооперация между Россией и значительной частью стран рассмотренных регионов пока имеет реактивный (в некоторых случаях ситуативный) характер.

- Конкуренция за рынки стран Персидского залива и АЮС сегодня находится на достаточно высоком уровне, особенно по таким направлениям как технологии искусственного интеллекта, кибербезопасности и программного обеспечения.

- В тройке лидеров по темпам и масштабам развития профильного диалога остаются (в порядке убывания влиятельности) КНР, США и страны ЕС. Стремительно наращивает показатели Индия. Россия стремится не вступать в жесткую конфронтацию ни с одним из передовых техноигроков, продвигая принципы открытой и честной конкуренции.

От Залива до Субсахарской Африки: развитие цифровых технологий и интересы России

Леонид Цуканов

Цифровые технологии играют все большую роль в мировой политике и экономике. По мере развития глобального сетевого общества потребность национальных государств в использовании высокотехнологичных инструментов для достижения внешне- и внутриполитических целей приобретает основополагающее значение, что обусловлено стремлением занять выгодные позиции в новом, высокотехнологичном мире.

Данная тенденция характерна для всех без исключения регионов мира, однако в каждом она проявляется по-разному. В рамках данного доклада предлагается остановиться на двух регионах – страны Персидского залива и Африки южнее Сахары (АЮС).

Несмотря на то, что эти два региона имеют непохожий экономический, социально-политический и культурный бэкграунд, они в равной степени заинтересованы в гармоничной интеграции в глобальный цифровой мир, а также в активном участии в мировых процессах.

Россия, как и другие мировые игроки, проявляет повышенный интерес к развитию потенциала регионов Персидского залива и Африки южнее Сахары, видя в этом в т.ч. возможность для достижения собственных долгосрочных целей, включая выход на новые цифровые рынки. На этом фоне вопросы, связанные с оценкой потенциала региональных держав в высокотехнологической отрасли (равно как и оценка потенциальных точек соприкосновения с интересами и возможностями Москвы), приобретают особую актуальность и значимость.

При проведении исследования упор был сделан на ряд категорий группы *цифровые технологии*, к которым Москва проявляет повышенное внимание:

- Вопросы цифровой безопасности[1];
- Цифровые технологии в экономике и управлении;
- Применение технологий искусственного интеллекта (ИИ);
- Национальные разработки в области ПО и сотрудничество в этой области.

[1] В силу наличия разных подходов к трактовке и соотношению понятий *международная информационная безопасность* и *кибербезопасность* в России и странах рассматриваемого региона группа дополнительно разделена на две подкатегории: технико-технологическая защита (кибербезопасность) и социальное измерение безопасности.

С целью более эффективного сопоставления показателей государств, находящихся по разные стороны Персидского залива, автором исследования введена категория *Персидский залив+* – для условного обозначения группы государств, включающей страны ССАГЗ (Королевство Саудовская Аравия, ОАЭ, Государство Катар, Королевство Бахрейн, Султанат Оман, Государство Кувейт)[2], а также Исламскую Республику Иран и Республику Ирак. Подобное методологическое допущение позволит избежать путаницы при использовании уже устоявшихся в научной литературе терминов, а также даст возможность анализировать показатели сразу восьми стран, не объединенных какой-либо отдельной интеграционной площадкой.

В случае с регионом Африки южнее Сахары перечень государств для анализа определен на основании классификации Всемирного банка и Общероссийского классификатора стран мира. Границы анализируемого региона определены в квадрате от Гвинейского залива Атлантического океана до Аденского залива и Индийского океана[3].

В качестве источниковой базы исследования использованы материалы международных организаций, отчеты и доклады министерств и ведомств региона, материалы СМИ, статистические базы. Были применены такие методы как системный анализ, ивент-анализ, моделирование, case-study, SWOT-анализ и ряд других методов научного познания – включая методы конкурентной разведки.

В предложенной научной записке в сжатом формате приведены основные выводы, касающиеся общих трендов развития государств из групп *Персидский залив+* и АЮС в разрезе высокотехнологического развития и вопросов обеспечения безопасности цифрового пространства.

Роль России в процессах цифрового развития стран рассмотренных регионов проанализирована как с позиции индивидуального участия (в государственном и частном секторах), так и с точки зрения работы на региональных и международных площадках.

[2] Также по тексту для условного обозначения стран ССАГЗ автором будет использоваться термин *аравийские монархии*.
[3] См., напр.: Sub-Saharan Africa // World Bank. URL: https://data.worldbank.org/country/C9

ОЦЕНКА ЦИФРОВОГО ЛАНДШАФТА ГОСУДАРСТВ РЕГИОНОВ ПЕРСИДСКОГО ЗАЛИВА И АФРИКИ ЮЖНЕЕ САХАРЫ В РАЗРЕЗЕ ВОПРОСОВ РЕГИОНАЛЬНОЙ И ГЛОБАЛЬНОЙ БЕЗОПАСНОСТИ

Среди стран группы *Персидский залив+* и государств Африки Южнее Сахары растет нацеленность на постепенное совершенствование национальных подходов к деятельности в цифровом пространстве. Представители обоих регионов видят в цифровизации *широкое пространство возможностей*[4], как экономического, так и социально-политического характера.

Работа по каждому из рассмотренных в рамках раздела тематических направлений (*цифровая безопасность*, *цифровые технологии в экономике и госуправлении*, *развитие ИИ-технологий*» и «*разработка ПО*) характеризуется постепенным зарождением системного подхода (за исключением тех стран, развитие цифровых систем которых отложено из-за внутренней смуты). Для обоих регионов также характерно стремление максимально охватить все сферы сразу, обеспечив тем самым гармоничное развитие разных направлений цифрового поля.

Конечно, масштабы *цифрового разрыва* (как и доступные ресурсы для его купирования) варьируются от страны к стране (*см. диаграмму* 1[5]) даже в рамках одного региона, а совместные подходы к обеспечению безопасности и политико-экономической кооперации в цифровом пространстве пока не прошли проверку временем и имеют в основном реактивный характер.

Это справедливо не только в случае с АЮС, где работа по формированию систем защиты критической информационной инфраструктуры (КИИ) началась сравнительно недавно и сопряжена с экономическими, политическими и социальными препонами; регион Залива испытывает во многом схожие проблемы.

Так, несмотря на то что во всех аравийских монархиях к настоящему моменту созданы общенациональные Группы реагирования на компьютерные инциденты[6], модерниза-

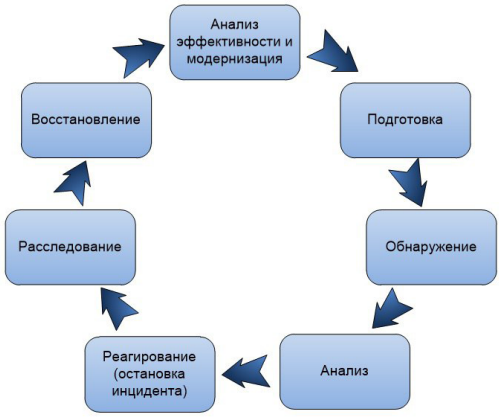
[4] См.: The potential impact of Artificial Intelligence in the Middle East // PwC. URL: https://www.pwc.com/m1/en/publications/potential-impact-artificial-intelligence-middle-east.html#help; Africa Has Become The First Region in The World to Implement a Child Online Safety and Empowerment Policy // African Union. 23.05.2024. URL: https://au.int/en/pressreleases/20240523/child-online-safety-and-empowerment-policy-africa-union и др.

[5] Пояснение к диаграмме: в силу смены методологии в *Индексах* МСЭ за 2021 г. и 2024 г. (в частности, отказа от сплошного рейтингования, повлекшего за собой появление большой группы государств с максимальными показателями), сравнение позиций в динамике носит обобщенный характер и призвано проиллюстрировать трансформацию подходов к оценке цифровых возможностей национальных государств. При этом категории анализа, на основании которых выведены итоговые показатели, значительных изменений не претерпели, что позволяет отслеживать основные тренды развития.

[6] Посчитано по: CERT-In. URL: https://www.cert-in.org.in/s2cMainServlet?page-

ция системы реагирования проводится только в двух странах (Катар, Оман). Еще в двух государствах (ОАЭ, Саудовская Аравия) дополнительные отраслевые группы CERT находятся в стадии формирования. При этом во всех аравийских монархиях функционируют частые мониторинговые группы и группы поддержки, обеспечивающие компьютерную безопасность критически важных сфер[7]. Кроме того, из единого строя волей-неволей выпадают Иран (позиционируемый как полностью самостоятельный цифровой полюс, отчасти конфронтирующий со странами ССАГЗ) и Ирак, испытывающий систематический кадровый и ресурсный дефицит.

Структура системы управления инцидентами



Общая схема реагирования CERT на инциденты в области цифровой безопасности

Источник: www.securelist.ru

Отдельное внимание следует заострить на феномене кибертерроризма – в каждом из рассмотренных регионов эта проблема раскрывается со своей спецификой. Несмотря на то, что возможность радикально-экстремистских группировок и движений в киберпространстве существенно ограничены – а сами радикалы предпочитают использовать Интернет как площадку пропаганды и априори не могут нанести серьезный ущерб КИИ крупных и технологически развитых держав[8] – все без исключения государства группы *Персидский залив+* включают его в группу основополагающих угроз, что отражено в национальных стратегиях[9].

В случае с АЮС проблема кибертерроризма, на первый взгляд, не получает значительного (в сравнении с группой *Персидский залив+*) выражения – в силу специфики социально-экономического ландшафта, а также более слабого присутствия исламистов в цифровом пространстве. Хотя члены радикально-экстремистских группировок и используют ИКТ-инструменты для решения смежных задач – например, ведения агитационной и вербовочной работы, сбора информации и координации действий джихадистских ячеек[10], какие-либо сведения о попытках африканских радикалов наладить контакты с хакерскими движениями для проведения совместных атак против КИИ или разработать собственные варианты *кибероружия* отсутствуют.

При этом страны АЮС не спешат списывать со счетов данный тип угрозы – тем более, что темпы цифровизации стран региона стремительно растут, а общее число Интернет-пользователей

id=ADWCERTVIEW
[7] Там же.
[8] Подробнее о развитии джихадистами системы цифровой борьбы читайте в Научной записке ПИР-Центра. См.: Цуканов Л.В. Взлеты и падения Киберхалифата: Аль-Каида* и ИГИЛ* в цифровом пространстве // ПИР-Центр, 2022. URL: https://pircenter.org/wp-content/uploads/2022/09/SI-RUS-%E2%84%9617-43-Tsukanov.pdf
[9] Выявлено на основе анализа национальных стратегий национальной безопасности и кибербезопасности, а также документов военного планирования государств группы *Персидский залив+*.
[10] Grobbelaar A. Can 'Cyberterrorism' Really Exist in Africa? // Global Network. 10.03.2023. URL: https://gnet-research.org/2023/03/10/can-cyberterrorism-really-exist-in-africa/

уже превысило отметку в 540 млн человек[11]. Радикально-экстремистские движения реагируют на изменения и стремятся расширить свое влияние, а в перспективе – еще и нарастить *ударные* средства, способные наносить ущерб критической инфраструктуре[12]. По этой причине государства АЮС определяют значимость террористической угрозы из киберпространства примерно на том же уровне, что и государства Залива.

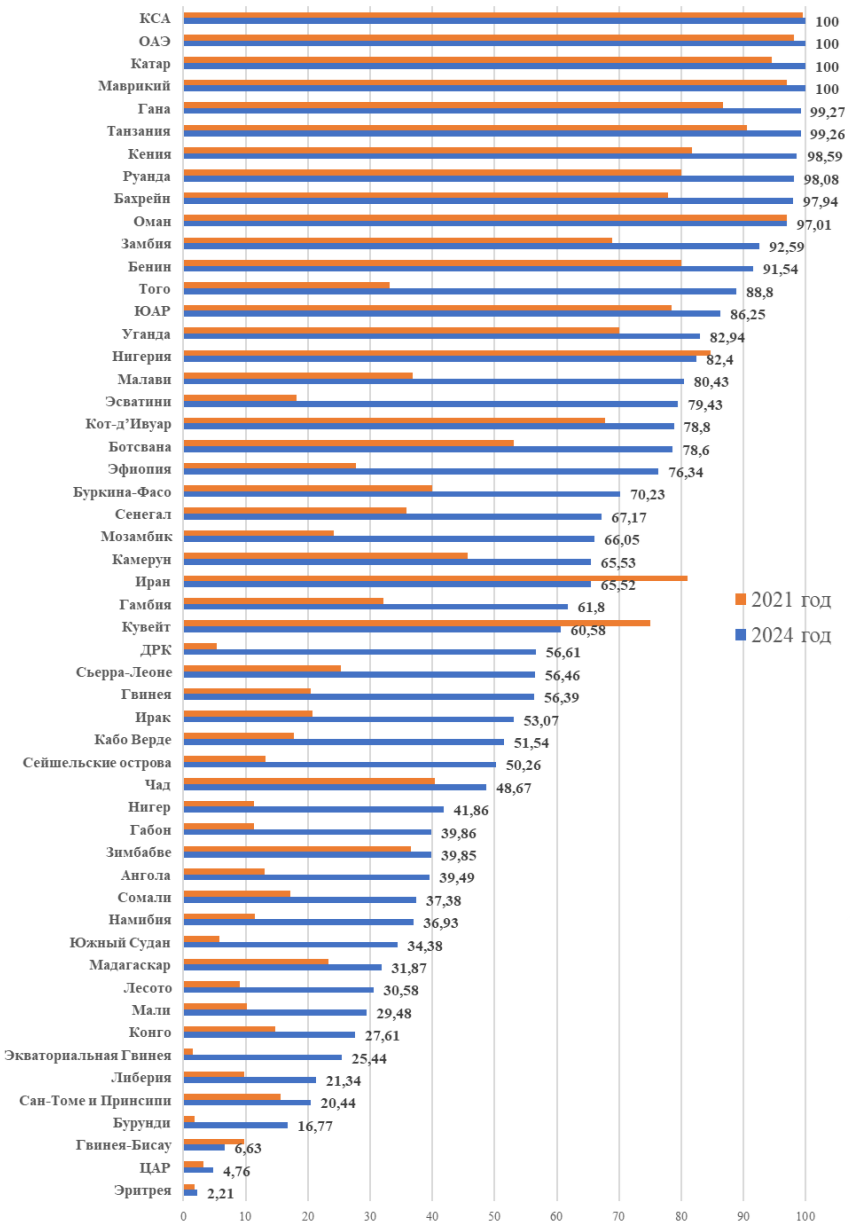


Диаграмма 1. Совокупный показатель киберготовности государств групп Персидский залив+ и АЮС по состоянию на 2024 г. (максимальный балл – 100; приведено в порядке убывания)

Составлено по: GCI-2020, GCI-2024

[11] Number of internet users in Africa as of January 2024, by country // Statista. URL: https://www.statista.com/statistics/505883/number-of-internet-users-in-african-countries/

[12] Соответствующие установки по развитию *джихадистской кибердоктрины* были, среди прочего, даны лидером Аль-Каиды Айманом аз-Завахири после вступления в должность в 2022 г.

Другими характерными чертами для Персидского залива и АЮС, помимо *позднего старта* подавляющего большинства рассмотренных держав в цифровом мире, являются инертность законодательной сферы, сохранение (пусть и только в части стран) устаревшей системы государственных институтов с дублирующим функционалом, дисбалансы в диалоге между государством и бизнес-сектором (как национальным, так и зарубежным)[13].

Открытым для обоих регионов остается и феномен значительной спонсорской помощи от передовых игроков – получение которой, как правило, не рассматривается как посягательство на национальный суверенитет. Напротив, в ряде случаев оно позиционируется как *необходимый этап* национальной трансформации. Подобные настроения фиксируются как в регионе АЮС, так и в зоне Персидского залива.

Вместе с тем, даже с учетом сохранения зависимости от внешней поддержки цифровых проектов, некоторые страны (Саудовская Аравия и ОАЭ в группе *Персидский залив+*, Маврикий, Гана и Танзания в АЮС) уже претендуют на звание глобальных *законодателей* цифровых процессов, по инвестиционной привлекательности не уступающих державам Старого света.

АНАЛИЗ ТЕКУЩЕГО ПРИСУТСТВИЯ РОССИИ В РЕГИОНЕ, ВЫЯВЛЕНИЕ СИЛЬНЫХ И СЛАБЫХ СТОРОН ВЫБРАННОЙ СТРАТЕГИИ ДЕЙСТВИЙ

Опыт России – как одного из активных акторов глобального цифрового пространства – интересен и востребован как со стороны АЮС, так и Персидского залива, ввиду чего степень вовлеченности Москвы в развитие цифровых систем рассмотренных регионов с течением времени растет.

Москва и державы рассмотренных регионов имеют общие взгляды на глобальный ландшафт цифровых угроз[14], а также, в целом, совпадающее видение перспектив развития инструментов цифровой экономики – как неотъемлемой части создания безопасной цифровой среды на национальном, региональном и глобальном уровнях.

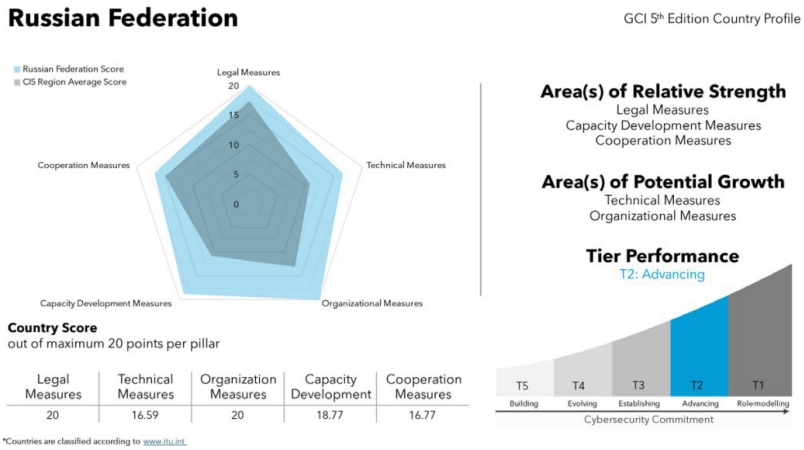
Несмотря на влияние некоторых деструктивных факторов (в первую очередь, попыток США и ряда недружественных стран

[13] См.: Arab Laws Online Database. URL: https://www.arablawsworld.com/; Cybersecurity threatscape of African countries 2022–2023 // Positive Technologies. 28.07.2023. URL: https://www.ptsecurity.com/ww-en/analytics/africa-cybersecurity-threatscape-2022-2023/ и др.

[14] Выявлено на основе анализа национальных стратегий национальной безопасности и кибербезопасности, а также документов военного планирования государств групп *Персидский залив+* и АЮС.

посредством санкционного давления и политического шантажа снизить темпы кооперации региональных акторов с Россией, а также ограничить расширение влияния российского IT-бизнеса), Москва выглядит перспективным партнером как для государств группы *Персидский залив+*, так и Субсахарской Африки по всем рассмотренным тематическим направлениям.

Ярким примером тому служит развитие профильной кооперации с Кувейтом. Страна традиционно занимает жесткую атлантистскую позицию и отдает приоритет американскому и европейскому технологическому бизнесу, сужая тем самым *окно возможностей* для российских компаний. Тем не менее, успешный опыт реализации техностартапа *Кет*[15], запущенного российскими IT-специалистами в 2023 г., повысил привлекательность услуг отечественных компаний – в первую очередь работающих в сфере финансовых технологий.



Национальный профиль России в Глобальном рейтинге киберготовности Международного союза электросвязи (2024)

Источник: www.ITU.ru

Аналогичным образом ситуация развивается и в случае с АЮС. Несмотря на то, что в опубликованном в сентябре 2024 г. рейтинге киберготовности МСЭ Россия в глобальном зачете уступила по совокупному показателю как минимум шести странам АЮС (Маврикию, Гане, Танзании, Кении, Руанде и Замбии)[16], ее практический опыт (особенно в части совершенствования национального потенциала и нормативно-правовой деятельности) востребован.

При этом говорить о *балансе направлений* в данном случае не приходится – наиболее востребованным для обоих регионов является опыт России по отражению массированных кибератак против КИИ, а также развития социального измерения цифровой безопасности[17]; повышенным интересом пользуются отечественные FinTech и EGov-решения[18]. При этом в сфере искусственного интеллекта и разработки программного обеспечения Москва пока находится на догоняющих позициях – хотя, благо-

[15] Как выходцы из России создали в Кувейте систему быстрых платежей // Forbes. 08.11.2023. URL: https://www.forbes.ru/investicii/499506-kak-vyhodcy-iz-rossii-sozdali-v-kuvejte-sistemu-bystryh-platezej

[16] Эксперты МСЭ объясняют уменьшение совокупного показателя РФ проседанием по техническим мерам и международному сотрудничеству, что обусловлено усилением санкционного режима и снижением интенсивности международных контактов РФ со странами Запада по профилю кибербезопасности. См.: Global Cybersecurity Index 2024 // ITU. 15.09.2024. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

[17] Чернышенко: к 2030 году сайты России будут подвергаться кибератакам каждые 2 секунды // ИТАР-ТАСС. 16.04.2024. URL: https://tass.ru/obschestvo/20560057

[18] См., напр.: Россия поможет Африке в цифровизации государственных сервисов // HSE Daily. URL: https://daily.hse.ru/post/rossiya-pomozhet-afrike-v-cifrovizacii-gosudarstvennyh-servisov; Суэф К. Цифровизация как способ преодоления неравенства в Африке // Россия в глобальной политике. 31.01.2024. URL: https://globalaffairs.ru/articles/czifrovizacziya-v-afrike/

даря развитию инструментов импортозамещения, и сокращает отставание от КНР и США.

Одной из сильных сторон российского подхода к диалогу с рассмотренными регионами можно счесть упор на отстаивание технологической независимости региональных держав и их права на защиту собственного *цифрового суверенитета*[19]. Такая тактика выгодно влияет на позиции Москвы на контрасте с политикой стран Старого света, чьи действия часто воспринимаются через *колониальную* призму.

Наконец, грамотное использование бренда БРИКС – как площадки кооперации стран разных регионов (в т.ч. технологической) в интересах совместного развития и процветания – дает возможность строить диалог без оглядки на географические границы, ускоряя формирование глобального цифрового общества[20].

Так, например, под эгидой БРИКС может продолжиться разработка совместных цифровых активов – с целью минимизации сопутствующих геополитических рисков, а также увеличения вовлеченности других заинтересованных держав (Индии и Китая). Еще в марте 2024 г. было анонсировано, что Россия будет стремиться к созданию в рамках объединения независимой платежной системы, основанной на цифровых валютах и блокчейне[21]. Как впоследствии отметил помощник Президента Юрий Ушаков, создание независимой и высокотехнологичной платежной системы отвечает долгосрочным задачам БРИКС, поскольку позволит повысить *удельный вес* как объединения в целом, так и отдельных его членов в мировой финансовой системе[22]. Эта тема также стала одной из магистральных на саммите БРИКС в Казани, который прошел в октябре 2024 г.[23].

Обсуждение вопросов международного цифрового сотрудничества на полях Казанского саммита БРИКС в форматах *аутрич* и *БРИКС+*, 24 октября 2024 г.

Источник: www.kremlin.ru

С другой стороны, профильное взаимодействие не лишено сложностей. В первую очередь, кооперация между Россией и значительной частью стран рассмотренных регионов пока имеет реактивный (в некоторых случаях ситуативный) характер. Также отмечено преобладание стремления развития национальных систем цифровой безопасности и защиты в сравнении с

[19] Что такое цифровой суверенитет и как Кремль его хочет достичь: главные цели до 2030 года // РАЭК. 02.07.2024. URL: https://raec.ru/live/smi/14494/
[20] В Кремле заявили о планах создания в БРИКС платежной системы на блокчейне // РБК. 05.03.2024. URL: https://www.rbc.ru/crypto/news/65e6c0a69a7947a2f97dc580; Минэкономразвития: РФ предлагает БРИКС использовать ИИ в совместных проектах // URA.RU. 06.06.2024. URL: https://ura.news/news/1052777935 и др.
[21] В Кремле заявили о планах создания в БРИКС платежной системы на блокчейне // РБК. 05.03.2024. URL: https://www.rbc.ru/crypto/news/65e6c0a69a7947a2f97dc580
[22] Кремль анонсировал создание в БРИКС платежной системы на блокчейне // ИТАР-ТАСС.05.03.2024. URL: https://tass.ru/ekonomika/20154635
[23] Строители платформ: что мешает созданию единого платежного механизма стран БРИКС // Forbes. 23.10.2024. URL: https://www.forbes.ru/mneniya/523569-stroiteli-platform-cto-mesaet-sozdaniu-edinogo-plateznogo-mehanizma-stran-briks

коллективными. Особенно ярко это выражается в случае с регионом Залива, где интенсивность профильного диалога с отдельными аравийскими монархиями кратно превышает аналогичное взаимодействие по линии *Россия* – ССАГЗ[24].

Также в числе уязвимых мест резонно упомянуть наличие атмосферы недоверия между передовыми региональными игроками, ограничивающее масштабы обмена опытом в области чувствительных технологий. В контексте этой проблемы любые попытки внешних акторов (включая Россию) *дирижировать* распространением технологий и работать над формированием общих инициатив в области цифровой защиты воспринимаются странами региона в штыки.

Москве при развитии сотрудничества важно помнить о ключевых угрозах; в первую очередь, урон диалогу может нанести усиление региональной напряженности, которое чревато переносом противостояния в цифровое пространство

Конечно, как уже отмечалось ранее, страны Персидского залива и АЮС постепенно делают ставку на активизацию диалога между двумя регионами по линии цифрового развития и безопасности – и используют для этих целей в том числе общие площадки – однако пока уровень этого взаимодействия характеризуется как весьма слабый.

Говоря о возможностях дальнейшего развития связей России и выделенных регионов, уместно отметить, что рост числа угроз в цифровом пространстве с одной стороны и ускорение темпов развития глобальной цифровой экономики с другой закладывают основу для более широкой кооперации как с АЮС, так и с Персидским заливом (особенно в контексте реализации совместных инициатив под эгидой международных и региональных площадок).

Тем не менее, Москве при развитии сотрудничества важно помнить о ключевых угрозах. В первую очередь, урон диалогу может нанести усиление региональной напряженности, которое чревато переносом противостояния в цифровое пространство. В свете разморозки ряда конфликтов как на Ближнем Востоке, так и на Африканском континенте, риск обострения противоречий между государствами увеличился, что в перспективе способно ограничить круг партнеров России на технологическом треке.

С точки зрения интересов самой России, основную угрозу несет перспектива усиления давления со стороны недружественных стран с целью воспрепятствовать укреплению российских позиций на новых рынках. Это давление может носить как прямой (искусственное ограничение работы российских компаний с помощью санкций), так и косвенный (запугивание стран-партнеров по диалогу) характер.

Оценка перспектив развития диалога РФ с рассмотренными регионами в контексте цифровой безопасности и развития (в

[24] Например, по состоянию на середину 2024 г., средняя доля российских IT-компаний, предоставляющих услуги на рынках стран группы *Персидский залив+*, составляет около 6%. Для сравнения: усредненный показатель США – 28%, КНР – 20%, Японии – 9,5%. Посчитано по: Global Database. URL: https://www.globaldatabase.com/

рамках выявленных общих трендов) представлена далее (*см. таблицу 1*).

	Положительное влияние	**Отрицательное влияние**
Внутренняя среда	***Сильные стороны (strengths)*** – общие взгляды на пространство цифровых угроз, схожие подходы к их градации – схожие цели и задачи долгосрочного развития, в которых цифровизация играет ключевую роль, формируя запрос на выработку коллективных мер цифровой защиты – ставка партнеров по диалогу на развитие международного сотрудничества, схожие подходы к выбору внешних партнеров	***Слабые стороны (weaknesses)*** – реактивный и ситуативный характер кооперации, приоритет развития национальных систем киберзащиты – слабая развитость профильных связей между странами внутри региона, низкий уровень межрегионального взаимодействия – наличие атмосферы недоверия, нежелание делиться чувствительными технологиями
Внешняя среда	***Возможности (opportunities)*** – неблагоприятный фон стимулирует кооперацию в сфере киберзащиты как внутри региона, так и между ними – развитие сотрудничества в рамках совместного участия в глобальных и региональных инициативах (в первую очередь, инициативах БРИКС)	***Угрозы (threats)*** – усиление давления на Россию (санкционного и пр.) и ее ближайших региональных партнеров для нарушения кооперации – рост региональной напряженности, перенос конфликтов в цифровое пространство

Таблица 1. Оценка перспектив развития диалога РФ с рассмотренными регионами в контексте цифровой безопасности и развития (в рамках выявленных общих трендов; SWOT-анализ)

Составлено автором

ВЫЯВЛЕНИЕ КЛЮЧЕВЫХ КОНКУРЕНТОВ МОСКВЫ В ОБОЗНАЧЕННОЙ СФЕРЕ, ОЦЕНКА ИХ ТЕКУЩИХ ПОЗИЦИЙ И ИНТЕРЕСОВ

Конкуренция за рынки стран Персидского залива и АЮС сегодня находится на достаточно высоком уровне. Передовые игроки стремятся охватить как можно больше профильных сфер и вывести сотрудничество на уровень стратегического взаимодействия как на межгосударственном уровне, так и в бизнес-среде.

При это в тройке лидеров по темпам и масштабам развития профильного диалога остаются (в порядке убывания влиятельности) КНР, США и страны ЕС. Стремительно наращивает показатели Индия, чей разрыв с лидерами группы в последние годы заметно сократился.

Первый в истории Глобальный саммит по безопасности искусственного интеллекта. Лондон, 2023 г.

Источник: www.gov.uk

Следует отметить, что КНР и Индия – единственные внешние акторы, в том или ином виде поддерживающие диалог со всеми без исключения странами Персидского залива и АЮС, в то время как в диалоге с западными странами сохраняются *белые пятна* (см. таблицу 2).

При этом в числе сфер, где конкуренция за рынки рассмотренных регионов имеет наиболее острый характер, следует выделить рынок технологий искусственного интеллекта, кибербезопасности и программного обеспечения. Для достижения лидерства на перечисленных направлениях передовые игроки используют весь доступный инструментарий, включая политический шантаж и санкционное давление.

Также в числе трендов отмечено постепенное вовлечение в профильное сотрудничество в качестве *внешнего игрока* тех стран (в некоторых случаях – групп стран), которые имеют географическую близость к рассматриваемому региону, но не относятся к нему напрямую (Турция на Ближнем Востоке, Арабские страны Северной Африки применительно к АЮС).

Примечательно, что все большую роль в продвижении инициатив глобальных акторов играют международные и региональные площадки, в рамках которых нередко оговаривается формула сотрудничества, а также возможная коллективная позиция участников взаимодействия.

Россия стремится не вступать в жесткую конфронтацию ни с одним из передовых техноигроков, продвигая принципы открытой и честной конкуренции на рынках Персидского залива и Субсахарской Африки, а также поддерживает курс дружественных стран (КНР, Индия и др.) на развитие коллективных цифровых компетенций региональных стран.

Страна	США	КНР	Индия	ЕС	Великобритания	Турция	Южная Корея	Япония	Аравийские монархии (общий средний показатель группы)	Арабские страны Северной Африки (общий средний показатель группы)	Иран
Ангола	2,25	2,25	1	1,5	*	0,25	*	*	1	1,25	0,5
Бахрейн	3	3	2,75	2,5	1,5	1,5	1,75	1	-	*	*
Бенин	2,5	2,25	1	1,75	*	0,5	*	*	1	1,5	0,5
Ботсвана	2,5	2,25	1,25	1,25	*	0,5	*	*	1	1,5	0,5
Буркина-Фасо	0	2,5	1	0	*	0,25	*	*	0,5	1,25	0,75
Бурунди	2,25	2,25	1	1,25	*	0,25	*	*	0,5	1,5	0
Габон	2,75	2,5	1,75	2	*	0,75	*	*	1	1,5	0,5
Гамбия	2,75	2,75	1,5	2	*	1,25	*	*	1,5	1,5	0,75
Гана	3	2,5	1,75	2,75	*	1,5	*	*	1,75	2	1,25
Гвинея	2	2	1	1,5	*	0,5	*	*	1,25	1,5	0,25
Гвинея-Бисау	1,5	2,25	1	1,25	*	0,25	*	*	0,75	1	0
ДРК	1,25	2,25	0,5	0,25	*	0,25	*	*	0,5	1	0,25
Замбия	2,25	2,5	1	2,5	*	0,75	*	*	1,25	1,5	0,25
Зимбабве	2	2,25	1	1,5	*	0,25	*	*	1,25	1,5	0
Ирак	2	2,75	2,5	2	1,25	1,75	1,75	1,5	*	*	*
Иран	0	3,5	2,75	0	0	1	0	0	*	*	-
Кабо-Верде	1,75	2	0,75	1,75	*	0,25	*	*	1	1,25	0
Камерун	2,75	2,5	1,5	3	*	1,25	*	*	1,75	1,25	1,25
Катар	3	3,25	3	2,25	1,5	2,75	2	1,5	-	*	*
Кения	3,25	3,25	2,25	3,25	*	1,75	*	*	3	3	2,25
Конго	2,25	2,25	1,25	2,5	*	1	*	*	1,25	1,75	0,75
Кот-д'Ивуар	2,25	2,75	1,5	1,75	*	0,25	*	*	1,25	1,5	0,25
КСА	4	3,5	3,5	2,5	2	1,75	2,25	2	-	*	*
Кувейт	2,25	2	2,25	2,25	1,75	1,25	1,75	1	-	*	*
Лесото	2	2,25	1	1,25	*	0,25	*	*	0,75	1,25	0,25
Либерия	1,25	2	0,5	1	*	0,25	*	*	0,75	1	0
Маврикий	3	2,5	2,5	3	*	1	*	*	3	2	0,75
Мадагаскар	2,25	2,5	2	2	*	0,75	*	*	1,5	1,5	0,5
Малави	2	2	1,25	1,5	*	0,25	*	*	0,75	1,25	0
Мали	0	2,25	1,25	0	*	0,25	*	*	0,75	1	1,25

Страна[25]	США	КНР	Индия	ЕС	Великобритания	Турция	Южная Корея	Япония	Аравийские монархии (общий средний показатель группы)	Арабские страны Северной Африки (общий средний показатель группы)	Иран
Мозамбик	1,75	2,25	0,75	1,25	*	0,25	*	*	1,5	1,25	0,75
Намибия	2,25	2,5	1,75	2	*	1	*	*	1,25	1,5	1
Нигер	0	2,75	1	0	*	0,5	*	*	1,5	1,5	1,25
Нигерия	3,25	3,25	2,5	2,75	*	1,25	*	*	2,25	1,5	1,25
ОАЭ	4	3,5	3,25	2,5	2	2	2,75	1,75	-	*	*
Оман	2,25	3	2,5	2,25	1,25	1,25	1,75	1,25	-	*	*
Руанда	2,25	2,75	2,25	2,5	*	1,25	*	*	2,25	2	1
Сан-Томе и Принсипи	2	2	1,25	1,5	*	0,25	*	*	0,75	1,25	0
Сейшельские острова	1,75	2,25	2	1	*	0,25	*	*	0,75	1,25	0
Сенегал	2,25	2,5	1,25	2	*	0,5	*	*	1,25	1,5	0,5
Сомали	1,25	2	1	1	*	1	*	*	1,25	0,75	0
Сьерра-Леоне	2	2	1,5	2	*	0,25	*	*	1	1,5	0,5
Танзания	3	3,5	1,75	2,75	*	1,5	*	*	2	2	2
Того	2,25	2,25	1,75	1,75	*	0,5	*	*	1,5	1,5	1
Уганда	2	2,75	1,5	2	*	0,5	*	*	1,25	1,5	2,25
ЦАР	1,25	2,25	1	0,75	*	0,25	*	*	1,25	0,75	0,5
Чад	2,25	2,25	1,5	2,75	*	0,5	*	*	1,5	1,5	0,5
Экваториальная Гвинея	1,75	2	1	1,75	*	0,25	*	*	1	1,25	0,5
Эритрея	1,5	2,25	0,75	1	*	0,5	*	*	0,75	1,25	0
Эсватини	2	2	0,75	1,5	*	0,25	*	*	0,75	1	0
Эфиопия	2,5	3	1,75	2,75	*	1	*	*	2,25	2,25	1,75
ЮАР	2,75	3,5	2,5	3,25	*	1,75	*	*	3,25	2,5	2,75
Южный Судан	1,25	2,25	0,75	1	*	0,25	*	*	1,25	1	0

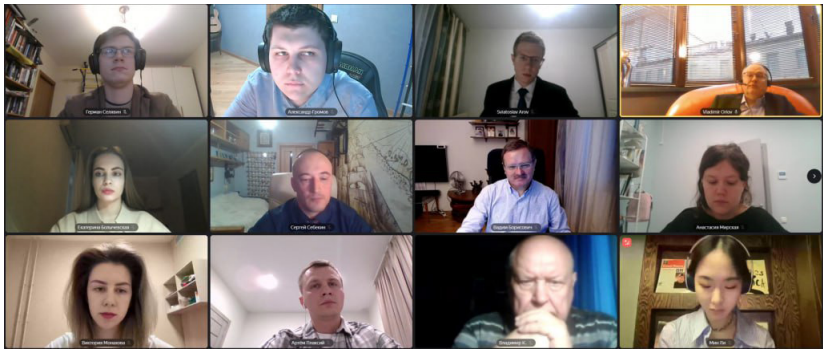
Таблица 2. Сводный показатель влияния внешних партнеров на рынках стран групп *Персидский залив+* и АЮС

Составлено автором

[25] Методология и условные обозначения: вовлеченность оценена по шкале от 1 до 5, где «1» – низкий уровень участия, «5» – высокий уровень участия; «0» – отсутствие участия (по политическим или иным причинам). При выведении показателя учитывалась интенсивность профильного диалога между странами, степень активности бизнеса и научно-экспертного сообщества, вовлеченность страны в реализацию мегапроектов и опыт их успешной реализации; наличие долгосрочных договоренностей (в т.ч. закрепленных документально) и т.д. «*» – страны, не включенные в анализ; «-» – страны из той же группы.

ЗАКЛЮЧЕНИЕ

Государства Персидского залива и Африки южнее Сахары с большим интересом следят за изменениями цифрового мира и стремятся заблаговременно укрепить позиции в передовых областях. Разумеется, между показателями экономического развития государств Персидского залива и Африки южнее Сахары пока нельзя ставить знак равенства – разница социально-политического и экономического ландшафта неизбежно накладывает отпечаток на развитие высокотехнологичных проектов. Ожидаемо отмечен явный *перевес* в сторону аравийских монархий, в прошлом десятилетии направивших значительную часть *нефтегазовых* средств на перестройку и цифровизацию национальных экономических систем, в то время как большинство других стран такой возможности были лишены.



Экспертный семинар ПИР-Центра «*От Залива до Субсахарской Африки*: развитие цифровых технологий и интересы России», 8 ноября 2024 г.

Источник: www.nonproliferation.world

Однако между двумя не похожими, на первый взгляд, регионами есть пересечения: так, их общими чертами стало форсированное наверстывание отставания в *цифровой гонке* (возникшее в силу *позднего старта* подавляющего большинства рассмотренных держав), параллельное развитие сразу всех высокотехнологичных направлений (кибербезопасность, FinTech-рынок, ИИ-технологии и пр.), а также ставка на международное сотрудничество – как основной *двигатель* проектов на национальном и региональном уровне.

В вопросах взаимодействия рассмотренных стран с остальным миром налицо тренд к постепенному переходу *пальмы первенства* в соревновании за влияние в технологическом секторе к азиатским акторам – и, в первую очередь, к Китаю. Это характерно как для стран Персидского залива, так и для региона АЮС. Пекин проявляет стратегическую гибкость, умело комбинируя философские, экономические и технологические инструменты, что позволяет ему плотно сотрудничать даже с государствами, находящимися *за рамками* диалога у западных конкурентов (Иран в регионе Персидского залива, Мали и Нигер в Африке и пр.) и увеличивать *удельный вес* как в государственном, так и в бизнес-сегменте взаимодействия. При этом влияние различных негативных конструктов (*долговая ловушка*, *цифровой неоколониализм* и пр.), присущих деятельности КНР в регионах, пусть и создает препятствия, не слишком снижает интенсивность профильных контактов.

С другой стороны, ожидать быстрой *сдачи позиций* со стороны ключевых западных игроков (США, ЕС) тоже не стоит.

Помимо того, что эти страны имеют достаточное влияние в секторе цифровых технологий, не уступая в репутационном плане азиатским конкурентам, ряд тактических преимуществ (географическое положение, политико-экономическое влияние и пр.) позволяет

Также оспорить лидерство Китая все чаще пытается Индия, которая позиционирует себя в качестве *равноудаленной* силы как от коллективного Запада, так и от Китая, а также страны, отрицающей любые «неоколониальные проявления». Хотя на деле индийская политика в отношении технологических рынков стран Залива и АЮС мало чем отличается от китайской.

Среди других тенденций следует отметить постепенное расширение сотрудничества между странами АЮС и Персидского залива в группе цифровых технологий (*см. диаграмму* 2)[26]. Конечно, в данном случае инициатива исходит, в первую очередь, от аравийских монархий и Ирана – и нацелена на укрепление экономических позиций на Африканском континенте. С другой стороны, растет представленность технологических компаний отдельных стран АЮС (ЮАР, Кения и др.) на рынках стран Персидского залива. И хотя масштабы взаимопроникновения пока несоразмерны, африканские страны постепенно сокращают отставание, что можно расценивать как позитивный тренд.

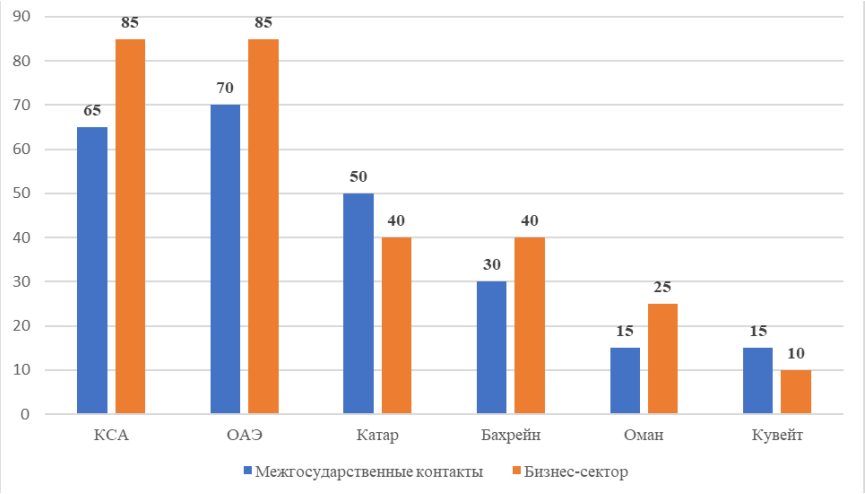


Диаграмма 2. Процент стран региона АЮС, охваченных контактами с аравийскими монархиями (по состоянию на начало 2024 г., %)

Составлено по открытым источникам

Российский опыт реализации передовых цифровых проектов по-прежнему востребован. На волне продолжающейся трансформации системы международных политико-экономических отношений растет вовлеченность России в *цифровые* дела рассмотренных регионов. Москва обладает, в целом, выигрышными позициями и, в отличие от европейских (а также частично, китайских) конкурентов, в меньшей степени подвержена влиянию *колониального дискурса*. Более того, последовательное отстаивание идеи незыблемости *цифрового суверенитета* национальных государств дает России некоторое преимущество в диалоге со странами региона – особенно с теми, кто борется за технологическую и экономическую независимость (Ирак в регионе Персидского залива, Южный Судан и Нигер в Африке), либо находится за рамками общерегионального диалога из-за несовпадения политических позиций с соседями (Иран в регионе Персидского залива, Мали и Буркина-Фасо в Африке).

[26] Категория *межгосударственные контакты* отражает наличие в активе стран хотя бы одного профильного соглашения (включая межведомственные). Категория *бизнес-сектор* отражает представленность активных национальных компаний стран ССАГЗ на рынке АЮС.

Растет значение БРИКС – как потенциальной *точки объединения* стран Персидского залива и АЮС. Не только Россия, но и другие внешние игроки (Китай, Индия) стараются продвигать цифровые инициативы, ориентированные на рассмотренные регионы, с опорой на *общность интересов* в рамках БРИКС.

С другой стороны, специфика цифрового мира неизбежно накладывает негласные ограничения на масштабы взаимодействия – как внутри регионов, так и на глобальном уровне, и это важно учитывать при выстраивании диалога по линии цифровой безопасности и технологий. Особенно в контексте того, что и в АЮС, и в регионе Персидского залива сохраняются *белые пятна* в виде стран, не вовлеченных в продвигаемые регионами цифровые проекты.

В целом, можно ожидать, что Россия продолжит постепенно наращивать присутствие на цифровых рынках двух регионов – в т.ч. на перспективных (FinTech, ИИ-сектор), делая ставку на принципы равенства и открытости диалога. Однако для повышения общей эффективности работы следует уделить большее внимание долгосрочным интересам региональных игроков и нарастить участие в развитии тех отраслей, конкуренция в которых пока находится на относительно низком уровне (сектор технологий в государственном управлении). ■

Индекс Безопасности – Научные записки

№4 (51), 2024

Леонид Цуканов

От Залива до Субсахарской Африки:
развитие цифровых технологий
и интересы России

Главный редактор: В.А. Орлов

Технический редактор: Е.Г. Чобанян

Рецензенты: В.Б. Козюлин, С.А. Себекин,
В.А. Орлов

В оформлении доклада используется фрагмент гравюры Альбрехта Дюрера *Носорог*

Работа над данной научной запиской
завершена 25 ноября 2024 г.

ИНДЕКС БЕЗОПАСНОСТИ

Индекс Безопасности – Научные записки – доклады, аналитические статьи, комментарии и интервью, которые отражают позиции российских и зарубежных экспертов по актуальным вызовам глобальной безопасности и политики России в этой сфере. Задача серии – дать понятный анализ проблем международной безопасности и предложить для них конкретные и реалистичные решения. Серия пришла на смену журналу *Индекс Безопасности*, издаваемому ПИР-Центром в 1994–2016 гг.

Авторы и редакторы серии будут рады комментариям, вопросам и предложениям, которые читатели могут направить на электронную почту inform@pircenter.org.

ПЕРСПЕКТИВЫ И ПОТЕНЦИАЛ СОТРУДНИЧЕСТВА РОССИИ С ГОСУДАРСТВАМИ ПЕРСИДСКОГО ЗАЛИВА В ВОПРОСАХ ГЛОБАЛЬНОЙ БЕЗОПАСНОСТИ И ВЫСОКИХ ТЕХНОЛОГИЙ

Проект *Перспективы и потенциал сотрудничества России с государствами Персидского залива в вопросах глобальной безопасности и высоких технологий* нацелен на совершенствование имеющихся методологических подходов к изучению ситуации в регионе Персидского залива и выработку научно-практических рекомендаций для аналитического сопровождения государственных ведомств и коммерческих организаций, имеющих внешнеполитическую направленность, что должно способствовать наращиванию профильного сотрудничества.

ПЕРСПЕКТИВЫ И ПОТЕНЦИАЛ СОТРУДНИЧЕСТВА РОССИИ С ГОСУДАРСТВАМИ АФРИКИ (ЮЖНЕЕ САХАРЫ) В ВОПРОСАХ ГЛОБАЛЬНОЙ БЕЗОПАСНОСТИ И ВЫСОКИХ ТЕХНОЛОГИЙ

В качестве ключевой задачи данного проекта определено суммирование и актуализация подходов к развитию сотрудничества России с государствами Субсахарской Африки на межгосударственном уровне и в формате бизнес-диалога в различных сегментах сферы high-tech (международная информационная безопасность, энергетика, биотехнологии и др.).