ПИР-Центр – МГИМО МИД России

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

Серия «Доклады ПИР-Центра. № 42»

ПИР-Центр – МГИМО МИД России

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

Аналитическая записка по потенциалу государств Персидского залива и Африки южнее Сахары в области цифровых технологий и по перспективам продвижения интересов России по данной проблематике

Л.В. ЦУКАНОВ

Серия «Доклады ПИР-Центра. № 42»

Москва
2025

Рецензенты:
Козюлин Вадим Борисович, кандидат политических наук, заведующий Центром глобальных исследований и международных организаций Института актуальных международных проблем Дипломатической академии МИД России;
Себекин Сергей Александрович, кандидат политических наук, участник международной группы по исследованию злонамеренного использования искусственного интеллекта и доцент кафедры политологии, истории и регионоведения Иркутского государственного университета

Подготовил:
Цуканов Леонид Вячеславович, кандидат политических наук, консультант (Проекты «Перспективы и потенциал сотрудничества России с государствами Африки в вопросах глобальной безопасности и высоких технологий» и «Перспективы и потенциал сотрудничества России с государствами Персидского залива в вопросах глобальной безопасности и высоких технологий» Блока «Научные исследования и прикладной анализ»), ПИР-Центр

Научный руководитель:
Орлов Владимир Андереевич, директор и основатель, ПИР-Центр; профессор кафедры ПАМП, МГИМО МИД России

Данная аналитическая записка (доклад) 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». Работа по подготовке данной аналитической записки (доклада) завершена в декабре 2024 г.

Данная аналитическая записка (доклад) доступна для скачивания по ссылке:

Информация о проекте ПИР-Центра «Перспективы и потенциал сотрудничества России с государствами Персидского залива в вопросах глобальной безопасности и высоких технологий» представлена на сайте:

Информация о проекте ПИР-Центра «Перспективы и потенциал сотрудничества России с государствами Африки (южнее Сахары) в вопросах глобальной безопасности и высоких технологий» представлена на сайте:

Серия «Доклады ПИР-Центра. № 42»

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Цифровые технологии играют все большую роль в мировой политике и экономике. По мере развития глобального сетевого общества потребность национальных государств в использовании передовых технологических 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 аудит 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.

С целью более эффективного сопоставления показателей держав, 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

[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.

[2] Также по тексту для условного обозначения стран ССАГЗ автором будет использоваться термин «аравийские монархии».

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.

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, PESTLE-анализ и ряд других методов научного познания – включая методы конкурентной разведки.

Доклад выстроен по принципу «геймбука» (*gamebook*), ввиду чего чтение разделов может иметь выборочный характер – для получения обособленного представления о потенциале как государств групп «Персидский залив+», так и стран АЮС[3]. Подобный подход позволяет сделать доклад более универсальным и доступным для широкого круга читателей без необходимости разделения его на два независимых (но имеющих идентичную методологическую основу) исследования.

При этом каждый тематический блок содержит дополнительный раздел с обобщением данных, в котором в формате краткого резюме приводятся основные выводы, а также характеризуются выявленные «точки соприкосновения», характерные для обоих рассмотренных регионов.

[3] Для изучения обстановки в регионе Персидского залива в разрезе цифровых технологий рекомендуется прочесть разделы 1.1, 2.1, 3.1 и Приложения 1 и 3; для изучения обстановки в регионе АЮС – разделы 1.2, 2.2, 3.2 и Приложения 2 и 3.

Раздел 1. Оценка цифрового ландшафта государств регионов Персидского залива и Африки южнее Сахары в разрезе вопросов региональной и глобальной безопасности

1.1. Регион «Персидский залив+»

Кибербезопасность (технико-технологическое измерение)

Государства группы «Персидский залив+», за редким исключением, относятся к категории стран с высоким уровнем цифровой защищенности и технико-технологического развития. Согласно данным «Глобального индекса кибербезопасности», составленного экспертами Международного союза электросвязи (МСЭ) при ООН, по меньшей мере три государства группы (Саудовская Аравия, ОАЭ, Катар) занимают лидирующие позиции не только на региональном (ТОП-5), но и глобальном уровнях и имеют показатели «абсолютной киберготовности» по версии МСЭ. Еще две державы – Бахрейн и Оман – входят в глобальный ТОП-50 (17 и 21 места соответственно)[4].

Следует отметить, что для государств группы «Персидский залив+» характерна некоторая неоднородность показателей уровня защищенности критической информационной инфраструктуры (КИИ) – это справедливо и по отношению к ССАГЗ, где в течение последнего десятилетия ведется работа по формированию совместных механизмов киберзащиты.

Так, несмотря на то что во всех аравийских монархиях к настоящему моменту созданы общенациональные Группы реагирования на компьютерные инциденты[5], модернизация системы реагирования и предупреждения 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[6].

Другая характерная черта цифрового пространства рассматриваемого региона – наличие самостоятельных полюсов кибербезопасности (Иран), отчасти конфронтирующих с другими передовыми государствами рассматриваемой группы (Саудовская Аравия, ОАЭ). Даже с учетом ирано-саудовской «разрядки» (2023 г.)[7] и попыток нормализации отношений Тегерана с другими аравийскими монархиями (например, с Бахрейном[8]), Иран по-

[4] 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
[5] Посчитано по: CERT-In. URL: https://www.cert-in.org.in/s2cMainServlet?pageid=ADWCERTVIEW
[6] Там же.
[7] Китайская переменная для «уравнения безопасности» на Ближнем Востоке // ПИР-Центр. 24.03.2023. URL: https://pircenter.org/editions/kitajskaja-peremennaja-dlja-uravnenija-bezopasnosti-na-blizhnem-vostoke/
[8] Ключевой форпост США в Персидском заливе приступил к примирению с Ираном // Regnum. 09.09.2024. URL: https://regnum.ru/article/3914811

прежнему воспринимается как источник комплексной угрозы, которая распространяется в том числе и на киберпространство. Это, вкупе с сохраняющимся санкционным режимом, препятствует интеграции Тегерана в систему цифрового сотрудничества региона – хотя Исламская Республика и оказывает серьезное влияние на вектор развития рынка кибербезопасности на Ближнем Востоке.

Важную роль в своевременной модернизации систем технико-технологической защиты играет международное сотрудничество. Ставку на развитие внешних контактов (как на межгосударственном уровне, так и по линии бизнеса) сделали все без исключения государства группы «Персидский залив+»[9]. Активизация контактов придает позитивный импульс развитию сектора высоких технологий региона, а также позволяет более эффективно бороться с глобальными угрозами из киберпространства.

Не секрет, что вопросы обеспечения кибербезопасности довольно тесно связаны с военным сектором. Тем более, что объекты критической инфраструктуры государств-оппонентов являются желанной целью как для регулярных подразделений (т.н. «киберармии»), так и для внесистемных игроков (хакерские преступные сообщества, радикально-экстремистские группировки).

Для стран региона «Персидский залив+» (как и для Ближнего Востока в целом) характерен упор на развитие системы киберподразделений и их использование для решения военно-политических задач. По состоянию на 2024 г., известно о наличии таких подразделений как минимум у четырех держав группы (Саудовская Аравия, ОАЭ, Иран, Катар), факт наличия профильных подразделений у Бахрейна и Омана оспаривается официальными властями.

Более подробно следует остановиться на иранской модели формирования киберсил, где, помимо официальных киберподразделений, «актив» страны составляют многочисленные хакерские команды и прокси-кибергруппировки (в том числе созданные из граждан лояльных Тегерану стран)[10].

Наличие подобных подразделений долгое время служило сдерживающим фактором развития напряженности на Ближнем Востоке – особенно в контексте ирано-саудовско-эмиратского противостояния – и частота применения «киберармий» в регионе Персидского залива в последние несколько лет постепенно шла на спад.

С другой стороны, эскалация напряженности в секторе Газа (включая активность киберподразделений ХАМАС на начальных этапах конфликта) сформировали убежденность об участии иранских киберподразделений в конфликте под «ложным флагом»[11], что негативно сказалось на уровне доверия между государствами региона, а также подтолкнуло аравийские монархии к совершенствованию модели кибероборонды.

Стоит также кратко упомянуть феномен кибертерроризма. Несмотря на то, что возможность радикально-экстремистских группировок и движений в киберпространстве

[9] Подробнее об основных направлениях сотрудничества с внешними партнерами см. Раздел 3.
[10] Проиранские хакеры: «пояс безопасности» Тегерана? // РСМД. 04.07.2022. URL: https://russiancouncil.ru/analytics-and-comments/analytics/proiranskie-khakery-poyas-bezopasnosti-tegerana/
[11] «Цифровой шторм» Аль-Акса: штрихи к противостоянию Израиля и ХАМАС // РСМД. 18.01.2024. URL: https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/tsifrovoy-shtorm-al-aksa-shtrikhi-k-protivostoyaniyu-izrailya-i-khamas/

существенно ограничены – а сами радикалы предпочитают использовать Интернет как площадку пропаганды и априори не могут нанести серьезный ущерб КИИ крупных и технологически развитых держав[12] – все без исключения государства группы «Персидский залив+» включают его в группу основополагающих угроз, что отражено в национальных стратегиях[13].

Социальное измерение цифровой безопасности

Поскольку неотъемлемой частью цифрового мира является человек, обеспечение стабильности социального измерения цифровой безопасности имеет не меньшую важность, чем физическая защита КИИ.

Данное направление включает защиту общества от деструктивного информационного воздействия извне, нацеленного на подрыв социальной стабильности и международного авторитета государства, а также противодействие использованию ИКТ в качестве инструмента вмешательства во внутренние дела суверенных государств, разжигания межэтнической и межконфессиональной розни.

Кроме того, в социальное измерение цифровой безопасности нередко включают вопросы, связанные с совершенствованием элементов системы безопасности (включая развитие кадрового и человеческого потенциала, отдельные аспекты совершенствования управленческих и законотворческих компетенций).

Характеризуя состояние систем цифровой защиты государств группы «Персидский залив+» с точки зрения социальной составляющей, следует отметить растущее внимание к совершенствованию национальных кадров, занятых в цифровом секторе. К 2024 г. все без исключения акторы запустили программы непрерывного развития компетенций, направленные на отбор и ведение перспективных для отрасли специалистов со старшего (в случае с Бахрейном и ОАЭ – среднего) школьного звена, развитие академической мобильности, бизнес-стажировок. Это не только позволяет увеличить число занятых в отрасли специалистов, поднимая ее престиж, но и формирует дополнительный ресурс для решения задач по контролю и развитию национальных систем цифровой защиты.

Некоторые позитивные подвижки отмечены и в нормативно-правовом секторе, однако здесь по-прежнему сохраняется большое количество лакун, препятствующих эффективному развитию профильного законодательства.

Так, уязвимым местом всех рассмотренных держав является защита личности в Интернете. Такие категории преступлений как «кибербуллинг», «вымогательство в социальных сетях или иные действия, причиняющие личный вред», «действия в цифровом пространстве, связанные с расизмом или ксенофобией», а также «отрицание или оправдание геноцида или

[12] 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

[13] Выявлено на основе анализа национальных стратегий национальной безопасности и кибербезопасности, а также документов военного планирования государств группы «Персидский залив+». См., напр.: National Security Strategy // TRDA. URL: https://tdra.gov.ae/userfiles/assets/vzjmlB3CM34.pdf; Qatar National Cyber Security Strategy (2014). URL: https://nsarchive.gwu.edu/sites/default/files/documents/3903662/Qatari-Government-Qatar-National-Cyber-Security.pdf и др.

преступлений против человечности с использованием цифрового пространства» представлены в НПА стран региона в сравнительно обтекаемых формулировках (и, зачастую, не имеют конкретизации)[14].

Аналогичная проблема прослеживается и на более высоком уровне: ни в Арабской конвенции о борьбе с преступлениями в области информационных технологий (2010 г.)[15], являющейся на данный момент единственным «общим знаменателем» профильного законодательства арабских стран, ни в других коллективных проектах нет *рецепта реагирования* на социальные угрозы в цифровом пространстве.

Налицо и проблема сохранения свободы слова в Интернете. В ряде стран (Бахрейн, Катар, Кувейт) существуют специфические НПА, причисляющие критику действий властей с использованием социальных сетей к категории киберпреступлений[16], что делает цифровые технологии инструментом косвенного давления на оппозицию и, по оценкам экспертов МСЭ, тормозит процесс формирования цифрового гражданского общества.

Однако, несмотря на перечисленные препятствия, процесс развития социальной составляющей цифровой защиты имеет позитивный вектор.

Цифровые технологии в экономике и управлении

Страны Персидского залива делают значительную ставку на развитие цифровых экономических инструментов и внедрение финансовых технологий (FinTech). Пандемия COVID-19 способствовала ускоренному переходу к удаленным формам деятельности, что позитивно сказалось на сегменте цифровых услуг и привело к росту числа FinTech-компаний почти во всех рассмотренных странах. Форсируется работа по развитию международного сотрудничества, что придает отрасли дополнительные стимулы к развитию.

Отдельные государства региона также сделали ставку на запуск специализированных проектов, призванных упростить взаимодействие государства и бизнеса в области финансовых технологий. В их числе, например, *Qatar FinTech Hub* (Катар, 2018 г.)[17], *Fintech-песочница* (Кувейт, 2018 г.)[18], Трансграничная цифровая инновационная платформа *FinHub* (Бахрейн, 2020 г.)[19] и др.

Особо следует коснуться вопроса добычи (*майнинга*) крипотовалюты в рассматриваемых странах. Несмотря на существенные подвижки в вопросах обращения с цифровыми

[14] Arab Laws Online Database. URL: https://www.arablawsworld.com/
[15]Arab Convention on Combating Information Technology Offences // League of Arab States, 2010. URL: https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf
[16] Internet Organizations Fostering Internet Governance & Digital Infrastructure In The Arab States // MENA FN. 06.09.2022. URL: https://menafn.com/1104350565/Internet-Organisations-Fostering-Internet-Governance-Digital-Infrastructure-In-The-Arab-States
[17] Qatar has ‘global appeal’ as hub for fintech growth, says QDB executive // Gulf Times. 24.07.2023. URL: https://www.gulf-times.com/article/665072/business/qatar-has-global-appeal-as-hub-for-fintech-growth-says-qdb-executive
[18] Kuwait stands at the dawn of a new digital banking era // The Banker. 25.03.2022. URL: https://www.thebanker.com/Kuwait-stands-at-the-dawn-of-a-new-digital-banking-era-1648197117
[19] FinTech & Innovation // Central Bank of Bahrain. URL: https://www.cbb.gov.bh/fintech/

активами в последние годы, большинство стран группы «Персидский залив+» по-прежнему находятся на догоняющих позициях. По оценкам международной консалтинговой компании Henley & Partners, в ТОП-25 мировых лидеров по совокупному показателю принятия криптовалют входит только одна страна рассмотренной группы – ОАЭ (3 место). При этом высокие позиции Абу-Даби обусловлены привлекательным экономическим ландшафтом страны (4 место по критерию), общественным консенсусом по вопросу применения и развития криптовалютных активов (2 место по критерию), а также комплексным стремлением к внедрению инноваций в экономику (4 место по критерию).

При этом по степени развитости профильной нормативно-правовой базы (17 место) и профильной инфраструктуры (15 место) страна заметно проигрывает как европейским, так и азиатским конкурентам[20].

Используя методологию и критерии оценки Henley & Partners, можно выстроить градацию совокупного показателя принятия криптовалют для группы «Персидский залив+» *(см. диаграмму 1).*

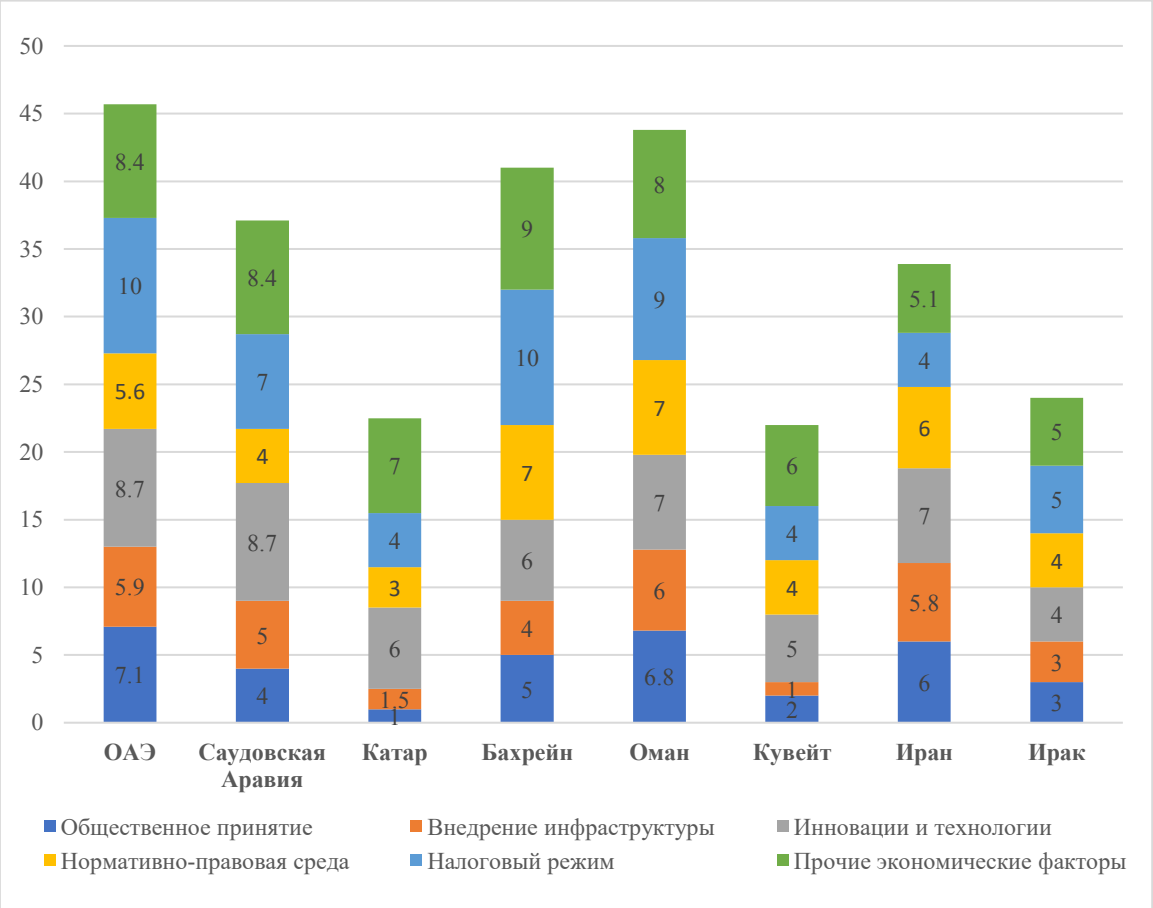

Диаграмма 1. Совокупный показатель принятия криптовалют в государствах региона (максимальный балл по каждому критерию – 10). Составлено автором на основе методологии Henley & Partners[21].

Как видно из приведенных выше данных, отношение к криптовалютам в регионе по-прежнему неоднозначное: встречаются как ярые сторонники (ОАЭ, Оман), так и

[20] The Crypto Wealth Report // Henley & Partners. URL: https://www.henleyglobal.com/publications/crypto-wealth-report/crypto-adoption-index
[21] Ibidem.

противники (Катар[22], Кувейт). Также в отдельных случаях эффективному развитию криптовалютных проектов, при отсутствии строгого запрета на их оборот, препятствуют разногласия между государственными институтами и гражданским обществом, а также духовно-нравственные установки (Саудовская Аравия, Ирак).

Другой общей проблемой является развитие профильной инфраструктуры (создание майнинговых центров, обеспечение их энергией и оборудованием и пр.) – помимо ОАЭ, продвинуться в этом направлении смогли только Оман и Иран. При этом, с точки зрения экономического потенциала и темпов совершенствования нормативно-правовой среды акторы группы «Персидский залив+» сохраняют позитивный вектор развития.

Определенный интерес представляют усилия государств группы «Персидский залив+» по развитию системы электронных правительств (так называемые «EGov») – как способа взаимодействия на основе использования ИКТ в целях повышения эффективности предоставления государственных услуг.

Работа над развитием систем «EGov» стартовала в регионе с началом 2010-х гг., хотя отдельные попытки развивать экосистему государственных сервисов предпринимались отдельными аравийскими монархиями еще в 2003 г.[23]. С принятием программ стратегического развития «Vision» эта деятельность приобрела системный характер, что обусловило быстрое формирование в государствах ССАГЗ многоступенчатой системы управления госсервисами. Технологический прорыв также позволил делиться профильными наработками с другими странами Арабского мира (в том числе с Ираком).

Сегодня аравийские монархии продолжают выделять существенные средства на модернизацию систем «EGov»: в ряде стран (ОАЭ, Саудовская Аравия) с момента начала работ сменилось уже четыре «поколения» электронного правительства.

Специальные меры поддержки, направленные на стимулирование работы над дальнейшим развитием EGov-систем, запущены и на уровне ССАГЗ. Одной из них можно считать Премию ССАГЗ в области электронного правительства, на ежегодной основе вручаемую государственным органам стран – членов объединения, показавшим наибольшую эффективность в развитии цифровых сервисов[24].

Отдельно следует сказать об иранском подходе к развитию системы электронных госсервисов. В отличие от арабских стран, где работа по встраиванию государственных организаций в систему электронных услуг находится в ведении министерств связи и цифрового развития, координация процессов в Иране ведется на более высоком уровне.

---

[22] В сентябре 2024 г. Катар объявил о незначительной либерализации законодательства по отношению к криптовалютам. Национальные регуляторы — Управление финансового центра Катара и Управление регулирования финансового центра Катара — объявили о нормативных базах, которые создают основу для регулирования цифровых активов в стране. В основу формата положен опыт ОАЭ. При этом о полноценной реабилитации криптоактивов речи пока не идет, проект находится в стадии технической обкатки. См.: Катар вводит нормативную базу для цифровых активов // Bitget. 03.09.2024. URL: https://www.bitget.com/ru/news/detail/12560604187636

[23] Один из примеров – система государственного управления услугами (2003 г.), разработанная в Саудовской Аравии. В дальнейшем наработки первого поколения были положены в основу информационной экосистемы «Yesser». См.: Yesser // Government of Saudi Arabia. URL: http://www.yesser.gov.sa/en/Pages/default.aspx

[24] About the GCC eGovernment Award // GCC. URL: https://gccegov.org/en/Award/About

Профильный функционал возложен на Центр прогресса и развития при президенте ИРИ, который занимает обособленное положение в иерархии государственных органов страны[25]. Есть определенные различия и в обозначении приоритетов развития данного направления в сравнении с другими государствами региона. Помимо стремления сократить бюрократию и повысить качество предоставляемых административных услуг, Тегеран нацелен на внедрение универсальных метрик оценки эффективности функционирования государственных институтов, а также на «создание условий для качественных прорывов в различных секторах экономики»[26]. Иными словами, Иран рассматривает EGov-систему не только как способ повысить эффективность работы госорганов, но и как драйвер комплексного развития и трансформации национальной цифровой экономики.

При этом процесс формирования системы «цифрового правительства» в Иране по-прежнему не завершен – хотя к середине 2024 г. цифровые инструменты при работе с населением на постоянной основе используют не менее 2/3 государственных институтов ИРИ. «Замыканию» экосистемы госсервисов препятствуют как внешние (санкционный режим), так и внутренние (например, нормативно-правовые разногласия) факторы.

Однако, в свете прихода к власти в Иране правительства реформистов во главе с Масудом Пезешкианом, чья предвыборная программа была построена на идее «экономической перезагрузки», можно ожидать, что Тегеран в ближайшие годы существенно нарастит работу по развитию цифровых сервисов.

Важно отметить, что во всех рассмотренных государствах, в соответствии с рекомендациями МСЭ, к настоящему моменту разработаны критерии оценки эффективности функционирования сервисов «EGov». Однако, в силу разных подходов к отбору данных и различающейся периодичности их оценки, сопоставление национальных отчетов в их исходном виде может повлечь за собой некоторые искажения.

При этом наиболее объективно динамику развития сектора «EGov» (как на национальном, так и на региональном уровне) отражает Индекс развития электронного правительства (*E-Government Development Index, EGDI*), который составляется раз в два года Департаментом экономического и социального развития ООН. Индекс состоит из трех «корзин», характеризующих состояние ИКТ-инфраструктуры, человеческого капитала и онлайновых государственных услуг.

Согласно последним замерам *EGDI*, в глобальном ТОП-50 остаются три страны группы «Персидский залив+» – ОАЭ (13 место), Саудовская Аравия (31 место) и Оман (50 место). Качественный рост по сравнению с предыдущими замерами продолжили демонстрировать только Эр-Рияд и Абу-Даби, остальные ухудшили позиции (*см. Таблицу 1*). При этом все рассмотренные государства (за исключением Ирака) преодолевают пороговый глобальный показатель, выведенный в рамках отчета (0.6102), что говорит о сохранении условий для дальнейших комплексных трансформаций.

[25] Digital Government // Center for Progress and Development. URL: http://en.cpdi.ir/Digital-Government
[26] Ibidem.

№	Страна	Место в глобальном рейтинге	Индекс
1	ОАЭ	**13 (+8)**	0.9010
2	Саудовская Аравия	**31 (+12)**	0.8539
3	Оман	**50 (0)**	0.7834
4	Бахрейн	**54 (-16)**	0.7707
5	Кувейт	**61 (-15)**	0.7484
6	Катар	**78 (-12)**	0.7149
7	Иран	**91 (-2)**	0.6454
8	Ирак	**146 (-3)**	0.4383

Таблица 1. Индекс развития электронного правительства для стран группы «Персидский залив+». Составлено по: E-Government Development Index[27].

Общей проблемой для рассмотренных стран является запутанность системы государственных услуг. Несмотря на масштабные реформы государственных институтов во второй половине 2010-х гг., добиться синхронности их функционирования пока не удалось. Также как минимум в двух государствах (Кувейт, Катар) все еще сохраняется дублирующий функционал у части министерств и ведомств, включенных в систему, что усложняет получение услуг.

Также в Ираке в качестве деструктивного фактора следует выделить проблемы с обеспечением бесперебойной работы цифровых сервисов. Хотя официальному Багдаду и удалось за прошедшие 5 лет повысить уровень проникновения Интернета до 98%[28], а также увеличить общую скорость передачи данных за счет создания инфраструктуры 3G и 4G, процент пользователей EGov-сервисов в этой стране по-прежнему кратно меньше, чем в аравийских монархиях и в Иране[29].

Применение технологий искусственного интеллекта

Технологии искусственного интеллекта (также ИИ-технологии) – это сравнительное новое явление для стран Ближнего Востока, одна его освоение и внедрение в производственные процессы идет стремительными темпами. Прогнозируемый объем инвестиций в отрасль постоянно растет.

Так, согласно оценкам *PwC*, к 2030 г. на Ближний Восток будет приходиться около 320 млн долларов – то есть порядка 2% от общего объема глобальных инвестиций в сектор ИИ[30]. При этом эксперты полагают, что глобальная ИИ-индустрия к 2030 г. преодолеет отметку в 15,7 трлн долларов[31].

Наибольшее внимание к развитию технологий искусственного интеллекта сегодня проявляют ОАЭ и Саудовская Аравия.

---

[27] 2024 E-Government Development Index // UN E-Government Knowledgebase. URL: https://publicadministration.un.org/egovkb/en-us/Data-Center

[28] Digital & Connectivity Indicators – Iraq // Statista. URL: https://fr.statista.com/outlook/co/digital-connectivity-indicators/iraq#:~:text=The%20Internet%20penetration%20in%20Iraq,to%206.17m%20in%202024

[29] 2024 E-Government Development Index // UN E-Government Knowledgebase. URL: https://publicadministration.un.org/egovkb/en-us/Data-Center

[30] 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

[31] Ibidem.

При этом ОАЭ позиционирует себя как «пионера» в вопросах внедрения ИИ во все сферы жизни. В 2021 г. Кабмин принял «Национальную стратегию в области развития искусственного интеллекта до 2031 года»[32], ставшую первым публичным документом подобного рода не только в регионе Персидского залива, но и на Ближнем Востоке в целом (хотя вопросы развития ИИ-технологий так или иначе затрагивались в документах стратегического планирования почти всех аравийских монархий). При этом Стратегия стала логическим продолжением программы долгосрочной экономической трансформации «Столетие ОАЭ» (*UAE Centennial 2071*), которая направлена на совершенствование и использование передовых инноваций в девяти сегментах, включая транспорт, здравоохранение, космос, устойчивую энергетику, водные ресурсы, инновации, образование, окружающую среду и транспорт[33].

Кроме того, в ОАЭ с 2017 г. работает Министерство искусственного интеллекта, основной задачей которого является направление ресурсов на передовые инновации и инструменты ИИ, которые будут применяться во всех сферах деятельности государства. Министерство дополнительно уполномочено работать с Министерством образования и Министерством высшего образования и научных исследований для включения ИИ в качестве основного аспекта национального образовательного плана, обучения и подготовки людей к работе в будущем[34].

При этом в вопросах освоения сферы искусственного интеллекта Абу-Даби с годами все больше наступает на пятки Эр-Рияд. Саудовская Аравия полноценно включилась в гонку в 2019 г. – с созданием Управления по данным и искусственному интеллекту[35]. Также Королевство с минимальным отрывом от ОАЭ разработало Национальную стратегию в области искусственного интеллекта и больших данных[36] – за тем лишь исключением, что Эр-Рияд выбрал более короткую дистанцию и установил в качестве ориентира для достижения поставленных в Стратегии целей 2030 г.

Кроме того, Саудовская Аравия борется за статус крупнейшего инвестора в сектор ИИ. Правительство страны еще в марте 2024 г. обсуждало возможность выделить 40 млн долларов на инвестирование в развивающийся сектор[37]. Саудовские чиновники параллельно прорабатывали вопрос создания технологических стартапов в стране – в том числе ориентированных на сферу ИИ[38].

Другие аравийские монархии также развивают компетенции в сфере искусственного интеллекта, однако пока не демонстрируют столь же комплексного подхода к освоению данной сферы – как это делают Абу-Даби и Эр-Рияд.

---

[32] UAE National Strategy for Artificial Intelligence 2031 // the UAE Government. URL: https://ai.gov.ae/strategy/
[33] UAE Centennial Plan 2071 // UAE Cabinet. URL: https://uaecabinet.ae/en/uae-centennial-plan-2071
[34] UAE National Strategy for Artificial Intelligence 2031 // the UAE Government. URL: https://ai.gov.ae/strategy/
[35] Королевство является одной из первых стран в мире, разработавших национальную стратегию в области искусственного интеллекта согласно Стэнфордскому международному индексу 2024 // Saudi Press Agency. 17.04.2024. URL: https://www.spa.gov.sa/ru/N2085583
[36] Де-факто документ был разработан еще в 2020 г., однако до середины 2021 г. существовал в формате драфта (на официальных ресурсах КСА публиковались лишь отдельные выдержки из него), и был обнародован только после публикации аналогичной стратегии ОАЭ. См.: NSDAI. URL: https://ai.sa/
[37] Саудовская Аравия планирует вложить $40 млрд в развитие искусственного интеллекта // ИТАР-ТАСС. 20.03.2024. URL: https://tass.ru/ekonomika/20290675
[38] Там же.

Интерес к соответствующим технологиям проявляет Ирак. Начиная с 2021 г. правительство страны работает над масштабной программой интеграции новых технологий в экономику и рассматривает сектор ИИ как «точку встречи» всех высокотехнологичных отраслей. В этом смысле Багдад опирается в том числе на предложения доктора Диаа аль-Джумайли, который считается одним из *пионеров* иракской школы ИИ-исследований[39].

Интересной чертой иракского подхода к разработке стратегии обращения с ИИ-технологиями, можно считать значительную опору на «исторический и культурный опыт» страны. Так, в проекте национальной ИИ-стратегии отправной точкой развития служит «Дом мудрости» — исламская академия, основанная в IX веке халифом аль-Мамуном в Багдаде и являвшаяся культурным и научным центром Древнего Востока (в иракской стратегии он маркирован как *Индустрия 0.0*, *см. рис.1*)[40].

Рис. 1. Визуализация стратегического подхода правительства Ирака к развитию технологий искусственного интеллекта и новых индустрий. Источник: Iraqi National Strategy for Artificial Intelligence[41].

Официальный Багдад стремится улучшить свою экономику за счет интеграции ИИ в сектор здравоохранения для повышения качества диагностики лечения; в ТЭК в рамках стратегии повышения эффективности нефтегазодобычи. Также в числе приоритетов – внедрение методов точного земледелия и развитие туризма с помощью инноваций на основе ИИ[42].

Разумеется, сфера искусственного интеллекта требует значительных ассигнований, что создает серьезную нагрузку на бюджет страны и ограничивает возможности Багдада при реализации крупных проектов. Однако данная проблема отчасти компенсируется активизацией профильного международного сотрудничества (включая международного государственно-частное партнерство). Так, например, при участии иностранных партнеров в Ираке в 2022 г. был открыт первый ИИ-хаб *AI Dojo*, ориентированный на поиск решений по внедрению передовых технологий в цифровую экономику страны[43].

[39] Правительство Ирака заинтересовано в развитии искусственного интеллекта // Красная весна. https://rossaprimavera.ru/news/acd68134
[40] Iraqi National Strategy for Artificial Intelligence // INSAI. URL: https://iraqi.ai/
[41] Ibidem.
[42] Ibidem.
[43] The First Artificial Intelligence Hub in Iraq // AI Dojo. URL: https://aidojo.co/about

Кроме того, импульс к развитию получили программы по развитию международной академической мобильности в сфере искусственного интеллекта, что также позитивно сказалось на развитии национального сектора. Например, на базе Среднего технического университета Багдада были проведены (совместно с австралийскими и европейскими учеными) эксперименты по обучению искусственного интеллекта приемам врачебной диагностики по цвету языка пациента[44]. Ожидается, что эти технологии будут постепенно интегрированы в систему здравоохранения Ирака, что позволит несколько снизить нагрузку на медицинский персонал.

Параллельно с этим Ирак стремится освоить нишу «страны-хозяйки» профильных мероприятий, составив конкуренцию другим игрокам. Например, иракское правительство в 2024 г. провело первую в истории страны международную конференцию-выставку по искусственному интеллекту[45]. Багдад планирует и дальше развивать этот формат и принимать международные мероприятия наравне с аравийскими монархиями.

Работу государств группы «Персидский залив+» по отношению к искусственному интеллекту уместно оценить и через призму Индекса ответственного применения искусственного интеллекта (*The Global Index on Responsible AI, GIRAI*) – исследовательского мегапроекта, призванного оценить эффективность работы государственных и частных акторов над комплексным развитием ИИ через техническую, социальную и политическую призму.

Обращение к показателям *GIRAI* полезно в том числе в контексте выявления как сильных, так и слабых мест национальных подходов к развитию данной инновационной сферы (*см. Таблицу 2*).

Приведенный совокупный индекс подчеркивает лидерство ОАЭ и Саудовской Аравии, однако в то же время позволяет заключить, что оно не является безоговорочным.

Например, Абу-Даби и Эр-Рияду заметно оппонирует Доха: Катар при более позднем (с учетом влияния последствий Дипломатического кризиса 2017-2021 гг.) старте демонстрирует более высокие показатели по ряду критериев – например, по уровню адаптированности национального законодательства и формированию специализированного правового режима – а по итоговому индексу даже несколько опережает саудитов. Это позволяет предположить, что соперничество за лидерство в отрасли между этими тремя аравийскими монархиями в дальнейшем будет только нарастать.

---

[44] Иракские ученые научили ИИ выявлять болезни по цвету языка // RTVI. 13.08.2024. URL: https://rtvi.com/news/irakskie-uchenye-nauchili-ii-vyyavlyat-bolezni-po-czvetu-yazyka/

[45] В Ираке стартовала первая конференция по искусственному интеллекту // WAM. 03.06.2024. URL: https://www.wam.ae/ru/article/13y4vaz-%D0%BF%D0%B5%D1%80%D0%B2%D0%B0%D1%8F-%D0%B8%D1%80%D0%B0%D0%BA%D0%B5-%D0%BA%D0%BE%D0%BD%D1%84%D0%B5%D1%80%D0%B5%D0%BD%D1%86%D0%B8%D1%8F-%D0%B8%D1%81%D0%BA%D1%83%D1%81%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D0%BE%D0%BC%D1%83-%D0%B8%D0%BD%D1%82%D0%B5%D0%BB%D0%BB%D0%B5%D0%BA%D1%82%D1%83

СТРАНА	ИНДЕКС						
		Законодательные рамки	Действия правительства	Роль негосударственных субъектов	Права человека и ИИ-технологии	Ответственные возможности ИИ	Ответственное управление ИИ
ОАЭ	44.66	46.40	55.62	19.24	40.58	51.15	45.66
Катар	29.84	27.91	38.33	16.72	42.66	37.10	17.44
Саудовская Аравия	28.95	25.60	42.87	7.81	26.28	38.96	27.69
Кувейт	19.11	0.00	35.79	23.99	23.39	18.92	15.85
Оман	14.8	23.54	13.03	0.86	13.85	16.06	15.12
Бахрейн	8.71	9.67	10.96	2.30	9.37	17.84	5.15
Иран	10.39	15.58	12.33	1	5.44	20.88	7.09
Ирак	5.34	1.57	10	2.37	8	7.33	3.81

Таблица 2. Индекс ответственного применения искусственного интеллекта. Составлено по: GIRAI[46].

Методология. Индекс оценивает обязательства правительств и потенциал стран в отношении ответственного развития ИИ через техническую, социальную и политическую призму. Индекс измеряет 19 тематических областей ответственного ИИ в трех измерениях. В каждой тематической области оценивается эффективность различных столпов ответственной экосистемы ИИ. Основные категории – законодательные рамки (состояние нормативно-правовой системы и наличие НПА, регламентирующих работу с ИИ); действия правительства (эффективность и системность государственной политики в области ИИ-технологий); роль негосударственных акторов (вклад частных структур и бизнеса в развитие ИИ-сектора); соблюдение прав человека в разрезе применения ИИ-технологий; ответственные возможности ИИ и ответственное управлении ИИ. Каждая тематическая область была оценена по каждому компоненту, масштабирована до диапазона от 0 до 100.

[46] The Global Index on Responsible AI (2024). URL: https://girai-report-2024-corrected-edition.tiiny.site/

Весьма специфически складывается ситуация в случае с Кувейтом, где вопрос обращения с ИИ законодательно не проработан и регулируется совокупностью имеющихся НПА (наименьший показатель среди рассмотренных стран). С другой стороны, Эль-Кувейт обладает наиболее высоким индексом вовлеченности негосударственных субъектов, что указывает на хорошие перспективы превращения страны в технологический бизнес-хаб.

Важно помнить, что искусственный интеллект может эффективно применяться для решения задач не только в гражданском, но и в военном секторе. Прежде всего речь идет о возможности внедрения в систему управления смертоносными автономными системами (САС) бот-программ с генеративным искусственным интеллектом, которые в режиме реального времени способны анализировать боевой потенциал выявляемых угроз и моделировать способы противодействия им. По мнению разработчиков, это позволяет существенно сократить количество тактических ошибок, обусловленных влиянием человеческого фактора, а также повысить общую эффективность применения передовых ударных средств[47].

Концепция *искусственного советника* также продвигается западными технологическими концернами (в первую очередь, американской «*Palantir Technologies*», специализирующейся на технологиях киберразведки и безопасности данных) и позиционируется как закономерный элемент развития национальных систем обороны, а отдельные решения напрямую тестируются на Ближнем Востоке[48].

В силу специфики данного сектора технологий информация о нем в открытых источниках представлена в крайне усеченном формате, а приводимые статистические данные, с высокой долей вероятности, искажены – во избежание неконтролируемых утечек чувствительной информации. Однако, с учетом трендов регионального развития, «гонка ИИ-вооружений» на Ближнем Востоке – и, в первую очередь, среди государств «Персидский залив+», где форсируется процесс милитаризации и обновления национальных арсеналов[49] – в ближайшие годы будет только нарастать.

Национальные разработки в области ПО

Государства группы «Персидский залив+» по-прежнему в большей степени склонны к покупке готовых технологических решений вместо их разработки, что объясняет преобладание зарубежных компаний[50] в секторе разработки программного обеспечения (ПО) по сравнению с национальными предприятиями (*см. диаграмму 2*) – хотя в большинстве стран и созданы условия для самостоятельного производства ПО.

[47] Чирко А. Бот-генерал: чем грозит боевое применение нейросетей // Россия в глобальной политике. 26.07.2023. URL: https://globalaffairs.ru/articles/bot-general/

[48] How AI is Redefining Middle Eastern Warfare // The National Interest. 09.05.2024. URL: https://nationalinterest.org/blog/techland/how-ai-redefining-middle-eastern-warfare-210960

[49] 2024 Military Strength Ranking // GFP. URL: https://www.globalfirepower.com/countries-listing.php

[50] В случае с Ираном в категории «зарубежные» учтены как официальные контакты, так и задокументированные случаи заказа профильного ПО через третьи страны.

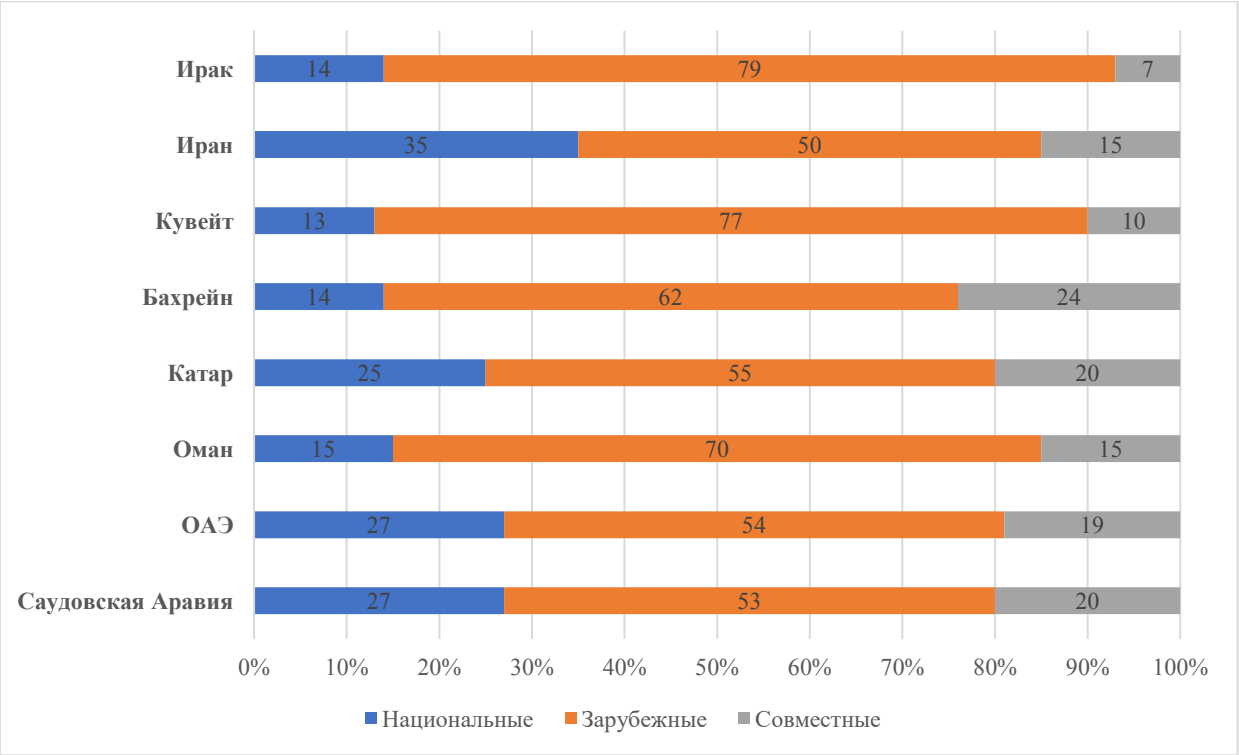

Диаграмма 2. Примерное соотношение национальных и зарубежных компаний в секторе разработки ПО в государствах региона (по состоянию на середину 2024 г.), %. Составлено и посчитано по открытым источникам.

Позитивным трендом последних лет можно считать стремление государств региона к созданию совместных IT-компаний, специализирующихся на разработке ПО. Подобный гибкий подход позволяет решить сразу несколько проблем. Во-первых, частично купировать проблему «утечки мозгов» из национального IT-сектора (которая одинаково остро стоит перед всеми без исключения рассмотренными странами), обеспечив специалистам работу в международных компаниях с конкурентной зарплатой. Во-вторых, активизация сотрудничества между фирмами создает хороший задел для развития государственно-частного партнерства и запуска масштабных технологических проектов.

Еще одним позитивным веянием можно считать первые попытки создания совместных фирм странами-соседями по региону. Так, например, к середине 2024 г. соответствующая работа уже проводилась в «двойках» Саудовская Аравия – ОАЭ; ОАЭ – Бахрейн; Саудовская Аравия – Оман и Ирак – ОАЭ[51]. Создание совместных фирм позволяет в том числе повысить уровень доверия между странами региона и ведет к постепенному снижению межнациональной напряженности и подозрительности.

Отметим, что наибольшая доля собственных компаний, специализирующихся на создании ПО, приходится на Иран, где жесткий внешний санкционный режим способствовал бурному развитию технологических стартапов и формированию технологического рынка, замкнутого на внутренние нужды. Аналоги зарубежных приложений (включая финансовые инструменты), разработанные в Исламской Республике, заняли большую часть внутреннего рынка, и данный сектор продолжает демонстрировать тенденцию к росту[52].

[51] Middle East Siftware Companies // Crunchbase. URL: https://www.crunchbase.com/hub/middle-east-software-companies
[52] FinTech Startups in Iran // Tracxn. URL: https://tracxn.com/explore/FinTech-Startups-in-Iran

Также позитивное влияние на внутренний технологический рынок Ирана оказал короткий период «оттепели» в отношениях с Западом в период существования СВПД (2015-2017 гг.) – в указанный промежуток Тегеран активно налаживал связи с иностранными фирмами. Впоследствии наработанные компетенции были использованы для более эффективной адаптации цифровой инфраструктуры под ограничительные меры – в частности, модернизации и развития Межбанковской сети передачи информации (*Shetab*)[53].

1.2. Регион Африки южнее Сахары

Кибербезопасность (технико-технологическое измерение)

Государства АЮС продолжают уделять повышенное внимание вопросам развития цифровых компетенций – особенно в части технической защиты объектов критической инфраструктуры.

Согласно последним замерам МСЭ, лидерство среди стран Африки южнее Сахары в вопросах защиты цифрового пространства сохраняется за Маврикием. Более того, показатели киберготовности страны к 2024 г. достигли максимальных показателей (100 у.п. из 100 возможных), что указывает на сбалансированное развитие национальной системы киберзащиты[54]. Также в группе передовых кибердержав региона оказались Гана, Кения, Руанда и Танзания – их показатели близки к максимальным (98 у.п. и выше)[55]. Остальные государства АЮС расположились в глобальном рейтинге следующим образом *(см. диаграмму 3).*

Значительная часть государств региона (за исключением Нигерии и Гвинеи-Бисау) заметно улучшили свой совокупный показатель киберготовности (в среднем, в два раза)[56], в отдельных случаях (например, Демократическая Республика Конго) показатель вырос в 10 и более раз. Столь резкое изменение показателей, демонстрирует систематизацию усилий стран АЮС в работе над развитием национального киберсектора.

Специалисты МСЭ по-прежнему относят большую часть стран АЮС либо к категории «Оформляющихся» (системные усилия на нескольких направлениях), либо «Развивающихся» (системные усилия хотя бы на одном из ключевых направлений) государств.

[53] Shetab Banking System. URL: https://www.cbi.ir/page/16090.aspx
[54] 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
[55] Ibidem.
[56] 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.

При этом темпы работы по совершенствованию технического потенциала стран Африки южнее Сахары по сравнению с периодами прошлых замеров (2014[57], 2018[58] и 2021[59] гг.) можно охарактеризовать как нарастающие – подавляющее большинство государств АЮС сделали упор на развитие системы управления профильными институтами, актуализацию национального нормативно-правового поля, совершенствование технического и кадрового потенциала.

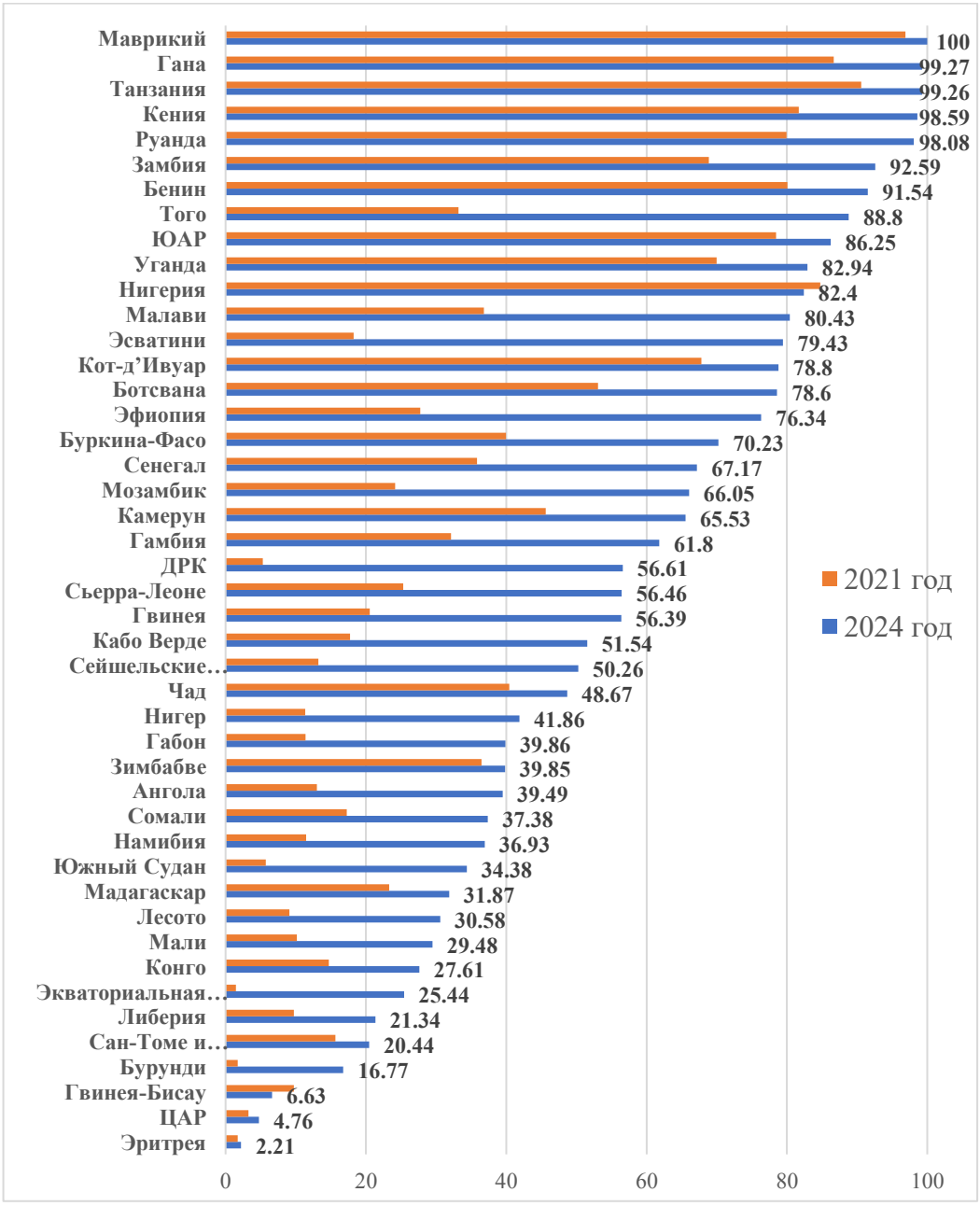

Диаграмма 3. Совокупный показатель киберготовности государств АЮС по состоянию на 2024 г. (максимальный балл – 100) Составлено по: GCI-2020[60], GCI-2024[61].

[57] Global Cybersecurity Index 2014 // ITU. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2014.aspx
[58] Global Cybersecurity Index 2018 // ITU. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
[59] Global Cybersecurity Index 2020 // ITU. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf
[60] Global Cybersecurity Index 2020 // ITU. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf
[61] Global Cybersecurity Index 2024 // ITU. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

При этом в большинстве государств АЮС процесс реформирования системы государственных институтов, ответственных за обеспечение национальной цифровой безопасности, еще не завершен: профильные министерства созданы в 14 африканских странах. В остальных функционал пока разделен между двумя и более государственными органами – нередко с существенным дублированием полномочий[62].

Другой характерной чертой Субсахарского региона является существенная неоднородность показателей уровня защищенности критической информационной инфраструктуры (КИИ), отличающихся от государства к государству, а также сохраняющийся «реактивный» подход большинства стран к выстраиванию модели киберзащиты (что заметно как на национальном, так и на региональном уровнях).

Только в половине стран АЮС созданы национальные Компьютерные группы реагирования на чрезвычайные ситуации (*CERT/CSIRT*), а наличием отраслевых кибергрупп может похвастаться только каждая третья страна[63]. Государства Субсахарской Африки пытаются купировать эту проблему различными путями – например, через создание в структуре государственных институтов специализированных исследовательских центров и агентств, нацеленных на мониторинг и выявление угроз из киберпространства (в отдельных случаях их функционал «вписан» в работу национального института, ответственного за управление цифровыми процессами в стране). Однако куда чаще задачи по охране и защите национальной КИИ делегируются частным фирмам и независимым киберкомандам, которые по функционалу замещают CERT (*см. таблицу 3*).

Страна	Национальная CERT / CSIRT	Отраслевые группы	Частные группы	Специализированные исследовательские центры и агентства	Членство в AfricaCERT
Ангола	Нет	Нет	Да	Нет	Нет
Бенин	Да	Да	Да	Нет	Да
Ботсвана	Да	Нет	Нет	Да	Да
Буркина-Фасо	Да	Нет	Да	Нет	Нет
Бурунди	Нет	Нет	Нет	Нет	Нет
Габон	Нет	Нет	Да	Да	Да
Гамбия	Да	Да	Нет	Нет	Да
Гана	Да	Да	Да	Нет	Да
Гвинея	Нет	Нет	Да	Нет	Нет
Гвинея-Бисау	Нет	Нет	Нет	Нет	Нет
ДРК	Нет	Нет	Да	Нет	Нет
Замбия	Да	Да	Нет	Нет	Нет
Зимбабве	Нет	Нет	Да	Нет	Нет
Кабо-Верде	Нет	Нет	Да	Нет	Нет

[62] В отдельных случаях (например, в Эритрее) «цифровой департамент» существует в структуре государственных органов (в данном случае – в структуре национального министерства связи и коммуникаций) только формально, в то время как нормативно-правовые рамки его деятельности, а также полномочия и цели стратегического развития, никак не определены. См.: Eritrea // UNIDIR Cyber Policy Portal. URL: https://cyberpolicyportal.org/states/eritrea

[63] National CIRTs worldwide // ITU. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/CIRTs/List-of-National-CIRTs.aspx

Камерун	Да	Нет	Да	Нет	Да
Кения	Да	Да	Да	Нет	Да
Конго	Нет	Нет	Да	Нет	Нет
Кот-д'Ивуар	Да	Да	Нет	Да	Да
Лесото	Нет	Нет	Да	Да	Да
Либерия	Нет	Нет	Нет	Да	Да
Маврикий	Да	Да	Да	Да	Да
Мадагаскар	Нет	Нет	Да	Нет	Нет
Малави	Да	Нет	Нет	Да	Нет
Мали	Да	Нет	Нет	Нет	Нет
Мозамбик	Да	Нет	Да	Нет	Да
Намибия	Да	Нет	Нет	Нет	Нет
Нигер	Нет	Нет	Да	Нет	Нет
Нигерия	Да	Да	Нет	Да	Да
Руанда	Да	Да	Да	Нет	Да
Сан-Томе и Принсипи	Нет	Нет	Да	Нет	Нет
Сейшельские острова	Нет	Нет	Нет	Да	Нет
Сенегал	Да	Нет	Нет	Да	Да
Сомали	Да	Нет	Нет	Нет	Да
Сьерра-Леоне	Нет	Нет	Да	Да	Да
Танзания	Да	Да	Да	Нет	Да
Того	Да	Да	Да	Нет	Нет
Уганда	Да	Да	Нет	Нет	Нет
ЦАР	Нет	Нет	Да	Нет	Нет
Чад	Нет	Нет	Нет	Нет	Нет
Экваториальная Гвинея	Нет	Нет	Нет	Нет	Нет
Эритрея	Нет	Нет	Нет	Нет	Нет
Эсватини	Да	Да	Да	Нет	Нет
Эфиопия	Да	Нет	Да	Нет	Да
ЮАР	Да	Да	Да	Нет	Нет
Южный Судан	Да	Нет	Да	Нет	Нет

Таблица 3. Уровень развития системы реагирования на компьютерные инциденты в странах АЮС. Составлено по: ITU CERT/CIRT Database[64], AfricaCERT[65]

При этом позитивным трендом можно считать активизацию работы африканских государств в рамках *AfricaCERT* – межгосударственной площадки, призванной координировать сотрудничество между национальными киберкомандами стран АЮС, международными организациями и частными компаниями по профилю цифровой безопасности и защиты.

Учитывая, что одним из направлений работы площадки является оказание помощи африканским странам в создании национальных CERT/CSIRT путем предоставления экспертных знаний и консультаций по формулированию инициатив (включая обмен опытом внутри региона), *AfricaCERT* служит еще и «точкой сборки» позитивного опыта

[64] National CIRTs worldwide // ITU. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/CIRTs/List-of-National-CIRTs.aspxx
[65] Members & Partners // GFCE. URL: https://thegfce.org/member-and-partner/

реагирования на киберугрозы. По состоянию на 2024 год, к мероприятиям *AfrciaCERT* присоединилось около половины государств АЮС[66].

Одним из важнейших драйверов развития Субсахарских систем кибербезопасности является международное сотрудничество. Ставку на развитие внешних контактов (как на межгосударственном уровне, так и по линии бизнеса) сделали все без исключения государства АЮС[67].

Особое место в системе соразвития компетенций государств региона в киберпространстве занимает Африканский союз (АС), на площадке которого в 2014 г. была принята Конвенция Африканского союза о кибербезопасности и защите персональных данных (*Конвенция Малабо*)[68], а в 2016 г. – провозглашен Глобальный подход к обеспечению кибербезопасности и противодействию киберпреступности в Африке[69], основанный на положениях данной Конвенции.

Кроме того, на базе АС на регулярной основе проходят многосторонние встречи представителей сектора связи африканских стран (в работе которых принимают участие в т.ч. представители региона АЮС), направленные на координацию усилий в борьбе с киберпреступностью и другими угрозами КИИ государств Африки[70]. Работа в рамках данной площадки позволяет государствам Субсахарской Африки поддерживать активный внутрирегиональный диалог, а также обмениваться данными об эффективных практиках в области цифровой защиты.

Проблема кибертерроризма на данный момент пока не получила значительного выражения в регионе Африки южнее Сахары – в силу специфики социально-экономического ландшафта, а также более слабого – по сравнению с другими регионами – 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[71], эта работа касается скорее социальной составляющей кибербезопасности: 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 полностью списывать со счетов данный тип угрозы – тем более, что темпы цифровизации стран региона стремительно растут, а общее число

[66] Members & Partners // GFCE. URL: https://thegfce.org/member-and-partner/
[67] Подробнее об основных направлениях сотрудничества с внешними партнерами см. Раздел 2.
[68] African Union Convention on Cyber Security and Personal Data Protection // African Union. URL: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf
[69] A global approach on Cybersecurity and Cybercrime in Africa // African Union. URL: https://au.int/sites/default/files/newsevents/workingdocuments/31357-wd-a_common_african_approach_on_cybersecurity_and_cybercrime_en_final_web_site_.pdf
[70] См., напр.: The African Union convenes the second African Cybercrime Forum // African Union, 2021. URL: https://au.int/sites/default/files/pressreleases/40556-pr-PR-Cybercrime_Forum_2021.pdf
[71] 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/

Интернет-пользователей уже превысило отметку в 540 млн человек[72]. Радикально-экстремистские движения реагируют на изменения и стремятся расширить свое влияние, а в перспективе – еще и нарастить «ударные» средства, способные наносить ущерб критической инфраструктуре[73].

Социальное измерение цифровой безопасности

Растущее влияние киберугроз на Африканский континент имеет серьезные последствия для социально-экономического развития стран региона, что подталкивает лидеров государств АЮС к наращиванию усилий по укреплению социального измерения цифровой безопасности.

Особый упор в данном случае делается на совершенствование законодательства, связанного с регулированием деятельности в цифровом пространстве. Учитывая, что темпы развития *digital-среды* кратно опережают скорость разработки и утверждения профильных нормативно-правовых актов, гармонизация национального правового поля становится серьезным вызовом для государств АЮС[74].

Особенно это заметно на примере НПА, направленных на защиту уязвимых категорий населения (например, детей и подростков). По состоянию на 2024 г., лишь около половины стран АЮС приняли законы, в которых предусмотрены (хотя бы косвенно) меры по защите подрастающего поколения от киберрисков[75]. При этом большинство этих законов либо ограничены по масштабу и применимости к детской онлайн-среде, либо еще не полностью применяются.

При этом наиболее комплексный подход к решению проблемы на данный момент демонстрируют только две страны АЮС – это Гана, где национальный закон о кибербезопасности (2020 г.)[76] весьма подробно определяет формат участия детей и подростков в цифровых процессах, а также прописывает обязательства поставщиков телекоммуникационных услуг по предупреждению и контролю киберрисков, и Руанда, где помимо «якорного» закона об ИКТ (2016 г.)[77] сформирована детально проработанная политика в области защиты прав детей в цифровой среде, а также принят пробный план действий на пятилетний период (2019-2024 гг.)[78]. Разработку профильных стратегий также ведут Кения, Замбия и некоторые другие страны АЮС.

---

[72] 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/

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

[74] Проблема инертности законодательной сферы, в целом, характерна для всех регионов мира, однако в случае с АЮС на нее дополнительно накладываются другие проблемы (недофинансирование, отсутствие стратегического планирования, нормотворческие разногласия), что усложняет работу над НПА.

[75] Посчитано по: Africa Laws Database. URL: https://www.africa-laws.org/Laws.php

[76] Cybersecurity Act, 2020 (Ghana) // CSDS Africa. URL: https://csdsafrica.org/wp-content/uploads/2021/08/Cybersecurity-Act-2020-Act-1038.pdf

[77] Rwanda ICT Law // MINICT. URL: https://www.minict.gov.rw/fileadmin/user_upload/minict_user_upload/Documents/Laws/ICT_LAW.pdf

[78] Rwanda Child online protection policy. URL: https://rura.rw/fileadmin/Documents/ICT/Laws/Rwanda_Child_Online_Protection_Policy.pdf

Следует отметить, что государства Субсахарской Африки стремятся компенсировать недостаток нормотворческой работы на национальном уровне активизацией межгосударственного сотрудничества в рамках региональных интеграционных площадок (Африканский союз, Восточноафриканский союз и др.)[79]. Наращивается диалог и по линии НКО и экспертных организаций – в числе наиболее крупных частных площадок следует отметить Африканский хаб цифровых прав, *CIPESA* и *Research ICT Africa*[80]. Однако, в силу сохраняющейся разобщенности между многими государствами, обеспечить систематизацию усилий (и тем самым мотивировать национальный киберсектор к более гармоничному развитию) пока не удается.

Вопрос развития кадрового потенциала в цифровом секторе государств АЮС по-прежнему стоит довольно остро. Согласно последним замерам экспертов МСЭ, к 2024 г. только 18 стран региона смогли преодолеть *экватор* по данному критерию, получив за него 10 баллов и более; максимального показателя достигли лишь две страны (Кения и Маврикий)[81]. Более того, показатели шести стран (Сан-Томе и Принсипи, Мали, Гвинея-Бисау, Эритрея, Конго, ЦАР) были охарактеризованы как «близкие к минимальным» (менее 1 у.п.)[82].

Столь заметная разница показателей в масштабах одного региона обусловлена тем, что далеко не во всех государствах АЮС выстроена система подготовки кадров, а также приняты долгосрочные стратегии развития национального потенциала в области цифровой безопасности. Кроме того, национальный IT-сектор испытывает заметную «утечку мозгов» в зарубежные компании. Данная тенденция особенно усилилась после пандемии COVID-19, когда повсеместное внедрение удаленного формата работы позволило перспективным кадрам работать на иностранные фирмы, не покидая места жительства.

Государства АЮС по-разному пытаются решать проблему нехватки кадров в динамично развивающейся цифровой отрасли – например, посредством запуска совместных предприятий с зарубежными IT-гигантами (как правило, западными)[83] или создания образовательных центров с зарубежным участием[84]. Укрепление связей между отечественным и зарубежным кибербизнесами, по замыслу национальных правительств, должно повысить общий престиж цифровых профессий и обеспечить приток молодых кадров в отрасль.

Еще один перспективный формат международного сотрудничества, позитивно влияющий на национальный цифровой потенциал – создание технопарков. Технопарки в данном

[79] В числе подобных инициатив – Политика ВАС в области защиты детей для укрепления систем защиты детей в Восточноафриканском сообществе, Типовой закон САДК об искоренении детских браков, Политика в отношении детей ЭКОВАС и др.

[80] 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

[81] Еще три страны АЮС к 2024 г. получили от экспертов МСЭ по данной группе критериев получили балл, близкий к максимальному: Руанда (19,76), Танзания (19,57) и Гана (19,27). 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

[82] Ibidem.

[83] Top 10: African Cybersecurity Companies // Cyber Magazine. 16.06.2023. URL: https://cybermagazine.com/articles/top-10-cybersecurity-companies-in-africa

[84] Cybersecurity Courses in Africa // EC-Council. URL: https://www.eccouncil.org/cybersecurity-courses-and-training-in-africa/; Cybersecurity Industrial Training // IBT Learning. URL: https://ibtlearning.africa/courses/cybersecurity-industrial-training/

случае выступают площадками для обмена технологиями и производственным опытом, масштабирования успешных бизнес-решений и привлечения инвестиций.

Лидером по числу созданных технопарков выступает ЮАР – в стране на постоянной основе функционирует как минимум три площадки (Финтех-кластер *Cape Innovation and Technology Initiative, TechnoPark Stellenbosch* и *The Innovation Hub*), которые ориентированы на развитие сотрудничества как по профилю кибербезопасности в целом, так и на решение смежных задач – например, интеграцию цифровых решений в сектор здравоохранения, АПК и пр.[85].

Также по стране создано порядка 80 малых площадок (т.н. «технохабов»[86]), ориентированных на технологическое развитие и совершенствование национального производственного и кадрового потенциала. Общее же число «технохабов» в Субсахарской Африке превысило отметку в 500 объектов – 80% всех созданных на Африканском континенте (*см. рис. 2*).

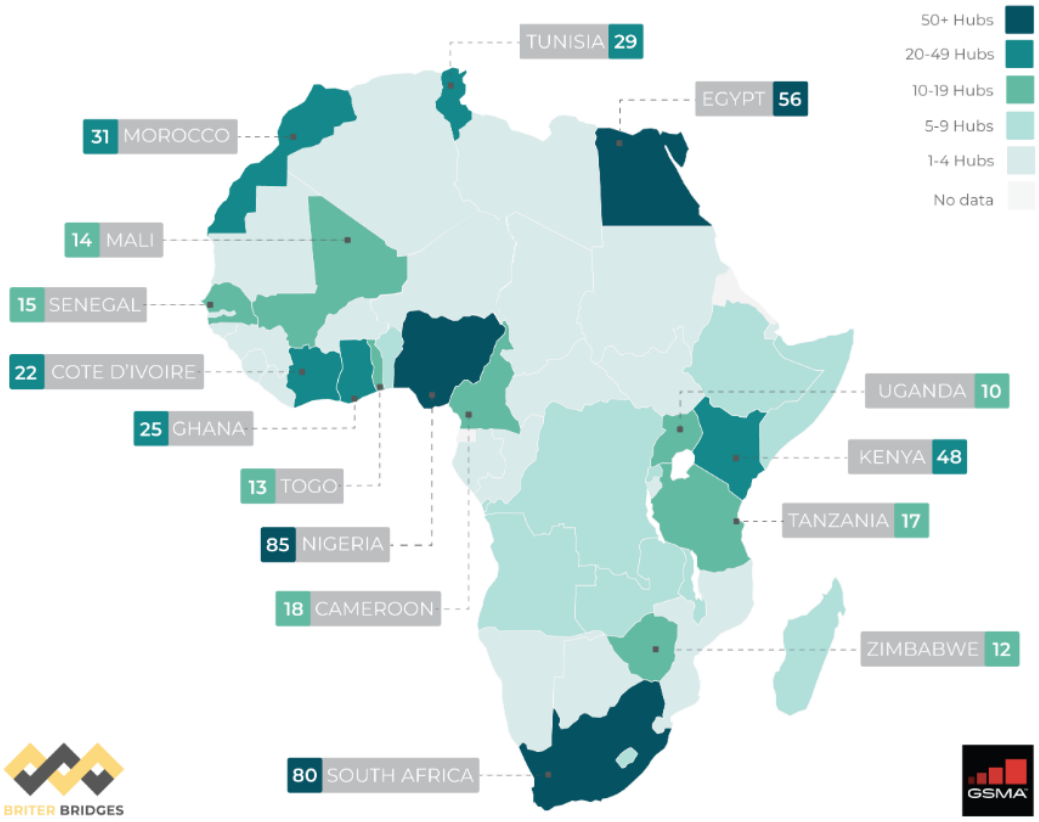

Рис.2. Количество действующих технологических хабов в странах Африки. Источник: Briter Bridges[87].

[85] Африканский стартап-лидер // ИД «Коммерсантъ». 04.07.2023. URL: https://www.kommersant.ru/doc/6082525

[86] Согласно определению Briter Bridges, активный технологический хаб — это организация, которая в настоящее время действует в регионе АЮС, имеет местную регистрацию (представительство или головной офис) и предлагает возможности и поддержку для технологических и цифровых предпринимателей, а также способствует развитию национального киберсектора в целом. См.: 618 Active Tech Hubs in Africa // Briter Bridges. URL: https://briterbridges.com/618-active-tech-hubs

[87] 618 Active Tech Hubs in Africa // Briter Bridges. URL: https://briterbridges.com/618-active-tech-hubs

По данным Всемирного банка, около 66% взрослого населения в странах Африки южнее Сахары лишены доступа к банковским услугам, а на 100 тыс. человек приходится лишь около пяти банковских отделений[88]. Это открывает невероятные возможности для мобильных банков и систем мобильных платежей и стимулирует развитие рынка финансовых технологий.

Моторами регионального FinTech-рынка являются Нигерия, Кения и ЮАР – именно на эти страны приходится наибольшее число стартапов с наибольшим уровнем доходности[89]. Кроме того, из десяти наиболее крупных, с точки зрения акционерного финансирования, компаний на Африканском континенте, не менее восьми созданы в упомянутых странах АЮС[90].

Характерная черта региона – разработка собственных микросистем для проведения бытовых транзакций. Для этих целей используются, например, платежные системы вроде *M-Pesa* (мобильные деньги), которую запустила кенийская телекоммуникационная компания *Safaricom* в 2007 г.[91]. Благодаря этому сервису за довольно короткое время Кения стала одним из мировых лидеров в области цифровых финансовых инноваций, а сервис достиг масштабов регионального оператора, преодолев в 2022 г. отметку в 50 млн пользователей[92].

Похожие системы также созданы и в ЮАР (*Vodacom*), которая предоставляет услугу через свои дочерние компании в Танзании, ДРК, Мозамбике, Лесото и Гане[93]. Более того, *Safaricom* и *Vodacom* работают над запуском совместных FinTech-продуктов. Например, в 2022 г. они совместно с платежной системой Visa запустили виртуальную карту для международных цифровых платежей[94], что позитивно сказалось на интенсивности и прозрачности финансовых операций в регионе АЮС.

Однако региональный рынок финансовых технологий не ограничивается только тремя странами. Стремительно наращивает позиции угандийская облачная платформа *Beyonic*, которая позволяет плательщикам использовать мобильные сети для платежей и предлагает

---

[88] Financial Inclusion in Sub-Saharan Africa—Overview // World Bank. 17.04.2024. URL: https://www.worldbank.org/en/publication/globalfindex/brief/financial-inclusion-in-sub-saharan-africa-overview

[89] https://startuplist.africa/industry/fintech

[90] В группу крупнейших FinTech-компаний входят TymeBank (цифровой банкинг, ЮАР), Moove (сервис каршеринга, Нигерия), M-Kopa (цифровой кредитор, Кения), Lulalend (сервис управления финансами, ЮАР), Lemfi (платежный сервис, Нигерия), Peach Payments (платежный сервис, ЮАР) Nomba (платежный сервис, Нигерия) и Stitch (платежный сервис, ЮАР). На перечисленные фирмы суммарно приходится порядка 60% акционерных вливаний. См.: 10 African Startups Dominate 75% of Fintech Equity Africa Funding in 2023 // FinTech News. 05.02.2024. URL: https://fintechnews.africa/43166/fintechafrica/10-african-startups-dominate-75-of-fintech-equity-africa-funding-in-2023/

[91] M-PESA App. URL: https://www.safaricom.co.ke/personal/value-added-services/information-services/m-pesa-app

[92] Vodacom: Leading Fintech Growth & Supporting SMEs in Africa // FinTech Magazine. 29.04.2024. URL: https://fintechmagazine.com/articles/vodacom-leading-fintech-growth-supporting-smes-in-africa

[93] M-Pesa celebrates reaching 50 million customers // Vodafone. 07.09.2021. URL: https://www.vodafone.com/news/services/m-pesa-celebrates-reaching-50-million-customers

[94] Visa and Kenya's Safaricom launch virtual card to support global digital payments via M-Pesa // Tech Crunch. 02.06.2022. URL: https://techcrunch.com/2022/06/02/visa-and-kenyas-safaricom-launch-virtual-card-to-support-global-digital-payments-via-m-pesa/

двусторонние цифровые платежные решения предприятиям[95]. Сильной чертой платформы является возможность подключаться с ее помощью более чем к 15 корпоративным приложениям, включая *Quickbooks*, *Xero* и *Salesforce*. Кроме того, проходящие через экосистему *Beyonic* данные регулярно резервируются и шифруются при хранении и во время передачи[96], что в условиях непрекращающихся попыток киберпреступных группировок завладеть личными данными пользователей АЮС является неоспоримым преимуществом.

Следует обратить особое внимание на африканский рынок криптовалюты – тем более, что активность на нем проявляют все больше стран АЮС. Согласно последним замерам авторитетного консалтингового агентства Henley & Partners, в глобальный ТОП-25 по совокупному показателю принятия криптовалют входит только одна страна региона (Маврикий, 20 место); еще одна страна (Намибия) вплотную приблизилась к группе лидеров, заняв 26 позицию[97].

Обе страны имеют, в целом, сбалансированные показатели с точки зрения уровня общественного принятия цифровых валют, их нормативно-правового регулирования и степени развития профильной инфраструктуры. При этом бросается в глаза крайне низкий «инновационный» коэффициент – 0,7 и 0,1 (при максимальном результате 10) соответственно[98].

Используя методологию Henley & Partners, можно выстроить градацию совокупного показателя принятия криптовалют для остальных стран АЮС (*см. диаграмму 4*). При этом, ряду государств региона, по объективным причинам, в рейтинге присвоен «нулевой» индекс, и в итоговую инфографику они не включены[99].

Как видно из представленных данных, большинство государств АЮС в настоящее время по-прежнему испытывают трудности с внедрением инновационной инфраструктуры, связанной с цифровыми активами, а также развитием правового режима. При этом, с точки зрения общественного принятия криптовалют (показателя, отражающего консенсус властей и рядовых пользователей) в регионе наблюдается позитивная динамика, а ряд государств (например, Кения, ЮАР и Сенегал) не уступают лидерам рейтинга.

Дальнейшему развитию профильных компетенций государств АЮС в области оборота цифровых валют во многом способствует участие внешних игроков. Например, в Кении работает британская криптовалютная биржа *Binance*, которая проводит образовательные

[95] В 2020 г. интегрирован в экосистему панафриканского платежного шлюза MFS Africa. См.: Mobile money gateway MFS Africa has acquired B2B digital payments player, Beyonic // Quartz. 30.06.2020. URL: https://qz.com/africa/1873964/mobile-money-giant-mfs-africa-acquires-beyonic-for-enterprise-solutions
[96] Ibidem.
[97] The Crypto Wealth Report // Henley & Partners. URL: https://www.henleyglobal.com/publications/crypto-wealth-report/crypto-adoption-index
[98] The Crypto Wealth Report // Henley & Partners. URL: https://www.henleyglobal.com/publications/crypto-wealth-report/crypto-adoption-index
[99] Согласно методологии Henley & Partners, «нулевой» индекс присваивается в том случае, если объективные данные в открытых источниках в достаточном количестве отсутствуют или противоречат друг другу – ввиду чего однозначно оценить готовность страны к использованию ЦФА проблематично.

мероприятия для студентов и участвует в обсуждениях мер контроля крипторынка с регуляторами[100], что позволяет постепенно развивать систему обращения с ЦФА в стране.

С другой стороны, значительная часть правительств Субсахарской Африки по-прежнему относится к криптовалютным операциям с большой долей подозрительности, видя в них удобный источник финансирования деятельности преступных, террористических и сепаратистских группировок[101].

Кроме того, открытым остается вопрос обращения с личными данными пользователей криптовалютных услуг. С учетом того, что африканские предприниматели регулярно становятся жертвами кибератак, нацеленных на кражу персональных данных, власти стран АЮС с повышенной подозрительностью относятся к любым проектам, где риск утечки чувствительной информации прогнозируется как вероятный.

Примером тому служит скандал вокруг криптовалютной биржи *Worldcoin*, возникший в 2023 г. из-за недостаточного внимания владельцев биржи к защите персональных данных ее пользователей. По итогу Министерство внутренних дел Кении приостановило деятельность криптопроекта в стране на неопределенный срок, чтобы госорганы оценили его потенциальные риски для общественной безопасности[102]. Это, в свою очередь, негативно сказалось на позициях *Worldcoin* не только на кенийском рынке, но и в регионе АЮС в целом.

[100] Binance To Hold A Week-long Educational Event at the University of Nairobi // Binance. 28.10.2022. URL: https://www.binance.com/en-NG/blog/all/binance-to-hold-a-weeklong-educational-event-at-the-university-of-nairobi-7323207019037373499

[101] FSB Sub-Saharan Africa group discusses vulnerabilities arising from high sovereign indebtedness and crypto-assets // Financial Stability Board. 06.10.2023. URL: https://www.fsb.org/2023/10/fsb-sub-saharan-africa-group-discusses-vulnerabilities-arising-from-high-sovereign-indebtedness-and-crypto-assets/

[102] Кения сообщила о приостановке проекта Worldcoin из-за рисков безопасности // РБК. 02.08.2023. URL: https://www.rbc.ru/crypto/news/64ca1d419a7947422a5853c8

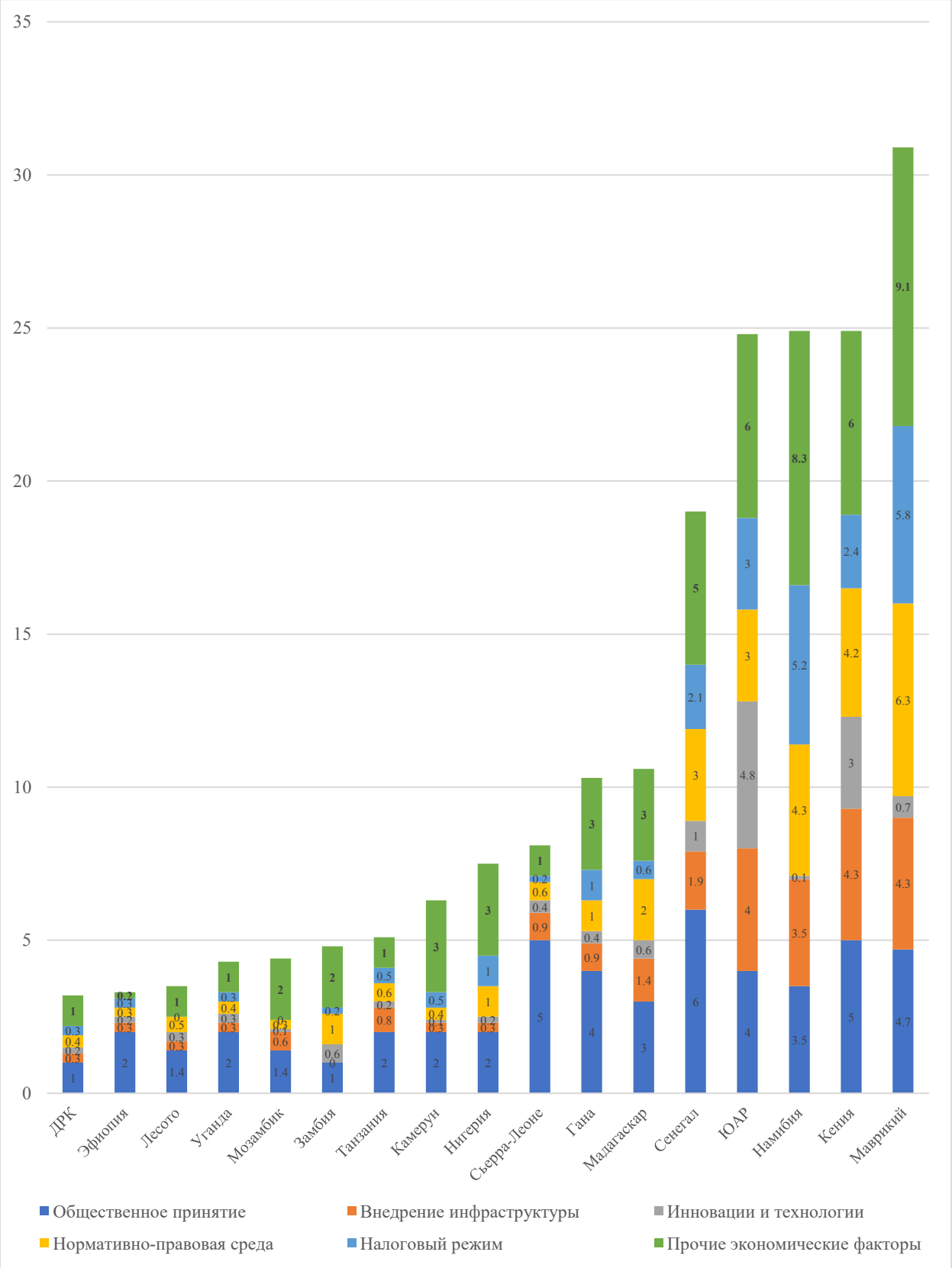

Диаграмма 4. Совокупный показатель принятия криптовалют в государствах региона (максимальный балл по каждому критерию – 10; предельный балл – 60). Составлено автором на основе методологии Henley & Partners[103].

[103] The Crypto Wealth Report // Henley & Partners. URL: https://www.henleyglobal.com/publications/crypto-wealth-report/crypto-adoption-index

Другая перспективная точка роста – сервисы государственных цифровых услуг («Электронное правительство»). Государства Африки проявляют к данному направлению повышенный интерес, поскольку интеграция систем и услуг электронного правительства позволит повысить эффективность предоставления государственных услуг, а также уменьшить расход ресурсов при взаимодействии граждан и государственных институтов. Кроме того, интеграция госуслуг в единую цифровую систему позволяет усовершенствовать и саму систему управления: за счет систематизации и маршрутизации услуг, устранения дублирующих и смежных полномочий у отдельных ведомств.

Однако в случае с Субсахарской Африкой мы можем наблюдать, что значительная часть государств только начинает работу по систематизации госуслуг. Так, согласно последним замерам ООН, в глобальный ТОП-100 Индекса развития электронного правительства входят только три государства АЮС (ЮАР, Маврикий, Сейшельские острова) – и разрыв между ними достаточно ощутимый (*см. Таблицу 4*).

Страна	Место в глобальном рейтинге	Место в региональном рейтинге
ЮАР	40	1
Маврикий	76	2
Сейшельские острова	92	3
Гана	108	4
Кения	109	5
Кабо-Верде	111	6
Ботсвана	112	7
Эсватини	113	8
Намибия	114	9
Руанда	118	10
Габон	121	11
Кот-д’Ивуар	124	12
Замбия	130	13
Сенегал	135	14
Нигерия	144	15
Бенин	146	16
Зимбабве	149	17
Уганда	150	18
Танзания	153	19
Сан-Томе и Принсипи	154	20
Камерун	155	21
Ангола	156	22
Лесото	157	23
Гвинея	160	24
Того	161	25
Малави	163	26
Конго	166	27
Мадагаскар	168	28
Эфиопия	169	29
Гвинея-Бисау	170	30
Сьерра-Леоне	172	31
Мали	173	32
Буркина-Фасо	175	33
Экваториальная Гвинея	176	34

Мозамбик	177	35
ДРК	179	36
Гамбия	181	37
Либерия	182	38
Бурунди	183	39
Нигер	187	40
Чад	189	41
Эритрея	190	42
Сомали	191	43
Южный Судан	192	44
ЦАР	193	45

Таблица 4. Индекс развития электронного правительства для стран АЮС. Составлено по: E-Government Development Index[104].

Цифровая трансформация сектора государственных услуг в Африке, направленная на повышение эффективности и доступности цифровых сервисов, сопряжена с растущим риском кибератак. EGov-платформы государств АЮС по-прежнему существенно уступают по уровню защищенности аналогичным платформам в странах Европы и Азиатского-Тихоокеанского региона, что создает новые вызовы национальной безопасности стран региона.

Так, кибератаки в отношении цифровой инфраструктуры Сенегала, Кении и ряда других стран АЮС, имевшие место в последний год[105], довольно ярко продемонстрировали как уязвимости в системе защиты EGov-сервисов могут осложнить доступ сразу к нескольким тысячам услуг и нарушить функционирование государственных институтов, создав повышенную нагрузку на их инфраструктуру. В свете этого дискуссии о развитии цифровых сервисов в странах АЮС *идут рука об руку* с вопросами развития национальных систем киберзащиты[106].

С другой стороны, в профессиональном сообществе царит осторожных оптимизм. Эксперты отмечают, что, несмотря на серьезное отставание от глобальных лидеров, потенциал развития EGov-сервисов в Африке достаточно велик.

Так, например, отсутствие «рудиментарных НПА» (*т.е. относящихся к начальному этапу развития цифрового пространства – прим. автора*) [107] в большинстве стран АЮС открывает возможности создания благоприятной цифровой среды с опорой на передовой международный опыт. Подобное *коллаборативное регулирование* позволяет обеспечить быстрый качественный прорыв в области внедрения цифровых сервисов и задействовать

[104] E-Government Development Index // UN E-Government Knowledgebase. URL: https://publicadministration.un.org/egovkb/en-us/Data-Center

[105] См.: Cyberattack targets government websites in Senegal // Africa News. 13.08.2024. URL: https://www.africanews.com/2023/05/27/cyberattack-targets-government-websites-in-senegal/; Kenyan gov't says its e-Citizen portal suffered cyberattack // Anadolu. 28.07.2023. URL: https://www.aa.com.tr/en/africa/kenyan-gov-t-says-its-e-citizen-portal-suffered-cyberattack/2956271 и др.

[106] Gauteng e-Government invests in Cyber Security for the province // South African Government. 27.08.2024. URL: https://www.gov.za/news/media-statements/gauteng-e-government-invests-cyber-security-province-27-aug-2024

[107] В данном случае подразумевается, что в большинстве стран АЮС цифровое законодательство создается с нуля, уже в условиях существования ИИ-технологий и сервисов цифрового правительства. По этой причине странам региона, как правило, нет необходимости пересматривать законы начала 2000-х г. (как в случае со странами Европы или Персидского залива). См.: African Countries E-Gov Challenges & Solutions // E-Governance Hub. URL: https://e-governancehub.ru/african-countries-e-gov-challenges/

для этих целей меньше ресурсов. С течением времени *коллаборативную* тактику перенимают все больше африканских государств[108].

Однако даже в этом случае последовательная модернизация сектора цифровых услуг неизбежно требует повышенной координации между государственными институтами и представителями профильной отрасли – особенно в случае трансформации разветвленного государственного аппарата с множеством государственных органов, каждый из которых имеет свои интересы и приоритеты.

Применение технологий искусственного интеллекта

Запрос на использование технологий искусственного интеллекта в странах АЮС стремительно растет. Как показывают последние замеры Google и Ipsos, африканские страны настроены по отношению к ИИ-технологиям более открыто и лояльно (по сравнению с представителями стран ЕС или Азии), позиционируя их как инструмент ускорения национальных экономик и оптимизации производственных процессов – наибольший спрос на внедрение ИИ-решений наблюдается в секторе промышленности и АПК[109].

При этом реальный уровень готовности государств Субсахарской Африки к внедрению новых технологий – с точки зрения адаптированности национальных институтов и нормативно-правового поля – пока оставляет желать лучшего.

Так, в подавляющем большинстве государств АЮС ИИ-сектор регулируется комплексом смежных НПА (например, законами о связи и телекоммуникациях, регулировании услуг связи, работе банковского сектора и пр.) – отдельные разделы по ИИ введены только в семи странах (Габон, Кения, Мадагаскар, Нигер, Сенегал, Сьерра-Леоне и ЮАР); профильные НПА, посвященные проблематике искусственного интеллекта, приняты в Бенине, Маврикии, Руанде и Эфиопии. (*см. таблицу 5*).

Страна	Стратегия развития ИИ	Профильные институты	Профильные НПА	Инициативы в области ИИ
Ангола	Нет	Нет	Нет	Нет
Бенин	Да	Нет	Да	Нет
Ботсвана	Нет	Нет	В разработке	Нет
Буркина-Фасо	Нет	Нет	Нет	Нет
Бурунди	Нет	Нет	Нет	Нет
Габон	Нет	Нет	Да (частично)	Нет
Гамбия	Нет	Нет	Нет	Нет
Гана	Нет	Нет	Нет	Нет
Гвинея	Нет	Нет	Нет	Нет
Гвинея-Бисау	Нет	Нет	Нет	Нет
ДРК	Нет	Нет	Нет	Нет
Замбия	Нет	Нет	Нет	Нет

[108] Подробнее о развитии систем электронных правительств в разрезе отдельных стран Африки см.: African Countries E-Gov Profiles // E-Governance Hub. URL: https://e-governancehub.ru/african-countries-e-gov-profiles/
[109]Our life with AI: The reality of today and the promise of tomorrow // Google Reports. URL: https://static.googleusercontent.com/media/publicpolicy.google/en//resources/our_life_with_ai_google_ipsos_report.pdf

Зимбабве	Нет	Нет	Нет	Нет
Кабо-Верде	Нет	Нет	Нет	Нет
Камерун	Нет	Нет	Нет	Нет
Кения	В разработке	Нет	Да (частично)	Да
Конго	Нет	Нет	Нет	Нет
Кот-д'Ивуар	Нет	Нет	Нет	Нет
Лесото	Нет	Нет	Нет	Нет
Либерия	Нет	Нет	Нет	Нет
Маврикий	Да	Да	Да	Нет
Мадагаскар	Нет	Нет	Да (частично)	Нет
Малави	Нет	Нет	Нет	Нет
Мали	Нет	Нет	Нет	Нет
Мозамбик	Нет	Нет	Нет	Нет
Намибия	Нет	Нет	Нет	Нет
Нигер	В разработке	Нет	Да (частично)	Нет
Нигерия	Да	Нет	Нет	Нет
Руанда	Да	Нет	Да	Да
Сан-Томе и Принсипи	Нет	Нет	Нет	Нет
Сейшельские острова	Нет	Нет	Нет	Нет
Сенегал	В разработке	Нет	Да (частично)	Да
Сомали	Нет	Нет	Нет	Нет
Сьерра-Леоне	Да	Нет	Да (частично)	Нет
Танзания	Да	Нет	В разработке	Нет
Того	Нет	Нет	Нет	Нет
Уганда	Нет	Нет	Нет	Нет
ЦАР	Нет	Нет	Нет	Нет
Чад	Нет	Нет	Нет	Нет
Экваториальная Гвинея	Нет	Нет	Нет	Нет
Эритрея	Нет	Нет	Нет	Нет
Эсватини	Нет	Нет	Нет	Нет
Эфиопия	Да	Нет	Да	Нет
ЮАР	Нет	Да	Да (частично)	Нет
Южный Судан	Нет	Нет	Нет	Нет

Таблица 5. Состояние национальной системы управления ИИ в государствах АЮС (по состоянию на 2024 г.). Составлено по: UNIDIR AI Policy Portal[110].

Схожим образом ситуация складывается и в разрезе вопросов долгосрочного планирования развития сектора ИИ. Профильные стратегии приняты в семи странах АЮС, еще в трех (Кения, Нигер, Сенегал) документ находится в разработке.

С учетом разницы стартовых позиций, государства региона ожидаемо обладают и разным уровнем привлекательности для бизнес-сообщества с точки зрения развития технологий искусственного интеллекта. По состоянию на конец 2023 г., в тройке лидеров оказались ЮАР, Нигерия и Кения (*см. диаграмму 5*). Также заметный прирост продемонстрировали Гана и Камерун.

[110] Artificial Intelligence Policy Portal. URL: https://aipolicyportal.org/

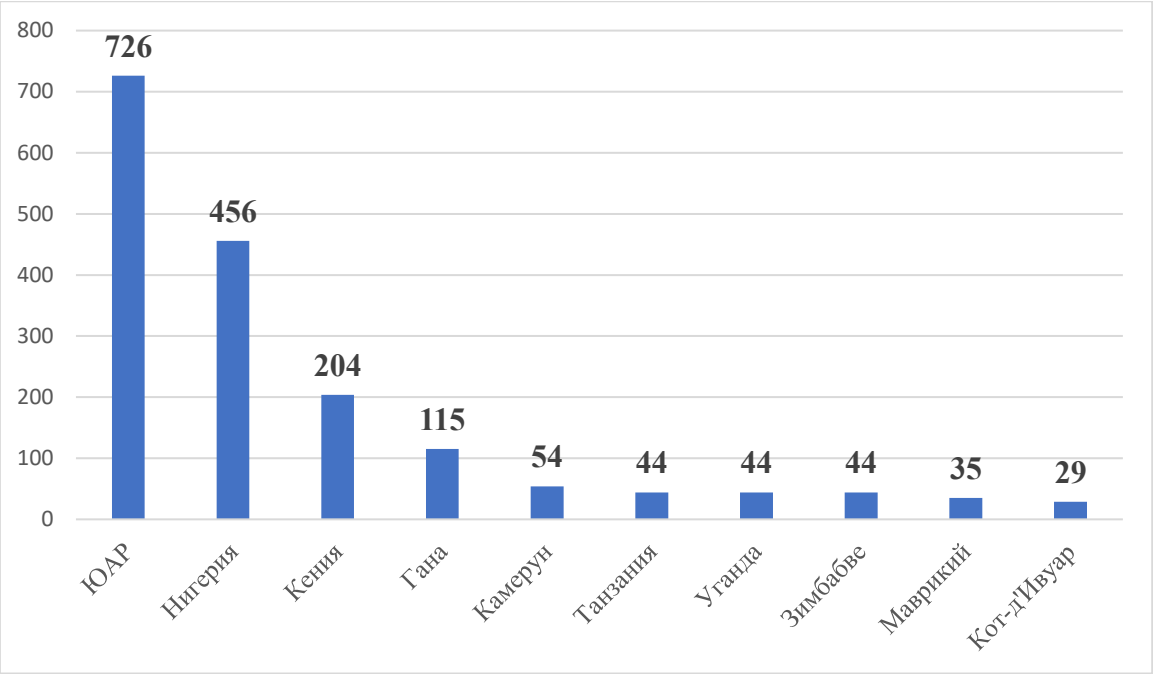

Диаграмма 5. Число фирм, специализирующихся на ИИ-технологиях в странах АЮС (ТОП-10) по состоянию на начало 2024 г. Составлено по: «Artificial Intelligence Revolution in Africa: Economic Opportunities and Legal Challenges»[111].

Темпы развития ИИ-бизнеса в отдельно взятых странах АЮС заметно выше, чем в Северной Африке. Для сравнения: у ближайшего конкурента из числа североафриканских держав, Египта, на балансе находится 246 компаний, специализирующихся на ИИ-технологиях[112]. Это почти в 3 раза меньше, чем в ЮАР и в 1,8 раз – чем в Кении. Однако значительная часть компаний либо являются дочерними предприятиями зарубежных фирм, либо замкнуты на конкретную отрасль работы (например, АПК) и не оказывают ощутимого влияния на национальный – а тем более региональный – рынок.

При этом все чаще встречаются и весьма крупные игроки, полноценно участвующие в развитии национального ИИ-ландшафта. Это, например, кенийская компания *Sama* (разработка передовых технологий обучения с использованием ИИ), южноафриканские *DataProphet* (интеграция ИИ-решений в производственные процессы) и *Curacel* (автоматизация обработки обращений граждан, противодействие кибермошенничеству), а также нигерийская *RxAll* (гиперспектральная платформа Интернета вещей с глубоким обучением и аутентификацией лекарств в режиме реального времени)[113]. Перечисленные стартап-компании на постоянной основе работают с национальными правительствами и оказывают заметное влияние на развитие ИИ-технологий в своих странах.

Зарубежные техногиганты, в целом, проявляют интерес к развитию рынка ИИ в странах Субсахарской Африки, что закладывает основу для нарастания конкуренции за влияние между зарубежными инвесторами[114].

[111] Jaid A. Artificial Intelligence Revolution in Africa: Economic Opportunities and Legal Challenges // Policy Paper. 10.07.2023. URL: https://www.policycenter.ma/sites/default/files/2023-07/PP_13-23%20%28Jaldi%20%29.pdf
[112] Ibidem.
[113] List of Artificial Intelligence Startups in Africa // Startup list. URL: https://startuplist.africa/industry/artificial-intelligence
[114] Подробнее см. Раздел 3.

Национальные разработки в области ПО

Темпы развития рынка программного обеспечения в странах Африки южнее Сахары можно охарактеризовать как высокие. Положительная динамика на данном направлении обусловлена несколькими основными макроэкономическими факторами, среди которых рост объемов внедрения цифровых решений в производственные процессы, популяризация электронной коммерции, а также увеличение спроса на цифровизацию всех отраслей экономики в целом. Кроме того, в странах АЮС с каждым годом увеличивается доля молодого населения, что закладывает запас для дальнейшего расширения рынка цифровых технологий и формирует спрос на ПО.

По оценкам экспертов, совокупная емкость рынка ПО в 2024 г. в регионе преодолела отметку в 5,35 млрд долларов, а к 2032 г. прогнозируется увеличение показателей более чем в 2 раза[115]. Наиболее перспективными, с точки зрения ассигнований, выглядит сектор мобильного ПО – поскольку население стран АЮС (включая представителей МСП), в большинстве своем, отдает предпочтение использованию мобильных, а не стационарных девайсов[116].

В результате продолжающихся инвестиций в мобильную широкополосную связь удалось охватить до 90% территории региона: к началу 2024 г. зафиксировано существенное преобладание доли пользователей, имеющих доступ к технологиям мобильных интернет-услуг, как минимум в 19 странах АЮС (*см. диаграмму 6*), и их число продолжает расти[117]. С другой стороны, ключевыми препятствиями к развитию рынка мобильно й связи (и, как следствие, рынка мобильного ПО) по-прежнему остаются недостаточный уровень цифровой грамотности населения отдельных государств АЮС, проблемы с организацией бесперебойного доступа в глобальную сеть, использование морально устаревшей инфраструктуры связи.

Государства АЮС в последние несколько лет наращивают инвестиции в сектор мобильных технологий, чтобы обеспечить его стабильность и эффективное развитие, а также уменьшить масштабы *цифрового разрыва*. Для этих целей привлекаются в том числе представители частного капитала – включая зарубежный[118].

---

[115] Middle East & Africa Enterprise Resource Planning (ERP) Software Market Size // Fortune Business. URL: https://www.fortunebusinessinsights.com/middle-east-africa-enterprise-resource-planning-erp-software-market-107426; Middle East and Africa Treasury Software Market – Industry Trends and Forecast to 2030 // Data Bridge Market. URL: https://www.databridgemarketresearch.com/reports/middle-east-and-africa-treasury-software-market

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

[117] Согласно замерам GSMA, к 2023 г. доля интернет-пользователей в странах АЮС, на постоянной основе использующих мобильный интернет, превысила показатель в 30 млн человек. При этом общая емкость рынка мобильного интернета (с точки зрения количества интернет-пользователей и плотности интернет-покрытия) составляет более 200 млн человек. См.: The State of Mobile Internet Connectivity 2023. Sub-Saharan Africa key trends // GSMA. URL: https://www.gsma.com/r/wp-content/uploads/2023/10/State-of-Mobile-Internet-Connectivity-2023-Sub-Saharan-Africa.pdf; 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/

[118] TowerCo of Africa Uganda Secures $40 Million Investment to Expand Rural Mobile Network Coverage // Empower Africa. 10.03.2024. URL: https://empowerafrica.com/towerco-of-africa-uganda-secures-40-million-investment-to-expand-rural-mobile-network-coverage/

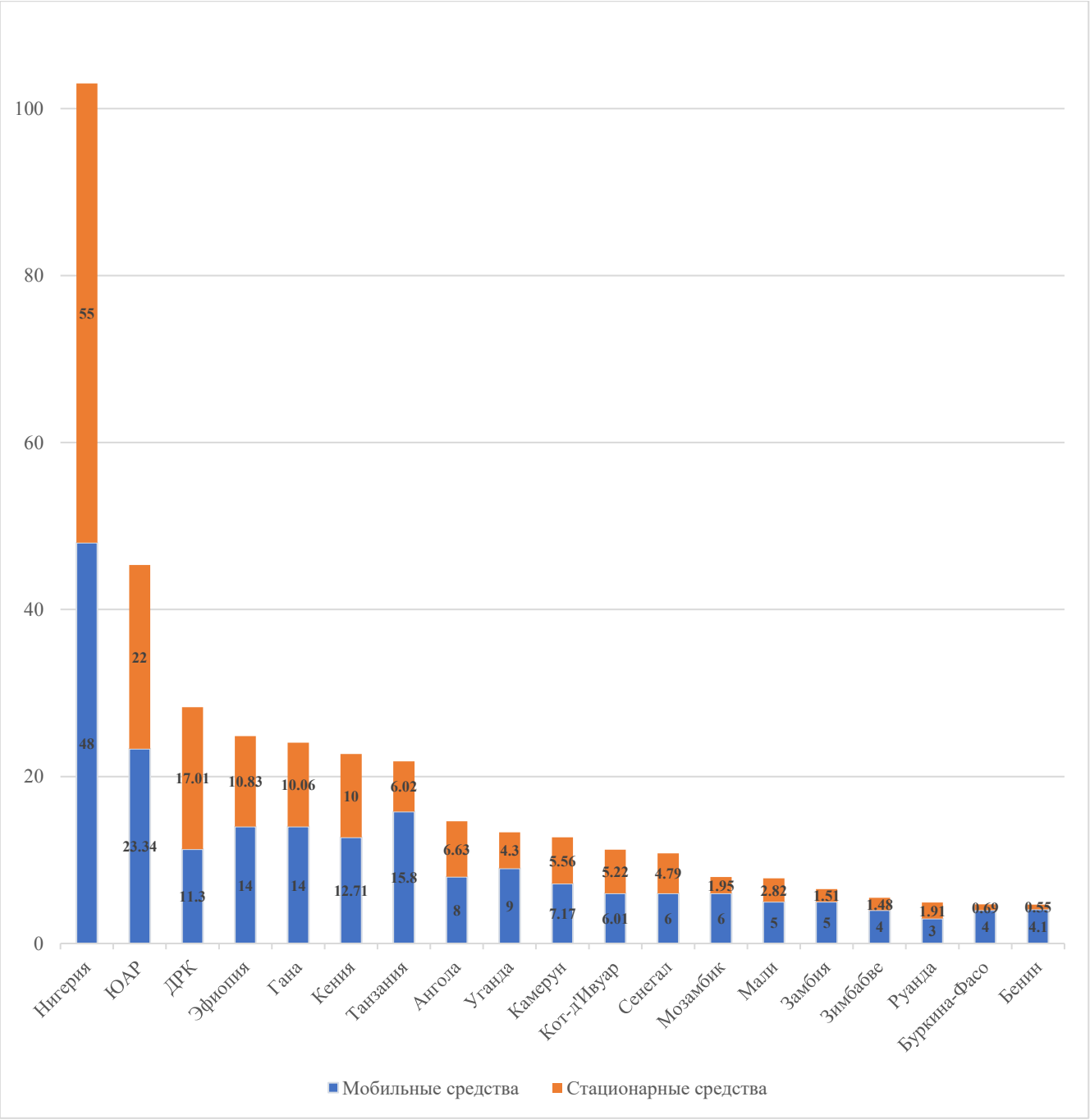

Диаграмма 6. Примерное соотношение пользователей мобильного и стационарного Интернета (по состоянию на начало 2024 г., млн чел.). Составлено по: GMSA, Statista Markets Insights[119]

Рост финансирования рынка ПО позитивно сказывается на кадровом потенциале стран АЮС. За последние 4 года отмечен взрывной рост числа специалистов, занятых в этом секторе (*см. диаграмму* 7). Наибольшие темпы увеличения численности профессионалов зафиксированы в Нигерии, где прирост за период составил более 48%, а также в Кении

[119] The State of Mobile Internet Connectivity 2023. Sub-Saharan Africa key trends // GSMA. URL: https://www.gsma.com/r/wp-content/uploads/2023/10/State-of-Mobile-Internet-Connectivity-2023-Sub-Saharan-Africa.pdf; 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

(прирост – 46%)[120]. При этом лидером по числу национальных специалистов по-прежнему остается ЮАР (133,2 тыс. человек).

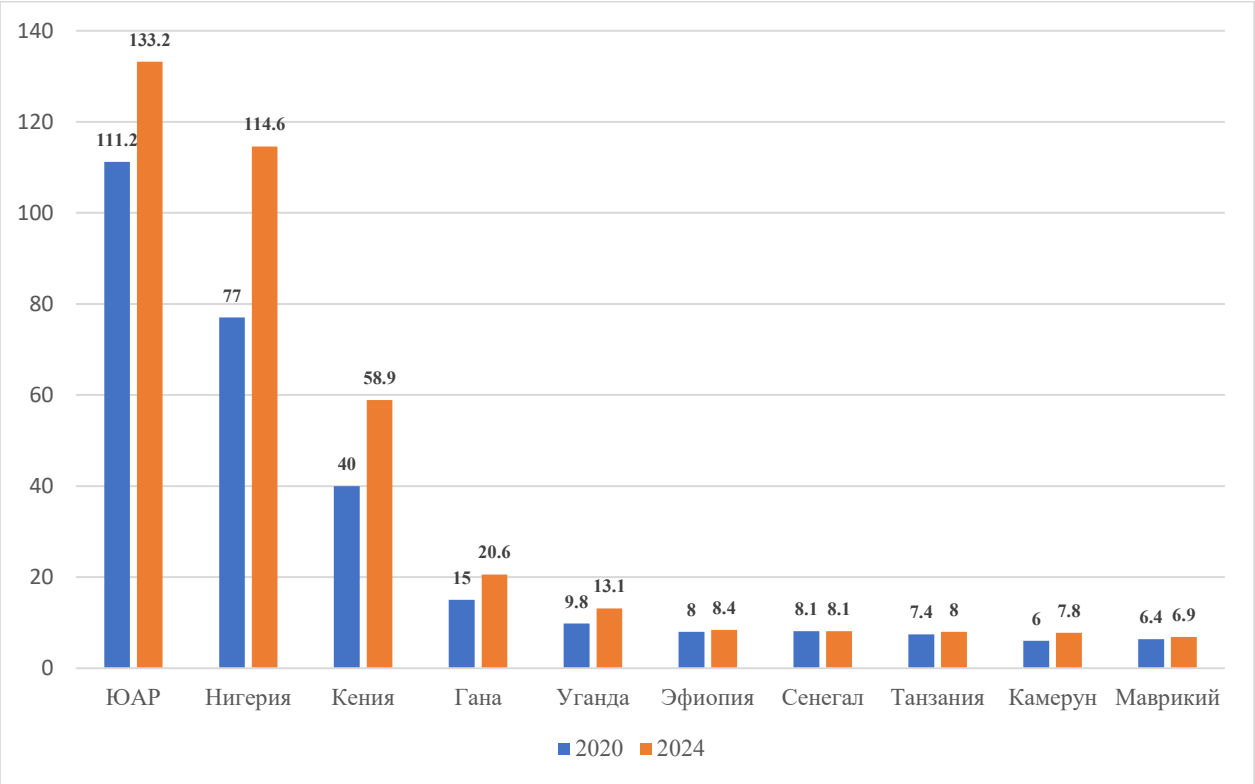

Диаграмма 7. Доля специалистов в области разработки ПО среди жителей стран АЮС (ТОП-10) – на начало 2020 г. и на начало 2024 г., в тыс. чел. Составлено по: Tunga[121], IFC[122].

Несмотря на значительный рывок вперед, рынок ПО стран АЮС продолжает сталкиваться с проблемами. Помимо общей экономической турбулентности (вооруженные конфликты, социально-политическая нестабильность и пр.), ограничивающей экономический рост части государств Субсахарской Африки, на отрасль крайне негативно влияет нарастающая с 2018 г. «утечка мозгов» из региона[123]. Попытки отдельных государств АЮС купировать проблему – например, посредством создания программ адаптации и кадровой мобильности внутри страны – оказывают временный эффект, но по-прежнему не решают проблему[124].

Кроме того, развитию национальных проектов во многом препятствует отсутствие достаточного финансирования стартап-разработок со стороны властей и склонность

[120] African Software Developers: Best Countries for Outsourcing in 2023 // Tunga. URL: https://tunga.io/african-software-developers/

[121] African Software Developers: Best Countries for Outsourcing in 2023 // Tunga. URL: https://tunga.io/african-software-developers/; Research: Africa offers Attractive Tech Talent Sourcing Options // Tunga. URL: https://tunga.io/research-africa-offers-attractive-tech-talent-sourcing-options/; Tech Hiring in 2024: Demand for IT Talent in the US // Tunga. URL: https://tunga.io/tech-hiring-in-2024-demand-for-it-talent-in-the-us/

[122] La technologie numérique pour favoriser la croissance des entreprises africaines // IFC. 12.06.2024. URL: https://www.ifc.org/fr/podcasts/audio-stories/2024/leveraging-digital-tech-for-african-business-growth; Opportunités du numérique dans les entreprises africaines // IFC. 16.05.2024. URL: https://www.ifc.org/fr/insights-reports/2024/digital-opportunities-in-african-businesses

[123] Kweitsu R. Brain drain: a bane to Africa's potential // Mo Ibrahim Foundation. 09.08.2018. URL: https://mo.ibrahim.foundation/news/2018/brain-drain-bane-africas-potential; Can West Africa Curb Its Brain Drain? // Council on Foreign Relations. URL: https://www.cfr.org/podcasts/can-west-africa-curb-its-brain-drain и др.

[124] См., напр.: Labour market: Brain drain in Ghana’s tech industry // Resilient Digital Africa. 25.11.2023. URL: https://resilient.digital-africa.co/en/blog/2023/11/25/labour-market-brain-drain-in-ghanas-tech-industry/

отдавать приоритет готовым решениям от зарубежных производителей. На данном этапе африканский технобизнес пока не способен конкурировать с китайскими, американскими и европейскими IT-гигантами, хотя попытки нарастить собственный *удельный вес* со стороны африканских фирм-разработчиков продолжаются.

1.3. Цифровой ландшафт Персидского Залива и АЮС: обобщая тренды

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», 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 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.

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).

Открытым для обоих регионов остается и феномен значительной спонсорской помощи от передовых игроков (о чем будет подробнее сказано в Разделе 3) – 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.

Раздел 2. Анализ текущего присутствия России в регионе, выявление сильных и слабых сторон выбранной стратегии действий

2.1. Регион «Персидский залив+»

С течением времени регион «Персидский залив+» играет все более значимую роль во внешней политике России. Уровень вовлеченности Москвы в процессы цифровизации и в развитие сектора кибербезопасности в странах данной группы к настоящему времени можно охарактеризовать как имеющий потенциал к росту.

В последние годы, особенно после принятия новой концепции внешней политики РФ (2023 г.)[125] и корректировки внешнеполитического курса, в рамках которого проблема безопасности в зоне Персидского залива вошла в число ключевых приоритетов на ближневосточном направлении, Россия заметно нарастила контакты с монархиями Залива (в первую очередь, ОАЭ и Саудовской Аравией), а также расширила стратегический диалог с Ираном – стороны финализировали работу над подготовкой Договора о всеобъемлющем стратегическом партнерстве, который был подписан в Москве в начале 2025 г.[126]. На высоком уровне развивается комплексное взаимодействие с Ираком, где технологии являются одни из ключевых проводников интересов Москвы[127].

Москва, в целом, позитивно оценивает курс стран региона Персидского залива на повышение взаимного доверия в цифровом секторе и предлагает собственные проекты в области региональной безопасности (включая киберсегмент).

Большое внимание традиционно отводится как технико-технологическому, так и социальному аспектам ***информационной безопасности***, что находит отражение в документах стратегического планирования. Так, согласно положениям «Стратегии развития отрасли связи в России на 2024-2035 годы» (2023 г.)[128] и «Основ государственной политики РФ в области международной информационной безопасности» (2021 г.)[129], Москва нацелена на укрепление технологического суверенитета (например, путем создания инструментов определения страновой принадлежности IP-адресов для защиты *цифровых границ* государства) с последующим распространением позитивного опыта на дружественные страны, а также на развитие международного сотрудничества в области

[125] Концепция внешней политики Российской Федерации (утверждена Президентом Российской Федерации В.В.Путиным 31 марта 2023 г.) // МИД РФ. 31.03.2023. URL: https://mid.ru/ru/foreign_policy/official_documents/1860586/

[126] Договор о всеобъемлющем стратегическом партнёрстве между Российской Федерацией и Исламской Республикой Иран // Президент РФ. 17.01.2025. URL: http://www.kremlin.ru/supplement/6258

[127]На что может опереться мягкая сила России в Ираке // Ведомости. 18.07.2024. URL: https://www.vedomosti.ru/politics/articles/2024/07/18/1050691-na-chto-mozhet-operetsya-myagkaya-sila-rossii-v-irake

[128] Распоряжение Правительства РФ от 24 ноября 2023 г. № 3339-р «Об утверждении Стратегии развития отрасли связи Российской Федерации на период до 2035 года» // Правительство РФ. 24.11.2023. URL: http://static.government.ru/media/files/Pc7fHuejbNvqv17b0RJNv0RIqTo20lUV.pdf

[129] Основы государственной политики Российской Федерации в области международной информационной безопасности // Совет Безопасности РФ. URL: http://www.scrf.gov.ru/security/information/document114/

противодействия организованной киберпреступности и кибертерроризму; повышение общего уровня доверия в киберпространстве.

Активную роль играет бизнес-сообщество: российские IT-компании стремятся расширить присутствие в нише цифровой безопасности, предлагая Ирану и аравийским монархиям передовые решения в области защиты данных. Разумеется, доля российских компаний на рынке региона по-прежнему не слишком велика[130], а в некоторых случаях еще и демонстрирует снижение – чему способствует санкционное противодействие со стороны США и ряда европейских стран (*см. диаграмму 8*).

С другой стороны, в ряде случаев отмечен существенный рост показателей – почти в 2 раза увеличилась доля российских компаний, занятых в цифровом секторе Ирана (в том числе за счет запуска совместных проектов). Примерно в полтора раза вырос российский сегмент на рынке ОАЭ, что обусловлено массовым открытием представительств IT-бизнеса в стране во второй половине 2023 г.[131]. В обоих случаях рост показателей, вероятно, продолжится и дальше, так как и Тегеран, и Абу-Даби настроены на развитие бизнес-коммуникации и расширение пула поставщиков технологий.

Интересен также кейс Кувейта. 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*[132], запущенного российскими IT-специалистами в 2023 г., повысил привлекательность услуг отечественных компаний – в первую очередь работающих в сфере финансовых технологий. Это обусловило некоторый рост представленности российских компаний на рынке Кувейта по итогам второго периода.

Резко (почти в два раза) сократилось присутствие российского технологического бизнеса на рынке Саудовской Аравии – хотя отечественные IT-продукты пользуются стабильным спросом со стороны Эр-Рияда, а российско-саудовское цифровое сотрудничество имеет восходящий вектор[133]. Снижение прямого участия обусловлено возросшим давлением на Саудовскую Аравию со стороны Вашингтона. США продолжают использовать политические и экономические рычаги, чтобы снизить влияние российских и китайских компаний на рынках Залива, и тем самым обеспечить доминирование американских поставщиков. При этом Эр-Рияд, с высокой долей вероятности, продолжает покупать необходимые технологии у оппонентов Вашингтона – однако уже при посредничестве других стран региона.

В остальных случаях (Катар, Оман, Ирак) колебания показателей куда менее значительны и находятся в пределах 1%.

---

[130] 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/

[131] IT-бизнес представил себя в ОАЭ // Коммерсантъ. 17.08.2023. URL: https://www.kommersant.ru/doc/6162039

[132] 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

[133] Российские ИТ и Smart City инновации в Саудовской Аравии: новый виток сотрудничества // Ведомости. 28.05.2024. URL: https://www.vedomosti.ru/press_releases/2024/05/28/rossiiskie-it-i-smart-city-innovatsii-v-saudovskoi-aravii-novii-vitok-sotrudnichestva

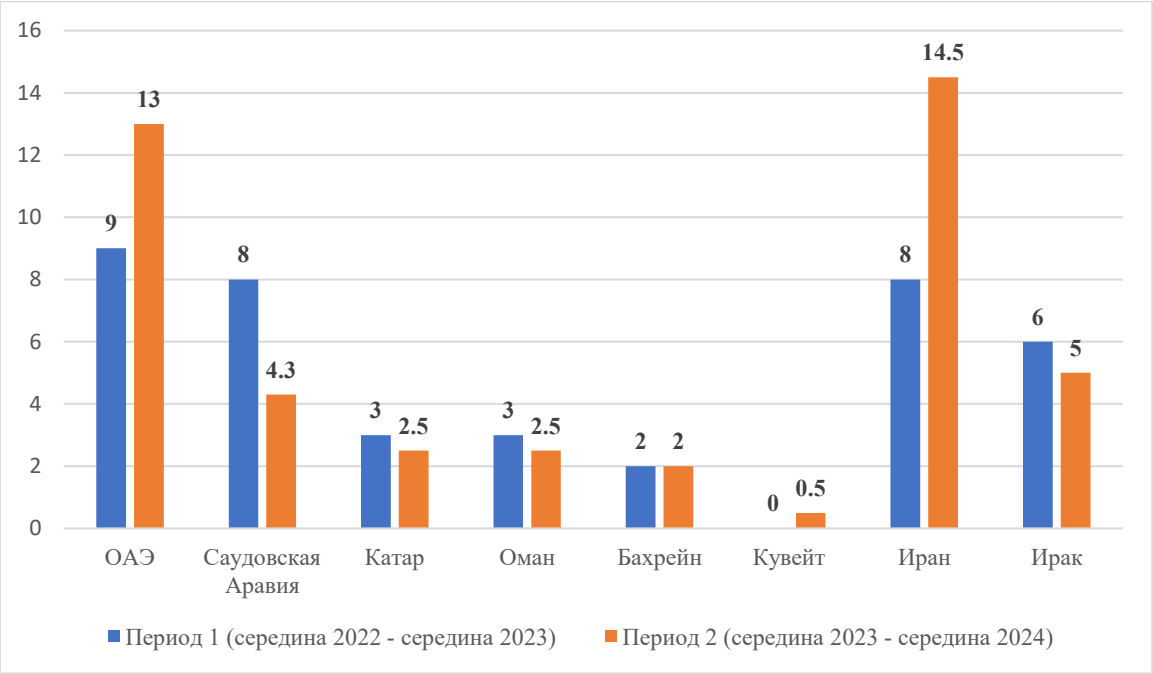

Диаграмма 8. Примерная доля российских компаний на рынке стран группы «Персидский залив+» в двух периодах, %. Составлено по: Global Database[134].

С точки зрения сотрудничества в области ***финансовых технологий***, Россия и страны Персидского залива пока не вышли на высокие позиции: взаимодействие носит «адресный» характер, хотя Москва в перспективе и рассчитывает дополнительно активизировать усилия в области финтеха – с опорой на регион Ближнего Востока в целом.

Промежуточной «точкой старта» для российских FinTech-компаний может стать пространство СНГ – в частности, рынки Узбекистана и Киргизии. По оценкам экспертов, динамично развивающийся рынок цифровых услуг этих стран позволит не только апробировать технические решения, нацеленные на Исламский мир (в частности, исламский цифровой банкинг), но и обеспечить приобщение к российским техническим продуктам представителей бизнеса аравийских монархий, чье присутствие на пространстве СНГ в последние годы растет[135].

Следует отметить, что хорошие перспективы развития сотрудничества наблюдаются в области ***криптовалютной торговли***. После легализации данной отрасли в России в августе 2024 г.[136] Москва нацелилась на достижение лидерства в этой сфере, что было подчеркнуто на самом высоком уровне[137]. А с учетом того, что страны группы «Персидский залив+», за редким исключением, проявляют интерес к развитию систем обращения с криптоактивами, данное направление в перспективе может стать полем активного взаимодействия – тем более, что Центробанки России и стран региона ищут варианты дедолларизации внешнеторговых сделок[138].

---

[134] Global Database. URL: https://www.globaldatabase.com/

[135] Содружество независимых клиентов // Коммерсантъ. 20.09.2023. URL: https://www.kommersant.ru/doc/6223281

[136] Путин подписал закон о криптовалютах // РБК. 08.08.2024. URL: https://www.rbc.ru/crypto/news/66b4c0f99a7947f7a51154dd

[137] Путин назвал Россию одним из мировых лидеров по майнингу криптовалют / РБК. 05.09.2024. URL: https://www.rbc.ru/crypto/news/66d96fde9a794711214056d2

[138] Набиуллина сфокусирует страны БРИКС на новых формах расчетов // Независимая газета. 30.01.2024. URL: https://www.ng.ru/economics/2024-01-30/4_8935_problems.html

Концепция разработки и внедрения *стейблкоинов* (цифровых активов, чей курс привязан к устойчивой фиатной единице – например, к доллару или евро[139]) для стимулирования обменов активами между Россией и странами Залива также вызывает все большую заинтересованность у региональных игроков. Помимо Ирана, который уже вовлечен в профильные разработки, интерес к проекту проявляют Саудовская Аравия, ОАЭ и Оман.

Не исключено, что разработка совместных цифровых активов продолжится под эгидой БРИКС – 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[140]. 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[141]. Эта тема также стала одной из магистральных на саммите БРИКС в Казани, который прошел в октябре 2024 г.[142].

Отдельно следует сказать о перспективах сотрудничества России и государств группы «Персидский залив+» в области ***искусственного интеллекта***. Руководствуясь положениями обновленной версии «Национальной стратегии развития ИИ» (2024 г.)[143], Москва заметно усилила внимание к вопросам ответственного использования ИИ-технологий и намерена на международном уровне продвигать свои подходы к обеспечению информационной безопасности в сфере ИИ, что отразилось и на тактике взаимодействия: пункты, связанные с реагированием на порождаемые искусственным интеллектом угрозы и вызовы, в том или ином виде фигурируют во всех профильных соглашениях между Россией и зарубежными странами.

При этом, с точки зрения экспорта российских решений в регион, к концу 2024 г. Москвой создан сравнительно неплохой задел (*см. Таблицу 6)*. Несмотря на то, что профильные соглашения к настоящему моменту подписаны только с двумя странами (Саудовская Аравия, Иран), научное и бизнес-сотрудничество налажено почти со всеми державами региона (за исключением Кувейта, где доминирует американская школа развития ИИ).

---

[139] Что такое стейблкоины и насколько рискованно хранить в них капитал // Forbes. 17.05.2022. URL: https://www.forbes.ru/investicii/465377-cto-takoe-stejblkoiny-i-naskol-ko-riskovanno-hranit-v-nih-kapital

[140] В Кремле заявили о планах создания в БРИКС платежной системы на блокчейне // РБК. 05.03.2024. URL: https://www.rbc.ru/crypto/news/65e6c0a69a7947a2f97dc580

[141] Кремль анонсировал создание в БРИКС платежной системы на блокчейне // ИТАР-ТАСС.05.03.2024. URL: https://tass.ru/ekonomika/20154635

[142] 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

[143] Указ Президента Российской Федерации от 15.02.2024 № 124 «О внесении изменений в Указ Президента Российской Федерации от 10 октября 2019 г. № 490 "О развитии искусственного интеллекта в Российской Федерации" и в Национальную стратегию, утвержденную этим Указом». URL: http://publication.pravo.gov.ru/document/0001202402150063

Страна	Соглашение о сотрудничестве	Совместные проектные площадки в области ИИ	Совместные научные исследования	Государственно-частное партнерство	Интенсивность контактов
Саудовская Аравия	Да	Да	Нет	Да	Средняя
ОАЭ	Нет	Да	Да	Да	Средняя
Катар	Нет	Нет	Нет	Да	Ниже среднего
Оман	Нет	Нет	Да	Нет	Ниже среднего
Бахрейн	Нет	Нет	Нет	Да	Низкая
Кувейт	Нет	Нет	Нет	Нет	Низкая
Иран	Да	Да	Да	Да	Высокая
Ирак	Нет	Нет	Да	Нет	Низкая

Таблица 6. Характеристика взаимодействия РФ и стран группы «Персидский залив+» в вопросах развития сферы искусственного интеллекта (по состоянию на середину 2024 г.). Составлено по открытым источникам.

Учитывая, что экономики государств рассмотренного региона по-прежнему довольно сильно ориентированы на нефтегазовый сектор, перспективным направлением сотрудничества может стать разработка ИИ-решений для нефтегазодобывающих предприятий, а также предоставление консультационных услуг по налаживанию производственных процессов[144].

С другой стороны, несмотря на укрепление позиций, Москва по-прежнему отстает в ряде сфер от Пекина и Вашингтона, которые используют экономические (китайский мегапроект «Один пояс, один путь») или военно-политические (стратегическое партнерство с арабскими странами, санкционные инструменты в отношении Ирана) для укрепления позиций на внутренних рынках стран Ближнего Востока. Этот фактор проявляется во всех сферах цифрового сотрудничества, и его необходимо учитывать при выработке стратегии взаимодействия со странами группы.

2.2. Регион Африки южнее Сахары

Подход России к выстраиванию отношений с Африканским континентом в последние годы характеризуется гибкостью, а интенсивность контактов между Москвой и странами региона – устойчивым ростом.

Руководствуясь идейными ориентирами, заложенными в рамках диалогового формата «Россия – Африка» в 2019 г., стороны стремятся увеличить число охватываемых в рамках многостороннего диалога направлений взаимодействия. Это, в контексте продолжающейся внешнеполитической переориентации государств региона, формирует возможности для наращивания дальнейшего взаимодействия.

[144] Искусственный интеллект проник в сферу нефтегаза // ComNews. 12.09.2024. URL: https://www.comnews.ru/content/235151/2024-09-12/2024-w37/1008/iskusstvennyy-intellekt-pronik-sferu-neftegaza

Наиболее интенсивный диалог наблюдается в секторе ***цифровой безопасности*** – с преобладанием внимания к технико-технологической составляющей защиты. Цифровая среда в африканском регионе развивается стремительно, однако отсутствие надлежащих мер по обеспечению кибербезопасности, вкупе с низким уровнем осведомленности части населения о специфике цифровых угроз и инертностью профильной законодательной базы, формируют устойчивый спрос на инструменты киберзащиты[145].

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)[146], ее практический опыт (особенно в части совершенствования национального потенциала и нормативно-правовой деятельности) востребован.

Согласно последним замерам ИБ-компаний, Россия является одной из самых атакуемых хакерами стран мира: за первое полугодие 2024 г. было выявлено 676 000 событий, связанных с попытками нарушить информационную безопасность[147], и показатель продолжает расти. Официальные лица РФ прогнозируют, что к 2030 г. российская цифровая инфраструктура будет подвергаться атакам каждые две секунды[148].

Кроме того, продолжает увеличиваться число попыток скомпрометировать ключевые государственные сервисы и информационные ресурсы. По данным *F.A.C.C.T.*, во II квартале 2024 года девять прогосударственных APT-групп вели кампании против организаций в России и СНГ. Несколько из них по ряду косвенных признаков можно отнести к проукраинским группам, другие — к азиатским и, предположительно, китайским[149].

При этом Москва сохраняет в целом позитивный настрой: отечественные ИБ-специалисты регулярно отрабатывают навыки на киберполигонах. Проведено более 50 масштабных киберучений и отражено более 10 миллионов учебных информационных атак[150].

В этом контексте российский опыт защиты КИИ в условиях растущего давления извне привлекает внимание африканских партнеров – особенно в разрезе вопросов безопасности финансового сектора, доля атак против которого по итогам 2023 г. достигла 18% (*см. рис.3*).

---

[145] 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/

[146] 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

[147] Количество кибератак на российские компании в первом полугодии выросло на 10% // Ведомости. 24.07.2024. URL: https://www.vedomosti.ru/technology/articles/2024/07/24/1051724-kolichestvo-kiberatak-na-rossiiskie-kompanii-viroslo

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

[149] Атаки запишем: хакеры-профи продолжают нападать на организации в России // Forbes. 15.07.2024. URL: https://www.forbes.ru/tekhnologii/516694-ataki-zapisem-hakery-profi-prodolzaut-napadat-na-organizacii-v-rossii

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

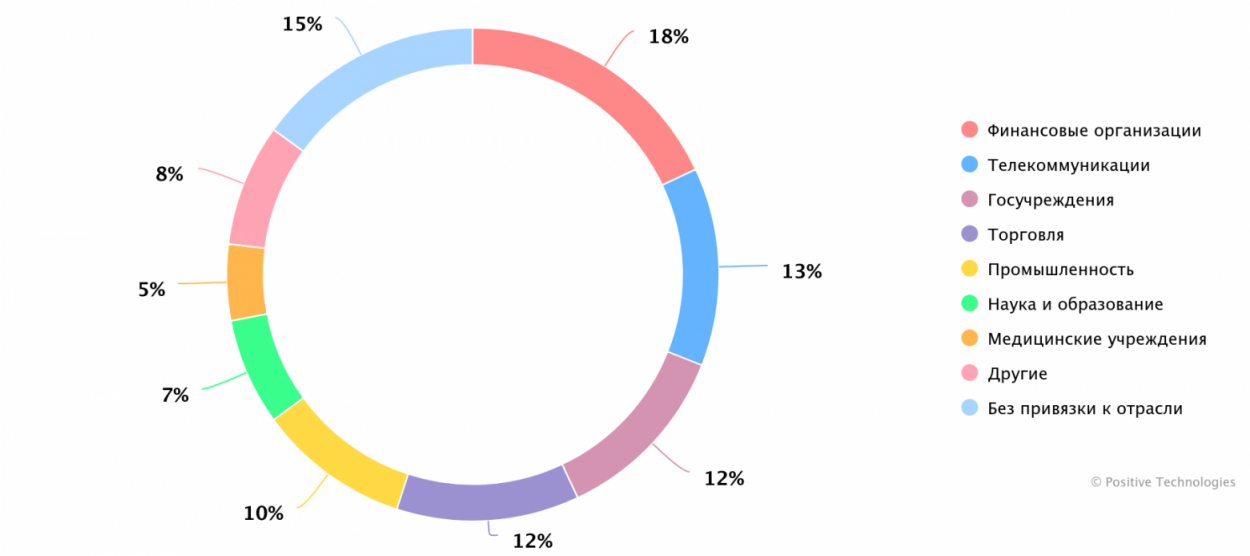

Рис.3. Категории жертв хакерских атак среди организаций стран Африки (по итогам 2023 г.). Источник: Positive Technologies[151].

Проблема низкого уровня защищенности в Африке настолько серьезна, что кибербезопасность второй год подряд признается первым фактором риска в финансовом секторе. Почти каждый руководитель африканского крупного финучреждения считает киберпреступность такой же опасной угрозой для региона, как и политическую и социальную нестабильность, а также непростые макроэкономические условия[152]. Это определяет негласные приоритеты сотрудничества России и стран АЮС по развитию системы киберзащиты.

Социальное измерение цифровой безопасности также не остается без внимания. В данном случае Москва ставит *во главу угла* идею «цифрового суверенитета», позиционируя его как важный элемент национальной безопасности и цифровой трансформации в целом[153].

Россия, наравне с Индией, является одним из наиболее активных и последовательных критиков *цифрового неоколониализма*, отстаивая права африканских стран на самостоятельное определение трека технологического развития и выбор круга партнеров[154]. Руководствуясь этими идеями, российская сторона строит диалог с регионом с опорой на такие столпы как укрепление безопасной цифрой среды, гармонизация законодательства, развитие национального кадрового потенциала и пр.[155].

---

[151] 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/

[152] African Financial Industry Barometer // AFIS Africa. URL: https://www.afis.africa/wp-content/uploads/2023/04/EN_Barometer-AFIS-2022-VF-Clean-Corrigee-1.pdf

[153] 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/

[154] 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/

[155] Суэф К. Цифровизация как способ преодоления неравенства в Африке // Россия в глобальной политике. 31.01.2024. URL: https://globalaffairs.ru/articles/czifrovizacziya-v-afrike/

Следует отметить, что усилия Москвы по поддержке «цифрового суверенитета» стран АЮС получают, в целом, позитивный отклик со стороны региона – данная тема, среди прочего, затрагивалась на профильной сессии международного форума *PHDays*, посвященного вопросам информационной безопасности в 2024 г.[156].

Обоюдный интерес у Субсахарских африканских стран и России вызывает совместная разработка решений в области ***финансовых технологий***. Бурное развитие этой отрасли на континенте и появление первых самостоятельных крупных игроков, экспортирующих собственные FinTech-решения за рубеж (Нигерия), открывает широкие возможности для реализации многосторонних проектов. Наиболее перспективными направлениями взаимодействия видятся разработка решений по автоматизации государственного сектора (система сбора и отслеживания налогов, электронный документооборот и пр.), а также инструментов обработки больших данных.

С легализацией криптовалютных операций открываются значительные перспективы экономического сотрудничества со странами АЮС – тем более, что африканский рынок цифровых активов занимает лидирующие позиции по темпам распространения и использования криптовалют[157].

Российские специалисты склонны рассматривать либерализацию российского подхода к использованию цифровых активов как инвестицию в международную торговлю с дружественными странами и способ преодоления некоторых специфических препятствий. Например, как отмечает гендиректор Консалтингово-аналитического союза Артем Генкин, использование цифровых финансовых активов (ЦФА) способно значительно расширить объем торговли между Россией и странами Субсахарской Африки, поскольку платежеспособный спрос со стороны африканских контрагентов существует, но он зачастую выражен в неденежной форме. Он может быть представлен имеющимися активами, в том числе полезными ископаемыми[158].

При этом конкретный механизм расчетов может быть реализован через выпуск цифровых финансовых активов, номинированных в рублях, иностранными (африканскими) эмитентами под имеющиеся у них запасы добываемых или приобретенных ими полезных ископаемых, на российских площадках с участием российских операторов по обмену ЦФА и операторов информационных систем. Эти ЦФА могут использоваться для оплаты поставок товаров в Африку российскими экспортерами, равно как и африканскими – за поставку своих товаров в Россию.

Российские опыт развития сервисов цифровых государственных услуг традиционно пользуется спросом. Наибольший интерес у африканских партнеров по-прежнему вызывают технологические решения, связанные со сферами налогообложения,

[156] Соответствующие ремарки в рамках сессии в том или ином виде сделали представители Уганды, Эфиопии, Камеруна и Буркина-Фасо. См.: Суверенитет кибербезопасности: промышленный и национальный уровень // Positive Events. 26.05.2024. URL: https://www.youtube.com/watch?v=MLFKCOyoJmA

[157] Согласно отчету CVVC за 2023 год, на долю Африки в настоящее время приходится 1,8% всего глобального финансирования блокчейнов. См.: Blockchain Industry Research Reports // CVVC. URL: https://www.cvvc.com/insights

[158] Как в африканских странах осваивают криптовалюту и поможет ли это торговле с Россией // Forbes. 11.03.2024. URL: https://www.forbes.ru/finansy/507561-kak-v-afrikanskih-stranah-osvaivaut-kriptovalutu-i-pomozet-li-eto-torgovle-s-rossiej

здравоохранения и правосудия; регулирования таможенных процессов – в случае с государствами АЮС данные направления, как правило, представлены наименьшим количеством интегрированных сервисов, и активизация взаимодействия может в перспективе помочь устранить данный дисбаланс[159].

С другой стороны, важно помнить, что Россия – не единственный перспективный поставщик цифровых технологий на Континент. Активным игроком и экспортером технологий в АЮС является КНР: Пекин за последнее десятилетие существенно нарастил объемы инвестиций в Континент (в т.ч. под эгидой проекта «Цифрового Шелкового пути»), обеспечив себе устойчивую нишу на рынке цифровых решений[160]. Кроме того, начиная с 2017 г., аналогичные усилия предпринимает и Индия, позиционирующая цифровизацию в качестве одного из драйверов диалога с Африкой[161]. И хотя текущий уровень конкуренции между Москвой, Нью-Дели и Пекином не является критичным, в перспективе он, вероятно, будет нарастать.

Рынок ***технологий искусственного интеллекта*** в странах АЮС рассматривается Москвой как потенциальная точка интенсивного сотрудничества. Россия готова делиться со странами Африки технологиями внедрения искусственного интеллекта – речь как об опыте реализации экспериментальных правовых режимов, так и о внедрении лучших бизнес-практик при участии российских компаний[162].

Сотрудничество в рамках госсектора ориентировано, в первую очередь, на содействие африканским странам в вопросах гармонизации профильного законодательства и разработку (в некоторых случаях – актуализацию) документов стратегического планирования[163]. Примечательно, что профильная работа ведется со значительной оглядкой на упомянутый выше «цифровой суверенитет» африканских стран[164]. В этой трактовке вопрос развития сферы искусственного интеллекта рассматривается как неотделимый от остального сектора цифровой безопасности.

Говоря о сотрудничестве в бизнес-секторе по профилю ИИ, резонно упомянуть созданный в 2019 г. Альянс в сфере искусственного интеллекта, основателями которого являются крупные игроки российского цифрового рынка (Сбер, Яндекс и др.), а также зарубежные компании-партнеры[165]. Альянс декларирует в числе основных целей комплексную работу по развитию технологий искусственного интеллекта и продвижение этического подхода к его использованию.

---

[159] На форуме Россия-Африка обсудили перспективы сотрудничества в области цифровых технологий // Минцифры. 18.04.2023. URL: https://platform.gov.ru/news/na-forume-rossiya-afrika-obsudili-perspektivy-sotrudnichestva-v-oblasti-czifrovyh-tehnologij/

[160] Questioning The Future Of Africa's Digital Sovereignty, Powered By China // Analytics India. 22.12.2021. URL: https://analyticsindiamag.com/questioning-the-future-of-africas-digital-sovereignty-powered-by-china/

[161] Africa-India Partnerships: E-governance identified as a key enabler of Africa's transformation // AFDB. 31.05.2017. URL: https://www.afdb.org/en/news-and-events/africa-india-partnerships-e-governance-identified-as-a-key-enabler-of-africas-transformation-17070

[162] Россия готова делиться со странами Африки опытом и лучшими практиками внедрения ИИ // Интерфакс. 13.04.2023. URL: https://www.interfax.ru/events/news/895892

[163] Africa's push to regulate AI starts now // Technology Review. 15.03.2024. URL: https://www.technologyreview.com/2024/03/15/1089844/africa-ai-artificial-intelligence-regulation-au-policy/

[164] Rio N. Russia's offensive on "digital sovereignty" in Africa // In-Cyber Portal. 12.04.2024. URL: https://incyber.org/en/article/russias-offensive-on-digital-sovereignty-in-africa/

[165] Альянс в сфере искусственного интеллекта. URL: https://a-ai.ru/#about

Участниками формата разработан Кодекс этики в сфере искусственного интеллекта (2021 г.), призванный обеспечить самостоятельное регулирование сектора ИИ на основе открытости и сотрудничества. По состоянию на конец 2024 г., его подписантами являются 820 компаний и организаций из 20 стран[166]. Из числа государств АЮС к Кодексу присоединились компании из Нигерии, Замбии, Сенегала, Уганды, Буркина-Фасо, Ганы, Мозамбика, Мали, Кении и ЮАР[167].

Наблюдаются также попытки использовать *политический бренд* БРИКС (куда входят ЮАР и Эфиопия) для более эффективного развития сотрудничества в секторе ИИ-технологий – в частности, участникам БРИКС предложено использовать искусственный интеллект при продвижении торгово-инвестиционного сотрудничества в рамках объединения[168].

Что касается совместной с африканскими странами ***разработки ПО***, то здесь по-прежнему сохраняются определенные сложности. В первую очередь, созданию совместных проектов в области разработки мешает санкционное давление со стороны США и европейских стран. Вашингтон и Брюссель на регулярной основе применяют тактику угроз вторичными санкциями за сотрудничество с РФ, что отпугивает значительное количество потенциальных партнеров[169]. Кроме того, российские разработки ПО пока уступают по уровню привлекательности американским и китайским предложениям, ввиду чего в диалоге России и стран АЮС по-прежнему преобладают другие направления сотрудничества (например, космические исследования, совместное развитие промышленного потенциала и др.).

С другой стороны, отмечены и позитивные сдвиги. Например, российские компании сделали ставку на участие в развитии национального кадрового потенциала стран Субсахарской Африки (включая сектор разработки ПО). В качестве площадок взаимодействия в данном случае выступают развернутые в странах региона технопарки[170]. Однако существенных качественных подвижек на данном направлении пока не отмечено.

---

[166] В рамках ТехКонгресса состоялось массовое подписание Кодекса этики в сфере ИИ // Альянс в сфере искусственного интеллекта. 18.06.2024. URL: https://a-ai.ru/?page_id=2634

[167] На форуме «Россия — Африка» к Кодексу этики искусственного интеллекта присоединились 15 зарубежных компаний // Альянс в сфере искусственного интеллекта.27.07.2023. URL: https://a-ai.ru/?page_id=2020

[168] Минэкономразвития: РФ предлагает БРИКС использовать ИИ в совместных проектах // URA.RU. 06.06.2024. URL: https://ura.news/news/1052777935

[169] Богданов М. США пытаются сорвать саммит Россия-Африка // Российский совет по международным делам. 27.02.2023. URL: https://russiancouncil.ru/analytics-and-comments/comments/ssha-pytayutsya-sorvat-sammit-rossiya-afrika/?sphrase_id=141024805

[170] Африканский разворот: какие проекты на континенте могут заинтересовать российский бизнес // ИТАР-ТАСС. 09.06.2023. URL: https://tass.ru/ekonomika/17966151

2.3. «Цифровое» присутствие России в регионах: обобщая тренды

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, 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 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.

При этом говорить о «балансе направлений» не приходится – наиболее востребованным для обоих регионов является опыт России по отражению массированных кибератак против КИИ, а также развития социального измерения цифровой безопасности; повышенным интересом пользуются отечественные FinTech и EGov-решения. При этом в сфере искусственного интеллекта и разработки программного обеспечения Москва пока находится на догоняющих позициях – хотя, благодаря 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*. 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. Разумеется, при использовании площадок БРИКС следует учитывать, что на данной площадке, помимо России, активно ведут *технологическое наступление* другие передовые державы (КНР, Индия и др.), использующие площадки объединения в своих (не всегда совпадающих с российскими) интересах. По этой причине уместно, помимо БРИКС, работать над развитием диалога и на других независимых площадках (например, продолжить развитие формата «Россия – Африка»).

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 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».

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.

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 пространства. 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.

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

Раздел 3. Выявление ключевых конкурентов Москвы в обозначенной сфере, оценка их текущих позиций и интересов

3.1. Регион «Персидский залив+»

США. Регион Персидского залива (включая его цифровую проекцию) остается зоной особых интересов США, что находит отражение в документах стратегического планирования (Стратегия по международному киберпространству и цифровой политике, Концепция кибердипломатии, Стратегия национальной безопасности и др.).

При продвижении своего подхода к ***кибербезопасности*** США апеллируют к концепции «цифровой солидарности» (под которой в Вашингтоне понимают *«готовность работать вместе над достижением общих целей, помогать партнерам наращивать потенциал и оказывать взаимную поддержку»*)[171]. При этом в этой же стратегии США открыто противопоставляют себя России и Китаю, которым отведена роль главных антагонистов и источников киберугроз, противостоять которым предполагается при содействии союзников и партнеров (включая представителей частного сектора).

Наиболее активно диалог в области кибербезопасности развивается с аравийскими монархиями – стратегическими союзниками Вашингтона на Ближнем Востоке. США вносят определяющий вклад в наращивание технологического и кадрового потенциала монархий Залива, а также в развитие индустрии кибербезопасности в целом, оказывая помощь в решении широкого круга профильных проблем – от совместной защиты банковских данных[172] до обмена информацией о киберугрозах в режиме реального времени (включая специфические направления – такие как киберзащита систем ПВО и морских батарей)[173]. Соответствующие договоренности достигнуты со всеми странами ССАГЗ.

При этом, с точки зрения частоты профильных контактов на передний план выдвигаются Саудовская Аравия и ОАЭ – на них приходится каждая четвертая профильная активность Вашингтона в регионе (*см. диаграмму 9*). Также активизация контактов наблюдается с Бахрейном, где расквартирован Пятый флот США.

Кроме того, примечательно, что активность США в диалоге с Эр-Риядом, Абу-Даби и Манамой заметно возросла. Это обусловлено как их вовлеченностью в асимметричный

[171] United States International Cyberspace & Digital Policy Strategy // US Dept of State. URL: https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/

[172] Treasury Announces Cyber Security Cooperation Memorandum of Understanding with the United Arab Emirates // US Dept. of Treasury. 16.10.2023. URL: https://home.treasury.gov/news/press-releases/jy1808

[173] U.S.-UAE Cybersecurity Cooperation Marks Needed Collaboration in the Region // FDD. 16.10.2023. URL: https://www.fdd.org/analysis/2023/10/16/u-s-uae-cybersecurity-cooperation-marks-needed-collaboration-in-the-region/; Readout of the New Round of U.S.-Gulf Cooperation Council Working Groups on Integrated Air and Missile Defense and Maritime Security // US Dept. of Defense. 14.02.2023. URL: https://www.defense.gov/News/Releases/Release/Article/3298553/readout-of-the-new-round-of-us-gulf-cooperation-council-working-groups-on-integ/

киберконфликт с Ираном (ОАЭ, Бахрейн)[174], а также комплексным развитием связей в военном секторе кибербезопасности в целом.

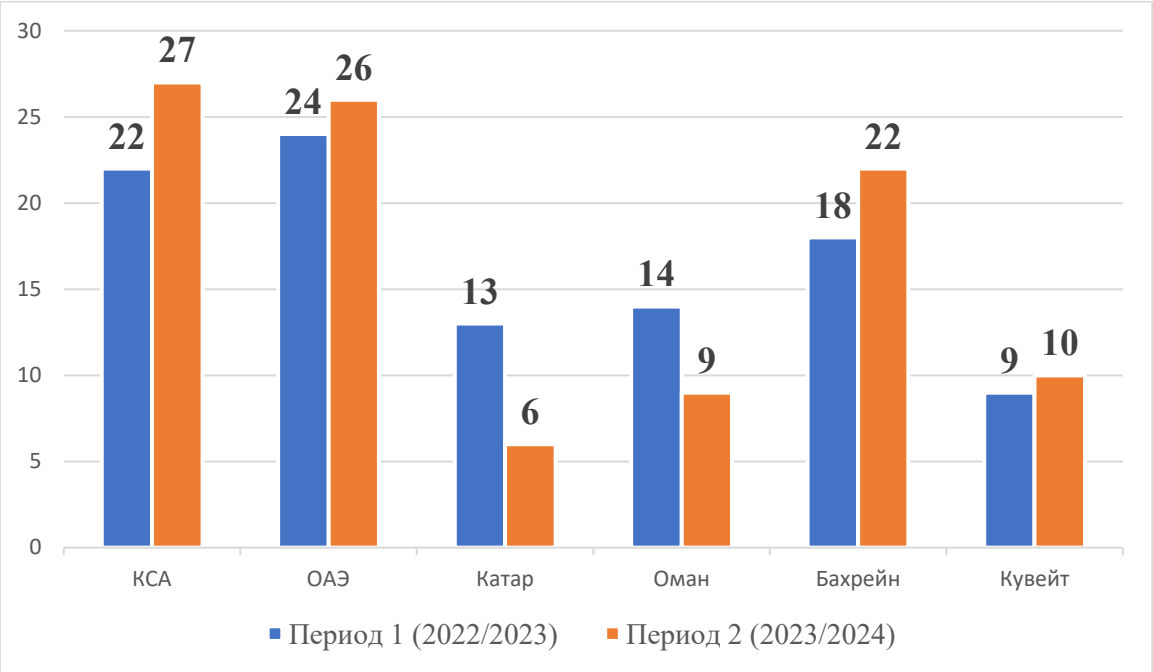

Диаграмма 9. Примерное соотношение доли контактов США и стран – членов ССАГЗ по вопросам сотрудничества в области кибербезопасности за аналогичные периоды (июль – июль) в 2022-2023 гг. и 2023-2024-гг, %. Составлено по официальным источникам[175].

Профильный диалог (пусть и заметно уступающий по интенсивности контактов показателям аравийских монархий) развивается с Ираком[176]. Де-факто сотрудничество основывается на *букве* Стратегического рамочного соглашения, заключенного между Вашингтоном и Багдадом в 2008 г.[177], ввиду чего сектор кибербезопасности не является ведущим в диалоге двух стран.

С другой стороны, в последние несколько лет США стремятся нарастить влияние на развитие иракской системы кибербезопасности, что заметно в том числе по тональности последних совместных заявлений Вашингтона и Багдада[178].

Рынок ***финансовых технологий*** тоже занимает весомое место в американской стратегии сохранения присутствия в регионе. Вашингтон поощряет сотрудничество национальных FinTech-компаний с фирмами аравийских монархий и национальными регуляторами (в том

[174] Несмотря на отсутствие эскалации в отношениях с официальным Тегераном, обе страны являются участниками «Соглашений Авраама» (2020/2021 г.) по нормализации отношений с Израилем; активно используют произведенное в Израиле ПО (включая средства киберразведки), а также предоставляют платформу для работы американских спецслужб против ИРИ, что делает их одной из возможных целей иранских контракций в киберпространстве.
[175] Для выведения показателей использованы данные, размещенные на официальных сайтах правительства и других ключевых государственных институтов США, а также публикации с сайтов министерств и ведомств аравийских монархий.
[176] U.S. Security Cooperation with Iraq // US Dept. of State. 16.07.2021. URL: https://www.state.gov/u-s-security-cooperation-with-iraq/
[177] Fact Sheet: The Strategic Framework Agreement and the Security Agreement with Iraq // George W. Bush (White House). 04.12.2008. URL: https://georgewbush-whitehouse.archives.gov/news/releases/2008/12/20081204-6.html
[178] Joint Statement on U.S.-Iraq Joint Security Cooperation Dialogue // US Embassy in Iraq. 24.07.2024. URL: https://iq.usembassy.gov/joint-statement-on-u-s-iraq-joint-security-cooperation-dialogue/

числе под эгидой совместных бизнес-советов[179]), а также продвигает экспорт американских технологических решений на Ближний Восток. Аналогичным образом ситуация складывается и в ***секторе разработки*** ПО, не связанном с цифровыми финансами, – несмотря на усиление позиций неамериканских поставщиков на рынках стран группы «Персидский залив+»[180], доля аффилированных с США киберкомпаний по-прежнему является преобладающей[181].

Само по себе доминирующее положение США на рынках цифровых технологий региона обусловлено глобальным технологическим лидерством страны, а также сохраняющимся за Вашингтоном статусом одного из главных *архитекторов* системы региональной безопасности на Ближнем Востоке и в зоне Персидского залива.

Также Вашингтон один из первых включился в гонку за право задавать глобальные тренды в области ***искусственного интеллекта*** (включая разработку модели его безопасного использования). В марте 2024 г. США внесли на рассмотрение в ООН первую в истории организации глобальную резолюцию по искусственному интеллекту, которую поддержали 123 страны (многие из которых – развивающиеся)[182]. В документе, среди прочего, подчеркивается необходимость «помогать развивающимся странам» и обеспечивать равный и справедливый доступ к преимуществам цифровой трансформации и безопасных систем ИИ.

Важную роль в продвижении американского подхода на глобальном уровне играют IT-гиганты, формирующие рамки будущего международного сотрудничества в области контроля ИИ. Так, в июле 2024 г. на Форуме по безопасности в Аспене Google и партнеры объявили о создании Коалиции по безопасному ИИ (CoSAI)[183]. В объединение также вошли Amazon, IBM, Microsoft, NVIDIA и OpenAI[184], что расширило возможности продвижения американского подхода к регулированию ИИ в других странах и регионах мира.

Вашингтон видит определенную долгосрочную выгоду в стремлении подавляющего большинства аравийских монархий стать *ИИ-сверхдержавами*[185], а потому поддерживает региональных партнеров за счет запуска совместных образовательных и научно-исследовательских проектов, а также формирования профильных рабочих групп. Однако здесь США вынуждены все больше соперничать с Китаем за право задавать тренды в области развития ИИ-технологий – особенно в частном секторе, где интенсивность конкуренции существенно выше[186].

---

[179] См., напр.: 24Fintech Conference (Supported Event) // US-Saudi Business Council. URL: https://ussaudi.org/24fintech-conference-supported-event/

[180] За исключением Ирана, где сотрудничество ограничено рамками санкционного режима.

[181] Посчитано по: Global Database. URL: https://www.globaldatabase.com/

[182] До этого вопросы регулирования ИИ-технологий уже косвенно затрагивались в проектах резолюций ГА ООН, посвященных вопросам кибербезопасности, однако данная резолюция стала первой, посвященной исключительно ИИ. См.: ГА ООН приняла первую резолюцию о регулировании искусственного интеллекта // ИТАР-ТАСС. 21.03.2024. URL: https://tass.ru/ekonomika/20309919

[183] Introducing the Coalition for Secure AI (CoSAI) and founding member organizations // Google. 18.07.2024. URL: https://blog.google/technology/safety-security/google-coalition-for-secure-ai/

[184] Ibidem.

[185] Why these Gulf states want to be AI superpowers // CNN. 16.09.2024. URL: https://edition.cnn.com/2024/09/16/middleeast/middle-east-artificial-intelligence-spc/index.html

[186] Navigating the US-China AI Race in the Gulf // Third Way. 11.10.2023. URL: https://www.thirdway.org/blog/navigating-the-us-china-ai-race-in-the-gulf

Следует отметить, что долгое время между Вашингтоном и Пекином существовало негласное *джентльменское соглашение* по участию в делах стран Персидского залива применительно к киберпространству и сектору высоких технологий в целом: США занимались развитием военных аспектов региональных союзников и созданием военной инфраструктуры (ориентированной в том числе на нужды НАТО), а КНР – гражданских, с упором на экономику и развитие государственно-частного партнёрство.

Однако с приходом администрации Байдена и ужесточением соперничества между двумя странами прежние договоренности постепенно перестали соблюдаться. Пекин существенно нарастил военную составляющую цифрового сотрудничества с аравийскими монархиями, а Вашингтон задействовал инструменты санкционного давления, чтобы искусственно ослабить позиции китайских IT-гигантов. А возвращение в Белый дом Дональда Трампа сулит лишь закрепление данного тренда.

Обобщенный показатель вовлеченности США представлен ниже (*см. таблицу 8*).

Страна	Цифровая безопасность	Цифровые технологии в экономике и госуправлении	ИИ-Технологии	Разработка ПО
КСА	4	4	4	4
ОАЭ	4	4	4	4
Катар	3	3	3	3
Кувейт	3	2	2	2
Бахрейн	4	4	2	2
Оман	3	2	2	2
Иран	0	0	0	0
Ирак	2	2	1	3

Таблица 8. Индекс вовлеченности в развитие системы цифровых технологий стран региона (по 5-балльной шкале)[187]. Составлено автором.

КНР. В отличие от США, сделавших основную ставку на военное измерение ***кибербезопасности***, КНР все еще отдает приоритет развитию гражданского сегмента. Быстрому продвижению Пекина на этом направлении во многом способствует сохраняющаяся связка действий китайского бизнеса в регионе с идеями глобальных инициатив «Один пояс, один путь» и «Цифровой Шелковый путь»[188].

КНР придерживается прагматичного подхода к международному цифровому сотрудничеству и стремится не допускать *белых пятен* в профильном диалоге. Во взаимодействие вовлечены не только аравийские монархии и Ирак, но и Иран, что делает положение Пекина в регионе более сбалансированным и устойчивым. При этом взаимодействие носит двухуровневый характер – диалог с международными площадками (ЛАГ, ССАГЗ, ОИС) сбалансирован активным взаимодействием в ГЧП-формате.

[187] 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.

[188] China’s Digital Silk Road taking its shot at the global stage // East Asia Forum. 09.05.2024. URL: https://eastasiaforum.org/2024/05/09/chinas-digital-silk-road-taking-its-shot-at-the-global-stage/

Большие перспективы дальнейшего укрепления влияния Китая в секторе ***ИИ-технологий.*** В июле 2024 г. ГА ООН была принята «китайская ИИ-резолюция», разработанная совместно с Россией[189]. В отличие от американской ИИ-резолюции, принятой в марте того же года, основной акцент в новом документе был сделан на международное сотрудничество – как элемент хеджирования цифровых рисков и сокращение цифрового неравенства. Китайскую резолюцию поддержали сразу 140 стран ООН (включая США и Россию), что превысило прежний рекорд (123 голоса поддержки за американский ИИ-проект)[190].

Кроме того, китайские специалисты в области ИИ в последнее время все чаще заявляют, что их национальная школа искусственного интеллекта начинает постепенно доминировать над американской, что выражается как в более эффективной модернизации процессов, так и повышении эффективности работы алгоритмов; росте глобального спроса на китайские ИИ-проекты. По их оценкам, Пекин станет абсолютным лидером ИИ-гонки уже к концу десятилетия[191].

Государства региона «Персидский залив+» в вопросах развития ИИ-технологий сегодня пытаются найти баланс между КНР и США – двумя ключевыми глобальными поставщиками профильных решений – однако с течением времени делать это становится все труднее – в том числе в силу попыток Вашингтона искусственно ограничить влияние Пекина на региональный рынок[192].

Китайские IT-компании сегодня занимают второе (после США) место в секторе экспорта готовых технологических решений в регион «Персидский залив+» – как в секторе ***финансовых технологий***, так и в части ***разработки ПО*** нефинансового назначения. Сотрудничество охватывает широкий спектр проектов в области цифровизации и киберзащиты, в том числе по развитию искусственного интеллекта, электронной торговли, криптовалюты, блокчейн-технологии и технологии, обеспечивающих безопасность трансграничных платежей, других элементов финансовой безопасности[193]. В секторе разработки ПО для работы с большими массивами данных, долгое время считавшимся «зоной исключительного влияния США» также наблюдается постепенное смещение инициативы в сторону Китая, главным образом за счет продолжающейся экспансии китайских образовательных платформ в странах региона[194].

Как уже отмечалось выше, рост влияния китайского технологического бизнеса на рынках региона в последние годы все больше ограничивается за счет вмешательства США и попыток Белого дома обеспечить дополнительное благоприятствование своим компаниям по сравнению с китайскими. Особенно ярко это проявляется в случае с аравийскими

[189] UN adopts Chinese resolution with US support on closing the gap in access to artificial intelligence // AP. 02.07.2024. URL: https://apnews.com/article/un-china-us-artificial-intelligence-access-resolution-56c559be7011693390233a7bafb562d1
[190] Ibidem.
[191] White J. China is writing its own rules on AI // Tortoise Media. 17.09.2024. URL: https://www.tortoisemedia.com/2024/09/17/china-is-writing-its-own-rules-on-ai/
[192] Gulf states balance China, US collaborations in AI space // Arab News. 17.04.2024. URL: https://www.arabnews.com/node/2494616
[193] China's Achilles' Heel in Relationship with Arab Gulf States // China-US Focus. 03.07.2024. URL: https://www.chinausfocus.com/foreign-policy/chinas-achilles-heel-in-relationship-with-arab-gulf-states
[194] China and the Middle East: A Strategic Convergence in AI // China Talk. 25.03.2024. URL: https://www.chinatalk.media/p/china-and-the-middle-east-a-strategic

монархиями, рост китайского влияния на которые Вашингтон трактует как вызов национальной безопасности и своим стратегическим интересам на Ближнем Востоке[195].

Несмотря на то, что США удалось добиться некоторых успехов на этом направлении (например, переориентировав ОАЭ на сотрудничество с американскими IT-гигантами в начале 2024 г.)[196], большинство аравийских монархий по-прежнему весьма плотно взаимодействует с Пекином по цифровым вопросам. Кроме того, КНР стремительно расширяет диалог с Ираном (как в рамках БРИКС, так и в двустороннем формате), повлиять на курс которого США не могут[197].

При этом слабой стороной китайского высокотехнологического бизнеса сегодня является его встроенность в мегапроекты Пекина. «Дипломатия чековой книжки», на которую делают ставку в КНР последнее десятилетие, имеет обратную сторону в виде *долговой ловушки* – когда в обмен на выгодные кредиты и содействие в развитии проектов Пекин получает влияние на внешнеполитические решения страны-партнера[198].

Учитывая стремление аравийских монархий позиционировать себя в качестве самостоятельных игроков, перспектива их возможного попадания в зависимость к кому-либо, ведет к всплеску алармистских настроений и снижает доверие к предлагаемым Китаем проектам. Кроме того, ужесточение соперничества КНР с США и попытки Вашингтона использовать политические инструменты для выдавливания китайского бизнеса с внутренних рынков государств Залива также оказывают влияние на итоговую вовлеченность Пекина в региональные дела.

Обобщенный показатель вовлеченности представлен ниже (*см. таблицу 9*).

Страна	Цифровая безопасность	Цифровые технологии в экономике и госуправлении	ИИ-Технологии	Разработка ПО
КСА	4	3	4	3
ОАЭ	4	3	4	3
Катар	2	3	4	4
Кувейт	2	1	3	2
Бахрейн	3	2	4	3
Оман	3	3	4	2
Иран	4	2	4	4
Ирак	2	3	3	3

Таблица 9. Индекс вовлеченности в развитие системы цифровых технологий стран региона (по 5-балльной шкале)[199]. Составлено автором.

[195] Stakes Rising In The US-China AI Race // Global Finance. 09.09.2024. URL: https://gfmag.com/economics-policy-regulation/us-china-competition-generative-ai/

[196] UAE's top AI group vows to phase out Chinese hardware to appease US // Financial Times. URL: https://www.ft.com/content/6710c259-0746-4e09-804f-8a48ecf50ba3

[197] Iran To Work With China To Create National Internet System // Radio Freedom. URL: https://www.rferl.org/a/iran-china-national-internet-system-censorship/30820857.html

[198] China's empire of debt: The Belt and Road Initiative // The New Arab. 07.01.2022. URL: https://www.newarab.com/analysis/chinas-empire-debt-belt-and-road-initiative

[199] 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.

Индия. Несмотря на то, что Индия осознала важность работы с цифровым измерением еще в начале 2000-х гг. и что отдельные аспекты реагирования на угрозу из цифрового пространства отражены в доктринальных документах (например, в военной доктрине 2004 г.[200]), Нью-Дели долгое время было сосредоточено на купировании отдельных аспектов *цифрового вызова*, а работа по обеспечению ***кибербезопасности*** неизбежно замыкалась на внутренний рынок.

Однако ко второй половине 2010-х гг. в системе цифровой защиты Индии произошли коренные изменения: после пандемии COVID-19 индийские власти не только поддержали намерение крупного национального кибербизнеса активнее участвовать в проектах государственно-частного партнерства на Ближнем Востоке, но и сделали это одним из элементов многосторонней дипломатии[201]. На данный момент у Нью-Дели стабильные деловые отношения со всеми аравийскими монархиями, а с четырьмя из них (Катар, Саудовская Аравия, ОАЭ, Оман) подписаны пакетные соглашения о развитии цифрового сотрудничества[202].

При этом ключевым партнером Индии в Персидском заливе уже много лет остается Оман: контакты Нью-Дели и Маската отличаются наибольшей частотой и демонстрируют тенденцию к расширению, прежде всего в бизнес-сегменте, за счет растущей роли индийской диаспоры в Султанате. Оман стал первой страной ССАГЗ, подписавшей с Индией соглашение о координации усилий по борьбе с террористической угрозой в киберпространстве в 2023 г.[203]. Кроме того, Маскат и Нью-Дели на регулярной основе проводят координационные мероприятия по защите объектов критической инфраструктуры, реализуют обмен кадрами[204].

Следует отметить, что в вопросах кибербезопасности Индия не ограничивается двусторонним сотрудничеством. Напротив, в качестве самостоятельного трека Нью-Дели рассматривает развитие комплексного взаимодействия с региональными объединениями – в первую очередь, с Лигой арабских государств[205], а также с ССАГЗ[206]. В обоих случаях на первый план выходят вопросы совместного развития искусственного интеллекта и цифровых бизнес-решений.

В целом, в вопросах кибербезопасности удается поддерживать рабочий диалог со всеми без исключения государствами группы «Персидский залив+» – хотя в некоторых случаях взаимодействие осложняется влиянием смежных факторов.

---

[200] Indian Army Doctrine (2004). URL: https://www.files.ethz.ch/isn/157030/India%202004.pdf

[201] India’s cyber diplomacy comes of age // Observer Research Foundation. 14.08.2023. URL: https://www.orfonline.org/expert-speak/indias-cyber-diplomacy-comes-of-age/

[202] Посчитано по: UNIDIR.

[203] India, Oman agree to jointly fight all manifestations of terror // The Economic Times. 18.01.2023. URL: https://economictimes.indiatimes.com/news/defence/india-oman-agree-to-jointly-figh-terror/

[204] Cyber security meet to focus on 'safe economy' in Oman // Zawya. 23.03.2022. URL: https://www.zawya.com/en/legal/crime-and-security/cyber-security-meet-to-focus-on-safe-economy-in-oman-qfwbjvbp

[205] India, Arab League eye more cooperation in green energy, tech // Arab News. 12.07.2024. URL: https://www.arabnews.com/node/2336531/world

[206] Indian businesses invest billions in GCC // The Jerusalem Post. 14.05.2023. URL: https://www.jpost.com/business-and-innovation/banking-and-finance/article-742959

Примером тому служит ирано-индийское сотрудничество. Несмотря на интенсивный диалог между государственными институтами двух стран, цифровая инфраструктура Нью-Дели сильно страдает от атак проиранских хакерских групп[207]. При этом индийских «ястребов» больше всего раздражает не сам факт проведения кибератак, а склонность иранских хакеров использовать клоны сайтов крупных индийских IT-компаний в качестве *ложного флага* при проведении атак. Такая практика не только вредит индийскому кибербизнесу, но и снижает уровень доверия между Нью-Дели и Тегераном.

Кроме того, Индия обеспокоена продолжающимся сближением Ирана и Китая, которое ускорилось на фоне посреднической деятельности Пекина в регионе Персидского залива. В то же время постепенное вовлечение Нью-Дели в израильский проект «Железный киберкупол» формирует у иранского истеблишмента убеждение, что он «косвенно поддерживает» интересы Тель-Авива в ирано-израильском асимметричном конфликте и в перспективе может стать одной из причин дополнительной активизации иранских хакеров в индийском киберпространстве[208].

За прошедшие с момента завершения пандемии COVID-19 несколько лет Индия смогла укрепить влияние на рынке ***финансовых технологий*** Ближнего Востока – чему во многом способствовало развитие системы Специальных экономических зон (СЭЗ) в аравийских монархиях. Среди крупнейших индийских FinTech-компаний, на постоянной основе оказывающих услуги на Ближнем Востоке, являются *M2P* (Интернет-банкинг), *PhonePe* (цифровые трансграничные платежи) и *Razorpay* (разработка и развитие платежных шлюзов)[209] – перечисленные компании сотрудничают как минимум с тремя аравийскими монархиями каждый, а также работают над расширением присутствия на иракском рынке.

Сотрудничество в области цифровых финансов также развивается и с Ираном – однако оно сконцентрировано в большей степени вокруг развития цифровой инфраструктуры иранского порта Чабахар, включенного в орбиту проекта «Транспортный коридор “Север – Юг”»[210].

Индийский опыт развития ***ИИ-технологий*** также пользуется определенным спросом в регионе. Отмечен рост присутствия индийских компаний, специализирующихся на развитии генеративного ИИ, на рынках ОАЭ и Садовской Аравии[211]. Кроме того, с подачи Нью-Дели налажена академическая мобильность в области ИИ со всеми аравийскими монархиями, а также с Ираком. С другой стороны, индийские компании пока существенно уступают в компетенциях американским и китайским конкурентам, что ограничивает масштабы их работы в регионе.

---

[207] India sees sharp increase in cyberattacks in Q1 2023: report // The Economic Times. 09.05.2023. URL: https://economictimes.indiatimes.com/tech/technology/sharp-increase-in-cyberattacks-in-india-in-q1-2023-report/articleshow/100096450.cms?from=mdr

[208] How India, UAE, Israel are trying to build secure cyberspace // The Week. 16.07.2023. URL: https://www.theweek.in/theweek/specials/2023/07/08/building-a-secure-cyberspace-through-the-india-uae-israel-cyber-security-partnership.html

[209] Can India export FinTech to the Middle East? // Eximus Echo. 30.08.2024. URL: https://eximiusecho.substack.com/p/can-india-export-fintech-to-the-middle

[210] Despite a Recent India-Iran Agreement, Challenges Loom for Chabahar Port // Stimson. 09.07.2024. URL: https://www.stimson.org/2024/despite-a-recent-india-iran-agreement-challenges-loom-for-chabahar-port/

[211] Indian Gen AI firm expands into Middle East // Khaleeej Times. 04.07.2024 URL: https://www.khaleejtimes.com/business/tech/indian-gen-ai-firm-expands-into-middle-east

Определенные подвижки наблюдаются и в секторе ***разработки программного обеспечения***: так, ряд индийских IT-компаний (например, «Web3 tech») за последний год расширили контакты с саудовской фирмой «Aba'ad Alkhayal», считающейся национальным флагманом развития передовых киберпроектов (включая технологии блокчейн и искусственного интеллекта)[212].

Обобщенный показатель вовлеченности представлен ниже (*см. Таблицу 10*).

Страна	Цифровая безопасность	Цифровые технологии в экономике и госуправлении	ИИ-Технологии	Разработка ПО
КСА	4	3	4	3
ОАЭ	4	3	4	2
Катар	4	3	4	1
Кувейт	3	2	3	1
Бахрейн	3	3	4	1
Оман	3	2	4	1
Иран	3	4	2	2
Ирак	2	4	3	1

Таблица 10. Индекс вовлеченности в развитие системы цифровых технологий стран региона (по 5-балльной шкале)[213]. Составлено автором.

Страны ЕС. Долгое время вопросы развития контактов в области ***кибербезопасности*** не входили в число приоритетных направлений сотрудничества между Брюсселем и странами группы «Персидский залив+» – хотя активный диалог в области высоких технологий начался еще в первой половине 2010-х гг. Несколько попыток перезагрузки отношений – включая развитие многосторонней кооперации с ЕС в рамках *доктрины Могерини* (2015 г.)[214] – не принесли существенного результата: основной формой взаимодействия оставались образовательные кадровые семинары под эгидой специалистов ЕС. Однако они имели нерегулярный характер, а по уровню организации уступали инициативам НАТО[215].

Качественный рост наметился после 2022 г., когда отношения ЕС со странами ССАГЗ были выведены на уровень стратегического партнерства[216], однако уровень влияния Евросоюза

[212] India-based Web3 technology company has strategically expanded into the Middle East // The FinTech Times. 03.08.2023. URL: https://thefintechtimes.com/india-based-web3-tech-company-expands-to-middle-east-with-saudi-based-software-partnership/

[213] 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.

[214] Неформальное наименование Глобальной стратегии ЕС, представленной в конце 2015 г. Среди прочего включает в себя усилия по противодействию киберугрозам через развитие международного сотрудничества и повышение мер доверия в киберпространстве. См.: Federica Mogherini launches the EU Global Strategy // EU External Action. 12.10.2015. URL: https://www.eeas.europa.eu/eeas/federica-mogherini-launches-eu-global-strategy-0_ru?s=63

[215] Webinar: "Euro-Gulf Regional Cybersecurity Collaboration" // Bussola. URL: https://www.bussolainstitute.org/euro-gulf-regional-cybersecurity-collaboration

[216] Joint Communication on a “Strategic Partnership with the Gulf” // EU External Action. 18.05.2022. URL: https://www.eeas.europa.eu/eeas/joint-communication-%E2%80%9Cstrategic-partnership-gulf%E2%80%9D_en; Также свою роль в процессе сближения сыграла стратегия «Global Gateway», принятая в 2021 г. и включающая развертывание защищенных цифровых сетей, продвижение ориентированного на человека подхода к

на профильные решения аравийских монархий по-прежнему существенно уступает не только США, но и азиатским конкурентам (КНР, Индия).

При этом ЕС внес (и продолжает вносить) существенный вклад в развитие модели *скрытой торговли* цифровыми технологиями между Израилем и аравийскими монархиями[217], а также способствовал развитию государственно-частного партнерства на пространстве ССАГЗ[218]. Брюссель и аравийские монархии продолжают наращивать обмен знаниями и ресурсами в области технологического развития, а также координируют усилия по развитию сотрудничества в частном секторе – особенно в вопросах цифровой экономики и больших данных.

Европейские фирмы, специализирующиеся на противодействии цифровым угрозам, сотрудничают со всеми монархиями Залива, а также с Ираком, участвуют в реализации ключевых национальных проектов (например, в строительстве «города будущего» NEOM в Саудовской Аравии). Профильный диалог с Ираном (в силу присоединения европейских стран к санкционному режиму в отношении ИРИ) заморожен.

Вопросы совместного развития ***инструментов цифровой экономики и госуправления*** также находятся в повестке ЕС. Брюссель рассматривает увеличения доли европейских компаний на Ближнем Востоке в качестве долгосрочной инвестиции в региональное влияние и с 2018 г. продвигает собственные FinTech-стартапы на рынки ближневосточных стран[219]. Тем не менее, выделить «якорных» партнеров на данном направлении из числа государств группы «Персидский залив+» весьма проблематично. Со всеми странами (за исключением Ирана) диалог выстроен по схожей модели – при этом в отдельно взятых случаях итоговый вклад ЕС в экономическую трансформацию можно оценить как существенный[220].

В ЕС в целом поддерживают бизнес-подход государств региона к развитию сферы ***искусственного интеллекта*** – в этом смысле организация ориентируется на положения стратегии «Global Gateway» (2021 г.), где развитие экономики данных и ИИ-инструментов обозначено в числе первоочередных приоритетов[221]. При этом политические дискуссии внутри ЕС пока в большей степени сосредоточены на совершенствовании цифрового управления в самой Европе и представляются изолированными от повестки развития

цифровизации, содействие сотрудничеству в области экономики данных и искусственного интеллекта, а также содействие повышению цифровых навыков, особенно для женщин и молодежи в странах ССАГЗ. См.: EU's 'Global Gateway' and the Gulf region: Addressing the blind spots of digital infrastructures and supply chains in the evolving AI landscape // Policy Review. 31.05.2024. URL: https://policyreview.info/articles/news/eu-global-gateway-and-gulf-region

[217] Zilber N. Gulf Cyber Cooperation with Israel: Balancing Threats and Rights // Washington Institute. 17.01.2019. URL: https://www.washingtoninstitute.org/policy-analysis/gulf-cyber-cooperation-israel-balancing-threats-and-rights

[218] The EU's International Cooperation on Cyber Capacity Building // European Commission, 2023. URL: https://www.eucybernet.eu/wp-content/uploads/2023/11/operational-guidance-for-the-eu-international-cooperation-on-ccb-1-1.pdf

[219] FinTech: Connecting Europe with the Middle East // The Parliament. 08.08.2018. URL: https://www.theparliamentmagazine.eu/partner/article/fintech-connecting-europe-with-the-middle-east

[220] Речь, например, о запуске в июне 2024 г. Национальной стратегии Центрального банка Ирака по банковскому кредитованию на 2024-2029 гг. Стратегия была разработана в рамках совместного проекта ЕС и Германии «Укрепление государственных финансов и финансовых рынков в Ираке» и реализуемая Немецким агентством по международному сотрудничеству, направлена на оказание надежной поддержки предприятиям частного сектора в Ираке. См.: EU Praises Iraq's National Bank Lending Strategy // Iraq Business News. 02.06.2024. URL: https://www.iraq-businessnews.com/2024/06/02/eu-praises-iraqs-national-bank-lending-strategy/

[221] EU's 'Global Gateway' and the Gulf region: Addressing the blind spots of digital infrastructures and supply chains in the evolving AI landscape // Policy Review. 31.05.2024. URL: https://policyreview.info/articles/news/eu-global-gateway-and-gulf-region

отношений с регионом Ближнего Востока. По этой причине диалог носит скорее декларативный характер и призван подчеркнуть серьезность намерений Брюсселя в долгосрочной перспективе.

Дополнительно следует отметить, что европейские страны в вопросах налаживания диалога со странами региона нередко действуют «в отрыве» от институтов ЕС, руководствуясь национальными экономическими и военно-политическими интересами. Несмотря на наличие среди европейцев сторонников активных экспансии (Франция, Германия), их контакты со странами региона носит гибкий характер. Однозначное доминирование какой-либо европейской страны (без учета *совокупного веса* ЕС как коллективного игрока) на цифровом рынке стран группы «Персидский залив+» в настоящий момент почти не прослеживается.

Обобщенный показатель вовлеченности представлен ниже (*см. таблицу 11*).

Страна	Цифровая безопасность	Цифровые технологии в экономике и госуправлении	ИИ-Технологии	Разработка ПО
КСА	3	3	2	2
ОАЭ	3	3	2	2
Катар	3	2	2	2
Кувейт	3	2	2	2
Бахрейн	3	3	2	2
Оман	3	2	2	2
Иран	0	0	0	0
Ирак	2	2	2	2

Таблица 11. Индекс вовлеченности в развитие системы цифровых технологий стран региона (по 5-балльной шкале)[222]. Составлено автором.

Великобритания. После выхода из состава ЕС Великобритания заметно пересмотрела подход к выстраиванию отношений с государствами Ближнего Востока – исходя из собственных стратегических интересов.

Одним из драйверов развития сотрудничества стала ***кибербезопасность***. «Якорным» партнером Великобритании в регионе по сегодняшний день остается Саудовская Аравия, профильное взаимодействие с которой осуществляется с 2018 г. и охватывает широкий круг направлений, включая совместное противодействие киберпреступному и кибертеррористическому сообществам[223].

Динамично развивается и британо-эмиратский диалог (сконцентрированный в большей степени на развитии инновационных проектов[224]) – однако на его динамику по-прежнему

[222] 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.

[223] United Kingdom-Saudi Arabia Joint Communiqué // UK Government. 10.03.2018. URL: https://www.gov.uk/government/news/united-kingdom-saudi-arabia-joint-communique

[224] UK Science & Innovation Network in United Arab Emirates // UK Government. URL: https://www.gov.uk/world/organisations/uk-science-innovation-network-in-united-arab-emirates

оказывают негативное влияние царящие в британском секторе связи алармистские настроения[225].

Британо-иракское сотрудничество в области кибербезопасности носит избирательный характер и сосредоточено вокруг развития стратегического диалога[226], профильный диалог с Ираном отсутствует.

Ситуация в бизнес-сегменте складывается схожим образом. Крупные британские киберфирмы (например, *Microminder Cyber Security, Darktrace* и др.) имеют свои представительства во всех странах Залива, а также осуществляют подготовку профильных специалистов аравийских монархий и Ирака.

Рынок ***финансовых технологий*** стран Залива представляет интерес для Лондона. На волне продолжающихся реформ отрасли цифровых финансов в большинстве аравийских монархий Великобритания стремится расширить сферу присутствия и удовлетворить запрос ближневосточных партнеров на укрепление международных связей. Упор ожидаемо делается на лидеров направления (например, Саудовскую Аравию[227]), однако Лондон стремится демонстрировать присутствие на рынках всех монархий Залива. Более того, на некоторых направлениях британский FinTech-бизнес по доле присутствия сумел перегнать европейский. Подобная ситуация сложилась, например, в Кувейте[228].

Британское правительство уделяет внимание сектору ***ИИ-технологий***. Великобритания выступает за повышение уровня доверия в вопросах развития искусственного интеллекта и следование *цифровой этике* (что было детально обозначено Лондоном в ходе профильного саммита в 2023 г.[229]) – соответствующие договоренности прорабатываются в двустороннем формате с региональными лидерами отрасли[230].

При этом в вопросах экспорта технологических решений в области ИИ на Ближний Восток Лондон проявляет осторожность и не делает это направление взаимодействия приоритетным, предпочитая работать по более широкому контуру кибербезопасности.

Следует отметить, что эффективность цифрового сотрудничества между Великобританией и странами группы «Персидский залив+» заметно снижается из-за постоянных перестановок в британском правительстве, влекущих неизбежную смену

---

[225] Например, в январе 2024 г. правительство Великобритании признало угрозой национальной безопасности факт владения эмиратских фирм 16% акций национального оператора связи. Это вызвало возражения со стороны официального Абу-Даби: UK says Emirates-backed stake in Vodafone poses national security risk // The Guardian. 25.01.2024. URL: https://www.theguardian.com/business/2024/jan/25/emirates-backed-stake-vodafone-security-risk-uae-uk-government

[226] Second UK-Iraq Strategic Dialogue, 2023: joint communiqué // UK Government. 04.07.2023. URL: https://www.gov.uk/government/news/the-second-uk-iraq-strategic-dialogue-2023-joint-communique

[227] UK Fintechs Head to Saudi Arabia After Finserv Reforms // FinTech Magazine. 29.01.2024. URL: https://fintechmagazine.com/articles/uk-fintechs-head-to-saudi-arabia-after-finserv-reforms

[228] AlRushood: New expansion in the UK is highly significant for KFH's global reach // KFH. 06.03.2024. URL: https://kfh.com/en/home/Personal/news/2024/AlRushood--new-expansion-in-the-UK-is-highly-significant-for-KFH-s-global-reach.html

[229] The UK AI Safety Summit Opened a New Chapter in AI Diplomacy // Carnegie Endowment. 09.11.2023. URL: https://carnegieendowment.org/posts/2023/11/the-uk-ai-safety-summit-opened-a-new-chapter-in-ai-diplomacy?lang=en

[230] См., напр.: Hornstein O. UK tech secretary visits UAE to build AI ties // UKTN. 27.02.2024. URL: https://www.uktech.news/ai/uk-tech-secretary-uae-ai-20240227

внешнеполитических приоритетов. Интересы лейбористского правительства Кира Стармера, пришедшего к власти в июле 2024 г., существенно расходятся с ориентирами прежних премьеров-консерваторов, что обуславливает частичный пересмотр прежних договоренностей.

Одним из примеров тому может служить работа по пересмотру приоритетов Великобритании в секторе ИИ в рамках формирования лейбористами новой структуры бюджета. Предполагается, что сторонники Стармера уменьшат расходы на это направление, отдав приоритет внедрению технологий в собственный госсектор. На этом фоне прямые инвестиции в промышленность, а также в поддержку международного сотрудничества в области ИИ, вероятно, будут кратно сокращены[231].

Также из поля взаимодействия полностью выпадает Иран (в силу поддержки Лондоном санкционного режима в отношении Исламской Республики), что делает охват рынка Персидского залива неполным.

Обобщенный показатель вовлеченности представлен ниже (*см. таблицу 12*).

Страна	Цифровая безопасность	Цифровые технологии в экономике и госуправлении	ИИ-Технологии	Разработка ПО
КСА	3	2	1	2
ОАЭ	3	2	1	2
Катар	2	2	1	1
Кувейт	1	3	1	2
Бахрейн	2	2	1	1
Оман	1	2	1	1
Иран	0	0	0	0
Ирак	1	2	1	1

Таблица 12. Индекс вовлеченности в развитие системы цифровых технологий стран региона (по 5-балльной шкале)[232]. Составлено автором.

Турция. Партнерство Турции со странами группы «Персидский залив+» имеет восходящий вектор. За прошедшие с момента включения в гонку за цифровое лидерство годы Анкаре удалось расширить профильный диалог с большинством аравийских монархий в области ***кибербезопасности***[233], нивелировав тем самым последствия Дипломатического кризиса (2017-2021 гг.)[234].

[231] More Signal. Less Noise // The Cyberwire. URL: https://thecyberwire.com/newsletters/caveat-briefing/2/36

[232] 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.

[233] См., напр.: UAE-Cyber: President Sheikh Mohammad's interest in cooperating with Turkiye note // Tactical Report. 13.07.2023. URL: https://www.tacticalreport.com/daily/62026-uae-cyber-president-sheikh-mohammads-interest-in-cooperating-with-turkiye

[234] В период острой фазы Дипломатического кризиса среди аравийских монархий существовали опасения, что Катар будет использовать союзнические отношения с Турцией для расширения «антиарабского фронта» (де-факто, фронта против Саудовской Аравии и ОАЭ), охватывающего в том числе киберпространство. Это, с учетом возросшей активности Турции в зоне геополитических интересов аравийских монархий, выводило Анкару в категорию потенциальных противников аравийских монархий и создавало препятствия для развития

При этом наиболее динамично профильное взаимодействие по-прежнему развивается с Катаром: здесь Анкара и Доха руководствуются теми же установками по развитию комплексного стратегического партнерства, что и в 2017 г.[235]. Среди прочего Катар заинтересован в дальнейшей интеграции турецкого опыта работы с национальным хакерским сообществом для решения внутри- и внешнеполитических задач[236].

Серьезным подспорьем для Анкары является частный сектор. Турецкие киберфирмы представлены на цифровых рынках всех аравийских монархий, а ведущие турецкие IT-компании (*Heraklet, ICterra* и др.) принимают участие в реализации проектов на пространстве ССАГЗ, включая косвенно связанные с развитием военного сегмента кибербезопасности. Так, например, турецкая компания *ICterra* в январе 2023 г. присоединилась к трехлетней программе наставничества Агентства НАТО по связи и информации (*NATO Communications and Information Agency, NCIA*), ориентированной на подготовку специалистов в области кибербезопасности и организацию стажировок для внеблоковых партнеров Альянса[237], в число которых входят и монархии Залива.

Сфера ***финансовых технологий*** пока не стала для Турции точкой значительного приложения усилий – предложения Анкары теряются на фоне аналогичных проектов западных стран. Однако встречаются и исключения. Например, Анкара планомерно наращивает сотрудничество с Ираком в области развития инструментов интернет-банкинга[238], что способствует укреплению влияния турецкого бизнеса на территории страны. Довольно динамично развивается диалог с Катаром (главным образом, по развитию системы трансграничных платежей)[239], что вполне укладывается в рамки стратегического партнерства двух государств.

Есть определенные перспективы роста и в сфере ***искусственного интеллекта***. Турция весьма комплексно осмысляет угрозы и возможности, связанные с внедрением ИИ-технологий (что отражено в документах стратегического планирования[240]) и поэтапно

сотрудничества в чувствительных областях. См.: https://gulfif.org/turkey-and-the-gcc-states-between-a-foe-and-an-ally/

[235] Qatar and Turkey Cooperate in Cybersecurity Field / QNA. 10.08.2017. URL: https://www.qna.org.qa/en/News-Area/News/2017-08/10/qatar-and-turkey-cooperate-in-cybersecurity-field

[236] Более подробно см. Приложение 1 Доклада.

[237] ICterra NATO NCI Collaboration // ICterra. URL: https://www.icterra.com/icterra-nato-nci-collaboration/

[238] Aktif Bank And Trade Bank Of Iraq (TBI) Invests For The Future Of Iraq // Aktif Bank. URL: https://www.aktifbank.com.tr/en/about-us/press-room/news-from-us/aktif-bank-and-trade-bank-of-iraq-tbi-invests-for-the-future-of-iraq

[239] Qatar and Turkey to explore opportunities in fintech sector // The Peninsula. 24.02.2022. URL: https://thepeninsulaqatar.com/article/24/02/2022/qatar-and-turkey-to-explore-opportunities-in-fintech-sector

[240] National Artificial Intelligence Strategy 2021-2025 // Digital Transformation Office. URL: https://cbddo.gov.tr/en/nais; Также Анкара работает над гармонизацией национального законодательства для облегчения работы с ИИ-технологиями. В частности, специализированный закон (т.н. «AI Bill») был внесен на рассмотрение в профильный парламентский комитет в июне 2024 г. Предполагается, что с его принятием Анкара сможет более эффективно работать с ИИ-технологиями (в том числе в вопросах развития профильного международного сотрудничества). См.: Turkey: AI bill submitted to Parliamentary Committee // Data Guidelines. 28.06.2024. URL: https://www.dataguidance.com/news/turkey-ai-bill-submitted-parliamentary-committee

развивает отношения с наиболее активными игроками отрасли – в частности, с ОАЭ[241] и Катаром[242].

Обобщенный показатель вовлеченности представлен ниже (*см. таблицу 13*).

Страна	Цифровая безопасность	Цифровые технологии в экономике и госуправлении	ИИ-Технологии	Разработка ПО
КСА	3	1	2	1
ОАЭ	3	1	3	1
Катар	4	3	3	1
Кувейт	2	1	1	1
Бахрейн	3	1	1	1
Оман	2	1	1	1
Иран	3	0	0	1
Ирак	3	2	1	1

Таблица 13. Индекс вовлеченности в развитие системы цифровых технологий стран региона (по 5-балльной шкале)[243]. Составлено автором.

Южная Корея. Флагманским партнером страны в вопросах ***кибербезопасности*** можно считать ОАЭ. Отношения Сеула и Абу-Даби вышли на уровень стратегического партнерства в 2010 г. (с 2019 г. – особое стратегическое партнерство)[244], а сектор кибербезопасности вошел в число приоритетных направлений сотрудничества – особенно после запуска в 2024 г. *цифрового трека* экономических отношений под эгидой Соглашения о всеобъемлющем экономическом партнерстве[245].

Кроме того, вопросы межведомственного сотрудничества в военном сегменте кибербезопасности интенсивно развиваются с Саудовской Аравией[246] и Катаром[247] – в обоих случаях стороны руководствуются идеей снижение региональной напряженности через создание устойчивого партнерства в цифровом пространстве.

Весьма динамично развивается частный сегмент рынка – здесь южнокорейские компании ориентированы на наращивание взаимодействия в области ***финансовых технологий*** и ***разработки ПО***. Проводниками интересов служат крупные IT-фирмы (*Naver Corp., Caulis*

[241] Türkiye, UAE to cooperate in space and AI // Anadolu. 20.07.2023. URL: https://www.aa.com.tr/en/economy/turkiye-uae-to-cooperate-in-space-and-ai/2950517

[242] Преобладает «B2B»-формат. См.: Turkiye gearing up for B2B sessions to boost ties in AI, says envoy // Gulf Times. 27.05.2024. URL: https://www.gulf-times.com/article/683458/business/turkiye-gearing-up-for-b2b-sessions-to-boost-ties-in-ai-says-envoy

[243] 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.

[244]Defense chiefs of S. Korea, UAE discuss cooperation in arms industry, cybersecurity // Yonhap. 22.02.2023. URL: https://en.yna.co.kr/view/AEN20230222001451325

[245] South Korea, UAE sign pact to boost economic relations // Anadolu. 29.05.2024. URL: https://www.aa.com.tr/en/asia-pacific/south-korea-uae-sign-pact-to-boost-economic-relations/3233818

[246] South Korea, Saudi Arabia sign agreement on defence cooperation // Reuters. 05.02.2024. URL: https://www.reuters.com/world/south-korea-saudi-arabia-sign-agreement-defence-cooperation-2024-02-05/

[247] South Korea, Qatar defence ministers agree to boost military ties –Seoul // Reuters. 07.02.2024. URL: https://www.reuters.com/world/south-korea-qatar-defence-ministers-agree-boost-military-ties-seoul-2024-02-07/

Inc. и др.)[248] Однако число присутствующих на рынке стран региона южнокорейских IT-компаний кратко меньше в сравнении с китайскими конкурентами.

С другой стороны, зафиксировано существенное увеличение числа фирм, специализирующихся на ***криптовалютных операциях*** и технологиях блокчейна. Особенно это заметно в случае с ОАЭ, где доля южнокорейских майнинговых компаний является одной из самых больших не только среди аравийских монархий, но и на Ближнем Востоке в целом[249].

Перспективным направлением развития взаимодействия является ***сфера искусственного интеллекта***. Сеул является одним из ключевых проводников идеи ответственного использования ИИ и продвигает различные форматы международного диалога. К числу таких инициатив относится и Международный ИИ-саммит, проведенный Сеулом в сентябре 2024 г. Участие в мероприятии приняли более 90 стран, включая аравийские монархии и Ирак[250]. Параллельно с этим продолжается экспансия корейских фирм, специализирующихся на искусственном интеллекте, на Ближний Восток (например, *Wrtn Technologies*)[251], что является частью «двухуровневой» стратегии Южной Кореи по укреплению позиций в регионе.

За рамками цифрового сотрудничества (как в государственном, так и в частном секторе) остается Иран, ввиду сохранения *спорадической напряженности* между Сеулом и Тегераном. В 2020 г. Южная Корея в одностороннем порядке решила заморозить все иранские активы в стране из опасения, что они могут быть направлена на финансирование иранского «военного атома». Решение Сеула вызвало недовольство Тегерана и негативно сказалось на уровне отношений между странами – хотя сторонам и удалось сохранить некоторые контакты в передовых областях, включая научное сотрудничество[252]. Кроме того, Южная Корея настороженно относится к продолжающемуся сближению Тегерана и Пхеньяна, что снижает уровень доверия и ограничивает пространство для взаимодействия двух стран[253].

Обобщенный показатель вовлеченности представлен ниже (*см. таблицу 14*).

---

[248] Middle East, land of dreams for South Korean IT firms // The korea Economic Daily. 09.04.2024. URL: https://www.kedglobal.com/tech,-media-telecom/newsView/ked202404090008

[249] S. Korean crypto firms rush to UAE for 50-year tax exemption // The Chosun Daily. 02.07.2024. URL: https://www.chosun.com/english/market-money-en/2024/07/02/ZLQIMHMTIVGEHKHBDSPLJYEHWU/; South Korean Crypto VC Hashed Expands to Abu Dhabi Via Hub71 Partnership // BlockHead. 27.06.2024. URL: https://www.blockhead.co/2024/06/27/south-korean-crypto-investment-giant-hashed-expands-to-abu-dhabi/

[250] South Korea international summit to target 'blueprint' for AI use in military // Al-Arabiya. 09.09.2024. URL: https://english.alarabiya.net/News/world/2024/09/09/south-korea-international-summit-to-target-blueprint-for-ai-use-in-military-

[251] Korean firm raises $18m to expand 'AI super app' in Middle East, SEA // Tech in Asia. 07.06.2024. URL: https://www.techinasia.com/south-korean-ai-firm-wrtn-raises-18m-expand-middle-east-sea

[252] МИД Южной Кореи заявил, что замороженные в республике средства принадлежат народу Ирана // ИТАР-ТАСС. 05.09.2023. URL: https://tass.ru/mezhdunarodnaya-panorama/18656075

[253] IntelBrief: Iran and North Korea Draw Closer // The Soufan Center. 07.05.2024. URL: https://thesoufancenter.org/intelbrief-2024-may-7/

Страна	Цифровая безопасность	Цифровые технологии в экономике и госуправлении	ИИ-Технологии	Разработка ПО
КСА	3	2	2	2
ОАЭ	4	3	2	2
Катар	3	1	2	2
Кувейт	2	1	2	2
Бахрейн	2	1	2	2
Оман	2	1	2	2
Иран	0	0	0	0
Ирак	2	1	2	2

Таблица 14. Индекс вовлеченности в развитие системы цифровых технологий стран региона (по 5-балльной шкале)[254]. Составлено автором.

Япония. Несмотря на то, что Япония является одним из признанных мировых лидеров в области цифровых технологий, ее текущее присутствие на рынке региона характеризуется как сравнительно невысокое.

Контакты в области ***кибербезопасности*** между государственными институтами Японии и стран региона «Персидский залив+» носят избирательный характер. Токио в большей степени сосредоточено на укреплении собственной киберсистемы на фоне кратно участившихся массированных кибератак[255]. С другой стороны, отмечено постепенное расширение контактов с Саудовской Аравией и ОАЭ по линии институтов, отвечающих за технологии и инновации[256], а в случае с Абу-Даби взаимодействие частично охватило и военный сектор кибертехнологий[257].

Токио продолжает делать упор на развитие международного сотрудничества в области ***финансовых технологий*** – акцент делается на развитие бизнес-отношений с аравийскими монархиями, которые уже обладают устойчивой экономико-технологической базой и заинтересованы в расширении круга партнеров.

Так, например, в конце 2023 г. японский финансовый гигант *SBI Holdings* и саудовская нефтяная компания *Saudi Aramco* подписали меморандум о взаимопонимании, предполагающий наращивание взаимных инвестиций в цифровые активы, развитие Web3 и поддержку японских стартапов, ориентированных на регион Ближнего Востока[258].

[254] 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.

[255] Japan's Rush to Play Cyber Defense Catchup // The Diplomat. 10.06.2024. URL: https://thediplomat.com/2024/06/japans-rush-to-play-cyber-defense-catchup/

[256] Japan-UAE Innovation Partnership Released // METI. 24.07.2023. URL: https://www.meti.go.jp/english/press/2023/0724_001.html

[257] Entry into Force of the Agreement between the Government of Japan and the Government of the United Arab Emirates (UAE) concerning the Transfer of Defense Equipment and Technology // Ministry of Foreign Affairs of Japan. 09.01.2024. URL: https://www.mofa.go.jp/press/release/pressite_000001_00088.html

[258] Digital Development in the Middle East: Japanese and Saudi Giants Invest in Blockchain and Semiconductors // CyberSec. 03.01.2024. URL: https://cybersecforum.eu/2024/01/03/digital-development-in-the-middle-east-japanese-and-saudi-giants-invest-in-blockchain-and-semiconductors/

Переговоры по укреплению отношений, с высокой долей вероятности, параллельно ведутся и с другими нефтегазовыми игроками – например, с катарским *RasGas*.

Форсированно развивается научно-техническое сотрудничество Японии и Ирака. Иракские власти весьма лояльно относится к японскому технологическому бизнесу, и приветствуют расширение его присутствия на национальном рынке. Кроме того, поощряется создание совместных с иракскими гражданами предприятий и стартапами (особенно в секторе связи)[259].

При этом в секторе ***искусственного интеллекта*** японские разработки практически не представлены – хотя японские фирмы, наравне с западными, рассматривают Ближний Восток в качестве перспективного направления экспансии[260].

Обобщенный показатель вовлеченности представлен ниже (*см. таблицу 15*).

Страна	Цифровая безопасность	Цифровые технологии в экономике и госуправлении	ИИ-Технологии	Разработка ПО
КСА	2	3	1	2
ОАЭ	2	2	1	2
Катар	1	3	1	1
Кувейт	1	1	1	1
Бахрейн	1	1	1	1
Оман	2	1	1	1
Иран	0	0	0	0
Ирак	1	3	1	1

Таблица 15. Индекс вовлеченности в развитие системы цифровых технологий стран региона (по 5-балльной шкале)[261]. Составлено автором.

3.2. Регион Африки южнее Сахары

КНР. Политика Китая в Африке имеет выраженный экономический базис. Опираясь на проект «Один пояс, один путь» и его составляющие (в частности, «Цифровой Шелковый путь»[262]), Пекин наращивает влияние на экономики африканских стран, а в некоторых случаях – косвенно определяет вектор их развития.

В рамках развития *техно-диалога* с Африканским континентом Китай развернул строительство транснациональной сетевой инфраструктуры, включающей подводные,

[259] Iraq Strengthens Ties with Japan in Technology and Communications // IINA. 11.09.2024. URL: https://www.iina.news/iraq-strengthens-ties-with-japan-in-technology-and-communications/

[260] Is the Middle East the Next Silicon Valley for AI? // CIO.Inc. 02.05.2024. URL: https://www.cio.inc/the-middle-east-next-silicon-valley-for-ai-a-24996

[261] 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.

[262] China's Digital Silk Road in Africa and the Future of Internet Governance // SAIIA. 01.01.2021. URL: https://saiia.org.za/research/chinas-digital-silk-road-in-africa-and-the-future-of-internet-governance/

наземные и спутниковые объекты – и ведущую роль в этом вопросе играет поддержка корпораций. Например, китайские корпорации *Huawei* и *ZTE* проложили оптоволоконные сети связи и электронного правительства в более чем двадцати странах АЮС[263]. Кроме того, китайские компании реализуют крупные международные проекты по прокладке подводных кабелей*: SAT3-WASC* (соединяет Южную Африку и Португалию вдоль западного побережья Африки)[264] и *2Africa* длиной 45 км (соединяет Африку и Великобританию)[265]. Это, в свою очередь, позволяет Пекину влиять на формирование сетевой инфраструктуры стран АЮС, включая сектор безопасности «точек входа» ключевых кабелей.

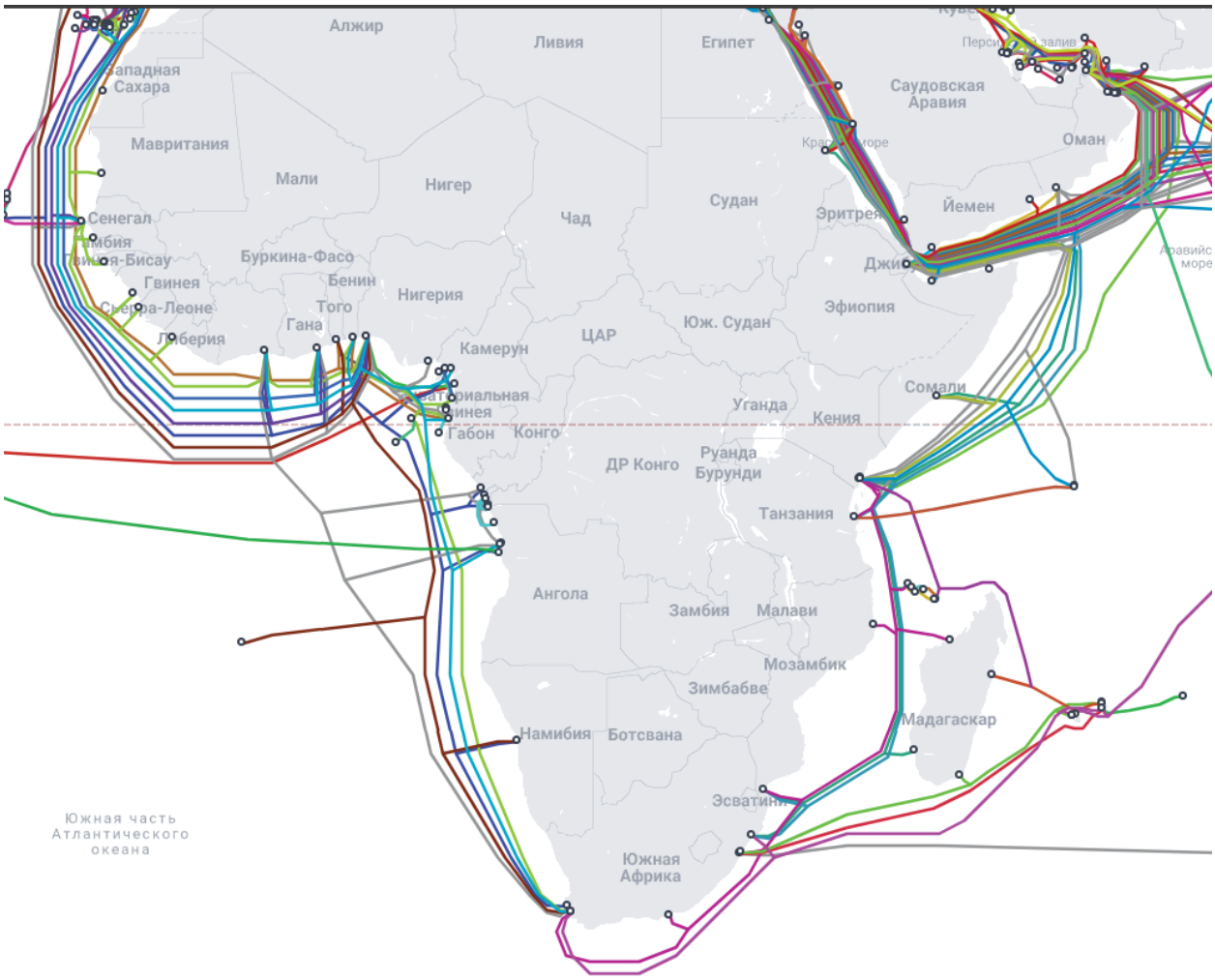

Рис.4. Схема расположения оптоволоконных кабелей (с указанием точек входа в странах АЮС). Источник: Submarine Cable Map[266].

Составляющая ***кибербезопасности*** является одной из ведущих в китайско-африканском диалоге. Поскольку речь зачастую идет о защите объектов критической инфраструктуры, Пекин уделяет первоочередное внимание повышению уровня киберготовности государств АЮС и совместной реализации инициатив в области цифровой безопасности.

[263] Посчитано по: Submarine Cable Map. URL: https://www.submarinecablemap.com/
[264] Ключевые «точки входа» SAT3-WASC в АЮС – Сенегал, Кот-д'Ивуар, Гана, Бенин, Нигерия, Камерун, Габон, Ангола, ЮАР.
[265] Ключевые «точки входа» 2Africa в АЮС – Сенегал, Кот-д'Ивуар, Гана, Бенин, Нигерия, Камерун, Габон, Ангола, ЮАР, Мозамбик, Мадагаскар, Танзания, Кения.
[266] Submarine Cable Map. URL: https://www.submarinecablemap.com/

Китай, среди прочего, делает ставку на совместное со странами Субсахарской Африки развитие стратегий борьбы с организованной киберпреступностью (наибольшую активность по этому профилю проявляет Танзания, с которой соглашение было достигнуто в числе первых, в 2017 г.[267]), а также на формирование рамок долгосрочного планирования развития ландшафта цифровой безопасности региона. Подспорьем в этом вопросе во многом стал Форум китайско-африканского сотрудничества (*FOCAC*), в рамках которого в 2021 г. стороны утвердили план комплексного взаимодействия (включая цифровой сегмент) до конца 2024 г.[268].

Общая логика взаимодействия Пекина и стран АЮС по-прежнему выстраивается с опорой на положения Международной стратегии по развитию сотрудничества в киберпространстве (*ISCC*), принятой в КНР в 2021 г[269]. Руководствуясь целями ISCC, КНР также инвестирует в прикладные цифровые отрасли, способствуя развитию культуры обращения с цифровыми активами, а также развитию Fintech-индустрии на Континенте. При этом, с точки зрения активности китайского бизнеса, наибольший интерес у Пекина вызывают Буркина-Фасо, Кения, Сенегал, Камерун и Замбия[270].

Также Пекин выступает за развитие комплексного цифрового диалога со странами Субсахарской Африки, входящими в БРИКС. В этом контексте власти КНР приветствуют инициативу России по созданию между участниками объединения реестр контактных пунктов для обмена информацией о компьютерных атаках[271], расширив тем самым диалог до уровня государственных команд CERT[272].

Флагманскими партнерами Пекина на рынке ***финансовых технологий*** среди стран Субсахарской Африки являются Кения, ЮАР и Танзания – контакты с ними характеризуются наибольшей частотой[273]; интенсивный профильный диалог развивается с Нигерией[274], ДРК[275] и рядом других стран региона. Также опыт китайских финансовых учреждений нередко позиционируется как «образец для подражания» при развитии системы цифровой коммерции в странах АЮС[276].

---

[267] TZ-China plan to curb cybercrime // The Citizen. 26.07.2017. URL: https://www.thecitizen.co.tz/News/Business/TZ-China-plan-to-curb-cybercrime/1840414-4032580-43cylk/index.html

[268] Forum on China-Africa Cooperation (FOCAC). URL: https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/202112/t20211202_10461183.html

[269] Ibidem.

[270] Why a growing number of Chinese investors are looking to Africa's tech space // South China Morning Post. URL: https://www.scmp.com/news/china/diplomacy/article/3226727/why-growing-number-chinese-investors-are-looking-africas-tech-space

[271] БРИКС создаст реестр контактных пунктов для обмена данными о компьютерных атаках // ИТАР-ТАСС. 17.04.2024. URL: https://tass.ru/politika/20576825

[272] До этого в рамках БРИКС с 2020 г. функционировал информационный канал, ориентированный на обмен информацией о кибератаках между национальными финансовыми регуляторами (BRISC). См.: Compendium BRICS BEST PRACTICES Information Security Risks: Supervision and Control (2021). URL: https://brics2021.gov.in/brics/public/uploads/docpdf/getdocu-54.pdf

[273] Roundup: China-Kenya fintech collaboration blossoms amid high mobile phone penetration // Xinhua. 31.08.2020. URL: http://www.xinhuanet.com/english/africa/2020-08/31/c_139329676.htm; China, South Africa upgrade ties to 'all-round strategic cooperative partnership' // Anadolu. 02.09.2024. URL: https://www.aa.com.tr/en/africa/china-south-africa-upgrade-ties-to-all-round-strategic-cooperative-partnership-/3319244 и др.

[274] China-backed fintech startup contributes to financial inclusion in Nigeria // Xinhua. 01.10.2021. URL: http://www.news.cn/english/2021-10/01/c_1310221960.htm

[275] DRC and China sign MoU to enhance digital cooperation // WeAreTech. 30.05.2023. URL: https://www.wearetech.africa/en/fils-uk/news/public-management/drc-and-china-sign-mou-to-enhance-digital-cooperation

[276] What African Banks Can Learn from Chinese Fintechs // Aza Finance. URL: https://azafinance.com/what-african-banks-can-learn-from-chinese-fintechs/

Пекин со своей стороны поощряет заход национальных компаний на африканский рынок, а также способствует развитию многосоставного диалога в этом секторе. Например, под эгидой Китайской академии финансовой доступности при Народном университете КНР в 2019 г. был запущен китайско-африканский диалог по финансовой доступности, ставший одной из крупнейших площадок обмена опытом между Пекином и странами АЮС в области финансовых технологий и цифровизации.

По итогам последней к настоящему моменту встречи (август 2024 г.) было существенно расширено поле взаимодействия, а в повестку включены вопросы модернизации цифровой инфраструктуры как в передовых, так и в «отстающих» странах[277]. Новые ориентиры развития цифровых экономик также были закреплены в Пекинском плане действий Форума по китайско-африканскому сотрудничеству на 2025 – 2027 г. (сентябрь 2024 г.)[278].

Что касается опыта использования цифровых валют в торговле со странами Субсахарской Африки, здесь подготовительная работа ведется с 2020 г. – когда был впервые протестирован *цифровой юань* (*e-CNY*)[279]. Переход на *e-CNY* в торговле со странами АЮС позволит облегчить и ускорить взаимодействие между сторонами, а также снизить риски дополнительных издержек. При развитии данного направления Пекин делает упор, в первую очередь, на диалог с Нигерией – единственной страной АЮС, имеющей активную цифровую валюту, рассчитывая в перспективе масштабировать опыт на остальной Континент[280].

Сектор ***искусственного интеллекта*** – одно из направлений, где КНР стремится обеспечить себе глобальное лидерство не только в технологическом, но и в идейном плане. В 2023 г. Пекин запустил Глобальную инициативу в области ИИ, направленную на продвижение китайского видения формата развития глобального сотрудничества и сопутствующих рисков развития ИИ-технологий[281]. Кроме того, Пекин является подписантом Блетчлианской декларации Саммита по безопасности ИИ (2023 г.)[282] и разделяет идею этического подхода к использованию передовых технологий.

ИИ-фактор в контексте диалога со странами АЮС раскрывается в несколько направлений. В первую очередь, это поддержка Пекином инициатив региональных объединений (например, «Повестки дня 2063 г.» Африканского союза, где подчеркивается значение передовых технологий в развитии экономик региона)[283]. Китайская сторона стремится подчеркнуть, что идеи, изложенные в «Повестке», перекликаются с китайскими

[277] 2024 China-Africa Digital Financial Inclusion Summit (CADFIS 2024) // Making Finance Work for Africa. URL: https://www.mfw4a.org/events/2024-china-africa-digital-financial-inclusion-summit-cadfis-2024

[278] Forum on China-Africa Cooperation Beijing Action Plan (2025-2027) // PRC Ministry of Foreign Affairs. 05.09.2024. URL: https://www.mfa.gov.cn/eng/xw/zyxw/202409/t20240905_11485719.html

[279] China's digital currency: Next stop, Africa? // the Interpreter. URL: https://www.lowyinstitute.org/the-interpreter/china-s-digital-currency-next-stop-africa

[280] China's Central Bank Digital Currency: A New Force in African Finance? // SAIIA. 28.03.2024. URL: https://saiia.org.za/research/chinas-central-bank-digital-currency-a-new-force-in-african-finance/

[281] 全球人工智能治理倡议 (Глобальная инициатива по управлению искусственным интеллектом) // Cyberspace Administration of China. 18.10.2023. URL: https://www.cac.gov.cn/2023-10/18/c_1699291032884978.htm

[282] The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023 // UK Government. 01.11.2023. URL: https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023

[283] The State of Cybersecurity in Africa: The Chinese Effect // Access Partnership. 23.06.2022. URL: https://accesspartnership.com/the-state-of-cybersecurity-in-africa-the-chinese-effect/

долгосрочными интересами в части развития глобального философского проекта «Сообщества Единой судьбы»[284].

Во-вторых, Поднебесная развивает собственные координационные форматы в сфере ИИ – в первую очередь, Китайско-африканский форум по развитию и сотрудничеству в области интернета, на котором в 2024 г. ИИ-сектор был признан самостоятельным направлением межгосударственной кооперации[285]. В рамках Сямыньского совместного заявления (апрель 2024 г.) КНР и страны Африки определили следующие приоритеты взаимодействия в сфере искусственного интеллекта:

- укрепление механизмов диалога и сотрудничества по вопросам политики, технологий, промышленности, приложений, управления и передового опыта в области ИИ;
- содействие технологическим исследованиям, разработкам и применению на китайских и африканских предприятиях, в университетах и научно-исследовательских учреждениях в таких областях, как анализ больших данных, технологии машинного обучения и др.;
- содействие промышленной кооперации, развитию и применению ИИ-технологий, в том числе в сельском хозяйстве, медицине, образовании и управлении городским хозяйством, а также поддержке цифровой инфраструктуры;
- проведение обмена талантами и наращивание потенциала, включая предоставление онлайн-курсов и профессионального обучения;
- создание прочных барьеров безопасности сети и данных, включая разработку проверяемых, контролируемых, отслеживаемых и надежных технологий искусственного интеллекта, а также предотвращение злоупотребления искусственным интеллектом при проведении кибератак[286].

Третье направление – взаимодействие в двустороннем формате. Пекин стремится наладить профильный диалог со всеми государствами АЮС, проявляющими интерес к технологиям ИИ и их внедрению в производственные процессы. Примечательно также, что при налаживании межведомственного взаимодействия КНР нередко апеллирует к глобальному и региональному форматам взаимодействия, тем самым придавая диалогу *флер* преемственности.

Весьма интересно раскрывается феномен китайско-американского технологического соперничества в секторе ИИ. Африканский рынок ИИ-решений остается одним из немногих мест, где Пекин и Вашингтон действуют скорее взаимодополняюще, а влияние в тех или иных странах региона практически не оспаривается другим оппонентом[287]. При этом подобный *паритет*, с высокой долей вероятности, не просуществует долго: трения между оппонентами нарастают, и баланс интересов в странах АЮС соблюдается между ними все меньше[288].

---

[284] China-Africa Collaboration for a Shared Future // Science and Technology Daily.09.09.2024. URL: https://www.stdaily.com/web/English/2024-09/09/content_226570.html

[285] 2024年中非互联网发展与合作论坛关于中非人工智能合作的主席声明 (Заявление Председателя Китайско-африканского форума по развитию и сотрудничеству в области интернета 2024 года по китайско-африканскому сотрудничеству в области искусственного интеллекта) // // Cyberspace Administration of China. 03.04.2024. URL: https://www.cac.gov.cn/2024-04/03/c_1713731793084792.htm

[286] Там же.

[287] China-US AI cooperation in Africa is crucial for continental development // Global Times. 07.08.2024. URL: https://www.globaltimes.cn/page/202408/1317549.shtml

[288] AI in Africa opens up new battlefront for China, US // Semafor. 30.04.2024. URL: https://www.semafor.com/article/04/30/2024/ai-africa-battlefront-china-us

Что касается ***сектора ПО***, то здесь КНР также действует весьма активно. По состоянию на 2024 г. достигнуты договоренности о профильном сотрудничестве с 2/3 стран АЮС – речь идет как о поставке готовых решений, так и совместной разработке (включая *нулевой*, подготовительный цикл, ориентированный на подготовку кадров в стране-партнере)[289]. Подобный подход последовательно реализуется Пекином с середины 2010-х гг.

Говоря о китайской стратегии покорения региона АЮС, следует обратить особое внимание на т.н. *Мастерские Лу Баня*[290] – международный образовательный проект Пекина, ориентированный на передачу китайского опыта в области производства и технологий (включая прикладные цифровые компетенции) слушателям из более чем 20 государств мира (включая страны Африки)[291]. Реализация «Мастерских» в государствах АЮС позволяет Пекину не только налаживать взаимодействие с региональными специалистами под эгидой предприятий КНР, но и эффективно *готовить почву* для дальнейшей передачи сопутствующих технологий более широкого спектра и тем самым обеспечить себе дополнительное упрочнение позиций на региональном рынке.

Вместе с тем, слабой стороной подхода КНР к налаживанию связей со странами Субсахарской Африки является неоднозначная репутация китайской модели инвестирования. Речь, в первую очередь, о феномене китайской *долговой ловушки* – когда в обмен на выгодные инфраструктурные кредиты и щедрое инвестирование в технологический сектор КНР получает рычаги влияния на политические решения того или иного государства[292]. Вызывает вопросы и феномен «китайского неоколониализма», подразумевающий, что Пекин ведет такую же политику в регионе, что и старые колониальные державы, маскируя свои реальные намерения яркими лозунгами[293].

В обоих случаях «скрепляющим» элементом взаимодействия выступают цифровые технологии. Для стран АЮС, большинство из которых болезненно реагируют на посягательства на собственный цифровой суверенитет, это выступает сдерживающим (хотя и не непреодолимым) фактором при развитии сотрудничества с Пекином – а некоторые лидеры Субсахарских стран и вовсе оспаривают данный тезис[294].

Обобщенный показатель вовлеченности представлен ниже (*см. таблицу 16*).

---

[289] China's contribution to skills development in Sub-Saharan Africa // Acts-Nt. URL: https://www.acts-net.org/blogs/foresight-africa-blog/china-s-contribution-to-skills-development-in-sub-saharan-africa; China-Africa Collaboration for a Shared Future // ST-Daily. URL: https://www.stdaily.com/web/English/2024-09/09/content_226570.html; China-Africa digital cooperation continues advancing, highlighted in infrastructure construction // Global Times. 29.07.2024. URL: https://www.globaltimes.cn/page/202407/1316981.shtml и др.

[290] Лу Бань – полумифический исторический герой, плотник, строитель, архитектор, по преданиям - изобретатель многих примитивных орудий и приспособлений, используемых по сей день. В народной традиции считается обожествленным покровителем плотников, ремесленников и строителей.

[291] Luban Workshop in Africa a valuable asset for vocational education empowering locals //Global Times. 05.09.2023. URL: https://www.globaltimes.cn/page/202309/1297616.shtml; China and Sub-Saharan Africa // EveryCRSReport. 08.01.2024. URL: https://www.everycrsreport.com/reports/IF12566.html

[292] The Innocent Lender: Is China Pursuing “Debt-Trap Diplomacy” in Africa? // CSIS. URL: https://interpret.csis.org/translations/the-innocent-lender-is-china-pursuing-debt-trap-diplomacy-in-africa/

[293] China in Africa: win-win development, or a new colonialism? // The Guardian. 31.07.2018. URL: https://www.theguardian.com/cities/2018/jul/31/china-in-africa-win-win-development-or-a-new-colonialism

[294] China is not pushing Africa into debt trap, South African president says // Reuters. 05.09.2024. URL: https://www.reuters.com/world/africa/china-is-not-pushing-africa-into-debt-trap-south-african-president-says-2024-09-05/

Страна	Цифровая безопасность	Цифровые технологии в экономике и госуправлении	ИИ-Технологии	Разработка ПО
Ангола	2	2	2	3
Бенин	2	2	2	3
Ботсвана	2	2	2	3
Буркина-Фасо	3	2	2	3
Бурунди	2	2	2	3
Габон	2	3	2	3
Гамбия	2	3	3	3
Гана	2	3	2	3
Гвинея	2	2	2	2
Гвинея-Бисау	2	2	2	3
ДРК	2	2	2	3
Замбия	3	2	2	3
Зимбабве	2	2	2	3
Кабо-Верде	2	2	2	2
Камерун	3	2	2	3
Кения	3	4	3	3
Конго	2	2	2	3
Кот-д’Ивуар	2	3	3	3
Лесото	2	2	2	3
Либерия	2	2	2	2
Маврикий	2	3	2	3
Мадагаскар	2	3	2	3
Малави	2	2	2	2
Мали	2	2	2	3
Мозамбик	2	2	2	3
Намибия	2	2	3	3
Нигер	3	3	2	3
Нигерия	3	4	3	3
Руанда	2	3	3	3
Сан-Томе и Принсипи	2	2	2	2
Сейшельские острова	2	2	2	3
Сенегал	3	2	3	2
Сомали	2	2	2	2
Сьерра-Леоне	2	2	2	2
Танзания	4	4	3	3
Того	2	2	2	3
Уганда	3	2	3	3
ЦАР	2	2	2	3
Чад	2	3	2	2
Экваториальная Гвинея	2	2	2	2
Эритрея	2	2	2	3
Эсватини	2	2	2	2
Эфиопия	3	3	3	3
ЮАР	4	4	3	3
Южный Судан	2	2	2	3

Таблица 16. Индекс вовлеченности в развитие системы цифровых технологий стран региона (по 5-балльной шкале)[295]. Составлено автором.

США. Уровень вовлеченности США во взаимодействие с Африкой несколько раз менялся в течение последнего десятилетия. С подачи демократической администрации Джо Байдена вовлеченность Вашингтона в дела африканских государств (особенно в регионе южнее Сахары) вновь начала расти.

Белый дом сочетает публичные высказывания с постепенной «перезагрузкой» подхода к развитию африканского технологического сектора. Например, в 2022 г. США представили новую стратегию развития отношений с Субсахарской Африкой, обозначив в качестве приоритетов диалога вопросы реагирования на новые вызовы[296].

Одним из направлений, на котором Вашингтон могут в перспективе серьезно продвинуться, является ***кибербезопасность***. Как и в случае с регионом Залива, США активно апеллируют к концепции «цифровой солидарности» (под которой в Вашингтоне понимают *«готовность работать вместе над достижением общих целей, помогать партнерам наращивать потенциал и оказывать взаимную поддержку»*)[297].

Американские государственные специалисты и частные IT-компании вовлечены в развитие национального кадрового потенциала, расширение государственно-частного партнерства, а также технических возможностей Субсахарской Африки. Кроме того, стремительно развивающихся африканских рынок цифровых решений вызывает повышенный интерес у американских инвесторов: в конце 2022 г. Вашингтон анонсировал выделение 350 млн долларов на запуск совместной с Африкой инициативы по *цифровой трансформации*, призванной расширить доступ к цифровым технологиям на Континенте[298].

Кроме того, Бюро по вопросам киберпространства и цифровой политики США поддерживает развитие проекта *ProCon Global*, направленного на оказание технического содействия развивающимся странам в сфере обеспечения связности за счёт расширения сети подводных интернет-кабелей при активном участии Google; на эти цели в 2024 г. дополнительно выделено 35 млн долларов[299].

Интерес у Вашингтона прослеживается и в секторе ***финансовых технологий***. США наравне с КНР входят в группу крупнейших *доноров* FinTech-сектора региона АЮС[300]. Согласно оценкам консалтингового агентства *McKinsey & Company*, американские инвесторы обеспечивают финансированием до половины профильных стартапов стран

[295] 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.

[296] U.S. Strategy toward Sub-Saharan Africa (2022) // the White House. URL: https://www.whitehouse.gov/wp-content/uploads/2022/08/U.S.-Strategy-Toward-Sub-Saharan-Africa-FINAL.pdf

[297] United States International Cyberspace & Digital Policy Strategy // US Dept. of State. URL: https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/

[298] US Invests in Africa's Fintech Sector // Voice of Africa. 23.04.2023. URL: https://www.voaafrica.com/a/us-invests-in-africa-fintech/7048008.html

[299] Exclusive: State Department cyber bureau preps funding blitz aimed at boosting allies' defenses // the Record. 24.09.2024. URL: https://therecord.media/state-dept-preps-funding-blitz-to-boost-cyber-defenses-fick

[300] US Invests in Africa's Fintech Sector // Voice of Africa. 23.04.2023. URL: https://www.voaafrica.com/a/us-invests-in-africa-fintech/7048008.html

Субсахарской Африки[301]. Приоритет ожидаемо отдается странам-лидерам рынка – Кении и Нигерии.

Взаимодействие ведется и на государственном уровне: представители Вашингтона регулярно принимают участие в профильных мероприятиях – в числе таковых, например, Африканский FinTech-Саммит (2023 г.)[302], являющийся продолжением переговорного формата «США – Африка».

Сектор ***искусственного интеллекта*** – это сравнительно новое направление партнерства. Однако здесь США выступают в роли одного из ключевых глобальных игроков. Вашингтон за последний год поддержал значительное количество международных инициатив в области ИИ, начиная от принятия первой резолюции по этой теме в Генассамблее в марте 2024 г. до подписания Рамочной конвенции Совета Европы (сентябрь 2024 г.)[303] – первого юридически обязательного (но не очень жёсткого) международного соглашение по ИИ. Белый дом поддерживает любые профильные инициативы, исходящие из Африканского региона – в частности, приветствует усилия по формированию взвешенного подхода африканских государств к применению новых технологий[304].

Кроме того, в рамках следования принципу «этического применения ИИ в бизнесе для совместного процветания», государственные институты США совместно с техногигантами запустили Партнёрство для глобальной инклюзивности в сфере ИИ (*Partnership for Global Inclusivity on AI*). Со стороны бизнеса партнёрами выступили 8 компаний, в т.ч. *Amazon Web Services, Google, IBM, Microsoft, OpenAI*. Госдепартамент и компании обещают потратить суммарно более 100 млн долларов на программы, связанные с устойчивым развитием – ориентированные в т.ч. на Субсахарский регион[305].

Следует отметить, что американо-африканское партнерство в области искусственного интеллекта пока ограничено преимущественно диалоговым форматом – в силу крайне неравномерного развития ИИ-ландшафта государств Субсахарской Африки. Вашингтон стремится своевременно занять зарождающуюся нишу (в т.ч. в части подготовки национальных кадров для нужд ИИ-сектора) – однако в этом вопросе он сталкивается с жесткой конкуренцией со стороны Китая, Индии и ряда других активных игроков[306].

Американские IT-корпорации прочно закрепились ***в секторе ПО*** региона АЮС, и по-прежнему контролируют *львиную долю* рынка. Кроме того, США уделяют повышенное внимание развитию кадрового потенциала стран-партнеров – рассматривая это как шаг к сокращению цифрового неравенства. Запуск профильных образовательных программ, ориентированных на устранение дефицита специалистов в отрасли разработки,

[301] Fintech in Africa: The end of the beginning // McKinsey. URL: https://www.mckinsey.com/industries/financial-services/our-insights/fintech-in-africa-the-end-of-the-beginning

[302] State Department Partners with Africa Fintech Summit // US Dept. of State. 10.04.2023. URL: https://www.state.gov/state-department-partners-with-africa-fintech-summit/

[303] US, Britain, EU to sign first international AI treaty // Reuters. 05.09.2024. URL: https://www.reuters.com/technology/artificial-intelligence/us-britain-eu-sign-agreement-ai-standards-ft-reports-2024-09-05/

[304] African Union committed to developing AI capabilities in Africa // African Union. 28.08.2024. URL: https://au.int/en/pressreleases/20240828/african-union-committed-developing-ai-capabilities-africa

[305] United States and Eight Companies Launch the Partnership for Global Inclusivity on AI // US Dept. of State. 23.09.2024. URL: https://www.state.gov/united-states-and-eight-companies-launch-the-partnership-for-global-inclusivity-on-ai/; State Department Partners with the Government of Nigeria to Host the "Global Inclusivity and AI: Africa" Conference in Lagos // US Dept. of State. 09.09.2024. URL: https://www.state.gov/state-department-partners-with-the-government-of-nigeria-to-host-the-global-inclusivity-and-ai-africa-conference-in-lagos/

[306] African Union committed to developing AI capabilities in Africa // African Union. 28.08.2024. URL: https://au.int/en/pressreleases/20240828/african-union-committed-developing-ai-capabilities-africa

инициирован США и крупными IT-компаниями как минимум в 20 странах Субсахарской Африки[307], и в перспективе Вашингтон планирует увеличивать этот показатель. Поддержка оказывается в том числе уже существующим форматам развития кадрового потенциала (например, проекту «Africa Training»)[308].

Следует отметить, что основной соперник США в регионе АЮС – это Китай. Пекин стремительно наращивает присутствие во всех высокотехнологичных секторах, а китайские компании не уступают американским в части инвестиционной и кооперационной привлекательности. Это вынуждает Вашингтон задействовать более широкий набор инструментов влияния, включая санкционный шантаж, с целью ограничить роль КНР в развитии цифровых систем стран Африки.

На данный момент наиболее уязвимой стороной американского подхода к диалогу со странами АЮС является отсутствие преемственности: каждый следующий американский президент, как правило, полностью пересматривает формат диалога с регионом, ввиду чего начатые при предшественниках проекты и инициативы, как правило, теряют значительную часть поддержки.

Выборы в США выявили наличие у ключевых кандидатов разных (и, более того, не совпадающих с приоритетами администрации Джо Байдена) подходов к выстраиванию взаимодействия с Африкой[309]. А с победой Дональда Трампа вероятность того, что приоритеты диалога «США – АЮС» будут в ближайшей перспективе пересмотрены вновь, увеличилась в разы.

Кроме того, из взаимодействия с Вашингтоном невольно выпадает несколько стран Субсахарской Африки, провозгласивших антизападных курс (Мали, Нигер, Буркина-Фасо) и попавших под санкции США и других западных стран[310].

Обобщенный показатель вовлеченности представлен ниже (*см. таблицу 17*).

Страна	Цифровая безопасность	Цифровые технологии в экономике и госуправлении	ИИ-Технологии	Разработка ПО
Ангола	3	2	2	2
Бенин	3	2	3	2
Ботсвана	3	2	3	2
Буркина-Фасо	0	0	0	0
Бурунди	2	3	2	2
Габон	3	3	3	2
Гамбия	3	3	3	2
Гана	3	4	3	2
Гвинея	2	2	2	2
Гвинея-Бисау	2	2	1	1

[307]Solving Africa's tech talent conundrum: a wicked problem, quality, and quantity // 54 Collective Tech. URL: https://54collective.vc/insight/solving-africas-tech-talent-conundrum-a-wicked-problem-quality-and-quantity/; Sub-Saharan Africa leads enrolments in professional courses // University World News. 10.08.2023. URL: https://www.universityworldnews.com/post.php?story=20230808143139882; AERC Training. URL: https://training.aercafrica.org/

[308] AERC Training. URL: https://training.aercafrica.org/

[309]Full Debate: Harris vs. Trump in 2024 ABC News Presidential Debate | WSJ (YouTube). URL: https://www.youtube.com/watch?v=VgsC_aBquUE

[310] Mali Sanctions // US Dept. of State. URL: https://www.state.gov/mali-sanctions/

ДРК	1	2	1	1
Замбия	3	2	2	2
Зимбабве	3	2	2	1
Кабо-Верде	2	2	2	1
Камерун	3	3	3	2
Кения	4	4	3	2
Конго	3	2	2	2
Кот-д'Ивуар	3	2	2	2
Лесото	2	2	2	2
Либерия	1	1	2	1
Маврикий	4	3	3	2
Мадагаскар	3	2	2	2
Малави	2	2	2	2
Мали	0	0	0	0
Мозамбик	1	2	2	2
Намибия	2	3	2	2
Нигер	0	0	0	0
Нигерия	4	4	3	2
Руанда	3	2	2	2
Сан-Томе и Принсипи	2	2	2	2
Сейшельские острова	1	2	2	2
Сенегал	2	3	2	2
Сомали	1	2	1	1
Сьерра-Леоне	3	2	2	1
Танзания	4	3	3	2
Того	3	2	2	2
Уганда	2	2	2	2
ЦАР	1	2	1	1
Чад	2	3	2	2
Экваториальная Гвинея	1	2	2	2
Эритрея	1	1	2	2
Эсватини	2	2	2	2
Эфиопия	2	3	3	2
ЮАР	3	3	3	2
Южный Судан	1	1	2	1

Таблица 17. Индекс вовлеченности в развитие системы цифровых технологий стран региона (по 5-балльной шкале)[311]. Составлено автором.

Страны ЕС. Африканский континент занимает специфическое положение во внешней политике европейских стран. Это направление позиционируется в качестве одного из «геополитических приоритетов» Евросоюза, а также как *ближайший сосед Европы* и *Братский Континент*[312].

[311] 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.

[312] Africa and the EU // European Union External Action. 30.11.2022. URL: https://www.eeas.europa.eu/eeas/africa-and-eu_en

В документах стратегического планирования ЕС подчеркивается, что два региона связывают тесные экономические связи, ввиду чего Брюссель стремится выстраивать диалог не только на национальном уровне, но и на уровне ключевых региональных (ЭКОВАС, Африканский союз и др.) и межрегиональных (Организация стран Африки, Карибского бассейна и Тихого океана) организаций[313].

Трек высоких технологий ожидаемо является одним из основополагающих в диалоге между странами ЕС и АЮС, и центральное место в нем занимают вопросы ***кибербезопасности***. Это обусловлено тем, что большинство стран Субсахарской Африки испытывают серьезное давление на национальную цифровую инфраструктуру со стороны киберпреступных группировок (в первую очередь, группировок-вымогателей), а их чрезмерная активность в некоторых случаях даже вредит международному имиджу страны[314].

Попытки полноценно интегрировать вопросы кибербезопасности в диалог «ЕС – Африка» предпринимаются с 2020 г., когда в коммюнике ЕС «На пути к всеобъемлющей стратегии с Африкой», помимо важности «цифровой трансформации» Континента, была признана также необходимость совместной работы над защитой от киберугроз[315]. В настоящее время в регионе АЮС под эгидой ЕС запущено несколько инициатив, ориентированных на кибербезопасность, включая регулирование по смежным вопросам – например, участие в развитии компетенций национальных правоохранительных органов[316] – однако все они ориентированы на малые группы партнерских стран (реже – на поддержку уже существующих инициатив региональных организаций[317]). При этом какой-либо профильной инициативы, разработанной с прицелом на весь регион АЮС, Брюсселем пока не предложено.

ЕС делает все больший упор на развитие гуманитарного цифрового сотрудничества. Например, в 2024 г. в Брюсселе состоялась первая в истории неформальная встреча послов ЕС и африканских стран в области кибербезопасности и цифровых технологий, нацеленная на расширение сотрудничества между ЕС и Африкой с использованием возможностей цифровой эпохи[318]. Однако первый опыт реализации проекта оказался сравнительно скромным – участие во встрече приняли лишь несколько представителей АЮС.

Стратегические диалог «Европа – Африка» также нацелен на развитие рынка ***финансовых технологий***. Руководствуясь целью к 2030 г. укорить обеспечение всеобщего доступа

---

[313] Africa and the EU // European Union External Action. 30.11.2022. URL: https://www.eeas.europa.eu/eeas/africa-and-eu_en

[314] Например, из-за феномена «нигерийских писем» (мошеннической информационной атаки с целью получения средств жертвы) Нигерия в 2024 г. заняла 5 место в глобальном рейтинге киберпреступности. См.: World-first “Cybercrime Index” ranks countries by cybercrime threat level // News and Events. 10.04.2024. URL: https://www.ox.ac.uk/news/2024-04-10-world-first-cybercrime-index-ranks-countries-cybercrime-threat-level

[315] Joint Communication to the European Parliament and the Council towards a comprehensive strategy with Africa // European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020JC0004

[316] Africa as a Cyber Player // EU Cyber Direct. 27.01.2021. URL: https://eucyberdirect.eu/research/africa-as-a-cyber-player

[317] Среди поддержанных ЕС инициатив – Конвенция о кибербезопасности и защите персональных данных (Малабоская конвенция), Экспертная группа по кибербезопасности (AUCSEG), флагман кибербезопасности в Повестке дня АС на период до 2063 года, Инициатива по политике и регулированию для цифровой Африки (PRIDA), Программа развития инфраструктуры для Африки (PIDA), Стратегия цифровой трансформации для Африки, Альянс «Умная Африка», Стратегия кибербезопасности ЭКОВАС и План действий САДК по кибербезопасности.

[318] EU-Africa Dialogue on Cyber and Digital Diplomacy // EU. URL: https://belgian-presidency.consilium.europa.eu/en/news/eu-africa-dialogue-on-cyber-and-digital-diplomacy/

жителей Африки к надежным интернет-сетям (в широком понимании термина)[319], страны ЕС реализуют ряд инициатив, направленных на снижение уровня цифрового разрыва в экономике. Среди них программа *Africa Connected*, направленная на мобилизацию инвестиций в поставщиков цифровой инфраструктуры и предприятия цифровых платформ в странах Субсахарской Африки[320]. Также свой вклад в комплексное развитие цифрового ландшафта вносит инфраструктурный трастовый фонд «ЕС – Африка»[321].

Бизнес-сегмент ЕС также играет свою роль, однако его вклад теряется на фоне действий институтов ЕС: прямое участие крупных европейских FinTech-компаний в развитии цифрового ландшафта стран АЮС прослеживается едва ли в половине стран региона.

Говоря о развитии ***технологий искусственного интеллекта***, следует упомянуть, что страны ЕС стремятся не только выйти на лидирующие позиции в отрасли, но и стимулировать развитие профильного рынка в странах АЮС (включая его нормативно-правовую составляющую). Например, Брюссель оказывает содействие Замбии в разработке национальной ИИ-доктрины[322], а также Кении в постепенной гармонизации национального законодательства[323].

При этом нормативно-правовые акты, принимаемые в самом ЕС, также оказывают существенное влияние на динамику развития ИИ-рынка АЮС. Так, принятый в конце 2023 г. «Закон ЕС об искусственном интеллекте»[324] устанавливает новый, более строгий стандарт регулирования и правоприменения ИИ для компаний, использующих ИИ-технологии в продуктах или услугах, ориентированных на жителей ЕС. Это создает дополнительные препятствия и риски для стран АЮС, экспортирующих готовые ИИ-решения в европейские страны (ЮАР)[325]. Среди других государств региона также идет активная дискуссия о пределах следования *букве* европейского закона и возможных рисках для национальных экономик[326].

Нередко эти дискуссии перекликаются с обсуждениями перспектив комплексной гармонизации нормативно-правового поля стран АЮС – тем более, что наличием достаточного количества профильных НПА могут похвастаться только 2/3 африканских стран[327].

---

[319] Accelerating the digital transition // EU. URL: https://international-partnerships.ec.europa.eu/policies/global-gateway/initiatives-region/initiatives-sub-saharan-africa/eu-africa-global-gateway-investment-package_en#accelerating-the-digital-transition

[320] Africa Connected // EU. URL: https://international-partnerships.ec.europa.eu/funding-and-technical-assistance/funding-instruments/european-fund-sustainable-development-plus/africa-connected_en

[321] EU-Africa Infrastructure Trust Fund. URL: https://www.eu-africa-infrastructure-tf.net/

[322] Zambia working with EU on AI strategy // CoinGeek. URL: https://coingeek.com/zambia-working-with-eu-on-ai-strategy/

[323] AI law: Should Kenya follow in the EU footsteps? // Business Daily Africa. 05.06.2024. URL: https://www.businessdailyafrica.com/bd/corporate/enterprise/ai-law-should-kenya-follow-in-the-eu-footsteps--4647674

[324] EU AI Act has implications for SA-based firms // IT-Web. 31.07.2024. URL: https://www.itweb.co.za/article/eu-ai-act-has-implications-for-sa-based-firms/raYAyqor2ANMJ38N

[325] Ibidem.

[326] AI law: Should Kenya follow in the EU footsteps? // Business Daily Africa. 05.06.2024. URL: https://www.businessdailyafrica.com/bd/corporate/enterprise/ai-law-should-kenya-follow-in-the-eu-footsteps--4647674

[327] Reforming data regulation to advance AI governance in Africa // Brookings. 15.03.2024. URL: https://www.brookings.edu/articles/reforming-data-regulation-to-advance-ai-governance-in-africa/

Другое направление профильной работы ЕС – развитие инновационных научно-исследовательских проектов с опорой на инфраструктуру Африканско-европейских кластеров передового опыта в области исследований (*CoRE*), к работе над которыми привлечены ведущие университеты Континента[328].

В вопросах ***разработки ПО*** наблюдается некоторая разнонаправленность. Европейские фирмы активно осваивают рынок ПО стран АЮС, конкурируя с американскими, индийскими и китайскими поставщиками, однако системная работа на этом направлении под эгидой Брюсселя пока не ведется.

Несмотря на довольно активное сотрудничество ЕС (как коллективного игрока) и стран АЮС по цифровым вопросам, некоторые члены ЕС (например, Франция и Германия), зачастую, предпочитают действовать вне рамок *Евросемьи*, выстраивая отношения с Африкой в индивидуальном формате. В вопросах кибербезопасности и Париж, и Берлин делают ставку на развитие двусторонней кооперации с африканскими государствами, ставя во главу угла противодействие организованной киберпреступности. Кроме того, определенная нагрузка по развитию цифровых компетенций африканских союзников возложена на профильные институты НАТО. Это влечет за собой некоторую рассинхронизацию действий Европы на африканском направлении, что сказывается на темпах сотрудничества.

Также в последние годы из «африкано-европейского диалога» волей-неволей выпали несколько государств – Мали, Буркина-Фасо и Нигер – легитимность властей которых по-прежнему оспаривается Брюсселем[329].

Обобщенный показатель вовлеченности (для группы в целом[330]) представлен ниже (*см. таблицу 18*).

Страна	Цифровая безопасность	Цифровые технологии в экономике и госуправлении	ИИ-Технологии	Разработка ПО
Ангола	2	1	2	1
Бенин	2	2	1	2
Ботсвана	2	1	1	1
Буркина-Фасо	0	0	0	0
Бурунди	2	1	1	1
Габон	3	2	2	1
Гамбия	2	3	2	1
Гана	3	3	3	2
Гвинея	2	1	2	1
Гвинея-Бисау	2	1	1	1

[328] New Africa-Europe Clusters of Research Excellence launched // ARUA. 25.09.2023. URL: https://arua.org/new-africa-europe-clusters-of-research-excellence-launched/

[329] Mali: Council renews restrictive measures for a further year // EU. 11.12.2023. URL: https://www.consilium.europa.eu/en/press/press-releases/2023/12/11/mali-council-renews-restrictive-measures-for-a-further-year/

[330] Для удобства дальнейшей оценки и сравнения с конкурентами показатели группы округлены до целых чисел.

ДРК	1	0	0	0
Замбия	2	2	4	2
Зимбабве	2	1	2	1
Кабо-Верде	2	2	2	1
Камерун	3	3	4	2
Кения	3	3	4	3
Конго	3	2	3	2
Кот-д'Ивуар	2	2	2	1
Лесото	2	1	1	1
Либерия	1	1	1	1
Маврикий	3	2	4	3
Мадагаскар	2	2	2	2
Малави	2	1	2	1
Мали	0	0	0	0
Мозамбик	2	1	1	1
Намибия	3	2	2	1
Нигер	0	0	0	0
Нигерия	3	3	3	2
Руанда	2	3	3	2
Сан-Томе и Принсипи	2	2	2	0
Сейшельские острова	2	1	1	0
Сенегал	3	2	2	1
Сомали	2	1	1	0
Сьерра-Леоне	2	3	2	1
Танзания	3	3	3	2
Того	2	2	2	1
Уганда	2	3	2	1
ЦАР	1	1	1	0
Чад	3	3	3	2
Экваториальная Гвинея	2	2	2	1
Эритрея	1	1	1	1
Эсватини	2	1	2	1
Эфиопия	3	3	3	2
ЮАР	3	3	4	3
Южный Судан	1	1	1	1

Таблица 18. Индекс вовлеченности в развитие системы цифровых технологий стран региона (по 5-балльной шкале)[331]. Составлено автором.

[331] 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.

Аравийские монархии. Государства Арабского мира также стремятся повысить уровень своего участия в делах Субсахарской Африки – этому способствует как географическая близость и совместная работа в рамках интеграционных площадок, так и растущая инвестиционная активность отдельных арабских держав (аравийские монархии) в регионе[332].

Сектор кибербезопасности является сегодня одной из основных точек приложения усилий – тем более, что как минимум три аравийские монархии (Саудовская Аравия, ОАЭ и Катар) достигли показателей абсолютной киберготовности по версии МСЭ[333].

Упор сделан как на развитие межведомственного сотрудничества по профилю цифровой защиты (соответствующие соглашения как минимум с одной монархией ССАГЗ подписаны у 70% африканских стран)[334], так и на интенсификацию диалога в бизнес-сегменте. При этом в тройку лидеров по частоте контактов входят Саудовская Аравия, ОАЭ и Катар; позиции наращивает Бахрейн. Оман и Кувейт демонстрируют кратно меньшую вовлеченность, однако также представлены на региональном цифровом рынке (*см. диаграмму 10*).

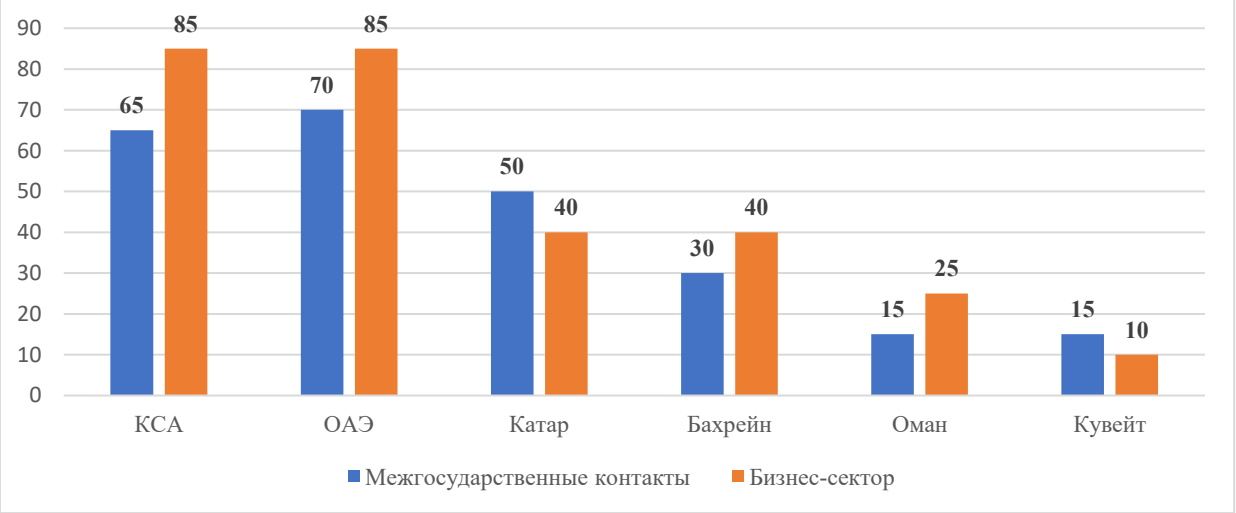

Диаграмма 10. Процент стран региона АЮС, охваченных контактами с аравийскими монархиями (по состоянию на начало 2024 г., %)[335]. Составлено по открытым источникам.

Кроме того, аравийские монархии стремятся привлечь киберкоманды государств АЮС к участию в крупных профильных конференциях[336] – чтобы, с одной стороны, обеспечить

[332] О деятельности Алжира, Египта и Марокко см. подраздел «Арабские страны Северной Африки».
[333] 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
[334] Qatar & Rwanda Partner to Boost Cybersecurity in Africa // Dark Reading. 15.11.2023. URL: https://www.darkreading.com/ics-ot-security/qatar-rwanda-partner-to-boost-cybersecurity-in-africa; Saudi Arabia and Ghana Strengthen Collaboration on Agricultural and Food Security // MEWA. 11.05.2024. URL: https://www.mewa.gov.sa/en/MediaCenter/News/Pages/News9212020.aspx и др.
[335] 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.
[336] Примером таких мероприятий служит Конвенция по кибербезопасности и хакерству «Black Hat», на ежегодной основе проводимая с 2021 г. в Саудовской Аравии. Конференция считается «точкой сборки» передовых команд Ближнего Востока и Африки. См.: BlackHat-ME-A. URL: https://blackhatmea.com/

обмен передовым опытом между странами ССАГПЗ и АЮС, а, с другой, выявить перспективных специалистов для дальнейшего наращивания сотрудничества.

С другой стороны, участие стран ССАГЗ в развитии социального измерения цифровой безопасности АЮС можно охарактеризовать как сравнительно низкое – в том числе потому, что инструменты защиты социального киберпространства в большинстве аравийских монархий еще находятся в стадии становления. По тем же причинам державы ССАГЗ практически не участвуют в гармонизации законодательного поля стран Субсахарской Африки.

Рынок финансовых технологий стран АЮС видится для аравийских монархий привлекательным. Большинство стран сделали упор на обмен профильным опытом между регионами в рамках специализированных FinTech-площадок[337]. Также для аравийского бизнес-сектора характерно стремление расширить сотрудничество с африканскими стартапами. При этом взаимодействие ведется исключительно в двустороннем формате – какие-либо инициативы, выдвинутые от лица ССАГЗ и ориентированные на африканских партнеров, в настоящий момент отсутствуют.

Сходим образом ситуация складывается и в части торговли криптовалютами, т.к. *криптовалютный ландшафт* ССАГЗ неравномерен, и использование этого типа активов полностью одобряет лишь несколько стран (ОАЭ, Бахрейн, Оман). Однако те страны, в которых криптовалютные операции поставлены «на поток» весьма преуспевают в диалоге со странами АЮС – способствуя, например, развитию национальных блокчейн-технологий и созданию инновационной инфраструктуры[338], что позитивно отражается на экономическом благосостоянии стран-партнеров и укрепляет стратегический диалог.

Прямое сотрудничество аравийских монархий и стран АЮС по развитию системы цифровых госсервисов практически не прослеживается – хотя почти все государства, входящие в ССАГЗ (за исключением разве что Кувейта) участвуют в развитии проектов, косвенно связанных с этим сектором – например, ориентированных на совершенствование инструментов «электронного здравоохранения»[339].

Взаимодействие в области развития ***ИИ-технологий*** между странами АЮС и аравийскими монархиями развивается скачкообразно и ожидаемо сконцентрировано на региональных лидерах отрасли (Маврикий, Руанда, Кения). Акцент сделан на создание инфраструктуры и поддержку научных исследований в странах АЮС, монархии Залива в данном случае выступают преимущественно как инвесторы[340].

---

[337] Arab-Afro Digital Payment Symposium Exhibit & Awards. URL: https://www.arabafrodigipaysymposium.com/

[338] Например, ОАЭ укрепили связи с Кенией, считающейся одним из лидеров регионального блокчейн-рынка. См.: Kenya partners with Abu Dhabi's Venom Foundation to build blockchain, Web3 hub // Coin Telegraph. 10.05.2023. URL: https://cointelegraph.com/news/kenya-partners-with-abu-dhabi-s-venom-foundation-to-build-blockchain-web3-hub

[339] См., напр.: OSP Announces Empowering Africa with Several Saudi Ministries. URL: https://www.moenergy.gov.sa/en/MediaCenter/ClimateWeek/Pages/OSP-Announces-Empowering-Africa-with-Several-Saudi-Ministries.aspx и др.

[340] UAE looks at Kenya to build AI and digital infrastructure // Edge. 01.04.2024. URL: https://www.edgemiddleeast.com/industry/uae-looks-at-kenya-for-ai-and-digital-infrastructure; Saudi Arabia, Mauritius Sign MoU on Direct Investment // Leaders. 29.05.2024. URL: https://www.leaders-mena.com/saudi-arabia-mauritius-sign-mou-on-direct-investment/ и др.

Что касается ***сектора разработки ПО***, то здесь сотрудничество аравийских монархий и стран АЮС носит весьма условный характер. Учитывая, что страны ССАГЗ (включая лидеров рейтинга киберготовности) по-прежнему склонны закупать готовые решения вместо разработки собственных, развитие сотрудничества по линии разработки собственных продуктов не входит в число первоочередных приоритетов. С другой стороны, отдельные национальные фирмы, специализирующиеся на разработке и локализации ПО (например, саудовская *Saudisoft*)[341], работают над расширением присутствия на рынке стран Африки южнее Сахары.

Обобщенный показатель вовлеченности (для анализируемой группы в целом[342]) представлен ниже (*см. Таблицу 19*).

Страна	Цифровая безопасность	Цифровые технологии в экономике и госуправлении	ИИ-Технологии	Разработка ПО
Ангола	1	1	1	1
Бенин	1	1	1	1
Ботсвана	1	1	1	1
Буркина-Фасо	0	0	1	1
Бурунди	0	0	1	1
Габон	2	0	1	1
Гамбия	1	3	1	1
Гана	2	3	1	1
Гвинея	1	2	1	1
Гвинея-Бисау	1	0	1	1
ДРК	0	0	1	1
Замбия	1	2	1	1
Зимбабве	2	1	1	1
Кабо-Верде	1	1	1	1
Камерун	2	3	1	1
Кения	3	3	4	2
Конго	1	2	1	1
Кот-д'Ивуар	1	2	1	1
Лесото	0	1	1	1
Либерия	0	1	1	1
Маврикий	2	4	4	2
Мадагаскар	1	3	1	1
Малави	1	0	1	1
Мали	0	1	1	1
Мозамбик	1	2	1	2
Намибия	2	1	1	1
Нигер	1	3	1	1
Нигерия	2	4	1	2
Руанда	2	2	4	1

[341] Saudisoft. URL: https://saudisoft.com/

[342] Для удобства дальнейшей оценки и сравнения с конкурентами показатели группы округлены до целых чисел.

Сан-Томе и Принсипи	1	0	1	1
Сейшельские острова	1	0	1	1
Сенегал	0	3	1	1
Сомали	2	1	1	1
Сьерра-Леоне	1	0	1	2
Танзания	3	2	2	1
Того	2	1	1	2
Уганда	2	1	1	1
ЦАР	1	1	1	2
Чад	1	3	1	1
Экваториальная Гвинея	1	1	1	1
Эритрея	0	1	1	1
Эсватини	0	1	1	1
Эфиопия	2	3	2	2
ЮАР	3	4	3	3
Южный Судан	1	2	1	1

Таблица 19. Индекс вовлеченности в развитие системы цифровых технологий стран региона (по 5-балльной шкале)[343]. Составлено автором.

Арабские страны Северной Африки. Решение рассмотреть Арабские страны Северной Африки (Алжир, Марокко и Египет) в отдельной подгруппе обусловлено их специфическим географическим положением *на стыке* Ближнего Востока и Африки, что позволяет им транслировать передовые практики сразу на два направления.

При этом при рассмотрении «Североафриканской группы» из анализа намеренно исключены Ливия и Судан, находящиеся в состоянии затяжной гражданской войны и потому не оказывающие прямого влияния на ландшафт цифрового сотрудничества стран АЮС.

В секторе ***кибербезопасности*** *пальма первенства* принадлежит Египту – единственной на данный момент североафриканской державе, достигшей (по версии экспертов МСЭ) показателя абсолютной киберготовности[344]. Каир в диалоге со странами АЮС выступает не только как поставщик технологий, но и как один из «двигателей» развития панафриканского диалога в области цифровой безопасности и защиты – используя для этих целей международные (например, Африканский союз[345] и Общий рынок Восточной и

[343] 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.

[344] Ближайший конкурент из Североафриканских стран – Марокко (19 место в глобальном рейтинге). 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

[345] Египет продвигает идею создания и развития под эгидой Африканского союза единой стратегии кибербезопасности для стран Африки. См.: The AU took important action on cybersecurity at its 2024 summit – but more is needed // Almendron. 26.02.2024. URL: https://www.almendron.com/tribuna/the-au-took-important-action-on-cybersecurity-at-its-2024-summit-but-more-is-needed/

Южной Африки[346]) и общественные (Региональный саммит по кибербезопасности и Первый арабский и африканский региональный симпозиум, 2016 г.[347]; экспертный круглый стол «Содействие региональной кибербезопасности и стабильности в Африке», 2024 г.[348]) площадки.

Специфическую роль играет Марокко. Благодаря нормализации отношений с Израилем в рамках «Соглашений Авраама» в 2020 г. Марокко существенно укрепило свои цифровые позиции: еще в 2021 г. стороны подписали соглашение о кибербезопасности[349], а в 2024 г. включили ряд смежных вопросов в повестку военного сотрудничества[350].

Открытость к взаимодействию с Израилем сделала Марокко своеобразной *точкой входа* израильских киберфирм в регион – особенно в условиях продолжающегося конфликта в секторе Газа, в свете которого израильское компании подвергаются скрытому давлению со стороны жителей мусульманских стран Африки[351]. Кроме того, Марокко стабильно инвестирует в развитие сектора цифровой безопасности соседей из региона АЮС, укрепляя тем самым влияние на региональные процессы в области цифровизации[352].

Что касается Алжира, то он участвует в развитии цифрового ландшафта АЮС не столь активно – в большей степени сосредоточившись на наращивании собственного киберпотенциала. При этом страна поддерживает общеафриканский курс на совместное противодействие основным киберугрозам – например, деятельности преступных группировок в цифровом пространстве[353].

Рынок ***финансовых технологий*** стран АЮС интересен для компаний, представляющих североафриканский кластер. Наиболее активно на этом направлении действует Марокко: Рабат стремится не только обеспечить присутствие марокканских стартапов на рынках стран АЮС (используя для этих целей в том числе инструменты цифрового исламского банкинга), но и вовлечь передовые компанию АЮС в открытие представительств на своей территории. Это перекликается с долгосрочной целью превращения страны в *FinTech-хаб*, поставленной властями Марокко.

---

[346] При активном участии Каира в 2011 г. разработан проект типового законопроекта о кибербезопасности для стран, входящих в группу. См.: Common Market for Eastern and Southern Africa (COMESA) // COMESA. URL: https://www.comesa.int/wp-content/uploads/2020/05/2011Gazette-Vol.-16.pdf

[347] Regional Cybersecurity Summit and FIRST Arabic and African Regional Symposium, Sharm El Shiekh, Egypt, 30 October - 3 November 2016 // ITU. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/RegSummit_and_FIRST_Symposium_for-Arab_and_Africa_Regions.aspx

[348] Advancing Regional Cyber Security and Stability in Africa – Expert Roundtable // Cybil. URL: https://cybilportal.org/projects/advancing-regional-cyber-security-and-stability-in-africa-expert-roundtable/

[349] Israel, Morocco sign accord for cybersecurity cooperation // Times of Israel. 15.07.2021. URL: https://www.timesofisrael.com/israel-morocco-sign-accord-for-cybersecurity-cooperation/

[350] Morocco, Israel agree to expand military cooperation // Africa news. 18.01.2023. URL: https://www.africanews.com/2023/01/18/morocco-israel-agree-to-expand-military-cooperation/

[351] Israel's Spyware Diplomacy in Africa // ORIENT. URL: https://orientxxi.info/magazine/israel-s-spyware-diplomacy-in-africa,5859; Morocco quietly continues cooperation with Israel despite tension over Gaza // Africa Intelligence. 10.06.2024. URL: https://www.africaintelligence.com/north-africa/2024/06/10/morocco-quietly-continues-cooperation-with-israel-despite-tension-over-gaza,110245854-eve

[352] Morocco: A Significant Investor in Sub-Saharan Africa // Africa Deployments. 16.08.2023. URL: https://africa-deployments.com/morocco-investor-sub-saharan-africa/

[353] Africa faces huge cybercrime threat as the pace of digitalisation increases // Invest Monitor. 16.06.2022. URL: https://www.investmentmonitor.ai/features/africa-cyber-crime-threat-digitalisation/

FinTech-диалог с отдельными странами Субсахарской Африки (например, с Кенией) также развивает Египет[354]. Однако, в отличие от подхода Рабата, Каир сделал ставку на развитие диалога в банковском секторе, включая совместную работу над гармонизацией нормативно-правового поля.

Алжир в гонке за лидерство на FinTech-рынке практически не участвует – так как страна включилась в развитие системы цифровой коммерции в 2017 г., позже значительной части соседей[355]. Тем не менее, выгодное географическое положение страны, а также курс властей на форсированное развитие технологического бизнес-сегмента (с активным заимствованием опыта ведущих держав) формируют позитивный тренд и оставляют возможность для более активного включения Алжира в диалог со странами АЮС уже в среднесрочной перспективе[356].

В вопросах ***развития технологий искусственного интеллекта*** преуспевают все рассмотренные североафриканские страны – профильные площадки для развития ИИ-компетенций созданы в каждой из них. Однако, с точки зрения вектора сотрудничества, преобладает диалог с лидерами отрасли – КНР и Западными странами. Взаимодействие же с АЮС носит скорее эпизодический характер, активный обмен профильным опытом не прослеживается.

В секторе ***разработки ПО*** в регионе АЮС абсолютное лидерство по-прежнему остается за Египтом – в среднем, на одну алжирскую или марокканскую IT-фирму приходится 3-4 египетских компании. Столь явный перевес обусловлен в том числе тем, что Каир сделал ставку на бизнес-диалог с регионом для позитивного подкрепления выносимых Египтом государственных инициатив.

С другой стороны, *догнать* Египет пытается Марокко: страна входит в пятерку лидеров на Африканском континенте по размерам сообщества разработчиков ПО[357], и нацелена на дальнейшую экспансию на рынки Континента. В этом вопросе Рабат рассчитывает в том числе на поддержку США[358].

Обобщенный показатель (для группы государств в целом[359]) вовлеченности представлен ниже (*см. Таблицу 20*).

---

[354] Egyptian firms eye Kenya's thriving sectors // STAR. 05.03.2024. URL: https://www.the-star.co.ke/business/kenya/2024-03-05-egyptian-firms-eye-kenyas-thriving-sectors/

[355] E-payments yet to gain widespread use in Algeria // Oxford Business Group. URL: https://oxfordbusinessgroup.com/reports/algeria/2018-report/economy/card-bargain-despite-legal-changes-e-payments-struggle-to-gain-foothold

[356] Algeria: A "Start-Up Nation" with Global Aspirations // Africa-Me. URL: https://africa-me.com/algeria-a-start-up-nation-with-global-aspirations/

[357] Morocco has the fifth-largest developer community in Africa // Atalayar. 09.06.2023. URL: https://www.atalayar.com/en/articulo/new-technologies-innovation/morocco-has-fifth-largest-developer-community-africa/20220309151707155450.html

[358] Africa's AI Leap: Morocco, US Push for Sustainable Development Through Tech // Morocco World News. 24.07.2024. URL: https://www.moroccoworldnews.com/2024/07/364085/africa-s-ai-leap-morocco-us-push-for-sustainable-development-through-tech

[359] Для удобства дальнейшей оценки и сравнения с конкурентами показатели группы округлены до целых чисел.

Страна	Цифровая безопасность	Цифровые технологии в экономике и госуправлении	ИИ-Технологии	Разработка ПО
Ангола	2	2	0	1
Бенин	3	2	0	1
Ботсвана	3	2	0	1
Буркина-Фасо	2	2	0	1
Бурунди	3	2	0	1
Габон	3	2	0	1
Гамбия	3	2	0	1
Гана	3	3	1	1
Гвинея	3	2	0	1
Гвинея-Бисау	2	2	0	0
ДРК	2	2	0	0
Замбия	3	2	0	1
Зимбабве	3	2	0	1
Кабо-Верде	3	2	0	0
Камерун	2	2	0	1
Кения	4	4	1	3
Конго	4	2	0	1
Кот-д’Ивуар	3	2	0	1
Лесото	3	2	0	0
Либерия	2	2	0	0
Маврикий	4	2	1	1
Мадагаскар	3	2	0	1
Малави	3	2	0	0
Мали	2	2	0	0
Мозамбик	3	2	0	0
Намибия	3	2	0	1
Нигер	3	2	0	1
Нигерия	3	2	0	1
Руанда	4	2	1	1
Сан-Томе и Принсипи	3	2	0	0
Сейшельские острова	3	2	0	0
Сенегал	3	2	0	1
Сомали	2	1	0	0
Сьерра-Леоне	3	2	0	1
Танзания	4	3	0	1
Того	3	2	0	1
Уганда	3	2	0	1
ЦАР	2	1	0	0
Чад	3	2	0	1
Экваториальная Гвинея	3	2	0	0
Эритрея	3	2	0	0

Эсватини	3	1	0	0
Эфиопия	4	3	1	1
ЮАР	4	4	1	1
Южный Судан	3	1	0	0

Таблица 20. Индекс вовлеченности в развитие системы цифровых технологий стран региона (по 5-балльной шкале)[360]. Составлено автором.

Индия. Текущая деятельность Нью-Дели в регионе выстраивается с опорой на *Кампальские принципы*, сформулированные и озвученные премьер-министром Нарендрой Моди в 2018 г.[361]. Согласно им, Индия будет стремиться оказывать Африке комплексную поддержку, сочетающую в себе меры по развитию инновационных технологий и навыков, а также созданию и модернизации инфраструктуры, углублению межгосударственного и государственно-частного партнерства.

Другой интересной чертой политики самопозиционирования Индии в регионе является публичный отказ от *блага взамен* и противопоставление себя *корыстным донорам* региона (под которыми, как правило, подразумеваются КНР, США и европейские игроки).

Одной из «точек опоры» Индии на африканском рынке высоких технологий является сектор ***кибербезопасности***. Страна существенно нарастила компетенции в этой области (хотя по комплексному показателю киберготовности по-прежнему уступает Кении, Танзании, Гане и Маврикию[362]) и стремится экспортировать наработанный опыт.

При этом наибольшая плотность контактов на межведомственном уровне зафиксирована в диалоге с Кенией, Маврикием, ЮАР, Того и Кот-д'Ивуаром (*см. диаграмму 11*).

[360] 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.

[361] Prime Minister's address at Parliament of Uganda during his State Visit to Uganda // Government of India. 25.07.2018. URL: https://www.mea.gov.in/Speeches-Statements.htm?dtl/30152/Prime+Ministers+address+at+Parliament+of+Uganda+during+his+State+Visit

[362] 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

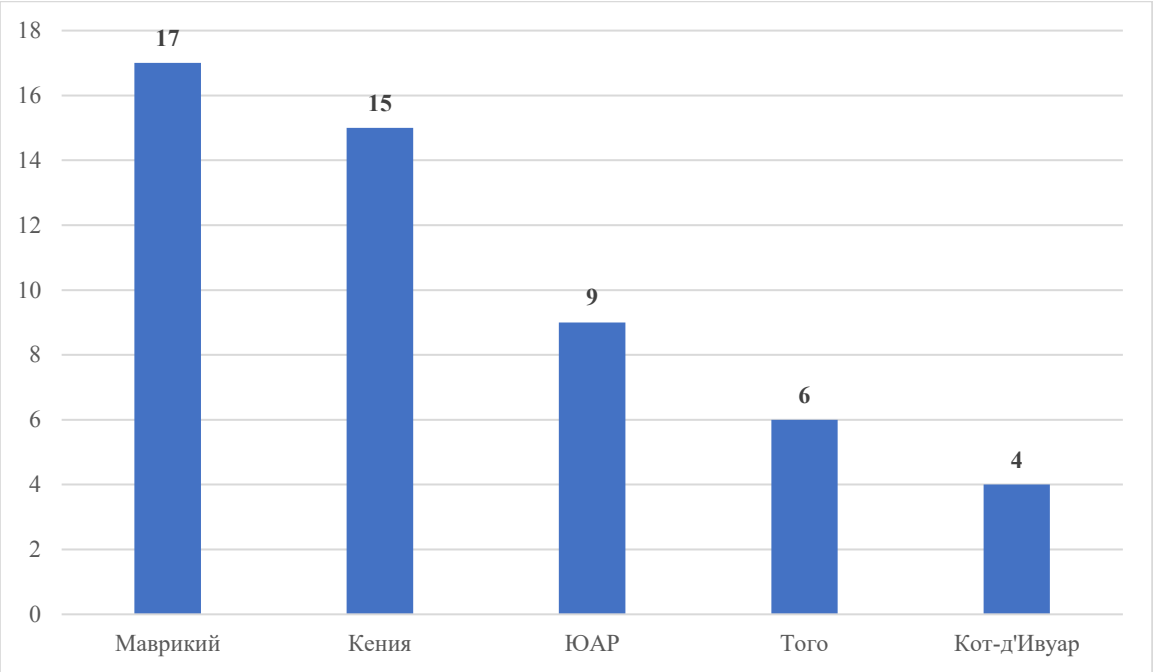

Диаграмма 11. Количество соглашений между Индией и странами АЮС в области кибербезопасности (включая отраслевые и межведомственные), по состоянию на 2024 г. Составлено по открытым источникам.

Индия также предлагает партнерам из региона адаптировать успешные индийские цифровые инициативы («Digital India», «BharatNet», «IndiaStack» и др.) под запросы национального сегмента киберпространства и тем самым купировать некоторые характерные для региона проблемы (например, «утечку мозгов»)[363].

Индийские решения в области ***финансовых технологий*** несколько проигрывают китайским и американских предложениям, однако по темпам развития профильного партнерства Нью-Дели ничуть не уступает Пекину и Вашингтону.

В частности, индийские FinTech-фирмы в том или ином виде представлены на рынках практически всех африканских стран (за исключением Южного Судана и Эритреи). Индийские инвесторы все чаще предоставляют не только капитал, но и технические знания и инновационные решения, которые развивают цифровую инфраструктуру и обеспечивают связь по всему континенту, что выгодно отличает их от конкурентов, заточенных под поставку готовых технологий[364].

Среди прочего Индия стремится способствовать повышению доступности банковских услуг для населения АЮС за счет более широкого внедрения инструментов цифрового банкинга. Например, в 2023 г. индийское правительство выделило 2 млн долларов на финансирование работы Африканского фонда охвата цифровыми финансовыми услугами (*ADFI*)[365].

[363] Mishra A. Elevating the India-Africa partnership to new horizons // Observer Research Foundation. 22.07.2022. URL: https://www.orfonline.org/expert-speak/elevating-the-india-africa-partnership-to-new-horizons/
[364] Tapping into India and Africa's strengths to drive a financial revolution // Africa Business. 22.08.2024. URL: https://africabusiness.com/2024/08/22/tapping-into-india-and-africas-strengths-to-drive-a-financial-revolution/
[365] India commits $2 million as new partner in Africa Digital Financial Inclusion Facility to boost digital financial inclusion across Africa // AFDB. 02.08.2023. URL: https://www.afdb.org/en/news-and-events/press-releases/india-commits-2-million-new-partner-africa-digital-financial-inclusion-facility-boost-digital-financial-inclusion-across-africa-63530

Одним из эффективных проводников индийских интересов в регионе АЮС является «Африканско-индийский FinTech-альянс» (*AIFA*), объединяющий профильные компании Нью-Дели и ряда африканских стран. Работа в рамках AIFA позволяет индийскому технобизнесу более эффективно продвигать свои проекты за счет постепенного включения в систему государственно-частного партнерства.

Сфера ***искусственного интеллекта*** рассматривается индийским руководством как потенциальный инструмент укрепления влияния в Африке[366] – тем более, что Индия в данном случае выступает не только в качестве технологической сверхдержавы, но и как один из полюсов «Глобального Юга». Нью-Дели подвигает ответственный подход к использованию ИИ[367], что находит отражение в диалоге со странами АЮС.

Кроме того, ИИ-составляющая нередко интегрируется в более крупные проекты цифрового развития, что расширяет рамки взаимодействия и не сводит диалог Нью-Дели и партнеров по АЮС к развитию ИИ-кооперации как отдельного явления. Это позволяет включаться в диалог даже тем странам Субсахарской Африки, где развитие ИИ-сектора находится на начальных этапах.

В секторе ***разработки ПО*** усилия Индии сосредоточены на развитии профильного кадрового потенциала в странах АЮС, где влияние индийских IT-фирм наиболее серьезное[368]. Запуск крупных проектов в области совместной разработки пока не получает приоритета.

В целом же, с точки зрения других долгосрочных интересов, Нью-Дели делает ставку на упрочнение своей роли в *зоне исторического контроля* (Сейшельские острова, Мадагаскар, Маврикий) и формирование *естественного противовеса* влиянию других заинтересованных игроков (Китай, Турция).

Обобщенный показатель вовлеченности представлен ниже (*см. Таблицу 21*).

Страна	Цифровая безопасность	Цифровые технологии в экономике и госуправлении	ИИ-Технологии	Разработка ПО
Ангола	1	1	1	1
Бенин	1	1	1	1
Ботсвана	1	1	1	2
Буркина-Фасо	1	1	1	1
Бурунди	1	1	1	1
Габон	2	2	1	2
Гамбия	2	1	1	2
Гана	2	2	1	2
Гвинея	1	1	1	1

[366] AI, energy, Africa to be in focus, says PM Modi as he leaves for Italy for G7 outreach session // Economic Times. 13.06.2024. URL: https://economictimes.indiatimes.com/news/india/ai-energy-africa-to-be-in-focus-says-pm-modi-as-he-leaves-for-italy-for-g7-outreach-session/articleshow/110973374.cms?from=mdr

[367] AI Safety Summit 2023: The Bletchley Declaration // UK Government. URL: https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration

[368] Mauritius announces several digital cooperation projects with India // WeAreTech. 03.10.2022. URL: https://www.wearetech.africa/en/fils-uk/news/public-management/mauritius-announces-several-digital-cooperation-projects-with-india

Гвинея-Бисау	1	1	1	1
ДРК	0	1	1	0
Замбия	1	1	1	1
Зимбабве	1	1	1	1
Кабо-Верде	1	1	1	0
Камерун	2	1	2	1
Кения	4	1	2	2
Конго	2	1	1	1
Кот-д'Ивуар	3	1	1	1
Лесото	1	2	1	0
Либерия	0	1	1	0
Маврикий	4	2	1	3
Мадагаскар	2	2	1	3
Малави	1	2	1	1
Мали	1	1	1	2
Мозамбик	0	1	1	1
Намибия	3	2	1	1
Нигер	1	1	1	1
Нигерия	3	2	2	3
Руанда	4	2	1	2
Сан-Томе и Принсипи	2	1	1	1
Сейшельские острова	3	2	1	2
Сенегал	2	1	1	1
Сомали	1	1	1	1
Сьерра-Леоне	2	2	1	1
Танзания	3	1	1	2
Того	4	1	1	1
Уганда	2	1	1	2
ЦАР	1	1	1	1
Чад	2	1	1	2
Экваториальная Гвинея	1	1	1	1
Эритрея	1	0	1	1
Эсватини	0	1	1	1
Эфиопия	2	1	1	3
ЮАР	4	2	2	2
Южный Судан	1	0	1	1

Таблица 21. Индекс вовлеченности в развитие системы цифровых технологий стран региона (по 5-балльной шкале)[369]. Составлено автором.

[369] 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.

Турция. В течение последних полутора десятилетий Анкара проявляет растущий интерес к Африке. Основу ее внешней политики применительно к региону составляет идея увеличения собственного влияния за счет использования инструментов категорий *soft power* и *smart power*.

Среди прочего Турция выступает одним из наиболее активных критиков «неоколониальной эксплуатации» стран Африки и ее проецирования на цифровое пространство[370]. Самопозиционирование Турции в статусе «защитника интересов африканских народов» приносит свои плоды: показатель влияния Анкары в регионе, начиная с 2021 г., демонстрирует устойчивый рост[371].

В вопросах ***кибербезопасности*** Турция сделала ставку на двустороннее взаимодействие – к настоящему моменту ею подписано как минимум по одному профильному соглашению с 2/3 стран АЮС[372]. В некоторых случаях (Гана, Нигерия, Руанда и др.) профильное сотрудничество охватывает не только гражданские, но и военные аспекты цифровой безопасности.

Общерегиональные форматы взаимодействия также играют свою роль в продвижении турецких приоритетов сотрудничества на африканском направлении. В частности, ключевые аспекты развития цифровой кооперации между Анкарой и Африканским континентом затронуты в Совместном плане действий на 2022-2026 гг.[373].

Кроме того, с 2016 г. Анкара развивает диалог в рамках общественной инициативы *Cybersecurity Alliance for Mutual Progress* (*CAMP*), к которой также присоединились более половины государств АЮС[374], а также на базе глобальной общественной платформы «Global Forum on Cyber Expertise»[375].

Турецкий технологический бизнес все активнее подключается к развитию цифровых систем «отстающих» государств (Сомали)[376], а также расширяет присутствие на внутренних рынках Восточной Африки[377]. Также турецкие IT-фирмы нередко действуют «в связке» с катарскими предприятиями (в рамках укрепления союзнических отношений Анкары и Дохи), что несколько упрощает расширение присутствия на региональном рынке.

Кроме того, Турция рассчитывает в перспективе экспортировать в Африку собственные решения в области кибербезопасности – в частности, модель сотрудничества между

---

[370] Beyond colonialism: Türkiye's unique approach to Africa // Inclusive Society. 17.05.2023. URL: https://www.inclusivesociety.org.za/post/beyond-colonialism-t%C3%BCrkiye-s-unique-approach-to-africa

[371] The Ankara Consensus: How Turkey is boosting influence in rising Africa // African Business. 06.02.2024. URL: https://african.business/2024/02/politics/the-ankara-consensus-how-turkey-is-boosting-influence-in-rising-africa

[372] Посчитано по: UNIDIR.

[373] Africa – Türkiye Joint Action Plan 2022-2026. URL: https://www.itkib.org.tr/files/downloads/Belgeler/2023/Afrika-T%C3%BCrkiye%20Eylem%20Plan%C4%B1.pdf

[374] CAMP Members. URL: https://www.cybersec-alliance.org/camp/membership.do

[375] The GFCE is the platform for international cooperation on strengthening cyber capacity and expertise globally // GFCE. URL: https://thegfce.org/

[376] Цуканов Л.В. Кибербезопасность по-сомалийски // Российский совет по международным делам. 17.01.2022. URL: https://russiancouncil.ru/analytics-and-comments/columns/africa/kiberbezopasnost-po-somaliyski/

[377] Unpacking Turkey's Security Footprint in Africa / SWP. 30.06.2022. URL: https://www.swp-berlin.org/10.18449/2022C42/

государством и несистемными акторами в цифровом пространстве[378]. Пока подобные договоренности не достигнуты ни с одной из стран АЮС, однако интерес к феномену «киберармий», в силу стремительного развития цифрового пространства Континента, постепенно растет.

Турецкие решения в области ***финансовых технологий***, несмотря на высокий уровень цифровизации национального банковского сектора, заметно проигрывают предложениям не только глобальных (США, Китай), но и региональных (аравийские монархии) конкурентов. Представленность турецких фирм, занимающихся электронными финансами, в странах АЮС низкая. Однако это не мешает Анкаре нацеливаться на укрепление позиций в среднесрочной перспективе.

В частности, турецкий Fintech-гигант Colendi планирует к 2025 г. открыть первый африканский офис, который «станет плацдармом для будущего распространения турецкого профильного опыта»[379]. При этом сама Анкара, судя по всему, пока предпочитает сосредоточиться на развитии внутреннего FinTech-рынка и не уделяет большого внимания его внешнему контуру.

Несмотря на то, что Турция активно работает над совершенствованием правового режима в области торговли криптоактивами, к 2024 г. профильный закон был принят в «экспериментальном» формате, и получил неоднозначные оценки[380]. В свете отсутствия исчерпывающего регулирования Анкара пока не делает большой ставки на развитие диалога со странами АЮС в контексте операций с криптоактивами.

Сектор ***ИИ-технологий*** видится перспективным в контексте приоритетов Турции на африканском направлении. Анкара стремительно развивает национальные ИИ-компетенции (как практические, так и нормативно-правовые)[381] и, с высокой долей вероятности, попытается поставить идею *гармоничного со-развития* турецкого и африканского ИИ-рынков во главу взаимодействия со странами АЮС. Тем более, что подобный подход перекликается с духом Блетчлианской декларации по безопасности применения ИИ 2023 г.[382], подписантом которой, наравне с другими передовыми державами, является Анкара. Однако на данный момент сотрудничество Анкары и стран АЮС носит скорее эпизодический характер и замкнуто на страны-лидеры отрасли.

---

[378] Цуканов Л.В. «Киберянычары»: пять лет на службе Турции // Российский совет по международным делам. 08.12.2022. URL: https://russiancouncil.ru/analytics-and-comments/analytics/kiberyanychary-pyat-let-na-sluzhbe-turtsii/; Также подробнее о «турецкой» модели организации взаимодействия с национальным хакерским движением См. Приложение 1.

[379] Turkish Fintech Colendi Launches AI Solution, Plans Africa Expansion // the Kenyan Wall Street. 19.09.2024. URL: https://kenyanwallstreet.com/turkish-fintech-colendi-launches-ai-solution-plans-africa-expansion/

[380] Unpacking Turkey's Crypto Draft Bill // Wyden. 25.06.2024. URL: https://www.wyden.io/intelligence/unpacking-turkeys-crypto-draft-bill-and-its-implications/#:~:text=In%20May%202024%2C%20the%20Turkish,written%20contractual%20agreements%20with%20customers.

[381] Turkey's AI roadmap looks to boost economy and add thousands of job // TRT. URL: https://www.trtworld.com/magazine/turkey-s-ai-roadmap-looks-to-boost-economy-and-add-thousands-of-jobs-49435; Turkey: AI bill submitted to Parliamentary Committee // Data Guidelines. 28.06.2024. https://www.dataguidance.com/news/turkey-ai-bill-submitted-parliamentary-committee

[382] Декларацию подписали 28 стран. Из стран АЮС среди подписантов фигурирует Нигерия. См.: AI Safety Summit 2023: The Bletchley Declaration // UK Government. URL: https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration

Сотрудничество Турции и стран АЮС в вопросах ***разработки ПО*** имеет сравнительно скромные масштабы. Турецкие фирмы, специализирующиеся на коммерческой разработке, представлены на рынках Кении, Ганы и ряда других африканских держав, однако их активность имеет скачкообразный характер, а по объемам сотрудничества они уступают конкурентам из КНР и США.

Обобщенный показатель вовлеченности представлен ниже (*см. таблицу 22*).

Страна	Цифровая безопасность	Цифровые технологии в экономике и госуправлении	ИИ-Технологии	Разработка ПО
Ангола	1	0	0	0
Бенин	2	0	0	0
Ботсвана	2	0	0	0
Буркина-Фасо	1	0	0	0
Бурунди	1	0	0	0
Габон	1	1	0	1
Гамбия	2	1	1	1
Гана	2	1	1	2
Гвинея	1	0	0	1
Гвинея-Бисау	1	0	0	0
ДРК	1	0	0	0
Замбия	2	0	0	1
Зимбабве	1	0	0	0
Кабо-Верде	1	0	0	0
Камерун	2	1	1	1
Кения	2	1	2	2
Конго	2	1	1	0
Кот-д’Ивуар	1	0	0	0
Лесото	1	0	0	0
Либерия	1	0	0	0
Маврикий	1	1	2	0
Мадагаскар	1	0	1	1
Малави	1	0	0	0
Мали	1	0	0	0
Мозамбик	1	0	0	0
Намибия	2	1	0	1
Нигер	1	1	0	0
Нигерия	1	1	2	1
Руанда	2	1	1	1
Сан-Томе и Принсипи	1	0	0	0
Сейшельские острова	1	0	0	0
Сенегал	1	1	0	0
Сомали	2	1	0	1
Сьерра-Леоне	1	0	0	0
Танзания	2	1	2	1
Того	1	0	0	1
Уганда	1	0	0	1

ЦАР	1	0	0	0
Чад	1	0	0	1
Экваториальная Гвинея	1	0	0	0
Эритрея	1	1	0	0
Эсватини	1	0	0	0
Эфиопия	2	1	1	0
ЮАР	2	1	3	1
Южный Судан	1	0	0	0

Таблица 22. Индекс вовлеченности в развитие системы цифровых технологий стран региона (по 5-балльной шкале)[383]. Составлено автором.

Иран. Рост присутствия Ирана на технологическом рынке стран АЮС – сравнительно новое явление. Несмотря на то, что африканское направление, находило то или иное отражение в иранских документах стратегического планирования с начала 2000-х гг., диалог со странами Континента развивался скачкообразно. Он приобрел устойчивые рамки только в период президентства Хасана Роухани, когда были подписаны первые профильные соглашения со странами региона[384].

Иранское сотрудничество со странами АЮС в секторе ***кибербезопасности***, на первый взгляд, носит довольно ограниченный характер – у Тегерана подписано лишь два профильных соглашения о межведомственном взаимодействии с Угандой (2014 г.)[385] и ЮАР (2017 г.)[386] – а по интенсивности контактов Исламская Республика сильно уступает конкурентам с Аравийского полуострова.

Однако, с учетом специфического политико-экономического положения Ирана, его прямое взаимодействие с зарубежными партнерами сильно ограничивается санкционным давлением со стороны США и европейских стран.

По этой причине Исламская Республика все больше упирает на развитие отношений в бизнес-сегменте (используя в качестве проводника интересов в т.ч. совместные с африканцами фирмы), где Тегеран ничуть не отстает от большинства аравийских монархий. Кроме того, начиная с 2014 г. Тегеран активно развивает диалог в рамках общественной инициативы *Cybersecurity Alliance for Mutual Progress* (*CAMP*), к которой также присоединились более половины государств АЮС[387].

[383] 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.

[384] Raisi Goes to Africa in Search of Allies for Iran // Stimson. 26.07.2023. URL: https://www.stimson.org/2023/raisi-goes-to-africa-in-search-of-allies-for-iran/

[385] Uganda – Iran: security cooperation // UPF. URL: http://www.upf.go.ug/security-cooperation-uganda-iran/

[386] Iran, South Africa agree to expand ICT cooperation // AzerNews. 21.09.2017. URL: https://tvcnews.tv/2017/09/iran-south-africa-agree-to-expand-ict-cooperation/

[387] CAMP Members. URL: https://www.cybersec-alliance.org/camp/membership.do

Также диалог с мусульманскими странами Африки ведется под эгидой ОИС и Исламского банка развития (ИБР), где Иран выступает в качестве одного из активных проводников идеи цифровой трансформации Исламского мира[388].

С другой стороны, на образ Тегерана, как потенциального *экспортера цифровой безопасности* деструктивно влияет деятельность лояльных ему хакерских команд, наносящих периодические удары по цифровой инфраструктуре африканских стран – среди государств АЮС от подобных выпадов на регулярной основе страдает, например, Танзания[389].

В секторе ***финансовых технологий*** сотрудничество ИРИ и африканских стран не столь значительно, и сконцентрировано преимущественно в секторе цифрового банкинга. Африканские страны проявляют интерес к иранским решениям – в первую очередь, опыту развития Межбанковской сети передачи информации (*Shetab*). Также повышенный интерес вызывает опыт Тегерана по выстраиванию «политики замещения» цифровых сервисов национальными аналогами и выстраивания диалога со стартап-сообществом.

В контексте оценки сотрудничества с использованием финансовых технологий следует обратить внимание на сектор криптовалютных операций – особенно с учетом стремительного роста популярности данного типа активов в государствах АЮС. Известно, что ранее Иран вел переговоры о проведении крипторасчетов как минимум с одной африканской страной (ЮАР, 2019 г.)[390]. Кроме того, начиная с 2019 г. Тегеран пытается (хотя и без особого успеха) привлечь мусульманские страны АЮС к проведению расчетов в *стейблкоинах*, чей курс привязан к золоту[391].

Сотрудничество по развитию цифровых госсервисов между Ираном и странами Субсахарской Африки, как таковое, не прослеживается – хотя власти Исламской Республики и поддерживают профильные инициативы ООН в отношении Африканского континента.

При этом потенциально интересным направлением взаимодействия в долгосрочной перспективе можно стать иранский опыт создания «внутреннего Интернета» – Национальной информационной сети (*NIN*), которая является платформой для предоставления государственных цифровых услуг и информации, но при этом не содержит деструктивного внешнего контента[392]. Для ряда стран АЮС, испытывающих систематическое информационное давление (например, для Мали, Нигера и Буркина-Фасо)

[388] Digital and Sustainable Trade Facilitation in the Organization of Islamic Cooperation (OIC) Asian Countries (2024) // ISDB. URL: https://www.isdb.org/publications/digital-and-sustainable-trade-facilitation-in-the-organization-of-islamic-cooperation-oic-asian-countries

[389] Telecom organizations in Africa targeted by Iran-linked hackers // The Record. 19.12.2023. URL: https://therecord.media/muddywater-cyber-espionage-africa-telecoms-iran

[390] Iran and cryptocurrency: Opportunities and obstacles for the regime // Middle East Institute. 27.12.2022. URL: https://www.mei.edu/publications/iran-and-cryptocurrency-opportunities-and-obstacles-regime

[391] Islamic stablecoin launched in Iran amid US sanctions // Gulf Times. 05.02.2019. URL: https://www.gulf-times.com/story/621295/islamic-stablecoin-launched-in-iran-amid-us-sanctions; Cryptocurrency Penetrates Key Markets in Sub-Saharan Africa as an Inflation Mitigation and Trading Vehicle // Chain Analysis. 19.09.2023. URL: https://www.chainalysis.com/blog/africa-cryptocurrency-adoption/

[392] The VPN Epidemic in Iran: A Digital Plague Amid Global Isolation // Stimson. 09.09.2024. URL: https://www.stimson.org/2024/the-vpn-epidemic-in-iran-a-digital-plague-amid-global-isolation/

разработка собственных аналогов *NIN* позволит снизить социальную напряженность, подогреваемую посредством социальных медиа.

Сотрудничество по вопросам развития ***технологий искусственного интеллекта*** между Ираном и странами АЮС в настоящий момент не получило выражения в публичной плоскости – в том числе в силу того, что данная технология еще не получила широкого распространения среди большей части лояльных Тегерану стран. При этом данное направление можно охарактеризовать как перспективное – с учетом того, что иранские власти планируют с помощью созданной в 2024 г. Национальной организации искусственного интеллекта[393] продвигать национальные ИИ-наработки более активно. Кроме того, сохраняются определенные перспективы налаживания профильного диалога с Эфиопией и ЮАР – в рамках усилий по развитию проектов в области искусственного интеллекта на пространстве БРИКС[394].

Что касается ***сектора ПО***, то здесь Тегеран пытается, несмотря на угрозы США вторичными санкциями в адрес африканских стран, укреплять сотрудничество с партнерами в регионе АЮС. Еще в 2023 г. Иран существенно расширил профильное взаимодействие с рядом стран Восточной Африки (Уганда, Кения, Танзания) по поставкам технологических решений для сектора АПК и нефтегазодобычи[395]. При этом основной упор в развитии диалога по-прежнему делается на Кению, где еще в 2021 г. был открыт первый на Африканском континенте иранский Дом инноваций и технологий[396].

Обобщенный показатель вовлеченности представлен ниже (*см. таблицу 23*).

Страна	Цифровая безопасность	Цифровые технологии в экономике и госуправлении	ИИ-Технологии	Разработка ПО
Ангола	1	1	0	0
Бенин	1	0	0	1
Ботсвана	1	0	1	0
Буркина-Фасо	2	0	0	1
Бурунди	0	0	0	0
Габон	1	1	0	0
Гамбия	1	1	1	0
Гана	2	1	1	1
Гвинея	1	0	0	0
Гвинея-Бисау	0	0	0	0
ДРК	1	0	0	0
Замбия	0	0	1	0

[393] Iran Inaugurates National AI Organization to Spearhead Technological Advancements // Iran Press. 09.07.2024. URL: https://iranpress.com/iran-inaugurates-national-ai-organization-to-spearhead-technological-advancements
[394] BRICS announces formation of AI study group // Dig. Watch. 23.08.2023. URL: https://dig.watch/updates/brics-members-announce-formation-of-ai-study-group
[395] Iran targets East Africa for technology products // Tehran Times. 01.09.2023. URL: https://www.tehrantimes.com/news/488579/Iran-targets-East-Africa-for-technology-products
[396] Iran in Africa: From Revolutionary Vision to Economic Alliances // Alafrica. URL: https://alafarika.org/4726/iran-in-africa-from-revolutionary-vision-to-economic-alliances/

Зимбабве	0	0	0	0
Кабо-Верде	0	0	0	0
Камерун	2	1	1	1
Кения	2	1	2	4
Конго	1	1	0	1
Кот-д'Ивуар	0	1	0	0
Лесото	1	0	0	0
Либерия	0	0	0	0
Маврикий	0	1	1	1
Мадагаскар	0	1	1	0
Малави	0	0	0	0
Мали	2	2	0	1
Мозамбик	1	1	0	1
Намибия	1	1	1	1
Нигер	2	2	0	1
Нигерия	1	1	1	2
Руанда	1	2	0	1
Сан-Томе и Принсипи	0	0	0	0
Сейшельские острова	0	0	0	0
Сенегал	0	1	1	0
Сомали	0	0	0	0
Сьерра-Леоне	0	1	1	0
Танзания	1	2	2	3
Того	1	1	1	1
Уганда	3	2	1	3
ЦАР	1	1	0	0
Чад	0	1	1	0
Экваториальная Гвинея	0	1	1	0
Эритрея	0	0	0	0
Эсватини	0	0	0	0
Эфиопия	2	1	2	2
ЮАР	3	3	3	2
Южный Судан	0	0	0	0

Таблица 23. Индекс вовлеченности в развитие системы цифровых технологий стран региона (по 5-балльной шкале)[397]. Составлено автором.

[397] 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.

3.3. Ключевые конкуренты Москвы: обобщая тренды

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.

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 24*).

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, а также бизнес-площадки, в рамках которых нередко оговариваются формула взаимодействия, а также возможная коллективная позиция участников кооперации[398].

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 держав. Вместе с тем реальный формат отношений между Москвой и региональными партнерами и конкурентами во многом зависит и от их готовности следовать схожим принципам.

[398] Также сводная таблица участия стран рассмотренных регионов в инициативах в рамках международных площадок представлена в Приложении 3, сводная таблица основных форматов двустороннего взаимодействия – в Приложениях 4 и 5.

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
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 24. Сводный показатель влияния внешних партнеров на рынках стран групп «Персидский залив+» и АЮС. Составлено автором.

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.

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. 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.

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 – российские проекты пользуются спросом как со стороны *передовиков цифровой гонки*, так и тех, кто пока вынужден сокращать цифровой разрыв.

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). Следует отметить, что некоторая разбалансированность цифровых систем, характерная для перечисленных держав, открывает возможности для более легкого сближения с новыми партнерами – за счет их потребности в получении новых знаний и технологий.

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).

ПРИЛОЖЕНИЯ

Приложение 1

После «Соколов пустыни»: краткий обзор «цифровых армий» стран группы «Персидский залив+»

В условиях острого регионального соперничества на Ближнем Востоке, неотъемлемой частью которого является *гонка кибервооружений*, популярность получил феномен «киберармий» – хакерских команд, решающих оперативные задачи какого-либо государства по нанесению урона оппонентам в киберпространстве, но отрицающих (либо не афиширующих) свои связи с государственными институтами.

Одной из первых официально атрибутированных ближневосточных «киберармий» является команда «Соколы пустыни» (*Desert Falcons*), которая проводила операции по кибершпионажу в период с 2013 по 2015 г. Набор ее цифровых инструментов, включающих в том числе уникальное многосоставное программное обеспечение, свидетельствовал о высоком уровне подготовки ее участников и наличии значительных финансовых ресурсов. Это позволило экспертам предположить, что за данной киберкомандой может стоять одно из арабских государств Персидского залива[399].

Однако и после ухода в тень (и возможного распада) данной группы «киберармии» не утратили прежнее значение. Скорее наоборот – этот формат приобретает все большую актуальность в контексте стратегических интересов стран региона «Персидский залив+», а над интеграцией хакерского движения в национальные системы киберзащиты в той или иной степени работают почти все государства.

Обзор по странам

Саудовская Аравия

В вопросах проведения сложных кибероперациий с привлечением лояльных киберкоманд Королевство относится к числу «пионеров» среди арабских государств Залива. Еще в 2012 г. Эр-Риядом была сформирована группа киберкоманд и хакеров-одиночек, объединенных под общим именем «Кибермухи»[400].

При реализации своих акций просаудовские хакеры сочетали применение киберинструментов (DDoS-атаки, использование программ-вымогателей и др.) с проведением информационно-психологических атак (создание DeepFake-контента, распространение ложной дискредитирующей информации и пр.), что первое время (до появления киберподразделения со схожим набором инструментов у ОАЭ) считалось их *визитной карточкой*.

[399] Kaspersky Security Bulletin 2015. Развитие угроз в 2015 году // SecureList. URL: https://securelist.ru/kaspersky-security-bulletin-2015-razvitie-ugroz-v-2015-godu/27466/

[400] Saudi Arabia seeks to tame powerful cyber armies // France24. URL: https://www.france24.com/en/20200807-saudi-arabia-seeks-to-tame-powerful-cyber-armies

«Кибермухи» показали высокую эффективность в период катарского дипломатического кризиса 2017–2021 гг. Отдельные дискредитирующие конструкты, созданные и раскрученные в рамках деятельности этой хакерской группировки (например, «посев» результатов «журналистского расследования» о вскрытии деятельности сети контролируемых государством каналов по отмыванию незаконных активов с помощью криптовалюты на территории Катара), по-прежнему оказывают негативное влияние на международный имидж Дохи и продолжают создавать проблемы в вопросах его внутреннего развития (например, препятствуют либерализации национального законодательства в области торговли цифровыми активами).

В «активе» саудовских «Кибермух» числятся и другие массовые *цифровые контратаки*, включающие взломы аккаунтов оппозиционных деятелей, а также «сочувствующих» из числа граждан других стран с целью получения компрометирующих сведений[401]. С другой стороны, Эр-Рияду пришлось заметно снизить активность данного подразделения и дистанцировать его от официальных властей после 2019 г., когда появились расследования об участии «Кибермух» в организации резонансного убийства оппозиционного журналиста Джамаля Хашогги (2018 г.)[402].

Несмотря на то, что Саудовская Аравия, вероятно, продолжает поддерживать тесные контакты с «Кибермухами» (чему в том числе способствовала передача полномочий по развитию диалога с хакерским сообществом Национальному управлению кибербезопасности в конце 2018 г.[403]), говорить о полноценной интеграции хакеров в структуру национальной кибероборонны все же преждевременно.

Взаимодействие Эр-Рияда с лояльными хакерами по-прежнему выстраивается хаотично, а сами хакеры не подчинены напрямую ни одному из ведомств (что усложняет целеполагание и объективный контроль их деятельности). Кроме того, саудовским властям весьма часто приходится выбирать между развитием ударных сил и соблюдением религиозных предписаний[404], что также сужает пространство для маневра.

Тем не менее, полностью отказываться от удобного рычага влияния на оппонентов Эр-Рияд едва ли будет. И, скорее всего, процесс интеграции хакерского движения в национальную систему кибероборонны (начатый еще в 2018 г.) будет продолжен.

---

[401] How Saudi Arabia's cyber chief Saud al-Qahtani - who went missing in wake of Khashoggi murder - spent years getting his hands on hacking equipment which UN suspects was used to hack Jeff Bezos // Daily Mai. 24.01.2020. URL: https://www.dailymail.co.uk/news/article-7920593/How-Saudi-cyber-chief-spent-years-acquiring-hacking-tools-thought-used-Bezos.html

[402] Исчезновение Хашогги: пять вопросов, на которые пока нет ответов // BBC. URL: https://www.bbc.com/russian/news-49915394

[403]Developing National Information Security Strategy for the Kingdom of Saudi Arabia // ITU. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/SaudiArabia_NISS_Draft_7_EN.pdf

[404] Среди саудовских богословов по-прежнему отсутствует консенсус по поводу правомерности различных аспектов хакерской деятельности. Многие духовные авторитеты считают хакерство (в любом его виде) грехом, даже если специалист действует из благих побуждений. См.: Saudi scholar issues fatwa against stealing WiFi // Independent. 01.06.2016. URL: https://www.independent.co.uk/news/world/middle-east/saudi-scholar-issues-fatwa-against-stealing-wifi-a7060431.html

ОАЭ

Как и Эр-Рияд, Абу-Даби, претендующий на региональное лидерство в области цифровой безопасности, не мог обойти феномен «киберармий» стороной. В 2016 г. стало известно о деятельности в ОАЭ проправительственной кибергруппировки «Соколы-невидимки» (*Stealth Falcon*), атаковавшей аккаунты эмиратовских диссидентов и оппозиционных журналистов, а также правозащитников[405].

В отличие от упомянутых ранее саудовских «Кибермух», делавших ставку на работу с соцмедиа, проправительственные хакеры ОАЭ более активно использовали технологии социальной инженерии и макровирусов (вредоносного кода, «вшитого» в текстовый документ, изображение или гиперссылку), что позволяло им проводить точечные и эффективные атаки без задействования социального ресурса. Кроме того, «Соколы» не объясняли свою деятельность патриотическими мотивами и отрицали какую-либо связь с государством (хотя де-факто руководствовались теми же целями, что и группировки, работавшие под эгидой оборонного *Project Raven*)[406].

Деятельность «Соколов-невидимок» имела несистемный характер, а эффект от проводимых атак и их периодичность стремительно снижались, что и обусловило ее «уход в тень» во второй половине 2010-х гг. и последующее вероятное поглощение другими сетевыми киберподразделениями (предположительно «Цифровой армией ОАЭ»[407]).

В то же время ряд экспертов допускает, что кибергруппировка продолжила свою деятельность в ограниченном формате и сосредоточилась на распространении вредоносного ПО в интересах ОАЭ – например, алгоритмов несанкционированного доступа (так называемый «бэкдор») *Deadglyph*, обнаруженных на устройствах ряда ближневосточных оппозиционеров и журналистов в сентябре 2023 г.[408].

С учетом нарастающего соперничества ОАЭ с другими аравийскими монархиями (в первую очередь, с Саудовской Аравией) за лидерство на Ближнем Востоке, а также обострения конфликта ОАЭ и Ирана на фоне эскалации в секторе Газа, развитие национальных киберсил и их укрепление за счет вовлечения в работу национального хакерского сообщества, скорее всего, останется в числе приоритетов политики Абу-Даби.

---

[405] Stealth Falcon group uses custom spyware // CSS Online. URL: https://www.csoonline.com/article/3076178/stealth-falcon-group-uses-custom-spyware.html

[406] Stealth Falcon // MITRE. URL: https://attack.mitre.org/groups/G0038/

[407] Группировка впервые упоминается в 2019 г. и позиционируется как хактивисткая, связанная с властями ОАЭ лишь предположительно. Тем не менее, участие группировки в отстаивании интересов ОАЭ (главным образом – оппонирование Саудовской Аравии), а также высокий уровень технической оснащенности (включая использование шпионского ПО проекта «Pegasus»), позволили предположить, что киберкоманда получает поддержку властей. См.: Sugarman L. The Week that Was: All of Lawfare in One Post // Lawfare Media. 02.02.2019. URL: https://www.lawfaremedia.org/article/week-was-all-lawfare-one-post-284; The death of 1,300 pilgrims and criticism of Saudi Arabia's performance in Hajj administration // Webangah. 26.06.2024. URL: https://en.webangah.ir/2024-06-26/news=146645/

[408] Deadglyph: New Advanced Backdoor with Distinctive Malware Tactics // The Hacker News. 23.09.2023. URL: https://thehackernews.com/2023/09/deadglyph-new-advanced-backdoor-with.html

Катар

Доха занимает двойственную позицию в отношении формата «киберармий». С одной стороны, катарские власти считают милитаризацию киберпространства деструктивным трендом, подрывающим и без того не слишком высокий уровень доверия между соседями на Ближнем Востоке. По этой причине Доха поддерживает любые общественные инициативы, направленные на развитие взаимодействия в цифровом мире – в числе таковых, например, «Парижский призыв к доверию и безопасности в киберпространстве» (2021 г.)[409].

В то же время в Катаре осознают необходимость развития инструментов реагирования на угрозу использования инструментов ИКТ в военных целях (включая упреждающие акции). Тем более, что страна оказалась в числе тех, кому кибероперации оппонентов нанесли значительный ущерб. В частности, масштабная медиакампания, запущенная саудовскими и эмиратскими киберспециалистами, де-факто спровоцировала Катарский дипломатический кризис (2017-2021 гг.)[410], в результате которого Доха оказалась частично изолирована от остального Арабского мира и несколько ослабила влияние на региональные процессы.

Катарская стратегия национальной кибербезопасности, рассчитанная до 2030 г., довольно обтекаемо характеризует набор инструментов, которые страна может использовать для обеспечения безопасности[411], допуская возможность привлечения к защите информационного пространства «патриотически настроенных киберкоманд».

В числе косвенных признаков, указывающих на рост оперативных возможностей Катара на этом направлении стала масштабная кибератака, проведенная «неназванной киберкомандой»[412] в преддверии Чемпионата мира по футболу 2022 г. Тогда в результате атаки были украдены личные данные Интернет-пользователей (включая политиков, журналистов и общественных деятелей), выступавших с критикой в адрес Дохи[413].

При этом о планах более плотно работать с хакерским сообществом официальная Доха по-прежнему не заявляет, предпочитая сохранять образ *цифрового миротворца*.

Весьма вероятно, что дальнейшее строительство катарской «киберармии» будет проходить со значительной оглядкой на опыт Турции (регионального союзника Дохи), где уже налажено эффективное взаимодействие между национальным хакерским движением и государственными структурами *(см. рисунок 5)*.

Такой формат вполне отвечает политическим интересам Катара, поскольку позволит поддерживать как наступательный, так и оборонительный потенциал.

---

[409] Paris Call. The supporters. URL: https://pariscall.international/en/supporters

[410] Cyber Warfare In Qatar Crisis // CLAWS. URL: https://www.claws.in/cyber-warfare-in-qatar-crisis/

[411] About the Strategy // MCIT. URL: https://www.mcit.gov.qa/en/cyber-security/national-cyber-security-strategy/about-strategy

[412] В качестве рабочей версии рассматривался найм Дохой нескольких индийских хакерских команд, однако были зафиксированы и следы работы арабоязычных специалистов. См.: How Qatar could spy on World Cup visitors // EuroNews. URL: https://ru.euronews.com/2022/11/06/ru-qatar-world-cup-critics-spied-on

[413] How Qatar hacked the World Cup // The Bureau of Investigative Journalism. 05.11.2022. URL: https://www.thebureauinvestigates.com/stories/2022-11-05/how-qatar-hacked-the-world-cup/

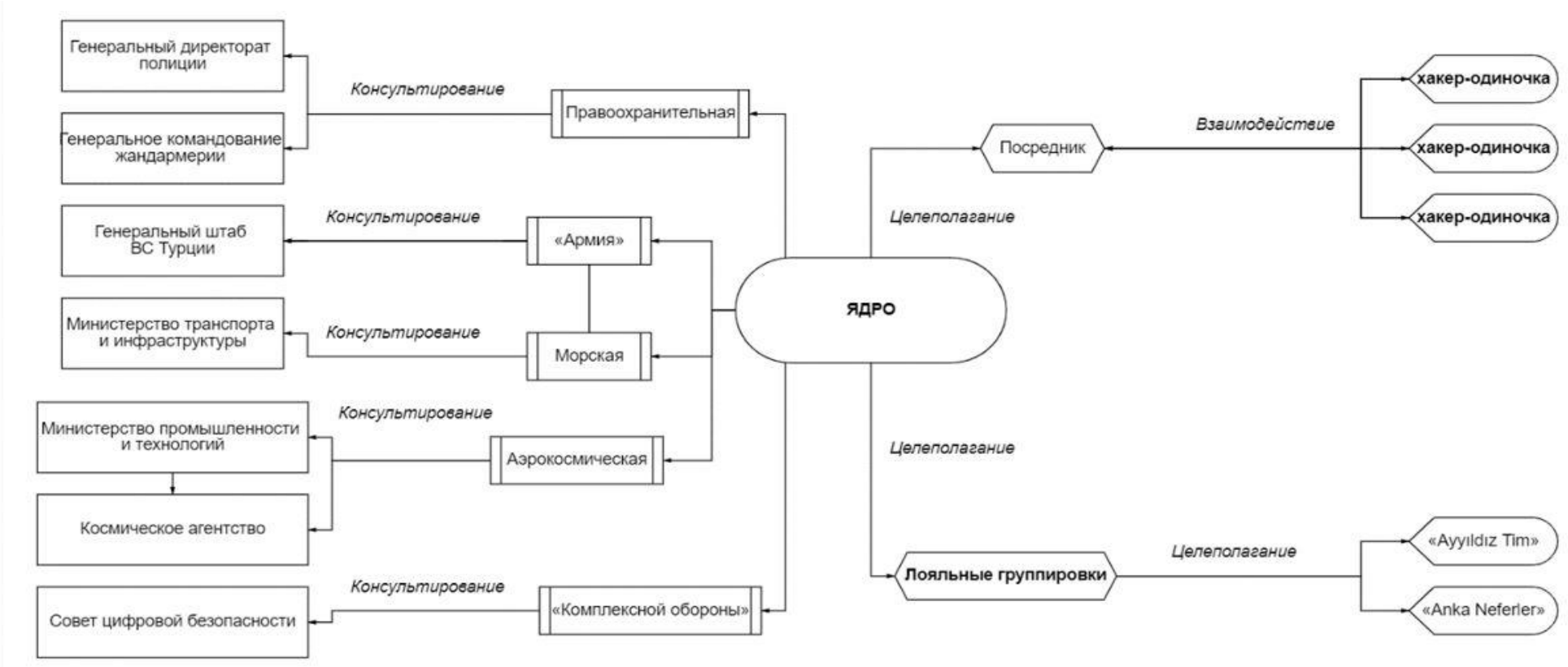

Рис.5. Модель интеграции хакерского сообщества в систему киберзащиты национального государства (на примере Турции). Составлено автором.

Бахрейн

Какие-либо сведения о развитии Бахрейном системы наступательных кибероперациий и работе с хакерским сообществом в рамках проекта «киберармий»[414] в открытых источниках отсутствуют.

В вопросах организации киберзащиты военной инфраструктуры Манама полагается на ресурсы профильных национальных институтов (например, национальный центр кибербезопасности[415]) и департаментов в составе национального МО. Также часть полномочий по обеспечению комплексной киберзащиты делегирована американским специалистам, базирующимся на территории данной страны[416].

Оман

Несмотря на то, что Оман занимает довольно высокие позиции в международных индексах киберготовности и имеет гармонично развитую структуру цифровой защиты с показателями, близкими к максимальным[417], Маскат стремится избегать излишнего включения в «гонку кибервооружений», развернувшуюся на Ближнем Востоке в начале 2010-х гг.

Как и Бахрейн, Оман не уделяет внимания развитию дополнительных «военных кибербрендов», предпочитая опираться на уже существующие государственные структуры[418]. При этом оманские специалисты активно участвуют в отработке моделей реагирования на киберугрозы (включая проведение собственных межведомственных учений), а официальный Маскат поддерживает довольно тесные контакты с «белым» хакерским сообществом[419], что создает задел для быстрого развития системы «киберармий» в будущем.

Кувейт

Позиция Кувейта по отношению к формату «цифровых армий» по-прежнему до конца не определена. С одной стороны, Эль-Кувейт в документах стратегического планирования (включая национальную стратегию кибербезопасности[420]) перечисляет среди приоритетов развитие инструментов реагирования на военные цифровые угрозы, оставляя за собой

---

[414] Принадлежность киберкоманды «Bahrain Cyb3R Army», которую долгое время включали в тройку аравийских «киберармий», обслуживающих интересы национальных правительств, к структуре органов безопасности Бахрейна в последние годы вызывает значительные сомнения – особенно после атаки на инфраструктуру базирующегося в Бахрейне Пятого флота США в 2024 г.

[415] NCSC. URL: https://www.ncsc.gov.bh/en/index.html

[416] U.S. – Bahrain Comprehensive Security Integration and Prosperity Agreement // US Embassy in Bahrain. 13.09.2023. URL: https://bh.usembassy.gov/u-s-bahrain-comprehensive-security-integration-and-prosperity-agreement/

[417] Global Cybersecurity Index 2024 // ITU. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

[418] MTCIT. URL: https://www.mtcit.gov.om/ITAPortal/MediaCenter/Document_detail.aspx?NID=120

[419] Bug Bounty Program at Oman. URL: https://bugbounty.om/

[420] National Cyber security Strategy for the State of Kuwait // CITRA. URL: https://citra.gov.kw/sites/en/LegalReferences/English%20Cyber%20Security%20Strategy.pdf. Несмотря на то, что действие документа формально ограничено 2020 г., Кувейт, в силу ряда причин, пока не представил новую публичную версию кибердоктрины, и продолжает при принятии политических решений руководствоваться положениями первого документа.

право самостоятельность определять масштабы и формат ответа на цифровые акции вероятного противника[421].

Также Кувейт, наравне с другими аравийскими монархиями, наращивает совокупный киберпотенциал и принимает участие в моделировании операций по отражению массированных кибердударов – учения проходят как в двустороннем (американо-кувейтская тренировка на базе *ARCENT University* в 2023 г.)[422], так и многостороннем форматах, с участием стран зоны ответственности Центрального командования и Киберкомандования США (учения *Eagle Resolve 23*[423]).

С другой стороны, несмотря на повышенное внимание к сектору цифровой безопасности, в стране к настоящему моменту пока официально не создано специализированных хакерских подразделений, ответственных за ведение наступательной киберборьбы и проведение «упреждающих» кибероперацийй[424].

При этом в структуре кувейтского минобороны существуют профильные единицы – например, департамент кибероперациий. Также специализированные подразделения созданы во всех родах войск, однако позиционируются как подразделения поддержки. При этом диалог с национальным хакерским сообществом носит весьма избирательный характер, что обусловлено в том числе спецификой национального законодательства.

Кроме того, Кувейт, в отличие от Саудовской Аравии, ОАЭ или Ирана, не уделяет внимание развитию и поддержанию *военных кибербрендов*: страна не выводит на передний план какие-либо киберкоманды, а также не комментирует деятельность хактивистов, причисляющих себя к «цифровым армиям». Программы взаимодействия с «белыми» хакерами на государственном уровне практически не продвигаются[425].

Важно отметить, что Кувейт среди аравийских монархий приступил к реформам цифрового сектора в числе последних, и процесс формирования национальной киберструктуры еще не завершен. Его новым «ядром» в ближайшем будущем станет Национальный центр кибербезопасности, создаваемый при активном участии Великобритании и США[426] – его полноценный запуск ожидается к 2025 г. Предполагается, что на Центр будут возложены

---

[421] National Cyber security Strategy for the State of Kuwait // CITRA. URL: https://citra.gov.kw/sites/en/LegalReferences/English%20Cyber%20Security%20Strategy.pdf

[422] U.S. Army Central and Kuwait Cyber Operations Directorate and Armed Forces Conduct Bilateral Cyber Defense Training // DVIDS. 23.05.2023. URL: https://www.dvidshub.net/image/7812049/us-army-central-and-kuwait-cyber-operations-directorate-and-armed-forces-conduct-bilateral-cyber-defense-training

[423] Eagle Resolve 23 // CENTCOM. URL: https://www.centcom.mil/Press-Release-View/Article/3409929/eagle-resolve-23-exercise-with-saudi-arabia/

[424] Kuwait – Design and Construction of the Kuwait Ministry of Defense Headquarters Complex // DSCA. URL: https://www.dsca.mil/taxonomy/term/1138

[425] Так, например, реализация программы по поиску уязвимости в цифровой инфраструктуре (т.н. «Bug Bounty») пока осуществляется только на посреднической основе: Эль-Кувейт сотрудничает с крупными зарубежными IT-компаниями, которые нанимают программистов по системе субподряда. Прямого взаимодействия с национальным хакерским сообществом по программе «Bug Bounty» в Кувейте в настоящее время не выявлено. См.: Bug Bounty Jobs in Kuwait // Naukri. URL: https://www.naukri.com/bug-bounty-jobs-in-kuwait

[426] Kuwait, UK Foster Investment Partnership, Cooperation in Cybersecurity // QNA. 29.08.2023. URL: https://www.qna.org.qa/en/News-Area/News/2023-08/29/0063-kuwait,-uk-foster-investment-partnership,-cooperation-in-cybersecurity; Joint Statement for the U.S.-Kuwait Strategic Dialogue // US Dept. of State. 27.01.2022. URL: https://www.state.gov/joint-statement-for-the-u-s-kuwait-strategic-dialogue/

задачи по комплексной координации национальных усилий в области цифровой безопасности – как в гражданском, так и в военном секторе. В этой связи вполне вероятно, что диалог государственных институтов Кувейта с национальным хакерским сообществом будет идти при непосредственном участии данного Центра.

В числе других трендов развития, которые проявят себя в среднесрочной перспективе, можно считать расширение профильного диалога с национальными компаниями в области кибербезопасности. Так, за последние несколько лет существенно нарастили вес «Хакеры Кувейта» (*Kuwait Hackers Company*) – первая крупная цифровая компания страны, позиционирующая себя как «точку сбора» национальных специалистов в области цифровой защиты[427]. В 2019 г. компания провела первую в истории страны высокоуровневую конференцию по кибербезопасности[428], а в 2023 г. участвовала в отражении атаки группы вымогателей *Rhysida* против государственных институтов Кувейта[429]. Весьма вероятно, что «Хакеры Кувейта» будут привлекаться к выполнению специализированных задач и далее, а их функционал – расширяться.

Иран

Главным толчком к форсированному строительству национальной системы кибербезопасности Ирана послужили кибернападения на ядерные объекты страны в 2010 г. с использованием сложного вируса *Stuxnet*, предполагаемыми разработчиками которого считаются США и/или Израиль[430]. За относительно короткий промежуток времени Ирану удалось выстроить многоуровневую систему кибербезопасности, которая может быть с успехом использована как для защиты национального киберпространства страны, так и для наступательных операций против других государств[431].

Современная структура иранской кибербезопасности, по сути, представляет собой квазисистему, поскольку ее формируют многочисленные самостоятельные кибергруппы, связанные с государством лишь формально. Центральной единицей этой квазисистемы является *Киберармия Ирана*[432] – совокупность хакерских группировок, декларирующих идеологическую приверженность правящему режиму Ирана. Государственным же институтам, в ведении которых находятся вопросы кибербезопасности (Министерство информации, Кибер-полиция FATA и др.), отводится роль «целеуказателей»: они координируют и контролируют деятельность хакеров, разрабатывают стратегию ведения кибервойн, обеспечивая тем самым защиту национального киберпространства.

Внутри *Киберармию Ирана* можно разделить на несколько крупных категорий (*см. рис.6*). Помимо хакеров-одиночек, которые, как правило, привлекаются разово для выполнения мелких задач (или задействуются в качестве вспомогательных сил в операциях, где

[427] Kuwait Hackers. URL: https://www.kuwaithackers.com/
[428] "Kuwait Hackers" opened the first Kuwait Cyber Security Conference under the sponsorship of "Central Agency for Information Technology", "youth" and "Al-Anbaa" // CAIT. 18.02.2019. URL: https://www.cait.gov.kw/en/media-center/news-events/kuwait-hackers-opened-the-first-kuwait-cyber-secur/
[429] The Rhysida ransomware group hit the Kuwait Ministry of Finance // Security Affairs. 26.09.2023. URL: https://securityaffairs.com/151501/cyber-crime/rhysida-ransomware-kuwait-ministry-of-finance.html
[430] Stuxnet: война 2.0. Habr. 12.10.2010. URL: https://habr.com/ru/articles/105964/
[431] Iran's Cyber Strategy, Institutions, and Capabilities // INSS. URL: https://www.inss.org.il/wp-content/uploads/2024/02/Part-2.pdf
[432] Ibidem.

требуется массовость), весьма крупным сегментом являются цифровые прокси-группировки.

Как правило, это локальные хакерские команды, которые отстаивают интересы лояльных Тегерану сил и, как правило, отвечают за цифровую борьбу в конкретном. Сюда входят как активные, так и «спящие» (временно бездействующие) группы. В настоящий момент лояльные Ирану кибергруппировки наиболее активно действуют в Ираке («Fatemiyoun Electronic Team», ранее также известная как «Fatemiyun Electronic Squad» или «FET»[433]), Ливане («Ливанский кедр»[434]) и Йемене («Йеменская киберармия» и «OilAlpha»[435]). Не исключается также вероятность скорого появления проиранского хакерского подразделения в Сирии (на базе *Лива Абу аль-Фадль аль-Аббас*).

На особом счету «ударные группировки» – хорошо оснащенные подразделения профессиональных хакеров, привлекаемые Тегераном к реализации наиболее сложных операций. Как правило, полномочия таких киберподразделений достаточно широки (и зона ответственности не заканчивается одним только Ближним Востоком как у значительной части проиранских киберкоманд), а целеполагание осуществляется высокопоставленными силовиками КСИР. К числу наиболее известных «ударных» иранских киберподразделений относится группировка «Charming Kitten»[436].

За время активной деятельности группировки ее *зоной ответственности*, помимо США, были страны Ближнего Востока — и, в первую очередь, региональные союзники Вашингтона. Признанным рекордсменом среди ближневосточных государств по числу выпадов можно считать Саудовскую Аравию. Так, в период наибольшей активности «Charming Kitten» (2017–2021 гг.) атакам подвергались крупнейшие саудовские компании (включая нефтегазового гиганта Saudi Aramco), банки и медиа, а также частные лица (включая их цифровые почтовые ящики и аккаунты в социальных сетях)[437]. Суммарный урон, нанесенный саудовской инфраструктуре в этот период, оценивается в несколько миллиардов долларов.

Еще одна сравнительно многочисленная группа — хакерские команды, отождествляющие себя с Ираном («мимикрирующие»). К таковым относятся группировки, выступающие от имени иранского правительства (или других элементов государственной системы — например, КСИР), но никак не подтверждающие эти связи. Среди множества «мимикрирующих» группировок выделяются несколько киберкоманд, уровень операций которых свидетельствует о наличии значительной финансовой и технической поддержки — это, например, «Bax 026» и «Hackers of Savior». Данные группировки принимали участие в качестве вспомогательных сил в наиболее сложных и громких операциях, реализованных Ираном против западных компаний в 2021–2022 гг.

---

[433] Profile: Fatemiyoun Electronic Squad // Washington Institute. 26.04.2021. URL: https://www.washingtoninstitute.org/policy-analysis/profile-fatemiyoun-electronic-squad

[434] Hezbollah-Linked Lebanese Cedar APT Infiltrates Hundreds of Servers // Threat spot. 01.02.2021. URL: https://threatpost.com/hezbollah-lebanese-cedar-apt-servers/163555/

[435] Researchers catch Yemeni hackers spying on Middle East military phones // Cyberscoop. 09.07.2024. URL: https://cyberscoop.com/researchers-catch-yemeni-hackers-spying-on-middle-east-military-phones/

[436] Также в разное время атрибутировалась как «APT35», «Newscaster», «Rocket Kitten», «Phosphorus», «Saffron Rose» и др.

[437] U.S. Confirms Iranian Intel Behind Hacker Group That Hit Israel, Saudi Arabia // Haaretz. 13.01.2022. URL: https://www.haaretz.com/israel-news/tech-news/2022-01-13/ty-article/.premium/u-s-confirms-iranian-intel-behind-hacker-group-that-hit-israel-saudi-arabia/0000017f-e8f1-dc91-a17f-fcfdefe50000

К этой категории «спорных» киберкоманд можно отнести те группировки, которые не заявляют о своих связях с Ираном (и, более того, часто выступают от лица других региональных сил), но, тем не менее, своими действиями способствуют упрочнению позиций Тегерана в регионе. Такие группировки стали появляться сравнительно недавно, однако специфика их целеполагания (а также стремительно растущий уровень компетенций) позволяет говорить о наличии заинтересованности в их деятельности со стороны иранских властей. Из наиболее активных в настоящий момент можно упомянуть «Black Shadow» (в первых пропагандистских материалах — группа хакеров из Европы, разделяющих идеи аятоллы Хомейни), «Moses Staff» (на начальных этапах выдавала себя за антисионистское сопротивление Израиля) и «Sharp Boys» (ранее — индийские и турецкие хакеры). Разумеется, в большинстве случаев, эксперты склонны считать эти группировки иранскими, действующими под «маской» других наций и объединений с целью создания видимости глобальной поддержки режима аятолл[438].

С учетом продолжающегося роста напряженности на Ближнем Востоке – включая повышенный градус эскалации между Ираном и Израилем, вероятность того, что Иран продолжит использовать цифровые средства для отстаивания собственных стратегических интересов, весьма высока.

[438] С началом конфликта в секторе Газа ожесточенные дебаты в экспертном сообществе вызвала группировка «Toufan Al-Aqsa», отождествляющая себя с ХАМАС. С другой стороны, почерк группировки и ее сравнительно высокий (в сравнении с другими палестинскими киберкомандами) уровень технической оснащенности косвенно указывает на то, что под флагом «Toufan Al-Aqsa» может действовать «ударная» команда (например, «Charming Kitten»). См.: Цуканов Л.В. Никто не знает о персидских котах: группировка «Charming Kitten» и стратегия безопасности Тегерана // Российский совет по международным делам. 08.08.2023. URL: https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/nikto-ne-znaet-o-persidskikh-kotakh-gruppirovka-charming-kitten-i-strategiya-bezopasnosti-tegerana/

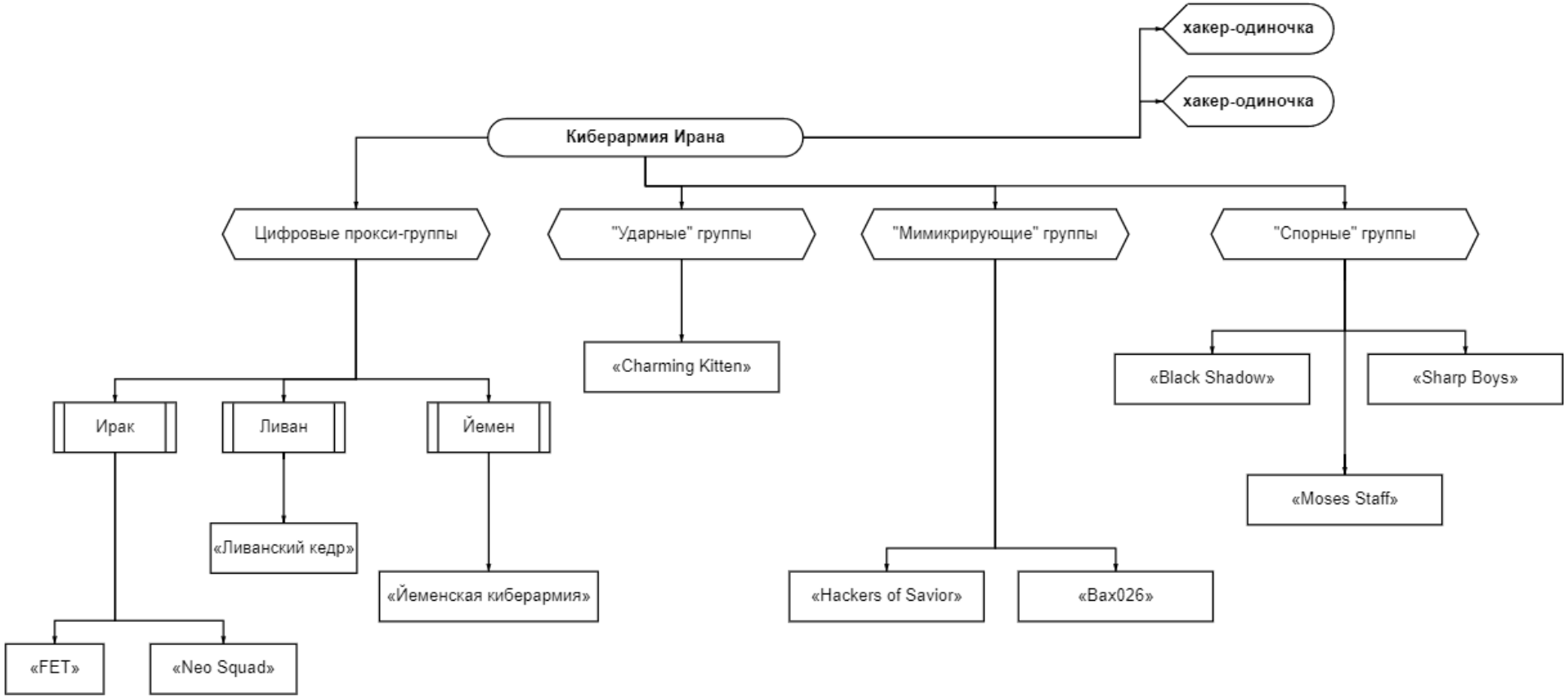

Рис.6. Схема организации «иранской киберармии» с разделением по категориям и примерами задействованных группировок. Составлено автором.

Ирак

Несмотря на то, что Багдад придерживается нейтралитета и, по заявлениям официальных лиц, «всячески препятствует незаконной деятельности любых хакерских группировок или команд»[439] на своей территории, в цифровом пространстве страны в последние годы наблюдается всплеск киберкоманд, причисляющих себя к группе «цифровых армий» и позиционирующих свою деятельность в качестве мер по защите интересов Ирака.

Как правило, подавляющее большинство таких самоназванных подразделений – это хактивистские подразделения, состоящие из граждан иракского происхождения. Основной способ борьбы –проведение дискредитирующих медиакампаний и действующие в интересах крупных парамилитарных формирований (например, *Рубу Аллах* и *Асаиб Ахль аль-Хак*)[440]. Однако в части технической оснащенности и оперативных возможностей подобные подразделения, как правило, сильно уступают саудовским и иранским коллегам. Несмотря на то, что деятельность «киберармий» нарушает иракское законодательство (в первую очередь, Закон об информации и массовых коммуникациях и Закон о свободе слова и мирных демонстрациях) до настоящего момента не зафиксировано ни одного случая вынесения обвинительного приговора против данной категории хактивистов.

Кроме того, неопределенным остается отношение к симпатизирующим Ирану киберкомандам со стороны официального Багдада. Так, например, серия масштабных DDoS-атак, реализованных в марте – апреле 2022 г. проиранской хакерской группировкой «al-Tahirah Team» против веб-сайтов Саудовской Аравии, ОАЭ, Турции и Израиля, была атрибутирована как осуществленная с территории Ирака. При этом интернет-инфраструктура страны (включая аналогичные веб-платформы) нападению не подверглась – хотя до этого, начиная с 2020 г., группировка на системной основе проводила интернет-рейды против иракских сайтов и сервисов (включая официальные аккаунты МВД[441]). В связи с этим у аналитиков появились основания полагать, что подобная атака была реализована с согласия местных властей, что противоречит тезису об отсутствии у них контактов с проиранским хакерским подпольем.

В свою очередь, подобные расхождения между официальной позицией Багдада и реальной обстановкой в стране поставили под сомнение честность и открытость иракских властей в вопросах противодействия цифровой угрозе и негативно сказались на уровне доверия к ним.

[439] A Commitment to Cybersecurity // Unipath. 20.12.2022. URL: https://unipath-magazine.com/a-commitment-to-cybersecurity/

[440] 'Cyber army' paves way for assassinations of Iraqi activists opposed to Iran // Al-Mashareq. 19.02.2021. URL: https://almashareq.com/en_GB/articles/cnmi_am/features/2021/02/19/feature-02

[441] Hackers zap official Iraqi websites with cyberattacks // Al-Monitor. URL: https://www.al-monitor.com/originals/2020/01/iraq-cybersecurity-hack-protests.html

Заключение

В целом, можно наблюдать, что формат «киберармий» завоевывает все большую популярность среди рассмотренных государств – даже те страны, что выступают за снижение напряженности в киберпространстве на деле параллельно ведут разработку соответствующих моделей реагирования.

Разумеется, в зависимости от рассматриваемой страны, меняются масштабы вовлечения хакерского сообщества в работу над формированием национальной киберзащиты, специфика управления кибероперациями и формат взаимодействия с официальными властями.

Тем не менее, во всех случаях «киберармии» превращаются в удобный инструмент решения политических задач и достижения целей без получения сопутствующего имиджевого ущерба. Можно ожидать, что в контексте эскалации палестино-израильского противостояния, повлекшего за собой углубление конфликта между Ираном с одной стороны и Израилем, США и рядом аравийских монархий с другой, трендом для Ближнего Востока на ближайшие годы станет работа по развитию цифровых подразделений – в качестве одного из инструментов ведения асимметричной борьбы.

Приложение 2

Россия и цифровой рынок Мали: перспективы и препятствия

Африканский рынок цифровых технологий развивается неравномерно – что обусловлено разными стартовыми условиями и доступными ресурсами. Тем не менее, опыт каждой из стран АЮС в той или иной степени интересен при формировании картины цифрового развития континента.

Среди государств Субсахарской Африки уместно обратить внимание на Мали, чей потенциал представляет исследовательскую и практическую ценность по ряду причин. В первую очередь, тем, что Бамако является одним из ключевых столпов сформированного в 2023 г. «Альянса государств Сахеля» (Мали, Нигер, Буркина-Фасо), и в настоящий момент страна переориентирована на развитие контактов с незападными компаниями – тем более, что представители европейского бизнеса оперативно покинули Мали после антифранцузского переворота в 2021 г.[442]. Помимо получения готовых решений, страна также ищет варианты развития кадрового и научно-технологического потенциала, что также не следует упускать из виду.

Кроме того, при оценке ситуации в Мали экспертным сообществом приоритет отдается изучению традиционных вызовов безопасности – например, оценке влияния террористической угрозы на стабильность малийских государственных институтов – в то время как передовая проблематика остается полностью *за кадром*, либо же представлена обрывочными сюжетами, хотя запрос малийских властей на цифровую трансформацию растет.

Данный аналитический срез позволяет в определенной степени устранить указанный пробел.

Оценка рынка Мали (PESTLE-анализ)

Для более эффективной и комплексной оценке состояния рынка цифровых технологий в Мали уместно прибегнуть к методу *PESTLE-анализа* и оценить обстановку по следующим категориям[443]:

- Политические факторы (P) – особенности внешней и внутренней политики страны, ее региональное положение.
- Экономические факторы (E) – уровень кадровой обеспеченности рассматриваемого сектора, экономический ландшафт, объемы инвестиций и пр.
- Социальные факторы (S) – социально-политическая обстановка в рассматриваемой стране (в разрезе рассматриваемого сектора).
- Технологические факторы (T) – основные тренды развития рынка технологий и инноваций.

[442] Второй военный переворот в Мали за девять месяцев. Главное // ИТАР-ТАСС. 27.05.2021. URL: https://tass.ru/mezhdunarodnaya-panorama/11472581

[443] В силу специфики рассматриваемого сектора экологические факторы (E) в расчет не взяты.

- Юридические факторы (L) – законы и иные нормативно-правовые предписания, оказывающие влияние на межгосударственное и бизнес-сотрудничество.
- Экологические факты (E) – влияние экологического фона на развитие рынка.

Как и в основном тексте доклада, рассмотрение рынка Мали предлагается произвести через призму четырех ключевых направлений – «Цифровая безопасность» (технологическое и социальное измерения), «цифровые технологии в экономике и госуправлении», «ИИ-технологии» и «Разработка ПО».

Политическая обстановка **(P)** в Мали характеризуется как напряженная. В стране отмечен рост сепаратистских настроений (активизация туарегского «Национального движения за освобождение Азавада»)[444]. Остается открытым вопрос реагирования властей на террористическую угрозу – резонансная атака боевиков на Бамако в середине сентября[445] серьезно ударила по привлекательности Мали для иностранных инвесторов и представителей крупного технологического бизнеса. Наконец, несмотря на некоторое потепление отношений между Мали и другими членами ЭКОВАС, соседи по региону по-прежнему относятся к Бамако с изрядной долей подозрительности, что сокращает пределы сотрудничества между Мали и другими странами АЮС.

С другой стороны, Бамако демонстрирует твердую политическую волю развивать национальную систему цифровой безопасности и работать над понижением уровня цифровых угроз в Мали – тем более, что страна входит в число лидеров африканского антирейтинга по количеству успешных кибератак против государственных институтов и частного сектора[446].

Отмечены попытки продвигать профильные инициативы и на уровне «Альянса государств Сахеля». Так, например, Мали, Нигер и Буркина-Фасо в августе 2024 г. приступили к совместной разработке коммуникационной стратегии и созданию цифровой платформы для вещания интернет-телевидения[447]. Данную инициативу можно считать первым шагом к соразвитию цифрового пространства в рамках данной конфедерации, а также попыткой обеспечить обмен опытом между государствами тремя странами.

При этом в числе приоритетов Бамако пока находятся только вопросы развития системы киберзащиты и активизации цифровой трансформации экономики, в то время как другие ниши (например, развитие сектора ИИ или собственных проектов в области ПО) получают кратно меньшее внимание.

[444] Малийское движение «Азавад» объявляет войну ЧВК «Вагнер» и армии страны // EADaily. 12.08.2023. URL: https://eadaily.com/ru/news/2023/08/12/maliyskoe-dvizhenie-azavad-obyavlyaet-voynu-chvk-vagner-i-armii-strany

[445] При нападении исламистов на столицу Мали 17 сентября погибли 77 человек // Интерфакс. 19.09.2024. URL: https://www.interfax.ru/world/982811

[446] Mali Profile // Netscout. URL: https://www.netscout.com/threatreport/emea/mali/; Cyber threat live map // Kaspersky. URL: https://cybermap.kaspersky.com/stats

[447] Альянс государств Сахеля создаст платформу для вещания интернет-телевидения // ИТАР-ТАСС. 23.08.2024. URL: https://tass.ru/mezhdunarodnaya-panorama/21667651

Экономическую обстановку **(E)** в Мали также можно охарактеризовать как имеющую высокий уровень турбулентности. Страна испытывает комплекс экономических проблем, усугубленных последствиями пандемии COVID-19 и давлением со стороны соседей по региону после антифранцузского переворота 2021 г.

В этом контексте освоение цифрового пространства населением Мали идет с некоторым отставанием от показателей других стран АЮС. По данным консалтингового агентства *Kepios*, в январе 2024 г. в Мали насчитывается порядка 7,82 млн пользователей Интернета (примерно 33% от общей численности населения); прирост по сравнению с прошлым годом составил 3,1%[448]. При этом средняя скорость фиксированного интернет-соединения в стране за прошедший год снизилась почти на 7%, составив 21,55 Мбит/с[449].

При этом массовый исход европейских (в первую очередь, французских) с рынка Мали укрепил возможности для развития профильных связей с представителями дружественных новому малийскому режиму стран – например, произошло значительное укрепление позиций представительства «Лаборатории Касперского» в Мали[450]. Официальный Бамако заинтересован в дальнейшем развитии сотрудничества с иностранными компаниями, готовыми делиться передовым опытом с малийскими специалистами и совместно обеспечивать стабильность цифровой системы страны.

Социально-политический ландшафт **(S)** в Мали характеризуется заметным всплеском антизападных настроений. Будучи одним из «столпов» антифранцузского движения в Субсахарской Африке, Мали всячески приветствует появление на национальном рынке цифровых компаний, пришедших на смену французским и другим европейским IT-фирм. За последние несколько лет отмечено укрепление позиций китайского, индийского, иранского и турецкого технокапитала.

Однако, помимо очевидных преимуществ от развития сотрудничества, в Мали видят в данном процессе и угрозу попадания в *цифровую зависимость*: представители национального кибербизнеса опасаются, что на смену французскому технологическому доминированию в стране довольно быстро придет незападное – например, китайское или индийское – при этом положение национальных предприятий в иерархии, вероятно, почти не изменится. Это несколько ограничивает темпы сотрудничества Мали с внешним миром по вопросам технологического развития, однако влияние данного фактора на принятие решений официальным Бамако на данный момент еще не достигло критических значений.

Технологическое развитие **(T)** Мали ведется под лозунгом расширения национального рынка и создания профильной инфраструктуры, а также развития национального кадрового потенциала – как неотъемлемой части экономической трансформации страны.

В последние годы в стране создается цифровая инфраструктура в сфере здравоохранения, АПК и финансов – во всех случаях весомую роль в ее формировании играет частный сектор (как национальный, так и зарубежный)[451]. Кроме того, малийское правительство работает

[448] Digital 2024: Mali // Data Report. URL: https://datareportal.com/reports/digital-2024-mali
[449] Ibidem.
[450] Kaspersky Mali. URL: https://kasperskymali.websites.co.in/
[451] Digital health initiatives in Mali – a detailed mapping // GDHub. 10.08.2022. URL: https://gdhub.org/digital-health-initiatives-in-mali-a-detailed-mapping%EF%BF%BC/; Mali Partners with Huawei to Speed Up Digital Transformation // Ecofinagency. 04.09.2024. URL: https://www.ecofinagency.com/public-management/0409-45846-

над запуском программ, направленных на насыщение ключевых цифровых отраслей квалифицированными кадрами. В этом вопросе Бамако ориентируется в том числе на стратегические ориентиры, заложенные Африканским союзом в начале 2010-х гг.[452].

Однако острая нехватка целевого финансирования (а также сохраняющееся дублирование полномочий между ключевыми государственными органами Мали, отвечающими за развитие системы цифровой безопасности) существенно сужают возможности Бамако на этом направлении. Примечательно также, что незападные технодержавы (в частности, Китай) не спешат напрямую вкладываться в развитие технологической инфраструктуры в Мали – хотя и поддерживают взятый новыми властями курс на повсеместную цифровизацию[453]. Столь осторожный подход Пекина обусловлен отчасти нежеланием портить диалог с другими странами АЮС, не поддерживающими курс малийского правительства.

Говоря о развитии кадрового потенциала в рамках комплексного технологического развития, уместно упомянуть некоторые общественные проекты, направленные на общее повышение цифровой грамотности населения. Один из примеров – инициатива *SheCodes*, запущенная одноименным фондом для обучения малийских женщин навыкам программирования и формирования более сбалансированного кадрового резерва[454]. Несмотря на то, что данный проект никак не связан с государством, малийское руководство оценивает его работу позитивно, и не препятствует организации профильных семинаров.

При этом «кадровое» направление по-прежнему является одним из наиболее слабых мест малийской цифровой системы, что подтверждается в том числе исследованиями ООН (*см. диаграмму 12*).

mali-partners-with-huawei-to-speed-up-digital-transformation; Mali Launches Digital Transformation of Payments and Public Services // Mobile Money AfricA. 24.07.2024. URL: https://mobilemoneyafrica.com/blog/mali-launches-digital-transformation-of-payments-and-public-services; Digital Agricultural Ecosystem in Mali // Feed the Future (2022). URL: https://developmentgateway.org/wp-content/uploads/2022/10/DAI_Report_vFinal_copyedited_2QL4hED-1.pdf и др.

[452]Bamako Digital Complex Support Project // AFDB. URL: https://www.afdb.org/fileadmin/uploads/afdb/Documents/Project-and-Operations/Mali_-_AR_TechnoMali_Project_.pdf

[453] Ван И провел встречу с главой МИД Мали А. Диопом // МИД КНР. 08.12.2023. URL: https://www.mfa.gov.cn/rus/wjb/zzjg/fzs/fzsgjlb/1590/1592/202312/t20231209_11198917.html

[454] The SheCodes Foundation supports ML Malian Women // SheCodes Foundation. URL: https://www.shecodesfoundation.org/mali

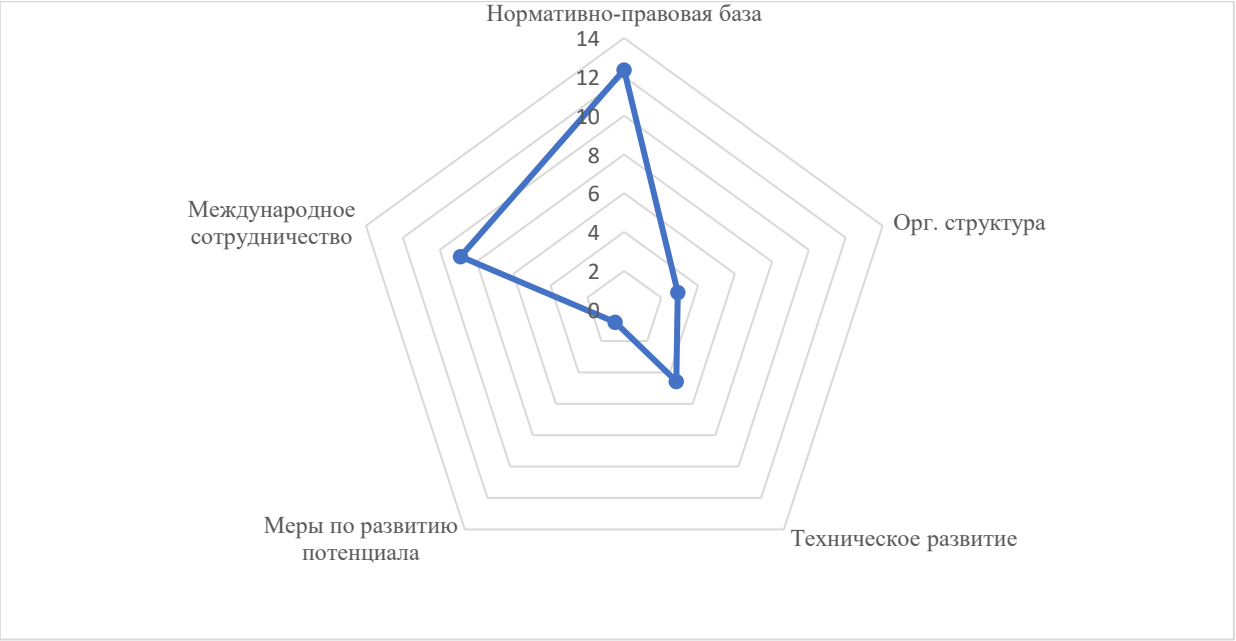

Диаграмма 12. Общее состояние системы цифровой безопасности Мали. Составлено по: GCI-2024[455].

С точки зрения ***законодательного регулирования*** (**L**), рынок Мали можно оценить неоднозначно. В стране приняты несколько профильных законов, направленных на регулирование цифровой сферы. Последний на данный момент профильный НПА, уточняющий порядок противодействия организованной киберпреступности, вступил в силу в конце 2019 г.[456]. Также отдельные вопросы цифровой безопасности регулируются национальным Уголовным кодексом (2001 г.)[457].

Схожим образом сложилась ситуация и в части разработки документов стратегического планирования – национальная стратегия цифровой трансформации (*Digital Mali*) принята (в драфтовом формате) в 2020 г. и с того момента не актуализировалась – хотя власти рассматривают ее в качестве основы цифровой деятельности Бамако.

Иными словами, все руководящие документы разработаны и приняты в период до антифранцузского переворота, в то время как новых НПА, касающихся регулирования цифровой сферы, новыми властями Бамако принято пока не было. Кроме того, страна практически не вовлечена в общерегиональные дискуссии по совместной защите киберпространства (в разрезе юридических вопросов), регулирования сферы искусственного интеллекта и пр.

Это, с одной стороны, усиливает цифровой разрыв Мали с другими государствами АЮС и повышает общую уязвимость национального цифрового сектора. С другой стороны, ситуация способствует большей открытости и гибкости малийских властей при общении с дружественными странами по вопросам развития системы законодательного регулирования с опорой на передовой опыт незападных юридических школ.

---

[455] Global Cybersecurity Index 2024 // ITU. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

[456] Journal Officiel de la Republique du Mali. URL: https://sgg-mali.ml/JO/2019/mali-jo-2019-43.pdf

[457] Речь о Статьях 264–271, в которых описаны правонарушения, связанные с конфиденциальностью, целостностью и доступностью автоматизированных данных и систем. См.: Mali Penal Code. URL: http://www.droit-afrique.com/upload/doc/mali/Mali-Code-2001-penal.pdf

Обобщенная информация о состоянии цифрового рынка Мали представлена ниже (*см. Таблицу 25)*.

	Возможности	Риски
P	Наличие политической воли у властей развивать систему цифровой безопасности (в том числе в конфедеративном формате), ставка на активизацию международного сотрудничества.	Политическая нестабильность (с преобладанием традиционных вызовов безопасности), оспаривание легитимности правящего режима (в т.ч. на международном уровне).
E	Наличие свободных ниш на технологическом рынке после ухода западных компаний из страны, востребованность передового опыта.	Санкционное и иное экономическое давление на заходящие на рынок страны компании со стороны как западных, так и ряда африканских стран.
S	Высокий уровень лояльности по отношению к незападным компаниям.	Растущие опасения по поводу «цифрового неоколониализма».
T	Ставка на расширение национального технологического рынка, попытки освоить новые направления.	Острая нехватка финансирования технологического сектора, растущий кадровый дефицит.
L	Попытки актуализировать профильную нормативно-правовую базу с опорой на передовой (незападный) опыт.	Наличие лакун в нормативно-правовом поле, инертность законодательной сферы.

Таблица 25. PESTL-анализ. Составлено автором.

Возможности и препятствия для России

Основываясь на изложенном выше, можно заключить, что цифровой рынок Мали является перспективным направлением для укрепления влияния российского технологического бизнеса, а также развития межгосударственного сотрудничества по треку высоких технологий в целом.

В силу специфики подхода Москвы к диалогу с Африканским континентом (в частности, отстаивания права африканских стран на *цифровой суверенитет*), Россию сложно упрекнуть в «неоколониальных настроениях», что выгодно отличает ее на фоне Китая, ключевого конкурента в зоне «Альянса государств Сахеля». Кроме того, российский опыт быстрой мобилизации национальной системы киберзащиты в условиях постоянных массированных кибератак вызывает интерес у нового малийского руководства. Это открывает возможности для выстраивания двухуровневого диалога между Москвой и Бамако.

С другой стороны, при развитии цифрового диалога с Мали важно помнить, что страна по-прежнему обладает достаточно шаткими позициями в регионе АЮС, а репутация нового правительства – неоднозначной. В этом контексте чрезмерно быстрое сближение Москвы и Бамако может вызвать протесты других партнеров России в регионе.

Приложение 3

Участие рассмотренных в докладе стран в глобальных и региональных инициативах, связанных с цифровым пространством (сводная таблица)

Страна	ООН				Региональные площадки				БРИКС				Общественные инициативы				Бизнес-инициативы				Отраслевые инициативы				Правовые инициативы (регион)			
	КБ	ФГ	ИИ	ПО	КБ	ФГ	ИИ	ПО	КБ	ФГ	ИИ	ПО	КБ	ФГ	ИИ	ПО	КБ	ФГ	ИИ	ПО	КБ	ФГ	ИИ	ПО	КБ	ФГ	ИИ	ПО
Ангола	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	1	0	0	1`	0	0	0	0	1	1	1	0
Бахрейн	1	1	1	1	2	1	1	1	0	0	0	0	1	0	1	1	2	0	2	2	2	1	1	2	1	1	1	1
Бенин	1	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	1	1	1	1
Ботсвана	1	1	1	0	1	0	2	0	0	0	0	0	0	0	1	0	0	0	1	1	2	0	0	0	1	1	1	0
Буркина-Фасо	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	1	1	1
Бурунди	1	1	1	0	1	0	0	0	0	0	0	0	1	1	1	0	1	0	1	0	0	0	0	0	1	1	1	1
Габон	1	0	1	0	1	0	1	0	0	0	0	0	1	0	1	1	1	1	1	1	0	0	0	0	1	1	1	1
Гамбия	1	0	1	0	1	1	1	1	0	0	0	0	1	0	0	1	1	0	1	1	1	0	1	1	1	1	1	1
Гана	1	0	1	0	1	1	1	0	0	0	0	0	1	1	1	1	1	1	1	2	1	1	1	1	1	0	1	1
Гвинея	1	0	1	0	1	0	1	0	0	0	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	1	1	1
Гвинея-Бисау	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	1	0	1	1	1	0	1
ДРК	1	0	1	0	1	0	0	0	0	0	0	0	1	0	0	1	0	0	0	1	1	1	1	1	1	1	0	1
Замбия	1	0	1	0	0	0	2	0	0	0	0	0	1	1	0	0	1	0	1	0	2	0	0	0	1	1	1	1
Зимбабве	1	1	1	0	1	1	1	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	2	1	1	1	1
Ирак	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1	0	1	1	0	1	1	1	1	1	1	1
Иран	1	1	1	1	1	2	1	0	1	0	1	0	0	0	1	0	1	1	1	2	1	1	1	1	1	1	1	0
Кабо-Верде	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	1	1	0	1
Камерун	1	1	1	1	1	1	1	0	0	0	0	0	1	0	1	0	1	0	1	1	1	1	1	1	1	1	1	1

Катар	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	0	2	1	2	1	2	1	1	2	1	1	1	1
Кения	1	1	1	1	1	1	2	1	0	0	0	0	1	0	2	0	1	2	2	1	1	2	1	2	1	1	1	1
Конго	1	1	1	1	1	1	1	0	0	0	0	0	1	0	0	1	1	0	1	1	1	1	1	1	1	1	1	1
Кот-д'Ивуар	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1	0	1	1	1	1	1	1	1	1
Кувейт	1	1	1	1	1	1	1	0	0	0	0	0	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Лесото	1	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	0	1	1	1	1	1
Либерия	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	1	1	1	1
Маврикий	1	1	1	1	2	2	1	1	0	0	0	0	2	1	2	1	2	1	1	2	1	1	1	1	1	1	1	1
Мадагаскар	1	1	1	1	1	1	1	1	0	0	0	0	1	0	1	0	1	1	1	1	1	1	1	1	1	1	1	1
Малави	1	1	1	1	1	1	1	0	0	0	0	0	1	1	0	0	1	1	1	1	0	0	0	1	1	1	1	1
Мали	1	1	1	0	1	1	1	0	0	0	0	0	1	0	1	0	1	0	0	1	1	0	0	1	1	1	1	1
Мозамбик	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	1	1	1	1
Намибия	1	1	1	1	1	1	1	0	0	0	0	0	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1
Нигер	1	1	1	1	1	1	1	0	0	0	0	0	1	0	0	0	1	0	0	1	1	1	1	1	1	1	1	1
Нигерия	1	1	1	1	1	2	1	0	0	0	0	0	1	1	2	1	1	2	0	2	2	1	2	2	1	1	1	1
ОАЭ	1	1	1	1	2	2	2	1	1	0	2	0	2	1	2	1	2	2	2	2	2	1	2	1	2	1	2	1
Оман	1	1	1	1	2	2	1	0	0	0	0	0	1	1	2	1	2	1	1	1	2	1	1	2	1	2	1	1
Руанда	1	1	1	1	1	1	1	0	0	0	0	0	1	0	1	0	1	1	0	1	1	1	1	1	1	1	1	1
Сан-Томе и Принсипи	1	0	1	1	1	1	1	0	0	0	0	0	0	0	0	1	0	0	0	1	1	1	1	1	1	1	1	1
Саудовская Аравия	1	1	1	1	2	2	2	1	1	0	1	0	2	2	2	1	2	2	2	1	2	1	2	2	2	1	2	1
Сейшельские острова	1	1	1	1	1	1	1	0	0	0	0	0	1	0	0	0	1	1	1	1	1	1	0	1	1	1	0	1
Сенегал	1	1	1	1	1	1	1	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Сомали	1	0	0	0	1	1	1	0	0	0	0	0	1	0	0	0	1	0	0	1	0	0	0	0	1	1	0	1
Сьерра-Леоне	1	1	1	1	1	1	0	0	0	0	0	0	0	0	1	0	1	1	1	1	1	1	1	1	1	1	1	1
Танзания	1	1	1	1	1	1	1	0	0	0	0	0	1	1	1	1	1	2	1	2	2	1	1	2	1	1	1	1
Того	1	1	1	1	1	1	0	0	0	0	0	0	1	0	1	0	1	1	1	1	1	1	1	1	1	1	1	1
Уганда	1	1	1	1	1	1	1	0	0	0	0	0	1	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1
ЦАР	1	1	1	0	1	1	0	1	0	0	0	0	0	1	0	0	0	1	0	0	1	1	0	1	1	1	1	1
Чад	1	1	1	1	1	1	1	1	0	0	0	0	1	0	1	0	0	0	1	0	1	1	1	1	1	1	1	1

Экваториальная Гвинея	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	1	1	0	1	1	0	1
Эритрея	1	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	1	0	0	1	0	1	0	1	1	1	0	1
Эсватини	1	1	1	1	1	1	0	0	0	0	0	0	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1
Эфиопия	1	1	1	1	1	1	1	1	1	0	1	1	1	0	1	0	1	1	1	2	2	1	1	2	2	1	1	1
ЮАР	1	1	1	1	2	2	1	2	1	0	1	0	2	1	2	1	2	2	1	2	2	1	1	2	2	1	2	1
Южный Судан	1	0	1	1	1	0	1	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	0	1	1	1	1	1

Таблица 26. Показатель активности государств групп «Персидский залив+» и АЮС в разрезе цифровой безопасности. Составлено по открытым источникам.

Условные обозначения: «КБ» – кибербезопасность; «ФГ» – цифровые технологии в экономике и госуправлении; «ИИ» – технологии искусственного интеллекта; «ПО» – разработка программного обеспечения. При этом «0» тождествен отсутствию инициатив и уклонению от какой-либо их поддержки, «1» – присоединению к инициативам; «2» – присоединение к инициативам и выдвижение собственных проектов.

Приложение 4

Основные форматы взаимодействия основных конкурентов России со странами группы «Персидский залив+» (сводная таблица)

Конкурент / Формат диалога	США	КНР	Индия	ЕС	Великобритания	Турция	Южная Корея	Япония	Израиль	Арабские страны Северной Африки
Диалог на уровне правительств	Да*	Да	Да	Да*	Да*	Да	Да*	Да*	Да*	Да
Диалог на уровне ведомств	Да*	Да	Да	Да*	Да*	Да	Да*	Да*	Да*	Да
Проведение конференций	Да*	Да	Да	Да*	Да*	Нет	Нет	Да	Да*	Да
Проведение выставок и ярмарок	Да*	Да	Да	Да*	Нет	Да	Нет	Нет	Да*	Нет
Работа по линии торговых представительств	Да*	Да	Да	Да*	Да*	Да	Да*	Нет	Нет	Да
Работа по линии корпораций	Да*	Да	Да	Да*	Да*	Да	Да	Да	Да*	Да
Иные форматы технологической кооперации	Курсы под эгидой НАТО	Нет	Нет	Курсы под эгидой НАТО	Курсы под эгидой НАТО	Курсы под эгидой НАТО	Нет	Нет	Тайное сотрудничество и диалог под эгидой «Соглашений Авраама»	Нет

Таблица 27. Форматы диалога ключевых конкурентов России со странами группы «Персидский залив+» в разрезе цифровой безопасности. Составлено по открытым источникам.

Условные обозначения: «*» – сотрудничество с исключениями (из диалога в рамках региона выпадает одна или несколько держав).

Приложение 5

Основные форматы взаимодействия основных конкурентов России со странами Субсахарской Африки (сводная таблица)

Конкурент / Формат диалога	США	КНР	Индия	ЕС	Великобритания	Турция	Южная Корея	Япония	Аравийские монархии	Арабские страны Северной Африки	Иран
Диалог на уровне правительств	Да*	Да	Да	Да*	Да*	Да	Да	Да	Да	Да	Да
Диалог на уровне ведомств	Да*	Да	Да	Да*	Да*	Да	Да	Да	Да	Да	Да
Проведение конференций	Да	Да	Да	Да*	Да	Да	Нет	Нет	Да	Нет	Нет
Проведение выставок и ярмарок	Да	Да	Да	Да	Нет	Нет	Нет	Нет	Нет	Нет	Нет
Работа по линии торговых представительств	Да*	Да	Да	Да*	Да	Да	Да	Да	Да	Да	Да
Работа по линии корпораций	Да	Да	Да	Да	Да	Да	Да	Да	Да	Да	Да
Иные форматы технологической кооперации	Курсы под эгидой НАТО	«Мастерские Лу Баня»	Нет	Курсы под эгидой НАТО	Курсы под эгидой НАТО	Курсы под эгидой НАТО	Нет	Нет	Нет	Курсы под эгидой Африканского Союза	Нет

Таблица 28. Форматы диалога ключевых конкурентов России со странами АЮС в разрезе цифровой безопасности. Составлено по открытым источникам.

Условные обозначения: «*» – сотрудничество с исключениями (из диалога в рамках региона исключены одна или несколько держав).

Глоссарий

Основные термины

Блокчейн – способ защищенного хранения и передачи данных в виде цепочки блоков, связанных друг с другом специальными ключами, в каждом из которых содержатся сведения о предыдущем.

«Видение» / «Vision» – обобщенное название проектов долгосрочных национальных реформ в области экономики. Характерной чертой «Vision» является упор на передовые технологии (цифовая экономика, искусственный интеллект и пр.).

Криптовалюта – разновидность цифровой валюты, учёт внутренних расчётных единиц которой обеспечивает децентрализованная платёжная система, работающая в полностью автоматическом режиме.

«Ложный флаг» (также *чужой флаг*) – тип тайной операции, осуществляемой с целью убедить общественность в том, что акции совершаются другими организациями или государствами.

Финтех (*FinTech*) – отрасль, состоящая из компаний, использующих технологии и инновации, чтобы конкурировать с традиционными финансовыми организациями в лице банков и посредников на рынке финансовых услуг.

Computer emergency response team (*CERT*) – Компьютерная группа реагирования на чрезвычайные ситуации. Постоянно действующая группа экспертов по компьютерной безопасности, занимающихся сбором информации об инцидентах, их классификацией и нейтрализацией.

Computer security incident response team (*CSIRT*) – Команда компьютерной безопасности по реагированию на инциденты. Группа экспертов по компьютерной безопасности, занимающихся сбором информации об инцидентах, их классификацией и нейтрализацией – как правило, имеет менее институционализированный характер, чем CERT, и может создаваться для ситуативного реагирования на киберугрозу.

Shetab – Межбанковская сеть передачи информации – иранская национальная платежная система, предоставляющая услуги проведения платежных операций и выпускающая банковские карты.

Основные сокращения

АС – Африканский союз.

АЮС – Африка южнее Сахары.

БПЛА (также БЛА) – Беспилотный летательный аппарат.

ГЧП – Государственно-частное партнерство.

ИИ – Искусственный интеллект

ИКТ – Информационно-коммуникационные технологии.

ИРИ – Исламская Республика Иран

КИИ – Критическая информационная инфраструктура.

ЛАГ – Лига арабских государств.

МСЭ – Международный союз электросвязи.

НПА – Нормативно-правовой акт.

САС – Смертоносные автономные системы.

СБП – Система быстрых платежей.

СВО – Специальная военная операция.

СВПД – Совместный всеобъемлющий план действий.

ССАГЗ – Совет сотрудничества арабских государств Залива.

ТЭК – Топливно-энергетический комплекс.

ЦБ – Центробанк / Центральный банк.

ЦФА – Цифровые финансовые активы.

AIFA – *Africa India Fintech Alliance* – Африканско-индийский FinTech-альянс.

APT – *Advanced Persistent Threat* – Постоянная серьезная угроза.

B2B – *Business to Business* – Бизнес для бизнеса (тип услуги).

CAMP – *Cybersecurity Alliance for Mutual Progress* – Альянс по кибербезопасности для взаимного прогресса.

CERT – *Computer emergency response team* – Компьютерная группа реагирования на чрезвычайные ситуации.

CSIRT – *Computer security incident response team* – Команда компьютерной безопасности по реагированию на инциденты.

GCI – *Global Cybersecurity Index* – Глобальный индекс кибербезопасности.

ISCC – Международная стратегия по развитию сотрудничества в киберпространстве (КНР).

ITU – *International Telecommunication Union* – Международный союз электросвязи.

NIN – *National Information Network* – Национальная информационная сеть (Иран).

QFTH – *Qatar FinTech Hub* – Катарский хаб финансовых технологий.

UNIDIR – *UN Institute for Disarmament Research* – Институт Организации Объединённых Наций по исследованию проблем разоружения.

Ярных А.Ю.

Ярных Андрей Юрьевич, член правления Регионального общественного центра интернет-технологий (РОЦИТ), член Экспертного совета ПИР-Центра

Доклад представляет собой существенный вклад в изучение перспектив регионального сотрудничества. Автор обстоятельно анализирует текущее состояние высокотехнологичного бизнеса, рассматривает факторы, способствующие развитию этого сектора, а также выявляет потенциальные угрозы и вызовы. Л.В. Цуканов представляет обширные агрегированные данные и аргументы, подкрепленные актуальными исследованиями, что делает его доклад интересным и информативным. Он также предлагает рекомендации и решения для улучшения позиции России, что является ценным вкладом в изучение вопросов внешней политики и экономики.

Козюлин В.Б.

Козюлин Вадим Борисович, к.полит.наук, главный научный сотрудник Центра военно-политических исследований Института актуальных международных проблем, Дипломатическая академия МИД России, Член Совета АНО «ПИР-Центр»

Автор доклада вложил немало труда и знаний, разбирая сложный цифровой ландшафт стран Персидского залива и Африки южнее Сахары, чтобы выявить ключевые тренды и определить возможности для России. В результате мы получили кладезь полезной информации для понимания этих регионов и формирования эффективных стратегий для нашей страны. Гибкий формат доклада позволяет изучать предлагаемые выкладки как в комплексе, так и порознь – в зависимости от исследовательских и практических интересов. Верю, что работа станет "настольной книгой", которая поможет российским специалистам определить свои способы выхода на новые рынки.

Себекин С.А.

Себекин Сергей Александрович, к.ист.наук, эксперт Института актуальных международных проблем Дипломатической академии МИД РФ, участник международной группы по исследованию злонамеренного использования искусственного интеллекта, доцент кафедры политологии, истории и регионоведения ИГУ

Представленный доклад является фундаментальным прикладным исследованием, в котором Л.В. Цуканов подвергает всестороннему анализу потенциал стран Персидского залива и Африки в сфере цифровых технологий. Потенциал представленного проекта как «настольной книги» (или даже «дорожной карты») очевиден. Доклад носит ярко выраженный практико-ориентированный характер, и может быть полезной для широкого круга лиц, участвующих в процессах принятия внешнеполитических решений, соответствующих структур, научно-аналитических центров и представителей бизнеса.

2025