НАЦИОНАЛЬНАЯ АССОЦИАЦИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ОСОБЕННОСТИ ПОЛИТИКИ ГОСУДАРСТВ-УЧАСТНИКОВ БРИКС В СФЕРЕ РАЗВИТИЯ ИКТ, ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ И МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

НАЦИОНАЛЬНАЯ АССОЦИАЦИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ОСОБЕННОСТИ ПОЛИТИКИ ГОСУДАРСТВ-УЧАСТНИКОВ БРИКС В СФЕРЕ РАЗВИТИЯ ИКТ, ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ И МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МОСКВА – 2024

Под общей редакцией президента НАМИБ, к.ю.н., Б.Н. Мирошникова

Редакционная коллегия:
Руководитель — В.П. Шерстюк, к.т.н., член-корреспондент Академии криптографии Российской Федерации, научный руководитель НАМИБ
А.А. Стрельцов, д.т.н., д.ю.н., профессор, заслуженный деятель науки Российской Федерации, член-корреспондент Академии криптографии Российской Федерации, вице-президент НАМИБ
А.И. Смирнов, д.и.н., профессор, член Российской академии естественных наук, помощник президента НАМИБ
В.В. Соколов, к.э.н., доцент, генеральный директор НАМИБ
А.А. Павлов, советник президента НАМИБ
Е.А. Михайлова, к.п.н., эксперт НАМИБ
Д.Ю. Рожков, сотрудник НАМИБ
А.В. Шлегель, сотрудник НАМИБ

Коллектив разработчиков:
С.В. Коротков, к.в.н., член-корреспондент Российской инженерной академии, начальник отдела НАМИБ
С.Г. Волкова, эксперт НАМИБ,
П.А. Карасев, к.п.н., эксперт НАМИБ
Е.А. Тарасов, эксперт НАМИБ

Сборник материалов разработан в интересах содействия председательству Российской Федерации в объединении БРИКС, которое вошло в новый исторический этап своего развития.

Основной целью подготовки сборника является изучение новой конфигурации объединения с точки зрения особенностей национальной политики и правовых баз в сфере цифровизации и развития ИКТ, исследования и внедрения передовых технологий, зрелости государственных систем обеспечения национальной и международной информационной безопасности. В этом контексте проведена систематизация положений деклараций БРИКС в части проблематики обеспечения безопасности использования информационно-коммуникационных технологий (ИКТ) и самих ИКТ, а также международной информационной безопасности (МИБ) и выделены механизмы их практической реализации. На основе открытых источников обобщены сведения о продвигаемых в БРИКС национальных, региональных и глобальных инициативах в сфере МИБ и заинтересованности новых участников в присоединении к сложившимся в объединении формам сотрудничества.

Результаты проведенного анализа могут быть использованы при определении перспективных для России сфер многостороннего и двустороннего взаимодействия в БРИКС по широкому спектру задач развития системы МИБ, при разработке переговорных позиций, налаживании эффективного и взаимовыгодного практического сотрудничества.

Материалы предназначены для профильных структур органов государственной власти, бизнес сообщества, научных работников, экспертов, специалистов и студентов, занимающихся проблемами МИБ и международного сотрудничества по этому приоритетному направлению деятельности.

Сборник разработан в соответствии с уставными задачами НАМИБ в целях содействия подготовке мероприятий на территории Российской Федерации и за рубежом, направленных на развитие государственно-частного партнерства в области формирования системы обеспечения МИБ, а также разработке материалов по вопросам реализации основных направлений государственной политики в указанной сфере.

ISBN 978-5-6044055-8-1

Содержание

6. Приложения

1. Новый исторический этап развития БРИКС: вызовы и основные задачи

БРИКС притягивает все больше сторонников и единомышленников — государств, которые разделяют принципиальные установки, лежащие в основе его деятельности. Это суверенное равенство, уважение выбора собственного пути развития, взаимный учет интересов, открытость, консенсус, стремление к формированию многополярного мироустройства и справедливой модели глобальной финансовой и торговой системы, поиск коллективных решений наиболее острых проблем современности.

В.В. Путин[1]

В 2009 году лидеры ведущих развивающихся государств — Бразилии, России, Индии и Китая (БРИК) в общих интересах положили начало развитию нового в своей основе «прагматичного, открытого и транспарентного диалога и сотрудничества» и «строительству гармоничного мира, в котором были бы обеспечены прочный мир и общее процветание»[2]. В декабре 2010 года к объединению присоединилась Южно-Африканская Республика, что привело к изменению наименования на БРИКС. За прошедшие годы многократно возросла роль объединения в глобальной политике и экономике.

Проведенный Южно-Африканской Республикой в 2023 году XVI Саммит БРИКС показал, что составляющие мировое большинство, развивающиеся страны всецело поддерживают цель формирования более справедливого многополярного мироустройства и проявляют неподдельный интерес к результатам взаимовыгодного сотрудничества объединения в сфере экономики и финансов, политики и безопасности, социального и культурного развития. Количество желающих стать членом этой «команды» постоянно растет, на «скамейке запасных» ожидают приглашения около 30 государств[3]. Поэтому принятое в Йоханнесбурге в 2023 году решение о расширении БРИКС можно без преувеличения назвать историческим. Оно дало старт началу нового этапа развития объединения, существенно повысило

1 Обращение Владимира Путина в связи с началом председательства России в БРИКС, 1 января 2024 года, http://www.kremlin.ru/events/president/news/73202.

2 Совместное заявление лидеров стран БРИК (г. Екатеринбург, Россия, 16 июня 2009 года).

3 Согласно процедуре, обсуждение процесса вступления является конфиденциальной информацией, поэтому некоторые данные в открытом доступе отсутствуют. По состоянию на февраль 2024 года около 30 государств официально проявили интерес к вступлению в БРИКС, т.е. уведомили МИД председательствующей страны. Подали заявки на членство в объединение 23 государства. По данным МИД России после официальной подачи заявок приглашение в БРИКС ожидают Алжир, Бангладеш, Бахрейн, Белоруссия, Боливия, Венесуэла, Вьетнам, Куба, Гондурас, Индонезия, Казахстан, Кувейт, Марокко, Нигерия, Пакистан, Палестина, Сенегал и Таиланд. Источник: Момент БРИКС: в МИД РФ обозначили статус стран — партнеров объединения // Известия, 2 февраля 2024, https://iz.ru/1643605/anastasiia-kostina/moment-briks-v-mid-rf-oboznachili-status-stran-partnerov-obedineniia.

Рисунок 1. Государства-участники и перспективы расширения объединения БРИКС

БРИКС – межгосударственное объединение, союз десяти государств:
1 – Бразилия, 2 – Россия, 3 – Индия, 4 – КНР, 5 – Южная Африка, 6 – ОАЭ, 7 – Иран, 8 – Египет, 9 – Эфиопия, 10 – Саудовская Аравия.

Подали заявки на вступление в БРИКС, ожидают приглашения:
11 – Алжир, 12 – Бангладеш, 13 – Бахрейн, 14 – Белоруссия, 15 – Боливия, 16 – Венесуэла, 17 – Вьетнам, 18 – Куба, 19 – Гондурас, 20 – Индонезия, 21 – Казахстан, 22 – Кувейт, 23 – Марокко, 24 – Нигерия, 25 – Пакистан, 26 – Палестина, 27 – Сенегал, 28 – Таиланд.

Заявка подана, но позднее отложена:
29 – Агрентина.

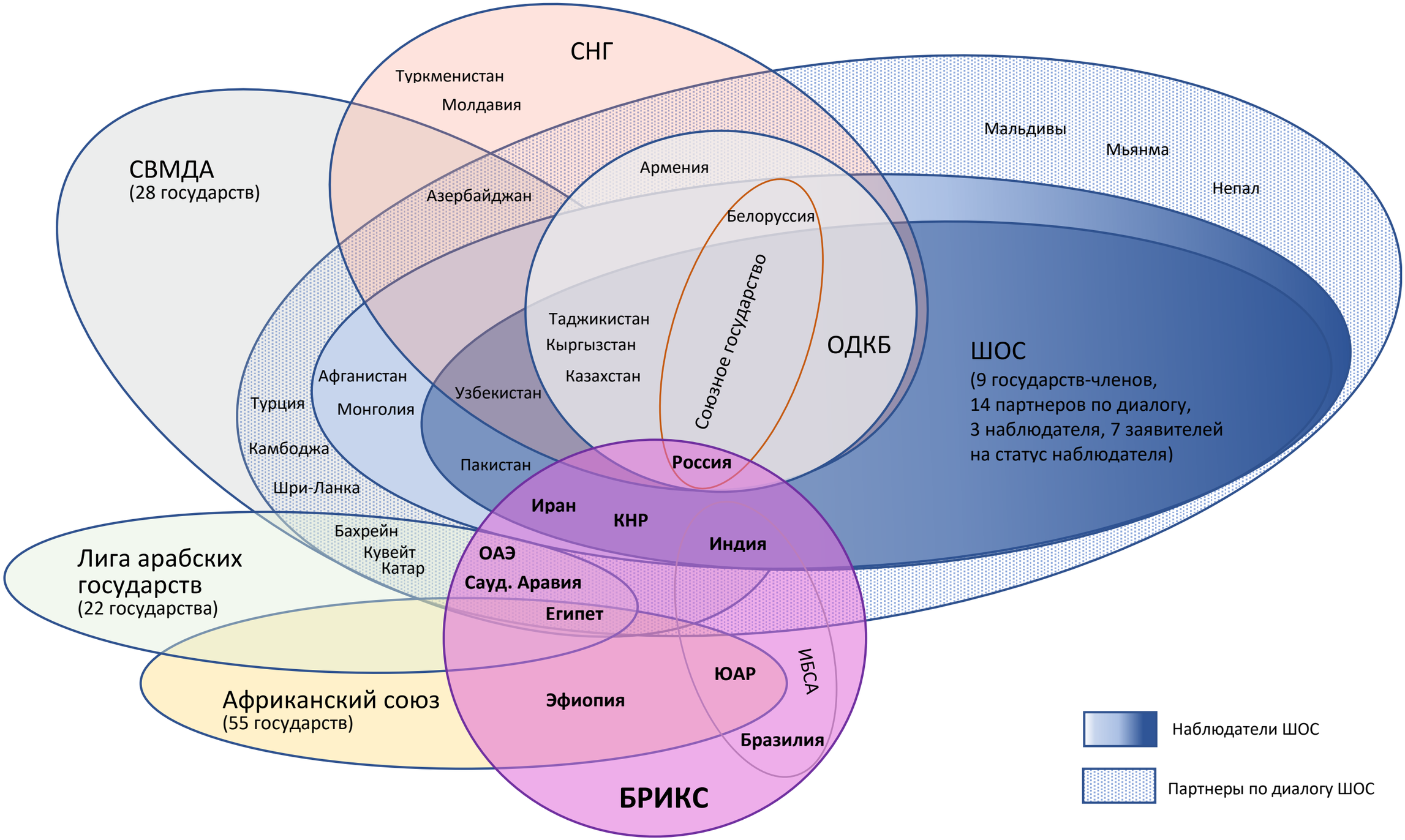


Рисунок 2. Основные международные объединения с участием государств-участников БРИКС*

* На рисунке не отражено участие пятерки БРИКС в различных экономических союзах: Бразилии в Общем рынке стран Южной Америки (МЕРКОСУР), России — в Евразийском экономическом союзе (ЕАЭС) и Союзе независимых государств (СНГ), Индии — в Южно-Азиатской ассоциации регионального сотрудничества (СААРК), ЮАР — в Сообществе развития Юга Африки (САДК), КНР — во Всеобъемлющем региональном экономическом партнерстве (ВРЭП) и Экономическом поясе Шелкового пути, а также в иных объединениях, являющихся инструментами реализации политики западных государств, например, Содружество наций (Индия, ЮАР), военный союз QUAD (Индия).

его коллективную ценность, политическое влияние и географический охват, что стало многообещающим фактором дальнейшего роста международного авторитета БРИКС.

К полноформатному участию с 1 января 2024 года приглашены шесть государств — Аргентинская Республика, Арабская Республика Египет, Исламская Республика Иран, Объединенные Арабские Эмираты, Королевство Саудовская Аравия и Федеративная Демократическая Республика Эфиопия[4]. Однако за два дня до этого срока Аргентина официально отказалась[5] от своей заявки, таким образом, на данном историческом этапе в БРИКС будет десять участников (Рисунок 1).

Название объединения решено сохранить, но ведущие российские и зарубежные эксперты обращают внимание, что с 2024 года это будет уже совсем другая сущность[6]. Образно можно сказать, что «БРИКС изначального образца передал франшизу на свой бренд другому хозяйствующему субъекту» [1]. Более важным в этом контексте видится неизменность базовых ценностей объединения, которые закреплены в руководящих принципах расширения:

- взаимное уважение, равенство и суверенитет, открытость и инклюзивность;
- решимость сохранить самобытность, согласованность и основанный на консенсусе характер БРИКС путем укрепления сотрудничества и содействия институциональному развитию;
- укрепление и реформирование многосторонней системы и соблюдение международного права;
- расширение представительства и более значительной роли развивающихся стран в международной системе;
- стремление к более справедливому и многополярному мироустройству за счет поддержки всеобъемлющей реформы ООН [2].

Для не попавших в данный этап расширения государств прорабатываются модальности новой категории сотрудничества — «государства-партнеры БРИКС» и механизмы их поэтапного привлечения к деятельности объединения. Одновременно обсуждаются механизмы взаимодействия членов БРИКС с различными

4 Пункт 91 Йоханнесбургской декларации-II XV саммита БРИКС (г. Сэндтон, ЮАР, 23 августа 2023 года).

5 Президент Аргентины Х. Милей 29 декабря 2023 года уведомил председательствующую в БРИКС Россию о том, что считает нецелесообразным в настоящее время вступать в объединение. Источник: Argentina Rejects BRICS Membership: President Millay Officially Reverses Decision, 30.12.2023, https://www.world-today-news.com/argentina-rejects-brics-membership-president-millay-officially-reverses-decision/.

6 Каждая из стран-основателей БРИКС помимо того, что является крупной развивающейся экономикой и входит в G20, обладает самобытной цивилизационной идентичностью и полным суверенитетом, то есть желанием и способностью (по своему совокупному потенциалу) проводить самостоятельную внешнюю и внутреннюю политику. Не все новые участники отвечают этим критериям. Источники: С. Лавров Не упустить главное: о плюсах и минусах расширения БРИКС // Россия в глобальной политике, 28.08.2023, https://globalaffairs.ru/articles/ne-upustit-glavnoe-briks/, Ф. Лукьянов Лучше меньше? Нет, больше! // Россия в глобальной политике, 25.08.2023, https://globalaffairs.ru/articles/luchshe-menshe-net-bolshe/.

региональными и субрегиональными экономическими и интеграционными объединениями развивающихся стран (сотрудничество через форматы БРИКС-плюс и БРИКС-аутрич в рамках программной и проектной деятельности объединения и его ключевых институтов) [3]. Таким образом, вокруг БРИКС складывается совершенно новая взаимосвязанная архитектура международного сотрудничества, построенная на свободном выборе партнеров и форм взаимодействия с полным уважением суверенитета и национальных интересов государств (Рисунок 2). Это может оказать существенное воздействие на формирование концепции многополярного мироустройства, поскольку фактически будет отражать позицию и интересы мирового большинства.

На данный момент БРИКС не является юридически оформленным межгосударственным объединением и не имеет свойственных таким структурам органов управления[7]. Почти все механизмы взаимодействия в рамках БРИКС поддерживаются политической волей и заинтересованностью участников[8]. За прошедшие годы была проделана огромная работа по сближению позиций и интересов стран-участниц, внешнеполитической координации, развитию инструментов многопланового экономического партнерства и созданию собственных финансовых и инвестиционных институтов, повышению связанности и разработки механизмов сотрудничества в сфере цифровизации и НТИ (наука, технологии и инновации) [4, 5]. Но полная внутренняя консолидация и определение организационно-правовой формы БРИКС еще не реализованы.

Двукратное увеличение участников БРИКС и значительное усложнение архитектуры взаимодействия, а также очевидная перспектива дальнейшего расширения БРИКС ставят вопрос формирования базовых управленческих механизмов для повышения эффективности деятельности, улучшения достижения консенсуса и информационного обеспечения (секретариат) и др. В связи с этим на председательствующую в 2024 году Российскую Федерацию ложится задача предложить к обсуждению формы более высокого уровня управления функционированием БРИКС, хотя четких сигналов по согласованию возможного кон-

7 Россия в рамках своего председательства в 2015 году предложила создать «виртуальный секретариат» — общий веб-сайт БРИКС как информационную платформу о работе объединения: принципах, целях и практиках (п. 75 Уфимской декларации). В настоящее время каждая страна ведет свой сайт, отражающий деятельность в рамках председательства в БРИКС, календарь событий, архив документов предыдущих саммитов и пр. По мнению заместителя председателя правления Национального комитета по исследованию БРИКС Г.Д. Толораи «необходимо как можно скорее ставить вопрос о создании секретариата, сначала с ограниченными функциями. Ведь не существует даже единого текста записи многосторонних встреч и договоренностей, дипломаты каждой из стран ведут свои собственные записи, что чревато недоразумениями. До сих пор не создан координационный центр по определению повестки дня, разработке текстов (этим занимаются шерпы).» Источник: Г. Толорая Зачем России БРИКС? На пути к новому мироустройству // Россия в глобальной политике, 19.02.2015, https://globalaffairs.ru/articles/zachem-rossii-briks/.

8 В качестве исключений можно привести следующие примеры: Соглашение о создании Нового банка развития (Agreement on the New Development Bank) и Договор о создании пула условных валютных резервов (Contingent Reserve Arrangement).

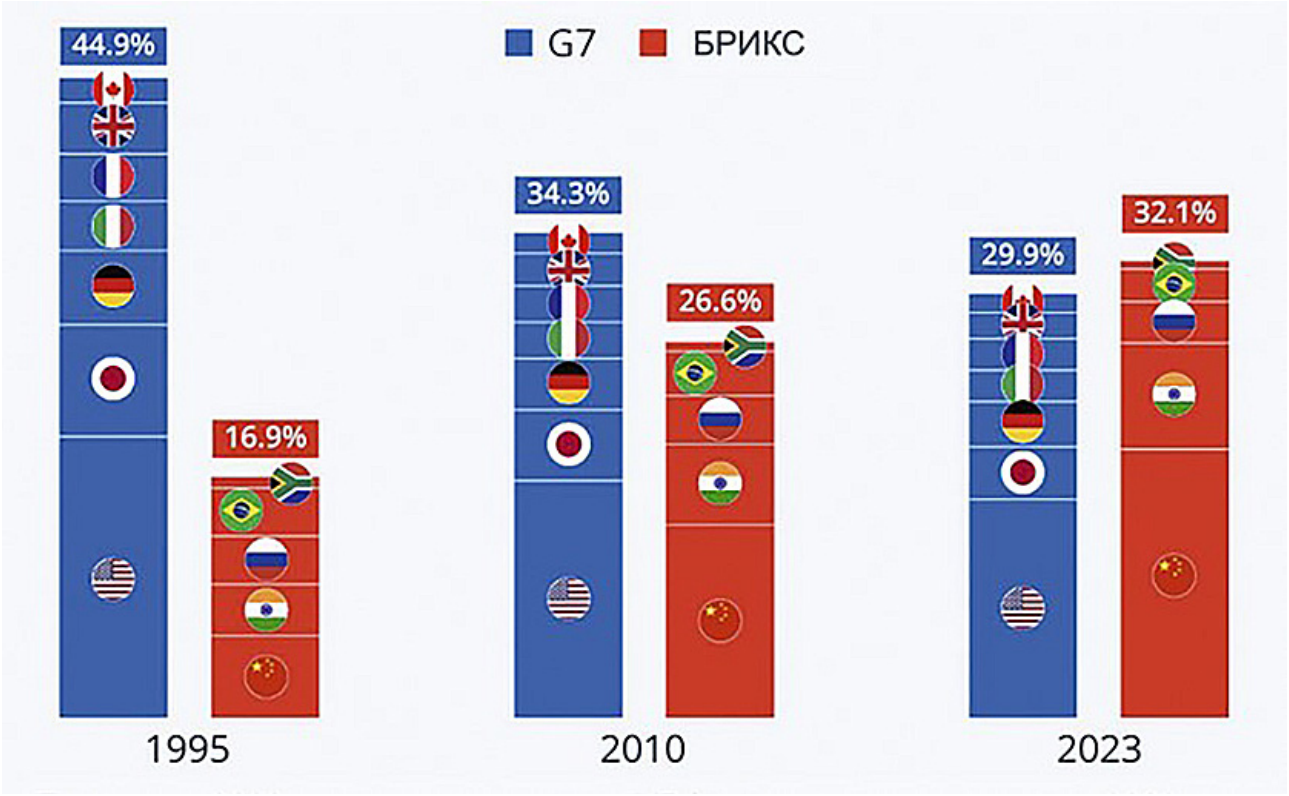


Рисунок 3. Доля «пятерки» БРИКС и G7 в мировом ВВП по паритету покупательной способности. Источник: Statista по оценочным данным МВФ на апрель 2023 года, https://www.vnedra.ru/lyudi/opit/tehnologii-stran-briks-novye-vozmozhnosti-dlya-gorno-metallurgicheskih-kompanij-23686/

тура институционализации пока не прозвучало[9]. Безусловно, это является внутренним вызовом, понижающим статус объединения в глазах международного сообщества. Для понимания сложности задачи институционализации отметим, что подобный процесс в аналогичных интеграционных объединениях занял значительное время[10].

Также нельзя игнорировать угрожающие объединению вызовы, формируемые внешними факторами. Очевидно, что в условиях геополитической и геоэкономической трансформации процесс расширения БРИКС и повышения роли объединения вступает в прямое противоречие с интересами коллективного Запада. Это неизбежно повлечет за собой увеличение политического и экономического давления, примерами чему служат ужесточение режимов санкций, ограничивающих взаимодействие государств-участников во многих сферах,

9 Пока сигналы взаимоисключающие: С. Лавров заявил, что не видит необходимости в создании Секретариата БРИКС, а Иран считает это необходимым. Из Индии поступают сигналы о необходимости подумать над формой сохранения «ядра» БРИКС внутри расширенного объединения. Западные эксперты детально изучают возможные варианты институционализации БРИКС и предлагают свое видение этого процесса. См. Institutionalization of BRICS: From Literature Review to Making Reality// InfoBRICS.org, December 29, 2023, https://infobrics.org/post/40173

10 В качестве примеров можно привести АСЕАН и Европейский союз.

в том числе дипломатической, создание политической напряженности и шантаж, провоцирование военных конфликтов на границах России, на Ближнем Востоке и в Юго-Восточной Азии.

Вызовы в политической сфере могут повлиять на способность объединения достигать консенсус по ключевым вопросам деятельности БРИКС. Не секрет, что присоединение новых игроков может нарушить сложившийся баланс и обострить имеющиеся проблемы двусторонних отношений, а также региональную конкуренцию между участниками с различными геополитическими и экономическими интересами, например, Индия — КНР, Иран — Саудовская Аравия, Египет — Эфиопия. Также следует принять во внимание, что с целью ослабления сплоченности объединения и снижения его привлекательности для новых претендентов коллективный Запад будет целенаправленно играть на этих противоречиях и усиливать давление. Сокращение политического влияния развивающихся государств на мировую политику может поставить под вопрос создание системы глобальной безопасности, формирование новых правил международных отношений и глобального управления, в том числе в сфере международной информационной безопасности.

Расширение БРИКС может столкнуться с серьезными экономическими вызовами. В последние десятилетия стабильный рост доли объединения в глобальной экономике явился позитивным сигналом для развивающихся рынков. В 2023 году совокупный ВВП пятерки БРИКС превысил показатель группы G7 в мировом ВВП (Рисунок 3). Сотрудничество стран-участниц способствует развитию национальных экономик: совокупная внешняя торговля БРИКС превысила 17% от глобального товарооборота. Международный валютный фонд прогнозирует, что несмотря на происходящую перенастройку мировых экономических связей, БРИКС продолжит развитие.

Пока экономики стран БРИКС объективно уступают государствам G7, прежде всего по уровню ВВП на душу населения (Рисунок 4). Соотношение показателей — 37% против 29,9% [6], но при этом следует принимать во внимание, что пятерка БРИКС представляет более 40% мирового населения, а в новом составе — 45,4%[11].

Новые государства-участники, за исключением Объединенных Арабских Эмиратов, обладающих значительным профицитом национального бюджета, имеют проблемы в национальных экономиках, что может оказать негативное воздействие на реализацию различных программ сотрудничества, например, таких как Стратегия экономического партнерства на период 2020–2025 годов [7].

Для БРИКС укрепление роста и повышение уровня конкурентоспособности экономик стран-участниц на международной арене является наиболее важным

11 Источник данных для расчета https://www.internetworldstats.com/stats8.htm

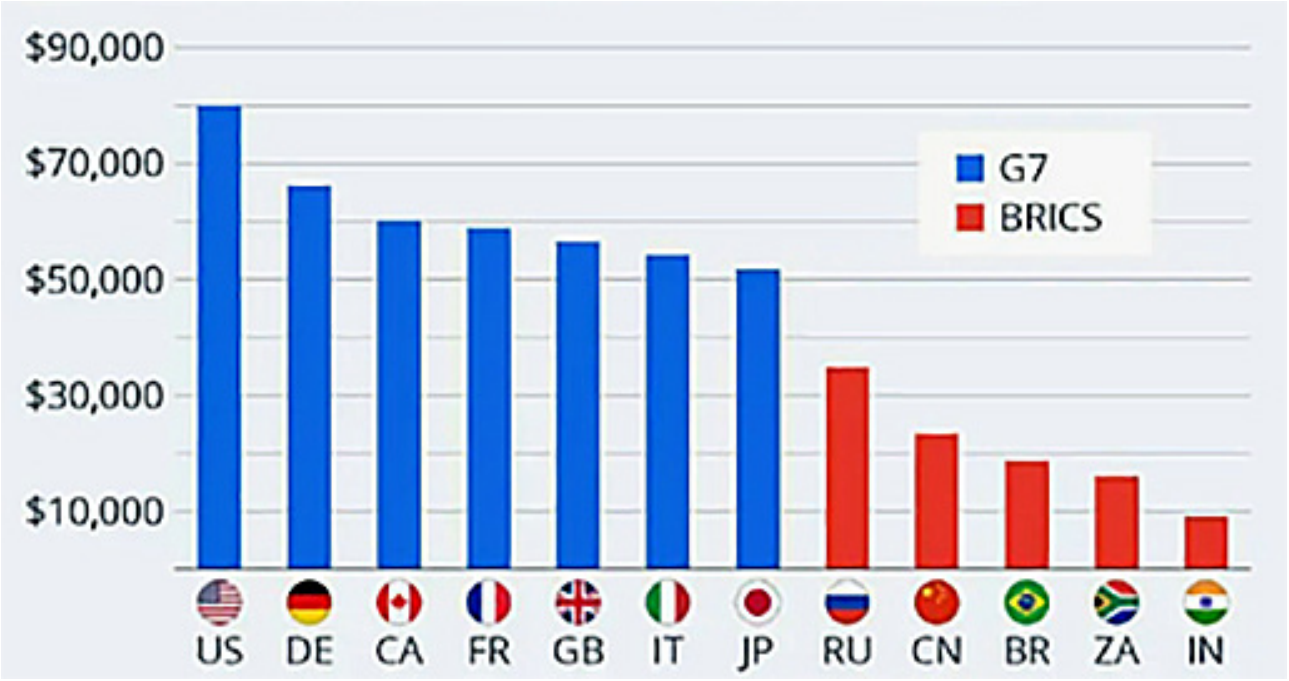


Рисунок 4. ВВП на душу населения в 2023 году в международных долларах по паритету покупательной способности стран G7 и БРИКС. Источник: SkyscraperCity Forum, https://www.skyscrapercity.com/threads/Мировая-экономика.1517936/page-20?u=618153

направлением сотрудничества, поэтому оно требует особого внимания. Предстоит сделать еще очень много и, прежде всего, усилить политическую и макроэкономическую координацию, торгово-экономическую интеграцию, найти формы взаимодействия для слабо сочетающихся экономических укладов и правовых систем, согласовать режимы регулирования деловой и инвестиционной активности, создать общую систему многосторонних расчетов в национальных валютах, а также повысить роль БРИКС в мировой финансовой системе [8, 9]. При наличии заинтересованности могут быть рассмотрены любые релевантные предложения, например, разрабатываемая российскими экспертами концепция общего экономического пространства [10].

При этом следует особо подчеркнуть, что все государства-участники БРИКС в своих стратегических документах определили цифровизацию ключевым инструментом экономического и социального развития. Поэтому приоритетное внимание будет уделено сотрудничеству в сфере информационно-коммуникационных технологий (ИКТ) и инноваций, обеспечения информационной безопасности и подготовки необходимых кадров.

Новая конфигурация объединения в указанных сферах деятельности, с одной стороны, добавляет определенные трудности, связанные с неравномерным экономическим и технологическим потенциалом стран-участниц БРИКС, а с другой — создает новые точки роста для сотрудничества (Таблица 1).

Например, Эфиопия, относящаяся к странам с низким уровнем дохода, испытывает проблемы как с развитием инфраструктуры, так и с обеспечением безопасного использования ИКТ, но при этом демонстрирует высокие темпы экономического роста, цифровизации и даже развития инноваций. Два государства из группы стран с высоким уровнем доходов — Саудовская Аравия и Объединенные Арабские Эмираты — несомненно усилят БРИКС. Эти страны в числе мировых лидеров цифровизации и ее нормативного регулирования, обеспечения национальной системы информационной безопасности, финансирования научных исследований и трансфера технологий, создания благоприятной бизнес-среды для инноваций. Египет и Иран относятся к группе стран с достатком ниже среднего, поэтому в рассматриваемой сфере несколько уступают ЮАР, которая в исходном составе БРИКС была самым слабым участником, однако они демонстрируют системную диверсификацию экономики, высокий уровень капитализации внутреннего рынка, доступности и использования ИКТ-инфраструктуры, рост научных исследований и их цитируемости. В сфере цифровизации Эфиопия заметно уступает другим участникам, но является самой быстрорастущей экономикой мира с огромным демографическим потенциалом, что делает ее крупным потребителем ИКТ-технологий и практик их использования.

Для успешного развития БРИКС важно, чтобы отличающиеся потенциалы государств-участников гармонично дополнили друг друга, содействуя повышению возможностей партнеров, создавая мультипликативный эффект для преодоления цифрового разрыва и укрепления объединения.

В этом контексте актуальной задачей является изучение новой конфигурации БРИКС с точки зрения особенностей национальных политик в сфере цифровизации и развития ИКТ, исследования и внедрения передовых технологий, зрелости, обеспечивающих их правовых баз и государственных систем национальной информационной безопасности. Необходимо оценить решимость новых участников присоединиться к реализации соответствующих положений деклараций БРИКС и готовность вписаться в уже действующие формы сотрудничества объединения. Не менее важно понимать цели и задачи каждого участника как в БРИКС, так и в других форматах международного сотрудничества, нужно также учитывать их подходы к формированию системы международной информационной безопасности.

Целью разработки представленного Вашему вниманию сборника было содействие председательству Российской Федерации в БРИКС, гармоничной интеграции новых стран-участниц в работу объединения, определению с учетом национальных особенностей перспективных сфер двустороннего и многостороннего сотрудничества, подготовке переговорных позиций и налаживанию эффективного практического взаимодействия.

Таблица 1. Уровень цифровизации и зрелости национальных политик в сфере ИКТ и обеспечения информационной безопасности в БРИКС

		Уровень цифровизации и инноваций				Стратегическое планирование		
		2023	ITU IDI 2023	UN DESA 2022	WIPO GII 2023			
		Уровень проникновения Интернет (% к населению)	Ранг в мире по индексу развития ИКТ (значение индекса)	Ранг в мире по уровню развития эл. правительства	Ранг в мире по инновационному индексу (значение индекса)	В сфере развития ИКТ/ цифровизации	В сфере кибербезопасности	В сфере искусственного интеллекта
1.	Бразилия	84	70 (81,9)	49 (оч.выс.)	49 (33,6)	2018	2010 2020	2021
2.	Египет	52,5	98 (75,8)	103 (выс.)	86 (24,2)	2012 2021	2018 2021	2021
3.	Индия	48,7	Нет данных	77 (выс.)	40 (38,1)	2015	2013 2020 (проект)	2018 (проект)
4.	Иран	91	75 (80,9)	91 (выс.)	62 (30,1)	2020	2020 (ВС Ирана)	—
5.	Китай	69,8	65 (84,4)	43 (оч. выс.)	12 (55,3)	2016 2021	2017	2017
6.	ОАЭ	103,3	10 (96,4)	13 (оч. выс.)	32 (43,2)	2021	2019	2017
7.	Россия	88,2	38 (88,9)	42 (оч. выс.)	51 (33,3)	2013 2017	2016 2021	2019
8.	Саудовская Аравия	99	11 (94,9)	31 (оч. выс.)	48 (34,5)	2016 2018	2013 2020	2020
9.	Эфиопия	17,9	158 (33,8)	79 (низ.)	125 (14,3)	2016 2020	2021	2023 (проект)
10.	ЮАР	57,5	89 (80,5)	65 (выс.)	59 (30,4)	2016 2021	2012	R&D

Национальное законодательство			Защищенность национального информационного пространства			
ITU G5 Benchmark 2023	Противодействие преступности в сфере ИКТ	Защита персональных данных	ITU GCI 2020 Глобальный индекс кибербезопасности			Нац. группа реагирования на компьютерные инциденты, год создания
Оценка зрелости системы правового регулирования ИКТ (значение индекса)			Индекс развития гос. политики в сфере кибербезопасности	Ранг в регионе	Ранг в мире	
развитая (75,31)	2012	2018 2020	96,6	3	18	CERT.br 2001
развитая (69,29)	2018	2003 2020	95,48	3	23	EG-Cert 2009
передовая (81,94)	2000	2023	97,5	4	10	CERT-In 2004
переходн. (53,70)	2009	2019 (проект)	81,06	12	54	IrCERT 2008
развитая (71,45)	2015	2016 2021	92,53	8	33	CNCERT/CC 2001
развитая (77,16)	2012	2017	98,06	2	5	aeCERT 2008
развитая (64,04)	2017 2022	2006 2023	98,06	1	5	НКЦКИ (cert.gov.ru) 2018
передовая (80,40)	2007	2019	99,54	1	2	Saudi CERT 2006
переходн. (50,62)	2016 2018	2023 (проект)	27,74	21	115	Ethio-CERT 2012
развитая (69,29)	2021	2013 2018	78,46	8	59	Cybersecurity Hub, 2012

Использованная литература

1 Ф. Лукьянов Бренд с франшизой // Россия в глобальной политике, 28.08.2023, https://globalaffairs.ru/articles/brend-s-franshizoj/?ysclid=ls99rkagjy317745687.

2 BRICS Membership Expansion Guiding Principles, Standards, Criteria and Procedures, 2023, https://brics2023.gov.za/wp-content/uploads/2023/11/BRICS-Membership-expansion-guiding-principles-criteria-and-standards-2023.pdf.

3 С. Лавров Не упустить главное: о плюсах и минусах расширения БРИКС // Россия в глобальной политике, 28.08.2023, https://globalaffairs.ru/articles/ne-upustit-glavnoe-briks/.

4 Strategy for BRICS Economic Partnership 2025, https://www.economy.gov.ru/material/file/3a71260309ef290a0cfa3fe698a55e83/Strategy%20for%20BRICS%202025.pdf?ysclid=ls8x4ausok190124174,

5 Implementation of the Strategy for BRICS Economic Partnership in the period 2015–2020. Overview Prepared by BRICS Russia Expert Council // National Committee on BRICS Research Russia, https://nkibrics.ru/ckeditor_assets/attachments/600e8d816272697eb40a0000/overview_-_implementation_of_the_strategy_for_brics_economic_partnership_in_the_period_2015-2020.pdf?1611566465.

6 Проректор НИУ ВШЭ Виктория Панова — о российском председательстве и новых возможностях объединения на фоне расширения состава участников // Известия, 2.01.2024, https://iz.ru/1621072/viktoriia-panova/vremia-briks.

7 Стратегия экономического партнерства БРИКС до 2025 года, http://static.kremlin.ru/media/events/files/ru/KT0SBHnIZjOpIuAj2AOXCnszNQA8u7HL.pdf.

8 Проректор НИУ ВШЭ Виктория Панова — о российском председательстве и новых возможностях объединения на фоне расширения состава участников // Известия, 2.01.2024, https://iz.ru/1621072/viktoriia-panova/vremia-briks.

9 А. Кузнецов БРИКС в мировой финансовой системе: необходимость выравнивания правил игры // РСМД, 14 декабря 2023, https://russiancouncil.ru/analytics-and-comments/analytics/briks-v-mirovoy-finansovoy-sisteme-neobkhodimost-vyravnivaniya-pravil-igry/.

10 К.В. Бабаев, С.В. Лавров И вширь, и вглубь // Россия в глобальной политике. 2023. Т. 21. № 5. С. 69–81, https://globalaffairs.ru/articles/vglub-i-vshir-brics./

2. Деятельность БРИКС по формированию системы международной информационной безопасности

1. Основные механизмы координации и форматы взаимодействия

С каждым годом БРИКС набирает свой геополитический вес и все более активно выступает в роли ключевого игрока мировой политики, продвигая интересы всех развивающихся стран[1]. Достигнутые успехи технологического развития позволяют странам-участницам БРИКС активно участвовать в формировании международной повестки в сфере развития информационных и коммуникационных технологий (ИКТ) и обеспечения их безопасности. Общие для участников объединения вызовы, прежде всего уязвимость критических информационных инфраструктур, киберпреступность и терроризм[2] — создают предпосылки для политического сближения в целях защиты национальных и общих интересов.

Важно отметить, что БРИКС не является международной организацией и не имеет свойственных таковым органов управления, однако достигнутый за эти годы прогресс в институционализации деятельности объединения очевиден. Прежде всего, он выражается в создании различных постоянно действующих механизмов координации и форматов взаимодействия.

---

1 Начиная с 2012 года, на саммитах БРИКС стали рассматриваться вопросы региональной безопасности: в Делийской декларации — Афганистан; в Этеквинской – Сирия, Палестина, мирный процесс на Ближнем Востоке, Иран, Афганистан, террористическая ситуация в Демократической республике Конго и ЦАР; в Форталезской — ситуация в отдельных регионах Африки, Сирия, Афганистан, ситуация на Украине, арабо-израильский конфликт, переговоры по Ирану, в Йоханнесбургской-II проблемы Судана и Южного Сахеля, Гаити и Украины.

2 Согласно Глобальному индексу терроризма, рассчитанному в 2022 году Лондонским институтом экономики и мира, страны-участницы БРИКС улучшили ситуацию по уровню террористических угроз, но он по-прежнему значителен: Индия на 12 месте в мире, Россия на 44, Китай на 67, Бразилия на 81 месте. Источник: Global Terrorism Index 2022 // Institute for Economics & Peace, https://www.visionofhumanity.org/wp-content/uploads/2022/03/GTI-2022-web.pdf.

К постоянно действующим механизмам относятся: Ежегодные саммиты БРИКС; Встречи лидеров «на полях» саммитов G20, Генеральной Ассамблеи ООН и других крупных международных мероприятий; Встречи высоких представителей, курирующих вопросы безопасности; Совет управляющих Новым банком развития; Встречи министров иностранных дел, руководителей других отраслевых министерств и ведомств (полноформатные и «на полях»); Встречи шерп/су-шерп (представители МИДов).

Среди основных форматов взаимодействия следует указать: Рабочие группы по сотрудничеству в различных областях[3]; Семинары, конференции и форумы; Обширную сеть неформальных диалоговых партнерств, включая взаимодействие деловых кругов, экспертных центров и академического сообщества, профсоюзов, парламентариев, молодежи и гражданского общества[4]. По итогам XV саммита БРИКС в Йоханнесбурге шерпам поручено продолжить обсуждение вопросов институционального развития, в том числе по консолидации сотрудничества БРИКС [5].

Кроме того, объединение стало платформой для развития внутри региональных и транс региональных связей и реализации политики «интеграции интеграций» [1]. Так, по инициативе ЮАР с 2013 года объединение активно развивает сотрудничество в формате БРИКС-аутрич, который позволяет привлекать к работе региональных участников, соседних по отношению к председательствующей в БРИКС стране. Расширяется и глобальный формат БРИКС-плюс по поиску совместных решений для общих вызовов с заинтересованными государствами, международными организациями и объединениями. На сегодняшний день около двадцати стран выражают активную заинтересованность во вступлении в БРИКС. По словам Президента Российской Федерации В.В. Путина, такие контакты с различными регионами мира способствуют росту авторитета БРИКС [2]. Сегодня можно уверенно говорить, что БРИКС постепенно трансформируется из дискуссионной площадки в прообраз политического и экономического союза государств, объединенных общими взглядами на проблемы мирового развития и глобального управления [3].

---

3 Действуют Рабочие группы по противодействию терроризму, вопросам сотрудничества в сфере ИКТ и высокопроизводительных вычислений, в том числе по передовым технологиям, информационной безопасности, борьбе с наркотиками, по торгово-экономическим вопросам, по защите интеллектуальной собственности, вопросам занятости, окружающей среды, противодействия коррупции, таможенным вопросам, сельскому хозяйству, здравоохранению, молодежной политике и др.

4 Начало работы «второй дорожки» БРИКС положило решение об организации Делового форума и Конференции экспертных центров параллельно с саммитом 2010 года в г. Бразилиа.

5 Пункт 88 Йоханнесбургской декларации-II, XV саммит БРИКС (г. Сэндтон, ЮАР Среда, 23 августа 2023 года).

2. Анализ деятельности БРИКС в сфере международной информационной безопасности

Главной целью объединения является взаимовыгодное сотрудничество в интересах устойчивого экономического и социального развития участников. Безопасность во всех ее аспектах (политическом, экономическом, финансовом, технологическом, общественном, социальном и т.д.) становится необходимым условием достижения этой цели, поскольку «природа мира и безопасности неделима».

Деятельность БРИКС развивается по трем ключевым направлениям: «Политика и безопасность», «Экономика и финансы», «Социальное и культурное развитие» [4]. Каждое из них за счет компонентов использования ИКТ и обеспечения безопасности этих технологий имеет связь с задачей формирования системы международной информационной безопасности (МИБ) и определенной в ней триадой угроз: использование ИКТ в террористических, преступных и военно-политических целях. Подход БРИКС основывается на обеспечении мирного использования информационного пространства, повышении потенциала и координации действий стран-участниц по использованию ИКТ, что позволяет объединению вносить более весомый вклад в глобальные усилия по обеспечению МИБ.

2.1. Направление «Политика и безопасность», аспект противодействия терроризму

Последовательное развитие концепции деятельности БРИКС в обеспечении глобальной безопасности наглядно прослеживается на примере аспекта противодействия террористической деятельности, в том числе с использованием ИКТ. Красной линией через все итоговые документы саммитов объединения проходит осуждение терроризма во всех формах и проявлениях, как угрозы миру и безопасности. Уже на первой встрече лидеров стран БРИК была продекларирована задача борьбы с этим негативным явлением.

Год от года в итоговых документах саммитов конкретизировались принципы и подходы к данному направлению деятельности, одновременно отмечалась центральная роль ООН в координации усилий по предотвращению террористических актов, использованию социальных медиа и других ИКТ для распространения идеологии терроризма и насильственного экстремизма. Последний может является питательной средой терроризма, источником его финансирования, в том числе посредством компьютерной преступности.

Страны БРИКС постоянно расширяли свои международные обязательства в этой сфере. С ростом осознания задач противодействия терроризму к обещанию руководствоваться при их решении принципами Устава ООН постепенно

добавлялись другие обязательства: соблюдение международного гуманитарного права[6], прав человека и основных свобод[7], прав беженцев[8].

Также постепенно происходил переход от призывов воздерживаться от всех видов пособничества терроризму и эффективно выполнять все обязательства, вытекающие из резолюций Совета безопасности и Генеральной Ассамблеи ООН и международных стандартов ФАТФ, к осуществлению конкретных действий. Сейчас БРИКС демонстрирует четкую позицию, состоящую в продвижении комплексного подхода и широкой международной коалиции всех заинтересованных сторон на принципах суверенного равенства государств, невмешательства во внутренние дела и неприемлемости двойных стандартов в отношении терроризма[9]. Начиная с 2010 года в концепции все более настойчиво формулируется необходимость завершения работы в рамках Комитета по разоружению над Всеобъемлющей конвенцией по международному терроризму, а также запуска широкого переговорного процесса по Международной конвенции о борьбе с актами химического и биологического терроризма[10].

Полное согласие по этим позициям позволяет БРИКС выступать единым фронтом на всех международных площадках и реализовывать практическое сотрудничество. Прежде всего здесь следует отметить Встречи высоких представителей, курирующих вопросы безопасности, где обсуждаются актуальные угрозы и меры противодействия, в том числе, международные и региональные очаги напряженности, борьба с терроризмом и транснациональной организованной преступностью, безопасность в сфере использования ИКТ, миротворчество, а также взаимосвязи между безопасностью и проблематикой устойчивого развития.

В 2016 году создана Рабочая группа по антитеррору БРИКС (РГАТ), которая постоянно расширяет направления своей деятельности. В 2023 году в ее составе были пять тематических подгрупп. Проведено несколько семинаров по актуальной проблематике: национальные стратегии борьбы с терроризмом, противодействие использованию Интернета в террористических целях, цифровая экспертиза и криминалистика, целевые финансовые санкции. Проводится подготовка сотрудников правоохранительных органов стран-участниц.

Опыт практического взаимодействия способствовал выработке Антитеррористической стратегии БРИКС, она принята в рамках российского председательства в 2020 году [5]. Стратегия включает укрепление взаимодействия в борьбе

---

6 Впервые тематика включена в Уфимскую декларацию VII саммита БРИКС (г. Уфа, Россия, 9 июля 2015 года).
7 Впервые тематика включена в Форталезскую декларацию VI саммита БРИКС (г. Форталеза, Бразилия, 15 июля 2014 года).
8 Впервые тематика включена в Йоханнесбургскою декларацию X саммита БРИКС (г. Йоханнесбург, ЮАР, 26 июля 2018 года).
9 Впервые тематика включена в Форталезскую декларацию (г. Форталеза, Бразилия, 15 июля 2014 года).
10 Декларация Бразилиа XI саммита БРИКС (г. Бразилиа, Бразилия, 14 ноября 2019 года).

с использованием ИКТ в террористических и иных преступных целях, подразумевает совершенствование практического сотрудничества спецслужб и правоохранительных органов, в том числе посредством своевременного обмена точной информацией, а при необходимости — даже создания правовой основы для такого обмена. В 2021 году был принят План действий по реализации стратегии, координация его выполнения возложена на формат Встречи высоких представителей, практическая реализация — на РГАТ.

2.2. Направление «Политика и безопасность», аспекты борьбы с киберпреступностью и повышения информационной безопасности

Как отмечено выше, БРИКС ставит перед собой масштабную задачу содействия развитию мирного, безопасного и открытого цифрового и Интернет-пространства, что отражается в декларациях БРИКС с 2011 года в контексте приверженности сотрудничеству в укреплении МИБ. В связи с этим киберпреступления и компьютерные атаки расцениваются как угроза глобальной безопасности, а борьба с ними — как одно из ключевых направлений сотрудничества [6]. В этих целях объединение взаимодействует с Комиссией по предотвращению преступности и уголовному правосудию Экономического и социального совета ООН (ECOSOC), где впервые от имени БРИКС в 2013 году был внесен проект резолюции «Укрепление международного сотрудничества в целях борьбы с киберпреступностью» [7], направленный на усиление действий мирового сообщества по изучению и реагированию на преступления в сфере высоких технологий.

Вместе с тем, БРИКС делает больший акцент на повышение безопасности ИКТ, защиту пользователей, в том числе прав и основополагающих свобод человека, на формирование системы, позволяющей обеспечить конфиденциальность и защиту персональной информации, на разработку общепризнанных норм и принципов международного права, адаптированных к особенностям ИКТ-среды, в том числе направленных против нарушения суверенитета государств, массовой электронной слежки и сбора по всему миру данных о частных лицах[11]. В текущих планах БРИКС — развитие инициатив в сфере защиты детей от сексуальной эксплуатации в сети Интернет и от другого цифрового контента, наносящего вред их здоровью и развитию[12].

С 2016 года БРИКС отмечает необходимость укрепления международного сотрудничества в борьбе с использованием ИКТ в преступных целях и продолжения работы над правилами ответственного поведения государств в ИКТ-среде. В этом контексте с 2016 года приветствуются результаты, достигнутые в ООН,

11 См. Уфимскую, Этеквинскую и Форталезскую декларации.
12 Нью-Делийская декларация XIII саммита БРИКС (г. Нью-Дели, Индия, 9 сентября 2021 года).

прежде всего — в Группе правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (ГПЭ по МИБ)[13], Рабочей группе ООН открытого состава (РГОС) по вопросам безопасности в сфере использования ИКТ и самих ИКТ[14], а также созыв новой РГОС на 2021–2025 годы.

В 2015 году БРИКС четко сформулирована задача разработки под эгидой ООН универсального юридически обязывающего инструмента по вопросам борьбы с использованием ИКТ в преступных целях, поскольку неправомерное использование информационного пространства может поставить под угрозу международный мир и безопасность. В связи с этим высоко оценены результаты работы Межправительственной группы экспертов по киберпреступности и запуск функционирования Специального комитета по разработке в рамках ООН всеобъемлющей конвенции о противодействии использованию ИКТ в преступных целях, созванного в соответствии с резолюцией Генеральной Ассамблеи ООН A/RES/75/282 от 12 мая 2021 года[15].

Практическая деятельность БРИКС в сфере кибербезопасности осуществляется в рамках Рабочей группы по вопросам безопасности в сфере использования ИКТ, созданной по инициативе России в 2015 году. Основными направлениями ее деятельности являются: обмен информацией и передовой практикой в вопросах безопасности в сфере использования ИКТ; эффективная координация мер противодействия киберпреступности; выделение уполномоченных по связям в государствах-участниках; сотрудничество между странами БРИКС с использованием существующих групп реагирования на компьютерные инциденты в области компьютерной безопасности; совместные проекты в области НИОКР; укрепление потенциала; а также разработка международных норм, принципов и стандартов[16]. Вместе с тем, в работе группы имеются сложности. Одной из них являются отличия в правовых основаниях борьбы с компьютерными преступлениями. Так, в 2022 году Бразилия ратифицировала Конвенцию Совета Европы о киберпреступности (т.н. Будапештская конвенция) [8] и, соответственно, присоединилась к ее процедурам и протоколам взаимодействия. Напротив, ЮАР ее не подписала, хотя была в числе разработчиков конвенции в 2001 году. Россия, Китай и Индия также не являются участниками этого международного договора. Другой сложностью является противопоставление «демократий» оси Юг-Юг

13 Декларация Гоа VIII саммита БРИКС (шт. Гоа, Индия, 16 октября 2016 года). Следует отметить, что представители БРИКС внесли значительный вклад в работу шести созывов ГПЭ по МИБ: Россия и КНР были членами группы всех 6 созывов, Индия — 5, Бразилия — 4, ЮАР — 3, кроме того Россия дважды была председателем (в 2004–2005 и 2009-2010 годах), а Бразилия возглавляла группу в 2014-2015 годах.

14 Первый созыв РГОС на 2019-2020 годы по резолюции ГА ООН A/Res/73/27 от 5 декабря 2018 года, второй созыв на 2021–2025 годы по A/Res/75/240 от 31 декабря 2020 года.

15 Отмечено в Пекинской декларации XIV саммита БРИКС (г. Пекин, КНР, 24 июня 2022 года).

16 Уфимская декларация VII саммита БРИКС (г. Уфа, Россия, 9 июля 2015 года).

(объединение IBSA — Индия, Бразилия, ЮАР) и «автократий» Россия-КНР, что зачастую приводит к проблеме нахождения баланса между интересами пользователей ИКТ и общественной безопасностью, несмотря на то что без достижения последней невозможно обеспечить защиту частных лиц.

В 2020 году были опубликованы комплексные документы, используемые в рамках специального Канала БРИКС по информационной безопасности и содержащие правила и передовые практики: Электронный справочник регуляторных актов стран БРИКС в сфере информационной безопасности и Сборник лучших практик по надзору и контролю за рисками информационной безопасности.

К настоящему моменту разработана Дорожная карта практического сотрудничества БРИКС в обеспечении безопасности в сфере использования ИКТ. Кроме того, ставится более масштабная задача — формирование нормативно-правовых рамок для взаимодействия стран БРИКС по вопросам МИБ. Например, предложение России о разработке соответствующего межправительственного соглашения о сотрудничестве в сфере использования ИКТ и инициатива Бразилии о разработке двусторонних соглашений между странами БРИКС по указанной тематике[17].

В 2023 году сделан дополнительный акцент на продолжение сотрудничества и поддержку инициатив в сфере информационной и кибербезопасности, включая обмен знаниями и опытом[18].

2.3. Направление «Политика и безопасность», аспект реформирования глобального управления

Цель БРИКС в укреплении и реформировании многосторонней системы глобального управления очевидна — создание более честного, справедливого, равноправного и представительного многополярного миропорядка для процветания всего человечества и совместного противостояния традиционным и нетрадиционным вызовам безопасности. Однополярный мир, возглавляемый коллективным Западом, уже не соответствует роли развивающихся стран в мировой экономике и политике.

Концепция действий БРИКС в этой сфере начала постепенно кристаллизоваться из тезиса о приверженности объединения многосторонней дипломатии и необходимости всеобъемлющего реформирования ООН с целью повышения эффективности организации в реагировании на современные вызовы[19]. В частности, начиная с 2011 года Россия и Китай ежегодно «подтверждают важность,

17 Московская декларация XII саммита БРИКС (г. Москва, Россия, 17 ноября 2020 года).
18 Йоханнесбургская декларация-II XV саммита БРИКС (г. Сэндтон, ЮАР, 23 августа 2023 года).
19 Совместное заявление лидеров стран БРИК (г. Екатеринбург, Россия, 16 июня 2009 года).

которую они придают статусу Бразилии, Индии и ЮАР в международных делах, понимают и поддерживают их стремление играть большую роль в ООН». Именно в этом контексте следует рассматривать тезис о реформе Совета безопасности ООН[20], подразумевающий включение Бразилии и Индии в число постоянных членов этого важнейшего органа. В 2018 году БРИКС был сделан следующий шаг — обозначена «давно назревшая и нерешенная задача по обеспечению надлежащего представительства африканских стран в ООН, особенно применительно к решению вопросов мира и безопасности»[21].

По мнению БРИКС, система глобального управления должна быть реформирована в гораздо большем объеме. Уже в 2010 году была поставлена задача увеличения квот голосов стран БРИКС в Международном валютном фонде (МВФ) и для участия в выборе руководителей МВФ и Всемирного банка[22]. В последующие годы список международных органов, деятельность которых должна быть «решительно обновлена», пополнился Всемирной торговой организацией[23], Экономическим и социальным Советом ООН[24] и Всемирной организацией здравоохранения [9]. Все указанные действия БРИКС направлены на расширение участия развивающихся стран в новом мировом порядке.

С этих же позиций следует рассматривать предложения БРИКС по реформированию системы управления сетью Интернет, которая является международным ресурсом, обеспечивающим, в том числе, достижение Целей устойчивого развития ООН 2030 [10]. Концепция действий в этой сфере развивалась постепенно. В 2015 году был взят курс на интернационализацию управления Интернетом на основе равноправного участия всех государств в развитии и функционировании глобальной сети, «принимая во внимание необходимость привлечения соответствующих заинтересованных сторон в определенном качестве и с определенными обязательствами», на основе открытого и демократического процесса, не подверженного влиянию решений, принятых в одностороннем порядке[25].

---

20 Декларация, принятая по итогам III саммита БРИКС (г. Санья, о. Хайнань, Китай, 14 апреля 2011 года).

21 Йоханнесбургская декларация X саммита БРИКС, Делийская декларация XIII саммита БРИКС, Пекинская декларация XIV саммита БРИКС.

22 Пункт 11 Совместного заявления глав государств и правительств стран-участниц II саммита БРИК (г. Бразилиа, Бразилия,15 апреля 2010 года).

23 Декларация Бразилиа XI саммита БРИКС (г. Бразилиа, Бразилия, 14 ноября 2019 года). Совместное заявление министров торговли БРИКС по поддержке многосторонней торговой системы и реформированию ВТО (Joint Statement by BRICS Trade Ministers on Multilateral Trading System and the WTO Reform) в рамках XII саммита БРИКС в Москве. В Йоханнесбургской декларации-II XV саммита БРИКС сформулированы конкретные цели, которые объединение намерено достичь в ВТО для обеспечения открытой, прозрачной, справедливой, предсказуемой, инклюзивной, равноправной, недискриминационной и основанной на правилах многосторонней торговой системы через участие в 13-й Министерской конференции, в том числе, восстановление полноценно и должным образом функционирующего двухуровневого обязательного механизма урегулирования споров, доступного всем членам и выбор без промедления новых членов Апелляционного органа.

24 Московская декларация XII саммита БРИКС (г. Москва, Россия, 17 ноября 2020 года).

25 Уфимская декларация VII саммита БРИКС (г. Уфа, Россия, 9 июля 2015 года).

В 2017 году этот тезис был конкретизирован: «структуры, управляющие основными Интернет-ресурсами и регулирующие их, необходимо сделать более представительными и инклюзивными»[26].

При этом следует отметить, что полностью консолидированной позиции объединения по этому вопросу нет. Россия и Китай придерживаются подхода, основывающегося на том, что государства являются гарантами обеспечения прав своих граждан и поэтому должны сохранять контроль над национальным информационным пространством и играть ключевую роль в глобальном управлении Интернетом. Однако Индия, Бразилия и ЮАР для защиты своих экономических и политических интересов акцентируют внимание на значении открытого информационного пространства. Они являются сторонниками так называемого «мультистейкхолдерного» подхода и отстаивают равноправные роли всех участников этого процесса, ставя на один уровень общественные организации и правительства без учета их роли и ответственности. Эти концептуальные разногласия ограничивают возможности БРИКС выступать в этом вопросе единым фронтом.

К настоящему моменту концепция действий БРИКС по многосторонней дипломатии настолько оформилась, что с 2018 года в декларациях саммитов появился отдельный раздел, посвященный укреплению и реформированию многосторонней системы управления. В 2021 году министрами иностранных дел было принято Совместное заявление БРИКС по этому направлению деятельности, включающее следующие задачи:

- сделать инструменты глобального управления более инклюзивными для развивающихся и наименее развитых стран, особенно Африки, в глобальных процессах и структурах принятия решений, повысив их приспособленность к современным реалиям;
- использовать в качестве основы всесторонние консультации и сотрудничество при уважении суверенной независимости, равенства, взаимных законных интересов и озабоченностей;
- сделать многосторонние организации более гибкими, эффективными, прозрачными, демократичными, объективными, ориентированными на действия и решения и внушающими доверие;
- использовать инновационные и инклюзивные решения, включая цифровые и технологические инструменты для содействия устойчивому развитию;
- укрепить потенциал как самих государств, так и международных организаций для более эффективного реагирования на новые и возникающие, традиционные и нетрадиционные вызовы, в том числе связанные с кибер-

26 Сямэньская декларация руководителей стран БРИКС IX саммита (г. Сямэнь, Китай, 4 сентября 2017 года).

пространством, инфодемией и распространением недостоверной информации;

- содействовать международному и региональному миру и безопасности, социальному и экономическому развитию [11].

При этом была достигнута договоренность о более активном сотрудничестве и тесной координации БРИКС по данной проблематике в рамках всех профильных многосторонних форумов и международных организаций, включая ООН и G20.

Как уже отмечалось выше, БРИКС решает вопросы глобальной политики через различные механизмы. В 2012 году один из них был создан для координации по вопросам глобального мира и безопасности в Совете безопасности ООН, позднее он был дополнен регулярными встречами постоянных представительств во всех штаб-квартирах организации (в Нью-Йорке, Женеве и Вене)[27]. Детальная проработка инициатив осуществляется в рамках соответствующих форматов сотрудничества.

2.4. Направление «Экономика и финансы», аспект трансформации глобальной финансовой системы

Наиболее решительные действия по изменению глобальной системы управления осуществлены БРИКС именно в финансовой сфере. В 2012 году Индией было предложено создать новые инструменты расчетов центральных банков стран-участниц[28]. В соответствии с Этеквинской декларацией[29] в 2014 году осуществлено создание Нового банка развития[30] для мобилизации ресурсов, предназначенных для осуществления проектов в области инфраструктуры и устойчивого развития в странах БРИКС и других странах с формирующейся рыночной экономикой и развивающихся странах, а также подписан Договор о создании пула условных валютных резервов (Contingent Reserve Arrangement, CRA), создающий страховочный механизм для поддержания финансовой стабильности стран-участниц. В 2015 году в Москве заключено Операционное соглашение между Центральными банками БРИКС, регламентирующее условия взаимной поддержки стран-участниц в чрезвычайных ситуациях с помощью указанного пула[31]. Тем

27 Сямэньская декларация руководителей стран БРИКС, IX саммит БРИКС (г. Сямэнь, Китай, 4 сентября 2017 года).

28 Делийская декларация IV саммита БРИКС (г. Нью-Дели, Индия, 29 марта 2012 года).

29 Этеквинская декларация V саммита БРИКС (г. Дурбан, ЮАР, 27 марта 2013 года).

30 Штаб-квартира Нового банка развития находится в Шанхае, региональный офис в Йоханнесбурге. В 2021 году к банку подключились Бангладеш и Объединенные Арабские Эмираты, в 2023 году – Египет. Потенциальный участник – Уругвай. Источник: Members - New Development Bank, https://www.ndb.int/about-ndb/members/.

31 Информация Банка России от 7 июля 2015 года “О подписании центральными банками стран БРИКС Операционного соглашения в рамках Пула условных валютных резервов”, 24 июля 2015 года, Источник:

самым создана альтернатива получения финансовой помощи без участия западных стран и разрушена монополия Всемирного банка и Международного валютного фонда, где интересы стран БРИКС представлены очень незначительно. Необходимым условием осуществления этих проектов является разработка цифровых платформ и развертывание инфраструктуры для систем оптовых платежей, обмена банковской информацией, заимствований, урегулирования задолженностей и страхования, стандартизации в БРИКС.

В 2018 году на форуме «Валдай» впервые был поднят вопрос о создании единой валюты БРИКС, как тогда виделось — в формате специальных прав заимствования[32]. Введение для расчетов внутри объединения денежной единицы R5[33] позволило бы не только пошатнуть монополию доллара США, но и избежать трудностей взаимных расчетов в условиях западных санкций. Однако в 2023 году после многочисленных обсуждений Индия не дала согласия на развитие этого проекта, что может отражать желание сохранить без изменения экономические отношения с Западом и сдержать своего конкурента — Китай. Но процесс дедолларизации и отказа от Бреттон-Вудской системы уже не остановить, приемлемые решения будут найдены в соответствии с геополитическими условиями и технологическими возможностями стран-участниц.

Для осуществления столь масштабных преобразований укрепляется сотрудничество стран БРИКС в формате встреч министров финансов и управляющих центральных банков, а также представителей налоговых органов «на полях» саммитов G20. В 2017 году подписано Межбанковское соглашение о предоставлении кредитных линий в национальных валютах в рамках Механизма межбанковского сотрудничества БРИКС[34]. В качестве платформы для обмена опытом и знаниями и обеспечения информационной безопасности в финансовом секторе в 2020 году создана Рабочая группа по сотрудничеству в платежной сфере центральных банков стран БРИКС.

Оценивая эту деятельность объединения с точки зрения разработки и внедрения необходимых информационно-коммуникационных инфраструктур и технологий, следует отметить огромный шаг по согласованию научно-технических и методологических подходов к обеспечению информационной безопасности финансовой и банковской сферы. Достигнутые успехи практической кооперации создают новую точку роста экономик БРИКС, что сильно тревожит западные страны, поскольку они лишаются важных рычагов давления.

Информационно-правовой портал Гарант, https://www.garant.ru/products/ipo/prime/doc/71020968/.

32 Special Drawing Rights — условная расчетная единица МВФ, используемая при международных расчетах и предоставлении кредитов.

33 Название образовано от наименования валют БРИКС (real, rouble, rupee, renminbi (юань), rand) и отражает смысл общей «корзины национальных валют».

34 Сямэньская декларация руководителей стран БРИКС, IX саммит БРИКС (2017).

2.5. Направление «Экономика и финансы», аспект развития ИКТ и научно-технологического сотрудничества в передовых технологиях

В условиях формирования многополярного мира и повышения значимости защиты национального суверенитета, все развивающиеся страны остро заинтересованы в повышении своей безопасности путем обеспечения справедливого и всеобъемлющего доступа к цифровым ресурсам, преодоления научного и технологического разрыва, снижения зависимости от западных ИКТ, развития собственных потенциалов, в том числе кадровых, для инклюзивного и устойчивого развития Индустрии 4.0. Именно поэтому экономический и финансовый блок задач БРИКС являются наиболее успешными и обширными.

В рамках направлений деятельности по формированию системы МИБ аспект развития ИКТ и научно-технического сотрудничества в передовых технологиях соответствует блоку задач повышения потенциала по защите национального информационного пространства, в том числе путем обеспечения безопасности ИКТ и их использования во всех отраслях экономики, социальной жизни и при международном сотрудничестве. Развитие и безопасность тесно взаимосвязаны, дополняют друг друга и являются важнейшими условиями обеспечения устойчивого мира. Для этого требуется «основанный на взаимном доверии и выгоде, равенстве и сотрудничестве всеобъемлющий, согласованный и решительный подход к устранению коренных причин конфликтов, в том числе в их политическом, экономическом и социальном аспектах»[35].

Концепция деятельности БРИКС в сфере научно-технологического и промышленного сотрудничества развивается быстрее всего. Если в 2009 году декларировалось «намерение продвигать сотрудничество между нашими странами в области науки и образования, в том числе в целях проведения фундаментальных исследований и разработки передовых технологий», то уже в сентябре 2011 года, в рамках китайского председательства, проведена встреча старших должностных лиц по научно-техническому сотрудничеству. С 2015 года к этому процессу подключены встречи министров образования, науки, технологий и инноваций стран БРИКС, с 2016 года — министров телекоммуникаций.

Среди востребованных направлений в сфере ИКТ можно отметить электронное правительство, цифровые финансовые услуги, электронную торговлю, диверсификацию рынка программного обеспечения и ИКТ-оборудования, умные города, здравоохранение, умную энергетику, Интернет вещей, облачные вычисления, большие данные и их аналитика, нанотехнологии, искусственный интеллект и 5G, а также их инновационное внедрение в целях совершенствования

35 Форталезская декларация VI саммита БРИКС (г. Форталеза, Бразилия, 15 июля 2014 года).

ИКТ-инфраструктуры и повышения ее взаимосвязанности в странах БРИКС. Нет сомнения, что укрепление научно-технологического развития и цифровизация стимулируют рост эффективности производства и уровня образования. Важной отличительной особенностью взаимодействия БРИКС являются совместные разработки, передача технологий и методик их применения, сотрудничество инновационных технопарков и предприятий, мобильность ученых, предпринимателей, специалистов и студентов.

Следует отметить, что согласованных направлений в сфере науки, технологий и инноваций (НТИ) так много, что задействован огромный набор форматов и механизмов, основанных на программах действий, среди которых важную роль играют следующие:

Меморандум о взаимопонимании стран БРИКС по вопросу сотрудничества в сфере НТИ (2015)[36];

Меморандум о взаимопонимании в области совместных исследований по вопросам распределенного реестра и технологий «блокчейн» в контексте развития цифровой экономики (2018);

«Декларация Кампинаса» — совместное заявление по итогам VII Встречи министров науки, технологий и инноваций стран БРИКС (2019)[37];

Декларация министров промышленности стран БРИКС об укреплении сотрудничества в сфере новой промышленной революции (2020);

Декларация министров науки, технологий и инноваций стран БРИКС (2020);

Рамочная программа БРИКС в сфере НТИ (2017)[38];

План действий БРИКС по вопросам развития ИКТ (2017);

Рабочий план стран БРИКС в области НТИ на 2019–2020 годы (2018);

Планы действий БРИКС по инновационному сотрудничеству на период 2017–2020 и 2021–2024 годов;

План действий Партнерства БРИКС по вопросам новой промышленной революции (2018)[39].

Осуществление работы по перечисленным планам потребовало определенных шагов по институционализации деятельности, для чего были созданы:

---

36 Приветствие подписания указанного меморандума содержится в Уфимской декларации VII саммита БРИКС.

37 В декларации особое внимание уделено безопасному развитию и внедрению технологий искусственного интеллекта для использования их потенциала во благо общества и человечества в целом, с особым акцентом на маргинализированные и уязвимые группы населения.

38 Провозглашена Сямэньской декларацией руководителей стран БРИКС (2017). Реализация программы способствовала развитию полномасштабного сотрудничества с привлечением многочисленных финансовых учреждений БРИКС и поддержке свыше сотни проектов в различных областях.

39 План предусматривает реализацию взаимовыгодных инициатив по шести направлениям: координация политики в контексте новой промышленной революции, человеческий капитал, цифровизация, развитие промышленности, инклюзивность, финансовые ресурсы.

Партнерство БРИКС по вопросам новой промышленной революции (ПартНИР/PartNIR) и его Консультативная группа для углубления сотрудничества в области цифровых технологий, индустриализации, инноваций и инвестиций, а также решения вызовов, формируемых четвертой промышленной революцией;

Институт БРИКС по изучению сетей будущего «BRICS Future», являющийся частью Сетевого университета БРИКС (2019). В нем созданы исследовательские группы по пяти наиболее актуальным направлениям: искусственный интеллект, сети связи следующего поколения, интернет-приложения в Индустрии 4.0, воздействие электромагнитного поля, блокчейн [12];

Новая архитектура БРИКС в сфере НТИ (2018) [13], координация которой реализуется через Управляющий комитет НТИ БРИКС. На данный момент она включает: Сеть инновационных исследований iBRICS [14], Платформу энергетических исследований, Сеть БРИКС по передаче технологий (Центры передачи технологий БРИКС), Центр промышленных компетенций стран БРИКС, Инновационный центр ПартНИР в Китае, промышленные и научные парки, технологические бизнес-инкубаторы, стартап-мероприятия БРИКС и сети коммерческих предприятий стран-участниц;

Рабочие группы БРИКС: по развитию предпринимательства и инновационного партнерства в научно-технологической сфере (2016); по ИКТ и высокопроизводительным вычислительным системам (2016); по вопросам сотрудничества в области ИКТ (2020); по вопросам цифровизации; по цифровой экономике.

Огромный объем выполняемой работы свидетельствует о высокой заинтересованности всех стран-участниц БРИКС в реализации совместных проектов по разработке и трансферу передовых ИКТ в интересах подъема национальных экономик в контексте развития четвертой промышленной революции. По оценке зарубежных экспертов, это является ярким подтверждением укрепления технологической кооперации БРИКС, особенно в сфере цифровых технологий [15].

2.6. Направление «Социальное развитие» в контексте использования ИКТ

Как декларирует Международный союз электросвязи, внедрение передовых ИКТ будет способствовать решению 11-и из 17-и целей Программы устойчивого развития ООН, прежде всего в части повышения качества жизни — здравоохранения и образования, решения экологических проблем, борьбы с голодом, бедностью, неравенством. По всем этим направлениям концепция деятельности БРИКС активно развивается с 2011 года, когда было объявлено о «твердой решимости усиливать диалог и сотрудничество в сферах социальной защиты, обеспечения достойными рабочими местами, достижения равенства полов, решения

проблем молодежи и общественного здравоохранения, включая борьбу с ВИЧ/СПИД». В целом, эти действия направлены на искоренение бедности к 2030 году.

В Форталезской декларации заявлено об исключительно важном значении демографического дивиденда стран-участниц, развитие которого имеет много компонентов. В частности, для БРИКС и других развивающихся стран наиболее остро стоит задача обеспечения всеобщего доступа к медицинским услугам и технологиям, сокращение распространения неинфекционных и инфекционных заболеваний (включая вирус Эбола, ВИЧ/СПИД, туберкулез и малярию). Она во многом решается благодаря внедрению услуг телемедицины и цифровых технологий тестирования и диагностики.

Признавая основополагающую роль системы ООН, включая ВОЗ, в координации всеобъемлющих глобальных мер борьбы с пандемией COVID-19, подчеркнут позитивный вклад стран БРИКС в международную безопасность в сфере здравоохранения, а также необходимость принятия как индивидуальных, так и коллективных скоординированных и решительных мер[40]. Для этого проводятся встречи министров здравоохранения и совещания высокого уровня по традиционной медицине, учрежден долгосрочный механизм обменов и сотрудничества в целях содействия взаимному обучению и передачи опыта будущим поколениям[41].

Очень важной задачей для решения проблемы голода является сотрудничество БРИКС в сфере развития сельского хозяйства, сохранения экологии, развития электронной торговли. Созданы механизмы в виде встреч министров экономики, энергетики и окружающей среды стран БРИКС, Платформа экологически безопасных технологий. Развиваются программы умных городов и зеленой энергетики.

Реализация демографического дивиденда стран-участниц БРИКС с высокой долей молодого населения, напрямую зависит от решения проблемы гендерного неравенства и обеспечения широкого спектра программ повышения квалификации, в том числе в сфере профессионально-технической подготовки, а также высшего образования посредством обмена передовыми практиками, знаниями и экспертным опытом, в первую очередь, в сфере использования цифровых технологий для дистанционной и смешанной форм обучения, обеспечения школ подключением к сети Интернет. Это необходимые инструменты предоставления высококачественного и доступного образования[42], и для их развития созданы различные механизмы сотрудничества. Например, разработан План действий БРИКС по сокращению масштабов нищеты посредством развития профессиональных навыков. Приняты Декларация министров труда и занятости стран БРИКС и Ра-

40 Московская декларация XII саммита БРИКС (2020).
41 Сямэньская декларация руководителей стран БРИКС, IX саммит БРИКС (2017).
42 Форталезская декларация VI саммита БРИКС (2014).

мочная программа сотрудничества стран БРИКС в области социального обеспечения. Созданы Сетевой университет БРИКС[43] и группа «ЮНЕСКО-БРИКС» для совместных разработок общих стратегий, проводятся симпозиумы научных центров [16].

Сфера культуры рассматривается в качестве важного направления для обеспечения социально-экономического развития и культурно-гуманитарного сотрудничества. Большое внимание уделяется сохранению культурного многообразия и самоидентичности, искусства и развития межкультурного диалога для сближения народов[44], которые осуществляются с помощью большого количество различных форматов межправительственного и государственно-частного партнерства (в том числе в сфере музеев, библиотек, детских и юношеских театров, кинематографии, породненных городов, Молодежного форума БРИКС)[45], а также путем обеспечения дистанционного доступа к культурным фондам и разработки соответствующего цифрового контента.

***

Результаты анализа действий БРИКС по основным направлениям сотрудничества объединения свидетельствуют о значительном сближении позиций стран-участниц по ключевым вопросам развития и глобального управления. Это отражается не только в насыщенности политической повестки и практического сотрудничества, но и в изменении модальности итоговых документов и заявлений старших должностных лиц.

Радикальное изменение геополитической ситуации требует более четких и решительных формулировок видения места объединения в новом многополярном мироустройстве, конкретизации целей и задач БРИКС.

Странам-участницам для укрепления международных позиций объединения следует прежде всего стремиться к укреплению внутреннего единства, что является залогом усиления своего легитимного влияния на глобальное управление и решение вопросов мира и безопасности. Успешность достижения этой цели, как показывает практика экономического и научно-технического сотрудничества, напрямую зависит от выгод совместных действий для укрепления национального суверенитета.

В этом контексте одной из важных задач является сокращение западной монополии на глобальную ИКТ-инфраструктуру за счет совместного продвижения и финансирования проектов БРИКС по укладке собственных кабельных

43 Согласно Меморандуму о создании Сетевого университета БРИКС от 18 ноября 2015 года информатика и информационная безопасность отнесены к приоритетным областям знаний. Источник: MoU SU BRICS, http://nu-brics.ru/media/uploads/filestorage/documents/MoU_SU_BRICS.pdf.

44 Уфимская декларация VII саммита БРИКС (2015).

45 Форталезская декларация VI саммита БРИКС (2014).

систем, разработке технологически нейтральных цифровых продуктов и услуг, осуществления совместных передовых разработок.

В части проблематики международной информационной безопасности также важно развивать более тесное взаимовыгодное сотрудничество в практической сфере. Например, по таким направлениям, как создание систем мониторинга угроз информационной безопасности и раннего предупреждения, центров обмена опытом и подготовки кадров, объединений киберкоординаторов и технических экспертов.

Следует активнее задействовать форматы государственно-частного партнерства и использовать для этого возможности Совета экспертных центров БРИКС, выступающего в роли платформы для взаимодействия национальных координаторов.

3. Список использованной литературы

1 Ли Цзинчэн Состояние и перспективы международного сотрудничества в рамках «БРИКС+», Управленческое консультирование № 3, 2020 С.110-120, https://spb.ranepa.ru/wp-content/uploads/2021/01/ac_03_2020.pdf.

2 Выступление В.В. Путина на встрече лидеров Бразилии, России, Индии, Китая и ЮАР в расширенном составе, 15 июля 2014 года, http://kremlin.ru/events/president/transcripts/46229.

3 О. Сухарева БРИКС в формате «аутрич» // Ритм Евразии, 4 августа 2018 года, https://www.ritmeurasia.org/news--2018-08-04--briks-v-formate-autrich-37839.

4 Неофициальные переводы итоговых документов встреч лидеров стран-участниц БРИКС // Объединенный центр делового сотрудничества БРИКС, https://ocds-brics.org/sammity-i-dokumenty

5 Антитеррористическая стратегия БРИКС // BRICS Russia 2020, https://brics-russia2020.ru/images/114/81/1148163.pdf.

6 BRICS main cooperation areas // BRICS Brasil 2019, https://web.archive.org/web/20190425190637/http://brics2019.itamaraty.gov.br/en/about-brics/main-areas-of-cooperation.

7 Резолюция Комиссии по предупреждению преступности и уголовному правосудию Экономического и социального совета ООН 22/7 «Укрепление международного сотрудничества в целях борьбы с киберпреступностью», https://russianembassyza.mid.ru/web/russianembassyza-ru/briks/-/asset_publisher/ZkbNLayaLJm3/content/antiterroristiceskaa-strategia-briks?inheritRedirect=false.

8 Chart of signatures and ratifications of Treaty 185, 24.07.2023, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185.

9 Совместное заявление министров иностранных дел стран БРИКС по укреплению и реформированию многосторонней системы от 1 июня 2021 года // МИД России, https://www.mid.ru/upload/archive/e698c4533972db9898a2c895349b7483.pdf.

10 Преобразование нашего мира: Повестка дня в области устойчивого развития на период до 2030 года, Резолюция Генеральной Ассамблеи ООН A/RES/70/1 от 25 сентября 2015 года, http://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_70_1_E.pdf.

11 Совместное заявление министров иностранных дел стран БРИКС по укреплению и реформированию многосторонней системы от 1 июня 2021 года // МИД России,| https://www.mid.ru/upload/archive/e698c4533972db9898a2c895349b7483.pdf.

12 Work Plan for BRICS Institute of Future Networks, Appendix to the Declaration of the 8th BRICS Communications Ministers Meeting (6 July 2022, People's Republic of China), https://bifn.org/upload/files/2023/7/AGREED_Declaration_of_the_8th_BRICS_Communications_Ministers_Meeting.pdf.

13 New BRICS Science, Technology and Innovation Architecture concept (2019), https://brics2021.gov.in/BRICSDocuments/2019/A%20New%20BRICS%20STI%20Architecture%20of%20BRICS%20Science,%20Technology%20and%20Innovation%20(STI).pdf.

14 Enabling Framework for the Innovation BRICS Network ("iBRICS NETWORK"), http://www.brics.utoronto.ca/docs/190920-Enabling_Framework_iBRICS_Network__Final.pdf.

15 CyberBRICS: Cybersecurity Regulations in the BRICS Countries, 2020 https://cyberbrics.info/wp-content/uploads/2020/11/CyberBRICS-Book-FINAL-author-version.pdf.

16 STI OVERVIEW. Five-Year Anniversary of Cooperation in Science, Technology and Innovation under the Memorandum of Understanding // BRICS Russia, 2020, https://mniop.ru/wp-content/uploads/2019/11/BRICS-STI_2000.pdf.

3. Особенности политики государств-участников БРИКС в сфере развития ИКТ, обеспечения национальной и международной информационной безопасности

Арабская Республика Египет

Официальное название: Арабская Республика Египет
Столица: Каир
Официальный язык: арабский

Территория: Площадь Египта является тридцатой в мире и составляет 1 001 450 км². Египет — трансконтинентальное государство, расположенное в Северной Африке и на Ближнем Востоке (Синайский полуостров). Граничит на западе с Ливией, на юге — с Суданом, на востоке — с Палестинской автономией, Израилем, имеет также морскую границу с Саудовской Аравией и Иорданией. Омывается на севере Средиземным морем, на востоке — Красным морем. Египту принадлежит один из самых крупных искусственно сооружённых каналов — Суэцкий канал, который соединяет Средиземное и Красное моря. По территории Египта с юга на север протекает одна из двух величайших по протяжённости рек в мире — Нил.

Население: На 1 марта 2024 года численность населения (постоянных жителей) Египта составляет 100 704 000 человек, что является 14 показателем в мире [1].

Государственно-административное устройство: Египет — республика. Административно страна разделена на 27 мухафаз, которые делятся на административные центры или районы (марказы) и города. Глава государства — президент, который одновременно является и главнокомандующим вооружёнными силами. Глава правительства — премьер-министр. Высший законодательный орган — двухпалатное Национальное собрание. Нижняя палата парламента, Народная ассамблея (Меджлис эш-Шаъб), состоит из 518 депутатов, 508 из которых избираются по мажоритарной системе, а 10 назначаются президентом. В Народной ассамблее имеются квоты для рабочих и крестьян, а также для женщин.

Экономика: Показатели валового внутреннего продукта по паритету покупательной способности (ВВП по ППС в текущих ценах) на 2022 год: 1675 млрд долл. США (19 показатель в мире). На душу населения: 15 091 долл. США (96 показатель в мире). Показатели валового внутреннего продукта (по номинальному значению, в текущих ценах) на 2022 год: 477 млрд долл. США (31 показатель в мире). На душу населения: 4 295 долл. США (115 показатель в мире) [2].

Дипломатические отношения с Россией были установлены 26 августа 1943 года.

1. Уровень развития информатизации страны и информационно-коммуникационной инфраструктуры, системы обеспечения информационной безопасности

По данным МСЭ [3], в 2022 году 72,2% населения Египта пользовались сетью Интернет, что было выше общемирового уровня в 66,3%, и почти вдвое превзошло показатель по Африке — 39,7%.

Египет является одним из самых развитых и быстро растущих рынков интернет-услуг с точки зрения числа пользователей, полосы пропускания международного трафика и спектра предлагаемых услуг. Благодаря наличию четырех конкурирующих операторов (*Orange*, *Vodafone Egypt*, *Etisalat Misr*, *Telecom Egypt*), цены на услуги фиксированной и подвижной широкополосной связи в этой стране являются одними из самых низких в регионе арабских государств [4].

Египет является крупным рынком подвижной связи с высоким уровнем проникновения. В 2007 году он одним из первых в регионе внедрил сеть 3G. В августе 2016 года оператор фиксированной связи *Telecom Egypt* (*TE*) получил от Национального органа регулирования электросвязи (*NTRA*) первую лицензию на единые услуги, что позволило ему предложить услуги в сетях LTE (4G). В середине 2016 года *NTRA* выдал четыре лицензии на LTE, и эта услуга официально предлагается с 2017 года. Ожидается, что широкое распространение этой технологии приведет принесет пользу гражданам и максимально увеличит информационные потоки, обеспечивая высокий уровень использования данных и информации, и, следовательно, переход к цифровой экономике. По стоимости 1 Гб данных в 2022 году Египет занимал 62 место из 237 и третье место из 7 в регионе Северной Африки [5]. В то же время, согласно Индексу сетевой готовности (*NRI*) 2023 года, страна занимает лишь 81 место из 134 [6], причем в своей группе стран с уровнем дохода ниже среднего и среди арабских государств Египет он занимает 9 место. В Египте находятся пять центров обработки данных, расположенных в Каире и Александрии, которыми управляют три организации. *Telecom Egypt* имеет наибольшее присутствие с тремя объектами, по одному у *GPX Global Systems* и *CityNet Telecom*.

Знания, инновации и научные исследования — одна из основ государственной программы Египта *Vision 2030*. В ней подчеркивается важность сектора ИКТ в качестве ключевого фактора будущего устойчивого экономического роста. Кроме того, она призвана способствовать развитию индустрии ИКТ как на региональном, так и на международном уровне. В 2016/2017 годах сектор ИКТ достиг 3,2% ВВП и демонстрировал самые высокие темпы роста по сравнению с другими отраслями экономики. В 2022 году рынок ИКТ Египта оценивался в 26,66 млрд долл. США, а с учетом совокупного годового темпа

роста на 6,23% ожидается, что к 2027 году объём рынка достигнет 36,06 млрд долл. США [7].

В рамках программы *Vision 2030* также идет развитие электронного правительства. По состоянию на 2022 год Египет занимал 103 место в Обзоре развития электронного правительства ООН (по сравнению со 111 местом в 2020 году) с показателем 0,59 по индексу развития электронного правительства (*E-Government Development Index*, *EGDI*). Это ставит Египет на 6 место среди стран Африки с самыми высокими значениями индекса *EGDI*. Согласно отчету Всемирного банка о зрелости технологий государственного управления за 2022 год, Египет перешел из группы B в группу A (группу лидеров) [8].

Обеспечению национальной информационной безопасности придается большое внимание, государство предпринимает широкий комплекс мер, благодаря чему Египет имеет очень высокий индекс кибербезопасности (по данным МСЭ за 2021 год 95,48 из 100) и занимает достаточно высокие позиции как в глобальном рейтинге (23 место), так и в рейтинге среди государств ЛАГ, входя в первую четверку по этому показателю [9]. Согласно прогнозам, рынок кибербезопасности Египта будет расти в среднем на 10,7% до 2026 года [10]. При этом, согласно Отчету Интерпола об оценке киберугроз в Африке за 2021 год [11], в 2020 году Египет стал целью почти 35% атак с использованием программ-вымогателей в регионе.

За последние несколько лет Египту удалось добиться большого прогресса в передовых технологиях. Индекс «Готовность правительства к искусственному интеллекту» показал, что в 2022 году Египет занимал 65 позицию в общем рейтинге 181 стран, в то время как в аналогичном рейтинге 2019 года он занял 111 место из 194 стран [12]. При этом сам индекс развития искусственного интеллекта (ИИ) Египта (49,42) в 2022 году выше среднемирового (44,61) [12]. В 2021 году Министр связи и информационных технологий и председатель Национального совета по искусственному интеллекту (*National Council for Artificial Intelligence, NCAI*) Амр Талаат объявил о создании национальной платформы ИИ. Она работает под эгидой *NCAI* и является официальным порталом Египта в области искусственного интеллекта. На ней собрана вся информация о существующих проектах, программах по наращиванию человеческого потенциала и подготовке сотрудников, предоставляемых Министерством связи и информационных технологий в сотрудничестве с различными ведомствами. Среди них — программы по повышению осведомленности, а также специальные программы для студентов и выпускников университетов, а также специалистов, вплоть до руководителей в частном и государственном секторе.

2. О стратегическом планировании в области цифровизации и информационной безопасности

2.1. Национальная стратегия в области ИКТ на 2012–2017 годы

В основе этой Стратегии, названной «На пути к цифровому обществу и основанной на знаниях экономике» (2012) [13], заложена идея поддержки египетского сектора ИКТ, который играет активную роль в достижении политических, социальных и экономических целей демократических преобразований в Египте. Миссия Стратегии заключалась в развитии демократического общества, основанного на знаниях, которое поддерживает сильную египетскую экономику, опирается на равноправный доступ к информационным и коммуникационным услугам, гарантирует цифровые права граждан и развитие национальной промышленности, основанной на человеческих талантах и творчестве.

Реализация Стратегии осуществлялась по ряду стратегических направлений: международное сотрудничество, ИКТ-инновации и предпринимательство, развитие отрасли ИКТ, цифровое гражданство, развитие человеческого потенциала, государственная инфраструктура ИКТ и цифровые услуги, инфраструктура телекоммуникаций и почтовой службы.

Стратегия включала в себя более 40 программ и 120 проектов, в том числе зеленые ИКТ, цифровой контент на арабском языке, облачные вычисления, управление цифровой идентификацией, электронная коммерция, мобильные приложения для разработки, производство планшетных компьютеров для образования, программное обеспечение с открытым исходным кодом и улучшение положения людей с ограниченными возможностями.

Стратегия также предполагала внесение поправок в ряд законов. Например, Закон о телекоммуникациях 2003 года требовалось привести в соответствие с демократическим переходом Египта, чтобы способствовать политической открытости и защите свободы выражения мнений. При этом в Стратегии была отмечена необходимость обеспечить баланс между свободой и национальной безопасностью, а информация, которая может нанести ущерб национальной безопасности или подвергнуть риску отношения с другими странами, является неприемлемой. Кроме этого, Стратегией предполагалось, что будет подготовлен и принят ряд новых законов и постановлений, охватывающих такие области, как свобода информации, кибербезопасность и электронная коммерция.

2.2. Стратегия электронной торговли (2017)

В декабре 2017 года Министерство связи и информационных технологий и Конференция Организации Объединенных Наций по торговле и развитию (ЮН-

КТАД) опубликовали Национальную стратегию электронной торговли Египта (Стратегия электронной торговли [14]). Ее главной стратегической целью стало «использование электронной торговли для увеличения благосостояния нации посредством экономического роста, конкурентоспособности экспорта, повышения производственного потенциала и создания рабочих мест». Документ включает шесть рекомендаций, шесть «мегапроектов» и дополнен планом действий. Египет поставил цель, чтобы к 2020 году электронная торговля составляла 2,35% ВВП. По некоторым данным, в 2019/2020 финансовом году объем торговли составил 4,8 млрд долл. США, или около 1,3% ВВП [15]. Шесть рекомендаций были направлены на: расширение возможностей ведения бизнеса посредством электронной торговли, использование электронной торговли для стимулирования охвата неформального сектора, использование электронной торговли для освоения возможностей ИКТ-сектора, стимулирование роста логистического сектора, ускорение роста сектора электронных платежей, создание потребительского рынка для электронной торговли.

Стратегией были определены следующие мегапроекты:

- создание центра содействия электронной торговле и национального электронного рынка для бизнеса;
- запуск инициативы по развитию электронной торговли в сельской местности;
- расширение прав и возможностей в сфере электронной торговли для молодежи и малых и средних предприятий (МСП);
- активация и создание дополнительных способов оплаты в электронной торговле;
- разработка и продвижение продуктов сектора ИТ-услуг Египта.

В документе также был рассмотрен вопрос управления реализацией Стратегии, в частности речь шла о новом министерском комитете по электронной торговле, возглавляемом министром связи и информационных технологий, и в который войдут главы министерства торговли и промышленности, министерства финансов, а также председатели Федерации торгово-промышленных палат.

2.3. Национальная стратегия искусственного интеллекта (2021)

Целью документа [16] является реализация следующего видения:

- использовать технологии ИИ для достижения целей устойчивого развития Египта на благо всех египтян;
- играть ключевую роль в содействии региональному сотрудничеству в африканском и арабском регионах и сделать Египет активным международным игроком в области ИИ.

Для достижения цели предполагается создание национальной индустрии ИИ, включая развитие навыков, технологий, экосистемы, инфраструктуры и механизмов управления для обеспечения устойчивости и конкурентоспособности.

Для реализации вышеизложенного видения и миссии Египет будет:

- внедрять технологии ИИ в государственные операции, чтобы сделать их более эффективными и прозрачными;
- использовать ИИ в ключевых секторах развития для решения местных и региональных проблем в поддержку стратегии устойчивого развития Египта и для достижения ЦУР ООН;
- поощрять инвестиции в исследования и инновации в области ИИ посредством государственно-частного партнерства и инициатив с университетами, исследовательскими центрами и частным сектором;
- развиваться как региональный центр образования и талантов в области ИИ, удовлетворяющий потребностям местного, регионального и международного рынка;
- оказывать поддержку программам непрерывного обучения и переподготовки, способствующим развитию рабочей силы и устойчивому трудоустройству;
- создавать процветающую экосистему ИИ, поддерживая местное предпринимательство и инновационные усилия, а также создавая академическую научную среду;
- продвигать ориентированный на человека подход к ИИ, в котором благополучие людей является приоритетом, и способствовать диалогу с участием многих заинтересованных сторон по вопросам использования ответственного ИИ на благо общества, а также для информационного сопровождения соответствующих политических дискуссий;
- использовать ИИ как инструмент включения маргинализированных слоев населения не только в программы социальной защиты, но и в инициативы, способствующие человеческому прогрессу и саморазвитию;
- содействовать сотрудничеству на арабском и африканском уровнях, работая над объединением арабских и африканских голосов и усилий в области ИИ на благо всех;
- активно участвовать в глобальных усилиях и играть активную роль на различных международных форумах по ИИ, особенно по темам этики ИИ, будущего рынка труда, ответственного ИИ и социального-экономического воздействия ИИ.

Стратегия опирается на четыре приоритетные задачи:

- ИИ для правительства: быстрое внедрение технологий ИИ посредством автоматизации государственных процессов и внедрения ИИ в цикл принятия решений для повышения эффективности и прозрачности;

- ИИ для развития: применение ИИ в различных секторах экономики на основе поэтапного подхода с целью повышения эффективности, достижения более высоких темпов экономического роста и повышения конкурентоспособности;
- наращивание потенциала: подготовка населения Египта к эпохе ИИ — от общей осведомленности всех уровней образования и профессиональной подготовки по техническим и иным дисциплинам;
- международная деятельность: принятие ключевой роли в развитии сотрудничества на региональном и международном уровнях, отстаивая соответствующие инициативы, представляя позиции африканских и арабских стран и активно участвуя в дискуссиях, связанных с ИИ.

2.4. Видение Египта до 2030 года (2022)

Первая версия Стратегии устойчивого развития: «Видение Египта до 2030 года» [17] была запущена в 2016 году, она легла в основу процесса комплексного развития с учетом национальных приоритетов и амбиций, направленного на достижение достойной жизни египетского народа, в том числе через максимальное использование всех возможностей государства. Эта программа стала ориентиром для достижения устойчивого развития в экономическом, социальном и экологическом измерениях, уделяя особое внимание концепциям инклюзивного и устойчивого роста и сбалансированного местного развития. Она направлена на то, чтобы к 2030 году Египет стал конкурентоспособной, сбалансированной и диверсифицированной экономикой, основанной на инновациях и знаниях, а также справедливости, социальной интеграции и участии, с экосистемой, направленной на достижение устойчивого развития и повышения качества жизни египтян без ущерба для будущих поколений.

Развитие национальной и международной обстановки привело к тому, что в 2022 году Министерство планирования и экономического развития вместе с представителями частного сектора и гражданского общества представило обновленную версию документа. В нем учтены результаты первого этапа национальной программы экономического развития и социальных реформ, а также раскрыты особенности второго этапа, который отдает приоритет высокопроизводительным секторам, фокусируясь на структурной и отраслевой реформах.

Определено семь инструментов обеспечения устойчивого развития: финансирование, технологический прогресс и инновации, содействие цифровой трансформации, производство и предоставление данных, создание благоприятной законодательной и институциональной среды, поддержка системы культурных ценностей, контроль роста населения.

Видение Египта до 2030 года основано на шести стратегических целях, отражающих ориентацию государства на дальнейшее достижение устойчивого развития:

1) «слагаемые достойной жизни», в том числе искоренение бедности, обеспечение продовольствием, предоставление высококачественных медицинских услуг, улучшение системы образования и обеспечение достойного жилья, обогащение культурной жизни, а также спорт для граждан Египта;

2) «социальная справедливость и равенство» заключаются в сокращении неравенства между социальными группами, особенно наиболее нуждающимися и уязвимыми, а также содействие преодолению разрывов в развитии между географическими регионами;

3) «интегрированная и устойчивая экосистема» предполагает реализацию такой модели глобального развития, в основе которой лежит концепция сохранения природных ресурсов и управление ими комплексным и устойчивым образом. Эта цель также направлена на стимулирование таких инновационных экономических моделей, как экономика замкнутого цикла и зеленая экономика;

4) «диверсифицированная, конкурентоспособная, основанная на знаниях экономика» призвана повысить способность создавать доход, управлять ресурсами и создавать рабочие места в различных областях;

5) «развитая инфраструктура» отражает важность предоставления основных и сопутствующих услуг, таких как энергия, электричество, водоснабжение и канализация, а также обеспечения безопасных и устойчивых транспортных систем, развития системы связи и передачи информации для создания привлекательной инвестиционной среды;

6) «управление и партнерство» воплощает комплексный план институционального развития в условиях верховенства закона и участия всех сторон в процессе принятия решений на национальном и местном уровнях в соответствии с законодательными и институциональными основами.

2.5. Национальная стратегия кибербезопасности на 2022–2026 годы

Эта Стратегия [18] пришла на смену Национальной стратегии кибербезопасности 2017–2021 (принятой в 2018 году) [19] и является частью усилий государства по поддержке национальной безопасности, развитию египетского общества, а также обнаружению и преодолению кибератак и проблем в цифровом обществе. Предполагается, что она поможет обеспечить комплексное социально-экономическое развитие, защитить национальные интересы и оградить граждан от рисков в киберпространстве. В Стратегии выделены следующие источники киберугроз: киберпреступность, кибервойны, терроризм, инсайдерские и

угрозы, исходящие от хакеров-дилетантов. Киберпреступники несут основную ответственность за разработку и использование вредоносных программ с целью получения финансовой выгоды. Кибервойны осуществляются государствами и спонсируемыми государствами группами, с целью проникновения в критически важные сектора других стран для осуществления шпионажа, получения политических и стратегических выгод или с целью диверсии. В ближайшие несколько лет кибервозможности террористов возрастут и они смогут нанести серьезный ущерб. С ростом использования информационных технологий внутри организаций увеличивается вероятность возникновения преднамеренных или непреднамеренных рисков со стороны сотрудников, уполномоченных использовать информационные системы. Они могут представлять угрозу для организаций, крадя конфиденциальные данные, что приводит к серьезным финансовым потерям или ставит под угрозу репутацию организации. Также есть категория хакеров-дилетантов, которые, тем не менее, используют программы, обладающие высокими разрушительными возможностями.

Оценку угроз можно использовать для создания национальной индустрии информационной безопасности, в которой будет работать множество молодых людей, способных разрабатывать и использовать специализированное программное обеспечение, а также распространять информацию о кибербезопасности в обществе в целом и среди тех, кто работает в этой сфере. При этом соответствующие научные исследования все еще находятся на ранних стадиях, что предполагает создание инфраструктуры для научных исследований в этой области, а также интеграцию программ информационной безопасности в учебные программы разных уровней образования. Еще одной проблемой является отсутствие обязательной структуры, координирующей работу государственных органов и владельцев/операторов критической инфраструктуры.

Программы национальной стратегии охватывают шесть основных областей: создание всеобъемлющей законодательной базы, изменение культуры общества в отношении кибербезопасности, укрепление национальных партнерств, создание сильной и устойчивой киберзащиты, поощрение научных исследований и содействие инновациям и росту, укрепление международного сотрудничества.

Развитие законодательства в Египте осуществляется по двум основным направлениям: криминализация деяний посредством Закона о преступлениях в сфере информационных технологий 2018 года и установки стандартов и мер контроля защиты информации и её содержания, а также информационных систем в соответствии с Законом о защите персональных данных 2020 года. Одновременно ведется работа над Законом о кибербезопасности, который определит обязанности, полномочия и задачи Национального центра кибербезопасности, аналогичного Центру защиты персональных данных, с целью повышения эффек-

тивности кибербезопасности в учреждениях, владеющих/управляющих критической инфраструктурой.

Обеспечение кибербезопасности является обязанностью всех учреждений, владеющих или управляющих информационной инфраструктурой. Они должны знать о рисках, связанных с их информационной структурой, и способах ее защиты. В рамках реализации Стратегии государственные учреждения, эксперты по кибербезопасности, образовательные учреждения и компании, работающие в этом секторе, должны сотрудничать между собой и участвовать в разработке и контроле за реализацией инициатив в области кибербезопасности. Программы по укреплению национального партнерства включают инициативы по разработке структуры управления кибербезопасностью, созданию консультативного комитета отрасли кибербезопасности, заключению двусторонних соглашений о сотрудничестве с владельцами/операторами критической инфраструктуры, созданию фонда развития индустрии кибербезопасности и базы данных кибербезопасности.

В развитие структуры управления кибербезопасностью Стратегией предусмотрено создание Национального управления кибербезопасности и подчиненных ему отраслевых, региональных и специализированных центров. Управление подотчетно премьер-министру и занимается организацией кибербезопасности и надзором за исполнением законов и обязательств. Закон о кибербезопасности определяет полномочия и обязанности Управления и всех связанных с ним отраслевых центров. Секторальные, территориальные и специализированные центры будут действовать под его техническим и административным надзором.

Роль программ международного сотрудничества включает разработку стандартов поведения государств до, во время и после киберинцидентов, применение международного права и управление Интернетом. Программа по расширению международного сотрудничества включает в себя разработку соответствующей стратегии, которая направлена на установление принципов и вектора египетской кибердипломатии на арабском, африканском и глобальном уровнях. Министерство иностранных дел Египта является органом, ответственным за это направление.

Программы по изменению культуры общества в отношении кибербезопасности включают в себя разработку и развитие программ повышения осведомленности для рядовых пользователей Интернета, пользователей в компаниях, государственных органах и учреждениях, а также участие в разработке специальных учебных программ для обучения студентов на разных уровнях образования по вопросам кибербезопасности. Кампании по повышению осведомленности нацелены на все слои общества, частный и государственный секторы, малый бизнес, пожилых людей, родителей, учителей и др.

2.6. Египетская хартия ответственного искусственного интеллекта (2023)

Этот документ [20] является первой попыткой сформулировать интерпретацию Египтом различных руководящих принципов этического и ответственного ИИ, адаптированных к местному контексту и в сочетании с практическими идеями, которые помогут обеспечить ответственную разработку, развертывание, управление и использование систем ИИ в стране. Он основан на руководящих принципах, разработанных ОЭСР, ЮНЕСКО, ВОЗ, IEEE, ЕС, а также ведущими странами, такими как Сингапур, Великобритания, США, Австралия.

В этом отношении этот документ служит двум целям:

- обеспечить «плавный старт», чтобы все заинтересованные стороны были осведомлены об этических аспектах ИИ и включали их в свои планы внедрения ИИ;
- сигнализировать о готовности Египта следовать ответственным практикам в области ИИ, что также поможет донести потребности и приоритеты Египта до иностранных разработчиков ИИ, желающих разрабатывать или продавать свою продукцию в стране.

Ожидается, что Хартия будет пересматриваться ежегодно, чтобы обеспечить ее постоянную актуальность и актуальность. Также ожидается, что перед каждым пересмотром будут проводиться общественные консультации для учета мнений всех заинтересованных сторон. Документ содержит две части — общие руководящие принципы, которые представляют собой всеобъемлющие правила, применимые ко всем членам экосистемы, и рекомендации по внедрению.

3. Нормативно-правовая база в сфере развития ИКТ, обеспечения информационной безопасности

По новой методике МСЭ оценки зрелости правового регулирования цифровизации, нормативно-правовая система Египта признана развитой, т.е. использующей научный подход к регулированию и управлению[1].

Основным законом страны является Конституция Арабской Республики Египет 2014 года, которая заменила собой документ 2012 года, принятый при президентстве Мухаммеда Мурси. Согласно Конституции, политические партии

1 В методике «G5 Benchmark» оцениваются 4 параметра: межотраслевое управление на национальном уровне, принципы разработки политик, Инструментарий цифрового развития (кибербезопасность, защита данных, телекоммуникации в чрезвычайных ситуациях и совместное использование межотраслевой инфраструктуры), повестка дня в области цифровой экономики (инновационная система, цифровая трансформация, участие в международных и региональных интеграционных инициативах). В 2023 году Египет получил оценку 69,29 (значения от 60 до 80 баллов соответствуют уровню «развитый»).

не могут основываться на «религии, расе, поле или географическом положении». Военные сохраняют за собой возможность назначать министра обороны страны на следующие 8 лет. Примечательно, что в Статье 31 зафиксировано: «Безопасность киберпространства является неотъемлемой частью экономической системы и национальной безопасности. Государство должно принять необходимые меры для ее поддержания, в соответствии и порядком, установленным законом».

3.1. Закон о телекоммуникациях (2003)

Одной из основных целей Закона [21] стало создание Национального органа регулирования электросвязи (*National Telecommunication Regulatory Authority, NTRA*). Его деятельность направлена на регулирование телекоммуникационных услуг, а также их совершенствование и развертывание в соответствии с самыми передовыми технологическими средствами, по наиболее подходящим ценам. *NTRA* также должен поощрять национальные и международные инвестиции в эту сферу в рамках правил свободной конкуренции, особенно в следующих областях:

- гарантированное предоставление телекоммуникационных услуг по всей стране, включая особые экономические зоны и регионы развития, городские, сельские и отдаленные районы;
- защита национальной безопасности и высших интересов государства;
- обеспечение оптимального использования радиочастотного спектра и повышение его прибыльности в соответствии с положениями настоящего Закона;
- гарантированное соблюдение действующих международных соглашений и резолюций международных и региональных организаций в области электросвязи, одобренных государством;
- мониторинг реализации программ технико-экономической эффективности различных услуг связи.

Для достижения своих целей *NTRA* имеет право предпринимать все необходимые действия, в частности: 1. Принимать стратегии, программы, правила и методы управления. 2. Учитывать достижения технического и технологического прогресса в области телекоммуникаций в соответствии со стандартами здравоохранения и окружающей среды. 3. Осуществлять подготовку и публикацию отчета с указанием услуг электросвязи, названий операторов, поставщиков услуг и общих правил выдачи лицензий и разрешений. 4. Определять общие правила, обязательные для исполнения операторами и поставщиками телекоммуникационных услуг. 5. Определять стандарты и правила услуг связи и устанавливать обязательства операторов и провайдеров по таким услугам в соответствии с положениями настоящего Закона. 6. Устанавливать правила, гарантирующие защиту пользователей, конфиденциальность телекоммуникаций, предоставление са-

мых современных услуг по наиболее подходящим ценам, обеспечение высокого качества этих услуг и создание системы приема, расследования жалоб пользователей и последующей связи с поставщиками услуг. 7. Осуществлять контроль за организациями, имеющими право на получение международных сертификатов в области связи по согласованию с Национальным институтом связи. 8. Устанавливать необходимые правила выдачи разрешений на оборудование. 9. Обеспечить создание Национального плана нумерации электросвязи и контроль его исполнения.

Согласно Закону, с учетом охраняемой законом неприкосновенности частной жизни граждан, каждый оператор и провайдер обязан за свой счет обеспечить в пределах своей ответсвенности все технические возможности, включая оборудование, системы, программное обеспечение и средства связи, позволяющие Вооруженным Силам и органам национальной безопасности осуществлять свои регламентированные полномочия. Кроме того, поставщики и операторы телекоммуникационных услуг и их маркетинговые агенты имеют право собирать точную информацию и данные о деятельности пользователей и различных организаций на территории государства.

3.2. Закон о борьбе с терроризмом (2018)

Закон о борьбе с терроризмом [22] криминализует ряд деяний, связанных с использованием ИКТ в террористических целях. Согласно Статье 29, создание или использование веб-сайта или других средств массовой информации с целью продвижения идей или убеждений, призывающих к совершению террористических актов или трансляции материалов, предназначенных для введения в заблуждение органов безопасности, влияния на ход правосудия в случае любого террористического преступления или обмена сообщениями между террористическими группами или их членами либо обмена информацией, касающейся действий или передвижения террористов или террористических групп внутри страны и за рубежом, наказываются лишением свободы с принудительными работами на срок не менее пяти лет. Лицо, которое неправомерно или незаконно осуществляет доступ к веб-сайтам, связанным с каким-либо государственным органом, с целью получения, доступа, изменения, удаления, уничтожения или фальсификации данных или информации, содержащихся на них, с целью совершения вышеупомянутых преступлений или их подготовки, наказываются лишением свободы с принудительными работами на срок не менее десяти лет.

Согласно Статье 46, прокурор или соответствующий орган по расследованию преступления, связанного с террористической деятельностью, может санкционировать мотивированный ордер на срок, не превышающий тридцати дней,

для наблюдения и записи разговоров и сообщений, полученных по проводным, беспроводным и другим телекоммуникационным каналам, а также конфискации обычной или электронной корреспонденции, писем, публикаций, посылок и телеграмм всех видов.

3.3. Закон о регулировании прессы и СМИ (2016–2018)

В соответствии с положениями Закона [23], печатным изданиям, средствам массовой информации или веб-сайтам запрещается публиковать или транслировать контент, который: нарушает Конституцию Египта, профессиональную этику, а также общественный порядок или мораль, содержит призывы к нарушению закона, провоцирует дискриминацию, насилие, расизм, ненависть или экстремизм.

Для контроля соблюдения этих требований создается новый орган — Верховный совет по регулированию СМИ (*Supreme Council for Media Regulation*). Закон также создает правовую основу, которая позволяет Верховному совету предотвратить в интересах национальной безопасности выпуск или распространение публикации из-за границы.

Закон запрещает прессе, средствам массовой информации и веб-сайтам публиковать или транслировать ложные новости и допускает цензуру контента, который нарушает этот запрет. При этом, персональные веб-сайты, блоги и аккаунты в социальных сетях с 5000 и более подписчиками отнесены к средствам массовой информации. В дополнение к этим ограничениям на медиаконтент Закон развивает систему регулирования, которая подвергает средства массовой информации ряду требований лицензирования и надзора, включая строгие требования к процессу получения разрешений, запрет журналистам и представителям средств массовой информации иметь возможность собирать пожертвования на свою работу, а также положение, обязывающее СМИ хранить любой контент в течение как минимум 12 месяцев, в течение которых Верховный совет будет иметь возможность доступа к нему.

3.4. Указ Премьер-министра №994 от 2017 года

Указ [24], который регламентирует работу Высшего совета кибербезопасности Египта, постановляет, что государственные органы всех уровней и компании государственного сектора в рамках реализации Национальной стратегии кибербезопасности должны выполнять резолюции и рекомендации Арабского регионального центра кибербезопасности (*ARCC*), касающиеся защиты их критически важной инфраструктуры связи и информационных технологий, и принимать все необходимые технические и административные меры для борьбы с киберугро-

зами и компьютерными атаками. Министр связи и информационных технологий должен разработать и определить правила и процедуры для обеспечения безопасности критической информационной инфраструктуры государственного сектора, а также следить за выполнением резолюций и рекомендаций Высшего совета кибербезопасности и исполнение положений настоящего Указа.

3.5. Закон о преступлениях в сфере кибербезопасности и информационных технологий (2018)

До своего принятия в 2018 году, проект Закона [25] неоднократно пересматривался. В свете ратифицированных международных, региональных и двусторонних соглашений или в соответствии с принципом взаимности египетские власти должны сотрудничать со своими иностранными коллегами посредством обмена информацией для предотвращения преступлений, связанных с информационными технологиями, а также для оказания помощи в расследовании и отслеживании исполнителей этих преступлений. Национальный центр реагирования на компьютерные и сетевые чрезвычайные ситуации является в этом отношении аккредитованным техническим центром. При условии соблюдения конфиденциальности, гарантированной Конституцией, поставщики услуг должны по запросу органов национальной безопасности и в соответствии с их потребностями предоставлять все технические возможности, которые позволяют таким органам осуществлять свои полномочия в соответствии с Законом.

Осуществляющий расследование орган может, в зависимости от обстоятельств, выдать обоснованное разрешение на:

- контроль, сбор или изъятие данных и информации или информационных систем или их отслеживание в любом месте, системе, программе, электронной поддержке или компьютере;
- поиск, проверку, получение доступа к компьютерным программам, базам данных и устройствам и информационным системам.

Он также может обязать поставщика услуг предоставить данные или информацию, а также данные пользователей.

Если имеются доказательства того, что веб-сайт содержит контент, который является незаконным, ставит под угрозу национальную безопасность или экономику, соответствующий следственный орган может через суд заблокировать его, если имеется соответсвующая техническая возможность. В случае, если ожидается неминуемый ущерб, органы дознания и правоохранительные органы могут обратиться в Национальный орган регулирования электросвязи, который должен немедленно уведомить поставщика услуг о временной блокировке веб-сайта, контента или ссылок. При любых обстоятельствах признание недействительным

решения о блокировке осуществляется путем вынесения постановления об отказе в возбуждении уголовного дела или вынесения окончательного оправдательного приговора.

Законом вводится ответственность за следующие виды правонарушений:

- посягательство на безопасность информационных сетей, систем и технологий;
- неправомерное получение выгоды от телекоммуникационных и информационных технологий и услуг;
- несанкционированный доступ;
- незаконное прослушивание сети;
- нарушение целостности данных, информации, информационных систем и сетей;
- посягательство на электронную почту, сайты или личные учетные записи;
- нарушение дизайна веб-сайта;
- нарушение работы государственных информационных систем;
- создание, обладание и использование программ и оборудования, используемых при совершении преступлений в сфере информационных технологий;
- преступления против кредитных карт, услуг и электронных платежных инструментов;
- создание фейковых веб-сайтов, личных учетных записей и электронных писем;
- нарушение конфиденциальности и незаконный контент.

3.6. Закон о защите персональных данных (2020)

Этот закон [26] направлен на защиту персональных данных (ПД) людей, устанавливая новый стандарт их защиты. Согласно ему, ПД не могут быть собраны, обработаны, раскрыты каким-либо способом, кроме как с явного согласия Субъекта данных или в случаях, когда иное разрешено законом. Трансграничная передача ПД может осуществляться только в том случае, если уровень защиты или безопасности данных в иностранном государстве соответствует (или превышает) требованиям, установленным настоящим Законом и при условии получения соответствующей лицензии или разрешения. Исполнительные положения Закона устанавливают политику, критерии, положения и правила, необходимые для трансграничной передачи, хранения, совместного использования, обработки или раскрытия ПД и их защиты.

В соответствии с Законом должен быть создан «Центр защиты персональных данных», на который возложена общая задача по защите ПД и регулированию их обработки. Среди прочего, Центр отвечает за:

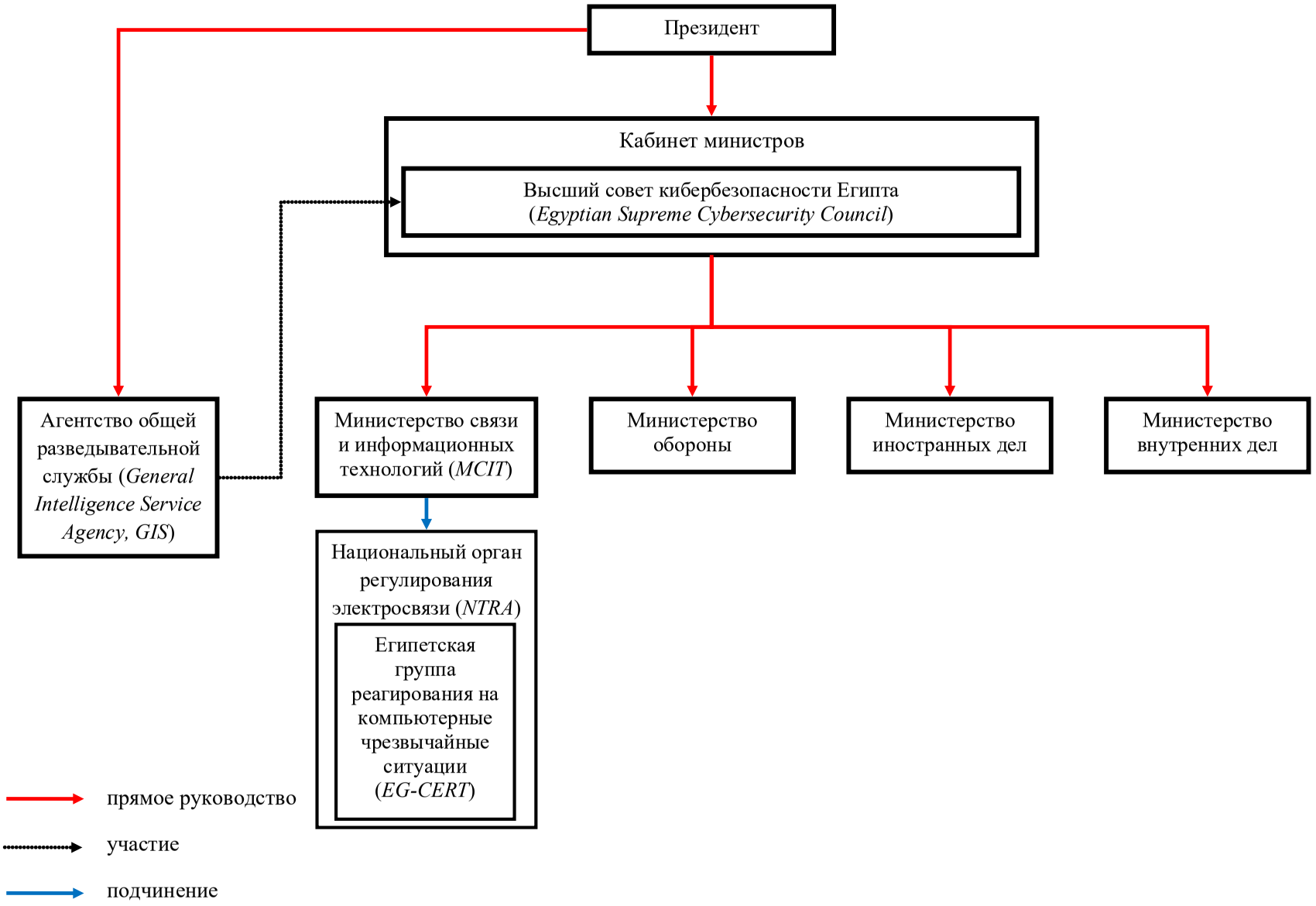
- установление и разработку политик, стратегических планов и программ, необходимых для защиты ПД;
- унификацию политики и планов защиты и обработки ПД в стране;
- установление и применение решений, правил, мер предосторожности, процедур и критериев, связанных с защитой ПД;
- установление руководящих принципов кодексов поведения, связанных с защитой ПД, и утверждение кодексов поведения различных организаций;
- сотрудничество со всеми организациями, государственными и неправительственными органами в реализации мер по защите ПД;
- поддержку развития компетентности персонала всех государственных и негосударственных организаций в области защиты ПД;
- выдачу лицензий, разрешений, сертификатов, связанных с защитой ПД;
- консультирование по проектам законов и международных соглашений, которые регулируют или затрагивают ПД;
- предоставление всех видов экспертиз и консультаций, связанных с защитой ПД;
- заключение соглашений и меморандумов о взаимопонимании, координации, сотрудничестве и обмене знаниями с международными организациями, имеющими отношение к работе Центра.

4. Государственные органы, входящие в систему обеспечения информационной безопасности и форматы государственно-частного партнерства

4.1. Высший совет кибербезопасности Египта

Высший совет кибербезопасности (*Egyptian Supreme Cybersecurity Council*) был учрежден в 2014 году, подчиняется кабинету министров и возглавляется министром связи и информационных технологий. Совет начал предварительную работу в январе 2015 года, а в июне 2016 года премьер-министр утвердил формирование Исполнительного бюро, Технического комитета Совета, их роли и обязанности. В состав Совета входят руководители государственных органов, участвующих в обеспечении национальной безопасности и управлении критически важной инфраструктурой: министерства обороны, иностранных дел, внутренних дел, нефти и минеральных ресурсов, электроэнергии и возобновляемых источников энергии, здравоохранения и народонаселения, водных ресурсов и ирригации, снабжения и внутренней торговли, связи и информационных технологий, Агентство общей разведывательной службы (*General Intelligence Service Agency*), Центральный банк Египта, а также три эксперта из исследовательских организаций и частного сектора, номинированных Советом.

Основные элементы структуры управления информационной/ кибербезопасностью в Египте



Совет разработал Национальную стратегию кибербезопасности и контролирует её реализацию и обновление.

На него возложены следующие функции:

- определение критически важных информационных инфраструктур (КИИ) во всех секторах государства и разработка основ для оценки и контроля обеспечения их безопасности;
- определение рамок, стратегий и политики в отношении КИИ для всех секторов государства;
- разработка планов и программ развития отрасли кибербезопасности и подготовки квалифицированных сотрудников и кадров для решения проблем и рисков кибербезопасности, создание основы для научных исследований и разработок в области кибербезопасности;
- сотрудничество и координация усилий на региональном и международном уровне с соответствующими организациями в области кибербезопасности и безопасности КИИ, разработка рекомендаций для необходимых законодательных мер обеспечения безопасности;
- определение для всех органов власти минимальных обязательных стандартов по обеспечению безопасности КИИ, включающих разработку планов действий в чрезвычайных ситуациях;
- разработка механизмов мониторинга рисков и периодического отслеживания киберугроз, распределение мандатов и ролей различных органов и учреждений на национальном уровне;
- разработка и внедрение стандартов и механизмов для определения надежности базовой и критической инфраструктуры;
- принятие стандартов кибербезопасности для систем в различных секторах, в том числе стандартов качества кибербезопасности;
- принятие механизмов оценки уровня безопасности, допуска и спецификации субъектов, управляющих критически важными коммуникационными и информационными инфраструктурами;
- разработка механизмов контроля и защиты официальных государственных информационных ресурсов и порталов в сети Интернет.

В рамках Совета функционирует комитет, которому поручено следить за киберпространством на предмет любого «отклоняющегося» общественного мнения и террористического контента.

4.2. Министерство связи и информационных технологий

Министерство связи и информационных технологий (англ. *Ministry of Communications and Information Technology, MCIT*), которое было создано

в 1999 году для развития национального сектора ИКТ, занимает важную роль в структуре управления кибербезопасностью Египта. Министр является председателем Высшего совета кибербезопасности, главой Национального органа регулирования электросвязи, а также созданного в 2019 году Национального совета по искусственному интеллекту, в функции которого входит управление реализацией Национальной стратегии в области искусственного интеллекта.

Миссия Министерства — обеспечить развитие общества, основанного на знаниях, и построить сильную цифровую экономику, опирающуюся на принцип равного и недорогого доступа к получению знаний, а также создать конкурентоспособную, инновационную национальную индустрию ИКТ. Оно также отвечает за планирование, составление и внедрение национальных планов и стратегий в области ИКТ.

Среди прочего, Министерство отвечает за реализацию программы «Цифровой Египет», которая построена на трех основных элементах: цифровая трансформация, цифровые навыки и рабочие места, а также цифровые инновации. В основе программы — развитие цифровой инфраструктуры, а также законодательной и нормативной базы.

4.3. Национальный орган регулирования электросвязи

Национальный орган регулирования электросвязи (англ. *National Telecom Regulatory Authority, NTRA*) был создан в 2003 году в подчинении Министерства связи и информационных технологий в соответствии с Законом о регулировании электросвязи. *NTRA* уполномочен регулировать и управлять сектором электросвязи, в том числе способствовать оказанию ИКТ-услуг в соответствии с самыми передовыми технологическими средствами. Орган также способствует привлечению в сектор внутренних и международных инвестиций в соответствии с правилами конкуренции.

У *NTRA* есть полномочия предпринимать различные действия для достижения этих целей, в том числе разрабатывать соответствующие стратегии, программы, правила и методы управления, а также осуществлять подготовку и публикацию правил лицензирования. В соответствии с этим мандатом, *NTRA* подготовил несколько нормативных инструментов и документов, связанных с цифровой экономикой, включая нормативную базу для центров обработки данных и услуг облачных вычислений, а также правила использования мобильных кошельков.

В соответствии со своим статусом в рамках Министерства, *NTRA* не обладает автономией в принятии решений и управляется советом директоров, в который входят исполнительный президент, а также представители Государственного совета, министерства обороны, министерства финансов, органов национальной

безопасности и Союза радио и телевидения, а также шесть членов, назначенных Министерством, и один сотрудник *NTRA*, делегированный Федерацией трудящихся Египта. Совет директоров осуществляет надзор за деятельностью, включая утверждение планов и программ, технических регламентов и стандартов качества, плана использования радиочастотного спектра и его лицензирование.

4.4. Египетская группа реагирования на компьютерные чрезвычайные ситуации (EG-CERT)

Египетская группа реагирования на компьютерные чрезвычайные ситуации была создана Национальным органом регулирования электросвязи в апреле 2009 года. Организационно EG-CERT состоит из пяти основных отделов: обработки киберинцидентов и непрерывности бизнеса, мониторинга и раннего предупреждения кибератак, тестирования на проникновение и анализа вредоносных программ, защиты критической информационной инфраструктуры и планов действий в чрезвычайных ситуациях, а также киберосведомленности и развития бизнеса. EG-CERT осуществляет функции сбора и анализа информации об инцидентах информационной безопасности, координации и посредничества между заинтересованными сторонами в решении инцидентов безопасности и сотрудничества с другими международными CERT. Группа также участвует в разработке соответствующей законодательной базы кибербезопасности с участием частного сектора и гражданского общества и руководствуется международными знаниями, опытом и инициативами – фактически является техническим исполнителем решений Высшего совета кибербезопасности Египта. Она также призвана создать национальную систему кибербезопасности и групп реагирования на компьютерные инциденты, а также развивать инфраструктуру, необходимую для обеспечения доверия к электронным транзакциям и защиты цифровой идентичности.

4.5. Министерство обороны

По имеющейся в открытом доступе информации, Министерство обороны Египта активно развивает свой потенциал в ИКТ-среде и внедрении ИИ в системы вооружений, в том числе через расширение взаимодействия с частным сектором, развитие партнерства с египетскими университетами и исследовательскими центрами [27]. Египет также принимает активное участие в учениях Центрального командования США *Bright Star*. В 2023 году в ходе учений особое внимание было уделено проведению операций в сфере кибербезопасности [28].

5. Участие в международном сотрудничестве с ООН и другими международными и региональными организациями в области формирования системы международной информационной безопасности

Можно утверждать, что в вопросах международного сотрудничества по информационной безопасности Египет занимает проактивную позицию как на уровне ООН, так и в региональных организациях, прежде всего — Лиге арабских государств и Африканском союзе.

Египет участвовал в работе Групп правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности в 2012/2013, 2014/2015 и 2016/2017 годах, он активный участник РГОС первого и второго созыва с представлением позиционных документов. Примечательно, что, в ходе 73 сессии Генеральной Ассамблеи ООН в 2018 году, Египет голосовал против американского проекта резолюции о новом созыве ГПЭ и за принятие российско-китайской инициативы о РГОС [29]. В то же время, в 2022 году Египет поддержал подготовленную Францией с ко-спонсорами резолюцию A/RES/77/37 «Программа действий по поощрению ответственного певедения государств при использовании информационно-коммуникационных технологий в контексте международной безопасности», которая противоречит позиции России.

Страна является участником Арабской конвенции 2010 года по борьбе с преступлениями в области информационных технологий. Не является подписантом Будапештской конвенции по противодействию компьютерным преступлениям и Конвенции по кибербезопасности и защите персональных данных Африканского союза.

Египет весьма активно продвигает инициативы, касающиеся управления ИИ, например, выступил за созыв под эгидой Африканского союза рабочей группы по ИИ с целью создания единой стратегии ИИ для Африки, а также Арабской рабочей группы по ИИ под эгидой Лиги арабских государств с целью разработки руководящих принципов для ИИ, общих рамок для совместных проектов, наращивания потенциала и повышения осведомленности о проблемах ИИ. В начале 2021 года Египет стал первой арабской и африканской страной, присоединившейся к Рекомендации Совета по ИИ Организации экономического сотрудничества (ОЭСР)[30]. Египет также играет важную роль в текущих обсуждениях в ЮНЕСКО относительно рекомендаций по этике искусственного интеллекта. Египет является активным участником различных мероприятий МСЭ, связанных с ИИ, таких как «ИИ во благо» (*AI for Good*), а также различных фокус-групп, занимающихся вопросами, связанными с ИИ, с целью повысить известность Египта и позиционировать его как одну из ведущих региональных стран в этой сфере.

В 2017 году лидерами Саудовской Аравии, Египта и США был создан Глобальный центр по борьбе с экстремистской идеологией «Этидал» (умеренность) в качестве многосторонней инициативы по борьбе с кибертерроризмом и киберэкстремизмом.

В марте 2024 года принята Совместная декларация о стратегическом и всеобъемлющем партнерстве между Арабской Республикой Египет и Европейским Союзом, где оформлена договоренность об углублении сотрудничества в области предотвращения и противодействия угрозам и вызовам безопасности, включая угрозы кибербезопасности [31].

Двустороннее сотрудничество с Россией

В 2016 году был подписан Меморандум о взаимопонимании между Министерством связи и массовых коммуникаций Российской Федерации и Министерством связи и информационных технологий Арабской Республики Египет о сотрудничестве в области электросвязи, почтовой связи и информационных технологий.

6. Возможные приоритеты в сфере обеспечения информационной безопасности и международной информационной безопасности в рамках БРИКС

В 2023 году министр иностранных дел Египта Самех Шукри, выступая с трибуны 78 сессии Генеральной Ассамблеи ООН заявил, что египетские власти намерены самым активным образом принимать участие в работе группы БРИКС: «Египет рассчитывает играть активную роль в БРИКС, чтобы отстаивать интересы и чаяния государств Юга» [32]. Заместитель министра иностранных дел и глава делегации Египта в БРИКС Раги Этреби на встрече шерп и су-шерп группы в рамках российского председательства в 2024 году заявил, что Египет готов обсуждать «углубление сотрудничества по таким направлениям, как инвестиции и торговля, промышленная трансформация, использование ИКТ в интересах развития, наращивание морского транспорта, логистика, а также решение проблем отсутствия продовольственной и энергетической безопасности» [33].

Принимая во внимание то, что Египет последовательно демонстрирует солидарность с российскими и китайскими инициативами на площадке ООН, можно ожидать, что участие страны в объединении БРИКС будет носить конструктивный характер. Одним из возможных направлений повышенного внимания может стать регулирование ИИ, так как Египет на протяжении длительного времени предлагает соответствующие инициативы на региональных форумах, и одновременно эта тематика набирает значимость в обсуждениях БРИКС.

7. Список использованной литературы

1. BDEX, https://bdex.ru/naselenie/egypt/.
2. The World Bank, https://data.worldbank.org/country/south-africa.
3. ITU Data Hub, https://datahub.itu.int/data/?e=EGY&c=701&i=11624.
4. МСЭ, Отчет «Измерение информационного общества» за 2018 год, https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR_Vol_2_R.pdf.
5. 'Worldwide Mobile Data Pricing 2022', Cable.co.uk, 2022, https://www.cable.co.uk/mobiles/worldwide-data-pricing/.
6. 'Network Readiness Index 2023 – Egypt', Portulans Institute, 2023, https://download.networkreadinessindex.org/reports/countries/2023/egypt.pdf.
7. Egypt ICT Market Size and Forecast to 2027, 2023, https://www.globaldata.com/store/report/egypt-ict-market-analysis/.
8. GovTech Maturity Index, December 2022, https://openknowledge.worldbank.org/server/api/core/bitstreams/5e157ee3-e97a-5e42-bfc0-f1416f3de4de/content.
9. Global Cybersecurity Index 2020, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.
10. Egypt's to kick-off International Security and Safety Exhibition and Conference on 19 June 2023, https://www.dailynewsegypt.com/2022/08/04/egypts-to-kick-off-international-security-and-safety-exhibition-and-conference-on-19-june-2023/.
11. INTERPOL report identifies top cyberthreats in Africa 21 October 2021, https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-identifies-top-cyberthreats-in-Africa.
12. 'Government AI Readiness Index 2022', Oxford Insights, 2022, https://www.unido.org/sites/default/files/files/2023-01/Government_AI_Readiness_2022_FV.pdf.
13. National ICT Strategy 2012-2017 Towards a Digital Society and Knowledge-based Economy, https://mcit.gov.eg/Upcont/Documents/ICT%20Strategy%202012-2017.pdf.
14. E-Commerce Strategy https://mcit.gov.eg/Upcont/Documents/Publications_1532018000_e-Commerce-Strategy-March2018.pdf.
15. Egypt's official retail trade sector is 14.5% of GDP at LE850B, ecommerce at $4.8B (Business Today Egypt, March 23, 2021), https://www.businesstodayegypt.com/Article/1/444/Egypt%E2%80%99s-official-retail-trade-sector-is-14-5-of-GDP.
16. National AI Strategy https://andp.unescwa.org/sites/default/files/2021-11/Publications_672021000_Egypt-National-AI-Strategy-English.pdf.
17. Egypt Vision 2030 https://mped.gov.eg/files/Egypt-Vision_2030.pdf.
18. National Cybersecurity Strategy 2022-2026 https://mcit.gov.eg/Upcont/Documents/Publications_1412024000_National_Cybersecurity_Strategy_2023_2027.pdf.
19. National Cybersecurity Strategy 2017-2021, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/EgyptNational%20Cybersecurity%20Strategy-English%20version-18%20Nov%202018.pdf.
20. Egyptian Charter for Responsible AI, https://aicm.ai.gov.eg//en/Resources/EgyptianCharterForResponsibleAIEnglish-v1.0.pdf.
21. Telecommunication Regulation Law https://www.tra.gov.eg/wp-content/uploads/2020/11/Law-No-10-of-2003.pdf.
22. Anti-terrorism Law, https://counterterrorlaw.info/assets/downloads/Law_95_of_2015_for_Confronting_Terrorism.pdf.
23. Law No. 180/2018 regulating the press and the media and the Supreme Council for Media, https://wwwex.ilo.org/dyn/natlex2/natlex2/files/download/111247/EGY111247.pdf.
24. Prime Minister's Decree No. 994 of 2017, https://escc.gov.eg/2017.pdf.
25. Anti-Cyber and Information Technology Crimes Law, https://cybercrime-fr.org/wp-content/uploads/2020/04/Egyptian-cybercrime-law-.pdf.
26. Personal Data Protection Law, https://wwwex.ilo.org/dyn/natlex2/natlex2/files/download/111246/EGY111246%20Eng.pdf.
27. A busy year for the Egyptian Armed Forces, 2022, https://english.ahram.org.eg/.NewsContent/50/1201/482577/AlAhram-Weekly/Egypt/A-busy-year-for-the-Egyptian-Armed-Forces.aspx.
28. Bright Star 2023 highlights the long-standing Egyptian-American ties, 2023, https://www.centcom.mil/MEDIA/NEWS-ARTICLES/News-Article-View/Article/3520694/bright-star-2023-highlights-the-long-standing-egyptian-american-ties./.

29. Advancing responsible State behaviour in cyberspace in the context of international security : resolution / adopted by the General Assembly, UN, 2018, https://digitallibrary.un.org/record/1657117?ln=ru.
30. Recommendation of the Council on Artificial Intelligence https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449#adherents.
31. Joint Declaration on the Strategic and Comprehensive Partnership between The Arab Republic Of Egypt and the European Union, 2024, https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_24_1513.
32. Египет готов активно участвовать в работе БРИКС, ТАСС, 2023, https://tass.ru/mezhdunarodnaya-panorama/18827759.
33. Египет уверен, что председательство РФ в БРИКС сможет отвечать вызовам в продбезопасности, ТАСС, 2024, https://tass.ru/ekonomika/19852459?ysclid=lublsui788590950665.

Исламская Республика Иран

Официальное название: Исламская Республика Иран (перс. Джомхурийе Исламийе Иран)

Столица: Тегеран

Официальный язык: персидский (фарси)

Территория: 1 648 195 км² (17 место в мире). Иран расположен в Юго-Западной Азии. Граничит на западе с Ираком, на северо-западе — с Азербайджаном, Арменией, Турцией, на северо-востоке — с Туркменистаном, на востоке — с Афганистаном и Пакистаном. С севера Иран омывается Каспийским морем, с юга — Персидским и Оманским заливами Индийского океана.

Существуют территориальные споры между Ираном и Объединенными Арабскими Эмиратами в отношении трех островов в Ормузском проливе, контролирующих вход в Персидский залив. В конце 1940-х гг. островами попеременно владели шейхи эмиратов Абу-Даби и Дубая, находившихся под британским протекторатом. В 1971 году, после ухода Великобритании из региона, острова должны были достаться ОАЭ, в состав которых вошли оба этих эмирата, но их захватил шахский Иран. На островах по сей день содержится значительный военный контингент. Также существует претензии на территории Азербайджана, Афганистана и части территории Пакистана.

Население: 88 550 570 чел. в 2022 году (17 место в мире)[1], на середину 2023 года число проживающих в стране оценивалось ООН в 89,44 млн чел.

Государственное устройство: По конституции, принятой в 1979 году, Иран является исламской республикой. На 2019 год страна являлась одной из немногих существующих в мире теократий.

Государственная власть осуществляется формально независимыми друг от друга законодательной, исполнительной и судебной ветвями власти, находящимися под контролем руководителя страны (принцип велаят-е факих).

Верховный руководитель Исламской революции определяет генеральную линию политики государства и осуществляет контроль над претворением её в жизнь; санкционирует проведение референдумов; назначает и освобождает от занимаемых должностей высших должностных лиц. Он осуществляет общее управление вооруженными силами; наделён полномочиями объявления войны, мира и всеобщей мобилизации; разрешает разногласия, возникающие между ру-

1 World Population by Country 2024 (Live), https://worldpopulationreview.com/.

ководством трёх ветвей власти страны; подписывает указ о назначении президента Ирана после его избрания и обладает правом снятия с поста президента (в случае если Верховный суд признает его не соответствующим занимаемой должности или если парламент вынесет решение об отставке президента)[2]. Верховный руководитель избирается Советом экспертов и подотчетен ему. С 1989 года этот пост занимает Али Хаменеи.

Исполнительная власть. Вторым по значимости должностным лицом в Иране является президент, который является гарантом конституции и главой исполнительной власти. Решения по ключевым вопросам принимаются только после одобрения Высшего руководителя. Президент возглавляет кабинет министров, назначает его членов и координирует работу правительства. Десять вице-президентов и 21 министр правительства утверждаются на пост парламентом. Хотя президент назначает министров обороны и разведки, их кандидатуры должны быть заранее одобрены Верховным руководителем. Президент избирается прямым всенародным голосованием на четырехлетний срок, с правом одного переизбрания. Кандидаты в президенты должны быть предварительно одобрены Советом стражей Конституции Исламской Республики Иран (Советом стражей). Действующий президент Ирана Ибрахим Раиси.

Законодательная власть представлена однопалатным парламентом — Меджлисом («Исламский консультативный совет»). Меджлис состоит из 290 членов, избираемых всенародным голосованием на четырехлетний срок. Все кандидаты в депутаты Меджлиса также утверждаются Советом стражей, который состоит из 12 членов, 6 из которых назначает Высший руководитель, остальные назначаются парламентом по представлению председателя Верховного суда. Основная обязанность Совета стражей — проверка законопроектов на соответствие исламскому праву. В случае если имеются разногласия с шариатом, законопроект отправляется на доработку. Кроме того, Совет стражей имеет право наложить вето на любое решение Меджлиса.

Собрание экспертов выполняет работу по организации, подготовке и проведению выборов руководителя страны; избирает руководителя страны, принимает его отставку, а в случае необходимости выясняет его дееспособность и целесообразность дальнейшего пребывания на посту; рассматривает и подготавливает изменения и поправки в Конституцию страны. Состоит из 86 шариатских правоведов-факихов (избираются всеобщим голосованием на 8 лет), пользующихся правом вынесения фетв.

Экономика: По данным Всемирного банка за 2022 год показатели Валового внутреннего продукта (ВВП) (по паритету покупательной способности):

2 ИРАН // Большая российская энциклопедия — электронная версия, https://old.bigenc.ru/geography/text/2019712?ysclid=lpful8pxn8612975029.

Итого: 1,601 трлн долл. (21 место в мире) На душу населения 18 075 долл. (80 место в мире);

Показатели ВВП (Номинал):

Итого: 389 млрд долл. (40-й показатель в мире).

На душу населения: 4 388 долл. США (114-й показатель в мире).

Согласно классификации ООН, Иран относится к группе стран со средним уровнем дохода ниже среднего.

Дипломатические отношения с Россией (СССР) установлены 26 февраля 1921 года.

1. Уровень развития информатизации страны и информационно-коммуникационной инфраструктуры, системы обеспечения информационной безопасности

К моменту начала Исламской революции (1978–79 гг.) страна активно развивала промышленность. Ее удельный вес во внутреннем валовом продукте (ВВП) за 1960–75 годы увеличился с 27,5 до 72,1%. За короткое время были созданы отрасли современной индустрии: металлургия, нефтехимическая, автомобильная и тракторостроительная промышленность, судо- и самолетостроение. По темпам роста экономики Иран занимал второе место в Азии после Японии [1]. Однако ряд негативных факторов (свержение шаха, захват американского посольства в Тегеране и его сотрудников) привел к введению в отношении Исламской республики Иран жестких экономических санкций США (ИРИ). Их режим много раз менялся. В 2012 году Вашингтоном введен полный запрет на экспорт иранской нефти, страна была отключена от системы передачи финансовых сообщений SWIFT, что создало дополнительные сложности для внешнеэкономической деятельности ИРИ, закупок западных технологий и комплектующих.

ВВП Ирана с 2010 по 2020 год упал в 2,4 раза, резко снизилась покупательская активность. ИТ-компании были вынуждены сократить инвестиции в инфраструктуру и разработку цифровых сервисов. Потребовалось время на адаптацию экономики. Спрос постепенно был восстановлен, стал развиваться национальный ИКТ-рынок (программное обеспечение, консалтинг и услуги, но аппаратное обеспечение по-прежнему закупается по схемам параллельного импорта). В 2012 году ИТ-сегмент (без учета коммуникаций) имел долю 0,13% ВВП страны, в 2013 году — 0,36%, а в 2019 году составил уже 0,71% ВВП [2]. По некоторым данным в 2022 году этот показатель достиг 4,6%.

Несмотря на то, что в 1992 году Иран стал первой страной в Юго-Западной Азии[3], подключенной к глобальной сети, уровень проникновения Интернета в 2010 году составлял всего 15,9% населения. За прошедшие годы картина радикально поменялась: в середине 2022 года согласно данным Internet World Stats [3] этот показатель достиг 91% (или 78 млн пользователей)[4], что является очень высоким уровнем не только в регионе, но и в мире.

В значительной степени это заслуга распространения подвижной связи, поскольку смартфоны остаются основным средством доступа к Интернету. Число

3 Иранский Центр исследований теоретической физики был подключен к глобальной сети первым.

4 Следует отметить, что статистические данные разных компаний существенно отличаются. Так согласно публикации «Страны с наибольшим числом пользователей Интернета (2023)» Иран занимает 16 место в мире по уровню проникновения Интернет с показателем 79,42% населения (или 69,83 млн чел.) https://explodingtopics.com/blog/countries-internet-users.

пользователей мобильной связи достигло 145,7 млн абонентов, идентифицируемых по заводскому номеру телефона[5]. Вся территория страны покрыта сетями 3G/4G, скорость таких соединений неуклонно растет (за 2022 год увеличение составило 62,7%). Активно развиваются сети подвижной связи пятого поколения 5G[6]. Поэтому качество подключения тоже быстро улучшается. Агентство по регулированию коммуникаций Ирана (CRA) в конце 2022 года заявило о регистрации 102,3 млн пользователей высокоскоростного мобильного широкополосного доступа (рост за год 11%). Общее количество абонентов фиксированных сетей связи составляет 29 млн, однако широкополосный доступ к Интернету по таким сетям доступен только 11 млн абонентов [4]. Темп развития инфраструктуры поддерживается высокий: к середине 2025 года планируется охватить высокоскоростной оптической сетью 20 млн домохозяйств и коммерческих предприятий [5].

Следует также отметить, что на территории Ирана 5 точек примыкания к международным системам подводных кабелей, которые обеспечивают стране беспрепятственный трафик с Кувейтом, ОАЭ и Оманом, а также выход через кабель FALCON на все страны ССАГПЗ и Индию [6].

Набирает темп развития и цифровая экономика Ирана, поскольку растет доступность информационных и коммуникационных технологий, которые являются ее ядром[7]. В том числе, большую роль играет национальная карточная платежная система SHAPARAK и мобильные банковские приложения. В период пандемии COVID-19 произошел всплеск интереса к онлайн-услугам (дистанционное обучение[8], электронная торговля[9], цифровая медицина и др.). Появились национальные аналоги успешных западных ИТ-сервисов. Так при поддержке государственной телекоммуникационной компании Irancell создан сервис SNAPP по функциям аналогичный Uber, с помощью госинвестиций созданы собственные поисковые системы Yooz и Rismoon. Иранская версия торговой площадки Amazon разработана компанией Digikala, созданной в 2007 году с участием ведущего венчурного фонда страны, в настоящее время она контролирует более

5 С 2017 года с целью борьбы с контрабандой и преступностью в Иране действует процедура обязательной регистрации мобильных устройств по заводскому номеру IMEI.

6 В Иране только три оператора мобильной связи: государственный Mobile Telecommunications Company of Iran (MCI, перс. - Hamrah-e Avval in Persian), Irancell и RighTel.

7 Доступность ИКТ в период 2016-21 гг. улучшилась на 43%. Источник: Рещиков О.И. Процессы цифровизации в Иране в период санкций, журнал Азия и Африка сегодня, 2022 №8, С. 26–33 https://sochum.ru/index.php?dispatch=materials.getfile&object_id=97083&object_type=pdf.

8 В 2022 году в период введения ковидных карантинных мер в школах, когда остро стоял вопрос о необходимости обеспечения непрерывности процесса обучения, наравне с трансляцией уроков по телевидению была запущена социальная сеть обучающихся Shad. Проект был реализован мобильным оператором MCI в сотрудничестве с Министерством образования Ирана. К системе были подключены 369 тыс. школ, 952 тыс. учителей и 35 млн школьников.

9 В 2020 году Иран в глобальном Индексе электронной торговли (рассчитывается Конференцией ООН по торговле и развитию, ЮНКТАД) занял 44 позицию, опережая своих соседей по региону Саудовскую Аравию, Оман, Катар и Турцию, https://unctad.org/system/files/official-document/tn_unctad_ict4d17_en.pdf.

85% внутреннего рынка онлайн-торговли. Всего в сфере цифровой коммерции функционирует около 350 тыс. предприятий.

Государство старается оказывать финансовую поддержку основанным на экономике знаний технологическим компаниям, в 2020 году они получили кредиты на сумму 137,6 трлн риалов (849,3 млн долл. США) [7]. К концу 2020 года доля цифровой экономики в ВВП страны возросла до 6,5% (среднемировой показатель 15,5%).

Укрепляется и сектор государственных цифровых услуг, расширяется география их доступности в сельских регионах страны. Введен цифровой надзор в здравоохранении, в том числе осуществлен переход на электронные рецепты. Улучшается регулирование деятельности частного бизнеса и запущена услуга по выдаче разрешений на работу предпринимателей. Согласно исследованию Управления по экономическим и социальным вопросам ООН «E-Government Survey Index 2022», Иран входит в группу стран с высоким индексом развития электронного правительства и занимает 91 место в мире [8]. Доля переведенных в онлайн-формат услуг в 2022–23 годах составила 95%, хотя пять лет назад было лишь 40%. На современном этапе правительство продолжает расширять спектр услуг, предоставляемых гражданам в электронном виде, планируется запустить портал «единого окна».

Национальная ИКТ-отрасль продолжит свое развитие благодаря высокому научному потенциалу страны. По данным Австралийского института стратегической политики, в 2023 году Иран вошел в десятку ведущих научно-технических сверхдержав, причем по 6 из 44 критически важных для цифровой трансформации технологий он входит в двадцатку лучших, опережая по этому показателю Японию[10]. Также он входит в тройку самых инновационных государств в регионе Центральной и Южной Азии, занимая 62 позицию в Глобальном инновационном индексе (WIPO, 2023), что очень хорошо для экономики со средним уровнем дохода ниже среднего. По прогнозам, к 2032 году Иран может войти десятку лидеров в сфере искусственного интеллекта, хотя еще в 2018–2019 годах он занимал лишь 13 позицию в мире по научным публикациям по этой тематике, опережая Бразилию, Нидерланды и Россию [9]. Однако по готовности к внедрению этой технологии Иран занимает лишь 75 место, поскольку не имеет достаточной производственно-технологической базы [10].

10 Расчет оценки сделан на основе наукометрических данных (количество научных публикаций, индекс цитирования, количество научных и учебных заведений по конкретной проблематике, входящие в Top20 в таких критически важных для стратегического преимущества в цифровой экономике технологиях, как мобильная связь 5G/6G и оптические коммуникации, искусственный интеллект, расширенная аналитика данных, распределенные реестры, машинное обучение, технологии обеспечения кибербезопасности, разработка и производство чипов, обработка естественных языков и распознавание речи. Источник: ASPI's Critical Technology Tracker The global race for future power, p.5, https://www.aspi.org.au/report/critical-technology-tracker.

Первоочередной задачей государства является создание благоприятных условий бизнесу для трансфера научных разработок в реальный сектор экономики. Страна уже поднялась с 34 на 16 место в мире по уровню наукоемкого производства[11]. Государством оказывается содействие инновационному бизнесу (в Иране базируется 4400 производств основанных на знаниях, 39 технологических парков[12], 167 центров развития технологий), но следует активнее развивать соответствующую регуляторную политику.

Расширение цифровизации повышает значимость защищенности сетевых ресурсов и надлежащего обеспечения информационной безопасности. Для Ирана необходимость решения этого вопроса в национальном масштабе является одним из факторов поддержания геополитической устойчивости страны [11]. Иран объявлен Вашингтоном врагом[13], против него западные страны постоянно осуществляют разведывательные и диверсионные кибероперации. Наиболее резонансной является «Olympic Game» по заражению вирусом Stuxnet критических информационных инфраструктур, по данным открытых источников осуществленная совместно США, Израилем и Нидерландами. Этот вирус в 2010 году вызвал глобальную эпидемию, но единственной целью операции был вывод из строя иранских центрифуг по обогащению урана, чтобы вынудить страну отказаться от ядерной программы.

Этот и другие инциденты[14] заставили руководство страны признать задачу обеспечения информационной безопасности критически важной для национальной безопасности и устойчивого развития. В настоящее время уровень потенциала Ирана в этой сфере оценивается высоко: в Глобальном индексе кибербезопасности (GCI, 2020)[15] Иран занимает 54 позицию, а в группе 38 азиатско-ти-

---

11 Согласно оценкам правительства, Иран в среднем ежегодно тратит около 4% ВВП на развитие образования. Благодаря этому страна находится на 44 месте по научным публикациям в мире. В показателях индекса качества знаний и образования, уровень грамотности повысился до 98%, по качеству фундаментальных наук и математики страна поднялась на 38 место в мире. В Иране получают образование 4,8 млн студентов в 2,5 тыс. центрах высшего образования. Источник: Report: Promising future expected for Iran's ICT sector, December 19, 2018, https://theiranproject.com/blog/2018/12/19/report-promising-future-expected-for-irans-ict-sector/.

12 Pardis Technology Park около Тегерана – один из самых больших в Западной Азии технологических парков, является иранским аналогом Силиконовой долины. Там расположено более 200 стратапов, продукция некоторых из них идет за рубеж. В 2020 году были объявлены планы о расширении и создании инновационной зоны для осуществления полного цикла внедрения новых технологий.

13 В Национальной стратегии кибербезопасности США (2023) указано: «Правительства Китая, России, Ирана, Северной Кореи и других автократических государств с ревизионистскими намерениями агрессивно используют передовые кибер средства для достижения целей, которые противоречат нашим интересам и общепринятым международным нормам. Их безрассудное пренебрежение верховенством закона и правами человека в киберпространстве угрожает национальной безопасности и экономическому процветанию США».

14 Многочисленные атаки на правительственные организации, нефтяную отрасль, в 2021 году атака на систему автозаправочных станций Ирана, создавшая коллапс системы получения через топливные карты субсидированного топлива.

15 GCI – интегральный индекс рассчитывается МСЭ по нескольким параметрам в 5 группах: развитие правовой системы обеспечения информационной безопасности; применение технических и организационных мер; реализации программ наращивания потенциала; участие в международном сотрудничестве.

хоокеанских стран — 12 (Китай среди них на 8 позиции, Таиланд на 9, Новая Зеландия на 10 позиции) [12]. Очень близкую оценку системе информационной безопасности Ирана в июле 2023 года дал Киберцентр НАТО[16], хотя методика расчета и параметры другие.

Несмотря на перечисленные выше достижения Ирана, общий уровень цифрового развития страны низкий. Эксперты видят этому целый ряд причин. Прежде всего, это дефицит цифровых технологий и недостаточный уровень развития ИКТ-инфраструктуры. Существует проблема с недостатком кадров, которая усугубляется «утечкой мозгов». Ежегодно страну покидает более 150 тыс. специалистов, львиная доля которых профессионалы технологического сектора. За иранскими программистами охотятся не только ведущие работодатели, но и спецслужбы.

Значимое негативное влияние оказывает ограниченность мер государственной поддержки по использованию ИКТ, бремя развития цифровой экономики возложено на частный сектор. Западными экспертами отмечается неэффективное управление проектами по внедрению цифровых технологий, а также отсутствие определенности в регулировании безопасности и использования персональных данных. Низкий уровень цифровой культуры обуславливает сложность внедрения цифровой аутентификации, которая является одним из основных инструментов изменения экономической структуры страны и перехода к цифровой экономике [13].

2. Основные документы стратегического планирования в сфере развития ИКТ и обеспечения информационной безопасности

Как отмечают многие исследователи, описание властной вертикали в принятии решений по вопросам стратегического планирования и национальной безопасности Исламской республики Иран является существенной проблемой. Национальная политическая конструкция (имамат[17], возглавляемый Верховным лидером Исламской революции) сильно отличается от принятой в большинстве стран мира, в ней непрозрачность политических процессов усугубляется присутствием многочисленных, взаимно конкурирующих центров влияния, преобладанием личностных взаимоотношений и патронажных сетей. Кроме того, понятийные

16 Иран: 54 место в мире по уровню кибербезопасности, 81 место по уровню развития ИКТ и 79 место по уровню сетевой готовности, https://ncsi.ega.ee/country/ir/.

17 Имамат является одной из важнейших институций в мусульманском мире. Это религиозное и политическое лидерство, которое состоит из вождей, выбираемых или назначаемых из числа верующих. Организация имамата основывается на традиционных принципах, установленных в исламской шариатской системе, а также на правовой базе, к которой относятся Коран и Сунна.

границы, политика и стратегия безопасности, а также идентификация угроз формируются под влиянием, прежде всего, исламских (революционно-клерикальных) воззрений. Принятие решений не всегда сводится к согласованию целей и средств. Определяющий принцип, возможно вполне рациональный, по-прежнему состоит в «целесообразности», то есть в сохранении имеющейся политической структуры, которое, с точки зрения правящей элиты, стало синонимом «национальных интересов» [14].

В силу этой особенности привычных нам документов стратегического планирования в Иране крайне мало. В частности, отсутствует документ, излагающий дорожную карту управления государственной системой обеспечения информационной безопасности страны [15]. При этом у исследователей нет сомнения, что гибридная и высоко адаптивная киберстратегия существует, и основана она на использовании частично децентрализованной и многокомпонентной системы сил и средств для ассиметричного ответа на существующие вызовы и угрозы национальной безопасности.

2.1. Программы социально-экономического развития

Среди общедоступных документов можно выделить долгосрочную программу социально-экономического развития **Перспективный план развития информационных технологий до 2025 года**, принятый в 2005 году и поставивший амбициозную задачу превращения Ирана в ведущую региональную державу, лидера по экономической, научной и технологической мощи [16], а также среднесрочные **Национальные пятилетние планы**, в которых определяется роль государства в реализации цифровых программ и ставятся конкретные задачи. Например, по развитию инфраструктуры связи и ее доступности гражданам и социальным учреждениям, информатизации всех сфер жизни, развитию цифровой экономики (умный город, электронное здравоохранение и обучение, финтех-услуги), по расширению спектра государственных услуг, развертыванию для этого инфраструктуры открытых ключей (PKI[18]), внедрению систем электронного документооборота в органах государственной власти, наращиванию научных исследований и подготовки кадров.

В этих документах также отмечается, что цифровые сервисы и услуги должны быть безопасными, ставятся задачи формирования необходимых органов и систем управления информационной безопасностью. В частности, Пятилетним планом на 2016–21 годы была поставлена цель выйти на ведущее место

18 В период с 2018 по 2020 год количество электронных подписей, оформленных в PKI возросло в 4,6 раза. Источник: Рещиков О.И. Процессы цифровизации в Иране в период санкций. Журнал Азия и Африка сегодня 2022 № 8. С. 30, https://asaf-today.ru/s032150750021324-8-1/.

в регионе по обеспечению кибербезопасности пользователей. Предписывалось ввести в государственных организациях наилучшую практику, разработанную национальной компанией по кибербезопасности AFTA, в частности, внедрить систему управления кибербезопасностью (ISMS). Для комплексного анализа киберугроз, улучшения мониторинга состояния информационной безопасности, обмена данными и методами снижения рисков рекомендовано создать отраслевые и ведомственные операционные центры информационной безопасности (ISOCs), сертифицировать безопасность всей ИКТ продукции в специализированных лабораториях[19].

По данным МСЭ на 2015 год, в Иране не было официально одобренных национальных или отраслевых требований кибербезопасности для применения международных стандартов информационной безопасности, а также отсутствовали требования к обеспечению информационной безопасности для сертификации и аккредитации государственных ведомств и их специалистов [17].

2.2. **Стратегия развития ИКТ** (2020)

Несмотря на то, что правительство Ирана назвало ИТ-сектор в числе трех главных национальных приоритетов в 2016–21 гг., документ долгосрочного планирования выработан не был. Опубликованная в 2020 году Стратегия развития информационных и коммуникационных технологий Ирана — первый документ, системно излагающий задачи в сфере информатизации и целевые показатели достижения поставленных целей [18]. Она является частью более масштабной стратегии развития импорта, которая направлена на построение в Иране основанной на знаниях экономики и выход страны на стратегические рынки. Ключевая роль в решении этой задачи отводится ИКТ. Стратегия ставит три первоочередные цели.

1. Оказать содействие укреплению экосистемы средних, малых и начинающих компаний ИКТ-сектора для улучшения бизнес-среды путем проведения институциональных реформ, снижения регуляторной неопределенности, улучшения финансовой политики, укрепления цифровых инструментов и доступа, развития государственно-частного партнерства, содействия импорту продукции (особо выделено разработка программного обеспечения).

2. Развитие человеческого потенциала и инновационных навыков, подготовка и переподготовка технических кадров, увеличение выпуска квалифици-

19 Указанные мероприятия выполнены частично: ISMS внедрено только в 39% государственных организаций, ISOCs созданы в 20% госучреждений, из запланированных 29 лабораторий для сертификации безопасности ИКТ созданы только 9. Источник: Cyber Wellness Not Up to the Mark // Financial Tribune, September 12, 2015, https://financialtribune.com/articles/people/25621/cyber-wellness-not-up-to-the-mark.

рованных специалистов, улучшение качества содействия стартапам, увеличение поддержки и инноваций в разработке иранского программного обеспечения.

3. Консолидация конкурентоспособности ИКТ-компаний для увеличения их экспорта. Оказание помощи для сертификации ИКТ-продуктов на соответствие международным стандартам, что повысит качество и откроет новые рынки сбыта. Создание благоприятных условий для инвестирования в ИКТ-рынок, формирование сетей из компаний, которые могут улучшить экспорт. Формирование цепочек поставок и поддержки, при этом особое внимание будет уделено развитию программного обеспечения, цифровым финансовым технологиям (финтех) и услугам для электронной торговли.

Следует отметить, что ключевые задачи обеспечения безопасности национального информационного пространства выполняют не гражданские, а силовые ведомства Исламской Республики Иран, в связи с чем стратегическое планирование в этой сфере большей частью недоступно.

2.3. **Национальная позиция Ирана** (2020)

В документе [19], опубликованном Генеральным штабом вооруженных сил страны, изложены концептуальные подходы к кибероборонe и защите военных, экономических, социальных, культурных «национальных интересов» и политической власти.

В статье I признается, что территориальный суверенитет и юрисдикция государств распространяется на все элементы киберпространства, и Иран будет развивать необходимый потенциал. Развитие наступательной и сдерживающей киберзащиты объявлено ключевым приоритетом для стратегического руководства государства. Любое использование киберпространства для незаконного проникновения в государственные или частные киберструктуры, осуществленное под контролем другого государства, может быть расценено Ираном как нарушение его суверенитета.

В статье III раскрывается понимание вооруженными силами принципа невмешательства во внутренние и международные дела Ирана. Как интервенция могут быть расценены вмешательство в выборы, манипуляции общественным мнением и провоцирование социальных волнений и беспорядков, осуществленные как через киберпространство, так и другими способами, влекущими последствия для осуществления государством внутренней и международной деятельности с использованием ИКТ-инфраструктуры и сервисов. Незаконными будут признаны осуществленные с помощью кибер- или иных средств попытки угроз руководству государства, политическим, экономическим, социальным и культурным органам.

Вооруженные силы будут рассматривать кибероперации, приносящие значительные материальные потери или смерть людей, как применение силы против Ирана. Если такие операции затрагивают критически важные национальные инфраструктуры, в том числе инфраструктуры для защиты (государственные или частные), то они приравниваются к нарушению принципа неприменения силы. Иран оставляет за собой право на самооборону, если уровень осуществленных против него кибероперацій будет сравним с применением конвенционального оружия (Статья IV).

Из этого можно сделать вывод, что Исламская Республика Иран оценивает риски применения разрушительных компьютерных атак выше, чем реальную войну, поэтому кибербезопасность и защита являются ключевым и жизненно важным элементом национальной обороны [20].

В контексте описанного документа важно отметить, что спектр угроз в киберпространстве, исходящих от внешних источников, дополняется внутренним фактором: устойчивость иранской государственной системы сильно зависит от внутриполитической ситуации. В свою очередь это связано с внутриэкономическими проблемами и сложной общественно-политической атмосферой, которая подвержена информационному воздействию оппозиции и поддерживающих ее внешних сил. Эти факторы ориентируют иранское руководство на приоритетное развитие эффективных механизмов по обеспечению контроля за интернет-пространством, мониторингу цифровой активности пользователей, содержания и распространения контента (он должен соответствовать исламским культурным ценностям, требованиям шариата и «национальным интересам») [21].

Принимая во внимание роль ИКТ в содействии волнениям «арабской весны», в стране введены официальные правила цензуры и контроля доступа к сети Интернет, ограничен доступ к зарубежным информационным ресурсам, введен запрет на использование для выхода в сеть анонимайзеров (в т.ч. частных виртуальных сетей VPN[20]) и средств коммуникации со сквозным шифрованием (в т.ч. WhatsApp, Telegram, Viber, Instagram), что не остановило их массовое использование[21]. Кроме этих мер правительство регулярно применяет отключение доступа к сети Интернет в условиях социальных беспорядков и волнений[22].

---

20 Рынок VPN в Иране оценивается в 21 млн долл. США в год. Некоторые VPN поддерживаются за счет грантов, финансируемых иностранными правительствами и фондами, такими как Psiphon.

21 Аудитория сервиса Telegram в Иране на начало 2023 года составляла более 40 млн пользователей, ежедневно активны 555 тыс. каналов на фарси. В Instagram зарегистрированы 24 млн иранцев (данные на февраль 2018 года, уже после блокировки Instagram на территории Ирана). При этом главные конкуренты Instagram — Twitter, Facebook и «ВКонтакте» были заблокированы еще в 2009 году.

22 Первым прецедентом стало отключение Интернет в ходе беспорядков, связанных с подозрением на фальсификацию результатов президентских выборов в 2009 году. В качестве других примеров американские авторы приводят: демонстрации в связи увеличением цены на бензин (2019), протесты на ограничение подачи воды в провинции Хузестан (2021).

Как средство решения указанных проблем правительством выбран путь создания автономной от глобального Интернета государственной сети **National Information Network** (на персидском — **SHOMA**), которая обеспечит высокоскоростной широкополосный доступ к национальному контенту и предотвратит доступ к нежелательным зарубежным ресурсам. По стоимости это самый дорогой ИКТ-проект правительства[23].

Планы по созданию SHOMA были озвучены еще в 2006 году, но реальное развертывание сети началось существенно позднее. В августе 2016 года завершена первая фаза проекта — развертывание инфраструктуры и отделение национального сегмента сети Интернет. В феврале 2017 года осуществлена вторая фаза — миграция онлайн-сервисов на хостинги на территории Ирана. В июле 2017 года завершился третий этап — в SHOMA реализован доступ ко всем электронным государственным сервисам[24]. Постепенно на SHOMA вынуждают мигрировать национальные коммерческие компании, в ней повышается качество инфраструктурных услуг для бизнеса и формируется экономика центров обработки данных.

С технической точки зрения SHOMA — внутренняя сеть (intranet) на IP-протоколе с собственной операционной системой, поисковым сервисом, электронной почтой, мессенджером, платформами для местных социальных сетей, центрами обработки данных для хостинга контента и цифровых сервисов, системой регистрации пользователей [22]. SHOMA позволяет властям отслеживать контент на основе политических, культурных и религиозных критериев, однако контроль за данными и трафиком в этой сети ограничивает конфиденциальность и защиту данных иранских пользователей, нарушает право на свободу слова[25]. Как показал опыт эксплуатации SHOMA, у пользователей она не пользуется популярностью, зато для обхода ограничительных мер возросло применение различных прокси-средств, активно поставляемых США и их союзниками (в том числе с использованием технологии космической связи, ПО Psiphon и Lantern) [23].

---

23 По опубликованным данным стоимость развертывания только инфраструктуры оценивается в 6 млрд долл. США. Разработка поисковой системы оценена в 1,5 млрд, приложения для обмена сообщениями в 135 тыс.
Источник: Iran's National Information Network: Faster Speeds, but at What Cost?, *Feb 21, 2018* https://cyber.harvard.edu/node/100145.

24 Китай оказал содействие в осуществлении проекта. Источник: China to Help Iran Implement Its Closed National Internet – Center for Human Rights in Iran, https://iranhumanrights.org/2014/01/china-iran-internet/.

25 Иран на протяжении многих лет входит в первую пятерку стран мира по уровню цензуры, нарушению права на доступ к информации и свободы слова.

3. Состояние нормативно-правовой базы в сфере развития ИКТ, обеспечения национальной и международной информационной безопасности

Правовое обеспечение безопасного использования ИКТ является важным компонентом стратегии кибербезопасности любого государства [24]. Нормативно-правовая база информационной безопасности Ирана утверждена Высшим советом национальной безопасности. При ее формировании особое внимание уделено решению следующих основных задач:

- развитию законодательной базы, регламентирующей информационную политику и функциональные действия государственных органов;
- налаживанию связей и сотрудничества с иностранными государствами в сфере обеспечения информационной безопасности;
- разработке собственного программного обеспечения, позволяющего удовлетворить потребности иранского населения;
- созданию SHOMA и образовательной/научной компьютерной сети высших учебных заведений Ирана;
- созданию национальной поисковой системы;
- обеспечению беспрепятственного доступа правоохранительных органов Ирана к данным о состоянии информационной безопасности, а также предоставления им возможности мониторинга активности пользователей;
- обязательной подготовке населения страны в области обеспечения информационной безопасности
- реализации комплекса мер, исключающего или минимизирующего возможность анонимного доступа к сети Интернет;
- организация долговременного хранения архивов с адресами посещаемых веб-сайтов и анализ деятельности интернет-пользователей.

На данном этапе уровень зрелости правового регулирования цифровизации в Иране по новой методике оценки МСЭ[26] оценивается как переходный, т.е. использующий поэтапный подход.

3.1. **Конституция Ирана** (1979)

Согласно статье 4 Конституции «все гражданские, уголовные, финансовые, экономические, административные, культурные, военные, политические нормы

26 В методике «G5 Benchmark» оцениваются 4 параметра: межотраслевое управление на национальном уровне, принципы разработки политик, Инструментарий цифрового развития (кибербезопасность, защита данных, телекоммуникации в чрезвычайных ситуациях и совместное использование межотраслевой инфраструктуры), повестка дня в области цифровой экономики (инновационная система, цифровая трансформация, участие в международных и региональных интеграционных инициативах).

и любые другие законы должны основываться на принципах ислама. Эти принципы главенствуют над всеми нормами Конституции и другими нормативными правовыми актами». Преступления против бога и государства, в том числе совершенные с использованием Интернета, считаются самыми тяжкими. Так статья 24 гласит, что «публикации и пресса обладают свободой выражения мнений», однако включает в себя оговорку о том, что не должно быть «нарушения основных принципов ислама или общественных прав». Могут быть введены и другие ограничения: например, статья 40 допускает ограничения прав, если их осуществление считается «вредным для других» или «наносящим ущерб общественным интересам». По сути, здесь нет юридических новаций, но присутствует вопрос к вольности трактовки использованных понятий.

В 2012 году Верховному совету по киберпространству было поручено сформулировать политику Ирана в отношении Интернета, а также разработать планы его регулирования в соответствии с Конституцией. В 2014 году была озвучена доктрина «Официальной системы идентификации в киберпространстве», согласно которой государству будут предоставлены полномочия по идентификации всех интернет-пользователей (данные о практической реализации системы в открытом доступе отсутствуют).

3.2. **Уголовный кодекс** (1991)

Уголовный кодекс (УК) представляет собой нормативный правовой акт, состоящий из пяти отдельных книг, принятых в разные периоды времени. Он является основным и наиболее важным источником уголовного права, в котором кодифицированы преступления и принципы уголовного наказания по шариату.

В соответствии с УК преступлением считается публикация в Интернете любого материала, оскорбляющего исламскую доктрину, ценности иранской революции, мысли имама Хомейни и Конституцию Ирана, ставящего под угрозу национальное единство страны, создающего положительный имидж незаконных организаций, разглашающего секретную информацию, содержащего рекламу курения, обвиняющего или оскорбляющего чиновников. Так Статья 500 гласит, что любой, кто занимается любого рода пропагандой против Исламской Республики Иран или поддерживает оппозиционные группы и ассоциации, должен быть приговорен к лишению свободы на срок от трех месяцев до года. Однако в законодательстве не содержится конкретного определения термина «пропаганда», что дает судьям широкие полномочия для квалификации сообщений пользователей [25].

3.3. Закон о компьютерных преступлениях (2009)

Закон № 71063 кодифицирует широкий ряд преступлений, связанных с использованием компьютеров и хранящихся в них цифровых данных, определяет строгие наказания за нарушение норм закона, а также процедуры судебного преследования по этим преступлениям [26]. Закон имеет и экстерриториальное применение — граждане Ирана и иностранцы, находящиеся вне границ страны, подпадают под действие закона, если преступление совершены в отношении компьютеров, телекоммуникационных систем и веб-сайтов трех ветвей государственной власти ИРИ.

Основные типы правонарушений против конфиденциальности, целостности и доступности данных и компьютерных систем:

- преступления против конфиденциальности данных и компьютерных систем посредством несанкционированного доступа к ним, а также компьютерное мошенничество с данными (если данные были секретными, то наказание в два раза строже);
- уничтожение или вмешательство в данные и компьютерные системы (неправомерное сообщение номеров, кодов, паролей или других средств доступа к любому компьютеру);
- кража и мошенничество в отношении компьютеров;
- преступления против милосердия и общественной морали, распространение порнографического контента;
- унижение достоинства, распространение угроз, лживой информации и новостей (заключение под стражу на срок до 2 лет);
- шпионаж (под которым понимается нарушение мер безопасности передачи и хранения секретных данных) и разглашение данных доступа зарубежным государствам, организациям, компаниям или группам и их агентам (до 15 лет тюрьмы);
- использование Интернета для террористической деятельности, включая кибертерроризм (до 10 лет заключения).

Лишением свободы до 1 года и/или штрафом от 5 до 20 млн риалов карается соучастие в преступлениях (действия по производству, распространению, обеспечению доступа, или торговля данными, программным обеспечением, вредоносным программным обеспечением, электронными устройствами для совершения компьютерных преступлений; распространение или предоставление доступа к обучающим материалам и контенту для совершения преступлений; продажа и распространение паролей или доступа к ним или любых данных посторонним людям).

3.4. **Закон об электронной коммерции** (2004)

Помимо обязательств сторон по виртуальным сделкам закон касается защиты прав продавцов и покупателей, в том числе, обеспечения безопасности данных электронных транзакций (Статьи 59–61).

Владельцы бизнеса электронной коммерции обязаны предпринимать меры по обеспечению сетевой безопасности: идентификации и аутентификации клиентов и поставщиков; внедрять меры авторизации для получения услуги; обеспечивать конфиденциальность полученных данных и доступность сервиса; администрировать политики безопасности; регулярно проверять их адекватность угрозам; реагировать на инциденты безопасности [27].

Закон также определяет «безопасную информационную систему» как адекватно защищенную от мошенничества или проникновения систему, процессы в которой администрируются на требуемом уровне и применяются соответствующие меры безопасности (проверка отправителя и получателя, выявление ошибок и модификаций в контенте, коммуникациях и местах хранения данных).

За нарушение правил обработки персональных данных грозит от 1 до 3 лет тюрьмы (Статья 71).

3.5. **Проект закона о безопасности персональных данных и защите** (2019)

Это первая попытка разработать нормативный правовой акт, определяющий общие принципы и правила обработки персональных данных (ПД) с учетом международных стандартов защиты информаии и обеспечения прав человека. Частично это решалось другими законами, где безопасность обладателей ПД была критична — суды и адвокатура, медицина и фармацевтика, электронная коммерция.

Проект включает требования локализации на территории страны обработки ПД граждан Ирана и данных национальных компаний или обработки их за рубежом только уполномоченными операторами.

Операторам обработки ПД вменяется в обязанность обеспечение безопасности данных, недопущение неавторизованного доступа, использования, изменения и уничтожения данных. По аналогии с Общим регламентом безопасности данных ЕС (GDPR) закон вводит право на забвение, а также создание независимого органа для контроля исполнения норм закона и защиты прав обладателя ПД [28]. Проект был внесен в парламент, но отклонен.

3.6. Проект закона о защите прав пользователей киберпространства и регулирование ключевых онлайн-сервисов (2021)

Законопроект, известный также под названием «Биль о защите»[27], был внесен в меджлис в июле 2021 года, в феврале 2022 года ратифицирован, но голосование было отменено регламентным отделом парламента. Его содержание важно для понимания ориентации правительства на увеличение контроля киберпространства путем централизации всех властных полномочий в отношении регулирования Интернета в одном государственном органе.

Законопроектом предлагалось передать Высшей комиссии по регулированию (SRC)[28] регуляторных и контролирующих функций, которые на данный момент относятся к Министерству ИКТ, Комитету по определению оскорбительного контента (CCDOC) и даже Высшему совету киберпространства, а именно:

- регулирование монополии на всех рынках, связанных с ИКТ, включая связь и онлайн-сервисы;
- регулирование, мониторинг и оценка деятельности организаций, предлагающих коммуникационные и ИТ-услуги;
- регулирование и надзор за проектами электронного управления и электронного банкинга;
- регламентирование применения иностранного программного обеспечения, необходимого для разработки и расширения местных сервисов;
- определение «ключевых» онлайн-услуг и требований к ним, выдача, продление и аннулирование их лицензий;
- регулирование личного, делового и государственного использования «ключевых» онлайн-сервисов;
- надзор за деятельностью иранского государства и правительственных чиновников на нелицензированных иностранных платформах;
- контроль разработки, распространения и использования виртуальных частных сетей (VPN) и прокси-сервисов, используемых для обхода введенных ограничений и доступа к заблокированному контенту;
- разработка правил и механизмов аутентификации и идентификации пользователей;

27 Под «защитой» понимается намерение правительства оградить иранских пользователей от контента, который считает «гнусным», неисламским, западным или продвигаемым «вражескими» элементами. Источник: Iran: Parliament's "Protection Bill" will Hand Over Complete Control of the Internet to Authorities, ARTICLE19, 2022, https://www.article19.org/resources/iran-parliaments-protection-bill-will-hand-over-complete-control-of-the-internet-to-authorities/.

28 Это орган Высшего совета киберпространства, состоящий из трех членов Высшего совета киберпространства, руководителей всех силовых структур, профильных министров, трех членов офиса премьер-министра и нескольких представителей ИКТ-отрасли (последние без права голоса), всего 21 человек.

- выработка правил и руководящих принципов в отношении конфиденциальности пользователей, киберграмотности, онлайн-рекламы и авторских прав;
- передача данных о любом нарушении законодательства в соответствующие судебные органы;
- регулирование международного сотрудничества в киберпространстве;
- предоставление Высшему совету киберпространства, парламенту и другим соответствующим органам регулярных отчетов об иранском киберпространстве, ИТ-услугах и «ключевых» онлайн-сервисах.

Кроме того, законопроект обязывал международные технологические компании назначать законного представителя в Иране для контроля соблюдения местных законов и сотрудничества с правительством в наблюдении за пользователями и цензуре онлайн-пространства[29]. Платформы, которые откажутся от соблюдения правил, будут подвергаться ограничению пропускной способности до тех пор, пока им не будут созданы иранские альтернативы [29].

4. Государственные органы, входящие в систему обеспечения информационной безопасности и форматы государственно-частного партнерства

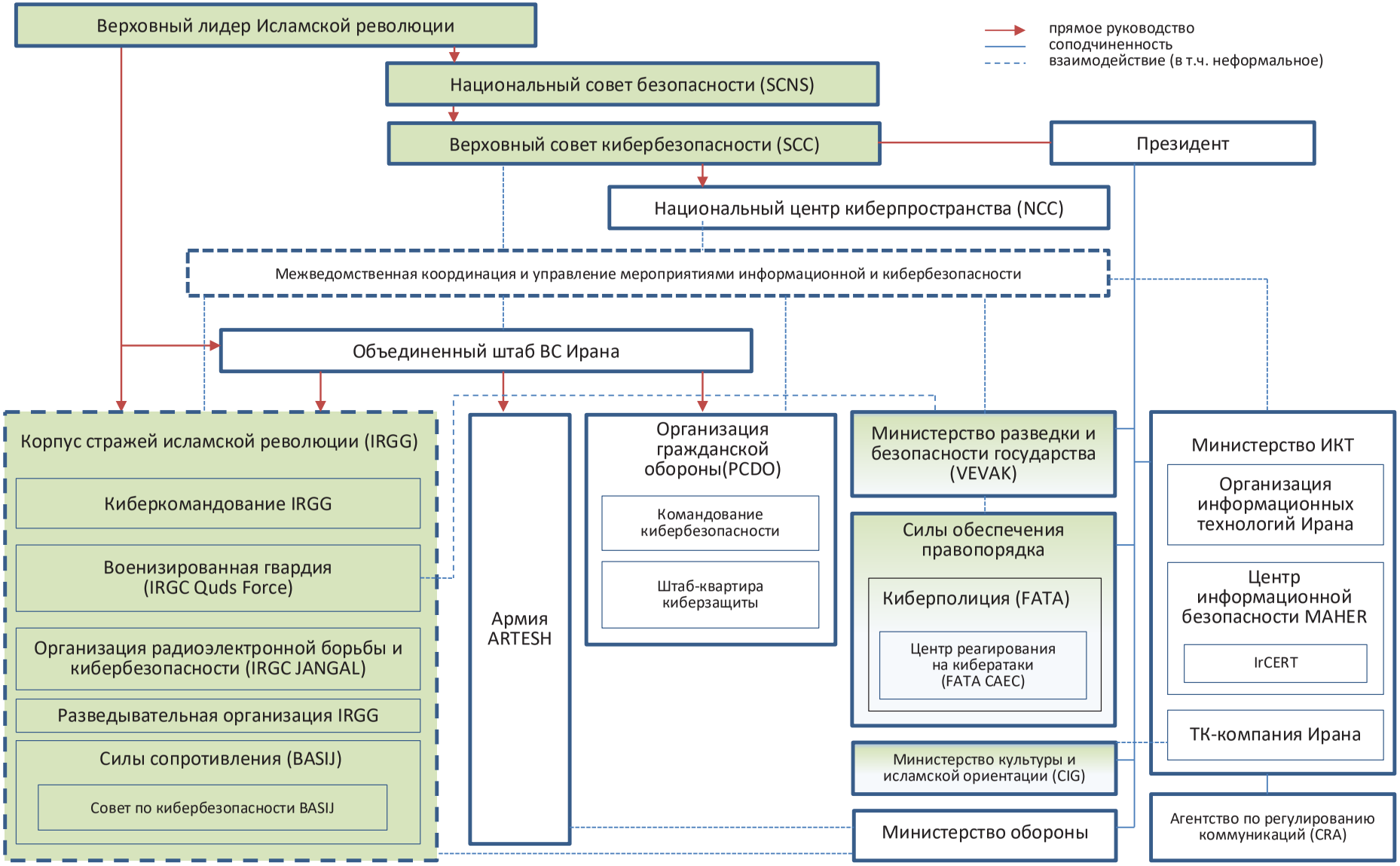
Как уже отмечалось, система государственного управления Исламской Республики Иран является уникальным примером синтеза авторитарного теократического режима с элементами светского правления (парламентаризм и выборные процессы), что отражается на структуре и взаимодействии органов управления в рассматриваемой сфере.

Верховный лидер страны[30] (рахбар, перс. факих) обладает полномочиями, имеющими верховенство по отношению ко всему механизму государственной власти [30]. Рахбар является главой государства, верховным главнокомандующим Корпуса стражей Исламской революции, реализует ряд функций законодательной, исполнительной и судебной власти, утверждает своим указом президента страны, назначает основных должностных лиц в государстве. В его непосредственном подчинении находятся следующие органы.

29 В марте 2016 года поисковой системе Яндекс был заблокирован доступ к местному рынку за несоблюдение иранской политики и «национальных ценностей». Несколько месяцев спустя было подписано новое соглашение с компанией Yandex.ir, зарегистрированной под управлением Вещательного агентства Исламской Республики Иран, Источник: Iran's Tech Co-operation with China and Russia, July 27, 2017, https://intpolicydigest.org/iran-s-tech-co-operation-with-china-and-russia/.

30 С 1989 года этот пост занимает Его Светлость Аятолла Али Хаменеи, до этого он два срока был президентом Ирана.

Схема. Основные элементы системы управления информационной безопасностью ИранаИспользованная литература



4.1. **Верховный совет национальной безопасности** (SCNS)

Совет назначается и возглавляется рахбаром, выполняет роль межведомственного политического органа, который вырабатывает политику и осуществляет стратегическое планирование в сфере безопасности государства.

4.2. **Верховный совет кибербезопасности** (SCC)

Создан на основании указа Верховного лидера от 2012 года, как ядро системы защиты национального информационного пространства[31]. Председателем SCC является президент Ирана (второе лицо в государстве). По должности в этот орган входят: спикер меджлиса Исламского совета (парламента), глава Верховного суда, руководитель государственной Иранской организации радио и телевидения (IRIB), по конституции подчиняющейся рахбару, секретарь SCC и одновременно директор Национального центра киберпространства, целый ряд профильных министров (связи, информационных и коммуникационных технологий, культуры и исламской ориентации, научных исследований и технологий, разведки и безопасности государства), председатель комиссии по культуре меджлиса Исламского совета, директор организации по исламской пропаганде, главнокомандующий Корпуса стражей Исламской революции и командующий Силами охраны правопорядка. Также в Совете есть 7 должностей на которые назначаются действительные (не юридические) члены сроком на три года, как правило это ученые и эксперты без права решающего голоса [31].

Основными задачами SCC являются: выработка концепции информационной политики государства, концепции формирования информационного общества в Иране, стратегии действий в сфере кибербезопасности, разработка и утверждение регламентирующих деятельность государственных органов в сфере ИКТ нормативных документов, реализация программы международного сотрудничества Ирана в ИКТ-сфере. Эти задачи решаются профильными комиссиями, состоящими из руководителей уполномоченных органов. Секретариат и рабочие органы Совета размещаются в государственном агентстве — Организации информационных технологий, созданной при Министерстве информационных и коммуникационных технологий (см. Раздел 4.8).

31 До этого момента деятельность в интернет-пространстве контролировалась Верховным советом культурной революции.

4.3. **Национальный центр киберпространства** (NCC)

Создан в 2016 году на основании указа Верховного лидера от 2012 года. Он подчиняется Высшему совету кибербезопасности и решает широкий круг задач. Для этого в структуре центра образовано несколько профильных высших комитетов, в том числе Высший комитет регулирования политики в области киберпространства (SCCPR), Высший комитет по безопасности киберпространства (SCCS), Высший комитет по совершенствованию и производству контента в киберпространстве (SCIPCC) [32].

4.4. **Корпус стражей Исламской революции** (IRGC)

В 2009 году сразу после подавления волнений «арабской весны» руководством Ирана были сделаны серьезные политические выводы и создан Корпус стражей Исламской революции (КСИР, англ. IRGC, перс. Pasdaran). Он напрямую подчиняется Верховному лидеру. Возглавляется старшим бригадным генералом. Подразделения и соединения КСИР состоят из служащих по контракту членов религиозно-политических группировок Ирана шиитского толка, уже прошедших срочную службу.

В КСИР сосредоточены основные силы и средства по защите национального киберпространства и осуществлению наступательных, разведывательных и защитных кибероперациий как на территории страны, так и за рубежом, также корпус выполняет задачи по физической охране наиболее важных объектов ИКТ-инфраструктуры. Западные эксперты, хоть и отмечают отставание КСИР от ведущих мировых держав в технологической сфере, но высоко оценивают его потенциал. По мнению разведывательных служб США, КСИР представляет серьезную угрозу для них и их союзников, в том числе на Ближнем Востоке [33].

Для координации действий различных структур КСИР, в том числе тридцати одного регионального командования в провинциях, создано **Киберкомандование КСИР**. Ему подчинены следующие силы: **Военизированная гвардия** (IRGC Quds Force, QF), которая осуществляет разведывательные и наступательные кибероперации вне территории страны и взаимодействует с национальной службой разведки; **Организация разведки КСИР**, которая создана в 2009 году и считается более мощной, чем Министерство разведки и безопасности; **Организация радиоэлектронной борьбы и кибербезопасности** (IRGC JANGAL).

Самостоятельная ветвь КСИР — **Силы сопротивления BASIJ** представляют собой добровольческую полувоенную организацию (военизированное ополчение), численность которой оценивается в 11 млн человек. В своей структуре также имеет **Совет по кибербезопасности BASIJ** с функциями управления и ин-

фраструктурного обеспечения мероприятий по информационной безопасности, кибершпионажа в отношении внутренних и внешних объектов, мониторинга оперативной обстановки в информационном пространстве, осуществления пропагандистской деятельности с публикацией тематических материалов в блогах и на специально созданных интернет-сайтах, а также размещением в киберпространстве комментариев к популярным видеоматериалам и статьям. По некоторым данным в полномочия BASIJ входит подготовка и вербовка хакеров в интересах КСИР и спецслужб [34].

4.5. Организация гражданской обороны

Организация гражданской обороны (англ. PCDO) создана в 2003 году, входит в структуру Объединенного штаба вооруженных сил Ирана[32] и является органом межведомственной координации и управления мероприятиями по обеспечению обороноспособности государства и гражданской обороны в случае военных действий.

В 2010 году в PCDO создано **Командование кибербезопасности** для управления действиями по обеспечению информационной безопасности и кибероперациями. В 2011 году после инцидента с вирусом Stuxnet при PCDO создана **Штаб-квартира киберзащиты** для обеспечения безопасности национальных критических инфраструктур и координации реагирования на компьютерные инциденты на их объектах. Ей даны полномочия использования всех национальных ресурсов, в т.ч. киберсредств, для выявления, предотвращения, идентификации и эффективного противодействия компьютерным атакам на национальные информационные системы и ресурсы со стороны зарубежных государств или поддерживаемых ими групп (в т.ч. местных). Штаб-квартира киберзащиты может заключать договоры с различными государственными, военными организациями и службами безопасности для эффективного сотрудничества и координации совместных действий[33].

4.6. Министерство разведки и безопасности государства (VEVAK)

Министерство разведки и безопасности государства (перс. Vezarat-e Ettela’atvaAmniyat-e Keshvar, VEVAK), в англоязычных источниках часто назы-

32 Вооруженные силы Ирана включают регулярную армию Artesh и Корпус стражей исламской революции. Согласно ежегодному рейтингу Global Firepower, в 2023 году совокупная военная мощь Иран поставлена на 17 место, Израиля на 18, а Турции на 11 (ядерный арсенал не учитывался). Вместе с КСИР армия Ирана имеет численность 860 тыс. военнослужащих, что делает ее одной из крупнейших армий мира. Источник: 2023 Iran Military Strength, https://www.globalfirepower.com/country-military-strength-detail.php?country_id=iran.

33 Американские эксперты говорят о сотрудничестве PSDO с Сирией, Ираком, ливанской кибер Хезболлой.

ваемое Министерством информации, формально подчинено правительству, но действует как независимый орган. Министра назначает рахбар, кандидат должен иметь степень в области иджтихада (способность интерпретировать исламские источники, такие как Коран и слова Пророка и имамов), воздерживаться от членства в какой-либо политической партии или группе, а также обладать политическим и административным опытом.

Главной задачей VEVAK является добывание стратегической разведывательной информации о планах и действиях враждебных Ирану стран в сфере информационного противоборства, борьба с особо опасными государственными преступлениями с применением информационных технологий, противодействие враждебному воздействию на информационные системы и другие объекты. VEVAK осуществляет надзор за этническими меньшинствами, выявляет диссидентов, преследует террористические организации. Министерством используются все имеющиеся средства, в том числе такие методы как проникновение в оппозиционные группы, мониторинг внутренних угроз, борьба со шпионажем и поддержание связей с иностранными спецслужбами и организациями, защищающими интересы Исламской Республики по всему миру. Согласно Конституции Ирана, все ведомства и организации обязаны предоставлять VEVAK необходимые данные [35].

4.7. Силы обеспечения правопорядка и Киберполиция (FATA)

Силы обеспечения правопорядка (перс. NAJA) являются Министерством внутренних дел Ирана. В 2011 году в их структуре для расследования компьютерных преступлений создано специальное подразделение **Киберполиция** (перс. FATA). В нем с 2016 года действует автоматизированная система уведомления о совершенных компьютерных преступлениях (интернет-мошенничество, кража данных и нарушение частной жизни, фишинг, взлом ресурсов, и др.) [36].

Другим направлением деятельности FATA является подавление инакомыслия. С этой целью она занимается мониторингом контента Facebook, Twitter и других социальных сетей, пользующихся популярностью у оппозиции и диссидентов, интернет-трафика и контента пользователей, выявлением запрещенного контента, а также проводит кибероперации, в том числе в отношении оппозиционных партий и диссидентов. Кроме того, в функционал FATA входит инспекция деятельности западных новостных агентств, аккредитованных в Иране, блокировка или ограничение работы недружественных Интернет-ресурсов.

Еще одной задачей FATA является сокращение неавторизованного доступа к Интернету, для этого продвигается новая биометрическая идентификационная карта для выхода иранцев в сеть [37].

FATA установила рабочие контакты с примерно 100 государствами мира, она обеспечивает участие иранских экспертов в работе Конференции по киберпреступности (Europol — Interpol) и ежегодной Неделе кибербезопасности, проводимой по линии европейского отделения Interpol. Также FATA участвует в международной операции «Operation Pangea» под эгидой Interpol по противодействию незаконной онлайн-продаже фальсифицированных медикаментов и лекарственных средств [38].

4.8. Министерство информационных и коммуникационных технологий

Министерство ИКТ создано в 2003 году. Занимается вопросами развития ИКТ-отрасли и организации всех видов связи, разработкой и реализацией программ управления страной с помощью телекоммуникационной и информационной инфраструктуры (спутниковые, радиорелейные, волоконно-оптические и др.). Важнейшую роль в выполнении этих функций играет **государственная телекоммуникационная компания Ирана** (ITC), которая является подразделением министерства. Через подведомственное **Агентство по регулированию коммуникаций Ирана** (CRA) осуществляется выработка требований и лицензирование деятельности операторов связи.

Организация информационных технологий Ирана создана в 2010 году как государственное агентство[34], возглавляется заместителем министра ИКТ по стратегическому развитию. Занимается главным образом техническими вопросами: развитие Интернета и Национальной информационной сети SHOMA, услугами электронного правительства, стартапами, разработкой программного обеспечения, безопасностью информации, сетей, программного и аппаратного обеспечения.

В структуре министерства действуют Телекоммуникационный исследовательский центр и **Центр информационной безопасности MAHER**, отвечающий за анализ киберугроз и вредоносного программного обеспечения, разработку средств защиты и методов реагирования на чрезвычайные ситуации. MAHER активно участвует в международном сотрудничестве, он член группы реагирования Организации исламского сотрудничества OIC-CERT и Международного партнерства по борьбе с кибертерроризмом ITU-IMPACT. В 2008 году на базе MAHER создана национальная группа реагирования на компьютерные инциденты в интернет-пространстве **IrCERT**[35]. Эта группа координирует деятельность

34 С 1998 года действовала как государственная компания «ITC Information Technology Company, Data communications corporation or Data works».
35 IrCERT также является членом OIC-CERT.

всех иранских групп реагирования, в том числе критически важных отраслей, телекома и крупнейших профильных технических ВУЗов. IrCERT является членом международного Форума групп реагирования FIRST и участником корейской инициативы CAMP (платформа для повышения общего уровня кибербезопасности участников посредством обмена опытом развития и тенденциями).

4.9. Министерство культуры и исламской ориентации (CIG)

Министерство и подчиненная ему Организация культуры и исламских связей являются главными пропагандистскими и контрпропагандистскими организациями, сфера деятельности которых распространяется как на территорию Ирана, так и на зарубежные страны. На министерство возложены также контрольно-цензорские функции надзора за деятельностью иранских СМИ и зарубежного журналистского корпуса, а также Интернет-провайдеров, цензура ввозимой в Иран печатной, кино- и видеопродукции, телевизионных материалов, программного обеспечения, контроль деятельности организаций гражданского общества.

4.10. Государственно-частное партнерство в сфере обеспечения информационной безопасности Ирана

В западных открытых источниках в сфере обеспечения кибербезопасности Ирана отмечается только один вид «партнерства» государства с частным сектором, который заключается в привлечении идеологически приверженных правящему режиму хакерских сообществ к осуществлению компьютерных атак на врагов республики и ислама.

Западные компании в сфере информационной безопасности считают аффилированными (highly likely) с правительством высокопрофессиональные хакерские группы, причастные к резонансным компьютерным атакам в разных регионах мира. По типу целей, использованному инструментарию и другим параметрам они условно именуют эти группы, при этом разные названия могут соответствовать одной группе. Наиболее часто упоминаются следующие группы: APT42, APT33, APT35, APT39, MuddyWater, Charming Kitten, Pioneer Kitten, Rocket Kitten, Copy Kitten, Magic Kitten, Sun Army, Infy, Leafminer, OilRig, Chafer [39]. Невозможно сказать каким образом эти наименования соответствуют реально существующим иранским хакерским сообществам, которые, как правило, берут на себя ответственность за успешно совершенные кибероперации (Iranian Cyber Army, Ashiyane, Tarh Andishan, Islamic Cyber Resistance Group, Cyber Fighters of Izz ad-Din al-Qassam, Sword of Justice, Ajax Security Team, Parastoo, Shabgard, Iran Black Hats, Cocaine Warriors from Persia, Cadelle, Chafer) [40].

Также аффилированными с киберкомандованием западники считают научные центры и ведущие технические ВУЗы, готовящие специалистов в области информационной безопасности: Центр информационных технологий и кибербезопасности при Тегеранском университете, Исследовательский институт по киберпространству при Университете имени Шахида Бехешти, Центр перспективных информационных и телекоммуникационных технологий и Институт перспективных коммуникационных исследований при Технологическом университете имени Шарифа[36].

На Университет имени Шахида Бехешти в связи с ядерными исследованиями давно наложены санкции США [41], Канадой, ЕС[37], Австралией и Швейцарией. Кроме того, ЕС введены санкции в отношении руководства КСИР и Организации гражданской обороны [42], а американский Фонд защиты демократии настоятельно рекомендует правительству:

включить в санкционный список за содействие в подготовке кадров для осуществления компьютерных атак Университет имени Шахида Бехешти и Технологический университет имени Шарифа [43];

разработать и реализовать план наступательной киберкампании против Ирана, который включает как сдерживание развития иранского ИКТ-сектора и введение санкций на его руководителей и предполагаемых исполнителей вредоносной деятельности в отношении США и их союзников, так и выстраивание Ближневосточной коалиции против Ирана через укрепление сотрудничества с Израилем по защите КИИ и осуществлению атак на сети Ирана;

усилить развертывание группировки спутников Starlink для расширения деятельности диссидентов, а также предоставить им другой инструментарий [44].

5. Участие в международном сотрудничестве с ООН и другими международными и региональными организациями в области формирования системы международной информационной безопасности

По оценке МСЭ, в последние годы Иран расширяет сотрудничество с целью повышения уровня взаимосвязей с другими государствами в области кибербезо-

36 Следует отметить, что подготовка кадров в области информационных технологий в Иране осуществляется на высоком уровне, большое количество университетов и институтов осуществляет программы обучения по передовым ИКТ, таким как искусственный интеллект (120 ВУЗов), машинное обучение (118), нейросети (104), когнитивные науки (97), сетевые вычисления (89), компьютерное зрение (88), компьютерная лингвистика (50), блокчейн и криптография (41). В мировой список ведущих учебных учреждений в сфере кибербезопасности вошли 84 иранских ВУЗа. Источник: Iran's 84 best Cyber Security universities [2023 Rankings], https://edurank.org/cs/cybersecurity/ir/.

37 В 2023 году ЕС исключил из санкционного списка 18 физических лиц и 19 организаций, обвиненных в 2011 году в содействии нарушению свободы слова, ограничению доступа к Интернет и блокированию западных соцсетей, Источник: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L:2023:020I:FULL&from=EN.

пасности, снижения киберрисков и обеспечения их более эффективного расследования [45].

В условиях американской политики изоляции страны, Тегеран в сфере международного сотрудничества отдает приоритет развитию взаимодействия со странами и организациями, проводящими, по его мнению, независимую от Вашингтона политику (прежде всего Россия и Китай). Такой подход обусловлен стремлением иранских властей обеспечить собственную информационную безопасность. Эта направленность внешней политики усиливается в связи с опасной эскалацией ситуации на Ближнем Востоке и возможным вовлечением Тегерана в вооруженный конфликт.

5.1. ООН

В целом Иран разделяет российские подходы к формированию системы международной информационной безопасности, а также инициативы Москвы в ООН по данной тематике. В частности, Иран стал соавтором инициированной Россией резолюции Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» (A/RES/73/27 от 8 ноября 2018 года)[38], на основании которой была создана первая Рабочая группа ООН открытого состава (РГОС) по вопросам безопасности использования ИКТ и самих ИКТ (2019-2021), а затем была поддержана резолюция по продлению работы этой группы (A/RES/76/19 от 6 декабря 2021 года).

Кроме того, он активно участвует в субстантивных сессиях и работе над текущим проектом доклада РГОС. Наиболее важные позиции Ирана следующие.

По нормам ответственного поведения. Иран выступает за разработку дополнительных норм ответственного поведения. Он отметил, что в отчете ГПЭ 2015 года приоритет отдается достаточности выполнения добровольных норм и исключается необходимость ведения переговоров по юридически обязательному документу. При этом Тегеран категорически против того, чтобы называть предложения по внедрению одобренных норм (ГПЭ 2015) «ориентированными на действия», и считает, что принятие такого подхода превращает их в предлагаемую Канадой и Египтом «Программу действий» для реализации рамок отчета ГПЭ 2015, что противоречит мандату РГОС.

Наращивание потенциала и меры доверия. Иран считает, что только те заинтересованные стороны, аккредитация которых уже была одобрена государствами на основе заведомых возражений, в соответствии с согласованными ус-

38 На этой же сессии Иран проголосовал против американской инициативы по созданию конкурирующей с РГОС новой ГПЭ по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности (A/RES/73/266 от 22 декабря 2018 года).

ловиями, могут заниматься аспектами наращивания потенциала. При этом национальные системы, механизмы и приоритеты должны быть обеспечены при любом взаимодействии с заинтересованными сторонами по аспектам мер укрепления доверия [46].

Применимость международного права. Иран совместно с Ираком, Кубой и Сирией поддержали разработку нового юридически обязывающего документа. Иран хотел бы, чтобы он определял ИКТ-терминологию и принципы международного права, предложив семь принципов, включая, но не ограничиваясь ими: принципы невмешательства во внутренние дела других государств, наряду с суверенным равенством в работе Справочника контактных пунктов[39]; принцип, позволяющий этим пунктам и их ресурсам не подвергаться ограничительным и блокирующим мерам, включая односторонние принудительные меры (UCM). Также Иран предложил Секретариату ООН запросить мнения государств о потенциале, необходимом для участия контактных пунктов в Справочнике, и о подходящих механизмах и действиях для создания такого потенциала [47].

В 2019 году на Генеральной ассамблее ООН Иран проголосовал за российский проект резолюции «Противодействие использованию информационно-телекоммуникационных технологий в преступных целях» (A/RES/74/247 от 27 декабря 2019 года), на основании которой в Третьем комитете ООН создан Специальный межправительственный комитет экспертов открытого состава для разработки всеобъемлющей международной конвенции о противодействии использованию ИКТ в преступных целях.

5.2. **Шанхайская организация сотрудничества** (ШОС)

В июне 2023 года Иран стал членом ШОС, но еще в 2009 году Тегеран принял на себя обязательства ШОС по международной информационной безопасности.

С 1 января 2024 года Иран стал полноправным членом БРИКС, что потребует расширения сотрудничества в сфере обеспечения безопасности ИКТ и передовых технологий. Новые вызовы в этой сфере иранское руководство прогнозирует на фоне вооруженного конфликта Израиля и группировки ХАМАС, спровоцировавшего обострение отношений Тегерана с Тель-Авивом и его западными союзниками [48].

---

39 В рамках деятельности РГОС основные элементы разработки и введения в действие глобального межправительственного реестра контактных пунктов сформулированы. Источник: Второй ежегодный доклад о проделанной работе, представленный Рабочей группой открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025 (A/78/265 от 1 августа 2023 года), https://digitallibrary.un.org/record/4020967?ln=en&v=pdf).

Официально Иран также выступает за создание международных и региональных органов для борьбы с кибертерроризмом и интернет-мошенничеством, в том числе в рамках ШОС и ООН.

5.3. **Евразийский экономический союз** (ЕАЭС)

С 2019 года действовало Временное соглашение, ведущее к образованию зоны свободной торговли между ЕАЭС и Ираном[40]. В документе, в частности, акцент сделан на том, что приоритет в обмене таможенной информацией отводится электронному формату. Это ставит задачу обеспечения информационной безопасности обмена данными в соответствии с межгосударственными стандартами информационной безопасности ЕАЭС, которые основываются на российских стандартах.

14 марта 2022 года подписан Протокол к Временному соглашению, предусматривающий продление его применения на три года или до вступления в силу соглашения о свободной торговле. Протокол вступил в силу 25 октября 2022 года, тем самым обеспечив неразрывность преференциального режима, действующего между ЕАЭС и Ираном. В декабре 2023 года в рамках заседания Высшего Евразийского экономического совета страны ЕАЭС подписали полноформатное соглашение о свободной торговле с Ираном [49].

5.4. Двустороннее сотрудничество

Объем и география двустороннего сотрудничества Исламской Республики Иран с другими странами в сфере развития ИКТ и обеспечения их безопасности показывает, что потенциальные партнеры вынуждены скрупулезно оценивать риски прямых и вторичных санкций США и их союзников.

5.4.1. Китайская Народная Республика

В последнее время Иран и Китай подчеркивают, что история их взаимодействия началась с древнего Шелкового пути и насчитывает уже 2500 лет, и это — отношения древнейших цивилизаций. В последние 50 лет пишется новая страница сотрудничества, которое «выдержало испытания изменчивой международной ситуацией и демонстрирует устойчивый прогресс». Экономи-

40 Временное соглашение, ведущее к образованию зоны свободной торговли между Евразийским экономическим союзом и его государствами-членами, с одной стороны, и Исламской Республикой Иран, с другой стороны от 17 мая 2018 года (ратифицировано Федеральным законом от 28 ноября 2018 года № 429-ФЗ, вступило в силу 27 октября 2019 г.), http://publication.pravo.gov.ru/Document/View/0001201910280037?index=13.

ческие отношения стали более тесными, последние 10 лет Пекин — основной торговый партнер Ирана[41] и один из его главных инвесторов[42].

Иран является «замковым камнем» в китайской инициативе «Один пояс, один путь», создавая возможность интеграции морского и сухопутного трансконтинентального торгового коридора между Ближним Востоком, Центральной Азией, Кавказом и Европой. Иран заинтересован в обходе американских санкций, притоке инвестиций, модернизации производства и выходе на новые рынки. Меморандум о взаимопонимании по сотрудничеству в рамках указанной инициативы заключен в ходе визита Си Цзиньпина в Иран в 2016 году. В ИКТ-сфере это позволило модернизировать инфраструктуру связи в ИРИ. При существенных объективных сложностях в международных отношениях компания Huawei развернула в стране на своем оборудовании сети мобильной связи 4G и 5G.

В 2021 году двусторонние отношения были повышены до уровня всеобъемлющего стратегического партнерства — Тегеран и Пекин подписали Соглашение о стратегическом сотрудничестве на 25 лет [50], включающее экономическую, политическую, военную, культурную, социальную, образовательную, научную и другие сферы, в том числе кибербезопасность[43]. По соглашению Китай инвестирует в инфраструктурные проекты в Иране 400 млрд долл. США и будет способствовать воплощению инициативы «Один пояс, один путь» [51].

В феврале 2023 года соглашение вступило в силу, и в рамках его реализации уже подписано 20 документов о сотрудничестве и меморандумов о взаимопонимании, обозначены несколько областей взаимного сотрудничества, включая антикризисное управление, коммуникационные и информационные технологии, интеллектуальную собственность, продвижение банковского, финансового и страхового сотрудничества, СМИ и культурное наследие [52].

Следует также отметить, что КНР всегда стремится выстраивать долгосрочные программы развития партнерства, прежде всего используя инструменты «мягкой силы». Например, в свободной зоне Чабахар в южной провинции Ирана Систан-Белуджистан с участием Международного университета Чабахара открыт Китайско-Иранский инновационный центр, который будет поддерживать малые и средние предприятия и стартапы и помогать подключать их к коммерческим и про-

41 При этом доля Ирана в общем объеме внешней торговли Китая составила всего 0,25%. Торговый обмен между Китаем и Ираном в 2022 году достиг 15,83 млрд долл. США, увеличившись на 7% по сравнению с 2021 годом. Экспорт Китая в Иран (товары народного потребления промышленная продукция, ИКТ) достиг 9,5 млрд долл. США, а импорт Китая из Ирана (полезные ископаемые, продукция сельского хозяйства) составил 6,4 млрд.

42 Пекин является четвертым по величине инвестором в Иране. В 2022 году рост объема инвестиций в Иран составил 150%, дополнительные 16 млрд долл. США инвестируются в форме финансирования.

43 Уже создана совместная группа по сотрудничеству в сфере ИКТ и обеспечению их безопасности, включая вопросы развития инфраструктуры, совместных НИОР, спутниковой связи, изучения угроз в киберпространстве и противодействия им. Источник: Iran, China sign protocol for ICT cooperation, IRNA, Tehran, Jan 22, 2016, https://theiranproject.com/blog/2016/01/22/iran-china-sign-protocol-for-ict-cooperation/.

мышленным фирмам Китая. Научный фонд Шелкового пути (SRSF), управляемый совместно вице-президентом Ирана по науке и технологиям и Китайской академией наук, ежегодно выделяет гранты на осуществление совместных проектов научной деятельности иранских и китайских исследователей. Благодаря этому, согласно международной базе данных цитирования Scopus, в период 2013–2020 гг. доля иранских статей с международным участием выросла на 209%, что сделало Иран ведущей страной исламского мира в научной дипломатии [53].

Иран и Китай сближают не только общие взаимовыгодные экономические и научно-технологические интересы, но и подходы ко многим политическим проблемам. По словам президента Э. Раиси Иран и Китай являются «друзьями в трудных обстоятельствах». Вторя ему и ссылаясь на запрет США в отношении двух крупных китайских компаний ZTE и Huawei[44], министр ИКТ Ирана М. Джахроми на встрече со своим китайским коллегой в июне 2019 года сказал: «Соединенные Штаты инициировали современный колониализм [в секторе ИКТ], надеясь распространить свою гегемонию на новые стратегические технологии, такие как искусственный интеллект[45]». «Мы сталкиваемся со схожими вызовами, поэтому нам нужно найти для них общие решения» [54].

Премьер-министр Китая Ли Цян заявил, что Китай готов укреплять связь и координацию с Ираном в рамках ООН, ШОС, БРИКС и других многосторонних механизмов, практиковать подлинную многосторонность и защищать общие интересы развивающихся стран. Он продолжит твердо поддерживать Иран в защите его национального суверенитета, территориальной целостности и национального достоинства и будет решительно выступать против любых внешних сил, вмешивающихся во внутренние дела Ирана [55].

5.4.2. Российская Федерация

Иран не рассматривает деятельность России на Ближнем Востоке как угрозу своей национальной безопасности и не планирует мероприятия по достижению превосходства над ней в сфере информационной борьбы.

В 2021 году Москва и Тегеран подписали «Соглашение между Правительством Российской Федерации и Правительством Исламской Республики Иран

---

44 В 2017 году Минюст США обвинил ZTE Corporation в 300 случаях поставок в Иран некоторых видов аппаратного и программного обеспечения, подпадающих под экспортные ограничения США (якобы это были контракты Huawei 2010/11 годов стоимостью 32 млн долл. США). За нарушения на ZTE были наложены жесткие санкции: она добровольно выплатила США беспрецедентный компенсационный штраф в сумме 892 млн долл., согласилась на постоянный регулярный мониторинг и аудит в течении 3 лет, кроме того, ее внесли в список компаний, с которыми американским поставщикам запрещено вести дела без одобрения правительства. Источник: Adam Ismail ZTE will pay U.S. government $892 million for illegally selling American tech to Iran, March 7, 2017, https://www.digitaltrends.com/mobile/zte-agrees-to-settlement-for-iran-sales/.

45 В феврале 2023 года в целях преодоления гегемонии США в искусственном интеллекте Китаем и Ираном заключено соглашение о сотрудничестве в этой сфере. Источник: Sino-Iranian Cooperation in Artificial Intelligence: A Potential Countering Against the US Hegemony,8 January 2023, https://link.springer.com/chapter/10.1007/978-981-19-6700-9_32.

о сотрудничестве в области обеспечения информационной безопасности». Соглашение одобрено меджлисом ИРИ только в декабре 2023 года [56], но взаимодействие между странами осуществлялось. В октябре 2021 года в Москве состоялся очередной раунд российско-иранских межведомственных консультаций по международной информационной безопасности (МИБ). Повестка дня мероприятия включала широкий спектр вопросов сотрудничества в сфере обеспечения МИБ на международных площадках и в двустороннем формате. Стороны обменялись мнениями о стратегических подходах России и Ирана в области МИБ и обсудили перспективы выстраивания прямого межведомственного диалога.

В рамках развития диалога в июне 2023 года в Тегеране прошло российско-иранское заседание по вопросам сотрудничества в области обеспечения информационной безопасности и телекоммуникаций между Министерством цифрового развития РФ и Министерством связи и информационных технологий ИРИ, в котором приняли участие «Ростелеком», «Ростелеком-Солар», Positive Technologies, «Центр речевых технологий», НТЦ «Протей», «Почта России», АНО «Организация развития видеоигровой индустрии» и другие. Со стороны Ирана присутствовала телекоммуникационная компания Telecommunication Infrastructure Company (TIC), которая отвечает за инфраструктуру телекоммуникационных сетей в Иране. Российские ИТ-компании предложили иранской стороне свои компетенции в анализе аудиоданных с использованием искусственного интеллекта, цифровизации бизнес-процессов, в создании центров реагирования на киберугрозы и аутсорсинга ИТ-услуг. В свою очередь, иранская TIC провела с «Ростелекомом» ряд встреч, чтобы договориться о расширении каналов передачи трафика по морскому маршруту и трансконтинентальному транспортному коридору «Север-Юг».

Кроме того, Россия, Иран, Турция и Азербайджан договорились совместно реализовать проект по созданию совместного рынка ИКТ. Четыре страны создадут консорциум с совместными инвестициями в размере 2 млн долл. США для содействия развитию центров стартапов, кибербезопасности и телекоммуникационной инфраструктуры (спутниковая связь, почта) [57].

5.4.3. КНДР

В сентябре 2012 года Ираном и КНДР подписано всеобъемлющее соглашение о научно-техническом сотрудничестве, предусматривающее, в том числе, объединение усилий в борьбе с «общим врагом в цифровом пространстве» [58]. Состояние сотрудничества на данном этапе неизвестно.

5.4.4. Венесуэла

В последние годы отмечено расширение связей с Венесуэлой. Тегеран планирует развернуть на территории этого государства специальные средства для

перехвата сетевого трафика и целевого противодействия кибератакам со стороны США. Налажено обучение венесуэльских специалистов в сфере информационной борьбы в Иране.

5.4.5. Республика Кения

В январе 2021 года Иран официально открыл Иранский дом инноваций и технологий (IHIT) в столице Кении Найроби. Он будет служить «базой для создания инновационных идей, их коммерциализации и экспорта иранских наукоемких продуктов и услуг на рынок Восточной Африки» [59].

5.4.6. Южно-Африканская Республика (ЮАР)

В 2022 году на полях Всемирного саммита по информационному обществу (ВВВУИО) в Женеве состоялись переговоры высокопоставленных официальных лиц Ирана и ЮАР, направленные на создание основы для двустороннего сотрудничества в области ИКТ. Иран проинформировал о достижениях в области электронных услуг и объявил о готовности страны к сотрудничеству с ЮАР в этом секторе. Стороны согласились обменяться знаниями и опытом работы на международных площадках (ICANN, МСЭ, ВВВУИО и РГОС ООН). Иран и Южная Африка договорились повысить сотрудничество в рамках председательства ЮАР в G20 и БРИКС, а также обменяться данными об ИКТ-индикаторах [60].

6. Возможные приоритеты Ирана в сфере обеспечения национальной и международной информационной безопасности в рамках БРИКС

Вхождение в БРИКС такого крупного и политически независимого игрока, как Иран, является знаковым событием. Насколько объединение сможет интегрировать всех новых членов и включить их в процесс многостороннего взаимодействия в сфере обеспечения безопасности ИКТ, покажет время.

Результаты проведенного анализа иранской политики в сфере кибербезопасности подтверждают, что предпринимаемые руководством страны в последние годы меры демонстрируют хорошие результаты.

На международной арене, в частности в РГОС ООН, Тегеран уже сейчас способствует продвижению общего для БРИКС подхода по соблюдению в информационном пространстве принципов Устава ООН, включая уважение суверенитета и невмешательство во внутренние дела.

Ключевые направления сотрудничества в сфере международной информационной безопасности, касающиеся противодействия использованию ИКТ в преступных целях и продолжения работы над правилами ответственного поведения государств

в ИКТ-среде, активно поддерживаются Ираном. По мнению Тегерана, расширенное взаимодействие в рамках ООН, БРИКС, ШОС и других международных организаций (максимально независимых от Запада во главе с Вашингтоном) будет способствовать созданию открытой, безопасной, устойчивой и доступной ИКТ-среды на благо развития и процветания. Это полностью соответствует положению Уфимской декларации БРИК, в которой сказано, что страны-участницы объединения не только «приветствуют включение проблематики ИКТ в Повестку дня в области развития на период после 2015 года»[46], но и признают «потенциал развивающихся стран в системе ИКТ и их важную роль в решении вопросов, связанных с проблематикой ИКТ» в рамках достижения Целей устойчивого развития ООН.

Для Ирана это особенно актуально. Государство взяло курс на развитие цифрового общества, повышение своей безопасности путем преодоления научного и технологического разрыва, снижения зависимости от западных ИКТ, развития собственного потенциала и расширение интеграции в глобальный ИКТ-рынок. Оно остро нуждается в доступе к финансированию и притоке инвестиций, в связи с чем очевидна востребованность у Тегерана услуг Банка развития БРИКС и других финансовых инструментов, включая расчеты в национальной валюте. В этой связи следует отметить, что Иран является сторонником процесса дедолларизации и торговли в национальных валютах, особенно в своповых поставках [61].

По мнению замглавы МИД Ирана по экономической дипломатии Мехди Сафари, присоединение Ирана к БРИКС предоставит этой организации огромные возможности. «Одна из них — транзит, вторая — энергетика, будь то нефть или газ, третья — новые технологии и наукоемкая сфера» [62]. Высокий потенциал Ирана в сфере научных исследований и искусственного интеллекта будет востребован в сфере научно-технического сотрудничества БРИКС, в том числе в форматах Партнерства БРИКС по вопросам новой промышленной революции, Сети БРИКС по передаче технологий, Центра промышленных компетенций стран БРИКС, промышленных и научных парков, технологических бизнес-инкубаторов, стартап-мероприятий БРИКС и многих других форматов.

Значительное содействие Ирану может быть оказано по направлению социального развития. Опыт Бразилии, Индии, России, Китая и ЮАР в развитии услуг электронного правительства, цифровой медицины, дистанционного образования будет способствовать эффективному использованию демографического дивиденда, обеспечению достойными рабочими местами, повышению социальной защиты, решению проблем общественного здравоохранения.

---

46 Повестка дня в области развития на период после 2015 года принята 70 сессией Генеральной ассамблеи ООН «Преобразование нашего мира: Повестка дня в области устойчивого развития на период до 2030 года» A/RES/70/1 от 25 сентября 2015 года, она определяет 17 целей устойчивого развития, из которых 11 будут достигнуты с помощью развития передовых ИКТ.

7. Использованная литература

1 Скляров Л.Е. Иран 60-80-х годов: традиционализм против современности. Революция и контрреволюция, Москва «Наука»/Издательская фирма «Восточная литература»,1993, https://aleksandrozerov.ucoz.ru/234/l.e-skljarov-iran_v_60-80-e_gody.pdf.

2 Рещиков О.И. Процессы цифровизации в Иране в период санкций. Журнал «Азия и Африка сегодня» 2022 №8, https://asaf-today.ru/s032150750021324-8-1/.

3 Middle East Internet Statistics, Population, Facebook and Telecommunications Reports, https://www.internetworldstats.com/stats5.htm.

4 Access to broadband internet in Iran rose 6.11% in 2022: CRA, 28 March 2023, https://www.presstv.co.uk/Detail/2023/03/28/700584/Iran--broadband-access-increase-2022-CRA-figures.

5 Monthly Commercial Report. India Embassy of India, Tehran, August 2022, https://www.imcnet.org/storage/content_gallery/international_collaborations/Iran%20MECR%20August%202022.pdf.

6 Submarine Cable Map, TeleGeography, https://www.submarinecablemap.com.

7 Братерский А. Иранский сценарий. Великий и ужасный IT-сектор, 15.06.22, https://www.finam.ru/publications/item/iranskiiy-scenariiy-velikiiy-i-uzhasnyiy-it-sektor-20220615-111503/.

8 E-Government Survey Index 2022, https://desapublications.un.org/publications/un-e-government-survey-2022.

9 Ben Wodecki Iran Vies to Become Top 10 AI Nation by 2032, February 2, 2022, https://aibusiness.com/verticals/iran-vies-to-become-top-10-ai-nation-by-2032#close-modal.

10 Government AI Readiness Index 2022, Oxford Insights, Dec 2022, https://static1.squarespace.com/static/58b2e92c1e5b6c828058484e/t/639b495cc6b59c620c3ecde5/1671121299433/Government_AI_Readiness_2022_FV.pdf.

11 Кибервойны – новая реальность Ближнего Востока, SecurityLab. 17.11.2003, http://www.securitylab.ru/news/213358.php.

12 Global Cybersecurity Index, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

13 Алексеева Ю.А., Феофилова Т.Ю., Имани М. Цифровая экономика Ирана: проблемы развития и особенности управления // π-Economy. 2022. Т. 15, № 4, https://cyberleninka.ru/article/n/tsifrovaya-ekonomika-irana-problemy-razvitiya-i-osobennosti-upravleniya?ysclid=lp43l47dn391992267.

14 Булавин А.В., Акимов А.Л., Старкин С.В. – Стратегическое планирование и процесс принятия решений в сфере национальной безопасности Ирана // Национальная безопасность / nota bene. – 2017. № 1, https://nbpublish.com/library_read_article.php?id=21874.

15 Pahlavi, Pierre and Ouellet, Eric. Iran: Asymmetric Strategy and Mass Diplomacy. Journal of Strategic Security 13, no. 2 (2020), https://digitalcommons.usf.edu/jss/vol13/iss2/6.

16 Вартанян А.М. Стратегия развития Ирана до 2025 года: промежуточные итоги, Институт Ближнего Востока, 6 сентября 2010, http://www.iimes.ru/?p=11270.

17 Cyberwellness Profile Iran, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Iran.pdf#:~:text=1.2.1%20CIRT%20Iran%20has%20an,implementing%20internationally%20recognized%20cybersecurity%20standards.

18 Information and Communications Technology Strategy Building the knowledge-based economy and connecting Iran to strategic markets, 2021, https://intracen.org/file/nesiran-ict22-3-2021webpdf-1.

19 National position of Iran, https://cyberlaw.ccdcoe.org/wiki/National_position_of_Iran_(2020).

20 The Islamic Republic of Iran's cyber security strategy: challenges in an era of cyber uncertainty , 2020, https://ebrary.net/173527/political_science/islamic_republic_iran_s_cyber_security_strategy_challenges_cyber_uncertainty.

21 Иран и кибервойны, Новое восточное обозрение, 22.12.2014, http://ru.journal-neo.org/2014/12/22/iran-i-kibervojny/.

22 Iran's Intranet: a Master Plan for Internet Censorship, November 1, 2020, https://www.millichronicle.com/2020/11/irans-intranet-a-master-plan-for-internet-censorship.html.

23 Iran's National Information Network: Faster Speeds But At What Cost?, Internet Monitor, 21 February 2018, https://thenetmonitor.org/bulletins/irans-national-information-network-faster-speeds-but-at-what-cost.

24 Filiz Katman The Islamic Republic of Iran's cyber security strategy: challenges in an era of cyber uncertainty, https://ebrary.net/173527/political_science/islamic_republic_iran_s_cyber_security_strategy_challenges_cyber_uncertainty?ysclid=loqs3kb6ib50563860.

25 Федотов А. Опыт регулирования информационного пространства в Иране, Digital Russia, 05.11.2020, https://d-russia.ru/opyt-regulirovanija-informacionnogo-prostranstva-v-irane.html.

26 Filiz Katman The Islamic Republic of Iran's cyber security strategy: challenges in an era of cyber uncertainty https://ebrary.net/173527/political_science/islamic_republic_iran_s_cyber_security_strategy_challenges_cyber_uncertainty.

27 E-commerce Law and Cybersecurity in Iran - ناراکـمه و یرگـسع یقوقح مسـوم ? https://asgarilaw.com/e-commerce-law-and-cybersecurity-in-iran/.

28 Iran: Personal Data Protection and Safeguarding Draft Act, June 27, 2019, https://www.article19.org/resources/iran-data-protection-draft-act/.

29 https://iranprimer.usip.org/blog/2021/oct/14/internet-freedom-iran-and-new-protection-bill.

30 Булавин А.В., Акимов А.Л., Старкин С.В. Стратегическое планирование и процесс принятия решений в сфере национальной безопасности Ирана // Национальная безопасность / nota bene. 2017, № 1, https://nbpublish.com/library_read_article.php?id=21874.

31 Указом Верховного Лидера создан и утвержден Высший совет киберпространства, 7 марта 2012, https://www.leader.ir/ru/content/9215.

32 Капошин О.А. Об оценке кибервозможностей Ирана экспертами Международного института стратегических исследований. Часть 2, Институт Ближнего Востока, 28 ноября 2021, http://www.iimes.ru/?p=81447.

33 Annual Threat Assessment of the U.S. Intelligence Community, February 7, 2022 https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf.

34 Хетагуров А. Кибермощь Ирана. Киберстражи Исламской Революции, РСМД, https://russiancouncil.ru/cyberiran?ysclid=lp14pgiryh645918570.

35 Булавин А.В., Акимов А.Л., Старкин С.В. Стратегическое планирование и процесс принятия решений в сфере национальной безопасности Ирана // Национальная безопасность / nota bene. 2017 № 1, https://nbpublish.com/library_read_article.php?id=21874.

36 Online Cybercrime Emergency Center, https://financialtribune.com/articles/people/33451/online-cybercrime-emergency-center.

37 Капошин О.А. Об оценке кибервозможностей Ирана экспертами Международного института стратегических исследований. Часть 2, Институт Ближнего Востока, 28 ноября 2021, http://www.iimes.ru/?p=81447.

38 Хетагуров А. Кибермощь Ирана. Киберстражи Исламской Революции, РСМД, https://russiancouncil.ru/cyberiran?ysclid=lp14pgiryh645918570.

39 M. Demboski Analysis of the Iranian cyber attack landscape, https://www.ironnet.com/blog/iranian-cyber-attack-updates.

40 Валиахметова Г.Н. Обеспечение национальной кибербезопасности в условиях виртуальных войн XXI в.: Опыт Исламской Республики Иран, 2016, https://elar.urfu.ru/bitstream/10995/40418/1/iuro-2016-152-09.pdf?ysclid=loq5lamj37860929795,
Evolving Menace: Iran's Use of Cyber-Enabled Economic Warfare, Foundation for Defense of Democracies, November 9, 2018, https://www.fdd.org/analysis/2018/11/06/evolving-menace,
The Dangers of Iran's Cyber Ambitions, CEEW Monograph, October 28, 2022, https://www.fdd.org/analysis/2022/10/28/the-dangers-of-irans-cyber-ambitions/#easy-footnote-bottom-90-134879.

41 Shahid Beheshti University – IFMAT, https://www.ifmat.org/12/22/shahid-beheshti-university/.

42 Decision of the Council of the European Union 2010/413/CFSP, https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX%3A32010D0413.

43 Evolving Menace: Iran's Use of Cyber-Enabled Economic Warfare, Foundation for Defense of Democracies, November 9, 2018, https://www.fdd.org/analysis/2018/11/06/evolving-menace.

44 M. Dubowitz, O. Kittrie Strategy for a New Comprehensive U.S. Policy on Iran, Foundation for Defense of Democracies, January 2023, https://www.fdd.org/analysis/2023/01/10/strategy-for-a-new-comprehensive-us-policy-on-iran/.

45 Global Cybersecurity Index, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

46 What's new with cybersecurity negotiations: The OEWG 2021–2025 annual report adopted, https://www.diplomacy.edu/blog/whats-new-with-cybersecurity-negotiations-the-oewg-2021-2025-annual-report-adopted/,
10th Meeting of the third session of the OEWG | Digital Watch Observatory, https://dig.watch/event/oewg-third-substantive-session/10th-meeting-third-session-oewg/.

47 What's new with cybersecurity negotiations? OEWG 2021-2025 fourth substantive session, https://www.diplomacy.edu/blog/whats-new-with-cybersecurity-negotiations-oewg-2021-2025-fourth-substantive-session/.

48 Россия и Иран начали сотрудничество в сферах ИБ и телекоммуникациях, 2023, https://www.cnews.ru/news/top/2023-077_rossiya_i_iran_nachnut_sotrudnichat?ysclid= lnhollnscc895606352.

49 Страны ЕАЭС подписали соглашение о свободной торговле с Ираном, 25.12.2023, https://ria.ru/20231225/torgovlya-1917946686.html?ysclid=lqoxlfkutt776220067.

50 Iran says 25-year China agreement enters implementation stage, 15 Jan 2022, https://www.aljazeera.com/news/2022/1/15/iran-says-25-year-china-agreement-enters-implementation-stage#:~:text=Iran%20says%2025-year%20China%20agreement%20enters%20implementation%20stage,year%20%5BMajid%20Asgaripour%2FWest%20Asia%20News%20Agency%20via%20Reuters%5D.

51 Farzad Ramezani Bonesh China's Multilateral Trade with Iran, Situation and 2023/24 Prospects, Jul 11, 2023, https://www.silkroadbriefing.com/news/2023/07/10/chinas-multilateral-trade-with-iran-situation-and-2023-24-prospects/.

52 Nigar Bayramli Iran, China Sign 20 Cooperation Documents, February 16, 2023, https://caspiannews.com/news-detail/iran-china-sign-20-cooperation-documents-2023-2-15-50/.

53 Iran-China joint scientific program enters new phase, Iran News Daily, https://irannewsdaily.com/2022/04/iran-china-joint-scientific-program-enters-new-phase/ .

54 Iran, China agree to jointly counter cyber threats, https://theiranproject.com/blog/2019/07/06/iran-china-agree-to-jointly-counter-cyber-threats/.

55 China to strengthen communication, coordination with Iran within multilateral mechanisms, says premier, 7 Oct.2023, https://news.cgtn.com/news/2023-10-27/China-says-to-strengthen-communication-coordination-with-Iran-1oeBJ3HJE76/index.html.

56 СМИ: Иран готовит соглашение с Россией в сфере информационной безопасности, 10.12.2023, https://ria.ru/20231210/iran-1914893273.html?ysclid=lqoxcwxtm387164202.

57 РФ, Азербайджан, Турция и Иран создадут консорциум для развития ИКТ, Вестник Кавказа, 2018, https://vestikavkaza.ru/news/RF-Azerbaydzhan-Turtsiya-i-Iran-sozdadut-konsortsium-dlya-razvitiya-IKT.html?ysclid=lp41q0hb99168241576.

58 Iran and North Korea Sign Technology Treaty to Combat Hostile Malware // V3.CO.UK. September 3, 2012, http://www.v3.co.uk/v3-uk/news/2202493/iran-andnorth-korea-sign-technology-treaty-to-combat-hostile-malware#.

59 China and Iran: Bilateral Trade Relationship and Future Outlook, August 20, 2021, https://www.china-briefing.com/news/china-and-iran-bilateral-trade-relationship-and-future-outlook/.

60 Iran, South Africa to cooperate in IT, Iran Mirror, June 7, 2022, https://www.iranmirrorbd.com/en/2022/06/07/iran-south-africa-to-cooperate-in-it/#:~:text=Iran%20and%20South%20Africa%20have,the%20Iranian%20Information%20Technology%20Organization.

61 ШОС и БРИКС должны идти по пути дедолларизации, считает Иран // РИА Новости, 3 января 2024 года, https://ria.ru/20240103/briks-1919550078.html.

62 В Иране рассказали, чем страна будет полезна для БРИКС // Радио Sputnik, 3 января 2024 года, https://radiosputnik.ru/20240103/briks-1919553053.html.

Китайская Народная Республика


Официальное название: Китайская Народная Республика
Столица: Пекин
Официальный язык: китайский, один из шести рабочих языков ООН.

Территория: 9,63 млн кв. км^2, по размеру уступает лишь России и Канаде. Государство расположено в Восточной и Центральной Азии. Континентальная часть на востоке омывается водами Желтого, Восточно-Китайского, Южно-Китайского и Бохайского морей (протяженность береговой линии — более 18 тыс. км).

КНР граничит с 14 государствами: на севере — с Монголией, на северо-востоке — с КНДР и Россией, на юго-востоке — с Мьянмой, Лаосом и Вьетнамом, на юго-западе — с Индией, Непалом и Бутаном, на западе — с Таджикистаном, Афганистаном и Пакистаном (по так называемой линии контроля в Кашмире), на северо-западе с Россией, Казахстаном и Киргизией. Протяженность сухопутной границы 22,8 тыс. км.

Население: 1 425 671 352 чел., т.е. второе, после Индии (по данным Фонда населения ООН на июль 2023 года). Официальный уровень урбанизации постоянно проживающего населения в 2022 году составил 65,2%.

В Китае четыре города центрального подчинения, приравненных по статусу к провинциям (Пекин, Тяньцзинь, Шанхай и Чунцин), 23 провинции (включая Тайвань), пять автономных районов и два специальных административных района — Гонконг и Макао (всего — 34 субъекта)[1].

Государственное устройство: унитарное государство. Конституция принята 4 декабря 1982 года. Форма правления — республика с полновластием представительных органов — собраний народных представителей (СНП), которые создаются на всех административных уровнях: волость — уезд — провинция. Высший орган государственной власти — однопалатное Всекитайское собрание народных представителей (ВСНП), состоящее из 2979 депутатов, избираемых сроком на 5 лет. Сессии ВСНП созываются раз в год, обычно в первой половине марта. Между сессиями соответствующие полномочия исполняет Постоянный комитет ВСНП (155 депутатов). Прямые выборы депутатов проводятся только на низовом и уездном уровнях, депутаты остальных уровней избираются СНП

1 КИТАЙ • Большая российская энциклопедия — электронная версия. https://old.bigenc.ru/geography/text/2068564?ysclid=lpjgnqxm4o994383778.

нижестоящего уровня. 5–11 марта 2024 года в Пекине состоялась вторая сессия ВСНП 14-го созыва.

Законодательная власть: ВСНП — высший законодательный орган, в компетенцию которого входит утверждение планов экономического развития и бюджета. Собственные органы законодательной власти действуют на территории специальных административных районов Гонконга и Макао.

Исполнительная власть: Государственный совет КНР — исполнительный орган ВСНП и высший государственный административный орган, которому подчинены все органы государственного управления. Ему предоставлено право принятия нормативных актов в рамках действующих законов.

Представительные органы власти на своем административном уровне формируют другие государственные органы, включая правительства, суды, прокуратуры, контрольные комитеты, которые перед ними ответственны и им подчинены. ВСНП избирает Председателя и Заместителя Председателя КНР (глава государства и его заместитель), председателей Центрального военного совета (ЦВС) КНР (высший орган государственного руководства вооруженными силами), Верховного народного суда и Верховной народной прокуратуры КНР, Премьера Государственного совета КНР (глава правительства — высшей орган исполнительной власти), заместителей Премьера и членов Госсовета, министров и руководителей других ведомств, включая председателя Народного банка Китая (Центральный банк) и главного аудитора.

Председатель КНР — Си Цзиньпин (с марта 2013 года, переизбран на третий срок в марте 2023 года). В марте 2023 года избраны Премьер Госсовета КНР — Ли Цян, Председатель Постоянного комитета (ПК) ВСНП — Чжао Лэцзи, Заместитель Председателя КНР — Хань Чжэн.

Система органов власти КНР работает под руководством Коммунистической партии Китая (КПК), ведущая роль которой в китайском обществе закреплена действующей Конституцией[2]. Генеральный секретарь ЦК Компартии Китая — Си Цзиньпин (избран на первом пленуме ЦК КПК 18-го созыва в ноябре 2012 года, переизбран на третий срок на первом пленуме ЦК КПК 20-го созыва в октябре 2022 года). По итогам XX съезда КПК (16–22 октября 2022 года) сформирован Центральный комитет КПК (205 членов и 171 кандидат в члены). На первом пленуме ЦК КПК 20-го созыва определены Политическое бюро (24 члена) и его Постоянный комитет (7 членов).

В КНР существуют восемь демократических партий, признающих руководство КПК в рамках многопартийного механизма сотрудничества. В их число входят Революционный комитет Гоминьдана Китая, Демократическая

2 Численность КПК началу 2022 года составляла более 96,71 млн чел.

лига Китая, Ассоциация демократического национального строительства Китая, Ассоциация содействия развитию демократии в Китае, Рабоче-крестьянская демократическая партия Китая, Китайская партия стремления к справедливости, Общество «3 сентября» и Лига демократического самоуправления Тайваня.

Спецификой политической системы КНР является существование «Единого народного патриотического фронта», который организационно оформлен в виде системы народных политических консультативных советов (НПКС), деятельность которых имеет совещательный характер. В советах представлены политические партии, общественные и деловые организации. НПКС, как и СНП, образованы на всех административных уровнях. Высший совещательный орган — Народный политический консультативный совет Китая (НПКСК)[3].

Экономика: По данным Всемирного банка за 2022 год показатели Валового внутреннего продукта (ВВП) (по паритету покупательной способности):

Итого: 30,327 трлн долл. (1 место в мире). На душу населения: 21 476 долл. (71 место в мире);

Показатели ВВП (Номинал):

Итого: 17,963 трлн долл. (2 место в мире).

На душу населения: 12 720 долл. США (63 место в мире).

Внешнеторговый оборот КНР в 2022 году вырос на 4,4% до 6,3 трлн долл. США, в том числе экспорт — 3,59 трлн долл. (+7%), импорт — 2,71 трлн долл. (+1,1%). Положительное торговое сальдо Китая составило 877,6 млрд долл.[4]

Дипломатические отношения с Россией (СССР) установлены 2 октября 1949 года. СССР стал первым иностранным государством, которое объявило о признании КНР. После распада СССР правительство КНР 24 декабря 1991 года признало Российскую Федерацию в качестве правопреемницы международных прав и обязательств бывшего Советского Союза.

3 Сайт Посольства РФ в https://beijing.mid.ru/ru/countries/kitay/politicheskaya_sistema/.

4 https://beijing.mid.ru/ru/countries/kitay/economica_knr/.

1. Уровень развития информатизации страны и информационно-коммуникационной инфраструктуры, системы обеспечения информационной безопасности

Развитие информатизации Китая стремительно по темпам и грандиозно по масштабам: за тридцать лет осуществлен рывок почти с зачаточного состояния ИКТ-отрасли до второй в мире цифровой экономики. По планам руководства страны к 2035 году уровень цифрового развития КНР выйдет на передовые позиции в мире [1].

Согласно Глобальному инновационному индексу за 2023 год[5] Китай занимает 12 позицию и претендует на роль мирового лидера в различных передовых технологиях шестого экономического уклада — искусственном интеллекте (особенно в машинном обучении, компьютерном зрении, технологиях дополненной и виртуальной реальности), Интернете вещей, роботизации, Больших данных, блокчейн и финтех. Кроме того, Китай разработал лучшие в мире технологии подвижной связи пятого поколения (5G) и обеспечил развертывание национальной сети 5G: количество ее базовых станций к концу 2022 года достигло 2,31 млн [2, 3], что составляет 60% от всей мировой инфраструктуры 5G. В развитии квантовых технологий КНР является одним из мировых лидеров[6], еще в 2017 году Пекин объявил о запуске своего уникального проекта «Цзинань» по созданию на основе квантовых технологий первой в мире «невзламываемой» сети передачи данных для нужд обороны и финансового сектора[7].

Страна почти полностью обеспечивает себя необходимыми для внедрения Индустрии 4.0 цифровыми технологиями. По данным Министерства промышленности и информационных технологий на июнь 2023 года, Китай занимал второе место в мире по общему объему вычислительных мощностей и количеству высокопроизводительных центров обработки данных (их более 450). Также КНР самодостаточна в космических системах связи, общая группировка спутников превышает 400 единиц [4]. Некоторый дефицит ощущается

5 В 2016 году в Global Innovation Index (WIPO) Китай был на 25 позиции.

6 КНР лидер в развитии наземных и спутниковых квантовых коммуникаций. В области квантовых вычислений наибольшие успехи достигнуты в сверхпроводниковой и фотонных платформах. За 10 лет в КНР зарегистрировано около 84 тыс. квантовых патентов — это примерно на 30% больше, чем в США. Уровень национального образования в этой сфере считается одним из лучших, Источник: Квантовый дайджест, Май 2023, https://www.rqc.ru/backend/uploads/Quantum_Digest_May2023_9d3e62b971.pdf.

7 Иванько А.Ф., Иванько М.А., Зеленкова Т.В. Особенности развития компьютерных сетей в Китае // Научное обозрение. Экономические науки, № 1 2019, С. 27–31, https://science-economy.ru/ru/article/view?id=992. Для сравнения в США первая квантовая «петля» была запущена в феврале 2020 года учеными Орегонского университета, а в июле того же года дан старт Национальной квантовой инициативе, целью которой является получение преимущество над Китаем в квантовых технологиях. Источник: U.S. Department of Energy Unveils Blueprint for the Quantum Internet at ‘Launch to the Future: Quantum Internet’ Event // Department of Energy https://www.energy.gov/articles/us-department-energy-unveils-blueprint-quantum-internet-launch-future-quantum-internet.

в нескольких сегментах ИКТ-рынка: в системах проектирования микросхем, программном обеспечении для промышленного оборудования, основных компонентах и базовых алгоритмах технологических процессов.

На базе созданной ИКТ-инфраструктуры активно развиваются всевозможные услуги и сервисы. В Китае онлайн-покупки регулярно совершают до 600 млн человек, а годовой оборот розничных продаж в Интернете в 2021 году составил 2,2 трлн долл. США. Вклад цифровой экономики в ВВП страны в 2022 году достиг 41,5%, что в абсолютном выражении составляет 50,2 трлн юаней или 7,25 трлн долл. США [5]. Провинции с наиболее развитой цифровой экономикой демонстрируют наибольший экономический рост (в первую очередь Пекин, Фудзянь, Гуандун, Шанхай, Джецзян). Уровень развития электронного правительства, определяемый Департаментом по экономическим и социальным вопросам ООН, в Китае очень высокий, что позволило стране в 2022 году занять 43 позицию в мире, сразу после России.

Тем не менее, показатели КНР по использованию ИКТ не самые высокие в мире, что говорит об огромном потенциале развития этого рынка и пока сохраняющейся диспропорции распределения цифровой инфраструктуры по регионам. Уровень проникновения Интернета (соотношение пользователей к населению страны) в декабре 2022 года составил 69,8%, что лишь немногим выше среднемирового 67,9%. Согласно индексу сетевой готовности, который рассчитывается по 4 блокам показателей (развитие технологической составляющей, человеческого фактора, управленческих навыков и влияния Интернета на все отрасли экономики и государство), в 2022 году Китай занял 23 место в мире[8], хотя еще в 2016 году был на [59].

Задача обеспечения информационной безопасности также требует внимания, в соответствии с Глобальным индексом кибербезопасности [6] КНР в 2020 году занимала 33 позицию, что существенно ниже, чем у большинства стран-участниц БРИКС[9]. Китай испытывает серьезный дефицит специалистов в области информационной безопасности[10].

---

8 Индекс ежегодно готовится INSEAD для ВЭФ https://networkreadinessindex.org/countries/.

9 Индекс GCI рассчитывается МСЭ, по нескольким параметрам в 5 группах: развитие правовой системы обеспечения информационной безопасности; применение технических мер; организационных мер; реализации программ наращивания потенциала; участие в международном сотрудничестве. В GCI 2020 Россия была на 5 месте, Индия на 10, Бразилия на 18.

10 По данным Национального института военных исследований Японии в условиях лавинообразной информатизации потребность Китая в ИТ-кадрах в 2021 году оценивалась от 700 тыс. до 1,4 млн человек. Ежегодно рынок труда получает 15 тыс. специалистов, например, самый передовой Национальный киберцентр в г. Ухань готовит 1,5 тыс. дипломированных ИТ-выпускников и еще 2,5 тыс. проходит переподготовку. Однако 95% вакансий в сфере информационной безопасности ежегодно остаются незаполненными.
Источник: Williams Evaluating China's Road to Cyber Super Power //STRATCOM, 17.11.2021, https://nsiteam.com/social/wp-content/uploads/2022/01/Williams_STRATCOM-2021-11-17D.pdf .

2. О стратегическом планировании в сфере развития ИКТ и передовых технологий, обеспечения кибербезопасности

Особенностью политики Пекина в области обеспечения информационной безопасности является четко выстроенная Центральным комитетом коммунистической партии Китая (ЦК КПК) долгосрочная комплексная стратегия. Она является всеобъемлющей за счет увязки воедино всех направлений, которые могут оказать воздействие на ее эффективность, включая индустриальное и научно-техническое развитие, обеспечение трансфера технологий в реальный сектор экономики, привлекательную инвестиционную политику, постоянное совершенствование нормативной базы, подготовку кадров, продвижение интересов страны на международной арене. В совокупности это системно укрепляет цифровой суверенитет КНР.

Эксперты выделяют три исторических этапа индустриального развития и стратегического планирования, каждый из которых решал определенные задачи.

2.1. Первый этап — технологическое развитие страны

Этот этап совпал с началом реформирования экономики в соответствии с принципами открытого рынка и свободной торговли, а также полноценным подключением КНР к сети Интернет[11]. Политика «открытых дверей» способствовала притоку в страну иностранных инвестиций и технологий. В 1986 году «Планом 863» была поставлена задача сформировать новые источники роста экономики за счет «догоняющего» развития высоких технологий, в том числе ИКТ. Через два года стартовала программа «Факел» по внедрению новых технических разработок в производство и созданию кластеров, объединяющих научные учреждения, экспериментальные площадки и промышленные предприятия. Таким образом, в сфере высоких технологий был изменен принцип взаимодействия государственного и коммерческого сектора, взят курс на преодоление обособленности государственных структур и бизнеса, а также производства и исследований, осуществлявшихся в основном за счет госбюджета [7,8]. Одновременно была запущена программа реформирования всех ступеней образования для обеспечения экономики национальными кадрами.

В конце 90-х годов в этот комплекс задач была включена выработка концепции защиты национального киберпространства от угроз информационной безопасности. В технической сфере — это главным образом уязвимости ИКТ и сетевые угрозы, в идеологической — борьба с использованием сети Интернет для

11 Домен верхнего уровня с кодом страны (ccTLD) для Китайской Народной Республики (.cn) введен 28.11.1990.

террористической и преступной деятельности. В 2000 году Китаем принят первый нормативный документ, кодифицирующий следующие преступления: взлом или уничтожение компьютерной системы; нарушение законных прав других лиц в Интернете; подрыв государственной власти, разрушение единства нации и национальностей; кража государственной тайны; участие в культовой деятельности путем публикации информации в глобальной сети [9].

2.2. Второй этап — инновационное развитие экономики

На этом этапе с опорой на созданную технологическую базу был взят курс на повышение роли инноваций в экономическом и технологическом развитии страны, чтобы таким образом трансформировать экономику в наукоемкую, требующую высокого уровня образования, знаний и квалификации. Эта концепция была сформулирована в принятой Госсоветом КНР **Национальной среднесрочной и долгосрочной программе научного и технологического развития** (2006)[12]. Среди приоритетных направлений было выделено развитие информационной промышленности и современной индустрии цифровых услуг[13]. В 2010 году Госсовет КНР выделил семь стратегически важных передовых технологий[14], научная разработка и внедрение которых должны были обеспечить рост ВВП на 8% к 2015 году. В передовых ИКТ были выделены следующие направления:

- ускорение строительства крупных, интегрированных и безопасных производственных мощностей, опытно-конструкторских работ по новому поколению подвижной связи, ключевому оборудованию и исследовательским комплексам для разработки нового поколения сети Интернет;
- ускорение конвергенции телекоммуникаций, широкополосного вещания и технологий на базе IP-протокола, проведение НИОКР в сфере Интернета вещей и облачных вычислений;
- концентрация на разработке ключевых и базовых сегментов ИКТ-рынка, в том числе интегральных микросхем, новых типах дисплеев, современном программном обеспечении и серверном оборудовании;

12 Программой были поставлены цели достичь к 2020 году следующих показателей - стать инновационной нацией, уменьшить степень зависимости от иностранных технологий как минимум на 30%, увеличить долю расходов на НИОКР в ВВП до 2,5% и более.
Источник: The National Medium- and Long-Term Program for Science and Technology Development (2006-2020), https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/China_2006.pdf.

13 Этот сегмент включает: сопутствующие информационные технологии и основные программные приложения для индустрии услуг; высокопроизводительные и надежные компьютеры; сенсорные сети и «умная» обработка информации; платформы цифрового медиа контента; большие плоские дисплеи высокого разрешения; базовые приложения, ориентированные на информационную безопасность.

14 К ним отнесли: энергосбережение и «зеленые» технологии; новое поколение ИКТ; биотехнологии; передовые технологии для производства; умная энергетика; новые материалы; транспорт на иных видах топлива, Источник: http://www.gov.cn/zwgk/2010-10/18/content_1724848.htm.

- обновление программного обеспечения и веб-сервисов, повышающих добавленную стоимость продукции, продвижение «умной» трансформации инфраструктуры;
- разработка цифровых и виртуальных технологий для продвижения их в креативные индустрии.

В государственные НИОКР была также включена проблематика обеспечения безопасности сетевых технологий, противодействия компьютерным атакам и защиты данных.

Кроме того, был обеспечен трансфер наукоемких технологий за счет реализации программы инновационного развития национального высокотехнологичного производственного сектора «**Сделано в Китае 2025**» [10]. Предложенные планом обеспечительные меры (льготная финансовая и налоговая политика, многоуровневая система подготовки кадров, оказание содействия малым и средним предприятиям, в том числе предоставление доступа к инфраструктуре для исследований и апробации технических решений) обеспечили ускорение цифровизации, урбанизации, модернизации всех отраслей экономики и государственного управления, снижение технологической зависимости КНР от западных стран[15].

Одновременно для управления этой деятельностью была создана система государственных и партийных структур[16]. Более четко оформились контуры национальной киберстратегии, базисом которой является неразрывная связь ускорения инноваций и обеспечения их безопасности. В 2012 году опубликовано «**Мнение Государственного совета о форсированном продвижении развития информатизации и о реальном обеспечении информационной безопасности**» [11]. Для достижения целей **Плана 12-й пятилетки по развитию передовых технологий** (2011–2015 годы) [12] на Государственный комитет по развитию и реформе КНР возложена обязанность координации действий всех ведомств, в том числе по разработке приоритетов, ключевых проектов и обеспечивающих политик для каждой отрасли. Следует отметить, что еще до этого было решено снизить уязвимость критических информационных инфраструктур за счет сертификации поставляемых в Китай западных криптографических средств и другой ИКТ продукции для частного и государственного сектора[17]. В 2008 году введением схемы

15 Одной из задач является обеспечение к 2025 году локализации 70% производства микросхем в КНР.

16 В частности, в 2001 году был создан офис информатизации Госсовета, а 2003 году Национальная малая группа координации кибер- и информационной безопасности разработала «Документ 27», который заложил основы политических решений по использованию ИКТ продукции в стране, в том числе, введение схем сертификации зарубежной ИКТ продукции, используемой в государственном секторе и критических информационных инфраструктурах, тестирования программного обеспечения для проверки его безопасности, продвижение ациональных криптографических алгоритмов для использования в коммерческом секторе (инфраструктура открытых ключей), разработки стандартов информационной безопасности, организации системных научных исследований и разработок. В 2014 году создана Центральная ведущая группа по кибербезопасности и информатизации, взят курс на переход на отечественное программное обеспечение, технологии и продукты.

17 Закон о криптографии КНР (1999).

многоуровневой системы защиты (MLPS) сертификация распространена на все импортное программное обеспечение.

2.3. Третий этап — курс на мировое лидерство в передовых технологиях

Современный, третий этап отличается модернизацией общества и экономики на основе инноваций, усилением конкурентоспособности китайской продукции на глобальных рынках. Китай потенциально готов стать мировым лидером в передовых технологиях, в связи с чем интенсивность системных действий по всем направлениям усилилась. В течение короткого периода были приняты взаимодополняющие друг друга документы стратегического планирования: **План национальной стратегии инновационного развития** (2016)[18], **Стандарты Китая 2035** (2016)[19], **План развития нового поколения искусственного интеллекта** (2017)[20], опубликована программная **Белая книга по блокчейн индустрии в Китае** (2018)[21].

Дополнительные меры развития цифровой экономики вошли в План 14-й пятилетки (2021–2025 годы), а в апреле 2023 года Госсовет КНР объявил это направление деятельности главным приоритетом страны[22]. Китай намерен формировать конкурентоспособные в глобальном масштабе цифровые промыш-

---

18 В Плане сделан акцент на продвижение технологий сетевой безопасности для защиты экономических преобразований и поддержания национальной сетевой безопасности.

19 «China Standards 2035» является важнейшим документом, обеспечивающим разработку национальных технологических стандартов по всему спектру передовых технологий и обеспечению их безопасности, создание системы мер для продвижения их на международный уровень, что будет способствовать более широкому распространению китайской ИКТ-продукции. Включает реорганизацию Национального комитета по киберстандартам, Национального технического комитета по информационной безопасности (NISSTC), введение новой схемы многоуровневой системы защиты ИКТ-продукции (MLPS 2.0).

20 В 2017 году правительство Китая выделило колоссальную сумму ¥150 млрд ($21,5 млрд) на программы развития искусственного интеллекта (ИИ) до 2030 года. К концу 2019 года создано 15 крупных инновационных научно-производственных кластеров по ИИ, где исследователи получают открытый доступ к уже созданным инструментам и библиотекам программного обеспечения, массивам Больших данных и вычислительным ресурсам. Источник: Guideline on Next Generation AI Development Plan, Chinese Government, State Council, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/.

21 Планы широкого внедрения технологии блокчейн были заложены в программу 13 пятилетки и развиты в планах 14 пятилетки (2021–2025), когда блокчейн по значимости был поставлен в один ряд с искусственным интеллектом, Большими данными и облачными вычислениями. Для ускорения внедрения технологии Китай реализовал беспрецедентный проект — национальную сеть для приложений блокчейн Blockchain Services Network (BSN), сделав себя в этой сфере практически недосягаемым для конкурентов. В 2020 году сеть была разделена на две связанные между собой экосистемы: национальную BSN China и международную BSN International, ее виртуальные узлы запущены в Гонконге, Сингапуре, Калифорнии, Париже, Сиднее, Сан-Паулу и Макао. Китай также нацелен использовать BSN для построения универсальной цифровой платёжной сети (UDPN) на основе цифровых валют центральных банков. Благодаря этому цифровой юань при прямых расчетах в национальных валютах станет независимой альтернативой системе SWIFT. Источник: Цифровые международные отношения, В двух томах. Том 1. Учебное пособие для ВУЗов под ред. Е.С. Зиновьевой, С.В. Шитькова, Т.1, изд. «Аспект пресс» 2023, С.82.

22 Предполагается ускорение крупномасштабного коммерческого применения мобильной связи 5G. Китай уже готов подключить более 500 млн домохозяйств к оптической сети со скоростью 1 Гбит/с, Источник: Digital economy to receive top priority, China Daily, April 4, 2023, https://english.www.gov.cn/news/202304/04/content_WS642b78a4c6d03ffcca6ec072.html.

ленные кластеры[23], при этом основное внимание направлено на развертывание традиционной и новой инфраструктуры и дальнейшую трансформацию предприятий в использовании передовых ИКТ.

Прежде всего это развитие широкополосных сетей связи. К июлю 2023 года в стране построено 6 млн базовых станций 5G[24], т.е. менее чем за 3 года мощности увеличены в 25 раз. Общий объем инвестиций в строительство сетей 5G к концу 2025 года достигнет 170 млрд долл. США. При этом общий экономический эффект, прямо или косвенно вызванный коммерческим использованием этой технологии в стране в период с 2020 по 2025 годы, должен достичь 3,5 трлн долл. США [13]. Дан старт программе «**5G плюс Промышленный Интернет**», в рамках которой уже создано более сотни крупных промышленных интернет-платформ, более 1800 производственных интернет-проектов 5G+, охватывающих 10 ключевых отраслей.

Технологии Интернета вещей являются основным источником Больших данных, которые объявлены Китаем национальным стратегическим ресурсом и фактором производства. Для его использования Министерство промышленности и информационных технологий в пятилетнем **Плане развития Больших данных** поставило цель к концу 2025 года достичь 25% годового темпа роста этого сектора ИКТ-отрасли, повысить коммерческое использование данных за счет разработки рыночного механизма их ценообразования, увеличить вычислительные мощности для обработки и развития передовых услуг, основанных на Больших данных, занять ведущую роль в разработке международных технологических стандартов в этой сфере, а также усилить контроль над трансграничной передачей данных.

Для достижения поставленных целей в июле 2023 года дан старт новой технологической инициативе по развитию «**Индустрии вычислительных мощностей**» как ключевых производительных сил в условиях четвертой промышленной революции. Инициатива включает 20 мер улучшения использования данных, в том числе за счет создания по всей стране (особенно в западных провинциях) современных центров обработки данных[25]. Их планируется объединить с национальными суперкомпьютерами в сеть C2NET, уже сейчас ее вычислительная мощность составляет более 3 экзафлопс[26].

---

23 Например, на уровне провинций (Пекин, Шанхай, Гуйчжоу, Хэбэй, Цзянсу, Чжэцзян, Хунань, Шэньчжэнь и Хайнань) создаются индустриальные парки, которым предоставлены разнообразные программы поддержки.

24 С апреля по июнь в КНР установили 600 тысяч вышек мобильной сети, общее количество станций приблизилось к трем миллионам, 21 июня 2023, Источник: https://bigasia.ru/kitaj-uskoryaet-stroitelstvo-bazovyh-stanczij-5g/.

25 В 2022 году Китай запустил мега проект, предусматривающий строительство 8 национальных вычислительных центров и 10 национальных кластеров центров обработки данных, что позволит снизить диспропорцию территориального распределения ресурсов и повысить эффективность их использования.

26 Flops — единица измерения производительности суперкомпьютеров, составляющая 1018 операций с плавающей точкой в секунду. На данный момент быстродействие самого мощного суперкомпьютера Frontier (США) составляет 1,2 экзафлопс. По данным Statistica за 2022 год из 500 самых высокопроизводительных компьютеров в Китае расположены 173, в США – 128, при этом эксперты отмечают, что данные о последних

Такие масштабные планы свидетельствуют, что решение 20 съезда КПК «сделать великое возрождение китайской нации необратимым историческим процессом» будут выполнены [14]. Однако для такого высокого уровня информатизации общества и производства риски информационной безопасности становятся критичными для экономических преобразований, модернизации и поддержания цифрового суверенитета, поэтому правительство КНР признало кибербезопасность неразрывной составляющей национальной безопасности [15]. В соответствии с этим тезисом государственная политика в этой сфере тоже модернизирована.

В ноябре 2017 года принята первая **Национальная стратегия безопасности киберпространства Китая** [16], разработанная Государственной канцелярией Интернет-информации. В документе изложена целостная концепция кибербезопасности, направления преобразования системы государственного управления сетевым пространством и обеспечения информационной безопасности, также определены интересы КНР в международном сотрудничестве. Реализация стратегии должна обеспечить увеличение экономического роста и стабильности, защиту от любого вмешательства в политическую, социальную и культурную жизнь государства, защиту законных прав своих граждан в сети Интернет и руководящей роли КПК.

Говоря о национальных приоритетах, КНР в стратегии выделяет следующие основные угрозы:

1. Использование сетевых технологий для вмешательства во внутренние дела других государств, что подвергает рискам политическую стабильность и информационную безопасность граждан.

2. Компьютерные атаки, направленные на критические информационные инфраструктуры и угрожающие экономической безопасности и общественным интересам.

3. Разрушение традиционных культурных ценностей, физического и ментального здоровья путем распространения вредоносной онлайн-информации, что дает неверные ориентиры и ведет к снижению безопасности культуры.

4. Нарушение общественной безопасности, создание угроз гармонии и стабильности государства за счет использования ИКТ в террористических и экстремистских целях, для нарушения законов, осуществления компьютерных преступлений.

5. Нарастание конкуренции в киберпространстве за контроль его стратегических ресурсов, право устанавливать собственные правила и занимать стратегически важные руководящие посты, соревнование в запуске стратегических инициатив.

разработках Пекин не публикует, Источник: https://www.statista.com/statistics/264445/number-of-supercomputers-worldwide-by-country.

В документе определены четыре принципа развития политики в сфере кибербезопасности: уважение и защита суверенитета в киберпространстве; его мирное использование; управление киберпространством в соответствии с законами; всестороннее управление кибербезопасностью и развитием. В соответствии с ними будут решаться следующие стратегические задачи по защите национальных интересов для обеспечения суверенитета КНР, безопасности и развития в киберпространстве, продвижения его мирного использования и совместного управления:

- решительная защита суверенитета в киберпространстве, всеми доступными мерами — экономическими, административными, научными, технологическими, правовыми, дипломатическими и военными (т.е. официально признано, что национальная кибербезопасность имеет военное измерение[27]);
- решительная защита национальной безопасности, предотвращение и борьба с использованием сетевых технологий для призывов к государственной измене, сепаратизму, подстрекательству к восстанию; предотвращение и наказание по закону за кражу государственных секретов и другие действия, ослабляющие национальную безопасность, в том числе осуществляемые иностранными державами;
- применение всех необходимых законных мер для защиты критических информационных инфраструктур, обеспечение которых является зоной распределенной ответственности государства, бизнеса и открытого общества;
- укрепление системы сетевой культуры путем развития онлайн идеологии и культуры противостояния негативным воздействиям, использования возможностей сети Интернет для продвижения и обмена между различными культурами, стимулирования прогресса всего человечества;
- противодействие кибертерроризму, кибершпионажу, компьютерной преступности, онлайн торговле оружием и наркотиками, кражам персональной информации, распространению в сети порнографии и другого запрещенного контента, нарушению прав интеллектуальной собственности и другим видам незаконной деятельности;
- совершенствование систем управления сетью Интернет на основе законности, открытости и транспарентности, улучшение регулирующих струк-

27 В этой связи делается упор на следующие приоритеты: мониторинг негативно влияющих на репутацию страны информационных операций зарубежных государств, связанных с оповещением о неудовлетворенности китайской политикой или приписываемыми КНР действиями за рубежом (такими, как морские территориальные споры или обвинения Китая в хакерской деятельности); подготовка к военным действиям и обеспечение военного превосходства в случае киберконфликта с противником посредством военной модернизации, исследования методов осуществления кибероперации и развитие человеческого капитала; изучение военной инфраструктуры потенциальных противников, их мотивации, целей, возможностей и ограничений в информационном пространстве.

тур, связанных с обеспечением кибербезопасности, установление системы доверия, повышение научного уровня и стандартов управления кибербезопасностью; повышение роли общественных организаций в защите прав пользователей, создание условий для разработки и распространения безопасных ИКТ-продуктов и услуг, развитие инфраструктуры и плана действий «Интернет+» для ускорения цифровой экономики и внедрения собственных передовых технологий, оптимизации рыночных условий и укрепления рынка информационной безопасности; развитие политик подготовки кадров и повышения осведомленности пользователей;

- увеличение возможностей для защиты национального суверенитета в киберпространстве, создание для этого сил и средств, соразмерных международному положению Китая, развитие инструментов защиты и своевременного выявления вторжений в компьютерные системы и обеспечения устойчивости к ним, а также привлечение ресурсов компаний для защиты национального киберпространства;
- укрепление международного сотрудничества в киберпространстве за счет развития уважения, доверия, диалога и кооперации на двустороннем и многостороннем уровне; продвижение реформы глобальной системы управления Интернетом и интернационализации системы управления его адресным пространством, корневыми серверами и другими ключевыми ресурсами глобальной сети; поддержка лидирующей роли ООН по выработке международных общепризнанных норм в киберпространстве, универсального соглашения по противодействию терроризму в киберпространстве, полноценного механизма правовой помощи в отношении проявлений компьютерной преступности. Стратегия призывает к углублению международного сотрудничества в сфере политик и права, технологических инноваций, стандартов и норм реагирования на инциденты, защиты критической информационной инфраструктуры; оказанию поддержки и помощи развивающимся странам и отсталым регионам в целях сокращения «цифрового разрыва», распространению Интернет-технологий и развертыванию инфраструктуры, в том числе путем продвижения инициативы «Один пояс, один путь» и созыва Всемирной конференции по Интернету и других международных платформ для диалога о безопасном развитии глобальной сети.

Столь развитый и конкретизированный блок международных задач говорит о курсе страны на повышение ее роли в управлении глобальным информационным пространством.

3. Состояние нормативно-правовой базы в сфере развития ИКТ и передовых технологий, обеспечения национальной информационной безопасности

В КНР сформирована многоуровневая система правового и нормативно-технического регулирования в сфере исследования и разработки, безопасного производства, внедрения и использования ИКТ, а также контроля содержания распространяемой с помощью этих технологий информации[28]. Общее число законодательных актов, положений и норм, включая принятые администрациями провинций, превышает 140 [17]. По новой методике МСЭ оценки зрелости правового регулирования цифровизации уровень Китая признан развитым, т.е. использующим научный подход к регулированию и управлению, но пока не соответствующий уровню «лидирующий» [29].

Постоянным развитием правовой системы занимаются органы КПК, правительство, государственные ведомства, прежде всего Администрация по киберпространству Китая, специализированные органы в области стандартизации и местные власти. Главная задача — защита национального цифрового суверенитета Китая, общественных интересов и личных прав граждан. Ее решению служат строго регламентированные действия всех участников ИКТ-экосистемы: от частных пользователей, бизнеса и общественных объединений, до государственных структур[30], специальных служб и Национально-освободительной армии КНР (НОАК).

3.1. Закон о кибербезопасности (2016)

Закон о кибербезопасности (в некоторых источниках он именуется Законом о сетевой безопасности) принят Всекитайским собранием народных представителей и вступил в силу 1 июня 2017 года. Этот нормативный акт является базовым в обеспечении информационной и сетевой безопасности государства, поскольку определяет взаимоувязанную систему общих требований к разработке и сопровождению ИКТ-продукции, предоставлению и получению телекоммуникационных и цифровых услуг, безопасному использованию данных.

---

28 Интернет, СМИ, телевидение и радиовещание.

29 В методике «G5 Benchmark» оцениваются 4 параметра: межотраслевое управление на национальном уровне, принципы разработки политик, Инструментарий цифрового развития (кибербезопасность, защита данных, телекоммуникации в чрезвычайных ситуациях и совместное использование межотраслевой инфраструктуры), повестка дня в области цифровой экономики (инновационная система, цифровая трансформация, участие в международных и региональных интеграционных инициативах).

30 Например, Положение об усилении управления безопасностью веб-сайтов партий и государственных органов (2014).

Согласно закону, основная доля требований возлагается на действующих на основании лицензий поставщиков аппаратного и программного обеспечения и операторов, предоставляющих доступ к сети и цифровым услугам. Они обязаны обеспечивать безопасность своей продукции и сервисов, проводя периодические проверки на соответствие установленным требованиям безопасности, а в случае выявления уязвимостей принимать необходимые меры по нейтрализации угроз и информировать об этом пользователей и компетентные органы. При необходимости применения зарубежного программного или аппаратного обеспечения, в отношении них должны быть проведены процедуры сертификации или тестирования на безопасность. Критическое сетевое оборудование и специальные продукты для обеспечения информационной безопасности могут быть предоставлены для использования или продажи только после получения сертификатов.

Повышенные требования безопасности предъявляются к защищенности критических информационных инфраструктур (КИИ), к которым отнесены государственные информационные и коммуникационные службы, ключевые для национальной безопасности, экономики и общественных интересов, а также наиболее важные отрасли: энергетика, финансы, транспорт, водное хозяйство, коммунальные услуги, электронное управление и другие[31].

Закон запрещает анонимное получение сетевых сервисов и услуг. Каждый пользователь должен быть зарегистрирован оператором по паспортным данным и при подключении к сети проходить процедуру верификации. Кроме того, пользователь должен соблюдать правила «кибергигиены» и поведения в социальных сетях и на цифровых платформах. Например, запрещено распространять вредоносное программное обеспечение и противозаконную информацию, создавать сайты и коммуникационные группы для мошенничества и других видов преступлений.

На государственные органы возлагаются требования по организации системы контроля выполнения норм закона, разработке подзаконных актов и планов реагирования на чрезвычайные ситуации, защите КИИ от компьютерных атак, вмешательства в их функционирование или нарушение доступности, целостности и конфиденциальности данных. К компетенции государства относятся противодействие компьютерной преступности, борьба с использованием ИКТ в террористических, экстремистских и других противоправных целях.

---

31 После опубликования проекта закона начался процесс разработки профильными министерствами подзаконных актов, касающихся защиты подведомственной КИИ. Регуляторами введены административные меры: по обеспечению безопасности данных в промышленности и ИТ; по кибербезопасности медицины и организаций здравоохранения; обеспечению безопасности критических инфраструктур автомобильных дорог и водных путей; по кибербезопасности ценных бумаг и фьючерсов, по оценке безопасности облачных вычислений. Источник: https://www.dataguidance.com/opinion/china-revised-cybersecurity-review-measures.

За нарушение норм закона предусмотрена преимущественно административная ответственность: максимальный штраф может достигать 1 млн юаней (160 тыс. долл. США), а злостная и повторная незаконная деятельность может привести к блокировке бизнеса или отзыву лицензии. Важно отметить, что в этом законе впервые реализован экстерриториальный принцип — ответственность за совершение атак на критическую информационную инфраструктуру Китая может быть возложена на субъекты, действующие из других юрисдикций, а Министерство общественной безопасности и другие уполномоченные структуры могут принять решение о приостановке деятельности нарушителей закона на территории страны.

В развитие положений закона в августе 2021 года Госсоветом КНР одобрено **Положение об обеспечении безопасности КИИ**[32], которое дало правовое определение КИИ, возложило координирующие функции на уполномоченные ведомства, ввело персональную ответственность руководителей за эффективность деятельности по защите их объектов от атак, вторжений, вмешательства и уничтожения, а также определило меры поддержки и укрепления процедур оценки рисков и соблюдения стандартов информационной безопасности. В мае 2023 года вошли в силу разработанные уполномоченным органом новые **Административные меры по оценке кибербезопасности**[33], которые детально определяют действия операторов любых КИИ. Они должны представить уполномоченному органу отчет о защищенности своей инфраструктуры для оценки ее влияния на национальную безопасность КНР и внутренних пользователей платформы. В случае, если предоставляются услуги за рубежом или размещаются там акции, такая оценка должна быть проведена для получения разрешения от уполномоченного органа на направление данных зарубежному уполномоченному органу.

Другие нормативные акты также конкретизируют положения Закона о кибербезопасности. Так, в следующих двух законах продолжено формирование концептуального подхода Китая в сфере использования данных и обеспечения их безопасности.

---

32 Regulation on Protection of Security of Critical Information Infrastructure.

33 Меры разработаны Администрацией по киберпространству Китая. Согласно документу, оценке подвергаются следующие факторы риска:
-незаконный контроль, вторжение или разрушение КИИ, вызванные использованием продуктов и услуг;
-ущерб бизнес-сообществу в случае прекращения поддержки продуктов или предоставления услуг;
-безопасность, открытость, транспарентность и разнообразие источников продуктов и услуг, надежность цепочек поставок, риски потери поддержки по политическим, дипломатическим, экономическим и другим факторам;
-соответствие продуктов и услуг законам КНР, административным мерам и отраслевым правилам;
-кража, утечки, незаконное использование или вывод из страны ключевых, важных и персональных данных;
-влияние, контроль или вредоносное использование указанных данных и КИИ Китая правительствами других стран и другие риски, Источник: https://www.dataguidance.com/opinion/china-revised-cybersecurity-review-measures

3.2. Закон о безопасности данных (2021)

Указанный акт принят Постоянным комитетом Всекитайского собрания народных представителей[34] и введен в действие Указом главы КНР с 1 сентября 2021 года [18]. Он является важным шагом для повышения эффективности использования цифровых данных за счет регулирования всех видов деятельности, связанных с развитием рынка Больших данных, их использования государственными органами, коммерческими организациями и исследовательским сообществом, а также содействия интеграции с глобальной цифровой экономикой.

С учетом централизации всей деятельности в киберпространстве введена классификация типов данных по возможному ущербу для национальной экономики и социального развития от неправильного обращения с ними. Полномочия определять значимость данных для конкретных регионов и отраслей отданы центральным и региональным правительственным органам Китая. Градация важна для определения требований к обеспечению безопасности данных и условиям передачи их различным участникам рынка. Уполномоченный орган (Администрация по киберпространству Китая) должен осуществлять координацию деятельности по обеспечению безопасности данных, включая оценку рисков, мониторинг выполнения требований, систему раннего предупреждения и реагирования на чрезвычайные ситуации.

Кроме того, закон вводит требования локализации на материковой части Китая используемых КИИ данных; персональных данных граждан; хранения в течении 6 месяцев всей размещаемой в сети информации в интересах спецслужб.

Закон стал первой системной попыткой Китая осуществить правовые полномочия в отношении иностранных ИКТ-компаний, осуществляющих свою деятельность на территории Китая, а также китайских компаний, выходящих на зарубежные товарные и финансовые рынки. От них могут потребовать проведение проверки соблюдения мер кибербезопасности и сертификации уполномоченным органом используемых для этого средств и методов информационной безопасности, попросить раскрыть детали сетевой безопасности, применяемой в других юрисдикциях.

Нормы закона предусматривают ограничения на трансграничную передачу «ключевых» данных, в том числе по запросам правоохранительных органов других стран, если их обработка за пределами территории КНР наносит ущерб национальной безопасности, общественным интересам или законным интересам отдельных лиц или организаций Китая, а также затрагивает перемещение данных о товарах, услугах и технологиях, подпадающих под действие закона об экс-

34 Data Security Law of the People's Republic of China (Adopted at the 29th Meeting of the Standing Committee of the Thirteenth National People's Congress on June 10, 2021).

портном контроле. Кроме того, регламентируются действия надзорных органов за оборотом данных и определяется ответственность за нарушение норм закона (штраф до 10 млн юаней или 1,6 млн долл. США, приостановка бизнеса или отзыв лицензии).

На Министерство промышленности и информационных технологий возложены функции надзора за обеспечением безопасности данных в промышленном и ИКТ-секторе, определение требований безопасности для операторов обработки данных в этих отраслях.

3.3. Закон о защите персональных данных (2021)

Данный нормативный акт конкретизирует положения Закона о безопасности данных и выстраивает национальную систему защиты персональных данных, разработку стандартов и руководящих принципов для их сбора и использования, а также создание системы рассмотрения жалоб и споров в этой сфере. Под персональными данными в законе понимается любая информация, идентифицирующая физическое лицо, от которого в явном виде должно быть получено согласие на обработку данных.

Введено определение оператора обработки персональных данных. Благодаря этому, под действие закона впервые попали финансовые институты, а также цифровые платформы, которые аккумулируют данные более 1 млн пользователей. Операторы должны соблюдать строгие правила информирования пользователей о целях сбора информации, соблюдать стандарты ее использования и безопасности. Законом им запрещена передача персональных данных третьим лицам без согласия пользователя, а также введена правовая новация – нарушение «личной конфиденциальности» частных лиц (по смыслу близко праву на неприкосновенность частной жизни). Физические лица получают больше прав по защите их персональных данных, они могут требовать от операторов внесения изменений, исправления ошибок и удаления информации[35].

Персональные данные относятся законом к «ключевым», поэтому их хранение должно быть локализовано на материковой территории страны, в том числе зарубежными компаниями, осуществляющими бизнес в Китае. Однако сделаны некоторые шаги по обеспечению функционирования трансграничных китайских цифровых платформ и электронной коммерции. Так для легального экспорта персональных данных местным компаниям будет необходимо пройти оценку безопасности или получить сертификат от Администрации по киберпространству Китая, подписать договор с зарубежным получателем данных и осуществлять

35 Аналогичные требования содержатся в Федеральном законе РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных» и Общем регламенте обработки персональных данных ЕС (GDPR) от 27.04.2016 г.

надзор за его деятельностью в соответствии с установленными КНР стандартами защиты данных[36].

3.4. Закон о криптографии (2019)

26 октября 2019 года Постоянный комитет Всекитайского собрания народных представителей принял закон о криптографии, который вступил в силу с 1 января 2020 года. Он регламентирует использование средств криптографической защиты для обеспечения информационной безопасности в трех сферах: защита государственной тайны, обеспечение конфиденциальности чувствительной информации, применение коммерческой криптографии на основе инфраструктуры открытых ключей (PKI) в электронной коммерции и других ИКТ-услугах цифровой экономики. Кроме того, закон определил наказания за нарушения норм информационной безопасности в государственных системах и правила разработки криптографических стандартов.

Как уже отмечалось выше, первостепенное внимание руководства государства обращено на обеспечение единства нации и защиту традиционной культуры. Для этого реализована техническая система «Золотой щит» (Great Firewall of China)[37], которая фильтрует запрещенный контент и ограничивает доступ с территории Китая к определенным зарубежным веб-ресурсам и сервисам, при этом законом запрещено использование VPN (виртуальных персональных сетей) для обхода этой блокировки. Администрацией киберпространства Китая планомерно формируется всеобъемлющее нормативное регулирование размещения информации в сети Интернет и предоставление к ней услуг доступа посредством различных сервисов[38].

---

36 Принято несколько административных регламентов, определяющих правила трансграничной передачи данных: Measures for the Security Assessment of Cross-border Data Transfer (2022); Rules on Authentication of Personal Information Protection (2022); Provisions on Strengthening the Management of Confidentiality and Archives in the Overseas Issuance and Listing of Securities by Domestic Enterprises (2022); Guidelines for the Declaration of the Security Assessment of Cross-border Data Transfer (проект); Standards for Security Authentication of Cross-border Processing Activities of Personal Information (проект); Regulations on Standard Contracts for the cross-border transfer of Personal Information (проект). Источник: https://hsfnotes.com/data/2022/07/13/important-updates-on-cross-border-data-transfer-in-china/.

37 В 1996 г. Госсовет КНР выпустил распоряжение, регулирующее связь локальных китайских провайдеров с международными точками обмена трафиком. В соответствии с подготовленным документом, «организации, предоставляющие услуги доступа к международным каналам, должны создать Центры управления сетью в целях усиления контроля над своими клиентами согласно законам и нормативным актам, а также в целях обеспечения лучшей защищённости и для обеспечения безопасности предоставляемого клиентам сервиса».

38 Перечень основных нормативных актов включает: Administrative Provisions for the Internet Audio-Video Programme Service (2007); Online Publication Provisions (2016); Provisions on Administration of Web Publishing Services (2016); Regulations on the Administration of Private Network and Directional Transmission of Audio-visual Programme Services (2016); Regulations on Administration over the Internet News Information Services (2017); Implementing Rules for the Administration of the Licensing for Internet News Information Services (2017); Administrative Measures on Internet Information Services (2000); Administrative Provisions on Internet Follow-up Comment Services; Administrative Provisions on Internet User Account Information; Administrative Provisions on Internet Pop-Up Information Push Services (2022).

3.5. Положение о контроле распространения дипфейков (2022)

Положение **«Об управлении Deep Synthesis технологиями на информационных сервисах в Интернете»** [19] разработано Администрацией по киберпространству Китая совместно с Министерством промышленности и информационных технологий и Министерством общественной безопасности, оно вступило в силу 10 января 2023 года. Таким образом, Китай стал первым государством, которое ввело комплексное законодательное регулирование по противодействию распространению «дипфейков», в документе под предметом регулирования понимается цифровой контент, искусственно сгенерированный с помощью технологий генеративных состязательных сетей, генеративного искусственного интеллекта, виртуальной и дополненной реальности, создающий угрозы в сфере прав и основных свобод человека и гражданина, а также государственного управления, общественной безопасности и общественного порядка.

Положение требует от производителей и провайдеров онлайн услуг применения технологий маркировки «дипфейков», их выявления, регистрации и верификации пользователей, контроля доступа к контенту и управления информационной безопасностью. Отраслевые организации должны способствовать усилению самодисциплины и структур управления дисциплиной, установлению норм и стандартов отрасли, улучшению управления информационной безопасностью контента[39]. Частным и юридическим лицам запрещено призывать к незаконной деятельности или посягать на чужие законные права и интересы, злоупотребляя сервисами «глубокого синтеза». Нарушение правил является основанием для применения мер административно-правового характера (штрафы 10–100 тыс. юаней), в отдельных случаях предусмотрена уголовная ответственность.

Важно отметить, что ограничений на создание и использование аудиовизуальных материалов, сгенерированных с помощью технологий «дипфейк» (за исключением использования в целях распространения ложной информации и новостей) не установлено, что будет способствовать развитию этих технологий в законных целях, например, в индустрии развлечений, образовании, медицине, торговле. Надзор за соблюдением указанных норм возложен на Государственную канцелярию Интернет-информации Госсовета, а на местном уровне — на соответствующие департаменты в администрациях.

---

39 Основная часть требований к провайдерам услуг установлена в 2018 году «Положением об оценке безопасности информационных интернет-сервисов, обладающих характеристиками формирования мнений или способных к социальной мобилизации» (Provisions on the Security Assessment of Internet Information Services with Characteristics of Opinions or Capable of Social Mobilization). Провайдеры открытых форумов, стриминговых платформ и других видов услуг доступа к информации обязаны проводить самооценку выполнения требований: верификации подлинности пользователей, принятых технических мер защиты персональных данных; внутренних механизмов обзора контента.

С 15 августа 2023 года вступили в силу **Временные меры по управлению генеративными службами искусственного интеллекта** [20].

В случае выявления криминальной, террористической, сепаратистской или другой запрещенной деятельности применяются следующие законы.

3.6. Антитеррористический закон (2015)

Помимо антитеррористической деятельности закон регламентирует действия органов общественной и государственной безопасности, структур НОАК по использованию технических средств в интересах оперативно-следственных мероприятий. На указанные органы возложены полномочия по дешифровке интернет-трафика, применение административных мер по изъятию у иностранных компаний и предприятий информации при подозрении в ее использовании для террористических целей, введение цензуры для новостной деятельности на территории КНР.

3.7. Закон о национальной безопасности (2015)

Статья 25 закона гласит: Государство создает национальную систему безопасности сети и информации; повышает потенциал защиты сети и информации; расширяет инновационные исследования; разрабатывает и использует сетевые и информационные технологии; внедряет основные методы безопасности и ключевую инфраструктуру для сетей и информации, информационных систем в важных областях, а также данных; улучшает управление сетью; предотвращает и прекращает незаконную и преступную деятельность в сетях, такую как сетевые атаки, проникновение в сеть, компьютерные кражи, распространение незаконной или вредоносной информации; поддерживает суверенитет киберпространства, безопасность и интересы развития[40].

Столь обширная и многоуровневая нормативная база создает большие сложности для контроля соблюдения ее положений, формирует барьеры быстрому внедрению инноваций за счет высоких затрат на выполнение многочисленных требований. При этом всеобъемлющими регуляторными рамками охвачены все сферы, необходимые для эффективного развития цифровой экономики, от кибербезопасности и криптографии, защиты данных и КИИ до научно-технического развития, что создает единую регуляторную систему. На повестке дня стоит завершение разработки подзаконных актов и необходимых технологических стандартов [21].

40 Детализация норм закона содержится в Положении о надзоре и проверке кибербезопасности органами общественной безопасности (2018).

Следует подчеркнуть, что обновление законодательной базы и технических стандартов информационной безопасности в КНР идет очень высокими темпами. Китайская академия информационно-коммуникационных технологий в 2022 году опубликовала Белую книгу по киберзаконодательству [22], где обозначены стратегически важные направления нормотворчества и ключевые принципы регулирования — системность и исполнимость правовых норм. Содержание документа однозначно свидетельствует, что в целях достижения национальных и геополитических интересов Китая взят курс на выстраивание эффективного сотрудничества государства и бизнеса.

4. Национальная система обеспечения информационной безопасности

Особенностью национальной системы обеспечения информационной безопасности Китая является некоторое дублирование функций органами КПК и Государственного совета КНР, а также значительной ролью в ней органов военного управления и НОАК. В частности, правом законодательных инициатив наделен Всекитайский съезд КПК и ЦК КПК, функциями контроля обладает Секретариат КПК[41], в подчинении которого находятся различные комиссии. Для оптимизации взаимодействия при решении конкретных задач создаются партийные и государственные ведущие, большие и малые группы, объединяющие руководителей государства, комитетов КПК и отдельных ведомств Госсовета (См. Схему).

4.1. Органы в структуре ЦК КПК

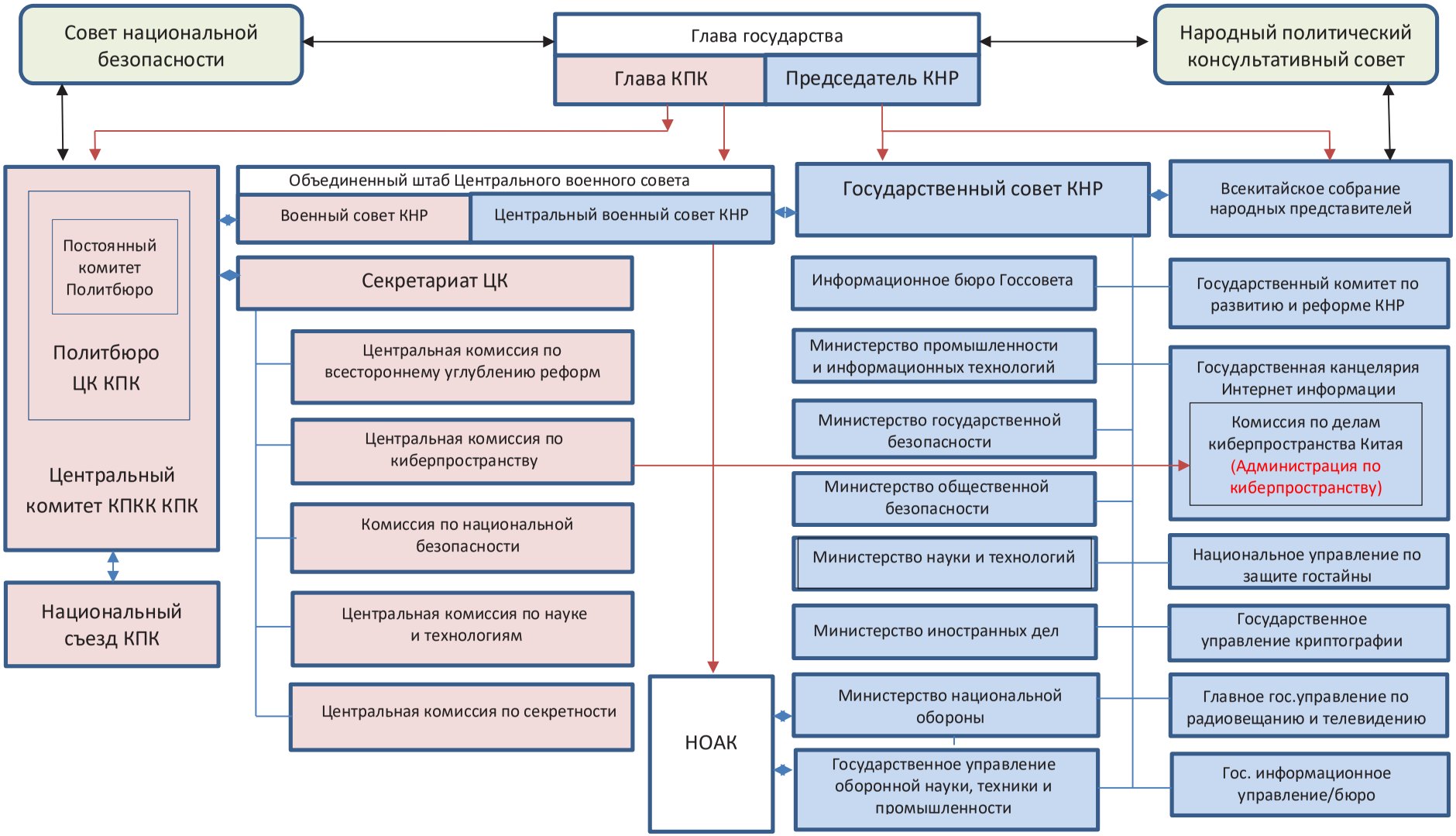
4.1.1. Центральная комиссия по киберпространству

Эта комиссия создана на основе одноименной Ведущей Центральной группы в результате партийной и государственной реформы 2018 года. Ее возглавляет лично Председатель КНР Си Цзиньпин — Генеральный секретарь КПК и Председатель Центрального военного совета КНР. Его заместителями являются глава Госсовета КНР и член Постоянного комитета Политбюро ЦК КПК, отвечающий за агитацию, пропаганду и идеологическую работу. В состав комиссии входят руководители Министерства общественной безопасности, Объединенного штаба Центрального военного совета[42], МИД, идеологических структур ЦК КПК,

41 Членами Секретариата являются 6 высокопоставленных должностных лиц, деятельность которых обеспечивают несколько управлений и центров. В частности, Секретариат контролирует работу Организационного отдела, Центральной канцелярии, Отдела пропаганды, Отдела Единого фронта и Отдела международного сотрудничества, их начальники по должности входят в состав Секретариата.

42 Военный совет ЦК КПК аналогичен составу Центрального военного совета Китая.

Общая схема обеспечения национальной информационной безопасности КНР



а также ряда других ведомств. Такой состав комиссии отражает ее значимость в управлении страной.

Функции ее исполнительного органа выполняет **Комиссия по делам киберпространства Китая** в структуре Государственной канцелярии Интернет-информации Китая Госсовета КНР, она же — Администрация по киберпространству Китая (см. Раздел 4.2.2). Это позволяет придать структуре КПК легитимность, как органа государственной власти.

4.1.2. Центральная комиссия по науке и технологиям

Комиссия занимается координацией программ научных исследований и трансфера технологий. В соответствии с решением 20 съезда КПК она будет обновлена в целях усиления контроля над ИКТ-отраслью.

4.1.3. Комиссия по национальной безопасности

Эта комиссия определяет и курирует весь комплекс задач в сфере обеспечения национальной безопасности.

4.1.4. Комиссия по секретности

Канцелярия этой комиссии организационно подчинена непосредственно Главной Канцелярии ЦК КПК и наделена директивными функциями, имеет и другое наименование — Государственное управление по секретности Госсовета КНР. Ее полномочия определены в «Законе КНР о защите государственной тайны» (2010) и в положениях о его реализации (2014). В структуре канцелярии Комиссии есть Научно-техническое управление, кроме того подведомственными организациями являются: Центр научно-технической оценки обеспечения секретности; Центр оказания технических услуг в вопросах обеспечения секретности в Шэньчжэне; Центр утилизации носителей секретной информации из органов ЦК КПК и государственных органов[43]; издательство «Цзиньчэн».

4.1.5. Совет национальной безопасности

Совет создан КПК в ноябре 2013 года для «координации принятия ключевых решений в области национальной безопасности, обороны, разведки, дипломатии и общественной безопасности». По функциям он близок Совету безопасности Российской Федерации и Совету национальной безопасности США.

43 Вторая «вывеска» — Центр оказания технических услуг в вопросах секретности для органов ЦК КПК и государственных органов.

4.2. Государственные органы, в системе обеспечения национальной информационной безопасности, подчиненные Госсовету КНР

Государственный совет КНР является правительством страны, возглавляется премьер-министром. Основная функция Совета — управление экономикой, поэтому не относящиеся к этому блоку министерства (обороны, государственной и общественной безопасности, культуры) напрямую взаимодействуют с кураторами из Политбюро КПК.

В части обеспечения технических аспектов цифрового суверенитета и информационной безопасности ключевыми органами Госсовета КНР являются следующие структуры.

4.2.1. Государственный комитет по развитию и реформе

Обеспечивает реализацию государственной стратегии развития индустриализации нового типа, выполняет функции межведомственной координации всех задействованных сторон. В части инновационного развития в ИКТ-сфере и информационной безопасности его Департамент промышленности[44] разрабатывает программы и производственную политику основных промышленных отраслей, руководит разработкой их нормативно-технических актов и стандартов, координирует работу по освоению и обновлению важнейших заимствованных технологий и комплексного оборудования. Департамент высокотехнологичных отраслей Комитета помимо выработки стратегий и программ развития организует трансфер ключевых технологий во все сферы экономики, организует и стимулирует их технологическое обновление в сочетании с повышением эффективности образования и исследований.

Напрямую Госкомитету подчиняются: НИИ безопасности, а также созданный по решению 20 съезда КПК новый орган — **Государственное управление данных Китая** (встречается наименование Национальное бюро данных). Оно получило функции регулятора в сфере обработки, использования и трансграничной передачи данных для достижения целей национальной стратегии Больших данных, а также координатора развития цифровой экономики и цифрового общества[45]. Новый орган будет исследовать различные цифровые риски, включая

44 Департамент выполняет функции Канцелярии Руководящей группы по работе исполнения Конвенции о запрещении химического оружия, Канцелярии по редкоземельным ископаемым, Канцелярии по управлению производством.

45 Основой для работы Госуправления станет Национальная интегрированная система Больших данных, основная часть которой должна быть введена в строй в 2025 г. В исходный каталог внесены сведения о более чем 3 млн государственных библиотек данных и свыше 20 млн информационных записей: данные о населении Китая, юридических лицах, природных ресурсах и национальной экономике. Система будет постоянно пополняться и расширяться: в неё планируется включить информацию об электронных лицензиях, медицине и здравоохранении, финансовых организациях, кредитных сервисах и пр. Источник: China outlines plan for National Integrated Government Affairs Big Data System, https://www.theregister.com/2022/10/31/china_government_big_data_system/.

использование алгоритмов для манипуляций с данными, эксплуатацию уязвимостей систем безопасности для осуществления компьютерных атак на алгоритмы обработки данных и их хранение.

4.2.2. Государственная канцелярия Интернет-информации Китая

Учреждена Госсоветом КНР 4 мая 2011 года, подчинена Пресс-канцелярии Госсовета КНР[46]. Это цензурный, надзорный и контролирующий орган, обеспечивающий информационную безопасность национального сегмента сети Интернет. Госканцелярия состоит из двух структур.

Службы **Центральной комиссии по делам киберпространства** (Администрация по киберпространству Китая [23]), которая напрямую подчиняется Центральной комиссии по киберпространству КПК. На нее возложены задачи по координации межведомственной деятельности по совершенствованию правовой, административной и технологической системы распространения Интернет-информации, по усилению контроля за информацией и контентом в национальном сегменте сети Интернет, административному лицензированию бизнес-проектов[47].

В состав Администрации по киберпространству входят более 20 подразделений, в части обеспечения информационной безопасности следует отметить следующие:

- Центр управления чрезвычайными ситуациями в области Интернет-безопасности.
- Центр отчетов о незаконной и негативной сетевой информации (по задачам близок к Роскомнадзору РФ).
- Бюро распространения новостной информации и анализа комментариев в Интернете, социальных сетях.
- Управление исследований политики (Правовое бюро).
- Бюро по комплексному управлению координацией и правоохранительным надзором.
- Бюро кибербезопасности.

---

46 Главой Государственной канцелярией Интернет-информации Китая является руководитель Пресс-канцелярии Госсовета, его заместители – вице-министр промышленности и информатизации КНР и заместитель министра общественной безопасности.

47 С 2011 г. зарегистрировать доменные имя может только юридическое лицо, получив лицензию на сайт. Согласно правительственным постановлениям, в сети Интернет должны быть закрыты все частные видео-хостинги, а официальное разрешение на размещение видеороликов в сети получат только государственные компании. В качестве альтернативы зарубежным хостингам было предложено либо создавать совместные предприятия с китайскими госкомпаниями, либо переносить техническую часть проектов на серверы и сети государственных телекоммуникационных компаний, с предоставлением полного доступа к системам видеообмена. В отношении ряда работающих на китайском рынке международных компаний, таких как Google, Yahoo, Microsoft, установлены фильтры, которые блокируют доступ к неблагонадежным, с точки зрения китайских властей, сайтам. В рамках борьбы с пиратством и распространением порнографии гражданам КНР также закрыт доступ к торрент-трекерам и социальным ресурсам, таким как YouTube, Facebook, Twitter.

• Бюро международного сотрудничества.

Администрации по киберпространству подчинены Китайский фонд развития Интернета, Исследовательский институт киберпространства, Китайский центр информации в сети Интернет, Центр изучения общественного мнения в Интернете [24].

Государственное информационное бюро Интернета (англ. SIIO) создано в 2011 году путем передачи части функций из Информационного бюро Госсовета КНР. В 2023 году ему передана часть задач по контролю Интернета от Администрации по киберпространству, также его задачами будут содействие разработке межотраслевых информационных ресурсов, развитие «умных» городов и строительство передовой цифровой инфраструктуры.

4.2.3. Министерство промышленности и информационных технологий

Министерство является регулятором ИКТ-отрасли и представляет интересы КНР в Международном союзе электросвязи. Оно является главным потребителем инновационных технологий в промышленности и связи, а также организатором общенациональной платформы научных исследований, обеспечивая открытый доступ к ее инфраструктуре и ресурсам. В связи с чем отвечает за разработку планов фундаментальных и прикладных исследований, программ и стандартов, развитие национальной системы трансфера технологий, повышение коммерческой эффективности результатов НИОКР за счет координации взаимодействия с университетами и исследовательскими институтами, укреплению интеграции гражданской и военной науки, надзор за Национальным фондом естественных наук Китая.

Министерство напрямую отвечает за технические аспекты информационной безопасности, в его ведении находится Центр сертификации безопасности информационных технологий [25], который ведет Национальную базу уязвимостей (China National Vulnerability Database, CNNVD) и осуществляет проверку реальной защищенности государственных информационных систем и КИИ. Подчинены министерству Национальные лаборатории разработок мобильных систем, технологий безопасности промышленных систем контроля, комплексной безопасности Больших данных.

В функции ведомства также входит привлечение зарубежных высокопрофессиональных специалистов, выявление и поддержка талантливой молодежи, повышение квалификации персонала государственных учреждений.

4.2.4. Министерство общественной безопасности

Основные функции министерства — пресечение противоправных действий, таких как терроризм, экстремизм, сепаратизм, в том числе с использованием ИКТ;

обеспечение деятельности сети профильных национальных лабораторий. Для борьбы с компьютерной преступностью в 2015 году на базе ранее действовавших подразделений в министерстве создана единая специализированная структура — **Сетевая полиция**, которая имеет подразделения во всех административных районах страны [26]. Для выполнения своих функций министерство поддерживает каналы взаимодействия с правоохранительными органами других стран.

Кроме того, Министерство общественной безопасности отвечает за единую научно-технологическую политику в сфере защиты критических информационных инфраструктур, в связи с чем является разработчиком технических стандартов и нормативных актов, осуществляет надзор за соблюдением требований сетевой безопасности, контролирует отрасль информационной безопасности, ведет мониторинг угроз и обеспечение безопасности национального сегмента сети Интернет.

4.2.5. Министерство государственной безопасности

Основными задачами министерства является внешнеполитическая разведка и осуществление контрразведывательных функций на территории страны[48], в том числе предотвращение или пресечение подрывной деятельности иностранных спецслужб против КНР и борьба против международного терроризма, внутреннего сепаратизма, и религиозного экстремизма. Значительные силы и средства министерства направлены на добывание разведывательной информации о передовых технологиях и потенциальных противниках КНР.

Выполнение этих задач требует комбинации различных инструментов, для чего вся разведывательная информация централизованно обрабатывается. Ключевыми структурами в этой сфере являются:

- 3-е управление, занимающееся научно-технической и экономической разведкой;
- 13-е управление, отвечающее за научно-техническое обеспечение технической разведки, в его составе действует Центр оценки информационной безопасности, который несет ответственность за устойчивость информационных систем правительственных структур и безопасность используемого в них программного обеспечения и аппаратного обеспечения;
- 14-е управление, занимающееся технической разведкой и его 11-е бюро, осуществляющее радиоэлектронную и компьютерную разведку;
- 16-е управление получает разведывательную информацию из обработки видеоматериалов.

48 Деятельность осуществляется на основе Закона КНР о государственной разведке от 27.06.2017, Закона КНР о контрразведке от 1.11.2014 и Подробными положениями о его реализации, утвержденного Постановлением №692 Государственного совета КНР 22.11. 2017 года.

В подчинении министерства находятся Китайский исследовательский институт современных международных исследований, Институт международных отношений, Социальный институт Цзяннань [27].

Для выполнения функций по анализу настроений и высказываний в Интернете министерством проводятся оперативно-технические мероприятия по мониторингу и анализу контента, в том числе в социальных сетях. В августе 2023 года МГБ КНР создало собственный аккаунт в китайской социальной сети WeChat[49], который используется для создания системы «народной защиты национальной безопасности от шпионажа».

4.2.6. Министерство обороны

Министерство дает легальную возможность НОАК участвовать в национальной системе защиты цифрового суверенитета и информационной безопасности. Основные его функции состоят в надлежащей защите собственных информационных сетей и систем, подготовке к противоборству в киберпространстве в случае вооруженного конфликта, включая разведку и информационные операции.

Кроме того, министерство участвует в концептуальном осмыслении проблемы МИБ в контексте защиты страны от внешних угроз, его эксперты активно участвуют в международных форумах.

4.2.7. Министерство науки и технологий

В структуре министерства действует Бюро общественной информации и надзора за сетевой безопасностью.

В некоторых источниках это министерство указывается в качестве разработчика национальной программы электронного правительства, которая отличается от других государств, поскольку существенно больше ориентирована на цифровое взаимодействие между ведомствами и региональными правительствами[50]. По данным ежегодного исследования ООН, КНР впервые вошла в группу стран с «очень высоким уровнем» развития электронного правительства в 2020 году, но отставание по таким критериям оценки, как готовность инфраструктуры, территориальная равномерность доступа к услугам, вовлеченность граждан, по-преж-

---

49 По данным за первый квартал 2023 г. ежемесячное количество активных пользователей WeChat по всему миру составляет 1,3 млрд чел. Источник: https://www.statista.com/statistics/255778/number-of-active-wechat-messenger-accounts/.

50 В 1999 году положено начало создания программы. В 2018 г. Госсовет КНР потребовал дальнейшего продвижения курса «интернет + госуслуги» в «Руководящих мнениях об ускорении развития общенациональной интегрированной платформы госуслуг». Техническая платформа предоставления доступа к госуслугам была запущена в 2019 г., она объединила платформы 31 административного субъекта и примерно 40 центральных ведомства, что в совокупности дало доступ к более 3 млн услуг. Источник: В.В. Кузнецова Практика цифровизации государственного управления в Китае, https://spa.msu.ru/wp-content/uploads/fgu_czifrovizacziya_pravit_kuzneczova.pdf.

нему удерживает Китай в четвертой десятке мирового рейтинга. Огромный толчок в развитии перечня услуг электронного правительства сыграли программы «умных» городов и эпидемия COVID-19.

На стратегическом уровне основные органы управления электронными государственными услугами включают: Центральную комиссию по сетевой безопасности и информации, Госкомитет по развитию и реформе, Центральную канцелярию Госсовета КНР, Общий отдел ЦК КПК. На уровне местных правительств действуют от одного до нескольких органов управления.

4.2.8. Иные структуры технологического блока

Среди важных государственных органов, имеющих отношение к разработке и регулированию использования технологий защиты информации следует упомянуть следующие:

Национальное управление по защите государственной тайны, которое обеспечивает выработку и контроль выполнения единых требований к защите засекреченной информации и функционирование Центра оценки безопасности информационных технологий.

Государственное управление криптографии ответственно за разработку, использование и оборот средств криптографической защиты информации.

Государственное управление оборонной науки, техники и промышленности вносит большой вклад в разработку средств защиты ИКТ.

Главное таможенное управление, которое в своем Центре сертификации информационных технологий осуществляет тестирование зарубежной ИКТ-продукции на соответствие национальным требованиям безопасности.

Национальная администрация по стандартизации КНР (подчинена Государственной администрации по регулированию рынка) координирует все действия по разработке и внедрению национальных и промышленных стандартов, представляет Китай в международных органах стандартизации (ИСО, МСЭ, Международной электротехнической комиссии и др.), тесно сотрудничает с Китайской ассоциацией стандартизации (CAS), Национальным институтом стандартизации Китая, Национальным институтом метрологии и отраслевыми органами.

Академия наук КНР, Центр исследования проблем развития, Исследовательский центр при Госсовете КНР и другие государственные научные учреждения, занимающиеся разработкой передовых ИКТ и их безопасностью.

В части обеспечения контроля в сфере оборота информации, благонадежность которой является неотъемлемой частью информационной безопасности страны, ключевыми органами Госсовета являются следующие ведомства.

4.2.9. Государственное управление по радиовещанию и телевидению

Управление создано на базе ранее существовавших Государственного управления по делам радио, кино и телевидения (1998–2013) и сменившего его Государственного управления печати, публикации, радио, кино и телевидения (2013–2018). Подчиняется напрямую Госсовету КНР.

Управление владеет и эксплуатирует, а также управляет многими тысячами релейных передатчиков МВт, FM, ТВ и коротковолновых диапазонов в Китае и арендованными за границей для внешнего вещания. Определяет технологическую политику и стандарты в указанных сферах деятельности. В функционал управления входит: регулирование деятельности всей индустрии радиовещания, телевидения, генерации и хостинга Интернет-контента, выявление запрещенного контента и блокировка распространяющих его ресурсов в китайском сегменте Интернета, также содействие продвижению китайских медиа-продуктов на внешние рынки.

Кроме того, ряд государственных ведомств выполняют иные важные функции в системе обеспечения цифрового суверенитета и информационной безопасности страны.

4.2.10. Министерство иностранных дел

Одной из задач МИД КНР является сопровождение национальной деятельности в сфере международной информационной безопасности. К ее решению подключены следующие департаменты министерства:

- правовой: курирует вопросы противодействия транснациональной преступности и киберпреступности, обсуждаемые на площадках ООН;
- международных организаций и конференций: участвует совместно с Министерством промышленности и информатизации в решении вопросов в формате МСЭ;
- информации: координирует деятельность с Пресс-канцелярией Госсовета;
- контроля над вооружениями и разоружением: отвечает за продвижение тематики МИБ в ООН, ШОС и других международных организациях, а также осуществление двусторонних контактов.

4.2.11. Комитет по управлению и контролю над ценными бумагами

Критические информационные инфраструктуры в финансовой и банковской отрасли относятся к одним из самых чувствительных в сфере обеспечения информационной безопасности. Поэтому в 2022 году для них были существенно ужесточены правила обеспечения конфиденциальности информации, в том числе персональных данных. Комитет является контролирующим органом по реализации указанной политики. В структуру комитета входят Национальная администрация финансового регулирования и Главное налоговое управление.

4.2.12. Национальное управление интеллектуальной собственности

В функции управления входит защита национальных интересов на глобальном ИКТ-рынке за счет регистрации прав собственности на научные открытия и разработки в сфере передовых технологий и связи. Управление планируется переподчинить из Государственной администрации по регулированию рынка напрямую Госсовету КНР, что говорит о возрастании его роли.

4.3. Национальная система реагирования на компьютерные инциденты

Ядром системы является **Центр управления чрезвычайными ситуациями в области Интернет-безопасности** Администрации киберпространства Китая, который координирует действия всех государственных ведомств, отраслевых центров и групп реагирования на компьютерные инциденты.

Национальный чрезвычайный план на случай инцидентов в области кибербезопасности впервые был разработан в 2014 году [28]. В зависимости от уровня угрозы все инциденты делятся на 6 категорий. Для «критических» инцидентов, таких как остановка большинства ключевых Интернет-сервисов и информационных систем, утечка государственных секретов или фальсификация информации, грозящих нанесением ущерба национальной безопасности и социальной стабильности, план предусматривает создание межведомственного штаба для мониторинга ситуации, координации межведомственных действий по снижению ущерба и ликвидации последствий в случае.

За осуществление практического реагирования на инциденты в национальном сегменте сети Интернет отвечает Координационный центр негосударственного некоммерческого **Национального центра по противодействию киберугрозам** (CNCERT/CC[51]). Он создан в 2001 году с целью разработки концепции сетевой и информационной безопасности министерств и ведомств, предприятий и организаций, а также отдельных потребителей и граждан КНР. Это очень авторитетный технический центр, который является членом международного Форума групп реагирования на компьютерные инциденты (FIRST), одним из основателей региональной группы реагирования АТЭС (APCERT) и сети контактных пунктов национальных групп реагирования, созданных в рамках реализации мер доверия ГПЭ по МИБ и АТЭС. CNCERT/CC заключил меморандумы о сотрудничестве в сфере кибербезопасности с 33 национальными группами реагирования других стран.

CNCERT приписывают разработку системы «Золотой щит». Центр осуществляет мониторинг и анализ угроз, выявление и реагирование на компьютерные

51 National Computer Network Emergency Response Technical Team/Coordination Center of China.

атаки, распространяет информационные бюллетени и предупреждения, осуществляет широкую просветительскую работу. Его деятельность курирует Министерство промышленности и информационных технологий, которое в 2017 году разработало детальный **План действий в чрезвычайных ситуациях для обеспечения безопасности сети Интернет общего пользования** [29].

4.4. Форматы государственно-частного партнерства в сфере обеспечения информационной безопасности КНР

Взаимодействие государства и бизнеса в Китае играет ключевую роль в реализации государственной политики в сфере цифровизации, развития инноваций и обеспечения информационной безопасности. В каждом сегменте ИКТ-отрасли действует свой альянс государственно-частного партнёрства, лидером которого является ведущая в этой сфере коммерческая компания-производитель. Главная их функция — саморегулирование на уровне отраслевых стандартов и правил поведения. Например, созданное в 2001 году **Китайское общество пользователей Интернета**, разработало большой набор правил действий пользователей сети[52].

Для содействия повышению уровня защищенности национальной информационной инфраструктуры и продвижению высококачественной национальной продукции для обеспечения информационной безопасности 200 китайских компаний в 2015 году объединились в **Альянс индустрии кибербезопасности** (CCIA)[53]. Он сотрудничает с государственными органами в разработке и реализации профильных законов и нормативных актов, способствует быстрому росту национального рынка информационной безопасности, участвует в международном сотрудничестве с различными странами и международными организациями. В декабре 2022 года CCIA выпустил Руководство по социальной ответственности в обеспечении безопасности данных и защите персональной информации, которое конкретизирует и дополняет для отрасли положения соответствующих законов, а также повышает рыночную привлекательность их продуктов и услуг. Одновременно альянс защищает геополитические интересы страны. Так в апреле 2023 года CCIA опубликовал анализ использования вредоносного программного

52 Конвенция об отраслевой самодисциплине в сфере интернета в Китае; Правила самодисциплины о запрете на распространение в интернете развратной, порнографической и другой недолжной информации; Конвенция о бойкотировании вредоносных программ; Конвенция о самодисциплине в области обслуживания блогосферы; Конвенция о самодисциплине в области борьбы с сетевыми вирусами; Манифест об отраслевой самодисциплине в области издательского права в интернете.

53 Принятие законов в сфере кибербезопасности и защиты персональных данных в Китае, а также последствия трансформации экономики под условия COVID-19 способствовали быстрому росту рынка информационной безопасности. По имеющимся оценкам в 2023 году этот сегмент ИКТ рынка достигнет отметки в 15,6 млрд долл. США (около 9% глобального рынка), а к 2027 году почти удвоится до 26,65 млрд долл. США. Источник: Growing opportunities in China's Cybersecurity Industry? January 26, 2023 https://daxueconsulting.com/chinas-cybersecurity-industry/.

обеспечения и компьютерных атак на информационные ресурсы и сети Китая, осуществленных разведывательными агентствами США [30]. Отчет увязывает эти акции с наиболее значимыми угрозами для мирового сообщества - атаками на ключевые инфраструктуры, воздействием на цепочки поставок, разработку «кибероружия».

Национальный центр по противодействию киберугрозам (CNCERT/CC) инициировал создание Китайского альянса по борьбе с сетевыми вирусами (ANVA), Китайского альянса по управлению киберугрозами (CCTGA) и «Партнерства международного сотрудничества CNCERT/CC» с 274 командами в 81 стране и территориях, а также меморандумы о сотрудничестве в сфере кибербезопасности с 33 из них.

5. Участие в международном сотрудничестве с ООН и другими международными и региональными организациями в области формирования системы международной информационной безопасности

В настоящее время позиция страны по всем ключевым вопросам МИБ является четко выверенной и нацеленной на достижение цифрового будущего страны. Китай последовательно отстаивает тезис о сохранении мирного, безопасного и открытого киберпространства, деятельность государств в котором должна осуществляться во благо развития и процветания на основе международного права и согласованных правил поведения. С каждым годом влияние Пекина в этой сфере растет благодаря развитию и укреплению государственной политики в области цифровизации и инноваций.

Проблематика формирования системы МИБ является одним из приоритетов внешней политики Китая, поэтому координация национальной деятельности по этому направлению осуществляется на самом высоком уровне — ее курирует заместитель премьер-министра Госсовета КНР, общее управление осуществляет Руководящая группа по вопросам координации в сфере МИБ, основным участником международных переговоров является Департамент контроля над вооружениями и разоружением МИД КНР.

С момента первого созыва в 2004 году Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (ГПЭ по МИБ) представитель Китая, как постоянного члена Совета безопасности ООН, принимал участие в ее работе. Пекин ежегодно выступал соавтором российских резолюций о включении в повестку дня Генеральной ассамблеи ООН вопроса о достижениях информатизации в контексте МИБ, активно способствовал выработке правил ответственного поведения

государств в ИКТ-среде, основанных на принципах равного суверенитета всех стран, мирного разрешения споров, неприменения силы и невмешательства во внутренние дела других государств.

Сейчас Китай развивает эту повестку в рамках Рабочей группы ООН открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025 (РГОС)[54]. Так в 2021 году МИД КНР сделал субстантивный вклад в РГОС, представив **Позицию Китая в отношении международных правил в киберпространстве** [31], в которой сформулирован призыв разработать в ООН общепризнанные нормы, правила и принципы регулирования киберпространства, чтобы совместно противостоять рискам и вызовам, отстаивать мир, безопасность и процветание. Правила в киберпространстве могут быть выработаны посредством создания всеобъемлющего и устойчивого процесса обсуждения с широким участием всех государств. Китай лишь дает свое видение общих принципов и считает, что следует обсудить как применяется международное право к использованию ИКТ государствами, принимая во внимание уникальные свойства ИКТ-среды, и далее развивать общее понимание по этому вопросу.

В 2011 году КНР совместно с Россией, Таджикистаном и Узбекистаном официально внесли на рассмотрение Генеральной ассамблеи ООН выработанные ШОС «Правила поведения государств в области обеспечения МИБ»[55].

Китай не только поддержал создание в Третьем комитете ООН Специального межправительственного комитета экспертов открытого состава для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях[56], но и призвал мировое сообщество к скорейшей разработке обязательной и универсальной конвенции в этой сфере.

При этом до недавнего времени Пекин воздерживался от самостоятельных шагов на международной арене, стараясь не входить в прямую конфронтацию с гегемонистской киберстратегией США. Даже инициатива по созданию глобальной транспортной и информационной инфраструктуры «Один пояс, один путь»[57], которая де-факто направлена на распространение на Азию и Африку тех-

54 РГОС на 2021–2025 годы созвана на основании A/RES/75/240 от 31 декабря 2020 года.

55 Правила поведения в области обеспечения международной информационной безопасности: письмо постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана при ООН от 12.09.2011 года на имя Генерального секретаря A/66/359, http://rus.rusemb.org.uk/data/doc/internationalcoderus.pdf Обновленная редакция текста правил была распространена в качестве официального документа 69-й сессии Генассамблеи ООН 9.01.2015 года от имени всех государств-членов ШОС.

56 Резолюция A/RES/74/247 от 27 декабря 2019 года «Противодействие использованию информационно-коммуникационных технологий в преступных целях».

57 Инициатива разработана в 2010 г. и предложена председателем КНР Си Цзиньпином во время визитов в Казахстан и Индонезию осенью 2013 года, объединяет два проекта: Экономический пояс Шелкового пути и Морской Шелковый путь XXI века, оба дополняются развитием современной ИКТ инфраструктуры

нологического влияния Китая, продвигалась как исключительно экономический проект. Лишь после резкого ужесточения тактики действий США в отношении Поднебесной из-за осознания Вашингтоном угрозы национальной безопасности в связи превосходством КНР в технологиях искусственного интеллекта, внешнеполитические шаги Пекина стали наступательными.

В 2017 году МИД КНР обнародовал первую **Стратегию международного сотрудничества в киберпространстве**, где представлены взгляды Пекина на национальные и международные проблемы в этой сфере, излагаются основные принципы, стратегические цели и ключевые действия Китая по работе с другими странами. В сфере формирования системы МИБ к ним относятся:

- защита национальных интересов, цифрового суверенитета и безопасности;
- формирование системы международных правил в киберпространстве;
- содействие справедливости в управлении Интернетом;
- защита законных прав и интересов граждан;
- содействие глобальному сотрудничеству в цифровой экономике;
- создание платформы для обмена культурой в сети.

В стратегии также изложен план действий для достижения этих целей. Прежде всего, это поддержание мира и стабильности в киберпространстве, урегулирование спорных вопросов в глобальном Интернет-пространстве исключительно мирным путем, обеспечение порядка, основанного на правилах; реформирование глобальной системы управления Интернетом в многостороннюю, демократичную и прозрачную платформу для взаимовыгодного сотрудничества всех государств. Не менее важно развивать международное сотрудничество в сфере борьбы с кибертерроризмом и компьютерными преступлениям, защищать права и интересы граждан, включая их конфиденциальность. Другими целями являются укрепление цифровой экономики и получение от нее выгод; развитие и защита глобальной информационной инфраструктуры; расширение культурного обмена в киберпространстве.

Для достижения поставленных целей еще в 2014 году Китай создал собственную площадку для обсуждения вопросов формирования системы МИБ Всемирную конференцию по управлению Интернетом (проводится в г. Учжень, провинция Чжэцзян, иногда именуется как Чжэцзянский форум)[58]. С 2020 года на нем продвигается китайская инициатива **«Совместного созда-**

и цифровизацией логистики транспортировки грузов.

58 Для повышения эффективности форум институализирован в организацию «Всемирная конференция по управлению Интернетом» с центральным офисом в Пекине и филиалом в г. Тунсян (провинция Чжэцзян). Ее основателями стали институты, предприятия и индивидуальные члены из 20 государств.
Источник: https://www.wuzhenwic.org/2020-10/15/c_547699.htm.

ния сообщества единой судьбы в киберпространстве»[59], которая в ноябре 2022 года обрела статус национальной стратегии[60]. Основными принципами создания такого сообщества являются: уважение киберсуверенитета всех государств, поддержание мира и безопасности, продвижение открытости и сотрудничества, поддержание должного порядка, создание справедливой системы управления Интернетом, обеспечение стабильности и безопасности ее ключевых ресурсов.

Также был дан старт международному трансферу нормативных практик Китая в отношении регулирования информационной безопасности, что свидетельствует о том, что он стремится перенести свои разработки в этой сфере на внешние рынки и создать с партнерами совместный контур безопасности [32]. В сентябре 2020 года была предложена **Глобальная инициатива по обеспечению безопасности данных**, направленная на уважение суверенитета всех государств, содействие развитию цифровой экономики, противодействие монополии глобальных ИКТ-компаний, в том числе посредством поддержания целостности каналов поставок цифровых продуктов и услуг, борьбы с хищением данных, неправомерным трансграничным доступом к информации, использованием «закладок» в продукции. Китай также призвал государства противостоять массовой слежке в киберпространстве и выводу на свою территорию данных, собранных ИКТ-компаниями в результате реализации бизнеса в других странах.

В ответ США незамедлительно запустили инициативу «Чистая сеть», направленную на дискредитацию безопасности китайских ИКТ-технологий, однако Пекин продолжил продвижение своих идей среди партнеров по инициативе «Один пояс, один путь». Так в марте 2021 года Китай возглавил сотрудничество Лиги арабских государств по безопасности данных, а в 2022 году оформил аналогичную инициативу с пятью государствами Центральной Азии (Казахстан, Киргизия, Таджикистан, Туркмения и Узбекистан). Кроме того, китайская сторона планирует предложить свой подход как основу глобальных договоренностей в виде проекта резолюции Первого комитета ГА ООН «Продвижение глобальной безопасности данных» [33].

---

59 Инициатива является адаптацией для киберпространства центральной концепции председателя КНР Си Цзиньпина о «сообществе единой судьбы человечества». Она призывает правительства, международные организации, интернет-компании, технические сообщества, общественные организации и всех заинтересованных лиц к выработке подходов к глобальному управлению на основе «достижения общего развития, гарантии общей безопасности, осуществления совместного управления и получения всеми пользы», развитию киберпространства как глобального сообщества, где развитие и безопасность достигаются всеми, дают совместные преимущества и общую ответственность. Включает 20 предложений в 4-х категориях: одобрение политик, защита кибербезопасности, единая политика управления, человеко-ориентированный подход в ИКТ-секторе.

60 Белая книга «Совместное создание сообщества единой судьбы в киберпространстве», Источник: Jointly Build a Community with a Shared Future in Cyberspace, https://www.chinadaily.com.cn/a/202211/07/WS63687246a3105ca1f2274748.html.

6. Основные приоритеты национальной политики КНР в рамках БРИКС

В феврале 2023 года правительство Китая заявило: «Мы будем расширять пространство для международного сотрудничества в цифровой сфере, активно участвовать в платформах цифрового сотрудничества в рамках многосторонних структур, таких как ООН, ВТО, G20, АТЭС, БРИКС и ШОС, и строить новую платформу для открытого сотрудничества в цифровой сфере с высоким качеством» [34].

Достижение к 2035 году лидерства в передовых технологиях не даст Китаю желаемого эффекта, если управление глобальной сетью Интернет останется в руках США. Изменение этого зависимого положения — ключевая задача внешней политики Пекина. В подтверждение этого тезиса Государственное бюро информации Госсовета КНР в марте 2023 года опубликовало концепцию **Китайского управления киберпространством в новую эпоху** [35]. Документ демонстрирует реализованные Пекином правовые подходы к обеспечению инновационного развития, предпринятые им действия для создания открытых международных механизмов обсуждения опыта и практик других государств в целях выработки взаимоприемлемых решений для защиты справедливости и законности в киберпространстве.

В этом контексте активная поддержка Китаем взаимодействия в рамках БРИКС по вопросу глобального управления является важным, но промежуточным звеном для достижения главной цели. Кроме того, полного единства в БРИКС по управлению Интернетом вряд ли удастся достичь: Индия и Бразилия не поддерживают главенствующую позицию государств в этом процессе.

Укреплению международных позиций Китая, как кандидата на глобальное лидерство, служит научно-техническое сотрудничество БРИКС. Китай обладает огромным ресурсом для трансфера своих передовых технологий, что подтверждают его инициативы — Партнерство БРИКС по вопросам новой промышленной революции (PartNIR) и Инновационный центр PartNIR в провинции Фуцзянь, Сетевой университет БРИКС и его Институт БРИКС по изучению сетей будущего «BRICS Future» в г. Шэньчжень, организация Форума БРИКС по новой промышленной революции и другие проекты. Их реализация создает условия формирования в странах-участницах общих методологических подходов к цифровизации экономики и признания технологических стандартов Китая де-факто международными. Однако и здесь есть «подводные камни», например, острая конкуренция с Индией, которая к 2030 году может стать третьей экономикой мира с собственными амбициями на лидерство.

Результаты анализа деклараций саммитов БРИКС показывают, что задача пресечения противоправной деятельности в киберпространстве, включая использование сети Интернет в террористических целях, является предметом взаимовыгодного интереса. Китай проявляет к этой теме повышенное внимание, поскольку его позиции в глобальных рейтингах кибербезопасности ниже, чем у Бразилии, Индии и России. Это подтверждает и Фучжоуская инициатива, выработанная в рамках подготовки IX саммита БРИКС в г. Сямэнь, которая рекомендует «…в борьбе с терроризмом расширять обмен разведданными и опытом, а также наращивать потенциал. Страны БРИКС также должны расширять сотрудничество в области кибербезопасности и содействовать развитию интернет-технологий и управлению киберпространством во всем мире» [36]. На данный момент сотрудничество в практической плоскости по вопросам противодействия киберпреступности развивается КНР только с Российской Федерацией (в рамках ШОС и двустороннего соглашения по международной информационной безопасности). Несмотря на то, что Бразилия является участником Будапештской конвенции о киберпреступности, здесь есть потенциал укрепления БРИКС, особенно в части обмена информацией об угрозах и вредоносной деятельности, и Китай может сыграть в этом важную роль.

7. Список литературы

1. Китай представил план развития цифровых технологий до 2035 года, PRC.TODAY 27.02.2023, https://prc.today/kitaj-predstavil-plan-razvitiya-czifrovyh-tehnologij-do-2035-goda/.
2. Digital economy to receive top priority, China Daily, April 4, 2023, https://english.www.gov.cn/news/202304/04/content_WS642b78a4c6d03ffcca6ec072.html.
3. Российская газета — Спецвыпуск: Дыхание Китая №158(8509) https://rg.ru/2021/07/15/pozicii-rossii-i-kitaia-po-voprosam-kiberbezopasnosti-vo-mnogom-sovpali.html.
4. Cyber Capabilities and National Power: A Net Assessment, International Institute for Strategic Studies, 2021, p.96 https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---china.pdf.
5. В 2022 году доля цифровой экономики в ВВП Китая выросла до 41,5%, ИА «Финмаркет» 2 мая 2023 года, http://www.finmarket.ru/news/5944720.
6. Global Cybersecurity Index, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.
7. Брутян М.М. Перспективы развития национальной инновационной системы Китая в условиях усложнения международных политико-экономических отношений, Вестник Евразийской науки, 2019 №3, https://esj.today/PDF/14ECVN319.pdf.
8. Решение о поддержании безопасности в Интернете, https://ru.chinajusticeobserver.com/law/toolkits/checklist-cyber-security-rules-in-china.
9. Решение о поддержании безопасности в Интернете, https://ru.chinajusticeobserver.com/law/toolkits/checklist-cyber-security-rules-in-china.
10. Made in China 2025, State Council, July 7, 2015, http://www.cittadellascienza.it/cina/wp-content/uploads/2017/02/IoT-ONE-Made-in-China-2025.pdf.
11. Н.Ромашкина, В.Задремайлова Эволюция политики КНР в области информационной безопасности, «Пути к миру и безопасности» №1 (58) 2020, С.122-138, https://www.imemo.ru/files/File/magazines/puty_miru/2020/01/07_Romashkina.pdf.

12. Уведомление Государственного совета о выпуске Национального стратегического плана развития промышленности «Двенадцатый пятилетний план», http://www.gov.cn/zwgk/2012-07/20/content_2187770.htm.
13. Stu Woo In the Race to Dominate 5G, China Sprints Ahead, The Wall Street Journal, September 2019, https://www.wsj.com/articles/in-the-race-to-dominate-5g-china-has-an-edge-11567828888.
14. Компартия КНР очертила новую модель развития страны до 2050 года, Российская газета, 17.10.2022, https://rg.ru/2022/10/17/kitaj-ochertil-novuiu-model-razvitiia-do-2050-goda.html.
15. Н.Ромашкина, В.Задремайлова Эволюция политики КНР в области информационной безопасности, «Пути к миру и безопасности» №1 (58) 2020, С.122-138, https://www.imemo.ru/files/File/magazines/puty_miru/2020/01/07_Romashkina.pdf.
16. Неофициальный перевод стратегии https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/.
17. China's Law-Based Cyberspace Governance in the New Era, The State Council Information Office of the People's Republic of China, 16 March 2023, https://english.www.gov.cn/archive/whitepaper/202303/16/content_WS6489542ec6d0868f4e8dcd56.html.
18. Order of the President of the People's Republic of China №84 June 10, 2021, http://www.npc.gov.cn/englishnpc/c23934/202112/1abd8829788946ecab270e469b13c39c.shtml.
19. R.Creemers and G.Webster Translation: Internet Information Service Deep Synthesis Management Provisions (Draft for Comment), February 4, 2022, https://digichina.stanford.edu/work/translation-internet-information-service-deep-synthesis-management-provisions-draft-for-comment-jan-2022/.
20. Временные меры по управлению службами генеративного искусственного интеллекта, 13 июля 2023 г., http://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm.
21. The 17th Waseda-IAC World Digital Government Ranking 2022, International Academy of CIO（IAC), https://iacio.org/wp-content/uploads/2022/11/20221122-FINAL-17th-Waseda-IAC-World-Digital-Government-Ranking-2022.pdf.
22. Развитие законодательства КНР в области цифровой экономики, https://ири.рф/upload/iblock/913/1q5f9meofx2hiphmcapx43n94d81acne/Развитие%20законодательства%20КНР%20в%20области%20цифровой%20экономики.pdf.
23. 中央网络安全和信息化委员会办公室 , англ. Cyberspace Administration of China (CAC), http://www.cac.gov.cn/
24. А.В. Шитов Государственная безопасность Китая и спецслужбы КНР. Центр военно-политических исследований, 14.07.2020, http://eurasian-defence.ru/?q=node/47183.
25. China Information Technology Security Evaluation Center, 14.03.2023, http://www.itsec.gov.cn/fz/en/.
26. А.Кокошин, В.Кашин РСМД: О подходах руководства КНР и китайских силовых структур к противоборству в киберпространстве, 25.07.2022, https://russiancouncil.ru/analytics-and-comments/comments/o-podkhodakh-rukovodstva-knr-i-kitayskikh-silovykh-struktur-k-protivoborstvu-v-kiberprostranstve/.
27. А.В.Шитов Государственная безопасность Китая и спецслужбы КНР. Центр военно-политических исследований, 2020, http://eurasian-defence.ru/?q=node/47183.
28. Уведомление Центрального информационного управления Интернета о выпуске «Национального плана действий в чрезвычайных ситуациях на случай инцидентов в области кибербезопасности», 27 июня 2017 г., http://www.cac.gov.cn/2017-06/27/c_1121220113.htm.
29. Emergency Response Plan for Unexpected Cybersecurity Incidents of the Public Internet, https://cyberpolicyportal.org/states/china.
30. Review of Cyberattacks from US Intelligence Agencies – Based on Global Cybersecurity Communities' Analyses, http://image.cns.com.cn/ecns_editor/73172ec7/20230411/review1.pdf.
31. Позиция Китая в отношении международных правил в киберпространстве (Рабочая группа открытого состава Организации Объединенных Наций по информационной безопасности), октябрь 2023, https://www.fmprc.gov.cn/wjb_673085/zzjg_673183/jks_674633/zclc_674645/qt_674659/202110/t20211012_9552671.shtml
32. А.Маслов Позиции России и Китая в области обеспечения цифровой безопасности и национальных целей развития во многом совпали, 15.07.2021, https://rg.ru/2021/07/15/pozicii-rossii-i-kitaia-po-voprosam-kiberbezopasnosti-vo-mnogom-sovpali.html.
33. О.Мельникова Опыт Китая в защите национального киберсуверенитета, журнал Международная жизнь №12 2022 год, https://interaffairs.ru/news/show/38218.
34. Китай представил план развития цифровых технологий до 2035 года, Портал PRC.TODAY, 27.02.2023 https://prc.today/kitaj-predstavil-plan-razvitiya-czifrovyh-tehnologij-do-2035-goda/.

35. China’s Law-Based Cyberspace Governance in the New Era, The State Council Information Office of the People’s Repblic of China, March 2023, https://english.www.gov.cn/archive/whitepaper/202303/16/content_WS6489542ec6d0868f4e8dcd56.html.
36. BRICS Must Write the Rules of a New Wave of Globalisation: Fuzhou Initiative, June 20, 2017, http://infobrics.org/post/25063.
37. Брутян М.М. Перспективы развития национальной инновационной системы Китая в условиях усложнения международных политико-экономических отношений, Вестник Евразийской науки, 2019 №3, https://esj.today/PDF/14ECVN319.pdf.

Королевство Саудовская Аравия

Официальное название: Королевство Саудовская Аравия
Столица: Эр-Рияд
Официальный язык: арабский

Территория: 2 149 690 км² (12 место в мире). Королевство расположено в Юго-Западной Азии, занимает около 80% территории Аравийского полуострова и ряда прибрежных островов в Красном море и Персидском заливе Индийского океана. На севере граничит с Иорданией, Ираком, Кувейтом, на юге и юго-востоке — с Йеменской Арабской Республикой, Народной Демократической Республикой Йемен, Оманом, Объединёнными Арабскими Эмиратами, на востоке — с Катаром.

Население: 36 947 025 чел. (по данным ООН на 1 июля 2023 года[1]), что является 40 показателем в мире. Моложе 30 лет более 60% граждан (ими могут стать только мусульмане). Колония иммигрантов на территории государства составляет порядка 30% населения (в основном экспаты).

Государственное устройство Саудовской Аравии определяется принятым основным законом Королевства, носящим название «Основной низам правления Саудовской Аравии» (1992). Согласно ему, Саудовская Аравия является абсолютной теократической монархией, управляемой сыновьями и внуками первого короля Абдул-Азиза. Закон основан на исламском праве. Король — глава государства и религиозный лидер страны (имам) — хранитель двух Священных мечетей и одновременно премьер-министр, главнокомандующий вооруженными силами и верховный судья. Он обладает всей полнотой исполнительной, законодательной и судебной власти, полномочия короля теоретически ограничены только нормами шариата и саудовскими традициями.

Исполнительная власть в виде Совета министров состоит из наследного принца (первый заместитель премьер-министра), трех королевских советников (государственные «министры без портфеля»), 5 государственных министров и руководителей 20 министерств. Ранг министров также имеют главы Национальной гвардии Саудовской Аравии, Центрального банка и Государственной корпорации Petromin, губернаторы Медины, Мекки и Эр-Рияда. Все министерские портфели распределены между родственниками короля и назначаются Королевским указом. Для конкретных вопросов по решению короля создаются профильные Комитеты.

1 Saudi Arabia Population 2023 (Live), https://worldpopulationreview.com/countries/saudi-arabia-population

Законодательная власть представлена в виде некоторого подобия парламента — Консультативной ассамблеи (Меджлис аш-Шура), действующей с декабря 1993 года. Все 150 членов Консультативной ассамблеи, состоящей из ученых, писателей, бизнесменов, видных членов королевской семьи, назначаются королем на четырехлетний срок. Совет призван разрабатывать рекомендации правительству по вопросам социально-экономического развития, готовить заключения по различным правовым актам и международным соглашениям. Не менее 10 членов Совета имеют право законодательной инициативы.

Судебная власть включает местные и высшие шариатские суды, апелляционные суды и Судебную контрольную комиссию в Мекке (высшая кассационная инстанция). Судопроизводство осуществляется в соответствии с нормами Корана и шариата. Король выступает в роли высшей судебной инстанции с правом амнистии.

Экономика: По данным Всемирного банка за 2022 год показатели Валового внутреннего продукта (ВВП) (по паритету покупательной способности) составляют:

Итого: 2 151 млрд долл. (17 место в мире).

На душу населения 59 065 долл. (20 место в мире);

Показатели ВВП (Номинал):

Итого: 1 108 млрд долл. (17 место в мире).

На душу населения: 30 463 долл. США (33 место в мире).

Дипломатические отношения с Россией (СССР) установлены 19 февраля 1926 года.

1. Обзор уровня развития информационно-коммуникационной инфраструктуры, информатизации и обеспечения информационной безопасности

Королевство Саудовская Аравия (КСА) является быстро развивающимся государством. Из всех арабских стран у КСА самый высокий уровень ВВП, в основном определяемый отраслями добычи и переработки углеводородов[2], поскольку на территории страны находится 90% всех мировых разведанных запасов нефти. В 1990-х гг. были поставлены задачи постепенной диверсификации экономики и повышения роли частного предпринимательства. Среди новых приоритетных отраслей экономики выделяются информационные и коммуникационные технологии (ИТ, ИКТ), которые именно в этот период времени получили импульс развития за счет глобального распространения Интернет.

В 1993 году одним из первых на Ближнем Востоке к Интернету по спутниковой связи подключился саудовский Университет нефти и минералов имени короля Фахда. Развитие технологий и технической инфраструктуры позволило постепенно распространить использование сети на академические институты, медицинские и правительственные учреждения[3]. Постепенно Интернет стал доступен для коммерческого и частного использования. Уже в 1999 году в Саудовской Аравии количество пользователей глобальной сети составило 100 тыс. С тех пор оно стремительно растет: в 2017 году — 21 млн, по данным на январь 2023 года — 36,3 млн [1], что составляет 99% жителей страны.

В 2022 году ИКТ-рынок КСА в регионе MENA[4] был самым большим по объему капитала (41,1 млрд долл. США) и расходам (80% составил импорт технологий). Старт переформатированию отрасли в 2016 году дал план стратегического развития «Видение Королевства Саудовская Аравия 2030» («Видение 2030») [2], в котором ИКТ и цифровая инфраструктура являются ключевыми элементами диверсификации экономики и перехода к технологиям четвертой промышленной революции. Выгодное географическое положение дает КСА хороший шанс стать крупным технологическим центром рынков Европы, Азии и Африки [3].

Цифровые амбиции Саудовской Аравии привлекли крупных технологических игроков и зарубежных инвесторов, что укрепляет ее экосистему ИКТ. Благодаря этому национальный ИКТ-рынок приобрел огромный потенциал и самый высокий темп роста среди стран G20[5], способствуя инновационному развитию

2 В 2022 году доходы от углеводородов составили 42% ВВП.

3 Государственная научная организация «Город науки и технологий имени короля Абдул-Азиза (KACST) осуществляет администрирование всех подключений и управляет местными магистральными каналами сети Интернет.

4 Регион включает государства Ближнего Востока и Северной Африки с населением в 355 млн человек.

5 По данным Международной корпорации обработки данных (IDC), в период с 2019 по 2021 год ИКТ-сектор

других секторов экономики, включая образование, здравоохранение и государственные услуги. Наиболее важные сегменты рынка: ИКТ-инфраструктура, в т.ч. сети подвижной связи 5G и центры обработки данных, кибербезопасность, а также передовые технологии — «умные» города, искусственный интеллект и Интернет вещей. Ожидается, что в до 2030 года рынок ИКТ и передовых технологий в КСА возрастет на 50% и в совокупности даст увеличение ВВП на 13,3 млрд долл. США [4].

Государство уделяет первостепенное внимание развитию высокоскоростных сетей связи. Рынок фиксированного широкополосного доступа к Интернет в последние годы заметно вырос, чему способствовали увеличение популярности социальных сетей и всплеск загрузок видео, онлайн-трансляций и игр, вызванный пандемией[6]. В конце 2021 года оптоволоконными каналами связи были обеспечены более 3,5 млн абонентов, из которых около 50% относятся к корпоративным клиентам[7]. Кроме того, в Красном море проложен подводный оптоволоконный кабель Saudi Vision Cable первый в мире с пропускной способностью 18 Тбит/с[8].

Сетями мобильной связи покрыта вся территория страны. Количество подписчиков их услуг в 2023 году составило 44,72 млн, что на 30% превышает количество жителей КСА (на одного пользователя приходится несколько sim-карт или смартфонов). В 2019 году Саудовская Аравия одной из первых в регионе MENA развернула коммерческую сеть подвижной связи 5G и в настоящее время остается одним из мировых лидеров по скорости передачи мобильных данных[9], особенно Мекке и Медине, где проходят многомиллионные хаджи[10]. Покрытие сетями 5G

аудовской Аравии вырос на 8%, достигнув стоимости в 32,1 млрд долл. США. По прогнозам ImarcGroup в 2024-2032 годах ежегодный темп роста ИКТ-рынка КСА составит 5,85%. Источники: Information and Communications Technology https://www.trade.gov/country-commercial-guides/saudi-arabia-information-and-communications-technology#:~:text=5G%3A%20Saudi%20Arabia%20was%20among,the%20first%20quarter%20of%202021, Saudi Arabia ICT Market Report by Type (Hardware, Software, IT Services, Telecommunication Services), Size of Enterprise (Small and Medium Enterprises, Large Enterprises), Industry Vertical (BFSI, IT and Telecom, Government, Retail and E-commerce, Manufacturing, Energy and Utilities, and Others), and Region 2024-2032, https://www.imarcgroup.com/saudi-arabia-ict-market

6 Наиболее посещаемые в КСА Интернет-ресурсы в 2023 году (в порядке убывания): зарубежные YouTube, Google, Twitter, Mangalek, Facebook, Wikipedia, Gmanga, Witanime, Instagram, Tiktok, Amazon.sa, а также местные платформы электронной торговли – haraj.com.sa и souq.com (последняя приобретена Amazon в 2017 году).

7 Следует отметить, что среднее число абонентов услуг фиксированной широкополосной связи по отношению к численности населения в странах Персидского залива невысоко и составляет около 20,88%.

8 Длина кабеля 1160 км, он обеспечивает бесперебойную связь между Джиддой, Янбу, Дубой и Хакле.

9 По данным 2021 года скорость передачи мобильных данных составляла 105,42 Мбит/с, что было пятым показателем в мире и вторым среди стран G20, превысив среднемировой показатель почти в 250 раз.

10 Обеспечение безопасности участников хаджа и Умры очень важно для престижа КСА. Поэтому в 2023 году в этих городах количество передающих вышек 5G увеличено на 41% (более чем на 2600), а также создано 11 тыс. точек доступа Wi-Fi, что гарантирует самую высокую в мире скорость загрузки данных с мобильных устройств (203 Мбит/с в Мекке и 223 Мбит/с в Медине). Министерство хаджа и Умры КСА предоставляет 121 цифровую услугу для 30 млн верующих в Саудовской Аравии и миллионов зарубежных паломников. Источник: With 41% increase in 5G towers, CITC announces full ICT readiness to serve pilgrims - Saudi Press, Dec 7, 2023, https://saudipress.com/with-41-increase-in-5g-towers-citc-announces-full-ict-readiness-to-serve-pilgrims

обеспечено во всех крупных городах и курортных зонах[11]. По итогам 2022 года было зарегистрировано более 11,2 млн 5G подписок, что превышает 25% всего сектора мобильной связи в стране [5]. Сети 5G — это стартовая площадка, необходимая для ускорения разработки и внедрения передовых технологий, таких как искусственный интеллект, Интернет вещей (IoT), облачные и периферийные вычисления. Саудовская Аравия ожидает, что к 2030 году инвестиции в 5G и Wi-Fi 6E увеличат вклад в ВВП страны до 18 млрд долл. США [6].

Важно отметить, что КСА не вводит требований закупки «демократичных» технологий, выбор оборудования остается за оператором связи. Так Saudi Telecom Company (STC) — крупнейший поставщик услуг 5G в Саудовской Аравии и регионе MENA и саудовская ИТ-компания Mobily[12] для ядра сетей 5G используют оборудование Huawei и Cisco, а аппаратуру Nokia и Ericsson для поддерживающих их радиосетей. Крупнейший провайдер мобильной связи Zain[13] в основном работает с Huawei, в том числе для локальных сетей (LAN), и частично с Cisco и Nokia.

Глобальные планы по строительству в КСА десяти «умных» городов[14] и дооснащению пяти существующих[15] повлекли активизацию рынка Интернета-вещей (датчиков, контроллеров, сенсоров, промышленных роботов, смарт-камер, беспилотных транспортных средств и других «умных» устройств). Согласно прогнозу International Data Corporation, этот сегмент ИКТ-рынка Саудовской Аравии будет ежегодно расти на 12,8% и к 2025 году достигнет объема в 2,9 млрд долл. США [7].

Обработка получаемых Больших данных потребует развития технологий искусственного интеллекта[16], местный рынок которых может возрасти до 35 млрд долл. США к 2030 году. Саудовская Аравия стремится стать мировым лидером в этих технологиях и привлечь к 2030 году 20 млрд долл. иностранных и местных инвестиций на осуществление исследований и разработок в этой сфере. В частности, в Эр-Рияде уже действует Национальный центр искусственного

---

11 В контексте развития «умных» городов Саудовская Аравия, последовав примеру США, создала условия для развития нелицензионных беспроводных технологий, выделив им весь диапазон радиочастот 6 ГГц. Благодаря этому беспроводная экосистема страны сможет поддерживать следующее поколение Wi-Fi 6 и технологии, основанные на стандартах 3GPP 5G NRU.

12 Mobily (Etihad Etisalat Company).

13 Zain (Mobile Telecommunication Company Saudi Arabia K.S.C.P.)

14 «Умные» города КСА: NEOM, Al Ula, Qiddiya, Red Sea Project, Jabal Omar, Amaala, Ad Diriyah, Al Widyan, King Salman Energy Park, Waad Alshamal.

15 В 2021 году Эр-Рияд занял 30 место по версии ООН в рейтинге самых устойчивых «умных» городов. Источник: 5G and other innovative technologies to encourage ICT growth in Saudi Arabia - Saudi Arabia 2020 // Oxford Business Group, https://oxfordbusinessgroup.com/reports/saudi-arabia/2020-report/economy/well-connected-5g-and-other-innovative-technologies-encourage-sector-growth

16 Наиболее перспективные направления анализа Больших данных в Саудовской Аравии: анализ данных геологоразведки и построение трехмерных моделей месторождений, оптимизация автоперевозок, анализ срока службы оборудования, прогнозирование сроков поставок и отслеживание активов, оптимизация логистических цепочек, анализ спутниковых/аэрофотоснимков, предупреждение отказов активов.

интеллекта (NCAI) и создается Международный центр исследований и этики в области искусственного интеллекта. По оценкам консалтинговой компании PricewaterhouseCoopers, в период с 2018 по 2030 год доля Саудовской Аравии в среднегодовом росте искусственного интеллекта в регионе MENA составит 31,3% [8].

Саудовская Аравия является перспективным центром предоставления облачных услуг[17] и обработки Больших данных не только для собственной экономики. Королевство занимает высокое место по конкурентоспособности облачных технологий в регионе MENA и является одним из немногих государств, где есть нормативная база их регулирования (см. Раздел 3.5). Также КСА является лидером по компонентам кибербезопасности облачных вычислений. Реализация программы перевода всех государственных органов на межведомственное взаимодействие в облачных сервисах (Cloud First Policy, 2019) способствовала выделению 18 млрд долл. США на развитие необходимой инфраструктуры и росту этого сегмента ИКТ-рынка на 16%. Существенный вклад в его объем вносят коммерческие предприятия сектора энергетики, финансов, связи и промышленность, однако самые высокие темпы роста до 2026 года ожидаются в сфере торговли, здравоохранения и образования.

В стране уже действуют 22 высокопроизводительных центра обработки данных (ЦОД), 13 из которых расположены в столице, а 7 — рядом с точками подключения к системам международных подводных кабелей (в городах Джедда, Даммам, Хубар) [9]. В 2021 году начата программа строительства новых центров, на что будет израсходовано 18 млрд долл. США.

Операторами самых производительных ЦОДов являются компании Oracle, Google, Alibaba и Huawei [10], также на рынке облачных вычислений КСА работают: Cisco Systems, SAP SE, IBM и саудовские NourNet, Wafai CLOUD, CloudSigma, Mobily и Sahara Net [11]. В феврале 2022 года Saudi Telecom Company анонсировала старт проекта стоимостью 26,66 млн долл. США по строительству нового ЦОД с подключением к точке обмена международным трафиком. Ежегодный рост этого сегмента ИКТ-рынка Саудовской Аравии в 2022–28 гг. прогнозируется на уровне 8%, что приведет к его капитализации в 2 млрд долл. США [12].

Несмотря на высокую покупательную способность жителей, электронная торговля в Саудовской Аравии стала развиваться позже других сегментов ИКТ-рынка. Причинами тому было недоверие покупателей к безопасности платежей, запрет на использование дебетовых карт для онлайн-транзакций, слабое развитие сервисов доставки и безналичной оплаты, привычка к наложенным

17 Имеется в виду предоставление сервисов: SaaS (программное обеспечение как услуга), PaaS (платформа как услуга), IaaS (инфраструктура как услуга).

платежам[18]. Правительством был принят ряд мер для расширения сегмента электронной торговли (введены необходимые правовые нормы) и стимулирования перехода к цифровым платежам, например, торговые точки и курьеры были оснащены платежными терминалами по субсидированным ценам, внедрены средства мобильных платежей, в том числе электронные кошельки (Apple Pay, Mada Pay[19], STC Pay и BayanPay). В 2019 году 36% совершенных торговых транзакций были безналичными платежами, а в 2021 году — уже 57%.

Согласно отчету Конференции ООН по торговле и развитию (UNCTAD) в 2019 году Королевство вошло в десятку развивающихся стран по индексу электронной коммерции между бизнесом и потребителями[20] и заняло 49 место в глобальном рейтинге. По состоянию на начало 2020 года объем рынка электронной розничной торговли в стране составлял около 5,4 млрд долл. США. В текущем году ожидается увеличение сегмента на 3,9%, прогнозируется ежегодный рост в 2023–27 гг. на 6,3% и выход на объем в 14,83 млрд долл. США [13].

Цифровизация государственных услуг является одной из главных целей «Видения 2030». Для ее достижения сделано очень много. В 2005 году принята первая многоцелевая программа «Yesser», которая осуществила подготовку перехода правительственных учреждений «в облако» путем разработки стандартов совместимости данных и метаданных, согласования технических стандартов [14]. На основе проделанной работы принята Стратегия «умного» правительства, создано специализированное государственное ведомство (DGA), доработана нормативная база. В рейтинге развития электронного правительства ООН (E-Government Development Index 2020) Королевство перешло из группы стран «с высоким уровнем» в группу «с очень высоким уровнем» развития, в регионе Саудовскую Аравию по этому индексу опередили только ОАЭ и Бахрейн.

В настоящее время 6 тыс. государственных услуг предоставляются онлайн (97% от общего числа). Идет поэтапное внедрение общегосударственного портала госуслуг для граждан и резидентов (my.gov.sa). Пока можно воспользоваться онлайн-платформой и приложением Absher для доступа к таким услугам, как доставка документов и продление паспорта. Под управлением Министерства финансов действует взаимосвязанная платформа Etimad, которая облегчает заключение контрактов, оплату, проведение торгов и закупок, оформление финансовых прав. В период пандемии COVID-19 использовались приложения Tawakkalna и Tabaud для контроля цифрового сертификата здоровья и сокращения возможного контакта с больными [15].

---

18 Даже в самой молодой демографической группе наличные по-прежнему являются предпочтительным выбором по сравнению с использованием платежных карт.

19 Саудовская платежная сеть Mada (ранее Span) – единственная и основная система платежей в Королевстве Саудовская Аравия, созданная Министерством финансов под надзором Центрального банка Саудовской Аравии.

20 «UNCTAD B2C E-commerce Index» измеряет готовность экономики поддерживать покупки онлайн.

На начальном этапе цифровизации правительства в качестве технической основы использовались продукты Oracle, в целях реализации приложений блокчейн для государственных и финансовых услуг заключено соглашение с IBM, но в последнее время в качестве подрядчика новых проектов упоминается китайская Huawei.

На фоне столь грандиозных цифровых преобразований экономики и государственного управления Саудовской Аравии бурно развивается рынок продуктов и услуг кибербезопасности, которые призваны не только защитить инвестиции в ИКТ, но и обеспечить поступательное инновационное развитие государства. По данным МСЭ рынок кибербезопасности Саудовской Аравии в 2020 году был самым большим на Ближнем Востоке и оценивался в 3,6 млрд долл. США. Прогнозируется, что его ежегодный рост до 2026 года составит 17,98% (среднемировой уровень 10,9%), что даст объем в 9,8 млрд долл. США [16]. Системная работа государства по укреплению национальной информационной безопасности дает результат. Согласно Глобальному индексу кибербезопасности 2020 года [17] за два года Саудовская Аравия стремительно поднялась с 13 места на вторую позицию, сравнявшись по индексу с Великобританией.

Масштаб деятельности в сфере кибербезопасности способствует развитию большого количества местных компаний и стартапов[21]. Однако собственного потенциала для решения всего спектра задач кибер- и информационной безопасности закупаемых за рубежом ИКТ у Саудовской Аравии нет. Значительную долю ее рынка кибербезопасности занимают зарубежные компании, в основном американские[22], из российских заметно присутствует только Kaspersky Lab.

Вся цифровая отрасль КСА испытывает дефицит кадров на уровне 20–25%, особенно остро он ощущается в сфере кибер- и информационной безопасности, разработке программного обеспечения, искусственного интеллекта, машинного обучения и анализа данных. При отсутствии местных специалистов усиливается потребность привлечения высококвалифицированных экспатов (для них введена «мгновенная» виза по запросу работодателя), что крайне важно для неболь-

21 Из наиболее крупных можно выделить Saudi Paramount Computer Systems, Al Arabiya Systems Engineering (ASE), MBUZZ, государственную военно-промышленную компанию SAMI, IT Security Training & Solutions, Al Moammar Information Systems, Sirar (дочка STC).

22 В 2017–18 гг. на рынке КСА работали американские компании информационной безопасности, входящие в ВПК США – Raytheon, Booz Allen Hamilton, Northrop Grumman и Lockheed Martin, IronNet Cybersecurity. В 2023 году среди ведущих игроков указаны американские компании – Palo Alto Networks, McAfee, IBM, Cisco Systems и NortonLifeLock. Также активно представлены: американские Check Point, FireEye и отпочковавшаяся от нее Trellix, Dell Technologies, Trend Micro, Tenable, Hewlett Packard, Fortinet, SAT Microsystems, NEC Saudi Arabia. Источники: Кибербезопасность в Саудовской Аравии: обзор основных государственных компаний // Online Defense, https://ru.difesaonline.it/evidenza/cyber/cyber-security-arabia-saudita-rassegna-delle-principali-aziende-governative?ysclid=lpx11y858s871414210, KSA Cybersecurity Market Size- By Security Type, By Solution Type, By Services, By End User, By Deployment Mode- Regional Outlook, Competitive Strategies and Segment Forecast to 2032, 2022, https://www.sperresearch.com/report-store/ksa-cybersecurity-market.aspx.

ших саудовских компаний [18]. Государственному сектору трудно конкурировать с бизнесом при найме специалистов.

Государство, в том числе через реализацию Программы развития человеческого потенциала, осуществляет широкий комплекс шагов по решению этой проблемы за счет изменения системы образования, подготовки необходимых кадров, привлечения зарубежных и местных талантов, а также репатриантов [19]. Обучение по программам STEM[23] осуществляют 104 научных центра. В партнерстве с зарубежными университетами и аналитическими центрами инициированы 22 новые учебные программы в области ИКТ в ведущих вузах страны, в частности в Саудовской электронной академии, Национальной академии информационных технологий и Саудовской федерации по кибербезопасности, программированию и дронам, их международные рейтинги стабильно растут[24]. Создано 14 лабораторий цифровых инноваций, в 2017–20 гг. там прошли обучение 26 тыс. человек и проведено 260 курсов повышения квалификации [20]. Программы подготовки и переподготовки кадров в сфере кибербезопасности для государственных учреждений реализует Университет науки и технологий имени короля Абдаллы [21].

Кроме того, осуществляется мощная программа наращивания национального потенциала в сфере внедрения передовых технологий. Правительство Саудовской Аравии взяло на себя обязательство ежегодно инвестировать 2,5% ВВП в сектор исследований, разработок и инноваций до 2040 года, но и бизнес-сообщество вносит вклад в финансирование НИОКР [22]. Аналитики IDC полагают, что в 2022–26 гг. сегмент разработки программного обеспечения в стране будет расти на 11,4%.

Значительная поддержка оказывается национальной экосистеме стартапов. В этих целях создана Саудовская венчурная компания (SVC) для финансирования и содействия начинающим, малым и средним предприятиям[25], благодаря измене-

---

23 Science, Technology, Engineering, Mathematics –естественные науки, технологии, инженерия и математика.

24 Например, Университет короля Сауда входит в Top 20 по исследованиям в области расширенной аналитики данных. Источник: ASPI's Critical Technology Tracker. The global race for future power, 2023, https://www.aspi.org.au/report/critical-technology-tracker. В 2021–22 годах в списке Центра мировых рейтингов университетов Государственная научная организация «Город науки и технологий имени короля Абдул-Азиза» заняла 278 место, а по объему исследований — 225, Университет науки и технологий имени короля Абдаллы (KAUST) в общем зачете занял 304 место, а Университет короля Сауда — 371. Одной из целей программы «Видение 2030» является вхождение 6 саудовских университетов в TOP200 лучших университетов мира. Источник: D. Little, Transforming the ICT sector in Saudi Arabia through foreign direct investment https://www.adlittle.com/cn-en/insights/report/transforming-ict-sector-saudi-arabia-through-foreign-direct-investment

25 Например, инициатива Garage по финансированию и поддержке стартапов в сфере передовых и прорывных технологий с инвестиционным фондом в 1,4 млрд долл. США, запущенная в 2022 году национальным центром KACST, Министерством связи и ИТ (MCIT) и Саудовской федерацией кибербезопасности, программирования и беспилотных летательных аппаратов (SAFCSP). Благодаря этому стартапы получают не только финансирование в 100-500 тыс. долл США, но и доступ к лабораториям KACST, цехам быстрого прототипирования, другому специализированному оборудованию, могут воспользоваться консультациями и наставничеством. Компания Aramco создала собственную высокоэффективную венчурную компанию Prosperity Ventures, поддерживающую разработки в ИКТ-сфере, которая была признана Лучшей венчурной фирмы Саудовской Аравии 2023. Она инвестировала некоторые из наиболее перспективных технологических компаний в сфере облачных технологий, таких как Wasabi, Stream Native, SignalWire, Zilliz, в интеллектуальную глобальную платформу для управления платежами и казначейством Sunrate,

нию нормативной базы упрощены инвестиции и обеспечена защита прав инвесторов и компаний[26]. Активно развивается система ускорения трансфера разработанных ИКТ в реальный сектор через инкубаторы, акселераторы, конкурсы[27]. Среди них можно отметить созданный в 2007 году технологический инкубатор BADIR, инкубатор-акселератор в Университете науки и технологий имени короля Абдаллы (KAUST), национальную сеть исследований и инноваций MAEEN, объединяющую уже 7 университетов, 20 государственных институтов, 7 исследовательских центров и 3 госпиталя.

Особое внимание инвесторов привлекают стартапы в сфере финтех, искусственного интеллекта, возобновляемых источников энергии и электронной торговли. Благодаря системным усилиям в 2020–21 гг. в Саудовской Аравии произошло увеличение количества заявок на патенты на 11%, регистрацию товарных знаков на 26%, промышленных моделей на 48% и авторских прав на 57%. Не удивительно, что в Глобальном инновационном индексе 2023 года, определяемом Всемирной организацией по интеллектуальной собственности, Саудовская Аравия поднялась на 48 место, обогнав Бразилию, Катар, Россию и Иран [23]. Однако в рейтинге она по-прежнему находится в группе стран с индексом, ниже ожидаемого для государств с высоким уровнем дохода. Также важно отметить, что только 15% стартапов в КСА работают в секторах «глубоких технологий» (среднемировой показатель 45%).

2. О стратегическом планировании в области цифровизации и обеспечении информационной безопасности

2.1. Национальная программа «Видение Королевства Саудовская Аравия 2030» (2016)

Программа «Видение 2030» [24] разработана по инициативе и под патронажем наследного принца Мухаммеда бен Салмана. Главная ее цель — дивер-

---

в Cequence Security — американский поиск решений для унифицированной защиты API, в блокчейн, финансовые и промышленные технологии, решения в области здравоохранения и образования.

26 Согласно отчету Magnitt о венчурном капитале Саудовской Аравии (VC) за 2021 год, Королевство привлекло 548 млн долл. США венчурных инвестиций — национальный рекорд и увеличение на 270% по сравнению с 2020 годом. В период с 2017-21 гг.объем инвестиций, вложенных в Королевство, вырос на 1174%. Прямые иностранные инвестиции (ПИИ) также продемонстрировали уверенный рост, увеличившись на 257% до 19,3 млрд долл. США в 2021 году. Из 4,4 тыс. выданных лицензий на долю ИКТ-компаний пришлось 133, что является шестым по величине показателем в секторе.

Источник: Saudi Arabia bolsters innovation through R&D — Saudi Arabia 2022 // Oxford Business Group https://oxfordbusinessgroup.com/reports/saudi-arabia/2022-report/ict/the-search-for-solutions-the-kingdom-is-working-to-bolster-its-economy-through-an-enhanced-research-development-and-innovation-ecosystem/

27 В качестве примеров можно привести Homathon Challenge Competition (2020) с 10 тыс. участников, NEOM AI Challenge (2020) среди 100 инновационных студенческих проектов, Thakaa Hackathon (2019) для программистов и аналитиков данных.

сификация экономики, повышение качества жизни и превращение государства в мирового лидера. Достижение цели будет осуществлено за счет реализации трех блоков задач: динамичного развития общества с использованием крепких основ нации, создания условий для полноценной жизни и формирования сильного фундамента; создания процветающей экономики путем расширения возможностей, привлечения долгосрочных инвестиций, повышения открытости для бизнеса и использования уникального положения страны; соответствия амбициям нации через эффективное управление и ответственное личное и коллективное участие.

Решить эти задачи планируется с помощью цифровой трансформации всех сфер жизнедеятельности. Руководство страны стремится сделать Саудовскую Аравию одной из ведущих стран мира в области ИКТ, создавая передовую инфраструктуру, развивая цифровую экономику, основанную на технологиях четвертой промышленной революции, совершенствуя цифровое управление. Среди основных показателей программы можно выделить следующие. К 2030 году доля «неуглеродных» отраслей в экономике возрастет с 16 до 65%, вклад малых и средних предприятий в ВВП увеличится с 20 до 35%, повысится конкурентоспособность экономики, и страна выйдет по этому показателю на 15 место в мире, а три саудовских города войдут в мировую сотню лучших. В Глобальном индексе эффективности управления страна поднимется с 80 на 20 место, а электронное правительство Саудовской Аравии войдет в пятерку лучших. На шесть лет увеличится продолжительность жизни, уровень безработицы снизится до 7%.

Столь амбициозные планы требуют не только колоссальных ресурсов (необходимый объем оценивается в 7 трлн долл. США), но и огромной работы на государственном уровне по координации выполнения взаимоувязанных планов. Для этого разрабатываются и реализуются около 20 программ, прежде всего по следующим направлениям — реструктуризация правительства, национальная трансформация, эффективное использование средств и управление проектами, пересмотр и доработка нормативной базы, контроль эффективности, реструктуризация открытых инвестиционных фондов, развитие человеческого потенциала и стратегического партнерства. В них детализированы механизмы и показатели достижения целей «Видение 2030» и оценки эффективности (KPI). Кроме того, повсеместно реализуются различные методы «обратной связи», с помощью которых оцениваются результативность государства по выполнению планов и удовлетворенность происходящими трансформациями потребителей (государственные органы, бизнес, граждане)[28].

28 Например, ежегодно проводятся массовый очный и дистанционный опрос и детальное анкетирование. В 2023 году в нем приняло участие 134 тыс. бенефициаров государственных цифровых услуг.

Для исключения дублирования функций и координации государственных органов в 2017 году созданы **Национальный комитет по цифровой трансформации** (NCDT)[29] и **Национальный комитет по регулированию** (см. Раздел 3).

2.2. **Программа национальной трансформации** (2016)

Программа национальной трансформации (англ. NTP)[25] стала первой ведомственной программой реализации «Видение 2030». Ее проект разработан Комитетом по связи и информационным технологиям в 2015 году при участии 24 государственных ведомств и после согласования принят в июне 2016 года [26]. Программа рассчитана до 2030 года и разбита на три этапа, отличающиеся ключевыми задачами экономического и социального роста, методами их решения и показателями.

На первом этапе (2017–20 гг.) с бюджетом около 75 млрд долл. США, из которых более 15 млрд предназначались на цифровизацию и информационные технологии [27], была осуществлена реорганизация государственных ведомств и начато формирование взаимодействия между всеми заинтересованными сторонами, сделаны шаги по улучшению государственного управления с помощью развития цифровых сервисов и обновления нормативно-правовой базы[30]. В ИКТ-отрасли проведена большая работа по регулированию радиочастотного спектра для расширения использования передовых технологий, дополнительно подключено к широкополосному Интернету 576 тыс. домохозяйств, увеличена скорость обмена данными в сети с 9 до 109 Мбайт/с. С помощью цифровых сервисов улучшились сектора здравоохранения и туризма, стало доступно 120 юридических услуг, снижена аварийность и загрузка автодорог и многое другое. Расширены возможности участия в Программе частного сектора, в том числе малых и средних предприятий (их количество возросло на 40%) [28]. Благодаря перечисленным и иным достижениям в 2020 году Саудовская Аравия заняла 8 место по индексу развития ИКТ-инфраструктуры среди стран G20.

На текущем этапе Программы национальной трансформации (2021–25 гг.) определены 34 стратегические цели, в том числе увеличение вклада цифровой экономики в национальный ВВП до 19,2%, повышение уровня зрелости электронного правительства и эффективности госслужащих[31]. Продолжится развитие

---

29 NCDT состоит из 11 членов кабинета министров, отвечающих за реализацию «Видение 2030», а также глав SDAIA, NCA, NDU и агентства по госзакупкам. Мандат комитета включает разработку политик и стратегий цифровой трансформации и разработку программ, необходимых для их скоординированной реализации.

30 Принято 5 законов, в том числе «Об электронной коммерции», осуществлено 555 нормативно-правовых реформ для облегчения привлечения инвестиций, улучшения бизнес-среды и расширения участия женщин.

31 Например, перевод в цифровую форму 85% юридических сервисов и достижение удовлетворенности ими в 85%, повышение прозрачности госсектора и улучшение на 15 позиций положение КСА в Глобальном рейтинге восприятия коррупции (42 место, CPI 2017). Источник: National Transformation Program Delivery Plan 2021–2025

цифровой инфраструктуры для государственного и частного сектора, индустриальных отраслей и энергетики. Расширится разработка нормативной и правовой базы для внедрения системы цифровой идентификации, защиты данных (цифровые подписи, кибербезопасность), использования открытых данных, обеспечения свободы доступа к информации. Будут расширены программы научных исследований и подготовки саудовских кадров.

2.3. Стратегия развития сектора ИКТ 2019–2023

Разработанная в 2019 году Министерством связи и ИТ отраслевая стратегия также ставит амбициозные цели. Среди них: привлечение в страну ведущих международных компаний из сферы передовых технологий, увеличение доли местного цифрового контента, улучшение технических навыков саудовских специалистов, повышение технологических и цифровых знаний, стимулирование инноваций путем поощрения исследований, разработок и экосистемы стартапов, поддержка реализации национальных мега-проектов, а также содействие координации и взаимодействию между соответствующими субъектами ИКТ в государственном и частном секторах.

Заявленные целевые показатели Стратегии: подготовка 25 тыс. специалистов для ИКТ-отрасли, увеличение на 50% объема рынка ИТ и передовых технологий, рост ИТ-сектора на 50%, расширение участия в нем женщин на 50%, увеличение за 5 лет вклада ИКТ-сектора в ВВП на 11 млрд долл. США, поддержка усилий по локализации технологий путём повышения местной рабочей силы до 50%, увеличение иностранных инвестиций. Для достижения этих целей разработана дорожная карта, включающая 24 стратегические инициативы[32].

2.4. Стратегия Комиссии по связи и информационным технологиям (2019)

В 2019 году Комиссия по связи и ИТ (англ. CITC, в 2022 году преобразована в Комиссию по связи, космосу и технологиям — CST, см. Раздел 4.6) разработала собственную стратегию **CITC Strategy 2023**, дополняющую рассмотренную выше отраслевую и отражающую изменение функционала этого государственного органа с ИКТ-регулирования к более широкому — цифровому регулированию. Стратегия включает четыре направления: защита пользователей, поощрение ин-

// Arab National Development Planning Portal, https://andp.unescwa.org/plans/1431

32 Например, в мае 2021 года запущен акселератор Riyadh Techstars для поддержки программ и инвестиций в местные цифровые стартапы и предпринимательство (в момент запуска оказана помощь 10 компаниям в размере 120 тыс. долл. США).

вестиций и конкуренции, активизация цифровизации и достижение совершенства в области регулирования. Воплотить это планируется путем применения политик кибербезопасности и использования передовых технологий, одобрения совместной и гибкой нормативной базы, которая повысит организационную эффективность и соответствие нормативным требованиям.

2.5. **Национальная стратегия в области данных и искусственного интеллекта** (2020)

Документ, развивающий «Видение 2030» на последующую перспективу, был анонсирован в октябре 2020 года под названием «Реализация нашего лучшего будущего. Описание стратегии»[29]. Он ставит еще более амбиционную цель — превращение Саудовской Аравии в один из мировых центров предоставления лучших данных и технологий искусственного интеллекта (ИИ).

Учитывая, что использование ИИ во многих отраслях изменит локальный и глобальный рынок труда, второй целью Стратегии является взращивание национальных кадров (предусмотрены три градации — эксперты высокого уровня, специалисты, квалифицированные сотрудники). К 2030 году планируется обучить 40% рабочей силы Саудовской Аравии базовым навыкам использования технологий ИИ и обработки Больших данных, подготовить в саудовских университетах порядка 15 тыс. специалистов и 5 тыс. экспертов.

В целях превращения государства в наиболее благоприятную территорию ведения ИИ-деятельности стоит задача разработки гибких и стабильных политик и регуляторных норм для привлечения в Саудовскую Аравию компаний, инвесторов, талантов. К 2030 году планируется достичь высокой зрелости регуляторной политики.

Для создания прочной экосистемы ИИ будет оказано максимальное содействие этическому развитию исследований и разработок, созданию открытых данных и доступу ученых и коммерческих компаний к государственным данным (в перспективе будет доступ ко всем государственным данным при обеспечении их безусловной безопасности, защиты и приватности). До 2025 года планируется перевести данные всех ведомств в унифицированный машиночитаемый стандарт и провести тестирование их использования заинтересованными организациями. К 2030 году КСА хочет войти в десятку лучших стран по индексу открытых данных.

Еще одной целью является создание благоприятного климата для местных и иностранных инвестиций, для чего будут созданы специальные фонды, финансовые механизмы и программы поддержки инвесторов. Ожидается получить на развитие ИИ Саудовской Аравии 8 млрд прямых иностранных инвестиций и 12 млрд местных вложений.

Будут увеличены и улучшены возможности для осуществления научных исследований и разработок в сфере ИИ и Больших данных, оказана поддержка трансферу инноваций в реальный сектор. Их тестированию будут способствовать уже начатые мега проекты «умных» городов, подобные футуристичному «городу будущего» NEOM, стоимость строительства которого оценивается в 500 млрд долл. США. Одновременно будут формироваться политики и нормы, стандарты и этические рамки, что является уникальной и весьма привлекательной возможностью для исследователей. Все это будет способствовать росту количества и качества научных публикаций, которые окажут глобальное влияние на развитие технологий ИИ, взаимодействие международных и национальных академических институтов.

Все перечисленное будет формировать целую экосистему сотрудничества и партнерства заинтересованных игроков и цифровых инфраструктур, платформ передовых знаний и поддержки стартапов (ожидается создание 300 инновационных компаний к 2030 году), отраслевых программ по использованию инноваций, просветительских кампаний об их результатах и пользе, что создаст предпосылки к масштабному внедрению технологий ИИ для социально-экономического роста и процветания.

В 2024 году планируется начать третью фазу реализации Стратегии, состоящую в осуществлении 15 национальных инициатив, в том числе программ сертификации специалистов, подготовки кадров, разработки регуляторных норм, развертывания инфраструктуры.

2.6. **Национальная стратегия кибербезопасности** (2020)

Следует отметить, что переосмысление рисков национальной безопасности, связанных с использованием ИКТ для разжигания «арабской весны», привело к принятию важных политических решений. В 2011 году была принята **Национальная стратегия информационной безопасности Королевства Саудовская Аравия** [30], обобщившая опыт в этой сфере ведущих государств мира. Стратегия впервые внедрила общегосударственный подход к защите национального информационного пространства и управлению кибербезопасностью, идентификации критических информационных инфраструктур и определению мер по их защите в соответствии с уровнем рисков, развитию национального потенциала в сфере кибербезопасности, в том числе кадрового и научного, установлению соответствующих механизмов обмена информацией и усилению партнерства.

Растущее количество изощренных компьютерных атак на объекты критической информационной инфраструктуры и государственный сектор[33], а также

33 Наиболее резонансные компьютерные атаки на КСА: 2012 год — Saudi Aramco подверглась атаке Shamoon,

реализация программы «Видение 2030» потребовали существенного усиления государственной политики в сфере обеспечения информационной безопасности. В декабре 2020 года была утверждена новая **Национальная стратегия кибербезопасности Королевства Саудовская Аравия** [31], разработанная Национальным управлением кибербезопасности. Она отражает стратегические амбиции Королевства обеспечить баланс между безопасностью, доверием и процветанием за счет устойчивого, надежного и безопасного национального киберпространства[34].

Стратегия определила 6 основных целей: комплексное управление безопасностью национального киберпространства; эффективное управление рисками информационной безопасности на национальном уровне; вовлечение в защиту киберпространства всех заинтересованных сторон; развитие и укрепление национальных возможностей в сфере защиты от киберугроз; укрепление партнерских отношений и сотрудничества в области обеспечения кибербезопасности; наращивание национального кадрового потенциала и развитие индустрии кибербезопасности в Королевстве. По данным открытых источников, в национальном информационном пространстве планируется усилить защиту и устойчивость систем управления и критических инфраструктур, повысить конфиденциальность данных государственных органов, инвесторов и обычных людей.

По оценке МСЭ, Саудовской Аравии удалось создать надежный и всеобъемлющий набор политик и стратегий для реализации всего потенциала цифровой трансформации в рамках программы «Видение 2030» [32].

3. Состояние нормативно-правовой базы в сфере цифровизации и обеспечения информационной безопасности

Описанные выше достижения Саудовской Аравии были бы невозможны без развития эффективной нормативной и правовой базы, а также создания механизмов сотрудничества регуляторов на национальном и международном уровне. С 2017 года **Национальный комитет по регулированию** (NRC)[35] осуществля-

---

результате которой было выведено из строя 30 тыс. рабочих терминалов и на неделю остановлена операционная деятельность компании; 2017 год — жертвами Shamoon 2 стали Saudi Aramco, Валютное агентство Саудовской Аравии (Центробанк КСА), Главное управление гражданской авиации, Министерство транспорта и еще 4 правительственных органа; осуществлены две изощренные атаки на произведенные в США контроллеры Schneider's Triconex управляющих систем National Industrialisation Company (Tasnee) и нефтеперерабатывающего завода Sadara Chemical Company, на последнем выведена из строя электростанция и была реальная угроза взрыва; 2021 год — злоумышленники похитили у Saudi Aramco 1Тбайт данных и требовали выкуп в криптовалюте эквивалентный 50 млн долл. США.

34 Концепция базируется на 6 элементах — интеграция, регулирование, обеспечение безопасности, защита, сотрудничество, строительство.

35 NRC — комитет высокого уровня из 9 национальных регуляторов, ответственных за цифровую трансформацию в ключевых экономических «вертикалях» (телекоммуникации и информация, технологии, транспорт, рынки

ет выработку и согласование программ развития и правовых рамок использования сквозных технологий в различных отраслях экономики, устраняет разрывы между внедрением передовых технологий и нормативной базой их применения. К достижениям КСА также относится создание в 2022 году специализированной Академии цифрового регулирования (DRA) для подготовки высококвалифицированных кадров, необходимых в большом количестве государственному и частному сектору для развития регуляторной среды в соответствии с лучшими мировыми практиками[36], соблюдения баланса интересов экономического развития и социальных выгод, повышения качества цифровых сервисов. Проделанная в этой сфере работа обоснованно вывела Саудовскую Аравию в лидеры рейтинга МСЭ 2023 года по новой методике оценки зрелости правового регулирования — первое место в регионе MENA и девятое среди стран G20[37].

3.1. Закон «О борьбе с киберпреступностью» (2007)

Закон о борьбе с киберпреступностью (англ. Anti-Cyber Crime Law, ACCL) принят Королевским указом № M/17 от 26 марта 2007 года [33]. Он наглядно отражает особенности религиозно-политического устройства государства и строгие требования к поведению мусульман, соблюдение которых контролируется оперативно-техническими методами[38]. Статья 2 определяет сферу применения ACCL как борьбу с компьютерными преступлениями за счет повышения информационной безопасности, защиты прав, относящихся к законному использованию компьютеров и информационных сетей, обеспечение защиты общественных интересов, морали и общих ценностей, а также национальной безопасности.

капитала, гражданская авиация, данные и искусственный интеллект, налоги/таможня, электроэнергия и конкуренция) путем выработки правил регулирования и законодательных норм.

36 Среди партнеров Академии указаны Международный союз электросвязи, Всемирный банк, Институт регуляторной политики (RPI) и международные тренинговые агентства. Источник: Digital Regulatory Academy Launched, by CITC, 9 Jan 2022, https://en.maaal.com/archives/202201/digital-regulatory-academy-launched-by-citc/

37 По методике оценки G5 Benchmark КСА получила 80,4 балла, страны БРИКС оценены следующим образом: Бразилия – 75,31, Россия – 64,04, Индия – 81,94, КНР – 71,65, ЮАР – 69,29, т.е. вся пятерка БРИКС попала в группу развитых государств (индекс от 60 до 80 баллов). Источник: Benchmark for Fifth Generation Digital Collaborative Regulation/ G5 Benchmark ITU, https://app.gen5.digital/benchmark/metrics?_ga=2.182559078.1565902013.1702625730-1451289763.1702625730&_gl=1*1ql4cot*_ga*MTQ1MTI4OTc2My4xNzAyNjI1NzMw*_ga_27GW57NRWK*MTcwMjYyODA3NS4xLjAuMTcwMjYyODA3NS4wLjAuMA..*_ga_6J744FX7L2*MTcwMjYyODA3Ni4xLjAuMTcwMjYyODA3Ni4wLjAuMA.

38 Государство блокирует многие зарубежные сайты, применяет методы фильтрации трафика. Анонимность в сети условная: активация sim-карты проводится на основе паспортных данных и отпечатка пальца. Это провоцирует активное использование на территории страны различных proxy-сервисов и виртуальных частных сетей (VPN) со сквозным шифрованием (по некоторым данным их применяют до 30% пользователей). В конце 2022 года Национальным управлением кибербезопасности была заключена крупная сделка с израильской компанией NSO, занимающейся разработкой систем слежения и компьютерной разведки. Судьба контракта в условиях Палестино-Израильского конфликта неизвестна. Источник: Cyber in Saudi Arabia, Huge investments with Israeli spying companies, 10 August 2022 https://saudileaks.org/en/cyber-%E2%80%8B%E2%80%8Bin-saudi-arabia-huge-investments-with-israeli-spying-companies/.

Статья 3 криминализует несанкционированное использование компьютеров, информационных сетей и других цифровых устройств любым из следующих способов: шпионаж, перехват или получение данных в информационных сетях или компьютерах; незаконный доступ к компьютеру с целью создания угроз и нанесения ущерба другому лицу; незаконный доступ к сайту или взлом с целью модификации или нарушения работы, использование его электронного адреса (URL); нарушение неприкосновенности частной жизни за счет использования камеры смартфона и пр.; распространение ложных сведений или нанесение другого ущерба с использованием информационных технологий. Дознание по таким делам может вести Государственная прокуратура[39], а решение выносит Уголовный суд, но с учетом законов шариата и традиций. Наказание может быть в форме тюремного заключения на срок до 1 года и/или штрафа до 500 тыс. SAR.

К более серьезным преступлениям относятся действия, связанные с нанесением материального ущерба физическому или юридическому лицу, такие как мошенничество или использование чужого имени или идентификационных данных с целью приобретения движимого имущества или облигаций, незаконный доступ к банковской карте для получения информации, средств или услуг (Статья 4), или незаконный доступ к компьютеру с целью удаления/кражи/уничтожения данных, изменения или нарушения персональных данных; вмешательство в работу информационных сетей для нарушения их работы, изменения или уничтожения данных и программного обеспечения; препятствование доступу к сервисам или нарушение их работы (Статья 5). Уголовный суд может назначить наказание за указанные деяния до 4 лет тюрьмы и/или штраф до 3 млн SAR.

Наиболее серьезные преступления касаются общественного порядка и национальной безопасности. Статья 6 криминализует передачу, публикацию или хранение материалов, несовместимых с общественным порядком или моралью, религиозными ценностями или нарушающих неприкосновенность частной жизни физического лица. Однако такая формулировка допускает очень широкое толкование норм закона. Криминализованы также другие общественно опасные преступления — распространение материалов порнографического характера[40] или другого аморального свойства, о торговле людьми или игорном бизнесе, продвижение/содействие употреблению или распространению наркотиков/ психотропных веществ. Эти преступления караются тюремным сроком до 5 лет и штрафом до 3 млн SAR.

---

39 В 2017 году Саудовское бюро расследований и прокуратуры (BIPP) МВД в ходе реформы государственных органов стало самостоятельным — Государственной прокуратурой (Public Prosecutor's office, PPO).

40 По данным за 2011-16 гг. в Саудовской Аравии 76% киберпреступлений относились к распространению детской порнографии. В ходе борьбы с этим социальным злом была прекращена деятельность 265 млн вебсайтов, причем до 22% их клиентов были женщины и девушки до 18 лет. Источник: 76 percent cybercrimes in KSA involve pornography, January 05, 2017, https://saudigazette.com.sa/article/170411

Статья 7 криминализует все формы пособничества терроризму, а также незаконный доступ к сайтам или информационным системам с целью получения данных для создания угроз внутренней или внешней безопасности государства или национальной экономике. Наказание — срок до 10 лет тюрьмы и штраф до 5 млн SAR, или другие наказания. Только определенные органы Министерства внутренних дел могут сообщать в Прокуратуру о случаях, связанных с этими деяниями, и никто не может присоединиться к такому делу с требованием возмещения ущерба. Как правило, такие преступления рассматриваются в рамках законов шариата и очень строго.

Следует отметить, что Саудовская Аравия в числе 18 членов Лиги арабских государств подписала Конвенцию по борьбе с использованием информационных технологий в преступных целях, но до сих пор ее не ратифицировала. Королевство не является участником Конвенции по киберпреступности ЕС (Будапештской конвенции, ETS №185), однако оно не поддержало российскую инициативу по созданию в Третьем комитете ООН Специального межправительственного комитета экспертов открытого состава для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях[41]. Возможно, это отражает намерение сохранить в КСА систему правосудия на основе шариата.

3.2. **Закон «Об электронных транзакциях»** (2007)

Закон об электронных транзакциях от 26 марта 2007 года [34], приравняв юридическую значимость традиционных и электронных сделок, цифровых документов и подписей, ввел правовой режим их использования. Кроме того, он определил меры защиты электронных документов и предупреждения злоупотреблений, мошенничества и растрат. Закон стал важной вехой развития в стране широкого спектра онлайн услуг: торговли, медицинских и образовательных, электронного правительства, финансовых и платежных систем.

Подзаконный акт, раскрывающий правила его применения, соответствует требованиям Комиссии ООН по праву международной торговли, устанавливает технические требования, которым должны удовлетворять электронные документы, чтобы бесспорно обеспечить предполагаемую юридическую силу, действительность и возможность приведения в исполнение. В частности, требуется, чтобы методы создания, хранения или передачи электронной записи исключали возможность ее изменения; обеспечивалась целостность электронных

41 Резолюция Генеральной Ассамблеи ООН № A/RES/74/247 от 27 декабря 2019 года «Противодействие использованию информационно-коммуникационных технологий в преступных целях».

документов за счет использования цифровых сертификатов и цифровых подписей, выданных уполномоченным поставщиком услуг, что создает правовую презумпцию для судов, что электронная подпись является действительной подписью.

3.3. Закон «Об электронной торговле» (2019)

Этот закон[42] разработан Министерством торговли и инвестиций. Он содействует цифровой трансформации Саудовской Аравии, поскольку определяет правовые рамки современной электронной торговли близкие к общепризнанным международным практикам и открывает внутренний рынок зарубежным игрокам, не имеющим регистрацию в KSA, но предоставляющим жителям страны свои услуги.

Закон повышает защиту торговых площадок и прав потребителей, в том числе от мошенничества, ложной и искаженной информации, стимулирует развитие этого сегмента ИКТ-рынка. Однако закон предполагает широкое экстерриториальное применение, обязывая не имеющих регистрацию в стране поставщиков услуг и торговые площадки (сервис-провайдеров) не только предоставлять данные о местонахождении платформ обработки данных, но и соблюдать требования обеспечения конфиденциальности данных пользователей, установленные в КСА.

Защите подлежат любые данные, которые могут привести к идентификации потребителя, включая имена, идентификационную информацию, адреса, контактные номера, номера лицензий, записи, номера личного имущества, номера счетов, фото и видеоизображения.

Согласно Статье 5, поставщик услуг не может хранить персональные данные или электронные сообщения потребителя, если между поставщиком услуг и потребителем не согласовано иное. Единственное исключение составляет период, необходимый для совершения транзакции электронной торговли. В течение этого периода поставщик услуг должен взять на себя ответственность за безопасность персональных данных потребителей. Он также несет ответственность за защиту таких данных, когда они попадают под контроль любых третьих сторон. Поставщику услуг не разрешается использовать персональные данные потребителей или электронные сообщения в любых нелицензионных или несанкционированных целях, или раскрывать их третьим лицам без согласия потребителя.

В случае утечки личной информации потребителя поставщик услуг должен уведомить Министерство торговли в течение 3 дней с момента, когда ему стало известно о нарушении, и проинформировать о масштабах инцидента, послед-

42 Electronic commerce Law одобрен Королевским указом № M/126 от 7 Зуль Када 1440 хиджры (соответствует 9 июля 2019 года).

ствиях и принимаемых мерах. Наказание за нарушение норм закона варьируется от простого предупреждения или денежного штрафа в размере до 1 млн SAR, до временной/ полной блокировки электронной торговли или веб-сайта.

Более детально меры защиты данных раскрываются в подзаконном акте «Правила электронной торговли», вступившем в силу в октябре 2019 года. Кроме того, Национальное управление кибербезопасности и Совет электронной торговли Саудовской Аравии подготовили «Руководящие принципы кибербезопасности для поставщиков услуг электронной торговли» и «Руководящие принципы кибербезопасности для потребителей электронной торговли». В первом из них предоставляются рекомендации по защите данных, устройств и услуг электронной торговли для их поставщиков, в первую очередь малым и средним предприятиям, продавцам малых и домашних офисов. Второй документ содержит рекомендации, которые помогут потребителям освоить безопасный опыт покупок и защитить свои устройства, данные и личную информацию во время онлайн-транзакций.

Пока неизвестно каким образом на выполнение закона «Об электронной торговле» скажется вступление в силу в октябре 2023 года первого в истории страны закона «О гражданских сделках» (Гражданский кодекс) [35], который обеспечит дополнительную определенность и гарантии в гражданских и коммерческих сделках в различных секторах, которые жизненно важны для Королевства.

3.4. **Закон «О защите персональных данных»** (2019)

Это первый в стране закон, определяющий правила обработки персональных данных (ПД), до него применялись принципы защиты приватности по законам шариата и наилучшие практики отраслевого регулирования [36]. Закон разработан Саудовским управлением по данным и искусственному интеллекту (SDAIA), принят в 2019 году [37] и полностью вступил в силу в 14 сентября 2023 года, но юридическим лицам предоставлен годичный льготный период для обеспечения соблюдения его норм.

Положения закона гармонизированы с Общим регламентом защиты данных ЕС (GDPR) и тоже включают суверенитет данных и экстерриториальное применение. Закон распространяется на государственные и иные организации, которые независимо от цели и формы обработки ПД осуществляют эту деятельность на территории Саудовской Аравии, а также на зарубежные компании, осуществляющие обработку ПД резидентов Королевства на территории иных стран. Контроль за выполнением норм возложен на Национальной отдел управления данными (NDMO) в структуре SDAIA (см. Раздел 4.3).

Закон регулирует отношения, связанные с защитой ПД физических лиц, проживающих в Королевстве (субъектов ПД), а также сбор, обработку, раскры-

тие, передачу, в том числе трансграничную, и хранение ПД. Следует отметить, что под термином ПД в законе понимаются не только идентификационные данные человека, но и косвенные, которые при использовании в сочетании с другими данными могут однозначно идентифицировать физическое лицо (например, IP-адреса, регистрационные номера транспортных средств, физические адреса, сведения о работодателе, информация о доходах).

Закон вводит категорию субъектов — «контролеры данных», определяющих цель и метод обработки ПД. Они должны предпринять достаточные шаги для проверки точности, полноты и актуальности ПД до их обработки и обязаны вести учет действий по обработке в течение периода своей деятельности по обработке данных и еще в течение 5 лет после ее прекращения. Они обязаны придерживаться принципов защиты данных и соблюдения приватности, оценивать риски, осуществлять информирование об утечках.

Юридические лица, должны зарегистрироваться в национальном реестре контролеров данных. Они обязаны выбирать операторов обработки ПД, которые предложат достаточные гарантии соблюдения положений Закона, регулярно проверять, что они выполняют их инструкции относительно защиты ПД. Трансграничная передача данных разрешена при условии, что у оператора есть конкретная законная цель для передачи ПД за пределы страны, а страна-получатель или юридическое лицо имеют действующие правила или гарантии для обеспечения надлежащей защиты данных без ущерба для уровня защиты, гарантированного законом. SDAIA собирается опубликовать «Белый список» стран, которые соответствуют их стандартам аккредитации по защите данных.

Операторы обработки ПД обязаны информировать регулирующий орган, в течение 72 часов с момента, когда им становится известно об утечке данных и представить всесторонний анализ нарушения, описать меры для предотвращения подобных инцидентов в будущем. Если нарушение представляет значительный риск для личной информации физических лиц, юридические лица должны без неоправданной задержки уведомить пострадавших.

Юридические лица должны получить согласие субъекта ПД на обработку его данных, которое он может отозвать в любое время. Закон определяет другие права субъектов ПД: на получение информации об обработке своих ПД и правовых основаниях для такой обработки; на доступ к своим ПД и получение копии всех своих данных, хранящихся у юридического лица; на исправление и/или обновление своих ПД; на запрос об удалении своих данных, если в них больше нет необходимости. Кроме того, субъекты ПД имеют возможность подать жалобы относительно исполнения закона в соответствующий регулирующий орган.

В отличие от GDPR, за нарушение норм закона предусматривается уголовное наказание в виде заключения под стражу до 2 лет, если это действие совершено с на-

мерением причинить вред субъекту ПД или получить личную выгоду. Лишение свободы может быть заменено или сочетаться со штрафом до 1,1 млн долл. США [38].

3.5. **Правовые рамки использования облачных вычислений** (2018)

Этот нормативный акт (англ. Cloud Computing Regulatory Framework, CCRF) [39] разработан Комиссией по связи и ИТ (CITC) в 2018 году. Он дополняет описанный выше закон в контексте использования облачных центров или сервисов для обработки ПД и способствует уточнению правовых рамок реализации государственной политики Cloud First. Является одним из немногих в мире примеров нормативно-правового регулирования облачных технологий, введен в действие в 2018 году, поправки внесены в 2019 и 2021 гг.

CCRF регулирует права и обязанности провайдеров облачных услуг и их потребителей в лице государственных и коммерческих предприятий, а также частных пользователей. Прежде всего, любой поставщик облачных услуг обязан зарегистрироваться в CITC и предоставить информацию о местоположении и основных характеристиках своих центров обработки данных, расположенных в КСА и за рубежом, которые он использует для обработки данных и контента облачных клиентов из Саудовской Аравии. Поставщики обязаны соблюдать стандарты безопасности, а также правила и рекомендации, связанные с обеспечением непрерывности бизнеса, аварийным восстановлением и управлением рисками, которые CITC считает обязательными.

При этом основная ответственность за обеспечение безопасности данных лежит на потребителе облачных услуг, поскольку он должен выбрать поставщика в соответствии с уровнем критичности своей информации и контролировать выполнение им требований регулятора:

Уровень 1: Конфиденциальный пользовательский контент частных лиц или компаний частного сектора, на который не распространяются какие-либо отраслевые ограничения на передачу данных на аутсорсинг.

Уровень 2: Конфиденциальный контент частных лиц или компаний частного сектора, на который не распространяются какие-либо отраслевые ограничения на передачу данных на аутсорсинг, и конфиденциальный контент клиентов государственных органов и их подрядчиков.

Уровень 3: Любой пользовательский контент из отраслей, регулируемых частным сектором, подпадающий под отраслевые правила или решения регулирующего органа; и конфиденциальный пользовательский контент государственных органов и их подрядчиков.

Уровень 4: Высокочувствительный или секретный контент клиентов, принадлежащий соответствующим правительственным агентствам или институтам.

Тем самым Саудовская Аравия вводит локализацию обработки чувствительных данных на территории страны, передача данных за рубеж должна быть оправдана и впрямую прописываться в контракте на оказание услуг.

Поставщики облачных услуг обязаны уведомлять клиентов облачных сервисов о любом нарушении информационной безопасности или утечке, которые могут повлиять на данные/ контент клиентов или на получаемые ими услуги. Регулятор (CITC) уведомляется в обязательном порядке, если указанные инциденты относятся к информации Уровня 3, или к данным или контенту значительного числа облачных клиентов или жителей Саудовской Аравии.

Важно отметить, что поставщики облачных услуг не обязаны осуществлять на своих платформах выявление размещенного третьими лицами противозаконного или нежелательного контента и не будут нести административную или уголовную ответственность в случае его выявления, однако они обязаны удалять указанный контент по предписанию правоохранительных органов в соответствии с законом «О борьбе с киберпреступностью» (2007) [40].

3.6. **Правовые рамки предоставления услуг Интернета вещей** (2019)

Данный нормативный акт [41] касается поставщиков услуг Интернета вещей (IoT), предоставляющих свои услуги посредством мобильной связи, фиксированных сетей связи и с использованием локальных сетей, использующих не подлежащие лицензированию радиочастоты. Он обязывает лицензированных поставщиков услуг IoT и разработчиков сетей IoT получать сертификат на свою продукцию, соблюдать требования регулятора по обеспечению безопасности данных, размещать все используемые для предоставления услуг IoT серверы и хранить все данные на территории Саудовской Аравии, а также соблюдать другие законы, правила и требования (все существующие и принятые в будущем) CITC или других органов, касающиеся управления данными, конфиденциальности и защиты данных. Срок хранения данных поставщиками услуг IoT определен в 1 год.

3.7. **Правовые рамки применения национальных криптографических стандартов** (2020)

Этот нормативный акт (NCS 1: 2020) определяет национальные криптографические стандарты[43], применимые для обеспечения защиты национальных данных, систем и сетей, а также для гражданских и коммерческих целей. Предполагает базовый и продвинутый уровень для более гибкого сочетания необходимых

43 В том числе, определяет политики и процедуры управления ключами шифрования, алгоритмы симметричного шифрования для потоков данных и алгоритмы блочного шифрования.

средств в зависимости от целей и объектов защиты. По сути является перечнем одобренных Национальным управлением кибербезопасности международных стандартов и наилучших практик. Данные о создании национального органа стандартизации в открытом доступе отсутствуют.

3.8. **Важные меры контроля кибербезопасности** (2018)

Важные меры контроля кибербезопасности (англ. Essential Cybersecurity Controls, ECC [42]), разработаны Национальным управлением кибербезопасности в 2018 году, являются базовым документом в сфере обеспечения информационной безопасности в Саудовской Аравии.

По сути ECC конкретизирует все рассмотренные выше нормативные рамки. Документ определяет минимальный набор требований кибербезопасности (конфиденциальность, целостность, доступность), основанный на наилучших практиках и стандартах управления рисками реализации внешних и внутренних угроз в отношении информации и информационных инфраструктур. Включает 114 «точек контроля» в 5 областях: управление кибербезопасностью, организация защиты, обеспечение устойчивости, кибербезопасность облачных вычислений и третьих сторон, кибербезопасность промышленных систем управления.

Нормы ECC обязательны для всех государственных учреждений, юридических лиц и компаний, аффилированных с ними, а также организаций частного сектора, которые владеют, эксплуатируют или размещают критически важную национальную инфраструктуру[44]. Они обязаны обеспечить обработку и хранение своей информации на территории Саудовской Аравии. В дополнение к ECC разработаны руководства по контролю кибербезопасности критических систем (2019); облачных сервисов (2020) и операционных технологий (OT) (2022).

Требования и руководства по кибербезопасности разработаны и отраслевыми регуляторами, например Национальным банком Саудовской Аравии (SAMA)[45], Министерством здравоохранения (MoH)[46], Советом кооперативного медицинского страхования (CCHI), Министерством людских ресурсов и социального развития (MHRSD), Министерством туризма (MoT) и др. Не все требования гармонизированы, в некоторых существуют значительные расхождения, что создает двусмысленность, поэтому совершенствование национальной нормативной и правовой базы будет продолжено.

---

44 Для остальных предприятий и организаций они носят рекомендательный характер.

45 Cyber Security Framework of the Saudi Arabian Monetary Authority (2017).

46 The Saudi Health Information Exchange Policies (2016), Saudi Health Information Exchange Testing and Certification Policies (2016), Telemedicine Regulations in the Kingdom of Saudi Arabia (2018)

4. Основные государственные структуры, участвующие в обеспечении национальной информационной безопасности

Национальную систему обеспечения кибер- и информационной безопасности можно охарактеризовать как достаточно зрелую и эффективную. Однако вертикаль власти выстроена на прямых родственных связях. Совмещение членами королевской семьи нескольких должностей приводит к нечеткому разграничению функций между государственными органами и структурами. Механизм принятия решений и координации всей системы непрозрачен.

Король Салман бен Абдель Азиз Аль Сауд является премьер-министром страны и главой Совета министров, а также главнокомандующим. Непосредственно ему подчинены Национальное управление кибербезопасности и Управление государственной безопасности, которые играют ключевую роль в обеспечении национальной кибербезопасности.

Наследный принц Мухаммед бен Сальман Аль Сауд, являющийся премьер-министром и председателем Совета министров, возглавляет два его подкомитета, принимающие политические решения[47]. Первый из них — **Совет по делам в области политики и безопасности[48],** состоящий из министров обороны, иностранных дел, национальной гвардии, начальника общей разведки, министра по делам ислама, пожертвований, призыва и руководства, а также двух государственных министров (без портфеля), один из которых возглавляет Управление государственной безопасности. Второй — **Совет по делам экономики и развития**, который состоит из 24 руководителей экономических и социальных ведомств, в том числе министров финансов, связи и ИТ, внутренних дел, СМИ, хаджа и Умры. Оба совета имеют отношение к выработке политики в области национальной кибербезопасности.

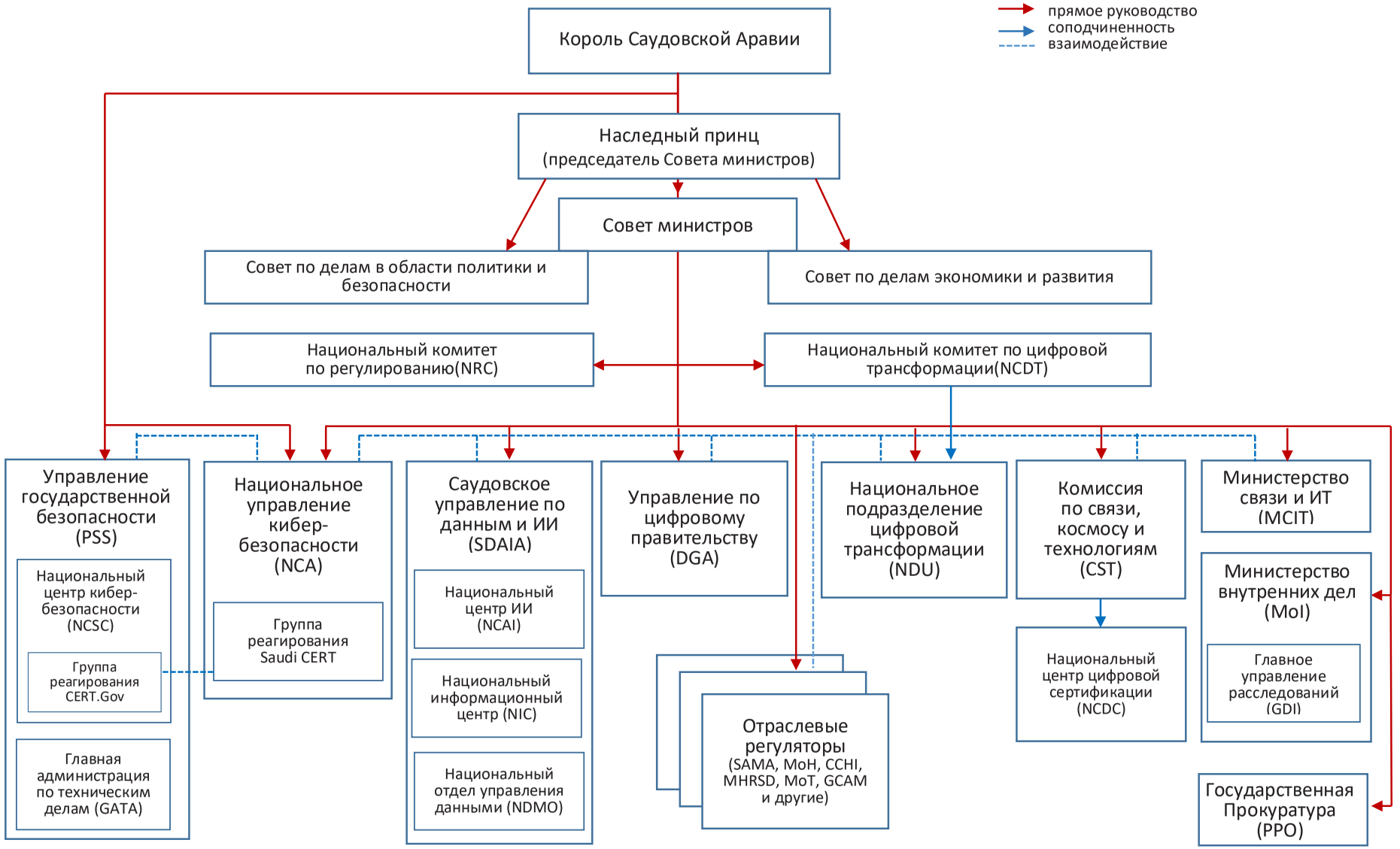
4.1. Управление государственной безопасности

Управление государственной безопасности (англ. Presidency of State Security, PSS) создано по Королевскому указу от июля 2017 года в качестве независимого органа, который напрямую подчинен премьер-министру. Является органом внутренней и внешней разведки, обеспечивает в рамках своих полномочий безопасность нации, противодействие разведке, терроризму, шпионажу и кибершпионажу, идеологическому вторжению всех видов. Руководителем PSS является совет-

47 Члены указанных Советов назначаются Королевским указом.

48 Совет по делам в области политики и безопасности создан в 2015 году вместо Совета национальной безопасности.

Схема. Основные элементы системы управления национальной информационной безопасностью КСАИспользованная литература



ник Короля по национальной безопасности — начальник Главного управления разведки[49].

При создании PSS переданы несколько структур из Министерства внутренних дел, которые позволяют Управлению решать задачи Национальной стратегии кибербезопасности: служба радиотехнической разведки — Главная администрация по техническим делам (англ. GATA), Национальный информационный центр (англ. NIC), а также Национальный центр кибербезопасности.

4.1.1. Национальный центр кибербезопасности

В 2013 году в Министерстве внутренних дел был создан Национальный центр электронной безопасности (англ. NCES), который позднее, в связи с расширением функционала, получил название Национальный центр кибербезопасности (англ. NCSC), в 2017 году переподчинен PSS.

Он является операционно-техническим подразделением и отвечает за разработку и использование комплексных мер защиты сетей и информационных ресурсов правительственных учреждений, а также критических информационных инфраструктур, прежде всего промышленных систем управления SCADA в энергетике и промышленном секторе [43]. В его функционал входит разработка национальных стандартов, правил и требований защиты информационных инфраструктур и критически важных объектов; выявление рисков и анализ угроз; разработка мер сквозной защиты безопасности; организация обмена информацией и распространение предупреждений об угрозах между различными секторами.

NCSC является ядром системы реагирования на компьютерные инциденты на объектах, находящихся в его оперативном обеспечении 24/7, и в случае необходимости осуществляет координацию действий всех уполномоченных структур для реагирования в национальном масштабе. Технические и операционные функции по обнаружению, пресечению и восстановлению после компьютерных инцидентов выполняет группа реагирования CERT.Gov [44].

4.2. Национальное управление кибербезопасности

Национальное управление кибербезопасности (англ. National Cybersecurity Authority, NCA) [45] создано по Королевскому указу № 6801 от 31 октября 2017 года, курируется лично наследным принцем, который одновременно возглавляет Министерство обороны. Управление деятельностью NCA осуществляет руководитель в ранге министра[50] и совет, в состав которого входят главы Управ-

49 С момента создания управления GIP (General Intelligence Presidency) должность руководителя занимает Abdulaziz bin Mohammed Al Howairini.

50 С 2021 года ее занимает Majid bin Mohammed Al Mazyad, который до назначения был заместителем министра

ления государственной безопасности, Главного управления разведки, заместитель министра внутренних дел, помощник министра обороны.

Миссия NCA состоит в выполнении целей «Видения 2030» по обеспечению безопасности национального киберпространства для повышения доверия к политике властей в этой сфере, содействия технологическому росту, социальному развитию и процветанию королевства. В связи с этим NSA имеет мандат на регуляторные, операционные и оперативные действия:

- разработку национальной стратегии кибербезопасности и контроль за ее реализацией;
- разработку нормативно-правовых актов в сфере обеспечения кибер- и информационной безопасности;
- разработку и внедрение политик, требований и руководств по обеспечению кибербезопасности, управлению рисками, реагированию на компьютерные инциденты, использованию криптографических средств защиты, а также надзор за их выполнением[51];
- укрепление и постоянное совершенствование национального потенциала в сфере защиты от киберугроз, выявление и пресечение компьютерных атак, в том числе через создание, контроль и эксплуатацию в Саудовской Аравии национальных и отраслевых (при необходимости) операционных центров/платформ кибербезопасности для анализа угроз, управления рисками, контроля соблюдения политик безопасности, мониторинга, реагирования и расследования инцидентов и обмена информацией с NCA;
- повышение осведомленности о киберугрозах путем взаимодействия с государственным и частным сектором и постановки перед ними задач, проведения семинаров, реализации учебных программ и выпуска печатных материалов;
- стимулирование роста национального сектора кибербезопасности[52], поощрение инвестиций и инноваций;

связи и ИТ, Комиссии по связи и ИТ, а также представлял Саудовскую Аравию в МСЭ.

51 В частности, NCA разработаны протоколы контроля безопасности аккаунтов организаций в социальных медиа, кибербезопасности (данных, облачных сервисов, телекоммуникаций, критически важных систем, операционных технологий); руководство по кибербезопасности пользователей электронной коммерции; национальные криптографические стандарты. Согласно National Assessment Cyber Plan в 2023 году на соответствие установленным требованиям будут проверены 7 тыс. предприятий.

52 В августе 2022 года NCA анонсировала инициативу CyberIC по ускорению развития этого сектора и, особенно, национальных инструментов и технологий кибербезопасности, обучающих методик и материалов. На первом этапе будет осуществлено повышение осведомленности в сфере кибербезопасности, улучшение навыков 1,5 тыс. государственных служащих как в части управления рисками и аудита соответствия стандартам, так и по программам оценки реальной защищенности (тесты на проникновение и активный поиск уязвимостей «red teams»). Будут поддержаны 40 стартапов через акселераторы и отобрано еще 20 через новую версию кибер-соревнований. Курсы повышения квалификации пройдут 10 тыс. саудитов, работающих в секторе кибербезопасности, а также 5 тыс. индивидуальных предпринимателей. NCA в кооперации с ведущими мировыми университетами предложит программы обучения для 150 руководителей отделов ИТ-безопасности (CISOs). Источник: Saudi Arabia launches CyberIC program to boost country's cybersecurity, https://fastcompanyme.com/news/saudi-arabia-launches-cyberic-program-to-boost-countrys-cybersecurity/

- установление связей с аналогичными агентствами за рубежом и частными организациями для взаимного обмена знаниями и опытом в области кибербезопасности.

Еще одной важной задачей является содействие развитию национального кадрового потенциала в области кибербезопасности. При непосредственном участии NCA разработаны квалификационные требования к специалистам в сфере кибер- и информационной безопасности и единая терминологическая база для работодателей и агентств по набору персонала в этой сфере [46], а также требования к образовательным программам ВУЗов по всему спектру необходимых специальностей [47].

В NCA базируется национальная группа реагирования на компьютерные инциденты Saudi CERT. Основная ее задача — повышение уровня осведомленности и знаний в сфере кибербезопасности, обнаружения, предотвращения, координации реагирования на компьютерные инциденты в национальном сегменте сети Интернет [48]. В соответствии с Регламентом NCA, все власти Саудовской Аравии должны в полной мере сотрудничать с Управлением и немедленно уведомлять о любом риске (существующем или возможном), киберугрозе или взломе. Saudi CERT является членом Международного форума групп реагирования FIRST, группы реагирования Организации исламского содружества OIC-CERT и Арабского регионального центра безопасности ITU-ARCC.

Также NCA совместно с бизнес и академическим сообществом разработало и поддерживает веб-портал HASEEN, который является доступной для национальных предприятий целостной платформой управления кибербезопасностью и наращивания потенциала в этой сфере[53]. Особое внимание уделяется управлению соответствием требованиям, обмену информацией, аутентификации электронных писем, верификации файлов и контактов.

4.3. Саудовское управление по данным и искусственному интеллекту

Независимое агентство — Саудовское управление по данным и искусственному интеллекту (англ. Saudi Data and Artificial Intelligence Authority, SDAIA) создано в 2019 году[54]. Вне всяких сомнений, оно является флагманским проектом наследного принца Мухаммеда бен Салмана (возглавляет совет директоров SDAIA), реализация которого должна вывести Саудовскую Аравию в мировые лидеры применения ИИ и преобразовать жизнь в стране на основе этой технологии.

53 Эти усилия возглавляются саудовской компанией SITCO, при участии CITC, МВД, Саудовской компании информационных технологий (SITE) и Государственной научной организацией «Город науки и технологий имени короля Абдул-Азиза».

54 SDAIA создано на основании Королевского указа No.74167 Thu Al-Hijjah, 1440 (30 августа 2019 года), https://sdaia.gov.sa/.

Основными задачами SDAIA являются:

- координация реализации Национальной стратегии по данным и ИИ;
- выработка необходимой нормативной базы, в первую очередь в сфере сбора и обработки Больших данных, использования технологий ИИ;
- продвижение этических принципов разработки и использования ИИ [55];
- внедрение государственных облачных сервисов и управление центрами обработки данных, распространение опыта КСА на всю экономику и глобально;
- развитие системы цифровой идентификации;
- развитие национальных цифровых платформ;
- содействие развитию национальных талантов и специалистов в области технологий ИИ и Больших данных, введение соответствующих курсов обучения в специализированных школах.

Для реализации этих масштабных задач в SDAIA действует несколько профильных подразделений.

В частности, **Национальный центр искусственного интеллекта** (англ. National Center for AI, NCAI) занимается координацией передовых разработок и внедрением инноваций в указанной сфере. **Национальный отдел управления данными** (англ. National Data Management Office, NDMO) является национальным регулятором и контролером использования данных, обеспечения их информационной безопасности и защитой частной жизни. При непосредственном участии NDMO разработано 7 национальных правил управления данными[56]: В функции отдела входит содействие улучшению обмена информацией, повышение совместимости наборов Больших данных для увеличения добавочной стоимости от их использования. Для этого NDMO выстраивает взаимодействие с государственными органами, коммерческими компаниями и другими заинтересованными сторонами для координации действий и выработки эффективного подхода к управлению данными. Кроме того, NDMO выполняет операционную работу по обработке государственных данных.

4.3.1. Национальный информационный центр

В структуру SDAIA Национальный информационный центр (анг. National Information Center, NIC) передан из Управления государственной безопасности

55 В сентябре 2023 года SDAIA опубликовало обновленную версию AI Principles 2.0, обязательную для соблюдения всеми разработчиками ИИ. https://www.dataguidance.com/jurisdiction/saudi-arabia.

56 Правила классификации данных в зависимости от уровня конфиденциальности, Правила предоставления открытых данных всем заинтересованным лицам, Правила улучшения обмена данными между государственными агентствами и получению данных из их ресурсов, Правила защиты персональных данных и обеспечении национального суверенитета над ними, Правила обеспечения свободы получения открытой информации от государственных органов, Общие правила передачи данных за географические границы КСА, Правила защиты ПД несовершеннолетних и защиты последних от неподобающей информации.

в 2019 году[57]. NIC позиционируется в качестве «первого поставщика видения и анализа методов ИИ», имеет большой опыт предоставления ИТ-решений и услуг другим правительственным учреждениям в различных частях Саудовской Аравии, является держателем **Национального банка данных**[58].

4.4. Управление по цифровому правительству

Государственное Управление по цифровому правительству (англ. Digital Government Authority, DGA) создано в 2021 году и начало действовать в марте 2022 года[59]. К нему перешли все программы, связанные с цифровизацией государственных органов, совершенствованием регуляторной политики, развитием стратегии и услуг электронного правительства, поддержки его цифровых и облачных платформ и сайтов, предоставление государственных услуг бизнесу и частным лицам, проведение оценок эффективности электронного правительства и пр. К концу 2022 года Саудовская Аравия запустила более 30 облачных сервисов, создала 169 центров обработки данных, объединивших более 175 млн наборов данных, успешно внедрила 8 цифровых политик для приведения к единой системе обмена данными 130 правительственных структур, обслужила 610 млн запросов на предоставление госуслуг [49].

DGA осуществляет лицензирование поставщиков технических решений и сервисов для государственных органов[60], ведет репозиторий программного обеспечения (в том числе с открытым программным кодом), автоматически верифицирует и валидирует источник программного кода, дает юридическое обоснование для размещения электронных сервисов на сторонних площадках, резервирует и проверяет доступность доменов и др.

Первыми шагами DGA после создания были действия по унификации 816 государственных платформ в различных ведомствах. Пока их количество

---

57 С 1979 года Центр под разными наименованиями действовал в структуре МВД. С 2017 года NIC предоставлял Управлению государственной безопасности высокоэффективные электронные услуги, несколько месяцев в 2019 году был частью указанного ведомства, в составе которого получил сертификат от British Standards Institution Group за предоставление высококачественных услуг облачных вычислений. https://www.eyeofriyadh.com/directory/details/7297_the-national-information-center-nic).

58 Национальный банк данных является централизованным репозиторием наборов данных государственных органов КСА, используется, в правительственных системах поддержки решений. Имеет службы повышения качества данных, единый индекс с учетом применяемой в бизнесе терминологии, руководство по всем сферам и взаимосвязям между системами различных ведомств. По данным с конца 2018 по 2020 год в банке данных объединено 169 дата-центров 90% государственных учреждений, 130 сервисов доступа и в октябре 2020 года запущен правительственный облачный сервис DEEM.

59 Digital Government Authority (https://dga.gov.sa/en) создано на основе Постановления Совета министров № (418) от 7/25/1442 АН (соответствует 3 марта 2021 года).

60 По состоянию на 2022 год были выданы лицензии трем компаниям: в сфере информационной безопасности Elm, цифровых сервисов для бизнеса Takamol, разработчику и оператору действующих платформ и продуктов для электронного правительства Thiqah. Источник: DGA licenses 3 technology firms to develop, operate 15 digital products for 10 govt agencies, June 13, 2022, https://saudigazette.com.sa/article/621719.

удалось снизить до 630, но планируется довести до 200. В дальнейшем предполагается совершенствование регуляторной политики, прежде всего для сокращения сегментации государственного сектора, а также для сквозного применения передовых технологий (искусственный интеллект, блокчейн) в различных отраслях и сферах применения, для управления глобальными кризисами (подобных пандемии COVID-19).

4.5. Национальное подразделение цифровой трансформации

Это подразделение (англ. National Digital Transformation Unit, NDU) является независимым агентством, созданным Королевским указом в 2017 году. Действует как исполнительный орган Национального комитета по цифровой трансформации (NCDT), выполняет три основных функции:

- содействие и ускорение цифровой трансформации во всех сферах, в том числе за счет сотрудничества с GDA и SDAIA;
- обеспечение обмена опытом цифровизации между государственными ведомствами и учреждениями, выработка рекомендаций по улучшению национальных и ведомственных стратегий цифровой трансформации, программ их реализации;
- реализация обязанностей секретариата NCDT, включая управление подкомитетами и целевыми группами, контроль выполнения решений и рекомендаций NCDT, подготовка докладов и рекомендаций, проведение исследований [50].

4.6. Комиссия по связи, космосу и технологиям

Комиссия по связи, космосу и технологиям (англ.CST)[61] в 2022 году стала «наследницей» действовавшей с 2003 года Комиссии по связи и ИТ (CITC). Новое название получено в связи с расширением полномочий Комиссии на сферу космической связи[62] и передовые технологии. Она действует как независимый орган и является национальной Администрацией связи. CST осуществляет свою деятельность по развитию секторов связи и ИТ, почтовой отрасли, по созданию высоко конкурентной среды и предоставлению телекоммуникационных услуг,

61 Значение интеграции коммуникаций, космоса и технологий подчеркнул Декрет Кабинета министров №235 о создании Communications, Space & Technology Commission.

62 В 2019 году Саудовская Аравия в сотрудничестве с американской Lockheed Martin запустила первый национальный спутник связи SGS-1. В труднодоступных районах КСА подключение к глобальной сети обеспечивается низкоорбитальной группировкой спутников (ее принадлежность не указывается, вероятнее всего StarLink).

формированию экосистемы для привлечения инвесторов. В соответствии с законом «Об электронных транзакциях» в ее функции входит:

- регулирование сектора связи и ИТ, в том числе выдача/отзыв лицензий операторам связи, провайдерам услуг, удостоверяющим центрам;
- разработка нормативной базы оказания услуг связи и ИТ, обеспечения их информационной безопасности[63];
- отслеживание и внедрение разработок в области технологий и услуг сектора связи и ИКТ;
- выработка и внедрение политики в области аудиовизуальной деятельности;
- выдача лицензий на передачу аудиовизуального контента;
- развитие условий для инвестиций в сектор коммуникаций и ИТ.

Также CST отвечает за функционирование в стране инфраструктуры отрытых ключей (PKI)[64] для обеспечения использования электронной подписи и цифровых документов, безопасной передачи цифровой информации между заинтересованными сторонами, включая правительство, граждан и бизнес. Правила использования PKI определены законом «Об электронных транзакциях», их выполнение возложено на подведомственный Национальный центр цифровой сертификации (NCDC).

CST совместно с Министерством финансов и NCDC управляет платформой обмена данными Saudi Electronic Data Interchange (Saudi EDI), которая вне зависимости от используемой технологической среды позволяет на основе унифицированных интерфейса и структуры данных обмениваться документами между партнерами по бизнесу или внутри организаций.

Кроме того, во исполнение закона «О противодействии терроризму» при помощи операторов связи и провайдеров услуг доступа к контенту Комиссия осуществляет выявление в национальном сегменте сети Интернет запрещенных законом, либо не соответствующих требованиям шариата или порочащих королевскую семью материалов. Она выдает решения о блокировке таких ресурсов, а данные о нарушителях передает в соответствующие службы. Содействие в решении этих задач оказывает Генеральная комиссия по аудиовизуальным средствам массовой информации (GCAM).

В августе 2022 года Комиссия запустила отраслевой центр реагирования на компьютерные инциденты ICT-CSIRT, который выявляет угрозы и уязвимости

63 Общие принципы защиты персональных данных (2020), Руководство по оценке рисков нарушения частной жизни (2020), Процедура «приземления» сервисов и продуктов, основанных на персональных данных пользователей или распространении персональных данных (2020), Временные правила защиты данных и их распространения (2020).

64 Public Key Infrastructure (PKI) применяется для обмена открытыми ключами при использовании схем ассиметричного шифрования.

в ИКТ-инфраструктуре и почтовых сервисах и оказывает содействие в предупреждении и снижении рисков [51].

Под эгидой CST регулярно проводятся обучающие и тренировочные кампании по информационной безопасности с целью защиты прав пользователей ИКТ, а также разрабатывается необходимая нормативная база.

4.7. Министерство связи и информационных технологий

Министерство связи и информационных технологий (англ. MCIT) осуществляет регулирование деятельности в области развития и использования ИКТ, определении общей политики и планов развития для индустрии связи и ИТ, инициирует и разрабатывает законодательство в рамках своих полномочий [52].

В функции MCIT входит обеспечение развития технических платформ для цифрового общества, цифровой экономики и цифровой страны, а также реализация программы Yesser по развитию инфраструктуры электронного правительства, для повышения производительности и эффективности государственного сектора путем эффективного обмена информацией и предоставления государственных услуг.

Важной задачей MCIT является взаимодействие с Министерством образования по разработке программ обучения цифровым технологиям.

4.8. Министерство внутренних дел

В части обеспечения национальной информационной безопасности министерство решает задачу расследования совершенных с использованием ИКТ преступлений и привлечения к ответственности нарушителей закона. Этим занимается Главное управление расследований (GDI), в функции которого входит проведение разведывательных и контрразведывательных мероприятий и борьба с угрозами национальной безопасности (от терроризма до подрывной политической деятельности), осуществляемые в том числе, с использованием ИКТ.

4.9. Элементы государственно-частного партнерства

Национальной стратегией кибербезопасности признается важность государственно-частного партнерства в этой сфере, однако за столь незначительный период действия по реализации стратегии пока не сформированы необходимое доверие и механизмы взаимодействия власти и бизнеса. Явный прогресс можно отметить по двум направлениям: инвестиции и образование.

Саудовская Федерация по кибербезопасности, программированию и дронам (SAFCSP) — национальное учреждение [53], действует под эгидой Олимпийского комитета Саудовской Аравии, стремится наращивать национальный и профессиональный потенциал в области кибербезопасности и программирования в соответствии с признанными международными практиками и стандартами, чтобы ускорить восхождение страны в ряды развитых стран в области технологических инноваций. В рамках достижения указанных целей Федерация занимается проведением конференций (более 240), повышением осведомленности общественности о важности кибербезопасности и программирования, поддержкой молодых талантов; проведением образовательных программ (более 154 программ тренингов), оказанием помощи в восстановлении и развитии самобытных национальных компетенций; проведением соревнований, поддержкой участия молодых талантов в местных или международных соревнованиях по кибербезопасности и программированию. В 2019 году Федерация организовала образовательную программу «Тувайкский киберкамп» — самое большое мероприятие подобного рода на Ближнем Востоке.

В 2018 году Федерация подписала Меморандумы о взаимопонимании по сотрудничеству с американскими компаниями, обслуживающими военно-промышленный комплекс США — Lockheed Martin, Raytheon Company, Northrop Grumman, с Booz Allen Hamilton о подготовке кадров и проведении соревнований в сфере кибербезопасности. В 2020 году SAFCSP подписала Меморандумы о взаимопонимании с Kaspersky Lab по осуществлению программ обучения молодежи в сфере кибербезопасности.

Центр передового опыта в области информационного обеспечения в Университете короля Сауда (CoEIA) является некоммерческой структурой, целью которой является разработка и предоставление решений в области безопасности для повышения уровня информационной безопасности как в государственном, так и в частном секторах [54]. Центр также предоставляет консультационные услуги по безопасности компьютерных сетей и информационных систем, применению международных стандартов, а также по разработке учебных программ по информационной безопасности. Тесно сотрудничает в этой сфере с большим количеством известных учреждений и исследовательских центров по всему миру.

5. Участие в сотрудничестве с ООН и другими глобальными организациями в области формирования системы международной информационной безопасности

Специалисты Института новой Европы отмечают, что еще совсем недавно Саудовская Аравия не считала проблематику информационной безопасности зна-

чимым элементом своей внешней политики и не вступала в международные блоки в сфере кибербезопасности [55]. После принятия программы «Видение 2030» приоритеты сменились, сдвиг геополитической обстановки также оказал влияние на действия Эр-Рияда.

Страна намерена выйти с регионального уровня на международный и стать заметным игроком G20 в сфере кибербезопасности и искусственного интеллекта. В подтверждение этого тезиса можно отметить полезные для укрепления имиджа КСА соглашения о сотрудничестве с МСЭ, МВФ и Конференцией ООН по торговле и развитию (UNCTAD) по измерению различных индексов цифровизации. Притязания на лидерство проявились и в инициативе проведения под патронатом короля Салман бен Абдель Азиз Аль Сауда Глобального форума кибербезопасности (GCF). Первый форум проведен Национальным управлением кибербезопасности в 2020 году в рамках председательства Саудовской Аравии в G20. Он получился очень представительным — 147 спикеров из 51 государства. Следующий GCF-2022 поднял актуальную тему «Переосмысление глобального киберпорядка», в нем приняли участие 4,5 тыс. приглашенных из 110 стран. В 2023 году масштаб форума на тему «Определение общих приоритетов» еще больше расширился: 150 докладчиков, охват 120 стран. Это свидетельствует о росте авторитета Саудовской Аравии и формировании Королевством нового центра силы в сфере кибербезопасности.

При этом у страны отсутствуют инициативы на тех площадках, которые оказывают влияние на формирование системы международной информационной безопасности, что может свидетельствовать как об определенной предосторожности, так и об отсутствии стратегии действий.

Участие в работе Организации Объединенных Наций

Саудовская Аравия не принимала участия в работе Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности ООН (ГПЭ по МИБ), но всегда поддерживала разработанные ею резолюции.

В одноименной Группе ООН открытого состава (РГОС) созыва 2019–21 гг. Королевство принимало участие, но не вносило документов, отражающих национальную позицию [56]. В РГОС созыва 2021–25 гг. аккредитована как негосударственный участник Саудовская Федерация по кибербезопасности, программированию и дронам [57].

Участие в работе Международного союза электросвязи

В конце 2020 года Национальное управление кибербезопасности в сотрудничестве с Международным союзом электросвязи подписало Соглашение о стра-

тегическом партнерстве по запуску глобальной программы безопасного и процветающего киберпространства для детей.

6. Участие в международном сотрудничестве с другими международными организациями и государствами в области формирования системы международной информационной безопасности

КСА является членом Организации исламского сотрудничества и Совета сотрудничества арабских государств Персидского залива (ССАГПЗ) и принимает участие в их деятельности по обеспечению региональной информационной безопасности, главным образом в формате конференций и взаимодействия национальных групп реагирования на компьютерные инциденты.

На данном историческом этапе Саудовская Аравия встала на путь заключения двусторонних соглашений с профильными ведомствами других государств по конкретным направлениям работы, в 2023 году эта деятельность заметно активизировалась, несколько соглашений подписано на полях GCF.

6.1. Российская Федерация

В октябре 2017 года состоялось подписание Меморандума о взаимопонимании между Министерством связи и массовых коммуникаций Российской Федерации и Министерством связи и информационных технологий Королевства Саудовская Аравия о сотрудничестве в области связи и информационно-коммуникационных технологий.

Меморандум закрепил обоюдное намерение партнеров вести совместную работу по целому перечню направлений сферы ИКТ, которые затрагивают не только отдельные вопросы развития сферы связи и ИТ, но и глобальные направления сотрудничества. Так, положениями меморандума предусматривается усиление сотрудничества в области широкополосного доступа в сеть Интернет, управления сетью Интернет, электронного правительства, совместная разработка программного обеспечения, цифрового контента, облачных вычислений, Больших данных, Интернета вещей. В рамках меморандума стороны осуществляют сотрудничество в области подготовки кадров в сфере связи и ИКТ, а также содействуют отраслевому сотрудничеству и инвестициям, совместным инновациям, проведению исследований, обмену технологиями в профильных областях.

В 2019 году Россия и КСА подписали Исполнительную программу технологического сотрудничества и Меморандум о сотрудничестве в области массовых коммуникаций. В рамках соглашений стороны договорились развивать совмест-

ные проекты в сферах искусственного интеллекта и «умных» городов. Тогда же подведомственный Минцифры России фонд «Росинфокоминвест» подписал Меморандум о взаимопонимании с Saudi Business Machines[65]. Документ подразумевает реализацию маркетинговых и образовательных проектов по темам кибербезопасности, обработки и анализа Больших данных и искусственного интеллекта.

6.2. Индонезия

В июле 2019 года Министерством связи и ИТ Королевства Саудовская Аравия подписан Меморандум о действиях в сфере цифровой экономики с Министерством связи и информатики Индонезии, который будет способствовать осуществлению Умры в Мекке и Медине паломниками из Индонезии за счет присоединения к саудовскому Umrah Digital Enterprise двух компаний-единорогов из Индонезии (Tokopedia и Traveloka) [58].

6.3. Индия

В августе 2023 года заключено соглашение между Министерством связи и ИТ Королевства Саудовская Аравия и Министерством железных дорог, коммуникаций, электроники и ИТ Индии о сотрудничестве в сфере развития цифровой инфраструктуры, дистанционного обучения и медицины, исследований, инноваций и использовании передовых технологий [59].

6.4. Финляндия

В октябре 2023 года подписан Меморандум о стратегическом сотрудничестве между Министерством связи и ИТ Королевства Саудовская Аравия и Министерством внешней торговли Финляндии о развитии цифровой экономики, обмене опытом, совместном проведении исследований передовых технологий, наращивании потенциала и координации частного сектора обеих стран [60].

6.5. Япония

В октябре 2023 года, уже после получения Саудовской Аравией приглашения в БРИКС, Министерство связи и ИТ Королевства Саудовская Аравия подписало Меморандум о взаимопонимании в сфере развития цифровизации и электронного правительства с Цифровым агентством Японии. Стороны намерены также

65 Официальный представитель IBM World Trade Corporation.

обмениваться политиками, осуществлять совместные исследования и инновационные практики [61].

6.6. Пакистан

В октябре 2023 года подписан Меморандум о взаимопонимании между Федеральным министерством ИТ, телекоммуникаций, науки и технологий Пакистана и Министерством связи и ИТ Королевства Саудовская Аравия в сфере коммуникаций и развития цифровой инфраструктуры с широкой программой действий. Планируется создать специальную группу для продвижения сотрудничества между малыми и средними предприятиями, экосистемами стартапов, содействия обмену информацией между бизнес-акселераторами и инкубаторами передовых технологий.

Сторонами будет организовано взаимодействие в сфере развития политик и нормативно-правового обеспечения цифровизации и развития сектора производства электроники. Партнеры намерены участвовать в международных мероприятиях друг друга и обмениваться информацией между государственными и частными предприятиями в сфере ИТ и электроники.

Сотрудничество коснется и вопросов эффективного инвестирования и использования венчурного капитала, электронного правительства, «умной» инфраструктуры, цифровой медицины и образования, передовых технологий (искусственный интеллект, Интернет вещей, робототехника, облачные вычисления, блокчейн и онлайн-игры), совместных исследований, программ подготовки специалистов и сотрудничества университетов, инновационных центров и центров обмена опытом. В сообщении также упомянуты оптоволоконные сети, центры обработки данных и облачные вычисления [62].

6.7. Сотрудничество с другими государствами в сфере кибербезопасности

Стали появляться и договоренности в сфере обеспечения информационной безопасности, так в ноябре 2023 года заключены Меморандумы о взаимопонимании с национальными органами кибербезопасности Кувейта, Катара, Испании и Румынии [63].

Результаты анализа тематик указанных выше межведомственных соглашений свидетельствуют, что Саудовская Аравия на данном этапе только присматривается к потенциальным партнерам в сфере цифровизации и наращивания потенциала и старается диверсифицировать риски оказаться между различными полюсами силы.

7. Возможные приоритеты КСА в сфере обеспечения национальной и международной информационной безопасности в рамках БРИКС

Саудовская Аравия является самой крупной экономикой Ближнего Востока. Ее участие в БРИКС существенно повышает совокупный вклад объединения в мировой ВВП.

Королевство проявляет большой интерес к новым финансовым институтам БРИКС и с мая 2023 года ведет переговоры по присоединению к Банку развития. Несомненно, что это направление сотрудничества будет содействовать упрощению взаимных расчетов Саудовской Аравии с ее основным торговым партнером — Китаем, а также с другими членами объединения, даст импульс новым инфраструктурным проектам БРИКС и повысит страхование рисков.

Учитывая масштаб диверсификации экономики и темпы развития национального ИКТ-рынка востребованными направлениями несомненно окажутся инструменты сотрудничества в сфере науки, технологий и инноваций (НТИ). Прежде всего это — ПартнерствоБРИКС по вопросам новой промышленной революции и его Консультативная группа для углубления сотрудничества в области цифровых технологий, индустриализации, инноваций и инвестиций, а также решения вызовов, формируемых Четвертой промышленной революцией, а также новая архитектура БРИКС в сфере НТИ, которая включает Сеть инновационных исследований iBRICS, Платформу энергетических исследований, Сеть БРИКС по передаче технологий, Центр промышленных компетенций стран БРИКС.

С учетом планов Саудовской Аравии по созданию регионального хаба обработки Больших данных, высока вероятность интереса к деятельности Рабочих групп БРИКС по ИКТ и высокопроизводительным вычислительным системам; по вопросам сотрудничества в области информационно-коммуникационных технологий; по вопросам безопасности в сфере использования ИКТ.

Со своей стороны, КСА может предоставить странам-участницам БРИКС возможности участия в своих проектах информатизации и тестирования технологий «умных» городов. Для России и других членов БРИКС будет полезен опыт регуляторной политики Саудовской Аравии в сфере ИКТ, что одновременно послужит гармонизации национальных законодательств.

8. Использованная литература

1. Saudi Arabia: number of internet users 2023, https://www.statista.com/statistics/1392844/saudi-arabia-number-of-internet-users/.
2. Saudi Vision 2030, https://vision2030.gov.sa/en.

3. Saudi Arabia – Information and Communications Technology, 2022-07-06, https://www.trade.gov/country-commercial-guides/saudi-arabia-information-and-communications-technology#:~:text=5G%3A%20Saudi%20Arabia%20was%20among,the%20first%20quarter%20of%202021.
4. Pete Bell Saudi Arabia's ICT Strategy 2023 Tracking 5G Deployments in the Middle East and Africa, Mar 27, 2023, https://blog.telegeography.com/tracking-5g-deployments-in-the-middle-east-and-africa.
5. Там же.
6. State of 5G in Saudi Arabia: Expectations and current reality, Apr 13, 2022, https://www.cio.com/article/308484/state-of-5g-in-saudi-arabia-expectations-and-current-reality.html.
7. Saudi Arabia – Information and Communications Technology, 2022-07-06, https://www.trade.gov/country-commercial-guides/saudi-arabia-information-and-communications-technology.
8. Saudi Arabia's Investments in Artificial Intelligence Aim to Transform Economy and Workforce, 25 September 2023, https://ts2.space/en/saudi-arabias-investments-in-artificial-intelligence-aim-to-transform-economy-and-workforce/#gsc.tab=0.
9. Saudi Arabia Data Centers, 2023, https://www.datacentermap.com/saudi-arabia/.
10. Saudi Arabia Cloud Computing Market Share & Industry Report, 2030, https://www.gmiresearch.com/report/saudi-arabia-cloud-computing-market/.
11. The Impact of Cloud Computing Technology in Saudi Arabia // KYM Global Insights, https://kymgl.com/saudi-arabia-cloud-computing/.
12. Saudi Arabia Data Center Market to Surpass Investment of $2 Billion by 2028, the Region is Witnessing Major Cloud Investments, May 10, 2023 https://www.bloomberg.com/press-releases/2023-05-10/saudi-arabia-data-center-market-to-surpass-investment-of-2-billion-by-2028-the-region-is-witnessing-major-cloud-investments.
13. Ecommerce in Saudi Arabia in 2023 August 12, 2023, https://istizada.com/ecommerce-in-saudi-arabia-the-complete-guide/, GCC E-Commerce Statistics - Growth in the GCC – IstiZada, October 5,2023, https://istizada.com/blog/gcc-e-commerce-statistics/.
14. YEFI – Yesser Framework For Interoperability Riyadh, October 28, 2005, https://www.unapcict.org/sites/default/files/2019-01/Saudi%20Arabia%20-%20Yesser%20Framework%20For%20Interoperability.pdf.
15. 5G and other innovative technologies to encourage ICT growth in Saudi Arabia - Saudi Arabia 2020 - Oxford Business Group, https://oxfordbusinessgroup.com/reports/saudi-arabia/2020-report/economy/well-connected-5g-and-other-innovative-technologies-encourage-sector-growth.
16. Saudi Arabia - Information and Communications Technology https://www.trade.gov/country-commercial-guides/saudi-arabia-information-and-communications-technology.
17. Global Cybersecurity Index 2020, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.
18. Saudi 'instant' work visa gives tech hiring, entrepreneurship a boost | CIO https://www.cio.com/article/193814/saudi-arabias-instant-work-visa-gives-tech-entrepreneurship-a-boost.html.
19. Human Capability Development Program 2021-2025, https://andp.unescwa.org/sites/default/files/2022-11/Human%20Capability%20Development%20Program%20Delivery%20Plan%20%282%29.pdf ,
The strategic plan of the Ministry of Education (на арабском языке) https://andp.unescwa.org/sites/default/files/2022-11/StrategyMOE001.pdf.
Deal signed to boost cybersecurity education in Saudi Arabia, March 24, 2021, https://www.arabnews.com/node/1830711/saudi-arabia.
20. vision-2030-achievements-booklet-2016-2020, https://www.vision2030.gov.sa/media/poghcang/vision-2030-achievements-booklet-2016-2020-1.pdf.
21. Цуканов Л.В. Система национальной кибербезопасности Саудовской Аравии: специфика и риски развития // Вестник Кемеровского государственного университета. Серия: Политические, социологические и экономические науки. 2021. Т. 6. № 4. С. 435–443. https://doi.org/10.21603/2500-3372-2021-6-4-435-443.
22. Here's how Saudi Arabia is investing in the technology of the future Jan 17, 2023, https://www.weforum.org/ agenda/2023/01/davos23-why-saudi-arabia-high-tech-future-davos2023/.
23. Global Innovation Index 2023, https://www.wipo.int/global_innovation_index/en/2023/.
24. Vision 2030 for Kingdom of Saudi Arabia, https://www.vision2030.gov.sa/v2030/vrps/ntp/.
25. National Transformation Program, https://na.vision2030.gov.sa/media/p0oftryh/document-ntp-copy.pdf.
26. Saudi Arabia National Transformation Plan approved: A quick guide, Bloomberg Jun 07, 2016, https://www.thenationalnews.com/business/saudi-arabia-national-transformation-plan-approved-a-quick-guide-1.211757.
27. Country review: Saudi Arabia's digital transformation and collaborative regulation, ITU 2022, https://digitalregulation.org/wp-content/uploads/21-00770_R3_Saudi-Arabia-digital-transformation_E_web.pdf.

28. https://www.vision2030.gov.sa/media/oisolf4g/vision-2030_story-of-transformation.pdf.
29. Realizing our Best Tomorrow. Strategy Narrative, Brochure NSDAI Summit version, October 2020, https://andp.unescwa.org/sites/default/files/2021-10/Brochure_NSDAI_Summit%20version_EN%5B1%5D.pdf.
30. Developing National Information Security Strategy for the Kingdom of Saudi Arabia, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/SaudiArabia_NISS_Draft_7_EN.pdf.
31. https://www.nca.gov.sa/files/national_cybersecurity_strategy-en.pdf.
32. Country review: Saudi Arabia's digital transformation and collaborative regulation, ITU 2022, https://digitalregulation.org/wp-content/uploads/21-00770_R3_Saudi-Arabia-digital-transformation_E_web.pdf.
33. Anti-Cyber Crime Law Royal Decree No. M/17 8 Rabi 1 1428 / 26 March 2007 First Edition 2009 https://sherloc.unodc.org/cld/uploads/res/document/sau/2007/anti-cyber_crime_law_html/Anti-Cyber_Crime_Law_E.pdf.
34. Закон Electronic Transactions Law одобрен Королевским указом № M/18 от 8 Раби Аваля 1428 хиджры (соответствует 26 марта 2007 года) https://web.archive.org/web/20170917170649/http://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Pages/ElectronicTransactionsLaw.aspx.
35. Закон Civil Transaction Act одобрен Королевским указом M/199 Зуль-Цида 29 1444 года хиджры (соответствует 16 июня 2023 года). https://conflictoflaws.net/2023/the-new-saudi-civil-transaction-act-and-its-potential-impact-on-private-international-law-in-saudi-arabia/.
36. Saudi Arabian Airlines, https://www.saudia.com/help/useful-links/legal-and-terms-and-conditions/data-protection-policy, SABIC, https://www.sabic.com/en/data-protection, Saudi Aramco, https://www.aramco.com/en/website-information/privacy-statement#.
37. Закон Personal Data Protection Law (PDPL) одобрен Королевским указом № M/19 от 17 сентября 2021 года, в него внесены поправки Королевским указом № M/ 48 от 27 марта 2023 года. На английском языке закон доступен по адресу: Data Protection Laws and Regulations Report 2023. Saudi Arabia, https://iclg.com/practice-areas/data-protection-laws-and-regulations/saudi-arabia.
38. Saudi Arabia's Personal Data Protection Law – What you need to know, 2023, https://www.herbertsmithfreehills.com/insights/2023-11/saudi-arabias-personal-data-protection-law-–-what-you-need-to-know.
39. Cloud Computing Regulatory Framework, https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/CCRF_En.pdf.
40. CITC's New Cloud Computing Regulatory Framework in Saudi Arabia, https://www.tamimi.com/law-update-articles/citcs-new-cloud-computing-regulatory-framework-in-saudi-arabia/.
41. Internet of Things (IoT) Regulatory Framework, Sep. 2019, https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/IoT_REGULATORY_FRAMEWORK.pdf.
42. Essential Cybersecurity Controls (ECC-1: 2018), https://nca.gov.sa/ecc-en.pdf.
43. Cyber capabilities and national power. Volume 2. Saudi Arabia, p. 95-108, International Institute for Strategic Studies, 2023, https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/09/cyber-capabilities-and-national-power-vol-2/cyber-capabilities-and-national-power_volume-2_09-saudi-arabia.pdf.
44. Saudi CERT is part of the National Cybersecurity Authority (NCA) https://cert.gov.sa/documents/55/RFC_2350_-_Saudi_CERT_73eYwyW.pdf.
45. National Cybersecurity Authority, https://www.nca.gov.sa/en/index.html.
46. The Saudi Cybersecurity Workforce Development (SCyWF), 2020, https://cybilportal.org/publications/the-saudi-cybersecurity-workforce-development-scywf/.
47. Saudi Cybersecurity Higher Education Framework, SCyber-Edu, https://seu.edu.sa/en/news/17102022/.
48. Сайт CERT.Gov https://www.cert.gov.sa/.
49. Saudi Arabia implements data driven-government to realise digital economy as part Vision 2030, 27 Sep 2022, https://www.khaleejtimes.com/business/saudi-arabia-implements-data-driven-government-to-realise-digital-economy-as-part-vision-2030.
50. NDU, About the National Digital Transformation, https://ndu.gov.sa/en/about
Country review: Saudi Arabia's digital transformation and collaborative regulation, ITU, https://digitalregulation.org/wp-content/uploads/21-00770_R3_Saudi-Arabia-digital-transformation_E_web.pdf.
51. https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/09/cyber-capabilities-and-national-power-vol-2/cyber-capabilities-and-national-power_volume-2_09-saudi-arabia.pdf
52. Ministry of Communications and Information Technology, https://www.mcit.gov.sa/.
53. Сайт SAFCSP, https://safcsp.org.sa/en/.
54. About CoEIA, https://coeia.ksu.edu.sa/en/about.
55. Cybersecurity in Saudi Arabia / Institute of New Europe, August 11, 2021, https://ine.org.pl/en/cybersecurity-in-saudi-arabia/.
56. Open-ended Working Group – UNODA, https://disarmament.unoda.org/open-ended-working-group/.

57. Open-ended working group on security of and in the use of information and communications technologies 2021–2025, A/AC.292/2023/INF/3, 22 May 2023, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/A-AC-292-2023-INF3_(List_of_non-governmental_entities)-advanced.pdf.
58. Indonesia, Saudi Arabia sign MoU on digital cooperation, 4th July 2019, https://en.antaranews.com/news/128359/indonesia-saudi-arabia-sign-mou-on-digital-cooperation.
59. Saudi Arabia, India sign cooperation agreement on Digital Economy, https://english.alarabiya.net/business/economy/2023/08/20/Saudi-Arabia-India-sign-cooperation-agreement-on-Digital-Economy.
60. Saudi Arabia, Finland Deepen Cooperation in ICT to Boost Digital Economy, 5 October 2023, https://english.aawsat.com/technology/4626876-saudi-arabia-finland-deepen-cooperation-ict-boost-digital-economy.
61. BRICS: Saudi Arabia & Japan Sign Digital Economy Partnership, Oct. 13, 2023 https://watcher.guru/news/brics-saudi-arabia-japan-sign-digital-economy-partnership.
62. Saudi Arabia & Pakistan sign MoU to accelerate digital transformation Mon, 2 Oct, 2023 https://www.gccbusinessnews.com/saudi-arabia-pakistan-sign-mou/.
63. Saudi Arabia, Four Countries Sign Cybersecurity MoUs, 3 Nov 2023, https://english.aawsat.com/business/4645086-saudi-arabia-four-countries-sign-cybersecurity-mous.

Объединенные Арабские Эмираты

Официальное название: Объединенные Арабские Эмираты (араб. Аль-Имарат аль-Арабия аль-Муттахида)

Столица: Абу-Даби

Официальный язык: арабский, широко распространены английский, персидский (фарси), индийский и урду.

Территория: по официальным данным правительства ОАЭ территория страны 83,6 тыс. км^2 (114 место в мире). Государство расположено в восточной части Аравийского полуострова на побережье Персидского и Оманского заливов, где имеет несколько сотен мелких островов. На юге и западе граничит с Саудовской Аравией, на востоке с Оманом, на северо-западе (по морю) с Катаром. Также имеет морскую границу с Ираном, с которым существует территориальный спор вокруг трех островов в Персидском заливе.

Население: 9,52 млн чел. (число постоянно проживающих в стране по данным на 2023 год [1]), что является 96 показателем в мире. Правительство ОАЭ оперирует цифрой в 10,04 млн чел., причем 9 млн из них являются городскими жителями, преимущественно в Абу-Даби и Дубае. Более 60% из постоянно проживающих — мужчины, при этом гражданами являются чуть более 62%, остальные резиденты/экспаты (больше всего индусов (37,96%), пакистанцев (16,72%), представителей Бангладеш и Филиппин (около 7%), вдвое меньше иранцев, непальцев и жителей Шри-Ланки [2].

Государственное устройство: по временной конституции, принятой 2 декабря 1971 года и утвержденной Высшим советом 20 мая 1996 года, ОАЭ являются федеративным монархическим государством, состоящим из семи эмиратов — конституционных монархий (Абу-Даби, Аджман, Дубай, Фуджейра, Рас-эль-Хайма, Шарджа и Умм-эль-Кайвайн), которые обладают самостоятельностью и суверенитетом над своей территорией.

Высший совет Федерации является верховным органом власти федерации и определяет общую политику государства. Он состоит из правителей эмиратов, которые формально из своего состава избирают президента сроком на 5 лет. Пост главы государства наследственно занимает эмир Абу-Даби, он является верховным главнокомандующим вооруженными силами, председателем Высшего совета обороны. Глава государства подписывает указы и постановления, подтвержденные Высшим советом Федерации, нормативные акты, принятые Советом министров. Кроме того, президент назначает членов дипломатического корпуса,

высших гражданских и военных чиновников, объявляет амнистию, либо подтверждает смертные приговоры.

Глава исполнительной власти — председатель Совета министров (пост наследственно занимает эмир Дубая), совмещающий свои обязанности с функциями вице-президента; формально назначается президентом и утверждается Высшим советом Федерации. Он формирует и представляет на утверждение президенту состав правительства, которое непосредственно проводит в жизнь внутреннюю и внешнюю политику страны. К полномочиям правительства относятся разработка законопроектов и федерального бюджета, принятие постановлений и инструкций для исполнения законов и других нормативных актов, наблюдение за исполнением судебных решений, ратификация международных договоров и соглашений, назначение и увольнение федеральных чиновников, которые не требуют особого распоряжения других высших органов государства. Федеральный национальный совет — совещательный орган парламентского типа, не обладающий законодательной инициативой, выносимые им заключения по проектам федеральных законов носят рекомендательный характер [3].

Судебная власть представлена Федеральным верховным судом, судами первой и второй инстанции, а также судами отдельных эмиратов.

Экономика: По данным Всемирного банка за 2022 год показатели Валового внутреннего продукта (ВВП) (по паритету покупательной способности):

Итого: 828 млрд долл. (33 место в мире).

На душу населения: 87 729 млрд долл. США (6 место в мире).

Показатели ВВП (Номинал):

Итого: 508 млрд долл. (28 место в мире).

На душу населения: 53 758 долл. США (16 место в мире).

Дипломатические отношения с Россией (СССР): Дипломатические отношения между ОАЭ и СССР были установлены 8 декабря 1971 года.

1. Уровень развития ИКТ-инфраструктуры и информатизации страны

Объединенные Арабские Эмираты являются примером эффективной диверсификации национальной экономики, которая еще 40 лет назад практически полностью зависела от добычи и экспорта углеводородов[1]. В этом масштабном процессе трансформации руководство страны основную ставку сделало на повсеместное внедрение информационных технологий и развитие высокотехнологичного производства. Основными драйверами цифровизации являются правительство, банковский сектор, здравоохранение, энергетика, логистика и туризм.

Достигнутые успехи страны впечатляют. Согласно рейтингу Глобальной цифровой конкурентоспособности 2023[2], ОАЭ занимают 12 позицию в мире и первое место в арабском регионе. Наиболее высокие показатели по следующим показателям: создание благоприятной среды для талантливых специалистов и молодежи (1 место в мире), уровень внедрения ИКТ (3 место), правовое регулирование (8 место).

Государство системно работает над улучшением условий для притока в страну капитала. Эмираты в настоящее время являются ведущим направлением инвестиций, связанных с ИКТ в странах Персидского залива, и стремятся, учитывая свои финансовые ресурсы и статус, выйти за пределы региона MENA[3] и стать глобальным центром технологий и инноваций. По данным Министерства экономики ОАЭ, общий объем иностранных инвестиций в сектор ИКТ эмирата Абу-Даби вырос с 1,9 млрд долл. США в 2013 году до 10,6 млрд долл. в 2021 году (в период 2019–20 гг. рост ускорился на 25,8%.). Огромный интерес к местному рынку проявляет зарубежный бизнес — прямые иностранные инвестиции в ИКТ-сектор ОАЭ в 2013–21 гг. выросли на 380%.

Значительные капиталовложения позволили создать в стране ИКТ-инфраструктуру мирового уровня. По данным британской аналитической и консалтинговой компании Global Data, в 2022 году рынок телекоммуникационных услуг ОАЭ оценивался в 8,4 млрд долл. США, по прогнозам он будет расти до 2027 года совокупными годовыми темпами в 2%. Этот сегмент рынка практически поделен между двумя крупными компаниями. Телекоммуникационный опера-

1 В 1980 году доходы нефтегазового сектора обеспечивали более половины ВВП страны (55,2%), к началу 2000 года показатель снизился практически в два раза (28,7%), а на конец 2021 года он составил 24,5%. Источник: https://finex.blog/kak_ustroena_ekonomika_obedinennykh_arabskikh_emiratov/

2 Индекс World Digital Competitiveness Ranking учитывает три группы параметров: знания (поиск талантов, образование и подготовка, научные исследования), технологии (в т.ч. регуляторная база и капиталовложения для их внедрения), готовность к будущему (адаптивные подходы, гибкость бизнеса, интеграция ИТ). Источник: IMD 2023, https://worldcompetitiveness.imd.org/countryprofile/AE/digital?internal=true

3 Ближний Восток и Северная Африка (Middle East & North Africa)

тор ОАЭ Etisalat, переименован в 2022 году в «e&», что ознаменовало новое направление развития компании как глобального игрока, ориентированного на цифровизацию и передовые технологии. Его основным конкурентом является Интегрированная телекоммуникационная компания Emirates (торговая марка «Du»), она предлагает услуги мобильной, фиксированной связи, широкополосного доступа и телевидение по IP-протоколу частным лицам, домашним хозяйствам и предприятиям.

Эмираты первые в арабском регионе и четвертые в мире приступили к развертыванию сетей подвижной связи 5G. Уже в 2019 году компания Etisalat предоставила своим клиентам первую полноценную коммерческую услугу на основе указанной технологии, чуть позже это сделала «Du». К февралю 2023 года охват населения сетями 5G достиг 97%: все основные городские районы и множество соединяющих их автомагистралей, включая Абу-Даби, Дубай, Шарджу, Фуджейру, Рас-эль-Кайму и Умм-эль-Кувейн. При этом средняя скорость загрузки контента была самой высокой в мире (более 557 Мбит/с). К концу 2025 года все города и поселения будут полностью покрыты сетями 5G. Выделение дополнительных радиочастот позволит операторам и ИКТ-провайдерам создавать совершенно новые сервисы и типы взаимодействия между устройствами Интернета вещей, что произведет революционные преобразования в способах взаимодействия компаний с клиентами, самый крупный и населенный эмират Абу-Даби позиционирует себя в авангарде развития связи следующего поколения (6G).

По данным Управления по регулированию телекоммуникаций ОАЭ, в июне 2022 года количество подписок на мобильную связь в два раза превышало население (около 204 подписок на сотню жителей), а общее количество активных мобильных пользователей достигло примерно 18,7 млн. Хорошая связанность создает условия для высокой инклюзивности, в настоящее время уровень проникновения сети Интернет составляет 103%, т.е. на каждого жителя приходится более одного уникального IP-адреса. В 2023 году в стране Интернетом пользовались 10,07 млн чел., из них 9,20 млн делали это с помощью смартфонов и генерировали почти 63,7% всего интернет-трафика.

Спрос на бытовую автоматизацию высокого уровня в сочетании с потреблением мультисервисных услуг (звук, видео, данные) быстро растет. Высокая плотность населения в крупных городах позволяет эффективно использовать наземную инфраструктуру связи: Эмираты занимают первое место в регионе Ближнего Востока по использованию для широкополосных подключений оптоволоконных кабелей. В ОАЭ зарегистрировано более 250 тыс. пользователей, подключенных к Интернету в своих квартирах и домах с помощью оптоволокна, в то время, как в Саудовской Аравии этот показатель достигает только 5 тыс., еще меньше он в Бахрейне и Египте. Услуги доступа в Интернет для домашних пользователей пре-

доставляются как правило вместе с телевидением по IP-протоколу и проводным домашним телефоном. Средняя скорость широкополосного доступа в 2023 году составляла 189,1 Мбит/с.

Также на территории страны, площадь которой лишь в два раза больше Московской области, расположены 5 точек примыкания к глобальным сетям подводных кабелей. Хорошо развита спутниковая связь. В настоящее время три оператора[4] эксплуатируют 9 спутников на геостационарной и низкой околоземной орбите, предоставляя более чем в 140 странах услуги мобильной и фиксированной спутниковой службы, спутникового вещания, дистанционного зондирования. Кроме того, запущены аппараты для образовательных и экспериментальных целей, такие как Nayif-1. С помощью Роскосмоса выведен на орбиту спутник PHI-Demo[5], предназначенный для хранения и пересылки на орбиту данных с подключенных к Интернету по 5G устройств, расположенных в отдаленных районах. К значимым технологическим достижениям ОАЭ следует отнести запуск в марте 2024 года крупнейшей на Ближнем Востоке квантово-оптической наземной станции сверх защищенной глобальной связи (ADQOGS), которая станет одним из узлов строящейся сети с квантовым распределением ключей шифрования [4].

Национальный ИКТ-рынок является одним из самых больших на Ближнем Востоке и, несмотря на некоторое замедление ежегодного роста до 12,77% в период пандемии COVID-19, по прогнозам Министерства экономики ОАЭ в 2024 году его объем составит 66 млрд долл. США [5]. Наиболее стремительно развитие в следующих секторах ИКТ-рынка, в каждом из которых есть значительные возможности для частных инвестиций: искусственный интеллект (ИИ) и Большие данные, кибербезопасность, Интернет вещей, программное обеспечение, компьютерные системы и облачные сервисы, телекоммуникации и 3D-печать.

На территории ОАЭ создана мощная инфраструктура для обработки Больших данных, наибольшее количество центров обработки данных (ЦОД) сконцентрированы в эмирате Дубай — 11 единиц, в городе Абу-Даби — 7 и еще один в Аль-Айне (эмират Абу-Даби) [6]. Основными поставщиками аппаратного и программного обеспечения для них являются IBM, Microsoft, Alibaba.

Значительное финансирование научных исследований и развития инновационной системы приносят свои плоды. В 2023 году ОАЭ вплотную приблизились к TOP30 мировых лидеров, заняв 32 место в Глобальном инновационном индексе. Причем по показателям уровня научных исследований, развития инфраструктуры и институтов управления страна заняла позицию в TOP20 [7]. Для разработки и внедрения передовых технологий ОАЭ одними из первых в Персидском

4 Thuraya Satellite Communication Company, Al Yah Satellite Communications Company, Космический центр Мохаммеда бин Рашида — MBRSC.

5 Все механические компоненты спутника изготовлены в ОАЭ в сотрудничестве с национальным частным сектором.

заливе стали создавать ИКТ-технопарки. Так при содействии Booz&Company[6] в 2000 году был запущен Dubai Internet City, положивший начало формированию кластеров специализированных технопарков (Dubai Techno Park, Dubai Silicon Oasis и CERT в Абу-Даби) [8]. Они оказывают значительное влияние на ускорение инновационного развития и трансфера технологий за счет динамичной экосистемы предпринимательства, льготных условий для стартапов, консалтинга и содействия продвижению ИКТ-продуктов на рынки. Правительство ОАЭ в рамках своей инициативы «Предпринимательская нация» намерено к 2030 году зарегистрировать более 8 тыс. малых и средних предприятий и стартапов с целью создания к 2031 году 20 компаний-единорогов[7]. Этому будут содействовать программы и инициативы эмиратов Абу-Даби[8] и Дубай[9].

Еще одним ключевым компонентом для превращения ОАЭ в лидера применения технологий ИИ является создание инфраструктуры высокопроизводительных систем. В настоящее время в стране расположены 13 суперкомпьютеров из мирового TOP500. Основные вычислительные мощности находятся в частном секторе — 89%, в научных учреждениях и университетах — 8% и 3% у федерального и местных правительств (в том числе, в Агентстве дорог и транспорта Дубая, Цифровом агентстве Абу-Даби и Национальной нефтяной компании эмирата Абу-Даби) [9].

Национальный лидер в технологиях ИИ — корпорация Group 42[10] — использует для облачных вычислений суперкомпьютеры Artemis (36 место в мире

---

6 Компания являлась дочерним предприятием американской Booz Allen Hamilton Inc., в 2014 году ее поглотила PricewaterhouseCoopers.

7 Компании-единороги (unicorn company) - молодые компании, которые менее чем за 10 лет смогли вырасти с нуля до бизнеса с капитализацией в 1 млрд долл. США и объемом инвестиций более 100 млн, причем для достижения этого не привлекались капиталовложения путем выпуска акций.

8 В 2023 году экосистема стартапов Абу-Даби признана самой быстро развивающейся в регионе MENA и 6-е в ире, в период с 1 июля 2020 года по 31 декабря 2022 года ее стоимость выросла на 134%. Наиболее значимые инициативы эмирата программа Gadan 21 и Университет искусственного интеллекта Мохаммеда бен Зайда (MBZUAI). Сообщество стартапов Hub71 расширилось до более чем 200 компаний, которые в совокупности собрали более 1 млрд долл. инвестиций. По состоянию на февраль 2023 года в Абу-Даби насчитывалось 79 финтех-стартапов, в тм числе в сфере мусульманского банкинга. Источник: Abu Dhabi startup ecosystem fastest growing in MENA region and 6th fastest globally, 20 June 2023, https://www.mediaoffice.abudhabi/en/technology/abu-dhabi-startup-ecosystem-fastest-growing-in-mena-region-and-6th-fastest-globally/

9 Одним из примеров инновационных инициатив в эмирате Дубай является DIFC Innovation Hub — сообщество более чем 700 технологических фирм, находящихся на стадии роста, устоявшихся инновационных компаний, цифровых лабораторий, фирм венчурного капитала, регулирующих органов и образовательных организаций. Это самый крупный акселератор финансовых технологий в регионе Ближнего Востока, Африки и Южной Азии.

10 Group 42 — конгломерат, включающий девять операционных компаний, центры обработки данных, облачные сервисы и исследовательский институт, который ориентирован на развитие технологий ИИ, облачных вычислений и обработку Больших данных, в том числе для геопространственной разведки, которую осуществляет с американскими партнерами. Основан в Абу-Даби в 2018 году, располагает самыми мощными суперкомпьютерами в стране. Group 42 возглавляет кровный брат наследного принца Абу-Даби шейх Тахнун бен Зайд аль-Нахайян – советник по национальной безопасности ОАЭ. Он также руководит First Abu Dhabi Bank, крупнейшим кредитором ОАЭ, возглавляет инвестиционную компанию ADQ и председательствует в конгломератах International Holding Company и Royal Group.

по производительности) и POD3 (304 место). В 2023 году Group 42 запустила в Калифорнии с помощью американской Cerebras свой первый специализированный и самый мощный в мире для обучения и развертывания моделей ИИ суперкомпьютер Condor Galaxy. Согласно контракту в 2024 году будут запущены еще 2 узла, ведутся переговоры о сети из 9 вычислителей общей производительностью 36 эксафлопс. Свободные мощности будут предоставляться оптом клиентам из сообщества искусственного интеллекта с открытым исходным кодом, но преимущественно в экосистеме США [10]. Это даст огромный толчок развитию систем ИИ в государственном секторе, здравоохранении, финансах, нефтегазовой отрасли, авиации и гостиничном бизнесе.

Передовые технологии эффективно внедряются в повседневную жизнь, прежде всего, через реализацию федеральной программы «Умных устойчивых городов»[11] и планов отдельных эмиратов (например, Abu Dhabi Economic Plan 2030 и Smart City Dubai 2021). Они нацелены на создание комфортной и безопасной среды, использование возобновляемых источников энергии, рациональное использование электричества и воды, полную переработку отходов. Кроме того, развиваются аспекты «умной» экономики (инновационных компаний и технопарков, портовых услуг, умных фондовых бирж и рабочих мест) и «умной» жизни (здравоохранение, образование, транспорт, коммуникации, туризм). Лидерами являются крупные города: Абу-Даби третий год подряд занимает первое место в регионе Ближнего Востока и Северной Африки и 13 — в мире, Дубай поднялся на 17 место в глобальном рейтинге[12]. Проекты «умных» городов внедряются также в Масдаре, Зайде, Шардже, Дезерт Роуз Сити.

Благодаря этому активно развивается национальная цифровая экономика. По данным на апрель 2022 года она обеспечивала 9,7% ВВП страны. Согласно Стратегии цифровой экономики ОАЭ, этот показатель к 2031 году должен превысить 20%, а общий объем достичь 140 млрд долл. США (в настоящее время 38 млрд.). Локомотивом развития станет эмират Дубай, который разработал собственную стратегию и создал надзорный комитет по ее реализации. Краткосрочные амбиции Дубая включают привлечение к себе более 300 новых цифровых компаний к концу 2024 года, создание за шесть лет более 20 компаний-единоро-

11 Умный город — инновационный город, который использует ИКТ и другие средства для улучшения качества жизни, эффективности функционирования городской инфраструктуры и услуг, а также конкурентоспособности, обеспечивая при этом удовлетворение потребностей нынешнего и будущих поколений в отношении экономических, социальных и экологических аспектов.

12 IMD Smart City Index report 2023, составленный Институтом развития менеджмента (IMD) в сотрудничестве с Сингапурским университетом технологий и дизайна (SUTD) на основе оценок жителей интеллектуальной инфраструктуры и услуг, охватывающих здоровье и безопасность, мобильность, деятельность, возможности и управление. Абу-Даби поднялся на 13 место, а Дубай на 14. Источник: Abu Dhabi named smartest city in Mena region, 13th globally; Dubai ranked 17th // Khaleej Times May, 1, 2023, https://www.khaleejtimes.com/uae/abu-dhabi-named-smartest-city-in-mena-region-13th-globally-dubai-ranked-17th

гов и цифровой экономики стоимостью более 100 млрд долл. США (для сравнения, в 2022 году ВВП государства составил 508 млрд).

Один из сегментов цифровой экономики ОАЭ — электронная коммерция. В 2023 году она оценивалась более чем в 9,5 млрд долл. США и, по прогнозам, вырастет до 11,7 млрд к 2025 году. Государственные программы поощряют совершенствование систем логистики и доставки, повышения доверия к электронным платежам[13] и безопасности транзакций. Лидерами в сфере электронной коммерции являются местные компании такие, как Amazon UAE, Noon и Namshi [11], на долю которых в совокупности приходится значительная часть розничных онлайн-продаж.

Но безусловным лидером цифровой экономики является государственный сектор. Уровень развития электронного правительства в ОАЭ — один из самых высоких в мире (13 место) [12]. По состоянию на апрель 2023 года более 1500 федеральных государственных услуг были предоставлены с помощью более 180 интеллектуальных платформ и приложений, а актуальная информация по целому ряду тем была доступна на 500 правительственных веб-сайтах. Кроме того, существует более 280 центров государственных услуг, предлагающих ресурсы и помощь.

В стране используется система цифровой идентификации по биометрии граждан, резидентов и приезжих — UAE PASS, которая применяется для безопасного доступа к государственным и коммерческим сервисам, а также для взаимодействия всех государственных служб и министерств.

Важным техническим элементом электронного правительства является федеральная сеть для доступа населения к госуслугам и обмена данными между правительственными ведомствами FedNet. Она представляет собой защищенную инфраструктуру связи государственных структур и облачную среду, масштабируемую по требованию и имеющую обширные вычислительные мощности и репозитории данных. Централизованный хостинг обеспечивает доступ к мобильным госуслугам и приложениям 24/7.

Очень высокий уровень цифровизации и концентрации капитала приводит к значительным рискам информационной безопасности и делает страну привлекательной мишенью для компьютерных атак, особенно к программам-вымогателям (более половины киберинцидентов), вирусам-шифровальщикам, многовекторным атакам по типу «отказ в обслуживании», фишингу и компрометации деловой электронной почты. Во время пандемии количество кибератак увеличилось более чем на 250%. Сейчас ОАЭ занимают второе место в мире по затратам, связанным с утечкой данных, что отражает экономические цели участников ки-

13 По данным PPRO, самым популярным способом онлайн-оплаты в ОАЭ в 2023 году были карты (около 48%).

беругроз на фоне процветания стран Персидского залива. Кроме того, отмечается значительный уровень политически и экономически мотивированных трансграничных компьютерных атак на государственный, банковский и коммерческий сектор, спонсируемых другими государствами. В начале 2023 года ежедневное количество атак достигло 50 тыс. [13] Согласно Отчету о состоянии кибербезопасности, выпущенному в 2024 году Советом кибербезопасности ОАЭ и национальным поставщиком решений в сфере кибербезопасности CPX Holding, на территории страны выявлено более 155 тыс. уязвимых активов, при этом более 40% критических уязвимостей оставались без внимания более пяти лет [14].

По оценке Всемирного экономического форума, риск сбоев в сфере кибербезопасности входит в пятерку основных угроз для ОАЭ. Защита от них становится для страны стратегически важной задачей. Основными направлениями обеспечения кибербезопасности являются: защита информационной инфраструктуры и сети Интернет, объединение усилий между государством, научной сферой и бизнесом для обеспечения кибербезопасности, разработка инновационных решений в этой сфере. Системная работа дает свои результаты: МСЭ в Глобальном индексе кибербезопасности 2020 поставил ОАЭ на пятое место (одинаковое значение индекса с Россией и Малайзией), хотя еще в 2018 году страна была на 33 позиции.

Введение жесткого государственного регулирования киберсферы стимулирует быстрое развитие сегмента решений информационной безопасности. Его объем в 2024 году оценивается в 590 млн долл. США, но уже к 2029 году он практически удвоится и составит 1,07 млрд долл. [15]. При этом важно отметить, что местные потребители стремятся к сервис-ориентированной модели и предпочитают передавать операции по обеспечению безопасности на аутсорсинг.

В связи с этим основными игроками в этом сегменте являются крупные американские компании (IBM, Cisco Systems, Juniper Networks, Oracle Corporation, Palo Alto Networks, Amazon), которые за счет партнерских соглашений расширяют свои предложения и получают устойчивое конкурентное преимущество [16]. Также на этом рынке присутствуют компании из Великобритании, КНР, Израиля и России. Даже Совет кибербезопасности ОАЭ опирается на экспертную поддержку мировых поставщиков, в 2022 году он заключил Меморандумы о взаимопонимании с Huawei, Amazon Web Services и Deloitte. Первый создаст независимый аналитический центр и центр передового опыта в области кибербезопасности для продвижения инноваций и исследований, окажет содействие в разработке стратегий кибербезопасности и укрепит взаимодействие в рамках государственно-частного партнерства, создаст новые возможности для развития местных талантов в области цифровой безопасности. Второй внедрит облачные сервисы для госучреждений, финансовых услуг и

здравоохранения, создаст руководящий комитет для обмена передовым опытом в области облачной безопасности. Deloitte обеспечит консалтинг и обучение в сфере кибербезопасности.

На данный момент наиболее сложной и долгосрочной задачей является подготовка национальных кадров в сфере ИКТ и информационной безопасности — местные компании и государственный сектор испытывают острый дефицит специалистов[14]. Проблема решается по двум направлениям. Прежде всего, реализуется широкий комплекс мер для привлечения, развития и удержания ведущих технических специалистов и для притока зарубежных инновационных компаний (100 тыс. «золотых» виз для переезда в Эмираты программистам и экспертам по передовым технологиям, меры господдержки — нулевой налог в особых экономических зонах, 100% владение иностранными инвесторами и другие экономические стимулы, содействие переезду в страну талантливых студентов[15] и предоставление им работы).

Параллельно в рамках реализации Национальной стратегии высшего образования ОАЭ на 2030 год реализуются программы популяризации инженерных специальностей и STEM образования[16], субсидируются выявление и обучение талантливой молодежи[17], стимулируется получение гражданами Эмиратов образования в мировых университетах[18]. Расширяется и укрепляется система ВУЗов[19]

---

14 Исследования показывают, что за последние два года в ИКТ-отрасли ОАЭ наблюдался 61% рост числа сотрудников, связанных с технологиями. В стране насчитываются десятки сотен ИТ-компаний с растущим спросом на облачных и сетевых архитекторов, инженеров для оптимизации и автоматизации процессов создания, развертывания программных приложений (DevOps), большим спросом пользуются менеджеры проектов и инженеры-программисты, что связано с разрастанием экосистемы ИТ-стартапов и притоком в страну штаб-квартир крупных технологических корпораций. Очень высоко ценятся специалисты в сфере ИИ, например, инженер по машинному обучению, инженеры и специалисты по интеллектуальной обработке данных, бизнес-аналитики и специалисты по кибербезопасности. Источник: Top 10 in-demand tech jobs in UAE https://theuaeblog.com/uae/top-10-in-demand-tech-jobs-in-uae/

15 ОАЭ являются лидером по приему индийских студентов: по данным на июль 2021 года в эмиратские ВУЗы были зачислены 219 тыс. индийских студентов, больше чем в Канаде, США, Великобритании и других странах.

16 STEM — практико-ориентированная система образования, включающая науку, технологии, инженерию и математику.

17 Предлагаются различные стипендии, например, Космический центр имени Мохаммеда бен Рашида (MBRSC) предлагает стипендии лучшим эмиратским студентам, изучающим инженерные или естественные науки, для изучающих телекоммуникации и информационные технологии (компьютерную инженерию, электронную инженерию и информатику) возможно получение стипендии BETHA.

18 За счет средств Фонда ИКТ ОАЭ, Министерства образования, Министерства по делам президента, Департамента образования и знаний и Министерства финансов ежегодно за границу отправляют около 15 тыс. студентов, большинство из которых обучаются на уровне бакалавриата. Основными направлениями являются Великобритания (6015 в 2019/20 году), Индия (2307 в 2019 году) и США (1737 в 2020/21 году). Канада и европейские страны также становятся все более популярными. Стипендиальная программа Khotwa (RizeUp) с финансированием в 520 млн долл. США оплачивает все программы обучения студентов, включая проживание в семье и до года изучения английского языка.

19 В Министерстве образования зарегистрирован уже 31 университет, некоторые из них специализируются на ИКТ (Университет Шарджа — 201 место в глобальном TOP500), математических науках (Университет ОАЭ — 351 место в глобальном TOP500), Халифский университет науки и технологий входит в TOP200 университетов QS world с интенсивным исследовательским фокусом на прикладных науках и инженерии.

и увеличивается присутствие иностранных образовательных учреждений[20]. Запущены различные программы по подготовке местных кадров, в том числе Национальная программа для программистов CodersHQ, «Миллион арабских программистов» и другие. Цель ОАЭ — достичь на душу населения максимального количества таких специалистов. Национальной стратегией кибербезопасности планировалось подготовить более 40 тыс. местных экспертов по кибербезопасности, вводилась программа поощрений академических исследований, стартапов и компаний, внедряющих меры защиты.

При наличии мощной экосистемы власти ОАЭ намерены активно внедрять передовые технологии в государственные и бизнес-процессы с целью стимулирования экономического роста и извлечения выгоды из своей развитой цифровой инфраструктуры, предоставляя ее возможности и услуги другим странам.

2. О стратегическом планировании в области цифровизации и обеспечения информационной безопасности

Четкий курс на диверсификацию экономики и цифровизацию страны наглядно отражается в документах стратегического планирования, принятых руководством ОАЭ в последние годы. Глубина планирования свидетельствует о безусловной уверенности руководства страны в достижимости цели превращения Эмиратов в глобального лидера нового технологического уклада, ключевым элементом которого является обеспечение безопасности информации и цифровых активов. Комплексность подхода выражена в большом количестве общих и дополняющих их планов, касающихся различных передовых технологий и отраслей экономики.

2.1. Перспективный план «Видение ОАЭ на 2030 год» (2016–2030)

«Видение ОАЭ на 2030 год» — амбициозная дорожная карта действий, направленных на то, чтобы сделать ОАЭ одной из самых конкурентоспособных и инновационных в мире, с государственной системой образования мирового уровня, процветающей экономикой и устойчивой окружающей средой. Этот тщательно продуманный план включает в себя ряд шагов, которые также призваны увеличить вклад частного сектора и способствовать росту малого и среднего бизнеса. Видение также предусматривает создание особых экономических зон для привлечения прямых иностранных инвестиций и поддержки диверсификации экономики путем содействия росту развивающихся отраслей, таких как высокие

20 В ОАЭ 26 международных филиалов университетов из 12 разных стран, в том числе Великобритании, США, Австралии, Канады.

технологии и возобновляемые источники энергии. В этих зонах инвесторам предоставят налоговые льготы и упрощенные правила ведения бизнеса.

2.2. Стратегия четвертой промышленной революции ОАЭ (2017)

Стратегия направлена на укрепление позиций ОАЭ как глобального центра нового производственного уклада, открытой лаборатории для приложений Четвертой промышленной революции (4IR). Фактически, ОАЭ объединили усилия со Всемирным экономическим форумом для создания первого постоянного политического подразделения для изучения и реализации мер, касающихся трансформации бизнеса и общества, вызванных технологическим прогрессом.

Реализация стратегии должна обеспечить увеличение вклада 4IR в национальную экономику посредством продвижения инноваций и технологий будущего по шести направлениям:

Человек. Образование, передовая медицина.

Безопасность. Обеспечение водоснабжения и продовольствия с помощью биоинженерии и передовых технологий использования возобновляемых источников энергии, экономическая безопасность за счет внедрения цифровой экономики и технологий блокчейн в финансовые транзакции и обслуживание, оптимизация использования спутниковых данных при планировании городов будущего, развитие передовых оборонных отраслей промышленности за счет развития национальной промышленности в области робототехники и технологий автономных транспортных средств.

Опыт. Интеллектуальные государственные услуги, интеллектуальный потребительский опыт розничной торговли и гостиничного бизнеса, умные города.

Производительность. Открытое аддитивное производство, строительство с использованием трехмерной печати, интеллектуальные сети будущего, обеспечивающие децентрализованное производство энергии, устойчивое потребление и умное управление активами, интеллектуальные цепочки поставок для устойчивого повышения производительности.

Рубежи будущего. Коммерциализация космоса, когнитивное улучшение человека.

Основы будущего. Подготовка национального кадрового резерва и предпринимателей к 4IR, интегрированная безопасная цифровая среда данных, необходимые политики и нормативные акты, ценности и этика, Глобальный центр для продвижения конкурентоспособной национальной экономики, основанной на знаниях, инновациях, технологиях и приложениях 4IR [17].

2.3. **Десятилетний перспективный план развития** (2021–2030)

Этот план развития производственного сектора страны, разработанный Министерством экономического развития, конкретизирует «Видение ОАЭ на 2030 год» и включает несколько инициатив [18]. Одна из них — «Operation 300bn» по увеличению вклада промышленного сектора в ВВП страны до 300 млрд дирхамов (82 млрд долл. США), на данный момент этот показатель составляет 133 млрд дирхамов. План предусматривает создание 13,5 тыс. современных промышленных предприятий и качественно новых рабочих мест. Инвестиции в НИОКР к 2031 году будут увеличены в 2,7 раза (с 21 до 57 млрд дирхамов). Благодаря реализации инициативы планируется ускорить цифровую трансформацию производства, превратить ОАЭ в мировой промышленный центр и улучшить положение страны в Глобальном индексе конкурентоспособности. Основная ставка в 4IR делается на передовые технологии: связь 5G, робототехнику, искусственный интеллект, цифровые двойники, Большие данные и блокчейн, зеленую и «умную» энергетику.

Другая инициатива «Производите в Эмиратах» (Make It In The Emirates) будет формировать условия для ведения бизнеса и инвестиций на территории ОАЭ, создаст новые рабочие места, поддержит отечественное производство и будет продвигать местные продукты во всем мире. Для обновления промышленной экосистемы будут осуществлены действия по модернизации национального законодательства, сокращены бюрократические процедуры, повышена квалификация местных кадров.

2.4. **План столетия ОАЭ до 2071 года** (2021)

Эта стратегия социально-экономического развития Эмиратов принята в 2021 году для превращения ОАЭ в лучшую страну мира к столетию государства в 2071 году. Она формирует четкую карту долгосрочной работы правительства, направленную на укрепление образа страны и ее «мягкой силы», инвестирование в будущие поколения для подготовки к освоению необходимых знаний.

План основан на четырех основных компонентах:

Правительство, ориентированное на будущее. Цели этого компонента включают признание оценки правительства ОАЭ как лучшего в мире, достижение счастья в обществе и распространение позитивных идей внутри страны и по всему миру, разработку механизмов мониторинга долгосрочных показателей в различных секторах.

Отличное образование. Этот компонент подчеркивает важность качества образования, включающего передовые науки и технологии, космическую науку,

инженерное дело, инновации и науки о здоровье. Другие образовательные меры включают обучение студентов механизмам раннего раскрытия их индивидуальных талантов. На институциональном уровне учебным заведениям рекомендуется быть инкубаторами предпринимательства и инноваций и международными исследовательскими центрами.

Диверсифицированная экономика знаний. Она должна быть конкурентоспособной и одной из лучших в мире. Этого можно достичь путем повышения производительности, поддержки национальных компаний, инвестиций в научные исследования и перспективные сектора, сосредоточения на инновациях, предпринимательстве и передовых отраслях промышленности, разработки национальной стратегии по формированию будущего экономики и промышленности, позиционирования ОАЭ среди ведущих мировых экономик.

Счастливое и сплоченное общество. Развитие сообщества является неотъемлемой частью «Плана столетия ОАЭ до 2071 года», включает создание безопасного, толерантного, сплоченного и этичного общества, которое ценит счастье, позитивный образ жизни и высокое качество жизни.

2.5. **Стратегия цифровой экономики ОАЭ** (2022)

Это документ долгосрочного планирования, рассчитанный на десять лет. Основными целями стратегии является развитие цифровой экономики, двукратное увеличение к 2030 году ее вклада в ВВП страны (с 9,7% до 19,4%), укрепление позиций ОАЭ как центра цифровой экономики в регионе и во всем мире. Документ включает в себя более 30 инициатив и программ, нацеленных на 6 секторов[21] и 5 новых областей роста. В частности, планируется привлекать 3 тыс. программистов ежемесячно и 100 тыс. программистов в течение года, чтобы расширить возможности рабочей силы цифровой экономики ОАЭ.

Для консолидации действий правительства и межведомственной координации на федеральном уровне создан Совет по цифровой экономике, который возглавляет шейх Омар Аль Олама[22] — государственный министр по искусственному интеллекту, цифровой экономике и приложениям для удаленной работы.

21 Умный, удобный для жизни и устойчивый цифровой город. Бережливое правительство. Конкурентоспособная на глобальном уровне экономика, основанная на прорывных технологиях. Взаимосвязанное общество с легкодоступными социальными услугами. Бесперебойный транспорт, обеспечиваемый автономными и совместными мобильными решениями. Чистая окружающая среда с помощью передовых инноваций в области ИКТ.

22 Во время работы в Департаменте будущего Министерства по делам кабинета министров ОАЭ он участвовал в разработке Стратегии Столетия ОАЭ на 2071 год, Стратегии четвертой промышленной революции в ОАЭ, национальной Стратегии искусственного интеллекта. В 2021 году Омар Аль Олама был назначен председателем Дубайской палаты цифровой экономики, в 2022 — заместителем председателя Высшего комитета по цифровой трансформации правительства, в 2023 году во время перестановок в кабинете министров назначен генеральным директором канцелярии премьер-министра, одновременно сохранив за собой должность государственного министра по искусственному интеллекту, цифровой экономике и приложениям для удаленной работы.

Созданием такой должности ОАЭ продемонстрировали уникальный пример поддержки государством развития и внедрения технологий ИИ.

2.6. **Национальная стратегия блокчейн** (2021)

Документ UAE Blockchain Strategy конкретизирует Национальную стратегию по инновациям в части развития «умных» городов, за счет внедрения в производство и управление комплекса передовых технологий, включая ИИ, микроэлектронику (нанотехнологии и полупроводники), трехмерную печать, а также необходимое программное обеспечение. Следует отметить, что в марте 2018 года была определена Регуляторная политика в отношении технологий Интернета вещей (IoT), которая ввела требования к оборудованию, используемому для создания локальных радиосетей для IoT, к сервис-провайдерам услуг на основе IoT, к лицензиатам, а также определила процедуры проверки соответствия указанным требованиям [19].

Флагманом внедрения технологий блокчейн является эмират Дубай, который еще в 2016 году начал реализовывать собственную стратегию в этой сфере. Это стало важным фактором, способствующим развитию правительства Дубая, которому удалось оцифровать 100% из более чем 10 тыс. видов внутренних и внешних транзакций и стать в 2021 году на 100% безбумажным правительством. Кроме того, запущено предложение «блокчейн как услуга» (BaaS), позволяющее всем организациям быстрее внедрять эту технологию в своих проектах без необходимости привлечения специалистов по блокчейну. В 2016 году правительство Дубая учредило Глобальный совет по блокчейну, в который входят 32 государственные структуры и некоторые из крупнейших мировых технологических гигантов, таких как Microsoft, SAP и Cisco.

2.7. **Национальная стратегия развития искусственного интеллекта до 2031 года** (2022)

Этот документ конкретизирует принятую в 2014 году Стратегию по инновациям ОАЭ в части развития ИИ, как ключевой технологии четвертой промышленной революции. Правительство страны ставит глобальную задачу — сделать Эмираты лидером в области технологий ИИ к 2031 году, а также разработать и внедрить интегрированную систему их использования во всех жизненно важных областях экономики: возобновляемые источники энергии, водоснабжение, технологии, образование, окружающая среда и дорожное движение.

Стратегия включает восемь глобальных целей и ряд инициатив для их достижения: укрепить позиции ОАЭ как мирового лидера в области технологий ИИ;

повысить конкурентоспособность сектора ИИ; организовать инновационный инкубатор для внедрения технологий ИИ; использовать ИИ-технологии в сфере обслуживания клиентов; подготовить перспективных специалистов для работы в этом направлении; привлечь зарубежные исследовательские группы для разработки и внедрения инноваций в области ИИ; создать возможность проведения масштабных практических экспериментов с использованием ИИ и их быстрого внедрения в реальный сектор экономики; оптимизировать управление проектами и регулирование с использованием технологий ИИ.

На первом этапе реализации Стратегии усилия будут сосредоточены на энергетике и добыче полезных ископаемых, космосе, транспорте и авиации, логистике, туризме, здравоохранении и безопасности. Ожидается, что благодаря этому к 2030 году ИИ будет играть важную роль в обеспечении почти 14% национального ВВП (96 млрд долл), а ежегодный рост вклада ИИ в экономику ОАЭ вырастет на 33,5% в период с 2018 по 2030 год [20].

Головным ведомством, отвечающим за реализацию стратегии, является Офис по искусственному интеллекту в аппарате премьер-министра, ему подчиняется лаборатория AI Lab, оснащенная суперкомпьютером, мощности которого доступны всем государственным учреждениям, национальным исследователям и инновационным компаниям для разработки новых цифровых продуктов и услуг.

2.8. Национальная стратегия электронного правительства ОАЭ до 2025 года (2023)

Стратегия UAE Digital Government Strategy 2025 направлена на ускорение внедрения цифровых государственных услуг, в реализации которых выявлены пробелы в период пандемии Covid-19. Ее основные принципы:

Инклюзивность. Открытые и инклюзивные процессы, доступность, прозрачность и подотчетность, преодоление любого цифрового разрыва, который может возникнуть у социально уязвимых групп пользователей, особенно пожилых и детей.

Устойчивость. Применение новейших технологий для создания потенциала в области предупреждения стихийных бедствий и кризисов.

Соответствие цифровому веку. Содействие межсекторальной и межведомственной координации и сотрудничеству, вовлечение всех заинтересованных сторон в реализацию цифровой повестки.

Человеко-ориентированность. Учет потребностей и удобство при формировании процессов, услуг и политики, внедрение инклюзивных механизмов.

Цифровизация по замыслу. Все политические процессы должны быть основаны на цифровых технологиях в качестве обязательного элемента управления.

Базирование на данных. Информация как ключевой стратегический актив для создания общественной ценности, при планировании, реализации и мониторинге государственной политики, применение этических принципов для их надежного и безопасного повторного использования.

«Открыто по умолчанию». Обеспечение доступности государственных данных и процессов разработки политики (включая алгоритмы) для общественности.

Проактивность. Способность правительства и государственных служащих предвидеть потребности людей и реагировать на них достаточно быстро.

Контроль реализации Стратегии возложен на Национальный комитет цифровой трансформации.

Развитие цифровой экономики и эффективного электронного правительства невозможны без выработки единой политики использования данных. В документе **Руководящие принципы политики в области открытых государственных данных** определены следующие принципы:

- повышение прозрачности и подотчетности путем предоставления гражданам и предприятиям доступа к правительственным данным;
- стимулирование инноваций путем предоставления государственных данных в распоряжение общественности, предпринимателей и разработчиков;
- содействие сотрудничеству путем предоставления общей платформы для обмена данными и доступа к ним;
- повышение эффективности за счет сокращения времени и ресурсов, необходимых для сбора и анализа данных, а также обеспечения обмена данными между государственными структурами и их повторного использования.

2.9. **Национальная стратегия кибербезопасности ОАЭ** (2019)

Стратегия National Cyber Security Strategy принята в 2019 году. Она основана на 5 основных принципах и включает 60 инициатив, направленных на мобилизацию всей экосистемы кибербезопасности в ОАЭ. Принципы обеспечения кибербезопасности включают:

- внедрение комплексной нормативно-правовой базы, необходимой для противодействия киберпреступности, обеспечения информационной безопасности существующих и новых технологий от компьютерных атак и содействующей малому и среднему бизнесу в обеспечении информационной безопасности;
- мобилизация экосистемы кибербезопасности страны путем развития рынка кибербезопасности (согласно оценкам, около 500 млн долл. США),

расширения возможностей более 40 тыс. экспертов в области кибербезопасности, поощрения образовательных мероприятий и продвижения карьеры в данной сфере, повышения осведомленности, а также поощрения достижений в области информационной безопасности с помощью национальных программ;

- разработка Национального плана реагирования на компьютерные инциденты;
- защита важнейших активов ОАЭ в таких секторах, как энергетика, ИКТ, правительство, электро- и водоснабжение, финансы и страхование, экстренные службы, медицина, транспорт, продовольствие и сельское хозяйство;
- развитие местных и глобальных партнерств для совместного достижения целей кибербезопасности, наращивания потенциала государственно-частного партнерства.

Инициативы по обеспечению кибербезопасности: развитие малого и среднего бизнеса в указанной сфере; поддержка инновационных проектов и НИОКР; стандартизация методик и планов по обеспечению кибербезопасности; развитие систем активного мониторинга кибербезопасности и др.

Головным уполномоченным органом по реализации Стратегии был определен Регулирующий орган по телекоммуникациям (TRA, позднее переименован в TDRA). Он мобилизует всю экосистему кибербезопасности для реализации инициатив по пяти стратегическим направлениям: разработка всеобъемлющей правовой и нормативной базы; укрепление динамичной экосистемы, в том числе разработка Национального плана реагирования на компьютерные инциденты; защита критически важных активов ОАЭ в ключевых секторах; развитие местных и международных партнерских связей. Общий объем финансирования реализации программ обеспечения кибербезопасности ОАЭ на 2022-2026 годы составляет 290 млрд дирхамов (79 млн долл. США) и является крупнейшим за всю историю страны [21].

По данным Индекса национальной информационной безопасности, рассчитываемый Академией электронного управления в Эстонии, уровень реализации Стратегии низкий — 14% [22], в частности, не завершена подготовка Плана реагирования на компьютерные инциденты[23], но разработана Национальная политика обмена информацией о компьютерных инцидентах[24].

---

23 При разработке Плана должны быть решены задачи оптимизации идентификации инцидентов кибербезопасности и отчетности о них, создания потенциала для устойчивости ко всем видам киберинцидентов. Они могут быть достигнуты с помощью четырех ключевых инициатив: постановки единой цели, подготовки рекомендаций по защите от угроз, активном контроле киберугроз и задействовании возможностей национальных спецслужб.

24 National Cyber Information Sharing Policy

2.10. Политика в области защиты критической информационной инфраструктуры (2021)

Документ Critical Information Infrastructure Policy [23] разработан Советом кибербезопасности ОАЭ. Он конкретизирует положения Национальной стратегии кибербезопасности и обязательных для всех государственных организаций Стандартов обеспечения информационной безопасности в отношении обеспечения безопасности и киберустойчивости национальной критической информационной инфраструктуры (КИИ). К такой категории относятся наиболее важные объекты информатизации в девяти секторах: энергетика, ИКТ, правительство, электро- и водоснабжение, финансы и страхование, экстренные службы, услуги здравоохранения, транспорт, продовольствие и сельское хозяйство. В соответствии с мировой практикой документ определяет последовательный и цикличный подход собственников КИИ к выявлению и оценке рисков для отрасли и национальной безопасности, разработке планов по их минимизации и управлению, постоянному мониторингу выполнения планов, их пересмотр с учетом выявленных недостатков и развития оперативной обстановки в киберпространстве.

3. Состояние нормативной базы в сфере цифровизации и обеспечения национальной информационной безопасности

Правовое регулирование ОАЭ по новой методике МСЭ[25] оценено как развитое и почти достигшее передового уровня зрелости. По этому показателю в БРИКС Эмираты уступают только Индии и Саудовской Аравии, а в мире занимают 26 место. Правовая база в сфере цифровизации и обеспечения национальной информационной безопасности включает несколько законов федерального уровня.

3.1. Конституция Объединенных Арабских Эмиратов (1971)

Конституция страны утверждена Федеральным законом №1 от 1971 года, поправки внесены в 1996 и 2024 годах.

Статья 30. Признается свобода мнения и его высказывания в устной и письменной форме. Также в рамках закона возможны прочие формы выражения мнения.

25 По методике оценки G5 Benchmark ОАЭ получила 77,16 баллов, что соответствует группе развитых правовых систем (индекс от 60 до 80 баллов). Источник: ITU Benchmark for Fifth Generation Digital Collaborative Regulation/ https://app.gen5.digital/benchmark/about

Статья 31. Конституция признает свободу почтовой переписки, передачи телеграфных сообщений и прочих средств связи.

3.2. Федеральный закон «О регулировании телекоммуникаций» (2003)

Федеральный закон №3 «О регулировании телекоммуникаций» с более поздними поправками включает в себя несколько имплементационных нормативных актов/политик, принятых Регулирующим органом по телекоммуникациям и цифровым технологиям (TDRA), в отношении защиты данных потребителей телекоммуникационных услуг в ОАЭ.

3.3. Федеральный закон «О защите персональных данных» (2021)

Закон (Personal Data Protection Law, PDPL), утвержденный Федеральным указом №45 от 2021 года, устанавливает требования к протоколам безопасности и конфиденциальности данных. Он применяется к компаниям, которые обрабатывают персональные данные (ПД) граждан ОАЭ и резидентов внутри страны или за ее пределами. Ключевые статьи охватывают такие вопросы, как ограничения на хранение ПД, прозрачность способов их обработки, утечки и их потенциальное влияние на частную жизнь личности, а также расширение прав граждан, связанных как с безопасностью ПД и их удалением. Установлены более строгие правила в отношении трансграничной передачи ПД и участия третьих сторон. Закон применяется к обработке ПД людей, проживающих в ОАЭ, или ведущих бизнес на территории страны; к каждому обработчику ПД внутри ОАЭ, независимо от того, принадлежат ли данные физическим лицам внутри или за пределами ОАЭ; к каждому обработчику, расположенному за пределами страны, который осуществляет деятельность по обработке ПД субъектов, находящихся на территории Эмиратов.

Под действие положений PDPL не подпадают организации, которые обрабатывают небольшие объемы ПД; а также данные, относящиеся к государственным структурам, личному здоровью, личной банковской и кредитной информации или свободным экономическим зонам, поскольку по этим вопросам существует отдельное законодательство.

PDPL сохраняет в неизменном виде действующие законы о защите данных и конфиденциальности в границах зон, свободных от финансовых операций ОАЭ, DIFC и ADGM[26], а также правила Dubai Health Care City, применимые местные законы, регулирующие медицинские, банковские и кредитные данные.

---

26 DIFC и ADGM — Международный финансовый центр Дубая и Международный финансовый центр Абу-Даби.

Исполнительный регламент PDPL соответствует положениям местных, региональных и международных компаний, полагающихся на ПД и их трансграничные потоки. Определяет требования в отношении передачи ПД за пределы ОАЭ, а также требования по обеспечению их безопасности и уведомлению регулятора по защите данных, а при некоторых обстоятельствах и субъектов данных, об утечках данных.

3.4. Федеральный закон «Об электронных транзакциях и трастовых услугах» (2021)

Данный закон [24], утвержденный Федеральным указом №46 от 2021 года, существенно обновил положения Федерального закона №1 «Об электронной торговле и транзакциях» (2006) в отношении получения и использования простой и усиленной цифровой подписи и цифровых сертификатов, а также требований к сервисам по их выдаче. Он направлен на повышение юридической уверенности в электронных транзакциях путем предоставления трастовых услуг[27]; усовершенствование процессов лицензирования на основе новых сервисов, поддерживающих цифровые транзакции и защищающих права клиентов; поощрение цифровой трансформации путем предоставления цифровых услуг и инвестиций; ускорение перехода ОАЭ к цифровой экономике.

Закон также устанавливает штрафы за нарушения со стороны удостоверяющих центров и незаконное раскрытие конфиденциальной информации.

Регулирующий орган по телекоммуникациям и цифровым технологиям ОАЭ (TDRA) регулирует услуги удостоверяющих центров, выдает им лицензии и в координации с заинтересованными организациями определяет правила, процедуры и стандарты, относящиеся к системам электронной идентификации, процедурам верификации и цифровому удостоверению личности. Федеральное управление по вопросам идентификации личности, гражданства, таможенной и портовой безопасности (ICP) уполномочено осуществлять контроль деятельности удостоверяющих центров, предоставляющих услуги государственному сектору.

3.5. Законодательство в сфере борьбы с киберпреступностью (2006, 2012, 2016, 2024)

Первым нормативным актом в рассматриваемой сфере стал **Федеральный закон о предотвращении преступлений в области информационных технологий №2 от 2006 года**. Он криминализировал любые преднамеренные действия,

27 Под этим термином в законе понимаются услуги удостоверяющих центров.

совершенные с целью получения доступа к веб-сайту или информационной системе путем нарушения мер безопасности, а также использование сети Интернет для демонстрации презрения к религиозным идеям и символам [25].

Его положения были существенно дополнены **Федеральным законом №5 от 2012 года**, который кодифицировал злоупотребление и неправомерное использование электронной информации посредством таких действий, как взлом, кража личных данных и мошенничество, а также преступлений типа «вторжение в частную жизнь», в том числе путем использования социальных медиа. Нормы закона установили уголовную ответственность за указанные правонарушения, в том числе экстерриториальные. Так Статья 29 ввела уголовное наказание за покушение на национальную безопасность, а Статья 30 — потенциальное пожизненное заключение за пропаганду свержения правительства посредством онлайн-активности. Также закон усилил полномочия TDRA и наделил полицию правом создать специализированные подразделения для расследования компьютерных преступлений и выявления правонарушителей.

В связи с развитием ИКТ очередные дополнения были внесены **Федеральным законом №12 от 2016 года**, направленные на обеспечение национальной безопасности. В частности, закон криминализовал взлом, атаки, фальсификацию государственных информационных систем и данных, распространение ложной информации или информации, которая наносит ущерб интересам и безопасности ОАЭ; ввел уголовную ответственность за использование VPN-сервисов с целью совершения преступления или предотвращения его раскрытия[28]. Помимо этого определены нормы ответственности за фальсификацию электронных документов, медицинских данных, банковских счетов и конфиденциальных кодов, электронное попрошайничество, шантаж, вымогательство и др.

Ожидается, что в 2024 году изменения в законодательстве могут расширить состав правонарушений, адаптируясь к меняющейся тактике киберпреступников и более широкому спектру криминальных действий, которые не охватывались в предыдущих редакциях. Законопроект расширяет юрисдикцию ОАЭ за пределы национальных границ, демонстрируя приверженность страны борьбе с киберугрозами в международном масштабе. В частности, законопроект включает положения, предусматривающие двойное наказание иностранцев, совершивших киберпреступления в отношении объектов и субъектов на территории ОАЭ. Более того, зарубежным правонарушителям грозят не только санкции, предусмотренные законом, но и немедленная депортация. Статья 47 расширяет сферу правоприменения, устанавливая юрисдикцию в отношении преступлений, совершенных за пределами ОАЭ.

28 При этом любой, кто использует легальный VPN-сервис в законных целях, не будет привлечен к ответственности. Хотя термин «легальный» VPN-сервис законом не определен.

3.6. Федеральный закон «О борьбе со слухами и киберпреступностью» (2021)

Федеральный закон №34 от 2021 года «О борьбе со слухами и киберпреступностью» обеспечивает всеобъемлющую правовую основу для решения проблем, связанных с неправомерным использованием и злоупотреблением сетевыми технологиями. Прежде всего, он нацелен на защиту правительственных информационных ресурсов и баз данных ОАЭ, борьбу с распространением слухов и фейковых новостей, защиту от электронного мошенничества и сохранение конфиденциальности и личных прав. В законе перечислены правонарушения и наказания в отношении любого лица, которое может создавать или использовать веб-сайт или любые средства информационных технологий для взлома, атаки или подделки государственных информационных систем и данных, распространения ложной информации или информации, которая наносит ущерб интересам и безопасности ОАЭ [26].

Государственная прокуратура ОАЭ опубликовала в социальных сетях разъяснение мер наказания за создание поддельных электронных писем, веб-сайтов и онлайн-аккаунтов. Статьей 11 предусматривается, что любое лицо, осуществляющее указанные действия, выдавая себя за физическое или юридическое лицо, подлежит тюремному заключению и/или штрафу в размере от 50 тыс. до 200 тыс. дирхамов. Уточняется, что преступник должен быть заключен в тюрьму минимум на два года, если он использует или позволяет любому лицу использовать поддельный веб-сайт, онлайн-аккаунт или электронную почту для причинения вреда жертве. Если такими действиями преступник выдает себя за юридическое лицо ОАЭ, то применяется наказание в виде тюремного заключения на срок не более пяти лет и штрафа в размере от 200 тыс. до 2 млн дирхамов [27].

3.7. Регламент ОАЭ по обеспечению информационной безопасности (2020)

В связи с быстро растущими киберугрозами, Регулирующий орган по телекоммуникациям и цифровым технологиям (TDRA) опубликовал в марте 2020 года очень важный документ, который касается любого национального оператора информационных активов — «Регламент ОАЭ по обеспечению информационной безопасности» [28]. Он заменил действовавшие до него Стандарты информационной безопасности для государственных органов (Information Assurance (IA) Standards NESA)[29], соответствие которым распространялось на подрядчиков госсектора и КИИ.

29 Указанные стандарты описывают для проведения аудита безопасности 60 точек контроля управления безопасностью и 120 технических точек контроля, причем 136 из них с разным уровнем риска от 1 до 4 являются обязательными для проверки и еще 564 детализируют их.

Регламент определяет минимальные требования к безопасности, описывает систему информационной безопасности на национальном, отраслевом и организационном уровнях, реализует риск ориентированный подход, дает краткое описание ролей и обязанностей ключевых заинтересованных сторон в планировании, разработке, внедрении, постоянном мониторинге и совершенствовании информационной безопасности. Регламент предлагает каталог общих средств контроля информационной безопасности для защиты от распространенных угроз, использующих известные уязвимости в области кибербезопасности.

Документ определяет реализацию отраслевых требований за счет предоставления специализированных средств контроля для удовлетворения специфических для каждой отрасли требований к обеспечению достоверности информации. Предлагает поэтапный подход к внедрению требований для устранения наиболее распространенных угроз, содействия обеспечению информационной безопасности и оптимизации стоимости, получаемой за счет ее внедрения. Определяет средства межведомственной и межсекторальной коммуникации для поддержки обмена информацией и повышения осведомленности о ситуации на национальном уровне.

Помимо описанных выше законов существуют также некоторые отраслевые нормативные акты федерального уровня (в банковской и финансовой сферах, здравоохранении), а также законодательные нормы на уровне эмиратов.

4. Основные государственные органы, входящие в систему обеспечения информационной безопасности и форматы государственно-частного партнерства

ОАЭ — федерация конституционных монархий. Эта особенность государственного устройства накладывает отпечаток на структуру органов управления, в том числе в сфере обеспечения национальной информационной безопасности. Все руководящие должности занимают члены королевских семей, а постоянная борьба за власть между ними приводит к причудливому сочетанию функционалов государственных ведомств и совмещению должностей в различных структурах.

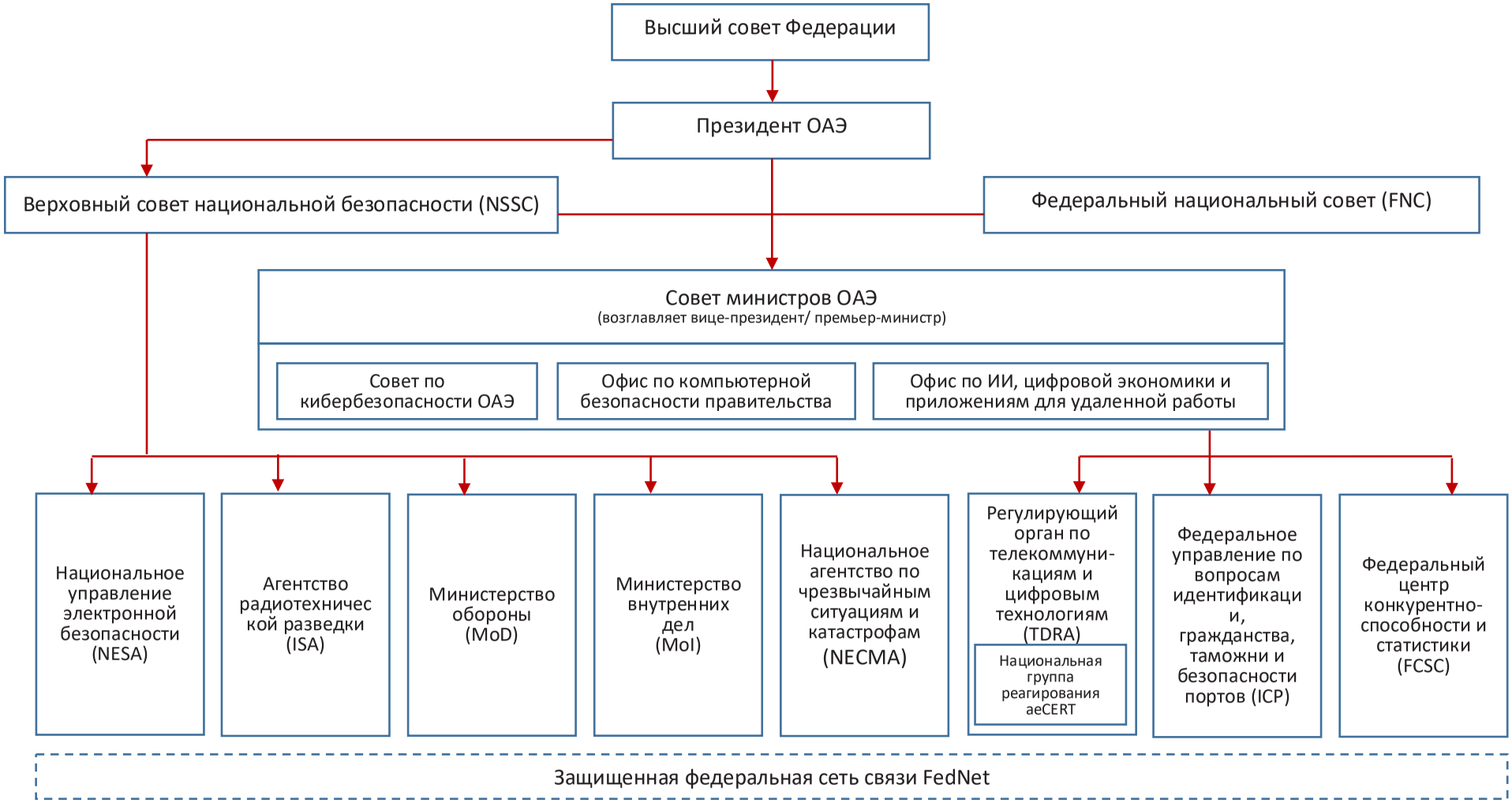
Согласно Конституции (Статья 45) к органам власти Федерации относятся:

Высший совет Федерации (эмиры всех 7 эмиратов);

Президент ОАЭ (эмир Абу-Даби шейх Мухамед бен Зайед) и вице-президент (эмир Дубая шейх Мохаммед ибн Рашид ибн Саид Аль Мактум);

Совет министров (его возглавляет в одном лице председатель Совета министров и вице-президент, в Совет входят 36 членов, включая трех государственных министров «без портфеля»);

Схема. Основные элементы управления системой национальной информационной безопасностью ОАЭ



Федеральный национальный совет — квази-парламент из 40 членов, выполняющих экспертизу законопроектов и консультационные функции;

Федеральная судебная система.

Президент ОАЭ возглавляет **Верховный совет национальной безопасности** (англ. National Supreme Security Council, NSSC). Должность его советника по национальной безопасности сейчас занимает кровный брат наследного принца Абу-Даби шейх Тахнун бен Зайд Аль-Нахайян. Он координирует всю разведывательную деятельность и наступательные операции, в том числе в космосе и киберпространстве. Одновременно возглавляет Национальный совет по искусственному интеллекту и собственный консорциум Group 42, занимающийся развитием и применением этих технологий. В январе 2024 года Аль-Нахайян назначен руководителям нового Совета по искусственному интеллекту и передовым технологиям (AIATC), который займется разработкой политик и стратегий для исследования технологий ИИ и привлечением необходимых инвестиций.

4.1. Аппарат Председателя Совета министров ОАЭ

Совет министров Федерации возглавляет вице-президент ОАЭ шейх Мохаммед Аль Мактум. В его аппарате созданы две структуры, имеющие прямое отношение к цифровизации и информационной безопасности.

Офис по искусственному интеллекту, цифровой экономике и приложениям для удаленной работы возглавляет государственный министр «без портфеля» шейх Омар Аль Олама. Этот офис с 2020 года играет решающую роль в формировании политики и законодательства, относящихся к указанным направлениям деятельности. Офис отвечает за достижение целей Национальной стратегии в области искусственного интеллекта и Стратегии цифровой экономики ОАЭ. В 2022 году Совет министров назначил Аль Оламу заместителем председателя Высшего комитета по цифровой трансформации правительства, который уполномочен координировать реализацию программы электронного правительства. Аль Олама также является управляющим директором Всемирного правительственного саммита, председателем Дубайской палаты цифровой экономики и Высшего комитета по технологиям будущего.

Офис кибербезопасности правительства ОАЭ обеспечивает контроль информационной безопасности правительственных структур. Возглавляет его шейх Мохаммед Аль Кувейти[30], который также является советником в области анализа и кибербезопасности ОАЭ и главой Национального совета по кибербезопасно-

30 Мохаммед Аль Кувейти имеет степень доктора философии в области компьютерной техники и сетевой безопасности, степень магистра в телекоммуникационных и компьютерных сетях, а также степень магистра в области международной и гражданской безопасности.

сти, исполнительным директором Агентства радиотехнической разведки (SIA), исполнительным директором Директората по развитию талантов Национального управления электронной безопасности (NESA).

4.2. Совет по кибербезопасности ОАЭ

Решением Кабинета министров ОАЭ от ноября 2020 года в его аппарате создан Совет по кибербезопасности ОАЭ (англ. Cyber Security Council, CSC), реальное осуществление функций осуществляется с 2021 года. Основная задача Совета — разработка всеобъемлющей стратегии кибербезопасности и создание в Эмиратах безопасной и мощной киберинфраструктуры. Совет, возглавляемый Аль Кувейти, отвечает за создание нормативно-правовой базы, охватывающей все виды киберпреступлений, обеспечение безопасности использования ИКТ и самих ИКТ, за координацию реагирования на федеральном уровне в случае масштабных компьютерных инцидентов. Также в его функции входит межведомственная координация программ подготовки необходимых кадров и повышения осведомленности об угрозах информационной безопасности и методах их снижения[31].

4.3. Национальное управление электронной безопасности

В 2014 году на основании Федерального законодательного декрета №3 от 2012 года было образовано Национальное управление электронной безопасности (англ. National Electronic Security Authority, NESA), уполномоченное на решение всего круга задач по защите национального киберпространства, в том числе в интересах разведки и обороны. Помощь в его создании оказали США в ответ на приписанные правительству Ирана факты кибершпионажа, выявленные в 2011 году. Функции NESA изначально были эквивалентны АНБ США, в том числе включали организацию защиты сетей связи и информационных систем ОАЭ и контроль электронных коммуникаций.

Как упоминалось выше, NESA были разработаны стандарты информационной безопасности для государственных органов (Information Assurance (IA) Standards NESA), требование соответствия которым наложено на их подрядчиков и КИИ, а в 2023 году — политика защиты критических информационных инфраструктур. В настоящее время ведомство проводит на национальном уровне оцен-

31 Одной из последних инициатив CSC, реализованной совместно с Федеральным агентством по развитию человеческих ресурсов и ведущими операторами связи, является программа Киберснайпер по повышению знаний и навыков 120 государственных специалистов в области кибербезопасности, поиску талантливых кадров для госсектора, повышения осведомленности об актуальных угрозах информационной безопасности. Первый ее этап осуществлен осенью 2023 года.

ку киберугроз, администрирует реализацию указанных выше стандартов и Регламента ОАЭ по обеспечению информационной безопасности. NESA подчиняется напрямую советнику по национальной безопасности.

4.4. Агентство радиотехнической разведки

В 2018 году после скандала, спровоцированного реализацией проекта Raven по электронной слежке за правительствами других стран, боевиками ИГИЛ и правозащитниками, функционал NESA был поделен между тремя ведомствами. Самым крупным из них стало Агентство радиотехнической разведки (англ. Signals Intelligence Agency, SIA), которое подчинено Верховному совету национальной безопасности. По некоторым данным, к агентству отошли наступательные кибероперации и компьютерная разведка[32], а за NESA остались функции выработки единой научно-технической политики в сфере информационной безопасности и контроль ее выполнения [29].

4.5. Регулирующий орган по телекоммуникациям и цифровым технологиям

Регулирующий орган по телекоммуникациям и цифровым технологиям (англ. Telecommunications and the Digital Government Regulatory Authority, TDRA) является федеральным ведомством. С 2003 до апреля 2021 года имел название TRA (Telecommunications Regulatory Authority). Штаб-квартира находится в Абу-Даби, имеется офис в Дубае. Возглавляется председателем совета директоров.

В функции TDRA входит обеспечение доступности телекоммуникационных услуг для всех эмиратов и развитие сектора связи, выдача лицензий операторам и контроль соблюдения лицензиатами установленных правил, в том числе осуществление фильтрации контента, разработка нормативной базы в области ИКТ, разрешение любых споров участников ИКТ-рынка в ОАЭ.

TDRA в своей деятельности стремится применять новейшие технологии: запущена новая система регулирования использования радиочастотного спектра, которая является первой в своем роде на Ближнем Востоке и второй по мощности в мире. Она включает 13 станций, которые способны эффективно обеспечивать покрытие территории ОАЭ [30].

---

32 Также имеются сведения, что в 2014 году в Штаб-квартире Национальных вооруженных сил создано Киберкомандование, однако данные о наличии стратегий или доктрин военного ведомства, а также задействованных силах и средствах отсутствуют. Источник: Hussein Ibish The UAE's Evolving National Security Strategy, The UAE's Evolving National Security Strategy, https://www.internetsociety.org/wp-content/uploads/2020/04/Internet_Infrastructure_Security_Guidelines_for_Arab_states-EN.pdf

Как национальная Администрация связи, TDRA представляет страну в Международном союзе электросвязи, на региональных и международных форумах.

В соответствии с законом №2 от 2018 года создана **Национальная группа реагирования на компьютерные инциденты (aeCERT)** Координационного центра кибербезопасности TDRA [31]. Ее задача — защита ИКТ-инфраструктуры от возможных угроз и взломов, повышение стандартов информационной безопасности. Она стремится поддерживать и обеспечивать безопасное киберпространство для граждан и резидентов ОАЭ, а также распространять информацию об угрозах, уязвимостях и инцидентах кибербезопасности. Группа ежемесячно отражает более 100 тыс. кибератак на учреждения федерального правительства. По статистике 73% из них являются вредоносными программами, 15% — уязвимостями и 12% — фишинговыми атаками.

Несмотря на то, что деятельность рассмотренных выше федеральных ведомств, обладающих полномочиями радиоэлектронной и компьютерной разведки контролируется Верховным советом национальной безопасности и Советом по кибербезопасности ОАЭ, остаются неизвестными механизмы их межведомственной координации, взаимодействия центров анализа угроз и принятия решений, обмена разведданными между ними, эмиратами и коммерческими компаниями.

4.6. Национальное агентство по чрезвычайным ситуациям и катастрофам

Это федеральное ведомство (National Emergency Crisis and Disasters Management Authority, NECMA) действует «под зонтиком» Верховного совета национальной безопасности. Оно отвечает за безопасность жизни граждан и жителей страны, программы гражданской обороны, подготовки к чрезвычайным ситуациям и кризисам, включая масштабные компьютерные атаки. Для этого осуществляются различные программы мониторинга, базирующиеся на технологиях искусственного интеллекта, часть из них реализуется Group 42.

В функции NECMA входит разработка для частного сектора руководящих принципов реагирования на компьютерные атаки [32]. Ведомство также обеспечивает доступ к открытым наборам данных по профилю своей деятельности.

4.7. Министерство внутренних дел

Министерство внутренних дел ОАЭ (англ. Ministry of Interior, MoI) в соответствии с Федеральным законом №5 от 2012 года создало специализированные подразделения полиции для расследования киберпреступлений. Аналогичные структуры имеются во всех эмиратах.

Следуя принципу полной цифровизации правительства, реализованы онлайн инструменты для уведомления уполномоченных органов о выявленном вредоносном контенте, совершенных компьютерных правонарушениях или подозрениях о них (веб-сайты: федеральный — eCrime, в эмирате Дубай интеллектуальный полицейский участок — Dubai Police и Центра электронной безопасности Дубая Al Ameen, мобильные приложения eCrime, RZAM, Aman service, My Safe Society). При этом используются технологии искусственного интеллекта для оперативного анализа криминальной деятельности и выявления преступников.

4.8. Федеральное управление идентификации, гражданства, таможни и безопасности портов

Этот орган (англ. Federal Authority for Identity, Citizenship, Customs & Ports, ICP) создан на основе Федерального законодательного декрета №14 от 2021 года путем объединения Федерального органа по идентификации личности и гражданству, Федерального таможенного управления и Главного управления по безопасности портов, границ и свободных зон. В функции ведомства входит разработка политик, стратегии и законодательства в части вопросов цифровой идентификации личности, гражданства, паспортов, въезда и проживания иностранцев, таможенной и портовой безопасности, а также получения соответствующих разрешений от Совета министров. Управление также будет работать над созданием, развитием и обновлением реестра населения и системы персональных данных в стране, управлять ими в соответствии с передовой практикой и требованиями информационной безопасности, а также над созданием систем, программ и процедур для обеспечения выдачи удостоверений личности всем гражданам и резидентам страны.

4.9. Федеральный центр конкурентоспособности и статистики

Этот правительственный центр (англ. Federal Competitiveness and Statistics Centre, FCSC), связанный с Министерством по делам Совета министров ОАЭ, активно участвует в повышении осведомленности о культуре конкурентоспособности и важности предоставления качественных и точных данных, влиянии статистики и конкурентоспособности на формирование политики и стратегическое планирование. Центр обеспечивает функционирование национального портала государственных открытых данных Bayanat, реализованного на облачной платформе Azure (Microsoft). В настоящее время на нем представлено 2649 наборов данных в сфере экономики, образования, общества, технологий, транспорта, окружающей среды, правительства, здравоохранения, инфраструктуры, предпри-

нимательства и рынка труда с почти 4,8 тыс. ресурсов. Доступ к ним возможен посредством 23 приложений [33]. Известно, что при последней модернизации портала в 2023 году был заключен контракт с американским ООО Datopian, которое координирует сообщество разработчиков программного обеспечения с открытым кодом для работы с Большими данными[33].

4.10. Примеры государственно-частного партнерства

Порой трудно провести грань между государственными и коммерческими предприятиями ОАЭ, поскольку многими из них владеют члены эмирских семей, что создает переплетение интересов и задач. Примеров такого государственно-частного партнерства очень много.

В частности, с 2022 года национальный технологический лидер в области облачных технологий и кибербезопасности Injazat, входящий в принадлежащую шейху Тахнун бен Зайд аль-Нахайяну консорциум Group 42, совместно с Советом по кибербезопасности ОАЭ реализует Стратегический меморандум о координации и сокращении времени реагирования на потенциальные кибератаки, что позволит всем правительственным и полугосударственным организациям быть защищенными службами обнаружения и реагирования Injazats Cyber Fusion Centers.

5. Участие в международном сотрудничестве с ООН и другими международными и региональными организациями в области формирования системы международной информационной безопасности

С момента образования в 1971 году Объединенные Арабские Эмираты являются членом ООН и ряда ее специализированных учреждений (например, МСЭ), с 1972 года — Лиги арабских государств, Движения неприсоединения, Организации Исламская конференция и Межпарламентского союза, с 1996 года — ВТО, Совета сотрудничества арабских государств Персидского залива.

Действия ОАЭ во внешней политике традиционно отличают взвешенный подход, ориентация на мирное разрешение международных проблем и достижение консенсуса. Основными задачами государства на мировой арене являются формирование благоприятного окружения, создание условий стабильного

33 В частности, использовался безопасный кластер Azure Kubernetes облачной архитектуры, фреймворк PortalJS, комплексная сеть архивов знаний CKAN2.9.5. Источник: Revolutionizing Open Data in the United Arab Emirates: The Creation of a New Open Data Portal with PortalJS and CKAN, https://www.datopian.com/showcase/case-studies/revolutionizing-open-data-fcsc

социально-экономического развития страны в контексте динамично меняющегося мира.

ОАЭ ни разу не становились членами Рабочей группы по информатизации и коммуникациям в контексте международной безопасности (ГПЭ ООН по МИБ), но поддержали следующие российские инициативы:

- принятие правил, норм и принципов ответственного поведения, а также создание Рабочей группы ООН открытого состава (резолюция Генеральной Ассамблеи ООН A/RES/73/27 от 5 декабря 2018 года);
- включение в повестку дня ООН обсуждения вопроса о противодействии использованию ИКТ в преступных целях (A/RES/73/187 от 17 декабря 2018 года);
- создание специального межправительственного комитета экспертов открытого состава для разработки всеобъемлющей международной конвенции о противодействии использованию ИКТ в преступных целях (A/RES/74/247 от 27 декабря 2019 года);
- созыв новой Рабочей группы ООН открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025 (A/RES/75/240 от 31 декабря 2020 года).

При голосовании по американскому проекту резолюции о созыве Группы правительственных экспертов ООН на 2019–2021 годы ОАЭ ожидаемо поддержали и этот проект (A/RES/73/266 от 22 декабря 2018 года).

ОАЭ присоединились к инициативе Франции — «Парижскому призыву к доверию и безопасности в киберпространстве», но не выступили соавторами ее инициативы – Программа действий ООН по продвижению ответственного поведения государств в киберпространстве.

6. Участие в международном сотрудничестве с другими государствами в области цифровизации и информационной безопасности

Приоритетом ОАЭ на региональном уровне является укрепление стабильности и безопасности в зоне Персидского залива и на Ближнем Востоке. В этой связи одно из центральных направлений внешней политики государства — развитие тесных отношений с соседними странами на Аравийском полуострове. Как уже отмечалось выше, ОАЭ претендуют на роль регионального лидера в области формирования системы международной информационной безопасности и к 2030 году ведущей державы в технологиях искусственного интеллекта. Для реализации этих амбиций правительство страны сотрудничает с большинством ведущих государств.

6.1. США

Сотрудничество между ОАЭ и США всегда было жизненно важным для поддержки интересов Вашингтона в регионе MENA. Вашингтон и Абу-Даби давно и плотно взаимодействуют в области обороны[34]. В настоящее время США занимают лидирующую позицию в перечне экспортеров вооружений и военной техники для Эмиратов, поставляя продукцию военного назначения, проводя обучение личного состава вооруженных сил и специалистов ОАЭ, участвуя в стратегическом планировании, организуя совместные учения и операции[35]. Однако охлаждение этих связей налицо, например, в 2023 году правительство предпочло американским F-35 французские истребители Rafale, а также закупило китайские L-15.

В экономике просматривается аналогичная тенденция. ОАЭ относятся к важным инвесторам США и в 2020 году вложили в них около 45 млрд долл. С 2009 года Эмираты являются главным экспортером американских товаров на Ближнем Востоке. Положительное сальдо торгового баланса США является шестым по величине в мире при том, что с большинством государств США имеют дефицит баланса [34].

В сфере ИКТ и информационной безопасности взаимодействие тоже очень глубокое, особенно в части развития военного аспекта кибербезопасности. Но сейчас приоритеты страны лежат в сфере цифровизации общества. По итогам визита Дж. Байдена в Абу-Даби в 2022 году, отмечена важность углубления сотрудничества в области политики и практики, влияющих на цифровую экономику, в трансграничной передаче данных и улучшении их интероперабельности, в совершенствовании для этого правовых механизмов и политик обеспечения конфиденциальности данных.

В октябре 2023 года подписан Меморандум о взаимопонимании по сотрудничеству в области кибербезопасности для «защиты целостности международной финансовой системы» и обмена информацией об инцидентах и угрозах кибербезопасности в финансовом секторе, повышения квалификации, включая киберучения и другие мероприятия по наращиванию потенциала [35].

Главным инструментом реализации сотрудничества в сфере цифровизации и информационной безопасности является активное присутствие американских компаний в качестве ведущих подрядчиков различных ИКТ-проектов, как в государственном, так и частном секторе. Однако они испытывают все более жесткую конкуренцию с китайскими корпорациями и инвестиционными компаниями,

34 Соглашение об общей безопасности военной информации 1987 года, Соглашение о приобретении и перекрестном обслуживании 2006 года и Соглашение о сотрудничестве в области обороны 2019 года.

35 После вторжения Ирака в Кувейт между ОАЭ и США было подписано действующее до сих пор соглашение, позволяющее Вашингтону временно использовать ряд военных баз на территории страны.

ориентированными на частный бизнес. Так в секторе телекоммуникаций ведущие производители КНР уже перекроили рынок в свою пользу, тем самым сделав вовлечение других производителей в развитие сетей 5G максимально сложным [36]. Постепенно и американские университеты утрачивают свое лидирующее положение в сфере ИКТ-образования в Эмиратах, кроме того, сокращается поток студентов в ВУЗы США, переориентируясь на более дешевое восточное направление. Это вызывает недовольство Вашингтона. Администрация Дж. Байдена настаивает, чтобы ОАЭ заменили оборудование Huawei в своей телекоммуникационной сети незападные технологии и предприняли другие шаги по отдалению от КНР.

6.2. Китайская Народная Республика

Китай является главным торговым партнером ОАЭ, который, как отмечено выше, нашел возможность заменить США в киберпространстве Ближнего Востока, включая ОАЭ [37]. Помимо развертывания сетей 5G на технологиях Huawei и ZTE, постепенно расширяется присутствие китайских компаний в секторе обработки Больших данных и облачных услуг. В 2016 году Alibaba Cloud запустила свой первый ЦОД в Дубае. Правительство КНР ведет в ОАЭ активную инвестиционную кампанию, вкладывая средства в перспективные сектора экономики в первую очередь в ИКТ.

ОАЭ запустили систему международных расчетов в цифровых валютах, разработанную совместно с Китаем, Гонконгом и Таиландом. Первый перевод с mBridge на 13,6 млн долларов в цифродирхамах уже отправлен в КНР.

Университет Объединенных Арабских Эмиратов (UAEU) в июне 2022 года заявил о финансировании шести совместных исследовательских проектов с Китайской академией наук по направлению обеспечения устойчивости исследовательской деятельности и укрепления международной позиции университета в области Больших данных [38].

6.3. Израиль

Известно, что даже при отсутствии официальных отношений между ОАЭ и Израилем, осуществлялось взаимодействие в сфере безопасности, в том числе в киберсфере[36]. После подписания в 2020 году соглашения о полной нормализа-

36 По мнению экспертов, сотрудничество в сфере безопасности между Израилем и ОАЭ не могло осуществляться без согласия руководства обеих стран, это подтверждают утечки дипломатической переписки, опубликованной Wikileaks в 2009 году, где фигурирует Советник по национальной безопасности принц Мухаммед бен Заид аль-Нахайян и бывший министр иностранных дел Израиля Ципи Ливни. Принимая во внимание, что израильская компания через свои дочерние подразделения (AGT, AIS и ATS) с 2008 года для эмирата Абу-Даби осуществляла

ции отношений и поиске мирного решения израильско-палестинского конфликта, достигнутого при посредничестве США, сотрудничество было расширено. Аналогичные «Авраамические соглашения» подписаны Бахрейном и Марокко, и в конце 2022 года эти страны совместно с ОАЭ объявили о намерении развивать вместе с Израилем проект «Cyber Dome» для повышения уровня региональной цифровой безопасности [39].

В апреле 2023 года вступило в силу Соглашение о всеобъемлющем экономическом партнерстве между Израилем и ОАЭ, что еще больше укрепило связи в коммерческом секторе. Абу-Даби совместно с Израилем планируют активизировать работу по совместному мониторингу и выявлению угроз в киберпространстве, а также нарастить обмен научными кадрами, чтобы «обеспечить понимание общей ситуации и использовать все доступные возможности для борьбы с врагами». В июле 2023 года Мохаммед Аль Кувейти посетил Израиль и заключил соглашение между израильской Rafael Advanced Defense Systems и базирующейся в Абу-Даби CPX о реализации проекта Crystal Ball, в рамках которого при поддержке Microsoft будет создана цифровая платформа для выявления компьютерных атак, обмена информацией и реагирования.

Глобальное сообщество кибербезопасности EliteCISOs, которое объединяет более 500 руководителей служб информационной безопасности из ОАЭ и Индии, подписало меморандум о взаимопонимании с израильской неправительственной организацией Cyber Together [40].

6.4. Индия

Индия является активным партнером в стратегическом сближении с ОАЭ в сфере обеспечения международной кибербезопасности. Обе страны входят в группу I2U2 (Индия, Израиль, ОАЭ, США). Ведется работа над созданием киберпартнерства Индии и ОАЭ, направленного на создание цифровых возможностей государственного и частного секторов, что даст новые инновационные решения в отношении растущих угроз экосистеме кибербезопасности [41].

В 2022 году ОАЭ и Индия подписали соглашение об экономическом партнерстве, которое включает сотрудничество по развитию блокчейна и других новейших технологий. Стороны ожидают, что благодаря этому объем двусторонней

проект Falcon Eye, в рамках которого использовались технологии Интернета вещей и обработки Больших данных, собранных с помощью датчиков и умных камер, по охране нефтедобычи и «умного» города, то взаимодействие очень плотное и масштабное. По заявлению главного исполнительного директора AIS Халфан аль-Шамси на выставке национальной безопасности в Париже (2012 года) «В ОАЭ нам принадлежит 80% рынка национальной безопасности». Источник: Falcon Eye: The Israeli-installed mass civil surveillance system of Abu Dhabi // Middle East Eye, 15 July 2015, https://www.middleeasteye.net/news/falcon-eye-israeli-installed-mass-civil-surveillance-system-abu-dhabi

торговли между Индией и ОАЭ в ближайшие пять лет может достичь 100 млрд долл. США, пока эта цифра составляет 60 млрд. Новое партнерство позволит Торговой палате Дубая стать на всем Ближнем Востоке эксклюзивным поставщиком торговых решений, в которых применяется блокчейн.

6.5. Республика Корея

Еще в 2009 году Республика Корея и ОАЭ договорились о создании ориентированного на будущее стратегического партнерства в области развития для общего процветания. Одновременно были подписаны шесть меморандумов о взаимопонимании, в том числе по ИКТ, который предусматривал следующие направления сотрудничества: инновации и предпринимательство в сфере ИКТ, законы и нормативные акты Республики Корея в этой области, развитие людских ресурсов, роль ИКТ в экономическом росте других секторов, использование цифровых технологий в обществе, зеленые ИКТ. По программам обмена знаниями между двумя странами были налажены различные интеллектуальные и практические взаимодействия. Эмират Абу-Даби высказал заинтересованность в реализации трех инициатив: поддержка системы управления информационной безопасностью; беспроводная широкополосная связь на территории всего эмирата; создание Центра исследований и разработок в области ИКТ.

Наибольший прогресс достигнут в сфере развития инновационных компаний. Так, лидер эмиратского рынка цифровой трансформации, облачных вычислений и кибербезопасности Injazat в октябре 2020 года подписал стратегический меморандум о взаимопонимании с южнокорейским центром стартапов Born2Global Center. Согласно совместной программе «Digital Bridge» Injazat поддерживает южно-корейские стартапы, желающие расширить свое присутствие в ОАЭ.

Доверие в технологической сфере между двумя государствами растет. В 2023 году руководители оборонных ведомств Кореи и ОАЭ провели переговоры в Абу-Даби и договорились укреплять сотрудничество в киберсфере и космосе, а также развивать научно обоснованные учебные программы [42].

6.6. Армения

В декабре 2023 года в Дубае замминистра высокотехнологичной промышленности Армении Геворк Манташян и руководитель Национального совета по кибербезопасности Мухаммед Аль Кувейти подписали Меморандум о взаимодействии в сфере кибербезопасности [43].

6.7. Российская Федерация

Взаимовыгодное сотрудничество России и ОАЭ заметно расширяется в различных сферах, в том числе в ИКТ и международной безопасности. Большой задел создан в освоении космоса[37]: в 2021 году заключено Межправительственное соглашение о сотрудничестве в исследовании и использовании космического пространства в мирных целях, в котором обеспечена надлежащая защита интеллектуальной собственности и конфиденциальной информации.

Расширяется сотрудничество в сфере обороны. Москве и Абу-Даби удалось создать полноценную законодательно-нормативную базу, которая включает Соглашение о военно-техническом сотрудничестве (подписано 13.11.2006 года), дополненное межправительственными соглашениями о взаимной защите секретной информации (вступило в силу 4 июля 2011 года), о взаимной охране интеллектуальной собственности в ходе двустороннего военно-технического сотрудничества (вступило в силу 17.03.2016 года), а также Декларацией о стратегическом партнерстве между Россией и ОАЭ от 1 июня 2018 года, в том числе в области безопасности и обороны.

Действует Межправительственная российско-эмиратская комиссия по торговому, экономическому и техническому сотрудничеству, ее 11 заседание прошло в марте 2023 года в Москве [44]. На нем были обозначены модальности взаимодействия в области космоса, энергетики, банковского и ИТ-секторов, а также в сферах промышленности и транспорта.

Перспективное и взаимовыгодное направление сотрудничества — ИКТ-сектор. Если в ОАЭ получат доступ к российским передовым технологиям в сфере кибербезопасности, защиты Больших данных, электронного правительства, искусственного интеллекта, то, с учетом офисного присутствия большинства ведущих глобальных ИТ-игроков в Дубае и Абу-Даби, наши компании смогут использовать страну в качестве платформы для расширения клиентской базы на Ближнем Востоке и за его пределами — в Азии и Африке, а также для быстрого продвижения инновационных стартапов, оптимальных бизнес-решений, новых продуктов и сервисов.

С 2015 года в ОАЭ открыли свои представительства ряд российских ИКТ-компаний, в том числе «Технопарк»/«Сколково», «Агрегатор технологий», «Гарант Парк технологии». Подобное партнерство приобретает структурированный характер: например, Российским экспортным центром совместно с Фондом «Сколково», ГК InfoWatch реализуется проект развития Центра поддержки рос-

37 Первый космонавт из ОАЭ Хаззаа аль-Мансури отправился в космос в 2019 г. с космодрома Байконур на корабле «Союз МС-15», а второй космонавт — Султан аль-Нейади впервые в истории арабских стран в апреле 2023 года вышел в открытый космос.

сийского экспорта информационных и цифровых технологий в рамках свободной экономической зоны Dubai Internet City [45]. Итогом общих усилий явилось соглашение о создании совместных предприятий, которое подписали в июне 2023 года отечественный разработчик ИТ-решений для цифровой трансформации государства и бизнеса Omega.Future и крупнейшая на Ближнем Востоке платформа электронной коммерции и маркетинга Sinaha [46]. Взаимная договоренность предусматривает строительство в Абу-Даби завода по производству 3D-принтеров и образовательной робототехники.

Национальный Совет по кибербезопасности ОАЭ в октябре 2023 года подписал Меморандум о взаимопонимании с российским лидером в области кибербезопасности Group-IB, стороны взяли на себя обязательство создать систему обмена знаниями об актуальных угрозах информационной безопасности, индикаторах компрометации и новых тактиках, методах и процедурах, используемых киберпреступниками, нацеленными на Ближний Восток, Турцию и Африку. Правительственные организации ОАЭ получат доступ к комплексному набору передовых решений Group-IB, включая анализ угроз, управляемую XDR, защиту от мошенничества и защиту от цифровых рисков.

ОАЭ также подписали Меморандум о взаимопонимании с Лабораторией Касперского. Стороны намерены обмениваться информацией по выявлению, расследованию и реагированию на киберугрозы, а также опытом исследования тенденций в области вредоносного программного обеспечения, индикаторах компрометации и рисках безопасности, с которыми сталкиваются экономические сектора.

Позитивным фактором служит растущее взаимопонимание и доверие между лидерами Российской Федерацией и ОАЭ, что подтвердил визит В. Путина в Абу-Даби в декабре 2023 года.

7. Основные приоритеты национальной политики ОАЭ в рамках БРИКС

Присоединение с 1 января 2024 года ОАЭ к объединению БРИКС укладывается в логику сбалансированной внешней политики государства. Официальные лица этой страны неоднократно заявляли о приоритете формирования эффективного многостороннего партнерства на основе открытости и активного взаимодействия со всеми заинтересованными сторонами.

Положение в международном сообществе и прочная экономическая база ОАЭ придадут объединению новую динамику. Эксперты утверждают, что инновационный подход ОАЭ к технологиям и устойчивому развитию схож с позицией БРИКС. Огромный опыт страны в области возобновляемых источников энергии,

особенно солнечной, наряду со значительными достижениями в разных секторах цифровой экономики, таких как финтех и строительство умных городов, может быть ценен для других государств-участников БРИКС, стремящихся диверсифицировать свою экономику.

Более того, хорошо развитые глобальные торговые сети ОАЭ и статус страны, как крупного финансового центра, могли бы значительно укрепить экономическую сплоченность внутри БРИКС, способствуя развитию торговых связей и облегчая инвестиционное взаимодействие. Акцент ОАЭ на многосторонности и сотрудничестве Юг-Юг согласуется с основными целями БРИКС, потенциально приводя к более интегрированной позиции и сотрудничеству по глобальным вопросам. Страны-участницы могут извлечь выгоду из стратегического географического расположения ОАЭ как транзитного государства[38] и его развитой логистической и транспортной инфраструктуры.

Важным аспектом также может стать упрощение перехода на расчеты в национальных валютах в международной торговле[39] и формирование новых платежных систем на фоне расширения БРИКС. ОАЭ уже запустили механизм расчетов в национальных валютах при сделках с сырой нефтью с Индией. Расширение такого подхода на страны-партнеры БРИКС вполне реально (в частности, с учетом того, что после расширения доля объединения в мировом производстве нефти выросла с 20 до 40%) и целесообразно для активизации процесса дедолларизации и снижения возможностей санкционного давления.

Вхождение ОАЭ в БРИКС знаменует значительный сдвиг в глобальной экономической и политической динамике. Этот стратегический альянс не только диверсифицирует экономические возможности и геополитическое влияние стран БРИКС, но и усиливает роль ОАЭ на мировой арене. С экономической точки зрения ОАЭ только выиграют от расширения торговых отношений и доступа к развивающимся рынкам, увеличения иностранных инвестиций. Политически этот шаг означает стремление ОАЭ играть более заметную роль в глобальном управлении, используя свое стратегическое географическое расположение и экономическую мощь для посредничества между Западом и глобальным Югом.

Для членов БРИКС присоединение ОАЭ, страны со значительным финансовым влиянием, повышает их авторитет на коллективных переговорах и на международных форумах. Для ОАЭ это открывает новые возможности для торговли, инвестиций и технологического сотрудничества, еще больше укрепляя их статус глобального центра коммерции и инноваций. Последствия этого партнерства вы-

38 Индия совместно с ведущими странами пыталась создать транспортный логистический коридор из АТР в ЕС через свою территорию, но отсутствие региональной стабильности на Ближнем Востоке этот проект отложен на неопределенную перспективу.

39 ОАЭ уже запустили механизм расчетов в национальных валютах при сделках с сырой нефтью с Индией.

ходят за рамки простых экономических сделок и, вероятно, повлияют на геополитические стратегии, энергетическое сотрудничество и культурные обмены, тем самым изменив международные отношения [47].

8. Использованная литература

1. World Population by Country 2024 (Live), https://worldpopulationreview.com/
2 United Arab Emirates (UAE) Population Statistics 2024 // GMI, https://www.globalmediainsight.com/blog/uae-population-statistics/
3 Об Объединенных Арабских Эмиратах// МИД России, https://uae.mid.ru/ru/countries/bilateral-relations/abouttheuae/
4 Abu Dhabi to play larger role in space communications with new optical ground station, Mar 08, 2024, https://www.thenationalnews.com/business/future/2024/03/08/abu-dhabi-to-play-larger-role-in-space-communications-with-new-optical-ground-station/
5 ICT sector // Ministry of Economy UAE, https://www.moec.gov.ae/en/-/ict-sector
6 United Arab Emirates Data Centers, https://www.datacentermap.com/united-arab-emirates/
7 WIPO Global Innovation Index 2023: Innovation in the face of uncertainty, https://www.wipo.int/global_innovation_index/en/2023/
8 GCC looks to ICT parks for economic diversification // Companies And Markets - Technology – Emirates24/7, https://www.emirates247.com/eb247/companies-markets/technology/gcc-looks-to-ict-parks-for-economic-diversification-2009-07-28-1.29512
9 AI Hardware Infrastructure Report UAE, 2020, https://ai.gov.ae/infrastructure_report/
10 UAE: World's largest AI training supercomputer launched by Abu Dhabi firm// Khaleej Times, 20 July 2023, https://www.khaleejtimes.com/uae/uae-worlds-largest-ai-training-supercomputer-unveiled-in-abu-dhabi, Cerebras Systems signs $100 million AI supercomputer deal with UAE's G42 // Reuters, 27 July 2023, https://www.reuters.com/technology/cerebras-systems-signs-100-mln-ai-supercomputer-deal-with-uaes-g42-2023-07-20/
11 United Arab Emirates E-commerce Market 2024-2032. Size, Share, Growth, https://markwideresearch.com/united-arab-emirates-e-commerce-market/
12 UN E-Government Survey 2022, https://desapublications.un.org/publications/un-e-government-survey-2022
13 The United Arab Emirates // International Institute for Strategic Studies, https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/09/cyber-capabilities-and-national-power-vol-2/cyber-capabilities-and-national-power_volume-2_13-the-united-arab-emirates.pdf
14 UAE Cyber Security Council and CPX Unveil Cybersecurity Report 2024: A Call to Action Against Rising Cyber Threats - Technology // Emirates24|7, https://www.emirates247.com/technology/uae-cyber-security-council-and-cpx-unveil-cybersecurity-report-2024-a-call-to-action-against-rising-cyber-threats-2024-03-11-1.730198
15 UAE Cybersecurity Market Size & Share Analysis - Growth Trends & Forecasts (2024-2029), https://www.mordorintelligence.com/industry-reports/uae-cybersecurity-market
16 Там же.
17 The UAE's Fourth Industrial Revolution (4IR) Strategy, https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/government-services-and-digital-transformation/the-uae-strategy-for-the-fourth-industrial-revolution
18 Operation 300bn, the UAE's industrial strategy // The Official Portal of the UAE Government, https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/industry-science-and-technology/the-uae-industrial-strategy
19 Regulatory Policy on the Internet of Things ('IoT'), https://tdra.gov.ae/-/media/About/regulations-and-ruling/EN/Regulatory-Policy---Internet-of-Things--IoT--pdf.ashx
20 Хома В.С. Основные направления цифровизации экономики в ОАЭ// Российский внешнеэкономический вестник № 2-2023, https://cyberleninka.ru/article/n/osnovnye-napravleniya-tsifrovizatsii-ekonomiki-v-oae
21 Cyber safety and digital security // The Official Portal of the UAE Government, https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security
22 NCSI: United Arab Emirates, https://ncsi.ega.ee/country/ae_2022/
23 Critical Information Infrastructure Protection Policy, 2023, https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/policies/transport-and-infrastructure/critical-information-infrastructure-protection-policy

24 Electronic Transactions and Trust Services law // The Official Portal of the UAE Government, https://u.ae/en/about-the-uae/digital-uae/regulatory-framework/electronic-transactions-and-trust-services-law
25 Federal Law No. 2 of 2006 on the Prevention of Information Technology Crimes, United Arab Emirates // WIPO, https://www.wipo.int/wipolex/en/legislation/details/13817
26 Cyber safety and digital security //The Official Portal of the UAE Government, https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security
27 Public Prosecution explains penalties of fake e-mails, websites, online accounts // Emirates News Agency , 2022, https://wam.ae/en/details/1395303032222
28 UAE Information Assurance (IA) Regulation // The Official Portal of the UAE Government, https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security/uae-information-assurance-regulation
29 The United Arab Emirates // International Institute for Strategic Studies, https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/09/cyber-capabilities-and-national-power-vol-2/cyber-capabilities-and-national-power_volume-2_13-the-united-arab-emirates.pdf
30 Telecommunication and Digital Government Regulatory Authority – UAE, https://github.com/TDRA-ae
31 Cyber safety and digital security, https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security
32 The United Arab Emirates // International Institute for Strategic Studies, https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/09/cyber-capabilities-and-national-power-vol-2/cyber-capabilities-and-national-power_volume-2_13-the-united-arab-emirates.pdf
33 Open Government Data Laws Policies And Platforms, 2024, https://u.ae/en/information-and-services/g2g-services/open-government-data/open-government-data-laws-policies-and-platforms
34 ОАЭ следующие в очереди на выпадение из орбиты США? // Forbes, 15.04.2023, ИноСМИ, https://inosmi.ru/20230411/oae-262100943.html
35 U.S.-UAE Cybersecurity Cooperation Marks Needed Collaboration in the Region// October 16, 2023, https://www.fdd.org/analysis/2023/10/16/u-s-uae-cybersecurity-cooperation-marks-needed-collaboration-in-the-region/
36 Борьба за киберпространство ОАЭ: КНР против США// РСМД, 7 октября 2022, https://russiancouncil.ru/blogs/Ural-associationmiddleeast/borba-za-kiberprostranstvo-oae-knr-protiv-ssha/
37 M.Salami The UAE's Balancing Act in the US-China Cold War. The New Arab. 30 Dec. 2021. https://english.alaraby.co.uk/analysis/uaes-balancing-act-us-china-cold-war
38 UAEU Announces Six Research Projects in Cooperation with Chinese Academy of Sciences // https://www.uaeu.ac.ae/en/news/2021/march/uaeu-announces-six-research-projects-in-cooperation-with-chinese-academy-of-sciences.shtml
39 Арабо-израильский «Киберкупол» // РСМД, 14 марта 2023, https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/arabo-izrailskiy-kiberkupol/
40 Group-IB Signs Agreement With UAE Cyber Security Council, https://securitymea.com/2023/10/18/group-ib-signs-agreement-with-uae-cyber-security-council/
41 How India, UAE, Israel are trying to build secure cyberspace // The Week, https://www.theweek.in/theweek/specials/2023/07/08/building-a-secure-cyberspace-through-the-india-uae-israel-cyber-security-partnership.html
42 Defense chiefs of Korea, UAE discuss cooperation in arms industry, cybersecurity // Koreajoongangdaily, February 2023, https://koreajoongangdaily.joins.com/2023/02/22/national/defense/defense-defense-ministry-defense-minister/20230222101842794.html
43 Армения и ОАЭ подписали меморандум о сотрудничестве, 2 декабря 2023, https://ru.armeniasputnik.am/20231202/armeniya-i-oae-podpisali-memorandum-o-sotrudnichestve-v-sfere-kiberbezopasnosti-69516827.html
44 О перспективах сотрудничества России и ОАЭ в сфере высоких технологий // РСМД, 18 января 2024, https://russiancouncil.ru/analytics-and-comments/analytics/o-perspektivakh-sotrudnichestva-rossii-i-oae-v-sfere-vysokikh-tekhnologiy/?sphrase_id=133392138
45 Глава InfoWatch Gulf приняла участие в Восьмом заседании Межправительственной Российско-Эмиратской комиссии по торговому, экономическому и научно-техническому сотрудничеству, 11 июля 2018, https://www.infowatch.ru/company/presscenter/news/20573
46 IT-компания Omega.Future откроет в ОАЭ производство 3D-принтеров и робототехники,https://spbit.ru/news/IT-kompaniya-Omega-Future-otkroyet-v-OAE-proizvodstvo-3D-printerov-i-robototekhniki-274175
47 ОАЭ в БРИКС: роль страны в будущем альянса // TVBRICS, 13 марта 2024, https://tvbrics.com/bricslife/oae-v-briks-rol-strany-v-budushchem-alyansa/

Республика Индия

Официальное название: Республика Индия (Bhārat Gaṇarājya)

Столица: Нью-Дели

Официальный язык: Конституцией официальными определены 21 местных языка, самый распространенный — хинди, его носителями является более 40% населения, в деловой переписке используется английский язык.

Территория: 3 287 590 км^2 (7 место в мире). Индия расположена на территории Южной Азии на северном побережье Индийского океана. На западе граничит с Пакистаном, на северо-востоке — с Бутаном, Китаем и Непалом, на востоке — с Бангладеш и Мьянмой. Имеет морскую границу на юго-западе с Мальдивскими островами, на юго-востоке — со Шри-Ланкой и Индонезией. Спорная территория Ладакх на границе с Афганистаном.

Население: самое большое в мире — 1428,6 млн чел. (по данным Фонда населения ООН на конец 2023 года).

Государственное устройство: федеративная республика с парламентской системой правления[1], объединяет 28 штатов и 8 союзных территорий.

Государственная власть в Индии состоит из законодательной, исполнительной и судебной.

Законодательная власть. Двухпалатный парламент, состоящий из нижней — Народной палаты (Лок Сабха) со сроком полномочий 5 лет и постоянно действующего Совета штатов (Раджйа Сабха), состав которого каждые 2 года обновляется на треть.

Исполнительная власть состоит из президента, вице-президента и Совета министров (кабинет министров является его исполнительным комитетом), возглавляемого премьер-министром, с 2014 года эту должность занимает Нарендра Моди. Премьер-министр назначается президентом, который также назначает других министров по совету премьер-министра. В индийской парламентской системе исполнительная власть подчинена законодательной: премьер-министр и Совет министров несут прямую ответственность перед нижней палатой парламента.

Глава государства — президент, избираемый на пять лет непрямым голосованием членов коллегии выборщиков, состоящей из избранных членов обе-

1 Индия, согласно Конституции страны, вступившей в силу 26 января 1950 года является суверенной, социалистической, светской либерально-демократической республикой.

их палат парламента и законодательных собраний штатов. С 25 июля 2022 года должность президента занимает представительница племенных народов Индии Драупади Мурму, она стала второй женщиной-президентом Индии после Пратибхи Патил (2007–2012).

Судебная власть состоит из Верховного суда, возглавляемого верховным судьей Индии, 21 Высшего суда и большого количества мелких судов. Верховный суд является юридически независимым и имеет право провозглашать законы или отменять законы штатов и территорий в случае, если они противоречат Конституции. Одной из наиболее важных функций Верховного суда является конечная интерпретация Конституции.

Экономика: По данным Всемирного банка за 2022 год показатели Валового внутреннего продукта (ВВП) (по паритету покупательной способности):

Итого: 11,875 трлн долл. США (3 место в мире), рост за год на 6,8%.

На душу населения: 8 379 долл. США (126 место в мире);

Показатели ВВП (по номиналу):

Итого: 3,385 трлн долл. США (5 место в мире).

На душу населения: 2389 долл. США (140 место в мире).

Дипломатические отношения с Россией (СССР): Индия и СССР установили дипломатические отношения 13 апреля 1947 года, за четыре месяца до получения Индией независимости от Великобритании, официально объявленной 15 августа 1947 года. Соглашение о всеобъемлющем партнерстве между Российской Федерацией и Республикой Индия было подписано в 2000 году.

1. Обзор уровня информатизации и обеспечения информационной безопасности Индии

В целях перехода к инновационному развитию Индия в 90-х годах прошлого века перешла на экспортно-ориентированную модель национальной экономики, что стимулировало укрепление высокотехнологичных производств. В современной цифровой трансформации страны ключевая роль отведена ИКТ-отрасли. Для ее развития были введены меры государственной поддержки, включая льготное налогообложение и кредитование, либерализацию привлечения частного и иностранного капитала[2], снижение бюрократического вмешательства в экономику, в том числе отмена лицензирования деятельности по разработке программного обеспечения (ПО) и упрощение процедуры регистрации ИТ-компаний. Были созданы государственные структуры для содействия развитию отрасли путем расширения ИКТ-инфраструктуры, организации производства и улучшения маркетинга, были проведены реформы высшего и среднего образования, сертификации специалистов, разработки стандартов. Это привело к бурному росту экспортных производственных зон и технопарков для разработки ПО[3], и за относительно короткий срок позволило создать развитую национальную индустрию ИКТ [1], однако со значительным присутствием иностранного капитала[4] и глобальных корпораций[5].

На данный момент Индия после Китая является вторым по объему национальным ИКТ-рынком, который ежегодно растет почти на 9% и к 2025 году может достичь 350 млрд долл. США. В 2022 году страна заняла третье место в мире по объему национальной экосистемы инновационных ИТ-компаний[6] и уже продолжительное время удерживает второе место по аутсорсингу ПО[7] и бизнес-процессов.

---

2 Доля иностранного участия в капитале индийских ИКТ-компаний была повышена до 51% при условии покрытия ими стоимости ввозимого ИТ-оборудования и до 100% для предприятий, ориентированных на экспорт (в сфере обработки данных, разработки ПО и компьютерных консультационных услуг; поставок ПО; консультационных услуг в области бизнеса и управления, услуг по исследованию рынка, услуг технического тестирования и анализа). Политика развития прямых иностранных инвестиций позволила привлечь (919 млрд долл. США, 65% которых получены в последние 9 лет с апреля 2000 г. по март 2023 г.).

3 Первыми аналогами американской Кремниевой долины стали технопарки в Мумбаи и Бангалоре, сейчас их более 20. Основная инновационная активность концентрируется в кластерах Ченнаи, Бангалор, Дели и Мумбаи, которые привлекают значительные инвестиции со стороны крупного бизнеса.

4 В период 2014–20 гг. общий объем финансирования со стороны ИКТ-компаний США составил 30 млрд долл. США, японских — 12 млрд, а китайских – 4 млрд (из которых 75% пришлось на Alibaba и Tencent).

5 По состоянию на сентябрь 2022 года ведущие ИТ-корпорации (Microsoft, IBM, Cisco Systems, Lucent Technology и др.) открыли в Индии более 1,5 тыс. Центров глобальных возможностей, в которых занято 1,3 млн чел. Источник: https://it-ros.ru/news/1153-kak-indija-prevraschaetsja-v-mirovoi-centr-tehnologii-i-uslug.html

6 В 2021 году в ИКТ-сфере Индии 150 стартапов был близки к получению статуса «единорогов» (компании с капитализацией более 1 млрд долл. США и принадлежащие своим создателям). В 2023 году появилось еще 23 новых «единорога» и 1300 ИТ стратапов. Источник: https://www.investindia.gov.in/ru-ru/sector/it-bpm

7 При этом надо принимать во внимание, что западными корпорациями на аутсорсинг отдается разработка ПО только вспомогательных функций, а разработка ключевых блоков ПО, сборка и «ноу-хау» остается за правообладателями, поэтому уровень индийских программистов хотя и высокий, но ниже «мирового» уровня.

Эти сегменты индийского ИКТ-рынка в совокупности дают более 60% экспорта услуг Индии и обеспечивают прямую занятость более 5 млн человек.

Высокий инновационный потенциал ИКТ-сектора обеспечивают научные и опытно-конструкторские разработки. По данным Австралийского института стратегической политики за 2023, год Индия прочно входит в пятерку ведущих технологических супердержав[8]. В 29 из 44 критически важных для цифровизации технологий страна третья по расширенной аналитике данных, распределенным реестрам, машинному обучению, технологиям обеспечения кибербезопасности, разработке и производству чипов, обработке естественных языков и распознаванию речи. В сфере искусственного интеллекта и постквантовой криптографии исследования Индии поставлены на пятое место. Кроме того, страна достаточно хорошо проявляет себя в сфере аппаратных ускорителей для высокопроизводительных вычислителей. По оценке Всемирной организации по интеллектуальной собственности, Индия занимает 40 позицию в Глобальном инновационном индексе 2023 [2].

Вместе с тем, налицо недостаточное финансирование НИОКР, низкий уровень коммерциализации их результатов в производственном секторе и медленное освоение новых технологий в экономике[9]. Для формирования ИКТ-инфраструктуры и национальной цифровой экосистемы страна полагается на импортируемое сетевое оборудование (Nokia, Samsung, Huawei)[10], значительная часть рынка мобильных технологий и комплектующих контролируется китайскими производителями [3]. В связи с этим запущена кампания «**Самодостаточная Индия**» — курс на повышение технологического суверенитета страны и национального производственного потенциала, предпринимаются усилия по развитию сектора микроэлектроники[11] и построению собственных суперкомпьютеров[12]. Страна уже

8 Расчет оценки сделан на основе наукометрических данных (количество научных публикаций, индекс цитирования, количество научных и учебных заведений по конкретной проблематике, входящие в Top 20) в таких критически важных для стратегического преимущества в цифровой экономике технологиях, как мобильная связь 5G/6G и оптические коммуникации, искусственный интеллект, расширенная аналитика данных, распределенные реестры, машинное обучение, технологии обеспечения кибербезопасности, разработка и производство чипов, обработка естественных языков и распознавание речи. Источник: ASPI's Critical Technology Tracker The global race for future power, 2023, https://www.aspi.org.au/report/critical-technology-tracker

9 В документе стратегического планирования «Политика в области науки, технологий и инноваций» (STIP-2013) подчеркивалась необходимость повысить уровень взаимодействия между государственным и частным секторами, между правительством, промышленностью и академическими кругами, а также ставилась цель увеличить расходы на исследования и разработки до 2% ВВП, в основном за счет вложений бизнеса.

10 Доля импорта на внутреннем ИКТ-рынке в 2019 году составляла 76,3%.

11 Согласно данным Индийской ассоциации производителей полупроводников, этот сегмент рынка в 2015–2020 гг. ежегодно рос на 29,4%. По прогнозам в 2025 году он может достичь объема в 400 млрд долл. США. Индия ежегодно разрабатывает около 2 тыс. чипов для различных отраслей экономики, преимущественно для бытовой электроники. В этом секторе ИКТ-индустрии занято до 20 тыс. инженеров, но для дальнейшего развития требуются крупные вложения, осуществление НИОКР и квалифицированный персонал. Источник: https://www.clearias.com/semiconductor-industry-india/, https://insider.finology.in/economy/semiconductor-industry-in-india

12 В рамках правительственной инициативы 2015 года по развитию вычислительных мощностей правительство Индии выделило 45 млрд рупий (более 630 млн долл. США) на строительство 40-60 суперкомпьютеров общей

занимает второе место после Китая по производству смартфонов и планирует в ближайшее время стать лидером не только в этом сегменте, но и в производстве электроники в целом [4].

Обладая очень значительным ресурсом для разработки ПО, Индия активно развивает цифровую экономику, которая по прогнозам может обеспечить 18–23% ВВП Индии к 2025 году, т.е. порядка 0,8–1 трлн долл. США. Одним из ее компонентов является электронная торговля, которая развивается огромными темпами[13] благодаря совершенствованию инфраструктуры доставки товаров, росту проникновения Интернет в сельские районы и увеличению доли платежей через электронные кошельки, доступные для молодежи через смартфоны без открытия банковского счета [5]. Основными площадками электронной торговли являются зарубежные платформы (Amazon, eBay, Alibaba), однако быстро растет доля индийских компаний (FSN e-Commerce Ventures Limited (Nykaa), Flipkart Private Limited), сервисы которых доступны через интерфейсы на местных языках. Активно развивается и другой сектор цифровой экономики — цифровая медицина. Объем рынка ее услуг в 2021 году достиг 195 млрд долл. США и по оценкам продолжит ежегодно расти на 16% в периоде 2022–30 гг.

Благодаря выгодному географическому положению в Южной Азии Индия в настоящее время является важным узлом глобальной сети Интернет. Несколько международных подводных кабельных систем имеют точки обмена трафиком в пяти крупных городах — Кочин, Тривендрум, Тутикорин и Ченнаи, а Мумбаи, в свою очередь, подключен к 9 межконтинентальным кабельным системам. В Глобальном индексе сетевой готовности 2020 [6], который рассчитывается МСЭ на основе показателей из 4 групп[14], Индия поднялась на 6 позиций вверх и заняла 61 место. При этом достигнуты следующие показатели: 2 место по трафику мобильного широкополосного Интернета внутри страны и пропускной способности международного трафика, 3 место по ежегодным инвестициям в телекоммуникационные услуги и размеру внутреннего рынка, 4 место по экспорту услуг ИКТ, 5 место по научным публикациям в области искусственного интеллекта.

Из года в год неравномерность географического распределения ИКТ-инфраструктуры снижается, но пока сохраняются проблемы с ее доступностью в сельских районах и значительным гендерным неравенством. В силу низкого уровня достатка, всего 11% домохозяйств могут позволить себе компьютеры, из них

производительностью 70 петафлопс. В 2023 году правительство заявило о введенных в эксплуатацию 28 высокопроизводительных вычислительных комплексах, развернутых в рамках Национальной миссии в области суперкомпьютеров. Эксперты признают, что индийские суперкомпьютеры сильно отстают от уровня передовых международных разработок из-за отсутствия инфраструктуры для производства компонентов.

13 По данным Unicommerce в 2023 году объем рынка онлайн-торговли Индии демонстрирует рост 26,2%. Источник: DFU Publications, 16.08.2023, https://www.dfupublications.com/news/trade/india-e-commerce-26-2-yoy-growth

14 Индекс рассчитывается по 4 показателям: технологической составляющей, человеческому фактору, управленческому навыку, влиянию на экономику и государство.

только 70,4 тыс. имеют широкополосные подключения [7]. Подавляющая доля пользователей для доступа к глобальной сети использует смартфоны (91,3%)[15], почти по всей стране доступны сети подвижной связи 4G, обеспечивающие полноценное использование сервисов Интернет. Постепенно внедряются сети и услуги 5G, на конец января 2023 года они запущены в 238 городах. Ожидается, что к 2025 году в Индии будет 920 млн уникальных мобильных абонентов, включая 88 млн подключений 5G [8].

Темпы повышения доступности сетевых услуг в Индии впечатляют: в 2018 году уровень проникновения Интернета был всего 31%[16], а на начало 2023 года — уже 48,7%, что в абсолютном выражении составляет 692 млн человек [9] (второе место после Китая). Однако с учетом численности населения, это существенно ниже среднемирового показателя, составляющего 67,9%. Миллионы людей в Индии не имеют доступа к Интернету из-за бедности или отсутствия электричества.

Предоставление электронных государственных услуг осуществляется преимущественно через мобильные приложения. Ключевым элементом доступа к ним является национальная система биометрической идентификации Aadhaar (в переводе с санскрита — основа/фундамент), ею охвачено 99% населения. По состоянию на конец 2022 года 36 штатов и союзных территорий Индии предоставляли для физических и юридических лиц более 12,3 тыс. государственных услуг. Несмотря на это, согласно Индексу развития электронного правительства ООН 2022 года, Индия заняла 105 место, что вызвано неравномерным развитием ИКТ-инфраструктуры и качеством сервисов, а также невозможностью доступа к ним значительной доли населения [10].

В условиях перехода к Индустрии 4.0 и быстрого развития геополитической динамики государству крайне важно активизировать свои усилия в развитии и управлении инфраструктурой, поддержке цепочек поставок ИКТ-продуктов, наращивании уровня образования и подготовки кадров, обеспечении трансграничной передачи данных и информационной безопасности.

В Глобальном индексе кибербезопасности МСЭ 2020 года[17] Индия расположилась на 10 позиции [11], в основном благодаря эффективности национальных компаний в сфере кибербезопасности[18] и практически удвоению этого сегмента рынка на фоне пандемии COVID [12]. В период 2019–2021 гг. национальная

15 По данным правительства, в конце 2022 года число владельцев смартфонов составило 600 млн, по прогнозам, к 2026 году этот показатель превысит 1 млрд чел.

16 Показатель равен соотношению пользователей сети Интернет внутри страны к ее населению.

17 Global Cybersecurity Index вычисляется по нескольким параметрам в 5 группах: развитие правовой системы обеспечения информационной безопасности; применение технических и организационных мер; реализация программ наращивания потенциала; участие в международном сотрудничестве.

18 Наиболее значимые компании — Infosys, Wipro и Tata Consultancy Services. В целом, в национальной индустрии информационной безопасности занято более 100 тыс. специалистов. Индия является одним из мировых лидеров в этой сфере.

индустрия кибербезопасности выросла с 5,04 до 9,85 млрд долл. США. Защита информационных систем и ресурсов стала приоритетом не только для технологических компаний, но и для предпринимателей, государственных органов и частных лиц. В результате количество специалистов в сфере кибербезопасности увеличилось со 110 тыс. человек в 2019 году до 218 тыс. в 2021 году, но все равно их нехватку ощущают более 49% респондентов опроса State of Cybersecurity 2021. Общий дефицит индийских кадров в этой сфере на 9% выше, чем в среднем по миру [13]. Правительство Индии сотрудничает со специалистами из США, Великобритании и Франции для повышения осведомленности о киберугрозах и обеспечения необходимых мер защиты.

Уровень киберпреступности в стране постоянно растет. Наиболее распространенными правонарушениями являются онлайн-мошенничество, взломы ресурсов, фишинг, кража персональных данных, кроме того Индия — мировой «лидер» по распространению детской порнографии.

Среди причин сложившейся ситуации — отсутствие в стране нормативных требований по внедрению компаниями политик информационной безопасности. Всего 30% коммерческих организаций имеют стратегии кибербезопасности и только 12% обладают ресурсом для реагирования на компьютерные инциденты, что приводит к серьезным последствиям. Так, в 2019 году были совершены успешные атаки на АЭС «Куданкулам» и штаб-квартиру Индийской организации космических исследований в штате Карнатака, в 2020 году — отключена энергосистема Мумбаи и страна заняла второе место в мире по поражению вирусами-шифровальщиками (82% индийских компаний подверглись заражению) [14], в 2022 году взломана государственная система мониторинга наводнений в Гоа (часть системы гражданской обороны). Ответственность за некоторые вредоносные атаки была возложена на КНР, в связи с чем в Индии были заблокированы 117 китайских мобильных приложений [15].

2. О стратегическом планировании в области цифровизации и информационной безопасности Индии

Особенностью национальной системы стратегического планирования в рассматриваемой сфере является отказ правительства Н. Моди от директивного (пятилетнего) планирования и переход к программам развития. Их разработкой занимается созданный в 2015 году и возглавляемый премьер-министром аналитический центр при правительстве — Национальный институт трансформации Индии (NITI Aayog). Его функции состоят в определении приоритетов развития экономики, обеспечении соблюдения интересов национальной безопасности, контроле над осуществлением экономической деятельности, создании системы поддержки зна-

ний, повышении качества управленческих практик, оценке реализации государственных программ и наращивании технологического потенциала [16].

NITI Aayog разработал широкий спектр программ развития напрямую касающихся ИКТ-отрасли. Они будут рассмотрены ниже, но начать следует со стратегии, которая радикальным образом изменила вовлеченность страны в цифровую экономику.

2.1. **Национальный план электронного правительства** (2006)

Первые попытки автоматизации в области государственного управления в Индии пришлись на 1990-е годы, а уже в 2005 году был разработан первый портал электронного правительства. Национальный план электронного правительства (NeGP), направленный на улучшение доступности государственных услуг для граждан и бизнеса, был принят в 2006 году. NeGP включал 31 проект по отдельным сферам госуправления (регистрацию фермерских хозяйств, реестр земельных участков, здравоохранение, образование, оформление паспорта, полиция, суды, администрирование муниципалитетами, налоги и казначейство).

Актуальность унификации и централизации системы госуслуг диктовалась необходимостью преодоления бедности и социального неравенства[19]. В 2009 году запущена платформа цифровой идентификации граждан на основе биометрических данных **Aadhaar** [20]. На ее внедрение ушло 3 года противодействия законодательному лобби, но благодаря Aadhaar удалось навести порядок в предоставлении социальной помощи (например, в период 2012–14 гг. избавились от 1,5 млн поддельных продуктовых карточек) и сэкономить государству около 5 млрд долл. США.

На базе Aadhaar создан целый набор национальных цифровых услуг India Stack[21], построенных на общих принципах: обязательная интеграция, предоставление инфраструктуры по запросу, облачные технологии, локализация для улучшения территориального управления. Из требований информационной безопасности для них следует отметить защиту данных, использование ПО с открытым кодом, строгое следование национальным стандартам и протоколам в области разработки ПО[22].

В India Stack входят: система электронной подписи eSign для совершения юридически значимых действий и проверки подлинности цифровых докумен-

---

19 В 2009–2010 гг. за чертой бедности жило около 30% населения страны (380 млн индусов), многие из которых не имели даже свидетельств о рождении, только 20% обладали банковскими счетами. Подавляющая часть пособий по бедности выдавалась «на руки», что приводило к колоссальной коррупции.

20 Биометрическая идентификация с учетом 10 шаблонов (отпечатков пальцев, радужек глаз, фотографии и других данных).

21 В настоящее время в Индии работает 70 государственных ИТ-систем, которые оказывают услуги населению и компаниям. Около 20 систем предназначено фермерам, поскольку 60% населения Индии занято в сельском хозяйстве, Источник: https://cdo2day.ru/practice/atmanirbhar-bharat-ili-nezavisimaja-cifrovaja-indija/

22 Доступ иностранных компаний к проектам NeGP строго регламентирован.

тов; облачное хранилище DigiLocker для размещения и сертификации цифровых документов любого Aadhaar-пользователя; система быстрых платежей UPI, разработанная и введённая в эксплуатацию в 2016 году Резервным банком Индии совместно с Ассоциацией индийских банков; система безналичных расчетов BHIM; система электронной идентификации клиентов e-KYC; платформа электронных госзакупок; единая цифровая налоговая система, распространенная на все штаты, ранее имевшие индивидуальные налоговые правила. Все эти цифровые механизмы работают через программный интерфейс приложений (API), что позволяет бизнесу эффективно встраивать их элементы в свою работу [17].

Простота и дешевизна Aadhaar и функциональность India Stack представляют большой интерес для других стран, многие из которых выразили намерение использовать индийский опыт[23]. Успех архитектуры Aadhaar привёл к разработке модульной платформы идентификации с открытым исходным кодом MOSIP[24], которая в настоящее время продвигается и предоставляется бесплатно Международным институтом информационных технологий в Бангалоре при поддержке ряда известных спонсоров[25].

С помощью Aadhaar государство значительно повысило доступность, прозрачность и точность предоставления общественных благ, пресекло коррупцию, стимулировало разработку приложений для цифровой экономики. Однако, некоторые эксперты подчеркивают добровольно-принудительный характер участия в системе: например, без регистрации в ней нельзя получить субсидии и льготы, сдать экзамены для поступления на престижные специальности (медицинские и инженерные). Есть вопросы к обеспечению информационной безопасности Aadhaar, что способствует различным инцидентам, в частности в 2017 году платформа была взломана [18].

2.2. **Программа «Цифровая Индия»** (2015)

Программа является флагманским проектом правительства по повышению качества жизни граждан, курируется лично премьер-министром Н. Моди[26].

---

23 Интерес проявили более 20 стран, среди них Афганистан, Бангладеш, Марокко, Филиппины, Эфиопия, Гвинея, Шри-Ланка, Кот-д'Ивуар, Того, Руанда, Тунис и Сингапур. Источник: https://www.skolkovo.ru/researches/india-goes-digital-from-local-phenomenon-to-global-influencer-2/

24 Сайт проекта MOSIP http://www.mosip.io

25 Среди спонсоров указаны: Omidyar Network, Фонд Билла и Мелинды Гейтс и Sir Ratan Tata Trust.

26 Ключевую роль в развитии инфраструктуры связи и сетей доступа сыграла корпорация Reliance Jio Infocomm Limited, созданная индийским нефтяным магнатом Мукешем Амбани. Она за шесть лет (2010-16) охватила мобильными сетями 4G практически 99% территории страны, а также снизила в 20 раз тарифы, разработала и предоставила в пользование дешевый кнопочный смартфон, что моментально увеличило клиентскую базу на 150 млн чел. В настоящее время компания Jio превратилась в мощную цифровую платформу, практически полностью монополизировав рынок (осталось два крупных оператора связи, которые выживают за счет отсрочек налоговых платежей и масштабных инвестиций со стороны иностранных акционеров), однако антимонопольное

Она разработана и реализуется под руководством Министерства электроники и информационных технологий в целях развития производственного потенциала страны и включает несколько ключевых инициатив в сфере ИКТ:

- развитие широкополосной инфраструктуры для высокоскоростного доступа к сети Интернет в любой точке страны. Для достижения этой цели запущено несколько проектов, включая создание за счёт государственно-частного партнерства Национальной оптоволоконной сети (NOFN) и 1,5 млн бесплатных точек беспроводного доступа (Wi-Fi) в общественных местах;
- обеспечение доступа к мобильным сетям, особенно в сельских и труднодоступных районах, в центрах обслуживания населения и почтовых отделениях Индии;
- электронное управление: реформа правительства посредством цифровых технологий (рассмотрено в Разделе 2.2);
- цифровая революция: развитие сервиса e-Kranti по предоставлению электронных услуг в сфере здравоохранения, образования, сельского хозяйства, юстиции, безопасности, финансовой инклюзивности и др.;
- информация для всех: за счет развития платформы открытых данных и предоставления доступа к государственным наборам больших данных, использования социальных сетей для управления, создания доступной для всех пользователей облачной системы кибербезопасности;
- собственное производство электроники, что отражает цель отказа от импортного сетевого оборудования (NET ZERO Imports);
- ИТ для повышения занятости[27] за счет цифровизации отраслей экономики, повышения цифровой грамотности и обучения молодых людей навыкам, необходимым в ИТ-сфере и смежных отраслях[28].

Благодаря комплексному решению указанных задач Индия всего за несколько лет совершила качественный скачок по многим направлениям цифровизации, уступая по скорости этого процесса только Индонезии. В силу «позднего старта» национальная ИКТ-инфраструктура «перепрыгнула» этапы развертывания сетей 2G/3G, на которые в других странах были потрачены годы, и сразу стала

законодательство к Jio не применяется, несмотря на значительную долю участия в ней иностранного капитала (в 2020 году Facebook и Google согласились совместно инвестировать в Reliance Jio Infocomm Limited более 10 млрд долл. США). Источник: https://digitalindia.gov.in/

27 Занятость — крайне актуальный вопрос для Индии: средний медианный возраст в 2023 году составил 27 лет, и ежегодно нужно создавать примерно 12 млн рабочих мест.

28 По государственной программе развития навыков (PMKVY) разные уровни повышения квалификации прошли 10 млн человек. В бюджете Индии на 2023-24 финансовые годы указано, что в течение трех лет планируется запустить четвертый этап PMKVY для подготовки кадров в сферах ИИ, робототехники, интернета вещей, 3D-печати и отраслях Индустрии 4.0, а также предложено создать 30 международных центров развития навыков Skill India и новые программы стажировок для 4,7 млн индийцев.
Источник: https://russiancouncil.ru/activity/workingpapers/tekhnologicheskaya-politika-indii/

формироваться на основе сетей связи 4G/5G. Также значительная часть населения страны пропустила этап внедрения привязанных к банковским счетам кредитных карт и сразу получила доступ к государственным услугам, цифровым платформам и финансовым технологиям со смартфонов, тем самым многократно увеличив в индийском обществе финансовую инклюзивность и финтех-развитие. Аналогичная ситуация сложилась с доступом к образованию и медицинским услугам.

В 2023 году программа «Цифровая Индия» была расширена, на ее мероприятия до 2026 года выделено 149 млрд рупий (около 1,79 млрд долл. США) [19]. Часть этих средств будет потрачена на обучение и повышение квалификации приблизительно 625 тыс. ИТ-специалистов, а также подготовку 265 тыс. профессионалов в сфере информационной безопасности. Будет оказано содействие примерно 1,2 тыс. начинающих компаний в ИТ-сфере. Планируется сделать доступными дополнительно 540 новых сервисов в приложении для предоставления госуслуг Umang (в дополнение к действовавшим в августе 2023 года более, чем 1,7 тыс. сервисов). Кроме того, будет повышена их доступность в мобильном приложении Bhashini для граждан-носителей 22 местных языков за счет включения поддержки интерфейсов для еще 12 из них.

Программа «Цифровая Индия» детализирована другими инициативами правительства. Например, **«Делай в Индии»** (2014) по развитию производства в 25 ключевых отраслях экономики или инициатива поддержки начинающих компаний **Startup India** (2016), включающая меры по ослаблению налоговой нагрузки и упрощению некоторых административных процедур.

2.3. Программа развития экосистемы производства микроэлектроники (2021)

Программа Design Linked Incentive (DLI) Scheme [20] является одним из компонентов стратегии «Самодостаточная Индия» и ставит задачу снижения объема импорта микроэлектроники. Она включает не только содействие строительству двух новых заводов для производства чипов[29], но и финансирование национальной экосистемы их разработки, усиление роли стартапов и малых предприятий в следующих сферах: компоненты, фотоника, сенсоры, тестирование, маркировка. Планируется реализация трех проектов стоимостью 31,6 млн долл. США для создания кластеров производства микросхем, но требования индийцев полной локализации всей цепочки поставок пока не позволяют сформировать консорциум из инвесторов и зарубежных технологических компаний. Кроме того, плани-

29 Сначала речь шла о технологиях 28-нм, после корректировки схемы финансирования проект сместился в сторону 40-нм техпроцесса.

руется создать Национальный институт электроники и информационных технологий в северных штатах страны, т.е. более равномерно территориально распределить инновационные производства.

2.4. Проект Национальной стратегии по искусственному интеллекту

Проект стратегии по искусственному интеллекту для всех (#AIforAll) по поручению правительства был разработан NITI Aayog в 2018 году [21]. Главная его цель — использование технологий искусственного интеллекта (ИИ) для социального преобразования жизни граждан за счет улучшения здравоохранения, сельского хозяйства, образования, развития «умных» городов и инфраструктуры, мобильности и транспорта. В этих целях планируется усилить исследования, подготовить кадры по инновационным специальностям, ускорить внедрение технологий ИИ во все сферы жизнедеятельности, укрепить безопасность, защиту частной жизни и этических принципов. В проекте даны анализ имеющихся проблем достижения этих целей и предложения правительству по их преодолению.

Однако данные о принятии документа отсутствуют, несмотря на то, что страна оценивается в Индо-Тихоокеанском регионе как наиболее подготовленная к использованию указанной технологии после Сингапура и Гонконга [22] и, как уже было отмечено, имеет развитую исследовательскую базу. По использованию приложений ИИ в промышленности Индия уступает только США и КНР. В настоящее время отдельные компоненты стратегии внедряются в рамках реализации государственных услуг, а также развиваются бизнесом и научным сообществом. В частности, Индийский институт технологий сотрудничает с американской Nvidia в создании первого в стране центра технологий искусственного интеллекта для ускорения исследований и трансфера их результатов в реальный сектор (сельское хозяйство, «умные» города, распознавание естественных языков и др.).

Реализация правительством Индии широкого спектра программ стратегического развития в сфере ИКТ свидетельствует о наличии политической воли для решения с их помощью внутри- и внешнеэкономических задач. В то же время, по мнению экспертов, детально анализирующих выполнение этих планов, ни один из них не реализован в полном объеме. На это есть как внешние причины (например, спад внешнеэкономической деятельности из-за COVID, обострение отношений с КНР), так и внутренние — прежде всего нерешенность инфраструктурных проблем: отсутствие стабильного доступа к электричеству и воде, низкий уровень развития транспортной инфраструктуры. Кроме того, иностранные компании при входе на индийский рынок сталкиваются с местной спецификой – коррупцией, бюрократической волокитой, низкой покупательной способностью

и дефицитом качественных трудовых ресурсов [23]. По этим причинам буксуют локализация производства на территории Индии и миграция в страну мощностей ведущих мировых корпораций из КНР.

2.5. **Национальная политика кибербезопасности** (2013)

Многие западные эксперты отмечают, что довольно продолжительное время обеспечение информационной безопасности не считалось приоритетным направлением государственной политики Индии. Профильные подразделения в правительственных ведомствах и государственных организациях, а также в частных фирмах комплектовались по остаточному принципу. При отсутствии необходимых специалистов многие ведомства передавали обеспечение своей информационной безопасности на аутсорсинг, привлекали зарубежные компании, в том числе американские. Толчком к радикальному пересмотру государственной политики стали вскрытые Э. Сноуденом факты электронного шпионажа США в государственном и частном секторах Индии. Были начаты работы по сокращению импорта ПО для оборонных задач, переходу на отечественные разработки, проектированию и производству собственных микропроцессоров.

Национальная политика кибербезопасности, опубликованная в 2013 году, является первым доктринальным документом, описывающим видение приоритетов политики Индии в обеспечении кибербезопасности государственного сектора, бизнеса и простых граждан. Политика разработана Министерством технологий и электроники и **считается на текущий момент стратегией кибербезопасности страны**.

Среди основных ее целей по обеспечению безопасного и устойчивого киберпространства указаны: укрепление регуляторной системы для повышения надежности; создание и функционирование на национальном и отраслевом уровнях системы мониторинга 24×7 угроз информационной безопасности; круглосуточное функционирование ядра экосистемы кибербезопасности — Национального центра защиты критической информационной инфраструктуры (см. Раздел 4.5); наращивание кадрового потенциала и подготовка к 2018 году 500 тыс. необходимых специалистов, а также укрепление международного сотрудничества.

В качестве основных инструментов политики указаны: укрепление нормативной базы, повышение возможностей в разработке необходимых технологий и открытых стандартов кибербезопасности, создание инфраструктуры для тестирования и проверки безопасности ИТ-продуктов, развитие механизмов получения информации об угрозах безопасности и разработка планов реагирования на национальном и отраслевом уровнях, осуществление НИОКР, расширение воз-

можностей правоохранительных органов для расследования и судебного преследования киберпреступности, формирование культуры информационной безопасности и осведомленности граждан, наращивание кадрового потенциала, а также укрепление международного взаимодействия [24].

Помимо этого, Стратегия призвала к созданию центрального уполномоченного государственного органа, ответственного за ее реализацию и координацию всей деятельности по вопросам кибербезопасности Индии, что до сих пор не реализовано.

2.6. Руководящие принципы реализации Национальной политики кибербезопасности (2018)

Документ (версия 5.0) разработан Министерством внутренних дел в 2018 году для государственного сектора. Он касается повышения сетевой безопасности, улучшения управления доступом и идентификацией, обеспечения физической безопасности, защиты данных, надежности и безопасности приложений, управления угрозами и инцидентами компьютерной безопасности.

2.7. Проект Стратегии кибербезопасности (2020)

В ноябре 2020 года для общественного обсуждения был предложен разработанный правительством проект Стратегии кибербезопасности Индии [25], который пока не принят. Документ помимо традиционных компонентов национальной политики касается безопасности передовых технологий (5G, Интернета вещей и др.) и национальной безопасности. Ожидается, что его реализация даст возможность успешнее бороться с компьютерными атаками за счет улучшения межведомственной координации и оптимизации расходов на обеспечение информационной безопасности.

2.8. Руководящий документ по обеспечению безопасности критических информационных инфраструктур

В июне 2023 года правительство завершило подготовку проекта указанного документа (National Cybersecurity Reference Framework, NCRF [26]), который планируется опубликовать для общественного обсуждения.

2.9. Документы в области военного планирования

Очень контрастно на фоне долгих согласований доктринальных документов в гражданской сфере выглядит комплексное развитие стратегического планирования в военной сфере и расширение спектра задач вооруженных сил Индии в киберпространстве, что говорит о приоритетах государства.

Объединенная стратегия армии Индии (2004)

Стратегия определяет кибер- и информационную сферы серьезными вызовами безопасности. Большой раздел документа касается развития национальных возможностей в сфере информационной войны.

Базовая доктрина ВВС Индии (2012)

В документе признается, что ведение кибервойны является самой незатратной моделью вооруженного конфликта, а для достижения национальных целей наступательные кибероперации могут проводиться как в военной, так и гражданской инфраструктуре. Согласно доктрине, развитие подготовки к двум компонентам действий ВВС в киберпространстве — кибервойне и информационной войне — следует проводить независимо.

Доктрина сухопутных войск Индии (2018)

Документ определяет войну в киберпространстве как подкатегорию информационной войны и компонент гибридной войны, и ставит задачу развития потенциала выполнения операций информационной войны во «всем спектре конфликта». Подчеркивается, что все силы/средства должны сохранять возможность действовать с помощью разрушительных возможностей в киберсреде, а индийская армия будет обновлять свой потенциал в сфере ведения кибервойны. В 2019 году создано Агентство киберзащиты, которое является ключевым звеном управления и контроля возможностей вооруженных сил Индии в этой сфере.

3. Состояние нормативно-правовой базы в сфере обеспечения информационной безопасности

Уровень зрелости правового регулирования цифровизации в Индии по новой методике оценки МСЭ[30] оценивается как «лидирующий», однако согласо-

30 В методике «G5 Benchmark» оцениваются 4 параметра: межотраслевое управление на национальном уровне, принципы разработки политик, Инструментарий цифрового развития (кибербезопасность, защита данных, телекоммуникации в чрезвычайных ситуациях и совместное использование межотраслевой инфраструктуры), повестка дня в области цифровой экономики (инновационная система, цифровая трансформация, участие в международных и региональных интеграционных инициативах). Источник: Benchmark for Fifth

вание новых законопроектов и поправок в действующие правовые нормы из-за сложных бюрократических процедур требует не одного года, поэтому обновление законодательной базы идет крайне медленно.

3.1. **Закон об информационных технологиях** (2000)

Этот комплексный нормативный акт в сфере использования ИКТ и обеспечения их безопасности принят в 2000 году. Он регулирует широкий спектр правоотношений, касающихся обработки и защиты персональных данных, юридической значимости использования электронных документов, цифровой подписи и электронных сертификатов, функционирования системы удостоверяющих центров для применения цифровых подписей в государственном секторе и бизнесе, а также определяет систему контроля соблюдения собственных норм и разработки подзаконных актов. Несколько глав закона касаются деятельности апелляционного суда, различных видов компьютерных преступлений и полномочий правоохранительных органов по их расследованию и осуществлению правосудия, в связи с чем, указанным законом внесены поправки в уголовный кодекс Республики Индия и ряд других законодательных актов.

Положения закона по необходимости редактируются. Наиболее существенные правки сделаны в 2008 году, когда было введено понятие «критические информационные инфраструктуры» (КИИ)[31] и определены требования к их безопасности, а также осуществлена кодификация кибертерроризма (карается пожизненным заключением). Правительственным агентствам в сфере безопасности и разведки в интересах обеспечения национальной безопасности были даны широкие полномочия по проведению законного перехвата, мониторинга и расшифровки любой информации, размещенной, передаваемой, генерируемой или получаемой любым компьютерным ресурсом (статья 69b). Кроме того, центральному правительству рекомендовано разработать и утвердить Национальную политику в сфере использования криптографии (статья 84a), что не сделано до сих пор, хотя в 2015 проект соответствующего закона был предложен.

Поправками 2008 года центральному правительству и штатам дано право выдавать распоряжения на блокирование доступа к услугам сети Интернет в интересах защиты суверенитета, территориальной целостности и безопасности

Generation Digital Collaborative Regulation/ G5 Benchmark, ITU, https://app.gen5.digital/benchmark/metrics?_ga=2.182559078.1565902013.1702625730-1451289763.1702625730&_gl=1*1ql4cot*_ga*MTQ1MTI4OTc2My4xNzAyNjI1NzMw*_ga_27GW57NRWK*MTcwMjYyODA3NS4xLjAuMTcwMjYyODA3NS4wLjAuMA..*_ga_6J744FX7L2*MTcwMjYyODA3Ni4xLjAuMTcwMjYyODA3Ni4wLjAuMA

31 Закон к КИИ относит 12 секторов, в том числе, генерацию и транспортировку электроэнергии; финансовую, банковскую и страховую деятельность, транспорт, телекоммуникации, государственное управление и электронное правительство; государственные предприятия и стратегические производство, оборону, правоохранительную деятельность, водоснабжение.

Индии, ее международных отношений или в целях предупреждения побуждения к совершению соответствующих правонарушений, включая акты терроризма (статья 69а). В августе 2017 года был опубликован подзаконный акт, определяющий полномочия должностных лиц по блокировке доступа к сети в случае чрезвычайных ситуаций или угрозы общественной безопасности [27]. По использованию указанного права Индия стоит на первом месте в мире [28].

Другой подзаконный акт — **Руководящие принципы для посредников и кодекс этики цифровых медиа** (2021) — изменил правила деятельности онлайн-платформ [29]. Ранее интернет-посредники были освобождены от ответственности за содержание информации, размещаемой на их ресурсах третьими лицами. Теперь они обязаны реализовывать политики контроля содержания контента и оказывать содействие государственным органам в расследовании компьютерных преступлений. В частности, при выявлении противоправного контента, размещенного индийскими гражданами (в том числе богохульного, экстремистского, эротического и порнографического содержания), онлайн-платформы или провайдеры доступа к услугам должны его сразу блокировать и в течение 24 часов с момента получения требования властей удалить его. Более того, крупные онлайн-платформы (более 5 млн пользователей) обязаны назначить контактное лицо, которое 24×7 будет доступно для связи с представителями правоохранительных органов в целях координации совместных действий. Указанные требования носят экстерриториальный характер, т.е. относятся ко всем компаниям, предоставляющим услуги на территории Индии[32].

3.2. **Закон о защите цифровых персональных данных** (2023)

Правила безопасного обращения с персональными данными (ПД) или конфиденциальной информацией, содержащей такие данные, впервые были определены подзаконным актом 2011 года [30]. Накопление правоприменительной практики, а также обобщение международного опыта дало возможность подготовить полноценный закон. Проект нормативного акта о защите ПД был разработан Министерством электроники и информационных технологий в 2018 году [31]. Он во многом опирался на положения Общего регламента защиты данных ЕС (GDPR), однако отражал национальную политику по повышению вовлеченности Индии в трансграничную передачу данных. В частности, проект предлагал: смягчить

32 Самой популярной социальной сетью в Индии является Facebook, она приняла предложенные экстерриториальные правила, поскольку это ее самый крупный национальный рынок. Компания Twitter дважды проигнорировала обращение индийских властей, после чего была лишена иммунитета. Верховный суд рассмотрел иск Министерства информационных технологий Индии к Twitter, и последняя согласилась исполнять новые национальные требования и включить в штат двух государственных представителей для контроля за их выполнением.

ограничения на локализацию и передачу данных; расширить область влияния на анонимные и «неличные» данные; внести корректировку правовых оснований для обработки данных; разработать новую политику конфиденциальности; смягчить уголовные наказания; расширить права личности; создать экспериментальную правовую «песочницу» для поощрения исследований и разработки новых технологий в области кибербезопасности.

В августе 2023 года после 5 лет согласований и многочисленных изменений проекта Н. Моди подписал закон «О защите цифровых персональных данных» (DPDPA) [32], который ввел права и обязанности «цифрового гражданина» в рамках Принципов обработки данных, требования к операторам обработки ПД, ввел локализацию обработки ПД на территории страны и оговорил право центрального правительства ограничить трансграничную передачу данных. Закон определил полномочия и функции независимого Совета по защите данных Индии, а также кодифицировал нарушения правил обработки ПД.

3.3. **Проект закона о цифровых валютах** (2021)

Активное развитие национального рынка криптовалют вызвало необходимость введения его правового регулирования. В связи с этим большие надежды возлагались G20 на выработку согласованных правил оборота криптовалют в рамках индийского председательства в 2023 году, однако этого не произошло. Положения проекта закона о цифровых валютах однозначно свидетельствуют, что правительство настороженно относится к номинированным в долларах США частным криптовалютам и рассматривает их как подрыв финансовой системы страны, в том числе как инструмент отмывания денег. В связи с этим Индией введен драконовский налог на прибыль от продажи криптовалют (30%), запрещен их майнинг и оборот. При этом законопроект создает условия для выпуска и использования цифровой валюты национального банка (цифровой рупии). С декабря 2022 года в стране осуществляются пилотные проекты по использованию цифровой валюты в розничной и оптовой торговле [33].

4. Основные государственные структуры, участвующие в обеспечении национальной информационной безопасности

Каркас национальной системы обеспечения информационной безопасности Индии сформирован более 10 лет назад на основе рассмотренных выше документов стратегического планирования и нормативной базы. По оценке Международного института стратегических исследований, впоследствии Индия сделала важные шаги по его укреплению, однако в формировании широкого и всеобъем-

лющего подхода сохраняются пробелы и дисбаланс в федеральной политической структуре.

Одной из ключевых проблем является отсутствие единого органа, отвечающего за разработку и реализацию национальной политики кибербезопасности, хотя деятельность государственных структур в рассматриваемой сфере в значительной степени централизована. Негативное воздействие на эффективность предпринимаемых усилий оказывают пересечение полномочий и бюрократические войны за сферы влияния.

В 2010 году была проведена переконфигурация подчиненных премьер-министру структур, отвечающих за выработку государственной политики в сфере безопасности [34], в результате чего **Правительственный комитет по безопасности** (CCS)[33] стал головной организацией, а **Национальный совет безопасности** (NSC)[34] сконцентрировался на обобщении позиций государственных ведомств, бизнеса, научных и экспертных сообществ для выработки согласованных предложений по насущным вопросам внешней и внутренней политики, в том числе по обеспечению национальной информационной безопасности. Для этого в состав Секретариата NSC входит **национальный координатор по вопросам кибербезопасности**[35], который отвечает за межведомственное взаимодействие в указанной сфере и одновременно возглавляет федеральное агентство, обеспечивающее функционирование национальной системы реагирования на угрозы кибербезопасности — Национальный центр координации кибербезопасности (NCCC) (см. Раздел 4.2).

Указанные выше структуры и остальные органы управления национальной информационной безопасностью связаны между собой защищенной системой обмена данными (см. схему).

4.1. Кабинет премьер-министра

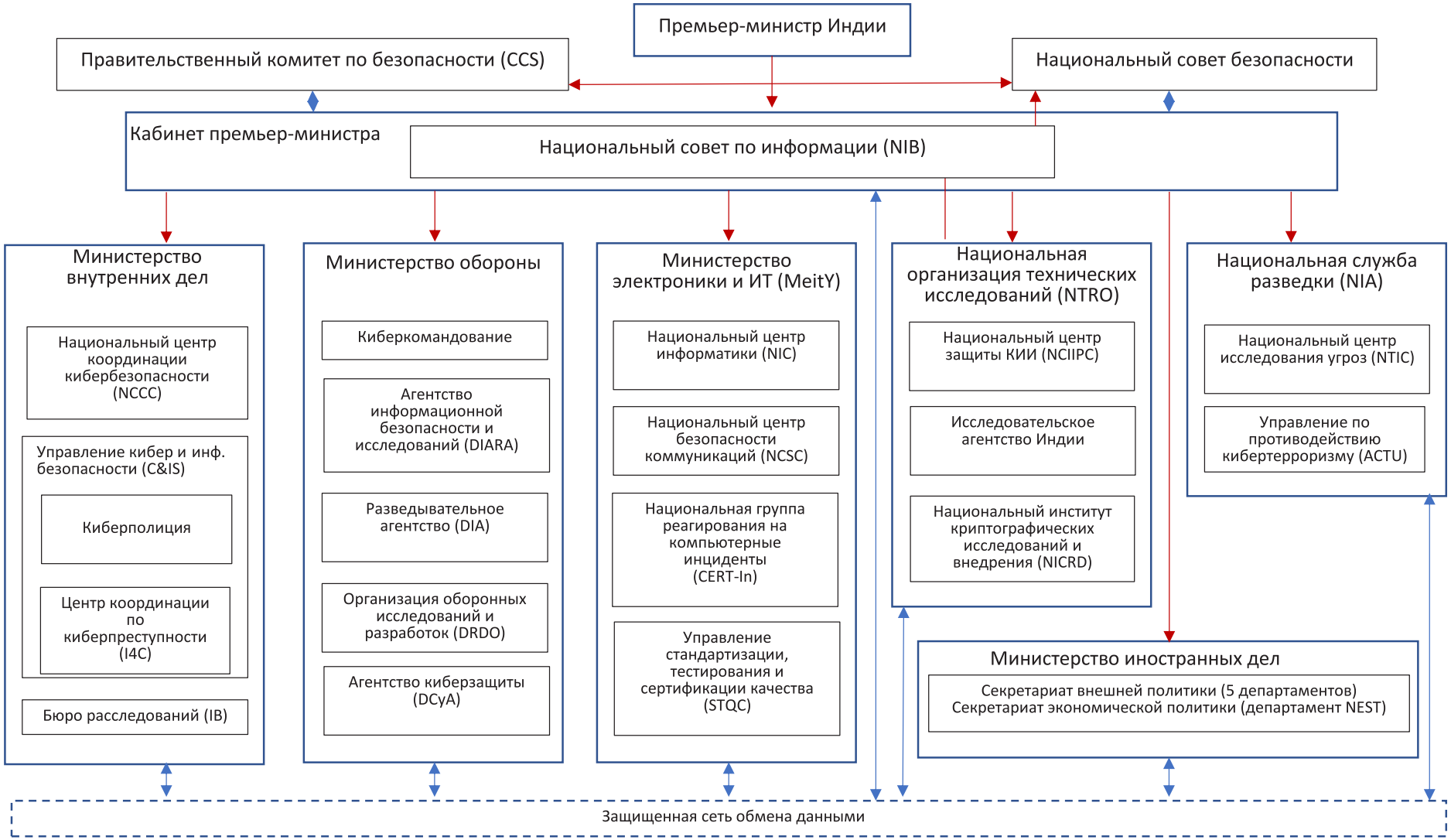
Кабинет премьер-министра состоит из 20 ключевых министров, прежде всего силового блока, и решает все важные вопросы государственной полити-

33 Комитет возглавляет премьер-министр, по должности в состав входят его советник по безопасности (NSA), секретарь Правительственного комитета по безопасности (CCS), министры обороны, внутренних дел, финансов, иностранных дел.

34 Межведомственный консультативный орган, действующий с 1998 года, в него входят премьер-министр, его советник по безопасности (NSA) в ранге члена правительства, являющийся секретарем Правительственного комитета по безопасности (CCS), секретарь Кабинета премьер-министра, командующие трех родов войск, главы Бюро расследований (IB) и Контрразведки (RAW), министры внутренней безопасности и обороны, глава Организации по исследованиям и внедрению МО Индии (DRDO) и приглашенные члены. Секретариат Совета национальной безопасности (NSCS) является исполнительным органом и обеспечивает межведомственное взаимодействие силовых структур и гражданских ведомств по вопросам кибербезопасности и управления Интернетом.

35 Эта должность введена в 2015 году в Кабинете премьер-министра, по рангу приравнивается к министру, в настоящее время ее занимает генерал-лейтенант (в отставке) Раджеш Пант.

Схема. Основные элементы системы управления информационной безопасностью ИранаИспользованная литература



ки и управления страной. Его возглавляет советник премьер-министра по безопасности (NSA), который имеет четырех заместителей (DyNSA), отвечающих за следующие направления: внутренние дела[36], оборона[37], финансы и внешняя политика.

В 2002 году в структуре Кабинета создан **Национальный совет по информации** (National Information Board, NIB), именно он является высшим органом, формирующим политику в области кибербезопасности. Акцент в деятельности NIB делается на кибер- и информационной безопасности отрасли телекоммуникаций (включая сети подвижной связи), которая в существенной степени зависит от иностранных технологий. Возглавляет NIB советник премьер-министра по безопасности, в состав входят 21 член, большинство из которых являются «силовиками». Совет периодически отчитывается перед Правительственным комитетом по безопасности. Секретариат NSC является исполнительным органом NIB.

4.2. Министерство внутренних дел

МВД — ключевое министерство в национальной системе информационной безопасности. Для выполнения этих функций под его юрисдикцией находится **Национальный центр киберкоординации** (National Cyber Coordination Centre, NCCC) в Бангалоре, занимающийся организацией взаимодействия государственных органов, служб электронной разведки, специальных и правоохранительных служб, частного сектора и государственно-частного партнерства для мониторинга национального киберпространства, выявления и сокращения рисков информационной безопасности, обмена данными об исследованных угрозах и вредоносном программном обеспечении, разработки средств борьбы с ними.

NCCC осуществляет мониторинг всего национального интернет-трафика, защиту от компьютерных атак государственных ведомств и координацию на национальном уровне реагирования на события кибербезопасности. Для сбора оперативной информации он подключен к центрам управления всех крупных национальных интернет провайдеров и CERT-In, точкам обмена внутренним и международным трафиком. По оценке ведущих экспертов, проблемным вопросом функционирования NCCC является отсутствия правовой базы, определяющей его полномочия, что негативно сказывается на защите права частной жизни и гражданских свобод пользователей.

В структуре министерства также действует **Управление кибер- и информационной безопасности**, которое занимается вопросами обеспечения сетевой

36 Он курирует блок задач, связанных с обеспечением кибербезопасности и развитием передовых ИКТ, и возглавляет Национальную организацию технических исследований Индии.

37 Курирует вопросы использования передовых технологий в вооруженных силах.

безопасности, пресечения компьютерной преступности, разработки и мониторинга состояния безопасности национального информационного пространства. Каждое из указанных направлений деятельности имеет собственную организационную структуру, в том числе во всех штатах Индии.

Для противодействия преступности в сфере высоких технологий в 2013 году были созданы: специализированное формирование — **Киберполиция** с региональными отделениями, **Центральная лаборатория киберкриминалистики** для проведения цифровых расследований. Кроме того, МВД Индии с 2001 года обеспечивает функционирование **Бюро расследований (BI)** и **Центра координации по киберпреступности** (I4C), который с 2016 года осуществляет мероприятия по выявлению и пресечению преступлений в ИКТ-сфере и выполняет обязательства Индии в рамках Соглашения о многосторонней правовой помощи.

4.3. Министерство обороны

Для реализации описанных выше стратегий во всех родах войск (армия, ВВС, ВМС) созданы необходимые силы и средства. Управление ими осуществляется видовыми киберкомандованиями, которые координируются объединенным **Киберкомандованием**. Кроме того, функционируют другие военные структуры в сфере кибербезопасности, в частности **Агентство информационной безопасности и исследований** (DIARA), **Разведывательное агентство** (DIA), **Организация оборонных исследований и разработок** (DRDO), на последнюю приходится 30,7% государственных расходов на НИОКР. В 2019 году создано, а в 2021 году вошло в полную операционную готовность **Агентство киберзащиты** (DCyA), подчиненное напрямую начальнику генерального штаба.

В 2023 году Индия провела несколько учений по обеспечению кибербезопасности. Одно общенациональное под руководством Агентства киберзащиты, другое — первые объединенные межведомственные киберучения QUAD[38]по защите КИИ [35]. Кроме этого индийские военные специалисты приняли участие в организованном британской армией тренинге Defence Cyber Marvel 2.

4.4. Министерство электроники и информационных технологий

Министерство электроники и информационных технологий (MeitY) отвечает за развитие ИКТ-отрасли, повышение роли Индии в управлении Интернетом. Также оно занимается руководством научными исследованиями и разработками, внедрением инноваций, подготовкой кадров, повышением эффективности циф-

38 Quadrilateral Security Dialogue - четырёхсторонний диалог по безопасности между США, Австралией, Индией и Японией, создан в 2007, возобновлен в 2017 году.

ровых сервисов и защитой интернет-пространства страны. MeitY взаимодействует с провайдерами интернет-услуг, обеспечивая работу системы мониторинга внутригосударственного трафика, координацию усилий по противодействию распространению спама и вредоносного программного обеспечения.

Структурное подразделение министерства — **Национальный центр информатики** (National Informatics Centre, NIC) — обеспечивает функционирование инфраструктуры и услуг электронного правительства, общенациональной научной сети и других значимых систем, в развитии которых предпочтение отдается программному обеспечению с открытым программным кодом. Также в министерстве действуют **Национальный центр по безопасности коммуникаций** (NCSC) и **Управление стандартизации, тестирования и сертификации качества** (STQC), которое обеспечивает реализацию национальной схемы сертификации безопасности всего ИКТ-оборудования (ITSARs [36]). Кроме того, NIC выполняет функции удостоверяющего центра для сертификатов безопасности и цифровых подписей.

В структуре MeitY на основании статьи 70b рассмотренного выше закона ITA в 2004 году создана **Национальная группа реагирования на компьютерные инциденты** (CERT-In). Она является уполномоченным национальным агентством по обеспечению безопасности общедоступного интернет-пространства Индии за счет мониторинга его состояния и сбора данных от критически важных объектов[39], своевременного оповещения об угрозах информационной безопасности и выявленных уязвимостях, разработки и участия в исполнении чрезвычайных мер для обработки инцидентов кибербезопасности, координации реагирования на компьютерные атаки. К CERT-In подключены центры реагирования всех министерств и критически важных отраслей экономики.

Для функционирования национальной системы реагирования каждая государственная организация и предприятия критической информационной инфраструктуры должны назначить ответственного руководителя, в чьи обязанности входит обеспечение информационной безопасности своих информационных сетей и систем. Также они несут ответственность за разработку планов реагирования на чрезвычайные ситуации, вызванные компьютерными инцидентами, проверку их работоспособности и взаимодействие с уполномоченными органами. За первую половину 2023 года CERT-In зафиксировал почти 112,5 тыс. инцидентов безопасности (в аналогичный период 2018 года их было 70 798).

Кроме того, в структуру CERT-In входит подразделение **Cyber Swachhta Kendra** для противодействия бот-сетям и анализа вредоносного программного обеспечения.

---

39 За непредставление информации CERT-In поставщик услуг, юридическое или физическое лицо наказывается лишением свободы на срок до года или штрафом.

4.5. Национальная организация технических исследований

Национальная организация технических исследований (NTRO) создана по примеру АНБ США в 2004 году и является службой технической разведки. Контролируется лично премьер-министром, возглавляется заместителем его советника по национальной безопасности. В сфере информационной безопасности NTRO отвечает за все виды радиоэлектронной, космической и аэроразведки, сбор и обработку данных о кибербезопасности, анализ оперативной обстановки в национальном информационном пространстве, разработку стратегически важного аппаратного обеспечения.

Одним из ее подразделений является созданный в 2014 году **Национальный центр защиты критической информационной инфраструктуры** (NCIIPC). Среди его основных функций — защита КИИ и консультирование по снижению их уязвимости киберугрозам, противодействие актам кибертерроризма и кибервойны.

В структуру NTRO входит **Национальный институт криптографических исследований и внедрения** (NICRD). Он создан в 2007 году для разработки криптографических средств в интересах обеспечения национальной безопасности, а также подготовки необходимых специалистов [37].

4.6. Национальная служба разведки

Национальная служба разведки (NIA) несет ответственность за своевременное выявление и оценку угроз в национальном киберпространстве. Для реализации этой функции создан **Национальный центр исследования угроз** (NTIC), к которому по защищенным каналам связи имеют доступ все ключевые министерства. NTIC в целях получения интегральной оценки уровня компьютерных угроз национальный безопасности и обеспечения межведомственного обмена информацией интегрирует данные отраслевых групп CERT/CSIRT, различных служб разведки, предупреждений информационной безопасности компаний-производителей. По некоторым данным, NTIC даны правовые полномочия на ликвидацию бот-сетей, фишинговых сайтов и пр.

В августе 2023 года в Службе создано **Управление по противодействию кибертерроризму** (ACTU) [38].

4.7. Министерство иностранных дел

МИД Индии играет важную роль в продвижении интересов национальной ИКТ-отрасли, защите национальных интересов в контексте задач обеспечения

кибербезопасности и управления Интернетом, формировании системы международной информационной безопасности.

Основной блок вопросов сосредоточен в секретариате внешней политики, где созданы 5 департаментов: по вопросам разоружения и международной безопасности; кибердипломатии; электронного правительства и информационных технологий; планирования политики и исследований; по вопросам использования криптографии, НПО, наблюдения и контроля.

В 2020 году на фоне горячей фазы американо-китайской торговой и технологической войны в секретариате экономической политики создан новый департамент по новым, передовым и стратегическим технологиям (NEST). Его задачей является организация взаимодействия индийских ИКТ-компаний с международными организациями и корпорациями в интересах развития национальной экономики, содействия развитию в Индии технологий искусственного интеллекта и 5G. Кроме этого, департамент будет вести многосторонние и двусторонние переговоры о разработке правил, стандартов и архитектуры управления технологиями [39].

Для организации взаимодействия всех указанных департаментов МИДа и централизованного сопровождения участия Индии в международном переговорном процессе введена должность **координатора по кибердипломатии**, а в NEST — **со-координатора по сотрудничеству в научно-технической сфере**.

4.8. Элементы государственно-частного партнерства

Значительная часть инициатив в рамках программы «Цифровая Индия» осуществляется при активном участии бизнеса. Для координации совместных действий созданы различные форматы, которые позволяют сочетать интересы крупного бизнеса и начинающих компаний и более эффективно взаимодействовать с государственными органами и зарубежными партнерами.

Управление электронного правительства MeitY спонсирует инициативу по развитию государственно-частного партнерства **Cyber Surakshit Bharat** в целях повышения осведомленности руководителей государственных органов в вопросах кибербезопасности и борьбы с компьютерной преступностью.

Национальная ассоциация производителей в области информационных технологий (NASSCOM) создана для содействия государственно-частному партнерству в 1988 году. Ее задачей стала поддержка развития сегмента разработки ПО и цифровых услуг, исследований в указанной области, повышение квалификации государственных служащих и сотрудников правоохранительных органов в сфере кибербезопасности, цифровых расследований. В задачи NASSCOM также входит лоббирование интересов отрасли для совершенствования налогового, торгового и инвестиционного законодательства.

Ассоциация производителей электроники и полупроводников (IESA) развивает двустороннее сотрудничество с Ассоциацией полупроводниковой индустрии США (SIA) для укрепления глобальной экосистемы производства чипов.

Киберсообщество Индии (CySI) — многосторонняя платформа, объединяющая государство, правоохранительные ведомства и бизнес для повышения осведомленности об угрозах информационной безопасности и мерах по их снижению.

По мнению ведущих международных экспертов, для улучшения системы защиты национальной информационной безопасности в проекте новой стратегии кибербезопасности Индии следует более четко определить зоны ответственности ключевых игроков, в том числе частного сектора, особенно в основных критических информационных инфраструктурах (финансы, телекоммуникации, энергетика), а также улучшить координацию как на уровне федерального правительства, так и отдельных штатов.

5. Участие в международном сотрудничестве по формированию системы международной информационной безопасности

По мнению Ракеш Бхадаурия[40], высказанному на Валдайском форуме, его страна перешла к активной и напористой дипломатии и расширяет возможности сдерживания своих конкурентов и противников, главным образом КНР и Пакистана. Индия тщательно оберегает свою линию на «мульти присоединение», то есть сотрудничество со всеми без ограничений [40]. Она проявляет высокую активность в международных процессах по формированию системы международной информационной безопасности (МИБ) в части обеспечения информационной безопасности и глобального управления киберпространством, что крайне важно для достижения геополитических целей страны.

ООН

Значимость Индии в глобальном переговорном процессе подчеркивается назначением в 2022 году посланником Генерального секретаря ООН по вопросам технологий индуса Амандипа Сингх Гилла[41], который будет консультировать старшее руководство организации по ключевым тенденциям в области передовых технологий и выполнять функции координатора, с тем чтобы государства-члены,

40 Директор Центра стратегических исследований и моделирования Объединённого института оборонных исследований Индии.

41 А. Гилл был исполнительным директором и со-руководителем Группы высокого уровня ООН по цифровому сотрудничеству (2018–19 гг.), главным исполнительным директором Международного совместного проекта по исследованиям в области цифрового здравоохранения и искусственного интеллекта (в Высшем институте международных исследований и исследований в области развития в Женеве).

предприятия в сфере технологий, представители гражданского общества и другие заинтересованные стороны знали, куда можно в первую очередь обратиться по этим вопросам в рамках системы ООН.

Весомо участие Индии в формировании системы МИБ. Из 6 созывов Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (ГПЭ по МИБ) представители Индии участвовали в пяти. Они активно использовали эту площадку для решения собственных задач, прежде всего в интересах формирования новых правил и норм поведения. Интересно отметить, что Индия добились включения в доклад ГПЭ по МИБ созыва 2016-2017 гг. своего предложения о праве государства на самооборону в киберпространстве (в результате действий США доклад не был согласован, и инициатива не имела развития).

Всемирная торговая организация (ВТО)

Индия крайне заинтересована в открытом глобальном информационном пространстве, как основе развития национальной ИКТ-отрасли и укрепления цифровой экономики страны. Поэтому она поддерживает все форматы международного сотрудничества, которые могут влиять на это. Для Индии неприемлемы любые барьеры, которые ограничивают трансграничное движение капитала, технологий и услуг. Это ярко проявляется в позиции Дели по расширению перечня ИКТ-продукции в Соглашении ВТО по информационным технологиям. Китай, являясь его подписантом, использует различные нетарифные барьеры (например, национальные стандарты и правила) и ограничивает проникновение Индии на свой рынок, что сильно осложняет двусторонние отношения с КНР [41].

Форум по управлению Интернетом

Для формирования более благоприятных условий Индия уделяет огромное внимание Форуму по управлению Интернетом, определяющему стратегию развития глобальной сети. Там совместно со своими партнерами по IBSA[42] Дели продвигает демократизацию управления глобальной сетью всеми заинтересованными сторонами (мультистейкхолдерный подход) и выступает против отстаиваемой Китаем и Россией главенствующей роли государства в этом процессе. В этом контексте можно отметить, что проект Уфимской декларации БРИКС (2015 год) был под угрозой несогласования его Индией без отражения роли стейкхолдеров, и Москве пришлось пойти на уступки.

42 Политико-экономическое объединение Индии, Бразилии и ЮАР.

БРИКС

Индия высоко оценивает сотрудничество в рамках БРИКС, способствующее развитию страны и укреплению позиций Глобального Юга, при этом ее основные усилия направлены на укрепление экономических связей. В 2012 году Индия выдвинула инициативу создания Нового банка развития БРИКС, а ее представитель стал первым главой банка. Также Дели предложил создать рейтинговое агентство БРИКС, что было важным шагом в создании альтернативы Бреттон-Вудской финансовой системе. Однако именно Индия в 2023 году высказалась против создания единой валюты БРИКС в интересах укрепления роли рупии в международных расчетах.

Несмотря на то, что Индия является участником межправительственного соглашения ШОС о сотрудничестве в области обеспечения МИБ и участвует в Рабочей группе БРИКС по вопросам безопасности в сфере использования ИКТ, внешнеполитический курс страны полностью диверсифицирован и содействует достижению собственных целей. Индия не присоединилась к Конвенции о киберпреступности ЕС, но придерживается положений Модельного закона по киберпреступности Содружества наций, возглавляемого Великобританией. Кроме того, Индия с 2015 года является членом Глобальной киберэкспертизы (GFCE), инициированной Великобританией. Поддержала она и Парижский призыв к доверию и безопасности в киберпространстве (2018).

G20

Очень эффективно Индия реализовала свое председательство в G20 для обозначения притязаний на стратегическое лидерство в сфере использования Больших данных. Она стала продвигать «новый золотой стандарт данных», включающий самооценку национальной архитектуры управления данными, модернизацию национальных информационных систем для регулярного сбора мнений и предпочтений граждан, а также принцип прозрачности в вопросе управления данными [42].

Двустороннее сотрудничество

Двустороннее сотрудничество по линии обеспечения кибербезопасности развивается как с соседями по региону, так и наиболее передовыми государствами. Наиболее тесные отношения в этой сфере имеются с США, кибердиалог ведется с начала 2000-х гг. и интенсифицирован в 2015 году путем подключения к нему бизнеса (так называемый трек 1,5). Кроме того, кибертематика является компонентом нескольких индийско-американских соглашений и включает обмен разведывательной информацией и оказание правовой помощи [43]. В совместном заявлении, сделанном накануне саммита G20 в Нью-Дели, Н. Моди и Дж. Байден подчеркнули определяющую роль технологий в углублении двустороннего стратегического партнерства и высоко оценили результаты индийско-американской инициативы по критически важным и передовым технологиям (iCET), направ-

ленной на создание открытых, доступных, безопасных и устойчивых технологических систем и цепочек поставок [44].

Другим важным партнером Индии является Великобритания, кибердиалог с которой ведется с 2012 года. Для повышения своего защитного потенциала Индия подписала с этим государством рамочное соглашение о сотрудничестве в сфере кибербезопасности и создании 4 совместных рабочих групп (по кибердипломатии, компьютерной преступности, реагированию на инциденты и цифровой экономике), а также достигла принципиального согласия о создании совместного Центра обмена опытом по подготовке в сфере кибербезопасности[43].

В 2016–17 гг. двустороннее сотрудничество Индии имело значительный всплеск, были заключены несколько меморандумов о взаимопонимании, сделаны заявления о стратегическом и техническом сотрудничестве, продолжены партнерские кибердиалоги. В частности, октябре 2016 года подписано Соглашение между Правительством Российской Федерации и Правительством Республики Индии о сотрудничестве в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий, которое вступило в силу в январе 2017 года. Новая волна активизации наметилась в 2020–2022 годах, когда западники стали активно вовлекать Индию в новые политические союзы Индо-Тихоокеанского региона. В частности, в 2020 году проведен 6 раунд кибердиалога с ЕС, создана совместная рабочая группа по информационным технологиям с Ирландией, заключен Меморандум о сотрудничестве в сфере кибербезопасности с Японией. В 2021 году сделано совместное заявление о стратегическом партнерстве с Австралией, в 2022 году об укреплении партнерства в сфере кибербезопасности с Великобританией и кибердиалог с Италией по вопросам противодействия кибертерроризму, экстремизму и компьютерной преступности [45].

Все эти действия говорят о том, что на данном этапе Индия успешно балансирует между несколькими полюсами силы, чтобы не только развивать собственную цифровую экономику за счет обмена опытом и технологиями, но и расширять сферу охвата, набирать политические очки и сдерживать конкурентов. Стратегической целью страны является оформление в самодостаточный центр влияния индийской цивилизации, что станет более заметно, когда ее ИКТ-сектор станет более технологически независимой, а экономика выйдет на вторую позицию в мире. Расширение БРИКС дает дополнительные возможности опережающего развития экономики Индии и росту ее влияния.

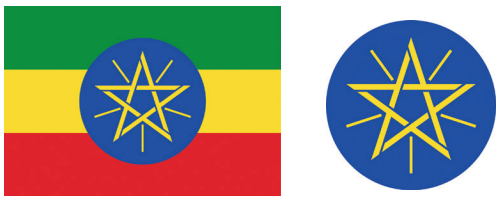
43 Joint Cyber Security Training Centre of Excellence

6. Использованная литература

1. Лазанюк И.В. Информатизация как основа развития инновационного сектора экономики Индии, 2005, https://www.dissercat.com/content/informatizatsiya-kak-osnova-razvitiya-innovatsionnogo-sektora-ekonomiki-indii?ysclid=lm4rhen37t541976805
2. Global Innovation Index 2023, https://www.wipo.int/global_innovation_index/en/2023/
3. Cyber Capabilities and National Power: a Net Assessment, International Institute for Strategic Studies (IISS), 28 June 2021, https://www.iiss.org/research-paper/2021/06/cyber-power---tier-three/
4. Кулик Л. Индийский профиль цифровизации: отличительные черты, Клуб «Валдай», 30.06.2021, https://ru.valdaiclub.com/a/highlights/indiyskiy-profil-tsifrovizatsii/?ysclid=lm4x35m88o550647211
5. India E-Commerce Market Size & Share Analysis — Industry Research Report — Growth Trends, https://www.mordorintelligence.com/industry-reports/india-ecommerce-market
6. Network Readiness Index 2022, https://networkreadinessindex.org/, https://indianexpress.com/article/india/india-climbs-six-places-61st-rank-network-readiness-index-8278175/
7. Digital Development Dashboard, https://www.itu.int/en/ITU-D/Statistics/Dashboards/Pages/Digital-Development.aspx
8. Телекоммуникационная отрасль в Индии — телекоммуникационный сектор, https://www.investindia.gov.in/ru-ru/sector/telecom
9. Christina Joshy Internet Users In India: Statistics and Data, September 26, 2023, https://www.grabon.in/indulge/tech/internet-users-statistics/
10. E-Government Survey 2022. The Future of Digital Government // Department of Economic and Social Affairs of the United Nation, p.216, https://ifap.ru/library/book652.pdf
11. Global Cybersecurity Index 2020, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
12. Обсуждение тенденций развития кибербезопасности Индии // Eurasian Research Institute, https://www.eurasian-research.org/publication/discussion-of-indias-cyber-security-development-trends/?lang=ru
13. Govind Choudhary Shortage of the cybersecurity workforce in India is 9% higher than the global average // Aug 19, 2021, https://www.expresscomputer.in/security/shortage-of-the-cybersecurity-workforce-in-india-is-9-higher-than-the-global-average-rv-raghu/78520/.
14. National Critical Information Infrastructure Protection Centre, NCIIPC Newsletter, January 2021, p. 2, https://nciipc.gov.in/ documents/NCIIPC_Newsletter_Jan21.pdf
15. India bans PUBG, 117 other Chinese apps for “stealing, transmitting users’ data” to servers outside India’, FirstPost, 20 September 2020, https://www.firstpost.com/india/india-banspubg-117-other-chinese-apps-for-stealing-transmitting-usersdata-to-servers-outside-india-8778561
16. Технологическая политика Индии: рабочая тетрадь № 82 / 2023 / [И. Ю. Щедров; под ред. Е. О. Карпинской, А. Ю. Толстухиной, С. М. Гавриловой]; Российский совет по международным делам (РСМД). — М.: НП РСМД, 2023, https://russiancouncil.ru/papers/India-TechPolicy-WorkingPaper82.pdf
17. Цифровизация Индии. От локального феномена — к фактору глобального влияния. // Институт исследований развивающихся рынков бизнес-школы Сколково (IEMS), 2021, https://www.skolkovo.ru/researches/india-goes-digital-from-local-phenomenon-to-global-influencer-2/
18. Cyber Capabilities and National Power: a Net Assessment, International Institute for Strategic Studies (IISS), 28 June 2021, https://www.iiss.org/research-paper/2021/06/cyber-power---tier-three/
19. Cabinet approves outlay of Rs 14,903 crore to expand Digital India programme, Aug 17, 2023, https://economictimes.indiatimes.com/tech/technology/centre-to-expand-digital-india-programme-525000-it-professionals-to-undergo-upskilling/articleshow/102770054.cms
20. File No. No: EE-9/5/2021-R&D-E Government of India Ministry of Electronics and Information Technology (MeitY) (R&D in Electronics Group) Dated: 30th December, 2021 Subject: Guidelines for Design Linked Incentive (DLI) Scheme, https://www.meity.gov.in/writereaddata/files/Guidelines%20for%20Design%20Linked%20Incentive%20%28DLI%29%20Scheme.pdf
21. National Strategy for Artificial Intelligence #AIforAll, NITI Aayog, June 2018, https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf
22. India’s Artificial Intelligence Strategy: AI for All, October 15, 2019, https://indbiz.gov.in/indias-artificial-intelligence-strategy-ai-for-all/
23. Технологическая политика Индии: рабочая тетрадь № 82 / 2023 / [И. Ю. Щедров; под ред. Е. О. Карпинской, А. Ю. Толстухиной, С. М. Гавриловой]; Российский совет по международным делам (РСМД). — М.: НП РСМД, 2023, https://russiancouncil.ru/papers/India-TechPolicy-WorkingPaper82.pdf
24. Республика Индия, Научно-технический центр ФГУП «ГРЧЦ», 14.10.2020, https://rdc.grfc.ru/2020/10/india/?ysclid=lm83qi1w5c288275665

25. National Cyber Security Strategy 2020, Submitted by Data Security Council of India, 2020, https://www.dsci.in/sites/default/files/documents/resource_centre/National%20Cyber%20Security%20Strategy%202020%20DSCI%20sumission.pdf
26. India Launches National Cybersecurity Reference Framework NCRF, June 16, 2023, https://cionews.co.in/india-launches-cybersecurity-reference-framework/
27. Ministry of Communications (Department of Telecommunications) NOTIFICATION, New Delhi, the 7th August, 2017 G.S.R. 998(E).—In exercise of the powers conferred by section 7 of the Indian Telegraph Act, 1885 (13 of 1885) (hereinafter referred to as the said Act), the Central Government hereby makes the following rules to regulate the temporary suspension of telecom services due to public emergency or public safety, https://dot.gov.in/sites/default/files/Suspension%20Rules.pdf?download=1
28. A Special Reference to The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, https://www.meity.gov.in/writereaddata/files/IT%20Rules%2C%202021%20with%20proposed%20amended%20texts%20in%20colour.pdf
29. Там же.
30. Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, https://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf
31. The Digital Personal Data Protection Bill, 2022, https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Protection%20Bill%2C%202022.pdf
32. The Digital Personal Data Protection Act, 2023, https://prsindia.org/files/bills_acts/bills_parliament/2023/Digital_Personal_Data_Protection_Act,_2023.pdf
33. India Has Clamped Down on Crypto. What Will It Do with Its G-20 Power, https://www.yahoo.com/lifestyle/india-clamped-down-crypto-g-170148179.html
34. R. Venkataraman National Security Mechanism and the HDO, https://capsindia.org/wp-content/uploads/2022/09/R-Venkataraman-1.pdf
35. India conducts national cyber defence exercise to safeguard critical infrastructure amid escalating threats, 28 May 2023, https://www.livemint.com/news/india-conducts-national-cyber-defence-exercise-to-safeguard-critical-infrastructure-amid-escalating-threats-11685248974907.html
36. The Cybersecurity Standards in India. How NCCS works, https://www.graniteriverlabs.com/en-us/market-access-services/country/india/nccs-mark
37. India Cyber Readiness at a Glance, December 2016, https://potomacinstitute.org/images/CRI/CRI_India_Profile.pdf
38. Specialised unit within NIA to lead probes into cyberattacks // Latest News India — Hindustan Times, Aug 13, 2023, https://www.hindustantimes.com/india-news/specialised-unit-within-nia-to-lead-probes-into-cyberattacks-101691867415960.html
39. MEA sets up NEST unit to focus on tech diplomacy, January 2, 2020, https://indbiz.gov.in/mea-sets-up-nest-unit-to-focus-on-tech-diplomacy/
40. Ф. Лукьянов Лучше меньше? Нет, больше! // Россия в глобальной политике 25.08.2023, https://globalaffairs.ru/articles/luchshe-menshe-net-bolshe/
41. Sachin Chaturvedi, Sabyasachi Saha "Competing Imperatives of Global Governance and National Interests within BRICS: An Indian Perspective" // Observer Research Foundation, 2017, https://risingpowersproject.com/competing-imperatives-global-governance-national-interests-within-brics-indian-perspective/.
42. Amitabh Kant India will set new data standards in G20 stint, Dec 26, 2022, https://www.hindustantimes.com/opinion/india-will-set-new-data-standards-in-g20-stint-101672020222996.html
43. Cyber Capabilities and National Power: a Net Assessment, International Institute for Strategic Studies (IISS), 28 June 2021, https://www.iiss.org/research-paper/2021/06/cyber-power---tier-three/
44. Joint Statement from India and US after bilateral talks between PM Modi and US President Joe Biden: Full Text Sep 8, 2023, https://timesofindia.indiatimes.com/india/joint-statement-from-india-and-us-after-bilateral-talks-between-pm-modi-and-us-president-joe-biden-full-text/articleshow/103517033.cms?from=mdr
45. UNIDIR, https://cyberpolicyportal.org/states/india
46. Лазанюк И.В. Информатизация как основа развития инновационного сектора экономики Индии, 2005, https://www.dissercat.com/content/informatizatsiya-kak-osnova-razvitiya-innovatsionnogo-sektora-ekonomiki-indii?ysclid=lm4rhen37t541976805

Федеративная Демократическая Республика Эфиопия



Официальное название: Федеративная Демократическая Республика Эфиопия. Основана 12 сентября 1974 года в результате Эфиопской революции.

Столица: Аддис-Абеба

Официальный язык: амхарский, распространен английский. Всего насчитывается 80 этнолингвистических групп, носителями которых являются около 100 народностей и этнических групп. Наиболее многочисленные из них: оромо (32%), амхара (30%) и тыграйцы (6%).

Территория: 1 104 300 км² (27 место в мире), водная поверхность составляет 0,7% территории. Эфиопия расположена на Африканском роге в восточной части континента, выхода к морю не имеет после отделения Эритреи 24 мая 1993 года. Граничит на севере и северо-востоке с Эритреей, на востоке с Джибути, на востоке и юго-востоке с Сомали и непризнанным государством Сомалиленд[1], на юге с Кенией, на северо-западе с Суданом и на юго-западе с Южным Суданом.

Население: 128 201 338 чел. по оценочным данным за 2023 год Отдела народонаселения Департамента по экономическим и социальным вопросам ООН (11 место в мире), в Африке Эфиопия вторая по численности населения после Нигерии. В начале 2023 года почти 80% населения проживало в сельской местности.

Эфиопия приняла христианство в 330 году н.э., в настоящее время эту религию исповедует 63% населения страны, из них 70 % православные. Мусульмане суннитского направления составляют 34% населения [1].

Государственное устройство: федеративная демократическая парламентская республика. Конституция принята 8 декабря 1994 года. Административное деление: 9 регионов и 2 отдельных округа, организованных по этническому признаку.

Глава государства: президент, избираемый парламентом на 6 лет, выполняет представительские функции. В настоящее время должность президента занимает Сахле-Ворк Зевде. Реальной властью обладает премьер-министр, который утверждается на пост парламентом по представлению партии, победившей на выборах (в настоящее время — Абий Ахмед Али).

---

1 Между Эфиопией и Сомалилендом 1 января 2024 года был подписан меморандум о взаимопонимании, по которому Эфиопия в обмен на возможное признание Сомалиленда независимым государством арендует на 20 лет порт Бербера на Красном море и 20-километровый участок побережья. Если это соглашение будет соблюдено, Эфиопия станет первым государством-членом ООН, признавшим эту самоопределившуюся нацию. Источник: https://kg24.news/politics/mir-stydit-efiopiyu-za-priznanie-somalilenda.html

Законодательная власть: двухпалатный парламент, депутаты которого избираются на 5 лет. Верхняя палата – Совет Федерации несет ответственность за соблюдение Конституции (108 мест, члены избираются представительными органами штатов). Депутаты нижней Палаты народных представителей избираются прямым голосованием в одномандатных округах простым большинством голосов (не более 550 депутатов, при этом не менее 20 мест из этого числа отводится представителям национальных и народных меньшинств). Они принимают законы по вопросам, перечисленным в конституции, вводят налоги, ратифицируют международные соглашения, заключённые главой исполнительной власти [2].

Исполнительная власть: Правительство — Совет министров, его состав должен быть одобрен парламентом. Возглавляет правительство премьер-министр — лидер партии парламентского большинства. Он также является главнокомандующим вооруженными силами Эфиопии.

Экономика: По данным Всемирного банка за 2022 год показатели Валового внутреннего продукта (ВВП) (по паритету покупательной способности):

Итого: 347 млрд долл. (56 место в мире).

На душу населения 2 812 (164 место в мире);

Показатели ВВП (Номинал):

Итого: 127 млрд долл. (60 место в мире).

На душу населения: 1028 долл. США (169 место в мире).

Эфиопия является одной из беднейших стран мира. Внутренний государственный долг в 2023 году составил 31,4% от ВВП, внешний около 28 млрд долл. США и по выплатам евробондов в декабре 2023 года страна вошла в технический дефолт.

Дипломатические отношения с Россией (СССР) были официально установлены в феврале 1898 года, их 125-летие было торжественно отмечено в 2023 году [3]. После Октябрьской революции отношения между двумя странами были фактически прекращены и возобновлены лишь в 1930–1940 гг., когда обе станы боролись против фашизма и нацизма. Дипломатические отношения возобновлены в 1943 году.

1. Уровень развития ИКТ-инфраструктуры и информатизации страны

Эфиопия несмотря на достаточно высокий номинал ВВП[2] является одним из самых бедных государств мира, что объясняется совокупностью внешних и внутренних факторов. После отделения Эритреи страна потеряла выход к морю, что создало дополнительную экономическую нагрузку (усложнение логистики, аренда портов, вынужденное строительство транспортных коридоров). Непростые отношения с соседними государствами, в том числе с Суданом и Египтом[3], вынуждают Эфиопию иметь значительные вооруженные силы[4]. Двухлетняя гражданская война в провинции Тыграй[5] закончилась в 2022 году хрупким миром с повстанцами и появлением миллионов беженцев[6]. Демографический фактор оказывает решающее значение на высокий уровень безработицы и бедность населения[7], 60% которого заняты в сельском хозяйстве (в основном микро, малые и средние предприятия)[8]. Климатические катаклизмы в 2023 году привели к гибели урожая, в настоящее время 4 миллионам жителей страны грозит голод [4].

---

2 С начала 21 века экономика страны стабильно росла в среднем на 10% в год. По ее объему в 2018 году Эфиопия опередила Кению, которая многие годы являлась экономическим лидером Восточной Африки. Источник: С. Шейхетов Финтех в Эфиопии. Pro et contra // Журнал ПЛАС №8 (263), 21 октября 2019 года, https://plusworld.ru/journal/2019/plus-8-2019/finteh-v-efiopii-pro-et-contra/?ysclid=

3 Одним из факторов осложнения отношений является строительство Эфиопией мощной гидроэлектростанции «Плотина великого возрождения» на крупном притоке Нила – Голубом Ниле, что привело к нарушению водных ресурсов в Судане и Египте.

4 Вооруженные силы Эфиопии занимают 49 позицию в мире. Источник: 2024 Ethiopia Military Strength, https://www.globalfirepower.com/country-military-strength-detail.php?country_id=ethiopia

5 Причиной вооруженного конфликта стало постепенное «выдавливание» из всех органов государственного управления Эфиопии тыграйцев (представители этого этноса, составляющего всего 6% населения, традиционно играли важную роль в руководстве страной). Гражданская война с Фронтом народного освобождения Тыграй стала самым кровопролитным конфликтом в 21 веке, она унесла жизни около 600 тыс. человек.

6 По данным ООН, в Эфиопии насчитывается 930 тыс. беженцев и искателей убежища, в основном из Южного Судана, Сомали и Эритреи. Число внутренних переселенцев составляет 3,1 млн человек. Всемирная продовольственная программа относит Эфиопию к шести странам, наиболее нуждающимся в продовольственной помощи. Источник: ООН в Эфиопии: от чрезвычайной помощи – к поддержке в области развития // Новости ООН, 20 октября 2023 года, https://news.un.org/ru/story/2023/10/1446042

7 Население Эфиопии превышает 128 млн чел. и является одним из самых быстрорастущих в мире с темпами увеличения 3,2% в год (ежедневный прирост составляет 8777 чел.), более 50% населения моложе 18 лет. При сохранении этой динамики население страны удвоится в ближайшие 30 лет. Уровень безработицы среди городского населения составляет 17,9%, а среди городской молодежи – 22,9%, при этом увеличение городов идет со скоростью 5,5%, что к 2030 даст 32,9 млн жителей. Эфиопия остается одной из самых бедных стран Африки и мира. В 2001 году она получила право на облегчение бремени по задолженности бедных стран в Международном валютном фонде (МВФ) и Всемирном банке, а в 2005 году стала одной из немногих, выигравших 100% по облегчению бремени задолженности кредитов от МВФ, Всемирного Банка и Африканского банка развития. Источники: Ethiopia Population 2024 (Live), https://worldpopulationreview.com/countries/ethiopia-population, Экономика Эфиопии, ВВП, производство, сельское хозяйство, 18.02.2020, https://mindinvest.ru/ekonomika-efiopii/, Ethiopia voluntary national review 2022, https://hlpf.un.org/sites/default/files/vnrs/2022/VNR%202022%20Ethiopia%20Report_1.pdf

8 В сельских районах Эфиопии проживает около 79% населения (данные ВОЗ). Аграрный сектор дает 32,7% ВВП страны и 82% экспорта. Источник: Developing Ethiopia's Digital Economy: Lessons from China // South-South Integration and the SDGs: Enhancing Structural Transformation in Key Partner Countries of the Belt and Road Initiative, UNCTAD/BRI PROJECT/RP21, 2021, https://unctad.org/system/files/official-document/BRI-Project_RP21_en.pdf

Наложение указанных факторов в совокупности с пандемией COVID-19 и нарушением мировой торговли в связи с проведением СВО привело к замедлению роста национальной экономики[9], но она по-прежнему остается одной из самых крупных и быстро развивающихся в Африке (средние темпы роста ВВП Эфиопии в 2012–21 гг. составили 8,6% в год [5]).

Сильными сторонами национальной экономики является почти полная обеспеченность электроэнергией[10], развитая индустрия авиаперевозок[11], разработка месторождений золота и тантала, укрепление производственных и новых отраслей (например, фармацевтики). Кроме того, Эфиопия обладает большим и быстро развивающимся внутренним рынком, огромным человеческим капиталом (доля трудоспособного населения очень высока), а также стратегически удобным положением на Африканском Роге, что делает ее связующим звеном между Африкой, Ближним Востоком, Европой и Азией. Положительная динамика в использовании этих возможностей очевидна. Согласно данным отчета Эфиопии по достижению Целей устойчивого развития ООН в период с 2017 по 2022 год, достигнут прогресс по пяти направлениям: люди, процветание, планета, мир и партнерство.

В первую очередь Эфиопия намерена стабилизировать экономическое и социальное положение в стране, чему должен способствовать курс на диверсификацию экономики, прежде всего за счет цифровизации ключевых отраслей (сельское хозяйство, туризм) и государственного управления. Этот вектор национальной политики стал формироваться в 2000-х годах, когда правительство признало, что информационные и коммуникационные технологии (ИКТ, ИТ) являются ключевым фактором будущего, и поставило амбициозную задачу: к 2030 году подключить к глобальной сети Интернет даже самые отдаленные территории Эфиопии. Развитие указанного курса было усилено с принятием в Африканским союзом «Повестки 2063: Африка, которую мы хотим» [6] и открытием в 2021 году Африканского рынка свободной торговли (AfCFTA). В этой связи остро встали вопросы разработки правовых механизмов для регулирования деятельности в ИКТ-среде, формирования национальной стратегии развития ИКТ-отрасли,

9 В 2023 году темп роста экономики Эфиопии упал до 5,3%. Источники: Ethiopia Economic Outlook // African Development Bank Group, https://www.afdb.org/en/countries/east-africa/ethiopia/ethiopia-economic-outlook

10 Генерация электроэнергии на 98,2% идет за счет возобновляемых источников, из них гидроэнергетика 87,4%, ветрогенерация 7,1%, биотопливо 5,9%, солнечная энергия 0,4%, геотермальная энергия 0,1%. Согласно данным государственной энергетической компании Эфиопии Ethiopian Electric Power, гидроэнергетический потенциал страны оценивается в 45 тыс. МВт, геотермальный потенциал в 10 тыс. Источник: Эфиопия: ESG-досье // ПАО Сбербанк 2022, https://sber.pro/bcp-laika-public/ESG_Ethiopia_1808_b18387a8cc.pdf?ysclid=lrbqswx4mm616495733

11 Ethiopian Airlines — флагманский авиаперевозчик Эфиопии и крупнейшая авиакомпания в Африке по пассажиропотоку, парку самолетов и направлениям. Она выполняет рейсы по более чем 120 международным и внутренним направлениям, включая США, ЕС, Азию и Австралию. Авиакомпания известна своей безопасностью, эффективностью и прибыльностью и получила несколько наград. Она является катализатором развития туристического и торгового секторов Эфиопии.

эффективной координации государственных институтов, преодоления кадрового голода и недостатка финансирования[12].

Данные Индекса сетевой готовности 2023 года[13] показывают, что эти проблемы пока удалось решить лишь частично, тем не менее Эфиопия занимает 7 место в группе из 60 стран мира с низким уровнем дохода[14], превышая средние значения индекса в указанной группе и на Африканском континенте по двум параметрам: развитию технологической составляющей и влиянию Интернет на все отрасли экономики и государство. Однако в указанном рейтинге среди 143 экономик страна занимает только 126 место. Причинами сохранения отставания ИКТ-отрасли Эфиопии являются низкий уровень электрификации удаленных районов[15] и проникновения услуг фиксированной/ мобильной связи и Интернета, сохранение значительной доли государственной монополии, а также отсутствие эффективного правового регулирования.

Следует отметить, что для решения широкого круга задач цифровизации правительство Эфиопии получает значительное финансирование от Африканского банка развития, Всемирного банка, Европейского инвестиционного банка и частных фондов, например, Mastercard. Также осуществляется сотрудничество с мощными технологическими державами (США, ЕС, Китаем, Индией, ОАЭ и Кореей) для развития национального ИКТ-сектора в рамках широкой стратегии, направленной на диверсификацию зависимости от единственного инвестора. Вооруженный конфликт в Тыграе резко снизил это финансирование и прямые иностранные инвестиции, а также повлиял на скорость реализации ключевых стратегий и их поддержку.

Доступ к современным ИКТ является ключевым для социально-экономической трансформации. Несмотря на наличие Национального плана развития ИКТ инфраструктуры (2003), ее уровень по-прежнему недостаточный [7]. Рост использования сети Интернет в значительной степени сдерживался ограниченным объемом зарубежной помощи выделяемой в целях развития Эфиопии[16], в том

12 В 2022 году США под предлогом нарушения прав человека в ходе конфликта в Тыграе лишили Эфиопию права беспошлинной торговли, осуществлявшейся в рамках закона США AGOA, направленного на оказание помощи экономикам стран Африки к югу от Сахары и улучшение экономических отношений между США и этим регионом. Источник: https://www.aljazeera.com/news/2022/1/2/us-removes-ethiopia-mali-and-guinea-from-agoa-trade-programme

13 Индекс NRI ежегодно готовится INSEAD для ВЭФ, рассчитывается по 4 блокам показателей: развитие технологической составляющей, человеческого фактора, управленческих навыков и влияния Интернет на все отрасли экономики и государство, https://download.networkreadinessindex.org/reports/countries/2023/ethiopia.pdf

14 К этой категории относятся страны с уровнем ВВП на душу населения менее 1085 долл. США, по состоянию на декабрь 2022 года их насчитывалось 60.

15 В 2019-20 гг. доступ к электричеству имело только 44% населения Эфиопии. При этом в 2020–21 гг. электрифицированными были 76% школ второй ступени и 30% начальной ступени, преимущественно в сельской местности. Источник: VNR 2022 Ethiopia Report, https://hlpf.un.org/sites/default/files/vnrs/2022/VNR%202022%20Ethiopia%20Report_1.pdf

16 В отчете Deloitte за 2017 год отмечено, что инвестиции в Эфиопию резко возросли и являются одними из самых

числе для развертывания ИКТ-инфраструктуры, ее низкой доступностью, особенно в сельских районах, высокой стоимостью услуг[17] и частыми перебоями в электросетях.

В связи с этим правительство предприняло решительные шаги: отказаться от государственной монополии в секторе связи и инициировать либерализацию ИКТ-рынка. В 2019 году законом «Об услугах связи» [8] созданы правовые условия для местных и зарубежных инвестиций, развития частного бизнеса, а также учрежден регулятор отрасли — Администрация связи Эфиопии (ECA). В 2022 году правительство повторно провело тендер на частичную приватизацию Ethio Telecom, единственным мажоритарным акционером которой является государство, отправило запрос о комментариях для выдачи третьей телекоммуникационной лицензии[18].

Главенствующее положение компании Ethio Telecom[19] сохранилось, но стали активнее развиваться национальные ИТ-провайдеры. В 2020 году ECA «приземлила» в стране международных операторов связи и интернет-услуг, включая французскую Orange, британскую Vodacom, южноафриканскую MTN, которые создали дочерние компании в Аддис-Абебе[20]. В 2021 году консорциум «Глобальное партнерство для Эфиопии»[21], возглавляемый кенийской Safari-

высоких в мире по отношению к ВВП страны. Согласно данным Ibex Frontier в 2018–19 гг. страна стала седьмой в мире по получению инвестиций в технологии, их объем достиг 11,3 млн долл. США. В текущем периоде объем прямых иностранных инвестиций (ПИИ) превышает заимствования в международных финансовых институтах, что свидетельствует о высоком интересе частных инвесторов к проектам на эфиопском рынке.

17 Цена самого дешевого домашнего Интернет-пакета превышает заработок государственного служащего начального уровня. Источник: https://www.kaspersky.com/blog/secure-futures-magazine/ethiopia-digital-transformation-strategy/39783/

18 В сентябре 2021 года Управление связи Эфиопии (ECA) запустило процедуру RFP (запроса предложений) на получение международных лицензий для зарубежных ИКТ-операторов. В ноябре 2023 года она прекращена, поиск подходящего кандидата отложен. В октябре 2022 года первым частным оператором стал консорциум во главе с кенийской Safaricom. Эфиопия также стремится продать до 45% акций Ethio Telecom международной компании, процесс, который также был возобновлен в ноябре 2022 года. Источник: Ethiopia cancels process for international telecoms licence -official // Reuters, November 17, 2023, https://www.reuters.com/world/africa/ethiopia-cancels-process-international-telecoms-licence-official-2023-11-17/

19 Ethio Telecom (ранее Эфиопская телекоммуникационная корпорация, ETC) 126 лет сохраняла монополию на услуги проводной и мобильной связи, а затем космической VSAT и Интернет, также обладала телеканалом ETV, Национальным радио, региональными радиостанциями. Спутниковый Интернет доступен некоторым крупным корпорациям, ETC также запрещает использование VoIP в интернет-кафе и населением в целом, хотя услуга включена в стратегию компании в области широкополосной связи. При этом, как отмечала в 2017 году Human Rights Watch, все коммуникации в стране находились под пристальным контролем государства.

20 MTN Ethiopia в 2020 году стала первой негосударственной компанией, получившей в Эфиопии телекоммуникационную лицензию. Второй по значимости оператор в Эфиопии Orange Ethiopia с 2018 года предоставляет мобильные сервисы, в том числе платежный Orange Money, имеет 20 млн подписчиков и планирует в течение 5 лет охватить 90% населения страны своими услугами. Vodafone Ethiopia вошла на местный рынок в 2021 году, получив как негосударственная компания лицензию в сфере обеспечения безопасности телекоммуникационных услуг. Планирует инвестировать в Эфиопию 850 млн долл. США и создать клиентскую базу в объеме 80% населения. Источник: Unlocking Ethiopia's Potential: A Look at the Country's Booming ICT Industry // Telecom Review Africa, 5 May 2023, https://www.telecomreviewafrica.com/en/articles/features/3380-unlocking-ethiopia-s-potential-a-look-at-the-country-s-booming-ict-industry

21 В Партнерство также вошли южноафриканская Vodacom Group, японская Sumitomo Corporation и российская CDC Group («Центр Корпоративных Разработок»).

com, получил первую лицензию на оказание в стране ИТ-услуг (срок лицензии 15 лет), что сбалансировало участие в национальном телекоммуникационном секторе США и Китая[22], а также африканских Tana Communications и Africom Technologies.

В апреле 2022 года Ethio Telecom и Safaricom завершили переговоры с ECA по Соглашению о совместном использовании инфраструктуры и взаимодействию сроком на 10 лет [9]. Это важно, поскольку Ethio Telecom по сути является монополистом первичных сетей связи, которые она недавно модернизировала с участием китайских ZTE и Huawei[23] и шведской Ericsson, а также использует два национальных спутника связи[24]. Реализация соглашения позволила предоставить телекоммуникационные услуги по выделенным линиям для сельского хозяйства, образования, здравоохранения и частного использования во всех 15 тыс. эфиопских деревень[25]. Кроме того, предприняты меры по расширению доступности широкополосной связи, проложена 21 тыс. км оптоволоконного кабеля вдоль автомагистралей страны и осуществлена часть работ по подключению Аддис-Абебы к обновленной Восточноафриканской подводной кабельной системе (EASSy, ее пропускная способность в 2022 году удвоена до 36 Тб/с, точки сопряжения с системой возможны в Судане, Джибути и Сомалиленде).

Конкуренция крупных игроков способствовала расширению предложения и повышению доступности услуг за счет снижения цен, что сразу отразилось на росте подписчиков. Если в 2014 году в стране менее 3% населения регулярно пользовалось Интернет и только 31% жителей имели мобильные телефоны, то в начале 2023 года по данным МСЭ уровень проникновения Интернет поднялся до 17,9%[26]. Это существенно ниже, чем в среднем по Африке (43,2%) и в мире

22 США с 60-х годов прошлого века поставляли в страну ИКТ оборудование, в настоящее время оснащают офисной техникой госучреждения и школы. Китай вошел на рынок Эфиопии относительно недавно, но активно инвестирует в развитие инфраструктурных объектов, в том числе в телекоммуникационные сети и объекты информатизации, поставляет аппаратные и программные решения. Источник: Ethiopia Telecoms Market Report. Telecoms, Mobile and Broadband - Statistics and Analyses, January 2024, https://www.budde.com.au/Research/Ethiopia-Telecoms-Mobile-and-Broadband-Statistics-and-Analyses

23 На основании крупнейшего в Африке соглашения Ethio Telecom с ZTE, заключенного при поддержке Банка развития КНР в 2006 году, ZTE обязалась вложить в капитальный ремонт и расширение телекоммуникационной системы Эфиопии 1,5 млрд долл. США. Через 6 лет аналогичное соглашение на 1,6 млрд было заключено ZTE и Huawei. Источник: I. Gagliardone The Politics of Technology in Africa. Communication, Development, and Nation-Building in Ethiopia // Cambridge University, November 2016, https://www.researchgate.net/publication/310604570_The_Politics_of_Technology_in_Africa_Communication_Development_and_Nation-Building_in_Ethiopia

24 Первый эфиопский спутник Ethiopian Remote Sensing Satellite ETRSS-1 запущен в 2019 году, второй ET Smart RSS2 – в 2020 году. Космическая связь применяется для обеспечения доступа к Интернет в сельских и труднодоступных районах, в частности Министерствами образования и здравоохранения.

25 Общенациональная волоконно-оптическая магистральная сеть охватывает все основные города и пограничные пункты на севере, востоке и юге страны. В других районах трафик передается с применением микроволновой и спутниковой связи. Источник: МСЭ – Отчет об измерении информационного общества, Том 2, 2018 год, https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR_Vol_2_R.pdf

26 По данным «International Business Ethiopia 2020», уже в 2017 году проникновение Интернет превысило 18,62%. Согласно Национальной стратегии цифровой трансформации к 2025 году этот показатель должен быть доведен до 50%.

(67,9%), в связи с чем в 2022 году Эфиопия заняла 6 место в глобальном анти-рейтинге «неподключенности к Интернет», который возглавляют КНДР (99,9%), Южный Судан (93%) и Сомали (90,2%) [10].

В силу низкой покупательной способности населения для доступа к сети Интернет преимущественно используются мобильные телефоны. В Эфиопии преобладают сети подвижной связи второго и третьего поколения. В Аддис-Абебе Ethio Telecom с 2015 года предлагает услуги 4G, а с 2022 года и 5G. Средняя скорость соединений для мобильного подключения составляет 19,1 Мбит/с, а по фиксированным линиям 15,9 Мбит/с [11]. Согласно отчету Национального банка Эфиопии, в начале 2023 года в стране было активировано в общей сложности 66,8 млн подключений к сотовой связи, что соответствует 53,5% населения (в 2020 году было 41%) [12]. Из них более четверти составляют подростки 12–17 лет (в городах их доля достигает 45%).

Увеличение доступа к Интернет играет важную роль в ускорении экономического развития Эфиопии, стимулируя формирование предложений в сфере цифровых услуг и сервисов на их основе. Следуя опыту Индии, государство оказывает содействие росту инноваций за счет финансирования строительства современных Центров обработки данных (ЦОД) и технопарков. Согласно «Плану развития и трансформации II» должно быть построено 20 технопарков различного профиля, на данный момент запущено двенадцать[27].

В 2015 году рядом с аэропортом Аддис-Абебы (Bole Lemi) начал функционировать промышленный технопарк, в котором производится ИТ-продукция, в том числе на экспорт[28], в настоящее время при содействии Группы Всемирного банка строится вторая очередь. В нем на площади в 200 га размещается ИКТ-парк мирового класса (Ethio ICT Village) стоимостью около 35,4 млн долл. США, проект осуществляет Ethio Telecom совместно с Министерством инноваций и технологий. ИКТ-парк имеет высокотехнологичное оборудование, в частности высокоскоростную сеть, систему сетевой безопасности и несколько част-

27 В октябре 2023 года Совет министров Эфиопии одобрил законопроект «О преобразовании IP-адресов в особые экономические зоны», который обеспечит правовую основу для преобразования существующей системы индустриальных парков в особые экономические зоны. Источник: Ethiopia Prepares First Personal Data Protection Law // Ethiopian Monitor, 7.10.2023, https://ethiopianmonitor.com/2023/10/27/ethiopia-prepares-first-personal-data-protection-law/

28 ИКТ-экспорт Эфиопии растет в среднем на 2,1% и к 2026 году может достичь 147 млн долл. США. Главным образом это недорогие мобильные телефоны для стран Африки, а также инновации и локализация ИКТ для использования эфиопами, например, клавиатура на амхарском языке. Высокотехнологичный экспорт Эфиопии в 2015-18 гг. вырос с нуля до 2%.

Источники: Ethiopia Science, Technology & Innovation Policy Revie// United Nations Conference on Trade and Development 2020, https://unctad.org/system/files/official-document/dtlstict2020d3_en.pdf, Ethiopia ICT Industry Outlook 2022 – 2026, https://www.reportlinker.com/clp/country/597055/726253

ных ЦОД уровня Tier III[29], в том числе от Raxio Group[30] и компании выходцев из Эфиопии Redfox Solutions[31].

В этом же ИКТ-парке в июле 2023 года компания Wingu Africa, базирующаяся в Джибути, открыла при содействии Инвестиционной комиссии Эфиопии (EIC) свой модульный ЦОД стоимостью 50 млн долл. США, который она будет предлагать для безопасного и надежного хостинга критически важных услуг. Более сотни компаний уже обосновались в ИКТ-парке, в том числе китайская ZTE и несколько стартапов, которые воспользовались услугами местных бизнес-инкубаторов [13] и льготами на использование инфраструктуры парка.

Российская компания BitCluster запустила в декабре 2023 года свой ЦОД мощностью 120 МВт в технопарке Kilinto на юге Аддис-Абебы, его клиентами станут компании и арендаторы, стремящиеся масштабировать свои мощности по добыче биткоина[32] (дешевая электроэнергия обеспечивается мощностями Kilinto, расположенными в технопарке).

Эфиопия имеет даже свою «Силиконовую долину» — инновационный и инкубационный центр Sheba Valley, построенный в Аддис-Абебе при инвестиционной поддержке Института искусственного интеллекта и робототехники для общества (Шэньжень, КНР). Sheba Valley позиционируется как эфиопский Центр исследования искусственного интеллекта, она также является центром социальных и образовательных инициатив, таких как GirlCode Academy, которая дает женщинам возможность делать карьеру в сфере STEM (наука, технологии, инженерия и математика).

В Sheba Valley базируется большое количество стартапов, которые получили уже мировое признание. Например, Icog-Labs стала первой эфиопской исследовательской лабораторией, специализирующейся на искусственном интеллекте, она разработала более 50% программного обеспечения для всемирно известного робота Sophia, который в 2017 году получил гражданство Саудовской Аравии.

---

29 Tier III — высокий стандарт надежности инфраструктуры и оборудования, соответствующий ему ЦОД имеет системы резервного питания, охлаждения и сетевого подключения, специальное дублирующее оборудование, которое позволяет выполнять ремонт и обслуживание систем без остановки работы. Отказоустойчивость составляет 99,982%, т.е. простой не превышает 1,6 часа в год.

30 Лидирующий в Африке провайдер Raxio Group основан в 2018 году американской инвестиционной фирмой Roha Group. Система ЦОД Raxio развертывается в 5 африканских странах (Уганде, Кении, Танзании, Руанде и Эфиопии), что позволит масштабировать услуги модульных ЦОД. Источник: Raxio Data Centre, https://callscenters.com/raxio-data-centre/

31 Согласно переписи населения 2020 года в США проживает более 291 тыс. этнических эфиопов и почти 320 тыс. потомков смешанных браков, общая численность людей с эфиопской кровью в населении США составляет 0,09%. Источник: How many Ethiopians live USA?, https://www.studycountry.com/wiki/how-many-ethiopians-live-usa

32 Правовые условия такой деятельности пока не очень ясны, поскольку Эфиопия запретила криптовалюты. В июле 2022 года Администрация безопасности информационных сетей (INSA) выпустила распоряжение, обязывающее всех физических и юридических лиц, которые участвуют в предоставлении криптоуслуг, включая майнинг и передачу, зарегистрироваться в INSA в течение 10 дней. Предприятия, которые не выполнят требование, столкнутся с серьезными уголовными наказаниями. Источник: Cryptography Regulation in Ethiopia: in Light of INSA's Call for Registration, https://kflip.info/2022/08/29/cryptography-regulation-in-ethiopia/

Другой пример — dVentus Technologies — одна из самых инновационных и высокотехнологичных фирм в мире, имеет несколько запатентованных продуктов и производит интеллектуальные преобразователи энергии, ветряные турбины, силовые установки для транспортных средств на экологически чистой энергии, она экспортирует продукцию в США и Европу. В своей штаб-квартире в Аддис-Абебе компания имеет передовую систему мониторинга в режиме реального времени для управления интеллектуальными сетями и взаимосвязанной аналитикой Больших данных во многих городах мира. Финтех-компания Kifiya обеспечивает бесшовный банкинг и цифровые платежи при взаимодействии правительства с гражданами и бизнеса с клиентами, в 2017 году компания заключила партнерство с Mastercard по созданию международного платежного сервиса, позволяющего семьям и друзьям за границей оплачивать счета с помощью своих дебетовых и кредитных карт, мобильных кошельков или напрямую со своего банковского счета из любой точки мира.

Есть еще ряд ярких примеров[33], их действительно пока не так много, национальная инновационная экосистема пока в зачаточном состоянии, а Эфиопия занимает только 125 место в Глобальном инновационном индексе 2023 года (WIPO оценивала 132 экономики). Гораздо важнее, что эти «первые ласточки» расширяют свое присутствие и выходят на новые рынки, вдохновляют других новаторов и привлекают внимание ведущих компаний и инвесторов со всего мира[34], которые заинтересованы войти на перспективный рынок и выстроить новые цепочки кооперации.

Благодаря этому ИКТ-рынок Эфиопии активно развивается. Его текущий вклад в ВВП составляет примерно 2%[35]. Цифровизация дает инклюзивный эко-

---

33 Yenepay — первое в Эфиопии решение для онлайн-платежей, а Apposit создала платформу мобильных платежей PAGA. Zayride разработала приложение по функциям близкое к Uber и адаптированные для низкоскоростных сетей 2G/3G решения для оплаты поездок. Стартап Flowius разработал доступную платформу поддержки водопроводной системы для многих домов в сельских районах Эфиопии и в 2017 году был принят в акселератор водных инноваций Imagine H2O, базирующийся в Кремниевой долине США. Waziup — приложение, призванное помочь различным секторам экономики континента, включая аквакультуру и сельское хозяйство, а также окружающую среду. Оно предоставляет аналитику Больших данных, начиная от интеллектуального ведения сельского хозяйства и заканчивая прогнозированием погодных условий. SEWE — интеллектуальная система мониторинга жизненно важных органов человека, способная проверять пациентов в режиме реального времени еще до того, как их сможет осмотреть врач. ИТ-отдел может обеспечить анализ больших объемов данных для профилактической, прогностической и упреждающей системы управления здравоохранением. EthioCloud создала платформу, которая позволяет разработчикам искусственного интеллекта работать на родном для Эфиопии амхарском языке, создавая продвинутый программный код. Gebeya действует как торговая площадка, которая объединяет африканских ИТ-специалистов с работодателями, планирует начать выпуск продуктов своих инкубируемых стартапов. Она нанимает, обучает в своем учебном центре и инкубирует лучшие африканские таланты. Источник: ‘Sheba Valley’ and Ethiopia’s buzzing tech ecosystem, https://www.addisherald.com/sheba-valley-and-ethiopias-buzzing-tech-ecosystem/

34 В 2022 году правительство учредило Управление по рынкам капитала в целях подготовки правовой базы для создания фондового рынка и взяло на себя обязательства по либерализации банковской деятельности в ближайшей перспективе. Источник: 2023 Investment Climate Statements: Ethiopia, https://www.state.gov/reports/2023-investment-climate-statements/ethiopia/

35 Согласно данным Google и IFC, ожидается, что цифровая экономика в Африке достигнет 5,2% ВВП в 2025 году и 8,5% в 2050 году. Источник: Ethiopia’s Digital ID Ecosystem: A Legal and Policy Review // Ethiopian Business

номический рост и занятость населения, особенно молодежи и женщин. Появляются стартапы в таких областях, как цифровая медицина[36] и финтех. Последняя сфера применения наиболее привлекательна для инвесторов, поскольку этот сегмент ИКТ-рынка и цифровых банковских продуктов может дать взрывной рост, поскольку он практически не освоен: даже коммерческие структуры предпочитают расчеты наличными[37], 67% граждан не имеют банковских счетов, для стимулирования использования платежных карт бюджетникам зарплату начисляют на карточные счета.

С целью продвижения безналичных расчетов государство сделало очень важный шаг, внедрив систему цифровых удостоверений личности на основе биометрических данных Fayda (см. Раздел 3.4). Это позволит ликвидировать барьер доступа к госуслугам, здравоохранению и социальной помощи, финансовым инструментам для огромного числа граждан и беженцев, которые не имеют свидетельств о рождении или удостоверяющих документов[38]. Благодаря этому на финансовом рынке Эфиопии в 2021 году произошло знаковое событие — Ethio Telecom впервые запустила общенациональный сервис Telebirr (бырр — национальная валюта) для электронных платежей и цифровых кошельков. Сервис позволил осуществлять онлайн платежи с использованием обычного телефона (транзакции через SMS и USSD[39]) или мобильного приложения[40]. Для удобства пользователей интерфейс реализован на языках пяти основных этносов. Партнерами сервиса стали уже 25 банков. В конце 2023 года объявлено, что более 55 государственных и частных учреждений интегрировали сервис Telebirr в системы расчетов, что позволяет всем резидентам осуществлять перечисление налогов и госпошлин, получать кредиты, участвовать в операциях финансового рынка [14]. За два года число пользователей взлетело почти до 40 млн, а объем совершенных транзакций через Telebirr превысил 1,44 трлн бырр.

Ближайший конкурент — кенийская платформа электронных платежей M-presa от Safaricom за несколько месяцев с момента запуска в Эфиопии набрала 7 млн пользователей и намерена довести свою клиентскую базу до 30% населе-

---

Review, https://ethiopianbusinessreview.net/ethiopias-digital-id-ecosystem-a-legal-and-policy-review/

36 В значительной степени успехи в этой сфере связаны с присутствием на местном рынке проектов Агентства США по международному развитию (USAID).

37 Для этого широко используется распространенная в арабском мире и Среднем Востоке неформальная финансово-расчетная система на основе взаимозачета требований и обязательств между брокерами Хава́ла.

38 На Африканском континенте 500 млн человек не имеют никаких документов, это более 40% населения (в основном молодёжь и женщины). Источник: С. Моктар Цифровизация как способ преодоления неравенства в Африке // Россия в глобальной политике, 1.01.2024, https://globalaffairs.ru/articles/czifrovizacziya-v-afrike/?ysclid=ls668ut03l923446251

39 Коммуникационный протокол USSD (Unstructured Supplementary Service Data, «неструктурированные дополнительные сервисные данные») используется в GSM-сетях для обмена короткими текстовыми сообщениями, которые не хранятся ни на стороне оператора, ни на устройстве абонента.

40 Следует отметить, что операторы связи оформляют клиенту SIM-карту только после предоставления подробной информации о себе, включая имя и адрес, удостоверение личности, фотографии и подписи.

ния страны. Эти перемены дают надежду на быструю активизацию цифровой экономики, причем не только в потребительском секторе. Например, M-presa создала повсеместно доступную платформу для использования финансовых сервисов мелкими фермерами, что способствует расширению экосистемы «умного» сельского хозяйства и финтеха, сбору данных для управления рисками, применения цифровых решений для изменения формирования стоимости и экспорта кофе, отслеживания цепочек поставок [15].

Ожидается, что к 2025 году объем финансовых онлайн транзакций в Эфиопии превысит 3 трлн бырр, что составляет 39% от общего ВВП страны. Это в свою очередь может стимулировать развитие сегмента онлайн торговли, который на данный момент практически отсутствует.

Развитие услуг электронного правительства является пока основным драйвером роста ИКТ-сектора, но уровень зрелости этого сегмента еще низкий: согласно Индексу развития электронного правительства ООН в 2022 году Эфиопия заняла лишь 179 место в мире [16]. На различных этапах разработки и внедрения находятся 24 платформы цифрового государства. Не менее пяти из них развиваются с участием КНР и международных организаций. Наиболее успешно и устойчиво функционируют портал госуслуг и Единая информационная система госзакупок.

Пять платформ находятся в процессе доработки. В частности, Единый реестр сведений о населении, Система сбора платежей с грузовых автомобилей (работает пока только в столице), Общенациональная цифровая транспортная платформа, Электронная виза (E-visa). Около 12 проектов находятся на начальной стадии разработки или внедрения, в их числе единая система идентификации и авторизации (Ethiopia National ID Program, NIDP) и ее биометрическая часть. В сентябре 2022 года началось тестирование системы цифровой идентификации Fayda, что предполагает создание системы распознавания лиц и единой биометрической системы. В стадии разработки платформа Центрального статистического агентства Эфиопии, которая должна способствовать межведомственной координации. Бюро защиты окружающей среды и управления земельными ресурсами заявило о начале реализации проекта единого национального кадастра. Министерство доходов ведет работу по созданию электронной налоговой службы. Разработка системы Европротокол онлайн (часть проекта TRANSIP) финансируется Всемирным банком [17]. Заявлены планы создания государственного облачного хранилища, подписано соглашение о строительстве центра обработки данных[41].

Большой объем различных проектов цифровизации, особенно в части обработки персональных данных, требует комплексного решения вопросов обеспе-

41 Монополия Ethio Telecom вынуждает использовать имеющиеся у компании центры обработки данных.

чения информационной безопасности. В этом направлении государству предстоит много сделать для улучшения ситуации. Согласно разработанному МСЭ Глобальному индексу кибербезопасности в 2020 году Эфиопия соответствовала уровню слабо развитой страны (115 место в мире). Среди участвовавших в рейтинге 38 африканских стран она заняла 21 место (лидеры – Мавритания, Танзания и Гана) [18]. Схожие оценки Эфиопии дал в июле 2023 года Киберцентр НАТО: по уровню кибербезопасности 103 место в мире, 170 — по уровню развития ИКТ и 127 — по уровню сетевой готовности [19].

Подавляющая часть средств обеспечения кибербезопасности поставляется в страну из-за рубежа (компаниями из США, ЕС, КНР, присутствует также Лаборатория Касперского). При этом наиболее сложной проблемой остается отсутствие квалифицированных национальных кадров, которые могли бы грамотно эксплуатировать закупленное оборудование и поддерживать системы информационной безопасности.

Эфиопия давно озаботилась вопросом повышения уровня образования и подготовки необходимых специалистов. По данным Всемирного банка она тратит в среднем 12% своего годового бюджета на систему образования, однако основная часть этих средств идет на начальную и среднюю школу, поскольку еще недавно только треть населения страны была грамотной. Реализуется Дорожная карта развития образования в Эфиопии (2020–2030), разработана Национальная ИКТ-политика для высшего и профессионально-технического образования [20]. Придавая особую значимость подготовке инженеров и исследователей, введена 70% квота на обучение по программам STEM, остальные 30% отданы специальностям в области социальных наук[42].

Подвижки уже есть, например, количество государственных университетов с 2000 года увеличилось с 4 до 40, а количество студентов — до 800 тыс., растет связка образовательных учреждений и бизнеса, создан Институт инноваций и развития технологических талантов[43]. Но недостаток вакансий приводит к «утечке мозгов» — массовому оттоку преподавателей, научно-технических и медицинских работников, а также перспективных студентов. По данным Международной организации по вопросам миграции, за последние 10 лет из Эфиопии

42 Однако отмечается, что такая пропорция была установлена без должной проработки потребностей экономики и оценки готовности инфраструктуры и преподавательского состава. По факту около 30% инженеров–выпускников не могут найти работу. Источник: Ethiopia Science, Technology & Innovation Policy Review // United Nations Conference on Trade and Development, 2020, https://unctad.org/system/files/official-document/dtlstict2020d3_en.pdf

43 В 2023 году Министерство инноваций и технологий открыло Центр развития талантов в области инноваций и технологий, который в первый год принял 500 одаренных студентов, количество обучающихся планируется довести до 1 тыс. Агентство безопасности информационных сетей учредило Центр талантов в киберсфере (Ethio-Cyber Talent Center) для подготовки квалифицированных кадров. Источник: Ethiopia's technological foundations in 2022, January 21, 2023, https://ethiopianpress.net/ethiopias-technological-foundations-in-2022/

уехало почти 75% квалифицированных специалистов[44]. В связи с этим особую значимость приобретает интеграция выпускников и молодых талантов в инновационную экосистему. Необходимы инкубационные и исследовательские центры, акселераторы для трансфера разработанных ИТ в реальный сектор экономики, посредники для маркетинговой поддержки стартапов. На рынке Эфиопии уже появились такие компании, как Gebeya, Iceaddis и Blue Moon, которые осваивают эту нишу, но им приходится конкурировать с сильными западными игроками. Важна также смычка с бизнесом и межотраслевые связи, в этих целях создана Академия стартапов, которая знакомит владельцев бизнеса и инвесторов с инновационной экосистемой Африки, запущен общенациональный портал Yegara для связи стартапов с инвесторами.

В настоящее время стоит задача налаживания эффективного управления и регулирования для создания благоприятной среды для экономического и социального развития.

2. О стратегическом планировании в области цифровизации и обеспечения информационной безопасности

2.1. **Десятилетний перспективный план развития** (2021–2030)

Эфиопия поэтапно осуществляет развитие страны: план на 2000–2010 гг. включал задачи ликвидации бедности и экономического роста, план на 2010–2020 гг. — устойчивого роста и экономической трансформации. В Перспективном плане развития на 2021–2030 появились задачи повышения производительности и конкурентоспособности частного сектора, главную роль в решении которых должны сыграть развитие технологических возможностей и цифровая экономика.

В предыдущем разделе отмечены стартовавшие программы по строительству национальных производственных и ИКТ-центров, а также ЦОД для анализа Больших данных наиболее важных секторов экономики (сельское хозяйство, финансы, инженерные разработки, демографические исследования, биоинформатика), по внедрению цифровой идентификации и экосистемы электронных платежей. Также в планах развитие электронной торговли, которая будет поддержана строительством в Аддис-Абебе Восточноафриканского логистического узла. Основные целевые показатели плана: ввод в действие трех государственных ЦОД, увеличение перечня госуслуг со 176 до 2,5 тыс., рост до 3,5 тыс. учреждений,

44 По оценочным данным, за годы после обретения независимости Африка в целом потеряла треть квалифицированных специалистов, т.е. порядка 300 тыс. чел. На сегодняшний день только в США работает больше африканских ученых и инженеров, чем во всех странах континента вместе взятых. Источник: С. Алексеева Эфиопия и диаспора: как остановить «утечку мозгов», 06.05.2015, https://ruvek.mid.ru/publications/efiopiya_i_diaspora_kak_ostanovit_utechku_mozgov_9719/

пользующихся услугами электронного маркетинга, за счет увеличения охвата электронными сервисами с 2% до 85% населения. Обеспечение 100% доступности Интернет и покрытия мобильной связью, подключение всех коммерческих предприятий к широкополосным сетям связи.

2.2. Национальная политика и стратегия в сфере информационных и коммуникационных технологий (2009, 2016)

Первый отраслевой документ стратегического планирования был принят в 2002 году, затем обновлен в 2009 году[45]. Национальная политика и стратегия в сфере информационных и коммуникационных технологий (2016) напрямую увязала задачи экономической трансформации с развитием сетей связи и цифровизацией. Однако ее частичное выполнение не позволило выровнять использование ИКТ в столице и регионах, недостаточное развитие современной инфраструктуры не дало возможности значимо использовать ИКТ в бизнесе и инновациях, высокая стоимость оконечных устройств и услуг связи не содействовали росту интеграции населения в производство и социальную жизнь, повышению осведомленности и цифровой грамотности.

В 2016 году политика в ИКТ сфере была доработана в части макроэкономических, структурных и секторальных реформ. Помимо задач развития инфраструктуры, подготовки кадров и расширения использования ИКТ государством, бизнесом и обществом, был взят курс на повышение роли частного сектора в ИКТ-отрасли, совершенствование правовой и регуляторной базы. В частности, на достижение следующих целей:

- создание условий для притока инвестиций, снижения налогов и бюджетной поддержки;
- содействие ключевому инструменту экономического развития — электронной торговле за счет внедрения электронных платежей, почтовых и логистических услуг, сотрудничества с международными игроками в этой сфере и повышения осведомленности населения;
- обеспечение всех универсальным доступом к ИКТ-сервисам, мониторинг качества сетевых услуг и их доступности.

2.3. Стратегия «Цифровая Эфиопия 2025» (2020)

В середине 2020 года был опубликован разработанный Министерством инноваций и технологий первый комплексный документ стратегического плани-

45 The National Information and Communication Technology (ICT) Policy and Strategy

рования в сфере экономической трансформации страны — «Цифровая Эфиопия 2025 — стратегия для всеобщего процветания Эфиопии» [21]. В отличие от рассмотренных выше планов он позиционирует цифровую экономику не только как инструмент внутренней реструктуризации и развития, но и как важнейшую задачу интеграции в глобальные производственные цепочки Индустрии 4.0. Поэтому в Стратегии определены четыре блока межотраслевых задач, для каждой из них даны анализ текущего состояния, имеющиеся инициативы и рекомендации по дальнейшим действиям:

- Развитие инфраструктуры, в том числе энергетической, транспортной, а также ядра ИКТ-инфраструктуры (мобильная связь, оптоволоконные сети, доступные оконечные устройства для подключения к Интернет);
- Формирование всеобъемлющей экосистемы для совмещения инфраструктуры с пользователями цифровых приложений и услуг (цифровые ID, системы электронных платежей, системы идентификации и аутентификации пользователей, скоординированная и централизованная система информационной безопасности);
- Разработка приложений, обеспечивающих цепочку создания добавленной стоимости в цифровой экономике (взаимодействие государства, бизнеса и граждан);
- Создание цифровой экосистемы, как базиса взаимодействия эффективной регуляторной политики; финансовая и монетарная политика; развитие человеческих ресурсов[46] и т.д.

Решение задач каждого блока будет происходить за счет реализации краткосрочных, среднесрочных и долгосрочных межотраслевых инициатив в интересах развития четырех приоритетных для Эфиопии секторов экономики:

Сельское хозяйство. Повышение эффективности аграрного сектора (технологии Интернета-вещей, блокчейн, цифровых платформ, Больших данных);

Производство. Развитие цепочек создания стоимости (робототехника, логистика);

Сервисные отрасли. ИТ-интеграция (широкополосное подключение, ЦОДы, искусственный интеллект);

Туризм. Цифровые технологии как фактор повышения конкурентоспособности в туризме (повышение доступности и связанности с Интернет, цифровой маркетинг, мобильные приложения).

Их реализацию планируется осуществить за счет благоприятной почвы для конкурентоспособного участия частного сектора в цифровой экономике. Стра-

46 Министерством высшего образования (MoSHE) разработаны «ICT Policy and Strategy for Higher Education and TVET» и «Digital Skills Action Plan 2020-2030», Источник: Digital Education in Ethiopia //Addis Ababa University, May 16, 2023, http://www.aau.edu.et/blog/digital-education-in-ethiopia/

тегией определены 15 краткосрочных инициатив, включая, реформу телекоммуникационного сектора; дерегулирование рынка мобильной связи для повышения конкуренции и снижения цены услуг; модернизация и развитие правительственной сети связи WoredaNet; внедрение универсального доступа; создание цифрового удостоверения личности; усиление кибербезопасности; развитие услуг электронного правительства; развитие электронных торговых площадок и разработка регулирования мобильных денег, подготовка кадров для цифровой экономики и создание рабочих мест, повышение цифровой грамотности, создание инкубаторов для стартапов, выстраивание взаимодействия бизнеса и государства.

Кроме того, определены 7 среднесрочных (от 18 мес. до 3 лет) и долгосрочных (3–5 лет) инициатив с указанием головных ведомств и основных заинтересованных участников, однако плановые показатели оценки достижения целей в Стратегии отсутствуют.

На реализацию «Цифровой Эфиопии 2025» Всемирный банк одобрил концессионное кредитное соглашение на сумму 200 млн долл. США [22]. Эти деньги будут вложены в Цифровой фонд Эфиопии, участниками которого являются несколько заинтересованных сторон: головной исполнитель и учреждение-получатель — Министерство инноваций и технологий (MInT), ведущий партнер-исполнитель — Администрация связи Эфиопии (ECA), Сеть образовательных и научных учреждений Эфиопии (EthERNet), Портал министерства финансов.

2.4. **Национальная программа цифровой идентификации** (2021)

Национальная программа цифровой идентификации (NIDP) является одной из инициатив стратегии «Цифровая Эфиопия 2025». Она реализуется под руководством Канцелярии премьер-министра путем введения единой общенациональной системы идентификации для резидентов страны, мигрантов и беженцев, отсутствие которой создает препятствия участию в основных видах деятельности официальной экономики, таких как открытие банковских счетов, получение денежных переводов и социальных субсидий, доступ к медицинской страховке и образованию, подача заявлений на получение государственных документов и многих других[47].

Следует отметить, что помимо свидетельства о рождении и удостоверения личности в Эфиопии широкое использование имеет Kebele ID — карточка с циф-

47 Идея Национальной программы идентификации была первоначально рассмотрена правительством Эфиопии еще в 2011 году по инициативе Национальной службы разведки и безопасности (NISS) в сотрудничестве с Агентством безопасности информационных сетей (INSA) и другими правительственными органами. До начала 2018 года Служба иммиграции и гражданства (бывшая INVEA) координировала усилия по созданию платформы цифрового ID. Однако из-за многих проблем усилия не привели к ожидаемому прогрессу и практическим результатам. Источник: National ID History, https://id.gov.et/en/history/

ровым идентификатором, выдаваемая государственными органами по месту жительства. Однако она не имеет единой информационной базы, идентификационные данные децентрализованы, что создает условия для злоупотреблений. Создаваемая национальная система цифровой идентификации Fayda должна стать инклюзивным, надежным, защищенным, единым источником идентификации, сократить утечки информации и мошенничество в государственных программах, обеспечить информационную безопасность и больший контроль над персональными данными, укрепить доверие к онлайн-транзакциям, придав важный импульс развитию Эфиопии.

Реализация NIDP в Эфиопии, как и во многих других странах Африки, осуществляется в интересах Целей устойчивого развития ООН. Движение цифровой идентификации континента ID4Africa[48] поддерживается Группой Всемирного банка[49], Комиссией Африканского союза, Африканским банком развития, Программой развития ООН и другими организациями. Подобные программы в Индии, Нигерии и Кении показали свою эффективность, поэтому с 2019 года начались разработки технической платформы Fayda, а затем и ее пилотное тестирование, в котором приняли участие 3,5 млн резидентов Эфиопии [23]. В 2023 году был принят закон «О цифровой идентификации» (См. Раздел 3.4), который стал правовой основой полномасштабного внедрения Fayda. Системой к 2025 году планируется охватить 70 млн человек, для чего количество лицензиатов для сбора идентификационных данных существенно расширено.

Для получения уникального 12-значного номера в системе Fayda необходимо предоставить демографические и биометрические данные. Если последние достаточно традиционны (отпечатки пальцев, радужные оболочки глаз и фотография), то перечень демографических данных, относящихся к конфиденциальной информации, достаточно обширный. В случае, если человек не имел ранее удостоверяющих документов от него потребуют имя и фамилию отца и деда, данные матери, почтовый и электронный адрес и, при необходимости, свидетельства трех членов его местного сообщества, обладающих цифровыми идентификаторами.

Технологическая платформа Fayda использует программное обеспечение с открытым программным кодом, развиваемое индийским некоммерческим товариществом MOSIP (Modular Open Source Identity Platform) [24]. После регистрации идентификация пользователя с помощью Fayda может осуществляться через ее веб-сайт или универсальный интерфейс для мобильных приложений (API), что дает доступ к сервисам электронного правительства, Национального

48 При этом штаб-квартира движения ID4Africa расположена в США, http://www.id4africa.com/

49 Всемирный банк в рамках своего проекта «Цифровое удостоверение для интеграции и услуг» выделил 350 млн дол. США на реализацию NIDP. Источник: National ID. World Bank Supports Ethiopia's Digital ID Project to Increase Access to Services and Economic Opportunities, https://id.gov.et/updates/Press/World-Bank-Supports-Ethiopia's-Digital-ID-Project-to-Increase-Access-to-Services-and-Economic-Opportunities

банка и других финансовых институтов, Министерства финансов и сборов, электронных торговых площадок и т.д. По предварительным оценкам, Fayda может сэкономить около 110 млрд часов за счет упрощения электронных государственных услуг и персонификации налоговых льгот, в финансовом секторе снизит финансовые мошенничества и облегчит реализацию инициативы «знай своего клиента (KYC)». В условиях расширения Африканской зоны свободной торговли (AfCFTA) преимущества цифрового удостоверения личности могут выйти за рамки национальных границ.

2.5. **Национальная политика и стратегия кибербезопасности** (2021)

В октябре 2021 года правительством была принята «Национальная политика и стратегия кибербезопасности Федеративной Демократической Республики Эфиопия» [25], которая скорректировала одноименный документ 2011 года с задачами цифровизации страны и актуальными угрозами информационной безопасности.

Целью Стратегии является защита национальных интересов путем создания самодостаточного потенциала кибербезопасности, позволяющего защитить национальные данные и критическую информационную инфраструктуру от компьютерных атак. При этом отмечено, что задача обеспечения кибербезопасности является общенациональной и требует повышения координации и партнерства государства с частным сектором и другими ключевыми участниками.

Документ определяет восемь основных направлений действий, а также цели и стратегии для их достижения: совершенствование правового регулирования, повышение национальной осведомленности в сфере кибербезопасности, наращивание потенциала, осуществление научных и конструкторских разработок, цифровая идентификация и обеспечение безопасности персональных данных, защита критических инфраструктур, национальное и международное сотрудничество.

Кроме того, определяются рамки реализации политики и стратегий и необходимые обеспечительные меры. Стратегическое руководство будет осуществлять Национальный совет кибербезопасности. Практическая работа возложена на Агентство безопасности информационных сетей (INSA) и его оперативное подразделение Эфиопскую группу реагирования на инциденты информационной безопасности (EthioCERT). Государственные учреждения и частные предприятия, владеющие критической информационной инфраструктурой обязаны разрабатывать и применять программы кибербезопасности, соответствующие национальной стратегии и международным стандартам. Под руководством INSA должна быть создана система мониторинга кибербезопасности, сбора и анализа

актуальных данных, система уведомления об угрозах и инцидентах, а также регулярная оценка эффективности применяемых мер.

В качестве индикаторов выполнения поставленных задач в документе указаны стабильные социально-культурные, экономические и политические условия, создание национального, отраслевого и объектового потенциала кибербезопасности, обеспечение собственными продуктами и услугами кибербезопасности, воспитание культуры безопасного поведения в информационном пространстве, создание с участием частного сектора индустрии кибербезопасности, укрепление на всех уровнях партнерства и сотрудничества для защиты национальных интересов и суверенитета.

2.6. Проект национальной политики в области искусственного интеллекта (2023)

По данным 2023 года, Министерство инноваций и технологий Эфиопии завершает разработку проекта национальной политики в указанной сфере. В документе будет описано текущее положение дел и направления будущего развития, включая управление данными, развитие человеческих ресурсов, исследования и разработки, содействие и поощрение, инфраструктуру, законодательство и этику, а также сотрудничество и координацию. Проект содержит подробные соображения по разработке национальных руководящих принципов обмена данными, качества и этики исследований, нормативно-правовой базы и руководящих принципов использования человеческих ресурсов в кооперации с заинтересованными сторонами. Политика определит более совершенную форму процедур, которые должны выполняться всеми регионами страны, городскими администрациями, а также международными институтами, партнерами и заинтересованными сторонами.

Эфиопия уже создала Национальный центр искусственного интеллекта и продолжит развивать экосистему профильных исследований. Университеты и колледжи должны иметь аналогичные центры и исследовательские подразделения, для этого инвестиции в создание и сбор данных будут увеличены.

2.7. Подготовка к разработке политики в сфере открытых данных (2016)

Исследование и внедрение технологий искусственного интеллекта невозможно без расширения обмена наборами данных, необходимых для машинного обучения и анализа. Во всех странах огромными массивами открытых данных обладают государственные ведомства, но для их использования необходимо разра-

ботать нормативную базу, а также привести данные к стандартизированному виду и создать условия доступа к ним. При поддержке Всемирного банка в 2014 году проведено исследование готовности правительства Эфиопии к применению и институционализации политики открытых данных, в результате которого разработан ряд предложений по интеграции принципов открытых данных в государственном секторе и разработке планов действий. Несмотря на то, что с участием отдельных ведомств был запущен государственный портал открытых данных[50], повторное исследование в 2016 году отметило отсутствие лидерства правительства в реализации необходимых преобразований [26]. В том же году коммерческие компании вышли с собственной инициативой, сформулировав основные принципы в рассматриваемой сфере, которые были одобрены правительством [27]. Проект «Национальной политики открытых данных правительства Эфиопии» [28] с 2018 года находится в стадии обсуждения, уровень реализации низкий.

Вместе с тем Министерством науки и высшего образования в 2019 году утверждена «Национальная политика открытого доступа в высшем образовании». Она предписывает всем 47 эфиопским университетам обеспечить размещение опубликованных статей, тезисов, диссертаций и результатов исследований во внутренних репозиториях и в Национальном академическом цифровом репозитории (NADRE), который поддерживается министерством. Доступ к научным материалам будет осуществляться с помощью Сети образовательных и научных учреждений Эфиопии (EthERNet). Все сотрудники, осуществляющие научные работы за счет государственного бюджета, должны обеспечить соответствие своих материалов следующим принципам: возможность поиска и повторного использования, доступность, интероперабельность. Реализация указанной политики будет способствовать возможности всему миру видеть научные достижения Эфиопии, распространению знаний, снижению дублирования исследований и затрат [29].

3. Состояние нормативной базы в сфере цифровизации и обеспечения национальной информационной безопасности

Реализация стратегии «Цифровая Эфиопия 2025» включает инициативу создания нормативно-правовой базы для цифровизации страны, которая должна быть безопасна для пользователей и обеспечивать баланс интересов государства, бизнеса и граждан[51]. В последние 5 лет нормотворчество значительно активизи-

50 Портал «data.gov.et» дает свободный и бесплатный доступ к открытым данным госучреждений, общее количество наборов данных не превышает 100. Источник: Data Catalog // Ethiopia Data Portal, https://ethiopia.opendataforafrica.org/data/#menu=topic

51 Конституция Эфиопии 1994 года является высшим законом страны. Парламент издает прокламации (законы), за которыми следуют постановления, принимаемые Советом министров, и директивы по их реализации, которые принимаются министерствами или агентствами. Правительство привлекает общественность для получения

ровалось, при формировании правовой базы особое внимание уделено решению следующих задач:

- развитие законодательной базы, регламентирующей информационную политику и функциональные действия государственных органов;
- создание национальной системы цифровой идентификации и национальной поисковой системы;
- налаживание связей и сотрудничества с иностранными государствами в сфере обеспечения информационной безопасности;
- разработка собственного программного обеспечения, позволяющего удовлетворить потребности населения Эфиопии;
- обязательная подготовка пользователей в области информационной безопасности;
- обеспечение беспрепятственного доступа правоохранительных органов Эфиопии к данным о состоянии информационной безопасности, а также предоставления им возможности мониторинга активности пользователей;
- реализация комплекса мер, исключающего или сокращающего до минимума возможность анонимного доступа населения к сети Интернет;
- организация долговременного хранения архивов с адресами посещаемых веб-сайтов и анализ деятельности интернет-пользователей.

Из приведенного перечня следует формирование двух нормативных блоков. Первый из них создает правовые условия для развития ИКТ-отрасли и цифровых услуг в рамках стратегии «Цифровая Эфиопия 2025».

3.1. **Конституция Федеративной Демократической Республики Эфиопия** (1995)

Конституция страны [30] содержит положения, касающиеся защиты частной жизни, которые отражают меры защиты, закрепленные в основных международных документах по правам человека. Так, Статья 26 предусматривает, что каждый человек имеет право на неприкосновенность частной жизни, [включая] право не подвергаться обыску в своем доме, обыску имущества и лично, или конфискации любого имущества, находящегося в его личном владении. Более того, Статья 26(2) предусматривает «право на неприкосновенность [своих] записей и корреспонденции, включая почтовые письма, а также на общение, осуществляемое по телефону, телекоммуникационным средствам и электронным

обратной связи перед принятием законопроекта посредством публичных собраний, а регулирующие органы запрашивают комментарии по предлагаемым нормативным актам у заинтересованных сторон. Министерства или регулирующие агентства не проводят оценок воздействия предлагаемых нормативных актов и обзоров по применению норм.

устройствам». Статья 26(3) предусматривает исключения, когда эти права могут быть ограничены, например, в «непреодолимых обстоятельствах и в соответствии с конкретными законами, целями которых являются обеспечение национальной безопасности или общественных целей, предотвращение преступлений или защита здоровья, общественной морали или прав и свобод других лиц».

Статьей 29 Конституции гарантируется право на свободу выражения мнений без какого-либо вмешательства. Это право включает свободу искать, получать и распространять информацию и идеи любого рода, независимо от государственных границ, устно, письменно или печатно, в художественной форме или с помощью других средств по своему выбору. Гарантирована свобода печати и средств массовой информации, а также свобода художественного творчества. Свобода печати, в частности, включает права: запрет цензуры в любой форме, предоставление доступа к информации, представляющей интерес для общественности[52]. Прессе должна быть предоставлена «институциональная независимость и правовая защита, позволяющие ей учитывать различные мнения и обеспечивать свободный поток информации, идей и мнений, необходимых в демократическом обществе». Конституцией закреплено, что «любые средства массовой информации, финансируемые или контролируемые правительством, должны быть организованы таким образом, чтобы учитывать различия во мнениях». Вместе с тем: «Ничто из вышеизложенного не освобождает кого-либо от ответственности, вытекающей из законов, принятых для защиты общественной морали, мира, человеческого достоинства и демократических прав граждан».

3.2. **Закон «Об электронной подписи»** (2018)

Закон № 1072/2018 юридически признал электронные подписи и цифровые документы, определил права и обязанности сторон, участвующих в информационном обмене: предоставление информации в электронной форме законодательно приравнено к предоставлению ее в письменной форме.

В законе введены два вида электронной подписи: «простая», когда подпись содержит «информацию в электронной форме, прикрепленной к электронному сообщению или логически связанной с ним, которая может использоваться для идентификации подписавшего в отношении электронного сообщения и для указания согласия подписавшего с информацией, содержащейся в электронном сообщении», а также «усиленная» — тип электронной подписи, использующей асимметричную систему шифрования и однозначно идентифицирующей подписанта.

52 Закон Эфиопии «О свободе средств массовой информации и доступе к информации (с поправками, внесенными законом «О средствах массовой информации» №1238/2021)

Статья 9 налагает на Агентство безопасности информационных сетей (INSA) осуществление функций корневого удостоверяющего центра, что на деле означает поддержание функционирования национальной инфраструктуры отрытого ключа (PKI), необходимой для всех цифровых сервисов в сети Интернет. INSA должна заверять цифровые сертификаты, которые будут действительны 5 лет, если они не будет отменены или аннулированы, возвращены или прекращены в соответствии с заявлением. Могут быть признаны не только отечественные поставщики сертификатов, но и зарубежные, если они соответствуют требованиям этого закона (Статья 20). INSA также имеет полномочия и обязанности выдавать лицензии поставщикам сертификатов и контролировать их деятельность, обеспечивать надежность и общую безопасность криптосистемы; определять рабочие процедуры и стандарты, которым поставщики сертификатов должны следовать. Последние обязаны хранить информацию, связанную с выдачей, приостановлением действия, отзывом сертификата или сопутствующими услугами в течение 2 лет, а также сохранять конфиденциальность персональных данных. Закон предусматривает различные институты урегулирования спорных ситуаций с сертификатами [31].

3.3. **Закон «Об электронных транзакциях»** (2020)

В 2020 году в Эфиопии принят очень важный «Закон об электронных транзакциях» № 1205/2020 [32], который направлен на создание ясных и безопасных условий предоставления цифровых государственных услуг, электронной торговли и иных цифровых коммерческих сервисов.

Закон признает действительность и возможность приведения в исполнение электронного контракта под эгидой подхода функциональной эквивалентности, предполагающий существование эквивалентных обычных договорных правил. Таким образом, появилась законодательная основа для электронной торговли, платежей и других видов сделок, которые можно осуществлять повсеместно, удаленно, виртуально, мгновенно и при участии электронного посредника (цифрового сервиса) [33]. Для этого закон регулирует службы электронных сообщений[53] и администрирование национальной доменной зоны «.et» и связанные с этим сферы. Это функционал Администрации связи Эфиопии (ECA).

В целях выполнения закона на Министерство инноваций и технологий возложен выпуск директив по стандартам ИТ, передаче электронных сообщений, ограничению ответственности посредников, защиты пользователей, цифровых госуслугах, федеральном электронном регистре законодательных актов (Federal

53 В законе под термином «электронное сообщение» понимается информация или электронный документ, созданный, переданный или хранящийся с помощью средств цифровизации.

Negarit Gazeta), управлении и сохранении электронных сообщений, методах проверки отправителя и верификации электронных сообщений и др. Кроме того, законодательно предписано создать Национальный совет цифровой экономики.

3.4. Закон «О цифровой идентификации» (2023)

Как было отмечено выше закон «О цифровой идентификации» № 1284/2023 [34] стал нормативной основой реализации Национального плана цифровой идентификации на принципах инклюзивности, безошибочности, минимизации данных, взаимосвязанности, транспарентности, доступности и технологичности.

Согласно закону, регистрация в системе цифровой идентификации и ее использование — это процесс, основанный на согласии, следовательно, любая аутентификация личности владельца регистрации должна осуществляться с согласия владельца регистрации. При регистрации в системе необходимо предоставить персональные данные, которые имеют разные характеристики. «Биометрические данные» относятся к физическим атрибутам, которые используются для уникального определения личности, такие как отпечатки пальцев, радужная оболочка глаза и фотографии лица (Статья 2(5)). «Демографические данные» определяются как небиометрические личные атрибуты резидента, введенные в систему цифровой идентификации, такие как имя, гражданство, дата рождения, пол, адрес и номер телефона (Статьи 2(6) и 9). Категория «конфиденциальные данные» обособляет чувствительные персональные данные, в т.ч. расовое или этническое происхождение, генетические данные, физическое или психическое здоровье или состояние, политические взгляды, религиозные убеждения или другие верования аналогичного характера, совершение или предполагаемое совершение правонарушения, а также любое разбирательство в связи с совершенным или предположительно совершенным правонарушением и прекращение такого разбирательства или приговор любого суда в ходе разбирательства (Статья 2(18)). Сбор данных, свыше требуемых, влечет за собой уголовную ответственность — штраф от 10 до 100 тыс. быр.

Регистрирующая организация обязана применять строгие административные, юридические, процедурные и технические меры предосторожности для обеспечения защиты персональных данных от стихийных бедствий или техногенных катастроф, электронных атак, кражи, уничтожения и других подобных потерь (Статья 17(12)), а также сохранять конфиденциальность персональных данных владельцев регистрации в течение всего цикла деятельности по цифровой идентификации, включая сбор, аутентификацию, хранение и обработку данных. Установлены общие запреты на сбор, раскрытие, распространение, печать, использование, передачу копии третьей стороне или

публичное раскрытие личной информации владельцев регистраций. Нарушение норм грозит наказанием от 1 до 5 лет обычного, а в особых случаях до 8 лет строгого тюремного заключения. Если указанное преступление совершено юридическим лицом, наказание будет в виде штрафа от 100 до 500 тыс. бырр (более 9 тыс. долл. США).

Согласно закону, Совет министров имеет право издать постановление о создании государственного органа, наделенного полномочиями для контроля реализации норм закона, или реструктурировать уже существующую государственную организацию. В их полномочия входит создание и организация национальной системы удостоверения личности, руководство сбором биометрических и демографических данных и выдачей цифрового удостоверения личности, организация демографических данных для принятия политических решений правительством и предоставление услуг аутентификации. По факту такой уполномоченной организацией является Офис Программы цифровой трансформации и регулирования Министерства инноваций и технологий.

3.5. **Закон «О защите персональных данных»** (2023)

Несмотря на запуск тестирования национальной системы цифровой идентификации, развитие услуг электронного правительства и коммерческих цифровых сервисов, единых нормативных требований по правилам сбора, обработки, хранения и обеспечения безопасности персональных данных (ПД) не существовало. Этот пробел был ликвидирован в конце октября 2023 года, когда первый всеобъемлющий закон «О защите персональных данных» был одобрен Советом министров Эфиопии и передан в парламент для дальнейшего обсуждения и ратификации.

По имеющимся данным закон соответствует международным стандартам защиты ПД, он создает правовую базу для поддержки культуры и практики защиты ПД в Эфиопии. В нем признается неприкосновенность частной жизни в качестве конституционного права и подчеркивается необходимость развития цифровой экономики при одновременной защите прав человека и основных свобод. В документе определены ключевые термины, обеспечивающие ясность и взаимопонимание между заинтересованными сторонами.

Закон предоставляет субъектам ПД больший контроль над их данными. Излагаются конкретные права, такие как право на доступ, исправление и удаление ПД, а также право возражать против их обработки (Статья 36). Субъекты данных уполномочены давать конкретное и осознанное согласие на обработку своих ПД.

Закон затрагивает различные аспекты их обработки, включая сбор, хранение, систематизацию, извлечение, использование, раскрытие и уничтожение ПД.

Подчеркивается важность получения согласия от субъектов данных и определяются условия законной обработки, гарантирующие, что ПД обрабатываются в конкретных и законных целях. Для повышения безопасности ПД закон вводит такие меры, как шифрование, псевдоанонимизация и ограничения на передачу данных. Это требует от организаций принятия соответствующих технических и организационных мер для предотвращения несанкционированного доступа, раскрытия или потери ПД. Признавая глобальный характер потоков данных, закон признает юрисдикцию зарубежных стран и международных организаций в области трансграничной передачи данных и поощряет международное сотрудничество и соответствие глобальным стандартам защиты ПД (на практике это положение означает отсутствие требования локализации данных на территории страны).

Для контроля соблюдения закона создается независимый орган, подотчетный только парламенту — Комиссия по защите персональных данных, которая уполномочена проводить расследования, издавать руководящие принципы и налагать штрафы за несоблюдение закона [35]. Контролеры данных должны обеспечивать законную и справедливую обработку, принимать соответствующие меры безопасности и уведомлять Комиссию о любых нарушениях закона.

3.6. Проект закона «О стартапах и инновационном бизнесе» (2020)

Нормативный акт [36] разработан Министерством инноваций и технологий в 2020 году и до сих пор проходит межведомственное согласование[54]. Его целью заявлено создание благоприятной среды для развития инноваций за счет поддержки стартапов и содействия получения ими финансовых ресурсов. В настоящее время стартапы не могут получить финансирование в основном из-за отсутствия обеспечения для заимствования в традиционных финансовых учреждениях[55], а также испытывают трудности с привлечением зарубежных средств из-за требований инвестиционного законодательства Эфиопии.

Закон определяет несколько важных инструментов поддержки. Прежде всего, Национальный совет по стартапам, в который войдут 7–9 членов и министр инноваций и технологий. Целью совета является «стимулирование экономического роста путем создания экосистемы, способствующей развитию инноваций и технологий, а также созданию новых рабочих мест». Совет будет наблюдать и поддерживать начинающие компании, для чего будет создан Технический консультативный совет из представителей как государственных, так и частных за-

54 По данным эфиопской прессы основным нерешенном вопросом является определение кто будет распоряжаться Инвестиционным фондом, который должен быть сформирован на основании закона.
55 Например, эфиопские банки требуют 100% обеспечение кредита.

интересованных сторон. Он будет иметь право принимать заявки на получение статуса «начинающий бизнес» и «инновационный бизнес», управлять этим процессом и принимать решения по заявкам, давать рекомендации Национальному совету по использованию средств Инновационного фонда.

Задачей последнего является финансирование стартапов и инновационного бизнеса в Эфиопии. Фонд, контролируемый Советом, будет использоваться для выплаты стипендий стартапам и сборов за регистрацию интеллектуальной собственности, расходов на административную поддержку, стимулов для разработчиков экосистемы и предоставления гарантий. Предполагается, что он будет пополняться за счет государственного бюджета, займов и внешних пожертвований.

Предлагаются и другие меры, например, стартапам и инновационным предприятиям будет предоставлено право открывать счета на FOREX, банковская карта для финансирования необходимых бизнесу онлайн-услуг. Они получат налоговые льготы и доступ к юридическим «песочницам». Стартапы освобождаются от сбора любых государственных налогов (с оборота, на добавленную стоимость, подоходного налога на 2 года), а также от бремени аренды офисов, которые являются обязательным условием получения лицензии.

Создателям экосистемы, таким как инкубаторы, будет разрешен доступ к возможностям финансирования и налоговым льготам. Инвесторы, работающие со стартапами, будут иметь право на налоговые льготы на прирост капитала и пр.

Второй блок нормативных актов обеспечивает сохранение контроля государства над национальным информационным пространством и соблюдение в нем верховенства закона.

3.7. **Уголовный кодекс** (2004)

Уголовный кодекс (УК)[56] представляет собой нормативный правовой акт, состоящий из положений, приятых в различные периоды времени. Он является основным и наиболее важным источником уголовного права, в котором введены преступления в компьютерной сфере и принципы уголовного наказания за них.

Также УК криминализует нарушение неприкосновенности частной жизни путем нарушения конфиденциальности корреспонденции или отправлений, включая, среди прочего, вторжение в чьи-либо письма, телеграммы, телекоммуникационные сети и другую электронную переписку. Наказание — штраф или тюремное заключение на срок до 6 месяцев (Статья 606). Более того, УК предусматривает уголовную ответственность за нарушение профессиональной тайны (Статья 399). Подлежат наказанию профессионалы, которые разглашают охраня-

56 The Criminal Code of the Federal Democratic Republic of Ethiopia Proclamation № 414/2004.

емую законом информацию, полученную в ходе выполнения профессиональных обязанностей, включая адвокатов, юрисконсультов, поверенных, арбитров, экспертов, присяжных заседателей, сотрудников частных компаний, врачей, стоматологов, медсестер и вспомогательный медицинский персонал.

Криминализация других правонарушений, связанных с запрещенным использованием современных средств связи и сети Интернет, осуществлена в большом количестве правовых актов, приведенных ниже.

3.8. Закон «О запрете мошенничества в телекоммуникациях» (2012)

Нормы указанного закона [37] направлены на защиту национальной безопасности и борьбу с экономическими потерями, связанными с мошенничеством в телекоммуникационных сетях.

Часть 2 разрешает деятельность в сфере телекоммуникаций и услуг связи только на основе лицензий. Запрещено использование в сетях связи аппаратного и программного обеспечения, не получившего лицензию Министерства связи и информационных технологий, сроками заключения до 15 лет и серьезными штрафами караются их ввоз, производство, обладание и продажа. Всем, кроме авторизованных провайдеров и законных пользователей, запрещено получать доступ к телекоммуникационным сетям, сервисам и системам. Запрещено незаконное подключение к сетям и незаконный перехват, использование аппаратуры для распространения террористических сообщений и другой противоправной деятельности[57]. Также запрещено получать мошеннический доступ к неоплаченным услугам, развертывание и подключение аппаратуры к чужим сетям связи, незаконные манипуляции и дублирование SIM-карт, кредитных карт, идентификационных номеров и данных. Помимо заключения под стражу и штрафов полагается конфискация аппаратуры.

Часть 3 касается правоохранительной деятельности по выявлению описанных выше деяний, сбору доказательств, а также предписывает создать в полиции специализированные национальные технические силы.

3.9. Закон «О запрете использования сервисов IP-телефонии» (2012)

Власти страны обосновали запрет использования VoIP обеспечением национальной безопасности и поддержанием монополии местных телекоммуникационных компаний. Под запрет попали сервисы, которые для передачи данных используют сквозное шифрование (такие как Skype, Google Talk), а также сер-

57 Перечень действий определяется законом «О противодействии террористической деятельности» № 652/2009.

вис анонимизации пользователей Tor. За применение указанных ИКТ-продуктов можно получить тюремный срок до 15 лет. Закон закрепил за Министерством инноваций и технологий право контролировать и выдавать лицензии всем негосударственным компаниям, импортирующим в страну оборудование, используемое для передачи информации [38].

3.10. Закон «О компьютерных преступлениях» (2016)

Закон «О компьютерных преступлениях» № 958/2016 регулирует неправомерное использование ИКТ и цифровой среды[58]. Криминализированы основные типы правонарушений против конфиденциальности, целостности, и доступности данных и компьютерных сетей:

- несанкционированный доступ к ним и компьютерное мошенничество;
- унижение достоинства, распространение угроз, лживой информации и новостей;
- производство, предложение, продажа, распространение, предоставление доступа или незаконное владение изображениями или видео с детской порнографией[59];
- вмешательство в компьютерные системы и уничтожение данных;
- шпионаж, разглашение данных;
- другие правонарушения в компьютерной сфере.

Закон вводит градацию наказаний в зависимости от типа объекта, в отношении которого осуществляются незаконные действия. Несанкционированный доступ к компьютерной системе, компьютерным данным или сети целиком/ее части наказывается простым тюремным заключением на срок до 3 лет и/или штрафом 30–50 тыс. бырр. Если деяние совершено в отношении объектов информатизации, которые предназначены для использования юридическим лицом или критически важной инфраструктурой, то наказание может повлечь строгое тюремное заключение от 3 до 20 лет и/или штраф в размере до 500 тыс. бырр (Статьи 4-6).

Государственные органы, которым стало известно о совершении преступлений, предусмотренных законом (включая нарушение конфиденциальности дан-

58 Computer Crime of the Federal Democratic Republic of Ethiopia Proclamation No. 958/2016 (2016), при этом следует отметить, что Эфиопия не подписала Конвенцию Африканского союза о кибербезопасности и защите персональных данных, которая была одобрена 27 июня 2014 года на 23 сессии Ассамблеи Африканского союза в г. Малабо, соответственно ее положения не имплементированы в национальное законодательство.

59 По данным Интерпола за 2021 год около 10% эфиопских подростков 12–17 лет, пользующихся Интернетом (преимущественно Facebook и Telegram), становятся жертвами сетей детской порнографии, унижения и травли. Источник: Protecting-children-in-Ethiopia-from-online-sexual-exploitation-and-abuse-The-way-forward, June 2022, https://respect.international/wp-content/uploads/2022/06/Protecting-children-in-Ethiopia-from-online-sexual-exploitation-and-abuse-The-way-forward-.pdf.

ных путем незаконного и неавторизованного доступа), или о распространении любого незаконного контента третьими лицами через компьютерную систему, которой он управляет, обязаны немедленно уведомить Агентство безопасности информационных сетей (INSA), сообщить о преступлении в полицию и принять соответствующие меры (Статья 27). Также введен ряд новых правил доказывания и процедуры, которые помогут в расследовании и судебном преследовании за компьютерные преступления. Однако закон вызвал критику, главным образом из-за некоторых его положений, ущемляющих права человека [39].

3.11. Закон «О допуске и контроле продуктов информационных технологий» (2023)

Указанный закон[60] принят в декабре 2023 года, но пока не опубликован. Он направлен на предотвращение угроз национальной безопасности, которые создают ввозимые без контроля ИКТ-системы и средства[61], а также на повышение осведомленности общественности об этих рисках. Его разработка свидетельствует, что правительство осознает роль ИКТ в процессах разрушения гражданского единства Эфиопии и дезинтеграции, построенной на принципе этнического федерализма[62]. Главенствующую роль в этом играют внешние силы. Своих целей на Африканском роге пытаются достичь не только региональные государства Восточного Средиземноморья и стран Персидского залива, но и такие глобальные игроки как США и Китай [40].

Закон ограничивает ввоз в страну технологических устройств и ИКТ со специальными возможностями (таких как, нарушение электронных сигналов, взлом информационных систем, дезинформация, удаление и кража данных). После вступления в силу закона потребуются разрешительные лицензии даже дипломатическим работникам для импорта в страну дронов, GPS-систем, спутниковой связи, видеокамер высокого разрешения.

Закон предоставляет Агентству безопасности информационных сетей (INSA) полномочия по внедрению соответствующих процедур и выдаче специальных разрешений на импорт/экспорт, производство и использование ИКТ

60 Information Technology Products Security Clearance and Control Proclamation.

61 Ввозимые средства содействуют созданию неконтролируемых государством каналов обмена информацией, которые сохраняются даже в условиях блокирования доступа к Интернет или к зарубежным социальным медиаплатформам. По некоторым данным Эфиопия является «лидером» Восточной Африки в отключении Интернет по политическим основаниям.

62 В соответствии со Статьей 39(1) Конституции «Каждая национальность, народность и народ Эфиопии имеет безусловное право на самоопределение, включая право на выход из состава государства». В последнее десятилетие происходит значительная политизация этничности, что приводит к значительным внутренним конфликтам, а также обострению отношений с Суданом и Египтом. По данным Национального исследования конфликтных ситуаций, с 2018 по 2023 год в Эфиопии произошло 5,3 тыс. конфликтов, в результате которых погибли тысячи людей.

ограниченного доступа. Национальная служба разведки и безопасности (NISS) будет сотрудничать с другими уполномоченными органами для составления списка технологических устройств, на которые будут наложены ограничения. Нарушения закона будут караться крупными штрафами и даже тюремным заключением до 5 лет [41].

В целом уровень зрелости правового регулирования цифровизации в Эфиопии по новой методике оценки МСЭ[63] оценивается как переходный, т.е. использующий поэтапный подход.

4. Основные государственные органы, входящие в систему обеспечения национальной информационной безопасности и форматы государственно-частного партнерства

Следует отметить, что система государственного управления Эфиопии не совсем прозрачна, а официальные информационные ресурсы министерств и ведомств находятся в процессе развертывания, в связи с чем содержат очень ограниченные наборы сведений. Основные элементы системы приведены на схеме.

4.1. Национальный совет кибербезопасности

Совет учрежден в 2011 году в рамках реализации задач «Национальной политики и стратегии кибербезопасности»[64]. Он является руководящим исполнительным органом правительства в сфере обеспечения информационной безопасности. В его непосредственном подчинении находится Агентство безопасности информационных сетей (INSA), которое административно входит в Министерство мира.

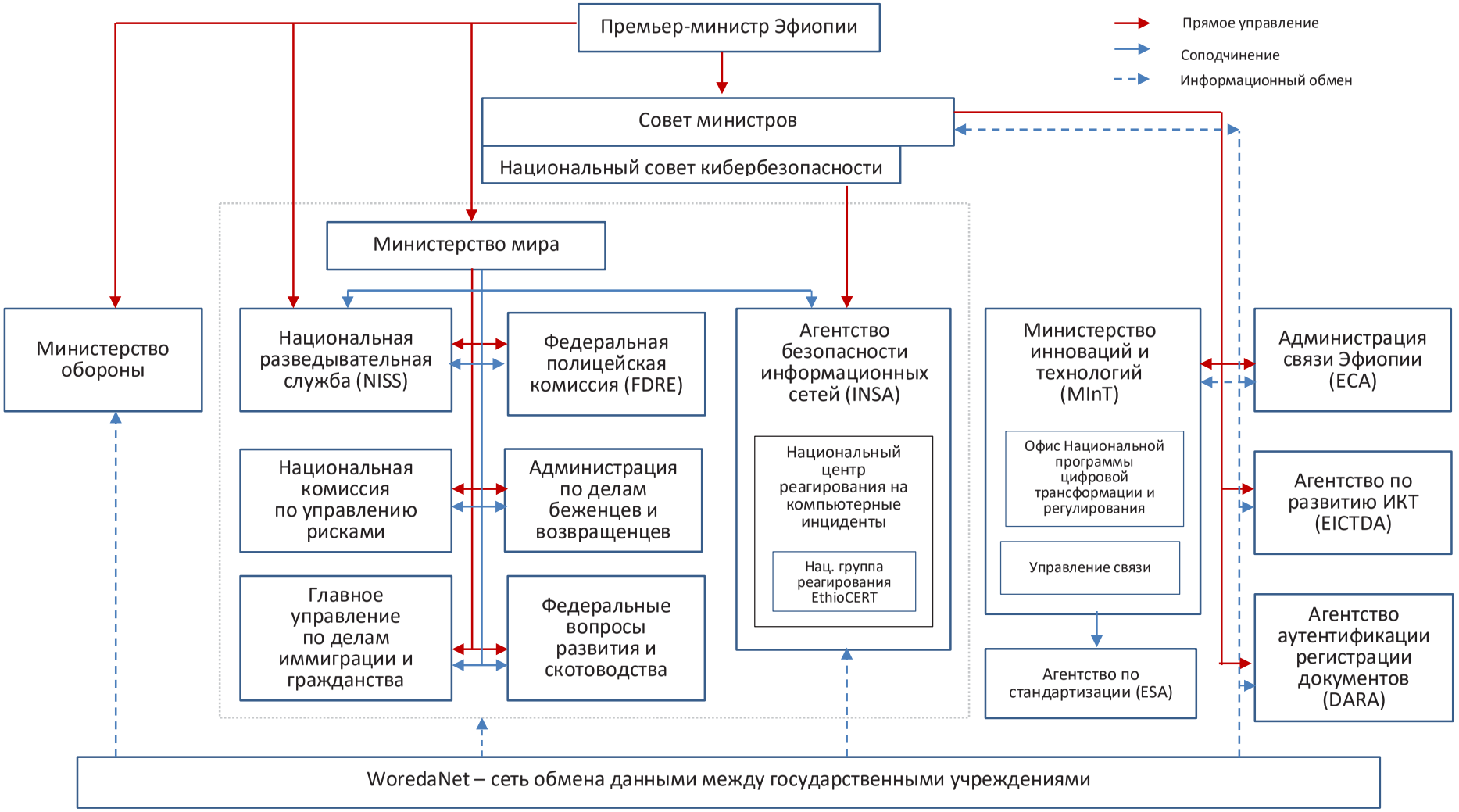
4.2. Министерство мира (МОР)

Формирование такого специфического государственного органа отражает попытки правительства сбалансировать интересы многочисленных этнических групп и противостоять попыткам дезинтеграции государства. Ведомство выделено из Министерства федеральных дел в рамках реорганизации государственного управления в 2018 году, его главной задачей является устранение внутренних конфликтов, а также предотвращение общественных потрясений,

63 В методике «G5 Benchmark» оцениваются 4 параметра: межотраслевое управление на национальном уровне, принципы разработки политик, Инструментарий цифрового развития (кибербезопасность, защита данных, телекоммуникации в чрезвычайных ситуациях и совместное использование межотраслевой инфраструктуры), повестка дня в области цифровой экономики (инновационная система, цифровая трансформация, участие в международных и региональных интеграционных инициативах).

64 В открытом доступе данные о функционировании Национального совета кибербезопасности отсутствуют.

Схема. Основные элементы управления системой национальной информационной безопасностью Эфиопии



содействие «миру, демократии и развитию» и «сосредоточение внимания на поддержании закона и порядка и создании политического единства среди народов и регионов страны». Функции министерства определены законом №1097-2018 [42], в том числе:

- выявление факторов нестабильности, которые могут привести к внутренним конфликтам;
- укрепление национальной разведки и безопасности, в том числе в части информационных сетей и финансовой сферы;
- надзор и развитие исполнительных функций, имеющих отношение к Федеральной полиции;
- ведение и развитие функций, связанных с гражданством, национальными идентификационными картами, иммиграцией, паспортами и регистрацией актов гражданского состояния и страхования;
- рассмотрение вопросов миграции, политических беженцев и репатриантов.

Для решения этих задач в структуре министерства действуют несколько самостоятельных федеральных служб, три из которых имеют прямое отношение к обеспечению информационной безопасности и контролю национального информационного пространства.

4.2.1. **Агентство безопасности информационных сетей** (INSA)

Ведет свою историю с 1999 года, когда было создано Национальное агентство по радиотехнической разведке и кибербезопасности Эфиопии для защиты от причинения вреда данным и национальной информационной инфраструктуре[65]. В 2006 году агентство воссоздано постановлением Совета министров № 130/2006 как INSA. Является автономным федеральным правительственным учреждением, подотчетно главе кабинета министров (генеральный директор назначается премьер-министром). Полномочия и функции агентства расширены правительственным постановлением № 250/2011 и законом № 808/2013. На данный момент они включают:

- разработку национальной политики, законов, стандартов и стратегий, позволяющих обеспечить безопасность информации и ключевых компьютерных инфраструктур, надзор за их исполнением;
- осуществление всех необходимых контрмер для защиты от компьютерных или электромагнитных атак на информационные и компьютерные инфраструктуры/системы или на психологическое состояние граждан;
- организация и администрирование деятельности Национального центра реагирования на компьютерные инциденты;

65 Создано на основании Постановления Совета министров № 130/1999.

- контроль импорта и экспорта ИКТ, датчиков и технологий для осуществления информационных атак;
- регулирование оборота криптографических средств и транзакций с их применением;
- выполнение функций национального корневого удостоверяющего центра;
- сотрудничество с правоохранительными органами (сбор цифровых доказательств по запросу о поддержке процесса расследования компьютерных преступлений может осуществляться даже дистанционно, по решению Генерального прокурора может вестись слежка за подозреваемым и перехват его электронных коммуникаций), оказание технической поддержки, предоставление информации о пользователях, проведение технического анализа собранных данных;
- проведение цифровой судебной экспертизы по ордеру суда и в сотрудничестве с полицией в отношении компьютерной техники или инфраструктур, которые предположительно подвергаются или являются источником компьютерной атаки, для предотвращения атак и обеспечения раннего предупреждения граждан;
- осуществление международного сотрудничества в рамках своих полномочий.

Национальный центр реагирования на компьютерные инциденты решает аналитические, организационно-технические и оперативные задачи в том числе мониторинг и обеспечение безопасности национального сегмента сети Интернет. **Эфиопская группа реагирования на компьютерные инциденты EthioCert** является его оперативно-техническим подразделением. Группа создана в 2011 году в целях реагирования на компьютерные инциденты в правительственных агентствах и критических информационных инфраструктурах. Ее функции включают мониторинг безопасности, анализ угроз, повышение защищенности от компьютерных атак, координацию реагирования на инциденты, наращивание потенциала и сертификацию. Только за первую половину 2022 года EthioCert выявила более 2 тыс. попыток осуществления кибератак, большинство из которых было направлено на финансовые учреждения, органы образования, службы безопасности и разведки, СМИ, правительственные учреждения и здравоохранение. INSA отреагировало на 91,5% из них, что сэкономило стране 15 млрд бырр [43]. Группа является членом Международного форума групп реагирования FIRST и региональной группы AfricaCERT.

4.2.2. **Национальная служба разведки и безопасности** (NISS)

Служба создана в 1935 году, многократно меняла названия и подчиненность, в 2013 году воссоздана под названием NISS [44], имеет статус министерства и напрямую подотчетна премьер-министру. В ее функции входит внешняя и внутрен-

няя разведка, анализ разведывательной информации в интересах защиты национальной безопасности, информирование об угрозах Национальных сил обороны и органов защиты правопорядка, борьба с терроризмом[66] и диссидентами, обеспечение общественного порядка, защита критических информационных инфраструктур, расследование серьезных преступлений, в том числе компьютерных [45]. На основании Статьи 14 закона «О противодействии терроризму» NISS имеет право осуществлять в отношении подозреваемых наблюдение и законный перехват электронных средств коммуникации (телефон, факс, радио, Интернет, почта). В 2022 году функционал Службы расширен на осуществление и координацию противодействия психологической войне, направленной на Эфиопию, а также на ведение общенациональной базы данных угроз национальной безопасности [46].

4.2.3. **Федеральная полицейская комиссия** (FDRE)

Ведомство создано в соответствии с директивами №720/2004 и 720/2011. В функции Федеральной полицейской комиссии входит: расследование преступлений, связанных с информационными сетями и компьютерными системами; предотвращение и расследование преступлений, связанных с подделкой валют и платежных инструментов; предотвращение и расследование преступлений, связанных с торговлей людьми, [...] борьба с терроризмом; содействие в разработке национальных стандартов и наращивании потенциала полиции; сбор, анализ и распространение информации о причинах преступлений на национальном уровне.

4.3. **Министерство инноваций и технологий** (MInT)

В современном виде MInT сформировано в 2019 году путем слияния Министерства науки и технологий (MOST) и Министерства связи и информационных технологий (MCIT)[67]. Его основная миссия – устойчивое развитие инновационной экосистемы Эфиопии и трансфер технологий в реальный сектор экономики. В части развития и использования ИКТ в полномочия министерства входят следующие задачи [47]:

- разработка и контроль выполнения национальных программ научных и технологических исследований с учетом приоритетов развития страны, планов институционального развития и человеческих ресурсов;

66 NISS заключила договоры о сотрудничестве в сфере борьбы с терроризмом с ФБР США, израильской службой Моссад и ФСБ России. Источник: Intelligence Files: Inside Ethiopia's National Security and Intelligence Service, February 7, 2023, https://theafricancriminologyjournal.wordpress.com/2023/02/07/ethiopias-national-security-and-intelligence-service/

67 Министерство инноваций и технологий Эфиопии (MInT) впервые учреждено как государственное учреждение на уровне комиссии в соответствии с положением закона № 62/76. В 2009 году комиссия была реорганизована в Федеральную комиссию науки и технологий со статусом министерства, преобразована в Министерство науки и технологий (MOST) законом № 1097/2011.

- профессиональная и техническая поддержка региональных инноваций и технологических организаций;
- разработка в сотрудничестве с уполномоченными органами стандартов обеспечения качества, надежности и безопасности ИКТ-услуг, контроль их применения;
- разработка и надзор за реализацией национальной системы идентификации, изучение и применение технологий с участием соответствующих органов;
- контроль того, чтобы задачи критических систем и сервисов в государственном секторе были обеспечены надлежащими технологиями и предоставлялись обществу лучшими сервис-провайдерами;
- создание базы данных инноваций и технологий, сбор информации, разработка национальных стандартов для управления информацией;
- в сотрудничестве с уполномоченными органами поддержка развития, применения и координации защищенной информационной сети государственных учреждений федерального и регионального уровня;
- координация деятельности заинтересованных участников по созданию и надлежащему использованию системы доменных имен верхнего уровня страны (национальный сегмент сети Интернет «.et»); назначение и контроль доменных имен государственных органов, регистрация IP-адресов для координации их информационных систем;
- лицензирование и регулирование операторов телекоммуникационных и почтовых услуг, проверка качества ИКТ-оборудования;
- выдача и контроль использования радиочастотного спектра.

Известно о некоторых структурных подразделениях министерства. Так Офис Программы цифровой трансформации и регулирования отвечает за ее реализацию, разработку и внедрение необходимых технологий и инфраструктуры. В функции Управления связи входит мониторинг информационного пространства на предмет выявления антиправительственных материалов, представляющих угрозу для суверенитета страны и дискредитирующие власти, а также информации, порочащей религиозные, духовные и культурные ценности или направленной на подрыв национального единства. Поиск в социальных сетях оппозиционно настроенных группировок и отдельных лиц, призывающих к смене власти, противодействие террористической и экстремистской деятельности с использованием сетей и ИКТ.

Под юрисдикцией министерства также находятся следующие исполнительные органы: Институт технологий и инноваций (Tech in), Управление радиационной защиты Эфиопии (ERPA); Эфиопский институт космической науки и техники (ESSTI); Эфиопский институт биотехнологии (EBTi); Институт геопространственной информации (GII), а также Агентство по стандартизации.

4.3.1. **Агентство по стандартизации Эфиопии** (ESA)

Государственное некоммерческое агентство, ведущее свою историю с 1970 года. Под наименованием ESA действует с 2010 года, подведомственно Министерству инноваций и технологий.

ESA ставит перед собой амбициозную задачу стать к 2025 году ведущим центром передового опыта в сфере стандартизации среди стран со средним уровнем дохода. Агентство намерено создать благоприятные условия для трансфера технологий и внести значительный вклад в социально-экономическое развитие страны за счет повышения конкурентоспособности национальных продуктов и услуг, продвигая признанную международным сообществом стандартизацию и систему управления качеством продукции, практику обучения и техническую поддержку. Кроме того, ESA занимается разработкой национальных технических стандартов, продвигает их внедрение, выпускает технические регламенты, осуществляет контроль соответствия, оказывает техническую поддержку, консультирование и помощь в применении стандартов.

ESA уполномочено взаимодействовать с органами стандартизации других государств и представлять интересы Эфиопии в международных и региональных органах стандартизации. В частности, Агентство является аффилированным членом Международной электротехнической комиссии (IEC), участником комиссии CODEX, основателем и членом совета Африканской региональной организации по стандартизации (ARSO). Кроме того, ESA является членом ISO/IEC JTC 1/SC 41, в том числе по тематике «Биометрия», «Умные транспортные системы», «Нанотехнологии», «Информация и документация», «Информационные технологии для обучения, образования и подготовки».

Одним из значимых результатов ESA стала международная стандартизация в ISO раскладки клавиатуры для арахамского языка и выработка стандартной компьютерной терминологии, что обеспечило на национальном уровне простую коммуникацию всех пользователей и взаимодействие разработчиков программного обеспечения [48].

4.4. **Администрация связи Эфиопии** (ECA)

Является самостоятельным федеральным органом, выполняет функции национальной Администрации связи и регулятора отрасли связи, а также национальной Администрации почтовой службы и Государственного агентства по сертификации ИКТ. Кроме того, ECA отвечает за функционирование национальной службы регистрации доменных имен, управления адресным пространством национального сегмента сети Интернет. В соответствии с законом «О цифровой идентификации» ECA обладает полномочиями по обеспечению информационной

безопасности, конфиденциальности и защиты данных, в соответствии с законом «Об услугах связи» имеет право издавать директивы для обеспечения защиты интересов потребителей.

4.5. **Агентство по развитию ИКТ** (EICTDA)

Агентство создано в 1995 году с целью обеспечения благоприятных условий для развития ИКТ и их эффективного применения в интересах национального социального и экономического развития. Отвечает за развертывание и функционирование правительственной сети WoredaNet. Это наземная широкополосная и спутниковая сеть для предоставления ИКТ-услуг, таких как видеоконференции, каталогизация, обмен сообщениями и передача голоса по IP-протоколу, а также подключение к Интернету федеральных, региональных государственных учреждений и организаций уровня «woreda» (район), всего более 900 органов.

EICTDA имеет мандат на разработку и координацию выполнения политик и стратегий в сфере ИКТ, в соответствии с ним Агентство принимало участие в разработке Национальной стратегии кибербезопасности [49].

4.6. **Агентство аутентификации и регистрации документов** (DARA)

DARA является специализированным государственным агентством при Генеральном прокуроре, осуществляет различные нотариальные действия, которые включают, помимо прочего, аутентификацию и регистрацию документов; сверку копий документов с их оригиналами и их регистрацию; хранение образцов подписи, составление типовых документов проверки и аутентификацию сделок с недвижимостью. В связи с увязкой деятельности Агентства с банковским сектором, DARA вовлечено в реализацию национальной программы цифровой идентификации и является одним из ведомств, на которые возложены обязанности по защите персональных данных и безопасности деловых транзакций [50].

4.7. Примеры государственно-частного партнерства

Эфиопская ассоциация кибербезопасности (ECySA) занимается повышением осведомленности общества и частного сектора об угрозах и видах рисков в киберпространстве. Осуществляет работу по повышению квалификации специалистов государственного и частного сектора в сфере информационной безопасности и защиты инфраструктуры, управлению рисками, адаптации к передовой практике и стандартам для различных информационных технологий. ECySA предоставляет консультационные услуги по внедрению политик кибербезопасности,

смягчению последствий компьютерных атак, обеспечению бесперебойной работы сетей и сервисов, предотвращению потерь данных и нарушения бизнеса.

5. Участие в международном сотрудничестве с ООН и другими международными и региональными организациями в области формирования системы международной информационной безопасности

Эфиопия является единственной африканской страной, которая не была колонизирована. Она возглавила на континенте антиимпериалистическую борьбу и Организацию Африканского единства, в 1923 году стала соучредителем Лиги наций, а в 2002 году инициатором создания Африканского союза[68]. В настоящее время Эфиопия играет важную роль в региональных делах и на международной арене[69].

Аддис-Абеба является крупным центром международной дипломатии. В ней расположены штаб-квартиры Африканского союза, Организации Африканского единства и Экономической комиссии ООН для Африки[70], Региональное бюро Программы развития ООН для Африки[71], Региональное представительство МСЭ[72], офис МВФ. Присоединение Эфиопии к БРИКС несомненно повышает политическое влияние объединения.

5.1. Организация Объединенных Наций

ООН работает над поддержкой Эфиопии в достижении национальных приоритетов и Целей устойчивого развития. В сфере цифровизации можно отметить

---

68 В Аддис-Абебе ежегодно проводятся сессии Ассамблеи глав государств и правительств стран-участниц ОАЕ, а Эфиопия часто выполняет на континенте посреднические функции по многочисленным обращениям африканских стран. Источник: В.С. Ягья Внешнеполитические факторы развития Эфиопии в новейшее время, https://libmonster.ru/m/articles/view/ВНЕШНЕПОЛИТИЧЕСКИЕ-ФАКТОРЫ-РАЗВИТИЯ-ЭФИОПИИ-В-НОВЕЙШЕЕ-ВРЕМЯ?ysclid=lr90wskkz9779615692

69 Эфиопия является членом Африканского банка развития, Африканского, Карибского и Тихоокеанского сообщества государств, Организации ООН по продовольствию и сельскому хозяйству, Группы 24, Группы 77, Межправительственной организации по развитию, МАГАТЭ, МБРР, Интерпола, Международной ассоциации по развитию, Международного фонда развития сельского хозяйства, МВФ, Международной организации по вопросам миграции, МСЭ, Многостороннего агентства по гарантированию капиталовложений, Движения неприсоединения, Организации по запрету химического оружия, Постоянного арбитражного суда, ЮНЕСКО, Международной организации по охране интеллектуальной собственности, Международной организации по туризму, ВТО (в качестве наблюдателя) и др. Источник: Участие в международных организациях и режимах, основные внешнеполитические контрагенты и партнёры, отношения с Россией // Политический атлас современности, http://www.hyno.ru/tom4/2043.html

70 Экономическая комиссия для Африки состоит из 54 государств-членов, это единственное учреждение ООН, которому поручено работать на региональном и субрегиональном уровнях в целях содействия социально-экономическому развитию Африки.

71 Региональное бюро Программы развития ООН для Африки состоит из Регионального центра услуг, расположенного в Аддис-Абебе и 46 представительств в странах Африки.

72 Региональное представительство МСЭ в Аддис-Абебе оказывает содействие 44 государствам-членам в регионе.

проект ЮНЕСКО при технической поддержке Huawei «Высокотехнологичные открытые школы для всех» (TeOSS), целью которого является содействие приобретению цифровых знаний, обучение преподавателей необходимым навыкам использования уже имеющихся и новых ИКТ-технологий для повышения качества обучения. Основное внимание уделяется созданию ИКТ-инфраструктуры для установления связей между экспериментальными школами, создания интегрированной с платформой подготовки учителей системы управления обучением [51].

Международный союз электросвязи, как специализированная организация ООН также оказывает содействие Эфиопии, в частности, при технической поддержке Cisco действует Центр цифровой трансформации, который ориентирован на подготовку кадров в удаленных районах страны, обучение женщин цифровым и предпринимательским навыкам, подготовку востребованных специалистов, разработку программ обучения [52].

Эфиопия стремится обозначать свое присутствие в глобальной ИКТ повестке. Правительство страны приняло участие во Всемирном саммите по информационному обществу (ВВИО, 2005). В 2022 году в Аддис-Абебе проведен XVII Форум по управлению Интернетом, в котором приняли участие более 5 тыс. человек из 170 стран мира. Среди тем, которые обсуждались: подключение всех людей к Интернет, недопущение фрагментации сети, обеспечение кибербезопасности, защита прав человека и уважение частной жизни, управление данными, применение передовых технологий, включая искусственный интеллект.

5.2. Африканский союз

Как член Африканского союза Эфиопия участвует в деятельности его органов и разработке документов стратегического планирования и нормативной базы, в частности «Повестки 2063», которая предусматривает развитие, цифровизацию, обеспечение гендерного равенства, «зеленую» экономику, использование возобновляемых источников энергии и др.

Африканский союз оказывает содействие экономической трансформации Эфиопии, в частности Африканский банк развития осуществляет финансирование правительства для реализации политики цифровизации страны.

Эфиопия не присоединилась к Конвенции о киберпреступности ЕС, но взаимодействие в правоохранительной сфере осуществляется посредством Механизма полицейского сотрудничества Африканского союза (AFRIPOL) [53] и Интерпола. Последний в 2021 году объявил о запуске при финансовой поддержке Великобритании новой инициативы по борьбе с киберпреступностью (AFJOC, стоимостью с £2,9 млн), которая включает повышение потенциала национальных правоохранительных органов, сбор и анализ информации о деятельности пре-

ступников; проведение скоординированных действий под руководством разведки; содействие сотрудничеству с членами AFRIPOL. Благодаря этому в 2023 году в африканских странах ликвидировано 24 преступных киберсети, которые намеревались завладеть более чем 40 млн долл. США [54].

5.3. Европейский союз

Политика ЕС в отношении Эфиопии в 1990-х годах была обусловлена стремлением стимулировать проведение в стране реформ и программ развития. Основная масса финансовой помощи ЕС поступает в страну в форме грантов. В стратегической перспективе ЕС видит Эфиопию членом ВТО. Помимо стимулирования социально-экономических преобразований программы помощи ЕС рассчитаны на демократизацию страны и повышение значения прав человека [55].

Главный инструмент внешней политики ЕС в Африке – трансфер политик управления и регулирования (в том числе в сфере цифровых финансовых услуг, наращивания потенциала, поддержки цифровой экосистемы) и создание гармонизированной нормативной базы для выгодного взаимодействия. В 2021 году ЕС создала Рабочую группу по цифровым финансовым услугам в Эфиопии, чтобы обеспечить платформу для сотрудничества между участниками отрасли. В части финансирования известно о поддержке Евросоюзом шести цифровых проектов в рамках Панафриканской программы, в 2021 году выделено 82,5 млн евро, из них 38,7% на развитие континентального рынка AfCFTA, 30,3% на продовольственную безопасность и мониторинг экосистем с использованием космических технологий и лишь 9,6% на цифровизацию и обмен знаниями. Планируется создать Европейскую группу по цифровизации, которая будет охватывать базовые цифровые услуги и доступ к финансированию для малых и средних предпринимателей в сельскохозяйственном секторе. Большинство проектов все еще находится на концептуальной стадии, проводятся обсуждения с различными заинтересованными сторонами, чтобы найти общие интересы и приоритеты [56].

6. Участие в международном сотрудничестве с другими государствами в области цифровизации и информационной безопасности

6.1. Китайская Народная Республика

Китай является основным экономическим и торговым партером Эфиопии, в 2022 году доля китайской высокотехнологичной продукции в общем объеме

импорта составила 29% (4,96 млрд долл. США)[73]. Пекин одновременно является главным инвестором Эфиопии и основным источником частных прямых иностранных инвестиций (в 2019 году — 60% ПИИ поступили из Китая).

Цифровая составляющая является одной из ведущих в китайско-африканском диалоге. Поскольку речь, зачастую, идет о защите объектов критической инфраструктуры (в т.ч. входящих в орбиту китайского глобального проекта «Один пояс, один путь»), Пекин уделяет первоочередное внимание повышению уровня комплексной киберготовности государств и совместной реализации инициатив в области цифровой безопасности [57].

Из значимых примеров содействия цифровизации Эфиопии можно привести описанные ранее: ИКТ-инфраструктура мобильных сетей связи по всей стране, ИКТ-центры с высокопроизводительными ЦОД, программа «Высокотехнологичные открытые школы для всех» (TeOSS), Национальный центр и Национальная инфраструктура для искусственного интеллекта [58]. Министерство инноваций и технологий Эфиопии подписало соглашение с Alibaba Group о создании в Аддис-Абебе Центра электронной всемирной торговой платформы (eWTP), что будет способствовать предоставлению интеллектуальных услуг в области логистики и реализации помощи эфиопским малым и микропредприятиям в достижении глобальных рынков [59].

В отличие от западных стран КНР осуществляет программы подготовки высококвалифицированных кадров в сфере ИТ и компьютерной безопасности, включая возможность обучения и стажировки в китайских центрах подготовки. Реальная передача передовых технологий без выдвижения политических условий способствует сближению двух стран, в том числе в сфере обеспечения информационной безопасности.

Эфиопия заявила о твердой поддержке китайской Глобальной инициативы по обеспечению безопасности данных [60], которая по мнению правительства соответствует целям национальной стратегии цифровой трансформации и будет способствовать развитию цифровой экономики.

6.2. Республика Корея

Между Эфиопией и Кореей имеются многолетние экономические связи, которые с 1991 года осуществляются при посредничестве Корейского агентства международного сотрудничества (KOICA). Инвестиции Сеула, особенно прямые, в производственный сектор и инфраструктурные проекты активно росли

73 Однако основным экспортером Эфиопии (преимущественно сельскохозяйственной продукции) являются США (10,8%), Саудовская Аравия (8,68%), Сомали (8,58%), Германия (8,36%). Китай занимает лишь 9 позицию (4,21% или 129 млн долл. США).

с 2005 года. Объем вложений в ИКТ-сектор был заметно меньше, но тем не менее Кореей внесен вклад в развертывание инфраструктуры связи, передачу технологий, поддержку стартапов [61]. В 2020 году подписано шестилетнее соглашение по развитию в Эфиопии бизнеса на основе ИКТ и поддержке малых и средних предприятий для создания качественных рабочих мест, объем инвестиций составит 10 млн долл. США, также подписано соглашение по развитию потенциала лидеров и тренеров для среднего профессионального образования на 8 млн долл. США [62].

На основании меморандума о сотрудничестве с правительством Эфиопии от 2013 года Samsung Electronics предоставила свои решения для услуг электронного правительства (в сферах образования, создания рабочих мест, общественной безопасности и цифрового здравоохранения). Корпорация создала Samsung Engineering Academy для подготовки местных технических специалистов для своих магазинов и сервисных центров[74].

Научно-техническое сотрудничество двух стран началось с соглашения 2011 года. С тех пор Корея предоставляет стипендии для эфиопских студентов и оказывает помощь в развитии научной инфраструктуры и технологий. Например, в 2019 году Корея выделила 5 млн долл. США на создание в Эфиопии центра по разработке искусственного интеллекта [63].

6.3. Индия

Текущая деятельность Нью-Дели в регионе выстраивается с опорой на «Кампальские принципы» (2018), согласно которым Индия стремится 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. Как и Китай, Индия провозглашает деполитизированный принцип отказа от «блага взамен». Она активно продвигает свои цифровые достижения, прежде всего для электронного правительства и разработок в сфере информационной безопасности [64]. В 2023 году в Аддис-Абебе с участием 50 национальных компаний прошла девятая выставка и конференция «Индия-Африка в сфере ИКТ», направленная на продвижение стратегии «Цифровая Эфиопия 2025» среди заинтересованных сторон [65].

74 Корея делает акцент содействие «зеленому» и безопасному цифровому будущему, основанному на данных, и предлагает на эфиопском рынке высокотехнологичную продукцию Samsung и LG, которые имеют офисы в Аддис-Абебе.

6.4. США

США всегда являлись одним из важнейших политических контрагентов Эфиопии. Ещё в начале 1950-х годов Вашингтон стал главным союзником и основным источником финансовой помощи Эфиопии. В обмен на военную помощь, США получили право на создание крупной военно-воздушной базы вблизи г. Асмэры (в Эритрее, на тот момент провинции Эфиопии). В период 1984–86 гг. Они оказали стране значительную финансовую помощь для борьбы с голодом (более 430 млн долл. США), что способствовало восстановлению полных дипломатических отношений в 1989 году [66].

Современные двусторонние отношения строятся на признании Эфиопией экономической мощи и роли, которую играют США на мировой сцене. Обновленная «Стратегия США в отношении стран Африки к югу от Сахары. Август 2022» декларирует продвижение совместно с партнерами демократических ценностей и общих для США и Африки приоритетов. В настоящий момент Эфиопию трудно отнести к приоритетным американским партнерам[75]. Несмотря на торговое соглашение США с Общим рынком Восточной и Южной Африки, в 2020 году Эфиопия исключена из списка стран, которые могут воспользоваться правом беспошлинной торговли отдельными видами товаров в соответствии с законом США о росте и возможностях Африки (AGOA).

Недавно обозначенное стремление увеличить американское присутствие в стране можно объяснить двумя целями Вашингтона: ограничить влияние КНР и России и создать собственный плацдарм на быстро растущем эфиопском рынке. Возможно поэтому на саммите лидеров США-Африка премьер-министр Абий Ахмед удостоился двусторонних переговоров с Э. Блинкиным.

Объем взаимной торговли в 2022 году по сравнению с предшествующим годом заметно вырос: Эфиопия закупила в США на 88,5% больше продукции (на 1,1 млрд долл. США, львиную долю составили гражданские самолеты и зерно), и экспортировала на 19,4% больше своих товаров, в основном кофе (на 718 млн долл. США).

Не изменяя своей тактике, Вашингтон активно действует не на государственном уровне, а через бизнес-структуры. Прямые иностранные инвестиции в Эфиопию в 2022 году выросли на 7,4% и составили 29 млн долл. США [67]. Повышенный интерес вызывает цифровая трансформация страны и либерализация ИКТ-рынка, например, корпорация Microsoft в рамках своей инициативы «Партнеры в обучении» подписала соглашение с Министерством образования Эфио-

75 По данным Associated Press, в 2016 году эфиопские власти уведомили посольство США в Эфиопии, что более нет необходимости в эксплуатации американской военной базы в г. Арба-Мынч, с которой осуществлялось управление беспилотными летательными аппаратами (БПЛА).

пии, направленное на преобразование методов обучения с использованием ИКТ. Американский миллиардер Т. Дрейпер заключил партнерство с базирующейся в Эфиопии компанией по разработке программного обеспечения Apposit для создания и обслуживания в Африке платформы финансовых услуг PAGA. При поддержке предпринимателя из США Б. Гертцеля создана научно-исследовательская лаборатория Icog-Labs, которая является флагманом Эфиопии в сфере искусственного интеллекта [68]. Явно присутствует заинтересованность в использовании потенциала эфиопских стартапов: в 2021 году проведены переговоры сотрудников Специального комитета Сената США по разведке и Министерства инноваций и технологий Эфиопии о возможностях сотрудничества в этой сфере [69].

Масштабный проект с государственным участием можно отметить только один, но крайне рискованный[76], поскольку локализация данных законодательно не закреплена. В 2019 году, еще до начала пандемии COVID, Агентство США по международному развитию (USAID) заключило пятилетний договор с Министерством здравоохранения Эфиопии стоимостью 63 млн долл. на модернизацию информационной системы здравоохранения, которая включает:

- консолидацию медицинской информации пациентов путем перехода от бумажных записей к системе электронных медицинских записей;
- обучение политиков на всех уровнях системы здравоохранения, поставщиков медицинских услуг, врачей, медсестер, специалистов по распространению медицинских знаний и политиков, более эффективному использованию технологий использованию технологий для укрепления системы здравоохранения страны и повышения качества услуг, особенно в сельских районах;
- партнерство с местными университетами для разработки курсов по развитию компетенций в области инноваций в области здравоохранения и электронных решений, а также подготовки лидеров завтрашнего дня и создания карьерных путей, которые позволят молодым эфиопам внедрять цифровые решения во всем секторе;
- создание цифровой системы эпидемиологического надзора за COVID-19, которая позволяет лучше отслеживать контакты и ускорять результаты анализов;
- поддержку развития Центра инноваций и обучения в области цифрового здравоохранения в Аддис-Абебе для поощрения дальнейшей модернизации существующих информационных систем здравоохранения страны (профинансировано Фондом Билла и Мелинды Гейтс) [70].

76 Следует принять во внимание практически одновременное развертывание в Джибути (Кэмп Лемонье) лаборатории Третьего военно-морского медицинского исследовательского центра США (NAMRU-3) для участия в программах общественного здравоохранения и изучения новых инфекционных заболеваний.

6.5. Российская Федерация

25 февраля 2023 года посольство Российской Федерации в Эфиопии торжественно отметило 125-летие установления дипломатических отношений между двумя странами, которые базируются на дружбе, взаимном уважении и доверии и ныне имеют многофункциональный, взаимовыгодный характер. Позиции обеих стран по вопросам международного сотрудничества часто совпадают — от необходимости развития равного партнерства и соблюдения прав человека до идей многополярности современного мироустройства. Об этом свидетельствуют постоянные контакты и деловые визиты представителей обеих стран, особенно это касается внешнеполитических ведомств [71].

Важный импульс для укрепления сотрудничества между Российской Федерацией и Эфиопией дал первый саммит Россия-Африка в октябре 2019 года. На саммите состоялись переговоры премьер-министра Эфиопии Абия Ахмеда с В.В. Путиным, подписаны десятки важных соглашений и продемонстрирован твердый настрой на поступательное развитие всестороннего взаимодействия в обеспечении международной информационной безопасности как одного из ключевых элементов системы глобальной безопасности.

В развитие этого взаимопонимания в октябре 2021 года было подписано «Соглашение между Правительством Российской Федерации и Правительством Федеративной Демократической Республики Эфиопия о взаимной охране результатов интеллектуальной деятельности и защите интеллектуальной собственности в ходе двустороннего военно-технического сотрудничества» [72]. Одобрение Соглашения парламентом Эфиопии было получено только в декабре 2023 года «с целью повышения потенциала Национальных сил обороны Эфиопии в области знаний, навыков и технологий» [73].

В Москве в апреле 2023 года был проведен международный ИТ-форум Россия-Африка «Цифровые технологии как драйвер государственного развития и международного сотрудничества», организованный Минцифры России и ФКУ «ГосТех». Мероприятие состоялось в преддверии Второго саммита «Экономический гуманитарный форум Россия-Африка. За мир, безопасность и развитие» (Санкт-Петербург, май 2023 года). При обсуждении вопросов цифровизации особое внимание участники ИТ-форума уделили реализации совместных проектов, проектированию информационных систем на единой цифровой платформе «ГосТех» и обеспечению информационной безопасности.

На полях саммита глава МИД России С.В. Лавров и государственный министр иностранных дел Эфиопии Месгану Арега подписали «Соглашение между Правительством Российской Федерации и Правительством Федеративной Демократической Республики Эфиопии о сотрудничестве в области обеспечения

международной информационной безопасности» [74]. Они подчеркнули, что документ — свидетельство высокого уровня доверия между странами и отражает совместный подход к противодействию вызовам и угрозам в сфере ИКТ. Кроме того, соглашение закладывает правовой фундамент для реализации совместных инициатив и предусматривает, в том числе, регулярные двусторонние консультации по информационной безопасности [75].

7. Основные приоритеты национальной политики Эфиопии в рамках БРИКС

Руководство государства и международные эксперты в один голос говорят, что вступление Эфиопии в БРИКС будет содействовать расширению экономических возможностей и торговых партнерств как внутри объединения, так и через его участников, а также доступу к альтернативным источникам финансирования, в частности к Новому банку развития. Более активное глобальное взаимодействие будет укреплять имидж Эфиопии как привлекательного направления для инвестиций.

Для успешной цифровой трансформации страна должна активно развивать инфраструктуру, и не только для ИКТ-отрасли, укреплять технологическое сотрудничество с остальными участниками БРИКС, в том числе, получать от них столь необходимые современные ИКТ. Чрезвычайный и Полномочный Посол Федеративной Демократической Республики Эфиопия в Российской Федерации Чам Угала Урят, среди основных преимуществ присоединения к БРИКС отметил взаимодействие в таких областях, как энергетика, информационные технологии и кибербезопасность, сотрудничество в промышленности, развитие инфраструктуры [76].

Чтобы извлечь дивиденды от своего демографического потенциала Эфиопии необходимы комплексные программы подготовки высоко квалифицированных специалистов и ученых, развития производства и создания новых рабочих мест. Для этого в БРИКС уже отлажены различные механизмы сотрудничества, которыми можно воспользоваться.

Для Аддис-Абебы важно и геополитическое измерение БРИКС, которое предоставляет своим участникам платформу для оказания большего влияния и потенциального изменения существующего мирового порядка. Эфиопия, как инициатор Движения неприсоединения, последовательно движется к цели увеличения роли развивающихся государств в деятельности международных институтов, в которых доминируют западные страны (например, Всемирный банк, МВФ), более значимого участия в глобальных процессах принятия решений, содействия строительству многополярной модели мира.

8. Использованная литература

1 Религия в Эфиопии: вера и боги, https://fb.ru/article/457798/religiya-v-efiopii-vera-i-bogi
2 Эфиопия // Большая российская энциклопедия — электронная версия, https://old.bigenc.ru/geography/text/4917478?ysclid=lr7z5xzo21533274279
3 Р.Н. Исмагилова Россия – Эфиопия: 125 лет дипломатических отношений // Институт Африки РАН, https://www.imemo.ru/files/File/ru/articles/2023/31032023-Africa.pdf
4 В ООН заявили о риске гуманитарного кризиса для 4 млн жителей Эфиопии из-за засухи, ТАСС, 10 января 2024 года, https://tass.ru/obschestvo/19702121?ysclid=lr8xlozstd152555806
5 Африка 2023: возможности и риски // Экспертно-аналитический справочник. Под общей редакцией А.А. Маслова, Издательский дом Высшей школы экономики, 2023, С.65, https://russiancouncil.ru/library/library_rsmd/afrika-2023-vozmozhnosti-i-riski/
6 Agenda 2063: The Africa We Want // African Union, 2015, https://au.int/en/agenda2063/overview
7 2017 Global ICT Readiness Index, https://www.itu.int/net4/ITU-D/idi/2017/index.html
8 Proclamation for the Communications Service № 1148/2019, 12 August 2019, https://www.lawethiopia.com/images/federal_proclamation/proclamations_by_number/2022-06-23T12-21-40.305ZCommunications-service-proclamation-1148-2019.pdf
9 Ethiopia – Information and Communication Technology (ICT), Ethiopia – Country Commercial Guide, https://www.trade.gov/country-commercial-guides/ethiopia-information-and-communication-technology-ict
10 Countries with the Highest Number of Internet Users (2024), November 22, 2023, https://explodingtopics.com/blog/countries-internet-users
11 Digital 2023: Ethiopia, 13 February 2023, https://datareportal.com/reports/digital-2023-ethiopia
12 Digital in Ethiopia — DataReportal – Global Digital Insights, https://datareportal.com/digital-in-ethiopia
13 Techno Mobile и Security Innovation Network. ICT Park Marks Sectional Data Center Completion, February 11, 2023, https://addisfortune.news/ict-park-marks-sectional-data-center-completion/
14 Tele Enables Authentication Agency Receive Service Fees via Telebirr // Ethiopian Monitor, September 1, 2022, https://ethiopianmonitor.com/2022/09/01/tele-enables-authentication-agency-receive-service-fees-via-telebirr/
15 Accelerating Innovations: Digital Ethiopia 2025 // Cambridge University Business School, January 2023, https://www.jbs.cam.ac.uk/wp-content/uploads/2023/01/cigb-report-accelerating-innovations-digital-ethiopia-2025.pdf
16 Исследование ООН: Электронное правительство 2022 // Департамент по экономическим и социальным вопросам ООН, https://desapublications.un.org/sites/default/files/publications/2023-01/UN%20E-Government%20Survey%202022%20-%20Russian%20Web%20Version.pdf
17 А. Маслова Эфиопия: цифровое государство // Центр изучения Африки - Национальный исследовательский университет «Высшая школа экономики», https://we.hse.ru/irs/cas/passet
18 ITU Global Cybersecurity Index 2020, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
19 NCSI :: Ranking, https://ncsi.ega.ee/ncsi-index/
20 National ICT Policy for Higher Education and TVET in 2020 (MoSHE, 2020), Источник: Developing Ethiopia's Digital Economy: Lessons from China, https://unctad.org/system/files/official-document/BRI-Project_RP21_en.pdf
21 Digital Ethiopia 2025 – A Strategy For Ethiopia Inclusive Prosperity, https://mint.gov.et/wp-content/uploads/2020/12/Digital-Ethiopia-2025-Strategy-English.pdf
22 Report No: PAD3617 International Development Association Project Appraisal Document on a Proposed Credit in the Amount of SDR138.9 million (US$200 million equivalent) to the Federal Democratic Republic of Ethiopia for an Ethiopia Digital Foundations Project, March 24, 2021, https://documents1.worldbank.org/curated/en/421681619316030132/pdf/Ethiopia-Ethiopia-Digital-Foundations-Project.pdf
23 Ethiopia: Parliament Ratifies Digital Identity Proclamation, 30 March 2023, https://www.2merkato.com/news/it-and-communication/7168-ethiopia-parliament-ratifies-digital-identity-proclamation
24 MOSIP partnership with Ethiopia on foundational digital ID expands, along with ecosystem, February 25, 2022, https://www.biometricupdate.com/202202/mosip-partnership-with-ethiopia-on-foundational-digital-id-expands-along-with-ecosystem
25 The Federal Democratic Republic of Ethiopia National Cyber Security Policy and Strategy, https://www.insa.gov.et/documents/20124/0/National+Cyber+security+Policy%26+StrategyFDRE.docx/03b2d42e-5cb3-f29e-f8f8-fe4ad3d94586?t=1639143692057&download=true

26 Open Data in Ethiopia Report on the Open Data Landscape in Ethiopia, Ministry of Communication & Information Technology (MCIT), September 2017, https://pub.sbc4d.com/2017/Ethiopia%20Open%20Data%20SBC4D.pdf
27 Ethiopia Extractive Industries Transparency Initiative (EEITI) Open Data Policy, December, https://eiti.org/sites/default/files/attachments/ethiopia_open_data_policy_december_2016.pdf
28 Consultation on the Recommendations and Working Text of the National Open Data Policy of The Government of Ethiopia // Ministry of Communication and Information Technology (MCIT), January 2018, https://mint.gov.et/wp-content/uploads/2020/10/Draft-Open-Data-Policy-and-Guideline.pdf
29 S. Mekonnen Ethiopia adopts a national open access policy, 9 October 2019, https://blog.okfn.org/2019/10/09/ethiopia-adopts-a-national-open-access-policy/
30 Ethiopian Constitution, https://www.africa.upenn.edu/Hornet/Ethiopian_Constitution.html
31 Six Key Points on the Electronic Signature Law in Ethiopia // Dagnachew & Mahlet Law Firm Limited Liability Partnership(LLP), June 18, 2020, https://dmethiolawyers.com/electronic-signature-in-ethiopia/
32 Proclamation to Provide for Electronic Transactions № 1205/2020, http://laws.eag.gov.et/Upload/Cassation-DecisionsDocument/a17f9c61-fe61-496f-9e94-e0ae5c5df05c.pdf
33 Regulation of Electronic Contract under New Ethiopian Electronic Transaction Proclamation № 1205/2020, http://etd.aau.edu.et/handle/123456789/29504?show=full
34 Digital ID Proclamation № 1284/2023, 2 July 2023, https://www.lawethiopia.com/index.php/volume-3/6967-digital-id-proclamation-no-1284-2023
35 Legal Review of Ethiopia's Personal Data Protection Proclamation // Birr Metrics, https://birrmetrics.com/legal-review-of-ethiopias-personal-data-protection-proclamation/
36 Proclamation to Provide for Start-Up Businesses, v(02.06.2020), https://www.lawethiopia.com/images/draft%20laws/Laws_ETH_Start-ups-English-2020-06-02.pdf
37 Telecom Fraud Offence Proclamation № 761/2012, https://sherloc.unodc.org/cld/uploads/res/document/eth/2005/telecom-fraud-offence-proclamation_html/Telecom_Fraud_Offence_Proclamation_2012_Official_English-Amharic.pdf
38 Эфиопия объявила Skype вне закона, 15 июня 2012 года, https://lenta.ru/news/2012/06/15/novoip/
39 Implications of the Ethiopian Computer Crime Proclamation on the Enjoyment of Human Rights// Adigart University School of Law, April 17, 2020, http://ijrar.com/upload_issue/ijrar_issue_20544193.pdf
40 В. Гончаров Кризис в Эфиопии: плоды «этнического федерализма»// Журнал «Международная жизнь», 20 сентября 2021 года, https://interaffairs.ru/news/show/31764?ysclid=lrol9c0rvb51984460
41 Ethiopian gov't Tightens Control Over Information Technology Device Entry over "National Security" concerns, 15 October 2023, https://borkena.com/2023/10/15/ethiopian-govt-tightens-control-over-information-technology-device-entry-for-national-security/
42 Proclamation No.1097-2018 Proclamation to Provide for the Definition of the Powers and Duties of the Executive Orangs of the Federal Democratic Republic of Ethiopia, https://www.dataguidance.com/sites/default/files/proclamation-no.1097-2018-definition-of-the-powers-and-duties-of-the-executive-orangs_1.pdf
43 INSA Discloses More than 2000 Cyber-Attacks Attempted in Six Months, https://www.insa.gov.et/web/en/w/news-2
44 The Information Network Security Agency Re-establishment Proclamation № 808/2013 // Federal Negarit Gazeta, 20th Year, No. 6, Addis Ababa, 2 January 2014, https://www.insa.gov.et/documents/20124/0/Information+Network+Security+Agency+re-establishment+Proclamation+No.808-2013.pdf/07db41af-d179-a796-adf0-1e6ceb61952e?t=1653485716858&download=true
45 Ethiopia intelligence intercepts US$110M cyber fraud // FurtherAfrica, May 12, 2020, https://furtherafrica.com/2020/05/12/ethiopia-intelligence-intercepts-us110m-cyber-fraud/
46 Proclamation №___/2022 a Proclamation to Provide for the Amendment of the National Intelligence and Security Service Re-Establishment Proclamation, https://1filedownload.com/national-intelligence-and-security-service-reestablishment-proclamation-seerota-keenya-resources/
47 Proclamation №1097-2018 Proclamation to Provide for the Definition of the Powers and Duties of the Executive Orangs of the Federal Democratic Republic of Ethiopia, https://www.dataguidance.com/sites/default/files/proclamation-no.1097-2018-definition-of-the-powers-and-duties-of-the-executive-orangs_1.pdf
48 Ethiopic Standards Development and Dissemination Program Development, http://yacob.org/papers/DanielYacob-IUC25.pdf
49 The Federal Democratic Republic of Ethiopia, https://unctad.org/system/files/non-official-document/CSTD_2013_WSIS_Ethiopia.pdf
50 Document authentication as a means of transaction control in Ethiopia, 2020, https://furtherafrica.com/2020/10/01/document-authentication-as-a-means-of-transaction-control-in-ethiopia/

51 Huawei и ЮНЕСКО реализуют проект по созданию систем цифрового образования в Африке, 6 декабря 2021, https://tass.ru/press-relizy/13119065
52 Launch of ITU Digital Transformation Centers Initiative in Ethiopia & Stakeholder Workshop Addis Ababa, 9-10 May 2022, https://www.itu.int/en/ITU-D/Regional-Presence/Africa/Documents/2022/DTC/Presentations/Launch_of_ITU_Digital_Transformation_Centres_Initiative_in_Ethiopia_9_May_2022.pdf
53 Afripol Cybercrime Strategy, https://rm.coe.int/afripol-strategy-on-cybercrime-v01-en/1680a30050
54 Interpol and Afripol dismantle cyber networks in Africa, https://furtherafrica.com/2023/10/06/interpol-and-afripol-dismantle-cyber-networks-in-africa/
55 Участие в международных организациях и режимах, основные внешнеполитические контрагенты и партнёры, отношения с Россией // Политический атлас современности, http://www.hyno.ru/tom4/2043.html
56 Ethiopia's digital economy is blooming, but needs investment, 21 November 2022, https://ecdpm.org/work/ethiopias-digital-economy-blooming-needs-investment
57 Л.В. Цуканов Технологический ренессанс в Африке южнее Сахары: вызовы и возможности для России // Доклады ПИР-Центра, № 37. М.: ПИР-Центр, 2023, 23-12-28-Аналитическая-записка-ПИР-Центра-по-научно-технологическому-потенциалу-стран-Африки-южнее-Сахары.pdf
58 Ethiopia, China Signs MoU on Establishing Nat'l Artificial Intelligence Infrastructure, November 29, 2019, https://www.ena.et/web/eng/w/en_11025
59 The Government of Ethiopia and Alibaba Group Sign Agreements to Establish eWTP Ethiopia Hub // Business Wire, 25 November 2019, https://www.businesswire.com/news/home/20191125005273/en/The-Government-of-Ethiopia-and-Alibaba-Group-Sign-Agreements-to-Establish-eWTP-Ethiopia-Hub
60 Ethiopia Is Committed and Strongly Supporting The Global Data Security Initiative Proposed By Chinese Government, https://mint.gov.et/ethiopia-is-committed-and-strongly-supporting-the-global-data-security-initiative-proposed-by-chinese-government/?lang=en
61 Messay Mulugeta, The Economic Development Component of the Ethiopia-South Korea Relationship, September 2019, https://www.researchgate.net/publication/335961856_The_Economic_Development_Component_of_the_Ethiopia-South_Korea_Relationship
62 Korea Finances Ethiopia's ICT based Business Creation Effort // Ethiopian Monitor, February 27, 2020, https://ethiopianmonitor.com/2020/02/27/korea-finances-ethiopias-ict-based-business-creation-effort/
63 Отношения Южной Кореи и стран Африки. Часть 1, 2023, https://dzen.ru/a/ZUI758KnrX6ydW_Z
64 Л.В. Цуканов Технологический ренессанс в Африке южнее Сахары: вызовы и возможности для России // Доклады ПИР-Центра, № 37. М.: ПИР-Центр, 2023, 23-12-28-Аналитическая-записка-ПИР-Центра-по-научно-технологическому-потенциалу-стран-Африки-южнее-Сахары.pdf
65 India Africa ICT Expo at Addis Ababa (9 August 2023), https://eoiaddisababa.gov.in/india-africa-ict-expo-at-addis-ababa-9-august-2023/
66 Участие в международных организациях и режимах, основные внешнеполитические контрагенты и партнёры, отношения с Россией // Политический атлас современности, http://www.hyno.ru/tom4/2043.html
67 Ethiopia // United States Trade Representative, https://ustr.gov/countries-regions/africa/east-africa/ethiopia
68 How the US Benefits from Foreign Aid to Ethiopia // The Borgen Project, February 20, 2018, https://borgenproject.org/u-s-benefits-from-foreign-aid-to-ethiopia/
69 US Senate Select Committee: the US is interested to invest in Ethiopia's Science Technology and Innovation sector, https://mint.gov.et/us-senate-select-committee-the-us-is-interested-to-invest-in-ethiopias-science-technology-and-innovation-sector/?lang=en
70 Ethiopia, USAID Launch $63m Five-Year Project to Expand Health Information Systems, November 14, 2019, https://ethiopianembassy.org/ethiopia-usaid-launch-63m-five-year-project-to-expand-health-information-systems-november-14-2019/, The Expansion of Digital Health Care in Ethiopia, https://borgenproject.org/digital-health-care-in-ethiopia/
71 Р.Н. Исмагилова Россия – Эфиопия: 125 лет дипломатических отношений // Институт Африки РАН, https://www.imemo.ru/files/File/ru/articles/2023/31032023-Africa.pdf
72 Двусторонние договоры - Министерство иностранных дел Российской Федерации, https://www.mid.ru/ru/foreign_policy/international_contracts/international_contracts/2_contract/60376/
73 Россия и Эфиопия укрепляют военное сотрудничество // ИА «Африканская инициатива», 16 декабря 2023, https://afrinz.ru/2023/12/rossiya-i-efiopiya-ukreplyayut-voennoe-sotrudnichestvo/
74 Распоряжение Правительства Российской Федерации от 08.04.2022 № 798-р «О подписании Соглашения между Правительством Российской Федерации и Правительством Федеративной Демократической Республики Эфиопии о сотрудничестве в области обеспечения международной информационной безопасности», http://publication.pravo.gov.ru/document/0001202204110034?ysclid=ls3hfoci1s408244613&index=1

75 РФ и Эфиопия подписали соглашение в области информационной безопасности, 29 июля 2023, https://news22.ru/2023/07/29/rf-i-efiopiya-podpisali-soglashenie-v-oblasti-informacionnoy-bezopasnosti.html

76 Посол Эфиопии в Российской Федерации: Присоединение к БРИКС – в интересах нашего государства // Международная сеть TV BRICS, 23.11.2023, https://tvbrics.com/tv-brics-projects/ https://tvbrics.com/news/posol-efiopii-v-rf-prisoedinenie-k-brics-v-interesakh-nashego-gosudarstva/?ysclid=lr3jye61u29820702

Федеративная Республика Бразилия

Официальное название: Федеративная Республика Бразилия

Столица: Бразилиа

Официальный язык: португальский

Территория: 8 515 767 км² (5 в мире). Страна занимает северо-восточную и центральную часть материка Южная Америка. Граничит на севере с Французской Гвианой, Суринамом, Гайаной и Венесуэлой, на северо-западе с Колумбией, на западе — Перу и Боливией, на юго-западе — Парагваем и Аргентиной, на юге — Уругваем. С востока омывается Атлантическим океаном, протяженность береговой линии — 7,4 тыс. км.

Население: На 1 ноября 2023 года численность населения (постоянных жителей) Бразилии составила 207 353 391 человек, что является 7 показателем в мире [1].

Государственное устройство: федеративная республика, разделенная на 26 штатов и 1 федеральный столичный округ. Согласно Конституции 1988 года, в стране существует разделение властей на исполнительную, законодательную и судебную.

Глава государства — президент, избираемый на четыре года. В настоящее время президентом Бразилии является Луис Инасиу Лула да Силва Альберто, победивший на выборах, состоявшихся в октябре 2022 года, и вступивший в должность 1 января 2023 года. Президент одновременно является главой кабинета министров.

Высшим законодательным органом является Национальный конгресс, который состоит из двух палат – Федерального сената (81 мест) и Палаты депутатов (513 мест). Федеральный сенат состоит из представителей штатов и федерального округа, избранных населением по мажоритарной системе. Каждые 4 года представительство субъекта попеременно обновляется на одну и две трети. Палата депутатов Бразилии избирается на четыре года на основе всеобщего мажоритарного голосования. Места в палате распределяются пропорционально численности населения субъектов.

Экономика: По данным Всемирного банка за 2022 год показатели Валового внутреннего продукта (ВВП) (по паритету покупательной способности):

Итого: 3,837 трлн долл. США (8 место в мире).

На душу населения: 17 822 долл. США (82 место в мире).

Показатели ВВП (по номинальному значению, в текущих ценах) на 2022 год:

Итого: 1,92 трлн долл. США (11 место в мире).

8 918 долл. США (78 место в мире) [2].

Бразилия, согласно классификации ООН, в 2023 году относилась к группе государств с достатком ниже среднего.

Дипломатические отношения с Россией (СССР): дипломатические отношения России и Бразилии были установлены 195 лет назад, 3 октября 1828 года.

1. Уровень развития информатизации страны и ИКТ-инфраструктуры, системы обеспечения информационной безопасности

Бразилия — наиболее развитое государство Южной Америки в сфере использования и внедрения современных ИКТ. По данным МСЭ на 2017 год, на 100 человек населения в Бразилии приходилось 118,9 абонентов сотовой связи. По состоянию на 2017 год сеть Интернет использовали 98% компаний [3] и 100% федеральных агентств и агентств штатов. В 2022 году уровень проникновения Интернета достиг 82,8%, что значительно выше среднемирового (67,9%), но ниже, чем в Чили (97,2%), Уругвае (93,2%) или Аргентине (91,1%). С учетом доли Бразилии в населении Латинской Америки, именно эта страна снижает средний по региону уровень проникновения сети Интернет до 84,4%. Китайская компания Huawei является главным поставщиком в страну программно-аппаратных средств для формирования, обработки и хранения информации. Одновременно Бразилия является крупным производителем средств телекоммуникационного оборудования и средств вычислительной техники с участием таких компаний как Dell, Cisco, IBM, LG, Sony, Hewlett-Packard. Девятнадцать подводных оптоволоконных кабелей обеспечивают подключение Бразилии к глобальной системе связи. На 2020 год в Бразилии имелось 195 центров обработки данных, управляемых 142 организациями [4], но стоимость облачных сервисов в сравнении с другими странами ОЭСР высока, что приводит к миграции национальных данных за рубеж [5].

Бразилия заняла 18 место в Глобальном индексе кибербезопасности МСЭ 2020 года [6]. На фоне развития ИКТ-сектора и цифровой экономики важно отметить, что в национальном сегменте сети находится множество фишинговых сайтов, а по некоторым данным — страна входит в десятку крупнейших источников кибератак в мире. Согласно отчету Европола за 2018 год «Оценка угроз организованной преступности в Интернете — IOCTA» [7], 54% кибератак, зарегистрированных в Бразилии, инициированы источниками внутри страны. С 2020 года произошло несколько крупнейших кибератак в истории Бразилии: на приложение Covid-pass ConectaSUS, Верховный суд и предприятия ядерной отрасли [8, 9]. Также имели место массовые утечки данных, которые затронули более 220 млн пользователей [10]. В настоящее время, в соответствии с Национальной стратегией кибербезопасности, противодействию угрозам использования ИКТ в преступных целях уделяется первостепенное внимание.

2. Основные документы стратегического планирования в сфере развития ИКТ, обеспечения национальной и международной информационной безопасности

Исходя из положений национальных документов стратегического планирования, можно сделать вывод, что в качестве основных угроз кибербезопасности рассматриваются:

- разведывательная деятельность иностранных спецслужб;
- кибератаки (в основном — со стороны криминальных структур);
- мониторинг информационных коммуникаций разведывательными службами иностранных государств;
- неправомерное раскрытие поставщиками интернет-услуг информации о пользователях (в том числе данные о подключениях).

При этом основные усилия правительства Бразилии сосредоточены на:

- отказе от иностранного программного обеспечения (ПО) и переходе на отечественную продукцию;
- совершенствовании законодательной базы в сфере обеспечения кибербезопасности;
- принятии необходимых мер по защите критической информационной инфраструктуры (КИИ) и контроле за ее состоянием со стороны правоохранительных органов;
- внедрении мер, исключающих возможность анонимного доступа к Интернет;
- подготовке квалифицированных кадров в области информационной безопасности;
- развитии сотрудничества в сфере обеспечения кибербезопасности с иностранными государствами, прежде всего с США, Израилем и Китаем.

Приоритетными задачами определены: защита объектов КИИ и обеспечение безопасности информационного обмена между государственными учреждениями.

Среди документов, повлиявших на формирование существующей политики национальной информационной безопасности Бразилии, можно выделить следующие.

2.1. **Стратегия национальной обороны** (2008)

Стратегия [11] стала первым официальным документом, где киберпространство было признано одной из стратегических областей национальной безопасности и обороны.

2.2. **Зеленая книга по кибербезопасности** (2010)

Этот документ посвящен взаимосвязи между информационной и кибербезопасностью в федеральных органах государственного управления (ФОГУ). В дальнейшем государственная политика в рассматриваемой сфере была расширена на другие критически важные для страны сегменты информационного пространства. Раскрытие Э. Сноуденом в 2013 году информации о масштабах разведывательной деятельности, осуществляемой США в глобальном информационном пространстве, послужило стимулом к созданию Парламентского комитета по расследованию шпионажа (CPI da Espionagem). Основным результатом его работы стала разработка и принятие **«Стратегии информационной и коммуникационной безопасности и кибербезопасности для органов государственного управления на 2015–2018 годы»**.

2.3. **Национальная политика информационной безопасности** (2018)

Этот документ стратегического планирования, принятый в декабре 2018 года [12], определил принципы, цели, инструменты, обязанности и компетенции в области обеспечения информационной безопасности для административных органов и федеральных субъектов. Политика предусматривала развитие в пяти областях: кибербезопасность, киберзащита, безопасность критической инфраструктуры, защита конфиденциальной информации и утечки данных.

Среди заложенных принципов важно выделить следующие:

- национальный суверенитет;
- уважение и продвижение прав человека;
- комплексный и системный взгляд на информационную безопасность;
- образование, как фундаментальная основа развития культуры информационной безопасности;
- интеграция и сотрудничество между органами государственной власти, бизнес-сектором, обществом и научными учреждениями;
- международное сотрудничество в области информационной безопасности.

Важнейшими задачами, на решение которых направлена Стратегия, являются:

- обеспечение безопасности личности, общества и государства;
- содействие научным исследованиям, технологическому развитию и инновационной деятельности, связанной с информационной безопасностью;
- постоянное совершенствование нормативно-правовой базы, связанной с информационной безопасностью;
- содействие подготовке и повышению квалификации кадров, необходимых для обеспечения информационной безопасности;

- укрепление культуры информационной безопасности в обществе;
- обеспечение безопасности данных, хранящихся государственными организациями;
- обеспечение безопасности критической информационной инфраструктуры;
- защита информации физических лиц;
- сохранение культурной памяти Бразилии.

В рамках реализации Стратегии создан **Руководящий комитет по информационной безопасности** (Comitê Gestor da Segurança da Informação, CGSI), которому поручено в рамках своей компетенции консультировать Президента Республики и Кабинет институциональной безопасности при Президенте (Gabinete de Segurança Institucional da Presidência da República, GSI/PR).

2.4. **Стратегия цифровой трансформации Бразилии** (2018)

Действие Стратегии E-Digital распространялось на период 2018–21 годов. Она была направлена на координацию различных правительственных инициатив, чтобы способствовать процессу цифровизации производства, продвигать образование и создание рабочих мест в цифровой среде, а также обеспечивать экономический рост. E-Digital поощряет НИОКР и модернизацию производственной структуры в таких областях, как микроэлектроника, автоматизация и робототехника, суперкомпьютеры, искусственный интеллект, большие данные, шифрование, мобильные сети пятого поколения (5G) и облачные вычисления.

В части развития инфраструктуры и доступа к ИКТ Стратегия предусматривала осуществление долгосрочных инвестиций и координацию инициатив развития национальной критической информационной инфраструктуры, а также привлечение частного сектора к разработке протоколов связи, криптографических средств и оборудования.

В части обеспечения безопасности использования ИКТ Стратегия предписывала:

- разработать национальную политику кибербезопасности, включая определение федерального органа, ответственного за формирование национальной системы кибербезопасности и за отношения с частным сектором;
- укрепить правовую базу, связанную с обеспечением кибербезопасности;
- разработать планы по предотвращению, реагированию на инциденты и смягчению последствий киберугроз, в том числе для критически важной инфраструктуры;
- создать механизмы государственно-частного партнерства с целью внедрения передового опыта, обмена информацией, принятия соответствующих стандартов безопасности, координации реагирования на инциденты и защиты критически важной инфраструктуры;

- обеспечить обучение государственных служащих в сфере обеспечения информационной безопасности и снижения киберрисков;
- реализовать широкие просветительские кампании по повышению осведомленности населения по теме информационной безопасности;
- инвестировать в исследования и разработки в области киберзащиты и кибербезопасности с целью продвижения национального технологического суверенитета.

2.5. **Национальная стратегия кибербезопасности** (2020)

Стратегией E-Ciber определены основные действия в сфере кибербезопасности, которые должны быть осуществлены правительством на национальном и международном уровне в период с 2020 по 2023 год.

В E-Ciber отмечено, что защита киберпространства требует видения и лидерства для управления постоянными политическими, технологическими, образовательными, правовыми и международными изменениями. В этом смысле правительство, промышленность, научные круги и общество в целом должны поощрять технологические инновации и внедрение передовых технологий, а также постоянно уделять внимание национальной безопасности, экономике и свободе выражения мнений. Заявленные стратегические цели:

- обеспечить процветание и надежность в цифровой среде;
- повысить устойчивость страны к киберугрозам;
- укрепить на международной арене национальную позицию в области кибербезопасности.

Помимо защиты правительственных сетей и систем, еще одним важным моментом является киберзащита компаний, являющихся владельцами и/или операторами критически важной инфраструктуры. При этом особо отмечено, что глобальная взаимосвязанность некоторых критически важных инфраструктур означает, что низкая защищенность таких объектов одной страны может представлять опасность для других государств.

Согласно Стратегии, управление кибербезопасностью включает в себя разработку и применение общих принципов, стандартов, процедур и программ, в том числе национальную адаптацию стандарта информационной безопасности ISO/IEC 17799. В 2023 году правительство продлило срок действия документа до конца 2024 года.

2.6. Стратегия цифрового правительства на 2020–2023

Основной целью реализации этого документа являлось повышение эффективности ФОГУ через внедрение и использование ИКТ. Стратегией опре-

делено 18 целей, которые можно сгруппировать по трем направлениям — цифровые услуги для граждан; информационная безопасность, в том числе защита данных, и использование новых технологий в государственном управлении. Среди них:

- предоставление простых и интуитивно понятных цифровых государственных услуг, консолидированных на единой платформе и с доступной оценкой удовлетворенности;
- предоставление широкого доступа к информации и открытым правительственным данным;
- обеспечение интеграции и совместимости государственных баз данных;
- продвижение государственной политики, основанной на данных, а также прогнозных и персонализированных услугах с использованием новых технологий;
- имплементация Общего закона о защите персональных данных в ФОГУ и предоставление гарантий безопасности платформ цифрового правительства;
- обеспечение доступности цифровой идентификации для граждан;
- внедрение облачных технологических процессов и государственных услуг;
- оптимизация инфраструктуры информационных и коммуникационных технологий;
- формирование правительственных команд с цифровыми навыками.

2.7. **Стратегия Бразилии в области искусственного интеллекта** (2021)

Принятая в 2021 году [13], Стратегия призвана направлять действия в отношении стимулирования исследований, инноваций и разработки решений искусственного интеллекта (ИИ), а также их ответственного и этичного использования. Согласно Стратегии, технологии ИИ должны приносить пользу людям и планете, способствуя инклюзивному росту и устойчивому развитию. Системы ИИ должны быть спроектированы таким образом, чтобы уважать верховенство закона, права человека, демократические ценности и многообразие и должны включать соответствующие гарантии. Организации и отдельные лица, играющие активную роль в жизненном цикле ИИ, должны взять на себя обязательство обеспечивать прозрачность и ответственное раскрытие информации в отношении систем ИИ. Они должны работать надежно, безопасно и быть защищенными на протяжении всего жизненного цикла. Потенциальные риски должны оцениваться и управляться на постоянной основе.

3. Состояние нормативно-правовой базы в сфере развития ИКТ и передовых технологий, обеспечения национальной информационной безопасности

Согласно данным МСЭ за 2023 год в Бразилии сформирована развитая система правового регулирования цифровой экономики[1].

3.1. **Закон о киберпреступности** (2012)

Основным законом, регулирующим противодействие противоправному использованию ИКТ в Бразилии, является Закон о киберпреступности №12.737/2012 от 30 ноября 2012 года, известный как «Закон Каролины Дикманн». Он криминализирует такие действия, как компьютерное вторжение (взлом), кража паролей, нарушение данных пользователей и раскрытие личной информации (фотографии, сообщения и т.д.). Принятый одновременно с ним Закон №12.735/2012 регулирует создание и полномочия полицейских подразделений, расследующих киберпреступления.

3.2. **Закон о цифровых правах** (2014)

В 2014 году был принят Закон о цифровых правах №12.965/2014 (Marco Civil da Internet), который регулирует использование в Бразилии Интернета, устанавливая принципы, гарантии, права и обязанности для тех, кто пользуется «всемирной паутиной». Среди его основных принципов: гарантия свободы слова, общения и выражения мысли в соответствии с положениями Федеральной конституции; защита конфиденциальности; защита персональных данных, предусмотренная законодательством; сохранение и гарантия сетевой нейтральности; сохранение стабильности, безопасности и функциональности сети посредством технических мер, соответствующих международным стандартам и поощрение использования передовых практик; ответственность субъектов за свою деятельность в соответствии с законом; сохранение коллективного характера сети; свобода бизнес-моделей, продвигаемых в Интернете при условии, что они не противоречат другим принципам.

1 По методике G5 Benchmark, включающей оценку регулирования телекоммуникационного сектора, ИКТ-отрасли и цифровой политики, правовых и регуляторных рамок, Бразилия получила 75,31 балла, что обеспечило ей попадание в группу развитых государств (индекс от 60 до 80 баллов). Источник: Benchmark for Fifth Generation Digital Collaborative Regulation/ G5 Benchmark, ITU, https://app.gen5.digital/benchmark/concepts

3.3. **Общий закон о защите персональных данных** (2018)

Закон LGPD (Lei Geral de Proteção de Dados Pessoais) содержит положения, регулирующие обработку персональных данных с целью защиты основных прав на свободу и неприкосновенность частной жизни, а также свободного развития личности. Основные принципы, заложенные в защиту персональных данных: уважение к частной жизни; свобода выражения мнений, информации, общения; неприкосновенность частной жизни, чести и имиджа; экономическое и технологическое развитие и инновации; свободное предпринимательство, свободная конкуренция и защита прав потребителей; обеспечение прав человека и свободное развитие личности.

Закон применяется к любой операции по обработке информации, осуществляемой физическим или юридическим лицом, независимо от носителя, страны происхождения или страны, где расположены данные, при условии, что:

- взаимодействие с информацией осуществляется на территории страны;
- деятельность направлена на предложение/поставку товаров или услуг или обработку данных физических лиц, находящихся на территории Бразилии;
- персональные данные, подлежащие обработке, собраны на территории государства.

3.4. **Положение о кибербезопасности телекоммуникаций** (2020)

Этот подзаконный отраслевой акт принят Постановлением № 740 Агентства связи Бразилии. Его целью является установление регламента и процедур обеспечения безопасности телекоммуникационных сетей и услуг, а также кибербезопасности и защиты критически важных телекоммуникационных инфраструктур.

Его положения применяются ко всем поставщикам общедоступных телекоммуникационных услуг, за исключением малых компаний. Физические или юридические лица, которые прямо или косвенно участвуют в управлении или развитии телекоммуникационных сетей и услуг, в отношении кибербезопасности должны: применять национальные или международные нормы и стандарты, а также передовую практику в области кибербезопасности; распространять культуру кибербезопасности; стремиться обеспечить безопасное и устойчивое использование телекоммуникационных сетей и услуг; выявлять, защищать, реагировать на инциденты кибербезопасности и обеспечивать восстановление после них; стремиться к сотрудничеству с различными заинтересованными сторонами в целях снижения киберрисков; уважать и обеспечивать права человека, в частности, свободу выражения мнений, защиту персональных данных,

защиту конфиденциальности и доступ к информации; поощрять внедрение концепций безопасности и конфиденциальности еще на этапах разработки («by design») и приобретения продуктов и услуг в секторе телекоммуникаций.

4. Государственные органы, входящие в систему обеспечения информационной безопасности и форматы государственно-частного партнерства

К 2018 году основные компетенции реализации стратегии и политики кибербезопасности были распределены по следующим организациям.

Совет национальной обороны (Conselho de Defesa Nacional, CDN). Является совещательным органом при Президенте, через который осуществляется координация оборонной политики и стратегии. Совет разрабатывает, предлагает и контролирует выполнение инициатив, необходимых для обеспечения независимости и защиты государства. Практическая реализация конституционных полномочий Совета обеспечивается через Кабинет институциональной безопасности.

Кабинет институциональной безопасности при Президенте (Gabinete de Segurança Institucional da Presidência da República, GSI/PR). Оказывает непосредственное содействие президенту в вопросах обороны и безопасности; анализирует, отслеживает и предотвращает национальные кризисы; координирует разведывательную деятельность на федеральном уровне через Бразильское агентство разведки; обеспечивает личную безопасность президента и безопасность физической инфраструктуры. В работе этого органа исторически велика роль силовых ведомств. Он является ключевым органом, ответственным за планирование, координацию и контроль деятельности по обеспечению информационной безопасности в органах государственного управления. Кабинет позиционирует себя как национальный координационный центр по разработке киберполитики и во внешней политике взял на себя ведущую роль в представлении страны на некоторых встречах, а в других случаях он участвует в переговорах вместе с представителями МИДа.

Для оказания содействия GSI/PR в части проведения аналитической работы и обобщения экспертных оценок ведущих специалистов государственного, частного и научного сектора в 2018 году был создан межведомственный консультативный орган — **Руководящий комитет по информационной безопасности** (Comitê Gestor da Segurança da Informação, CGSI). В него входят представители министерств и различных федеральных органов государственного управления. Его задачей является консультирование Кабинета институциональной безопасности в вопросах, связанных с информационной безопас-

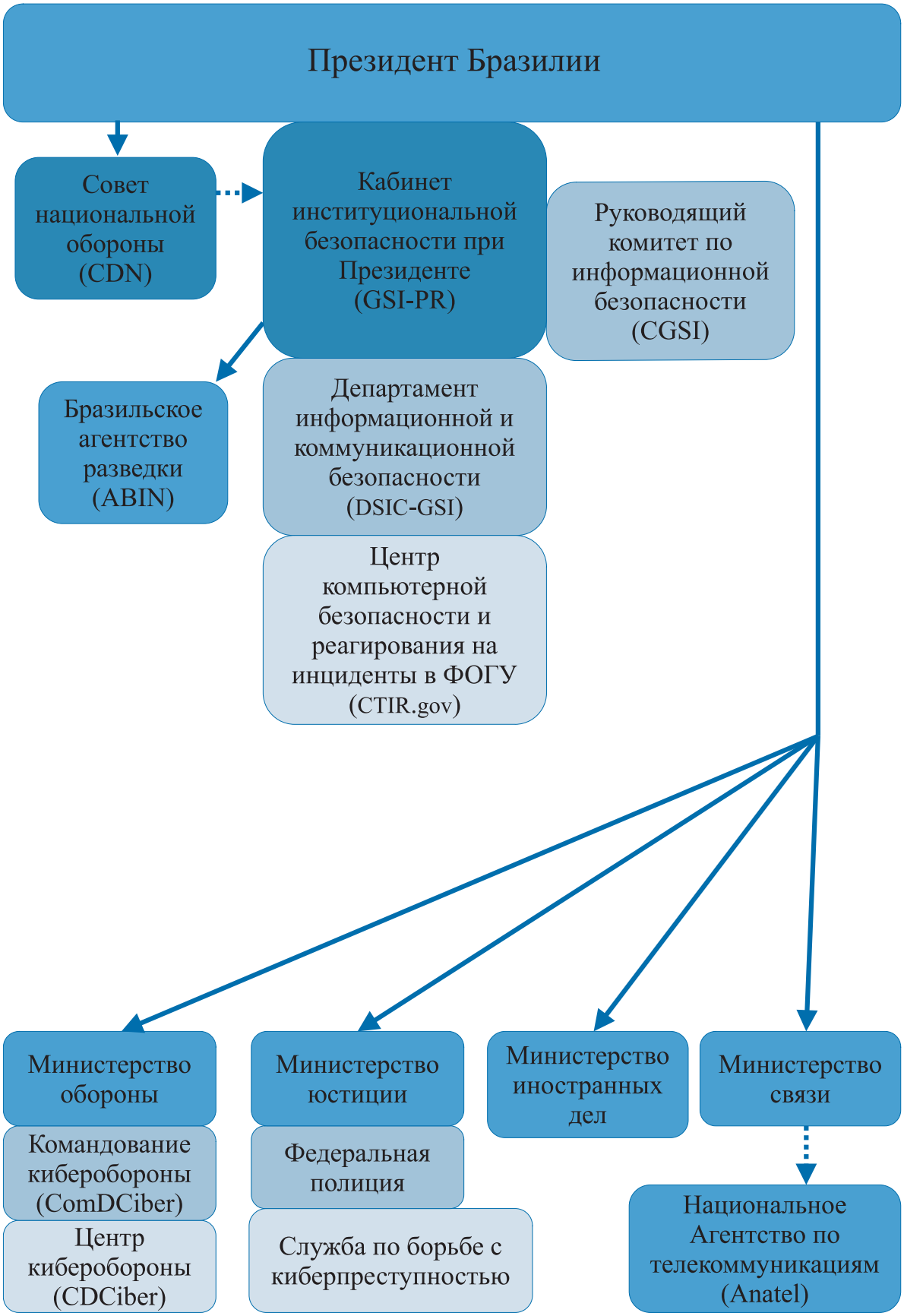


Рисунок 1. Основные элементы структура управления информационной и кибербезопасностью Бразилии

ностью, включая подготовку предложений по стратегиям и законодательным нормам. В этих целях в CGSI могут создаваться технические группы для обсуждения конкретных тем. Комитет также служит для информирования ФОГУ по профильным вопросам.

Практическая реализация функций Кабинета по направлению кибербезопасности осуществляется входящим в него **Департаментом информационной и коммуникационной безопасности** (Departamento de Segurança da Informação e Comunicações, DSIC-GSI), который руководит работой **Центра компьютерной безопасности и реагирования на инциденты** в ФОГУ (Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, CTIR.gov), а также координирует техническое сотрудничество в рамках ФОГУ и национальной сети групп реагирования на инциденты компьютерной безопасности.

Бразильское агентство разведки (Agência Brasileira de Inteligência, ABIN). Осуществляет разведывательную и аналитическую деятельность в киберпространстве и разработку систем защищенной связи для ФОГУ.

Деятельность **Министерства обороны** в киберпространстве осуществляется через Командование кибероборонь (ComDCiber) и Центр кибероборонь (CDCiber), которым поручена координация и интеграция усилий по кибероборонe между всеми родами войск.

Министерству юстиции подчинена Федеральная полиция, которая через **Службу по борьбе с киберпреступностью** проводит расследования киберпреступлений, в том числе против ФОГУ и для выполнения принятых международных конвенций, а также расследует компьютерные атаки на критически важные системы и инфраструктуры.

Министерство связи воссоздано в июне 2020 года (в 2016–20 годах его функции выполняло Министерство науки, технологий и инноваций) в целях укрепления национальной политики в области телекоммуникаций и телерадиовещания, и почтовых услуг. Оно также отслеживает взаимодействие между федеральным правительством и региональной, национальной и международной прессой, обеспечивает функционирование обязательных радио- и телевизионных сетей, занимается опросами общественного мнения и сотрудничает с системой общественного телевидения Бразилии.

Национальное агентство по телекоммуникациям (Anatel) является специализированной структурой, которая начала свою работу в 1997 году. Агентство является административно и финансово независимым и работает в особом правовом режиме, однако сохраняет взаимодействие с Министерством связи. Агентство призвано содействовать развитию телекоммуникаций для обеспечения страны современной и эффективной инфраструктурой. Среди его обязанностей можно выделить: реализацию в рамках своих полномочий национальной политики

в области телекоммуникаций; представление Бразилии в международных телекоммуникационных агентствах; сертификацию продукции с учетом установленных норм и стандартов, в том числе в области кибербезопасности.

За пределами федеральных органов государственного управления существует несколько академических и технических организаций, например, университетов, CERTs и CSIRTs, а также частных организаций, таких как малый и средний бизнес, крупные корпорации технологического сектора, которые играют важную роль в обеспечении кибербезопасности в Бразилии.

5. Участие в международном сотрудничестве с ООН и другими международными и региональными организациями в области формирования системы международной информационной безопасности

Внешняя политика Бразилии по вопросам кибербезопасности реализуется через координацию действий Министерства иностранных дел и иных федеральных органов государственного управления, в том числе Министерства обороны, а также Кабинета институциональной безопасности. За последние несколько лет были предприняты шаги для постепенной консолидации кибердипломатии на министерском уровне. В 2019 году введена должность дипломата по вопросам кибербезопасности, а в 2021 году МИД назначил своего первого «технического посланника», который отвечает за взаимодействие с технологическими компаниями в Кремниевой долине (США).

В соответствии с Национальной стратегией кибербезопасности предполагается расширение сотрудничества в области кибербезопасности с максимальным количеством стран и укрепление международной позиции Бразилии. Для этого предложены следующие меры:

- стимулирование международного сотрудничества в сфере кибербезопасности;
- поощрение дискуссий по кибербезопасности в организациях, форумах и международных группах, участником которых является Бразилия;
- расширение связей со странами Латинской Америки;
- продвижение международных мероприятий и учений по кибербезопасности;
- участие в международных мероприятиях;
- расширение соглашений о сотрудничестве в сфере кибербезопасности;
- расширение использования международных механизмов борьбы с киберпреступностью;
- участие в будущих регулятивных инициативах, например, в отношении стандартов безопасности передовых технологий;

- выявление, стимулирование и использование новых коммерческих возможностей в области кибербезопасности.

На протяжении многих лет Бразилия играла значимую роль в вопросе управления Интернетом с участием многих заинтересованных сторон. В 2013 году она вместе с Германией предложила проект знаковой резолюции ООН о праве на неприкосновенность частной жизни в эпоху цифровых технологий [14]. В 2014 году Бразилия провела Глобальную встречу с участием всех заинтересованных сторон для обсуждения будущего управления Интернетом (NETmundial).

Страна была членом пяти созывов ГПЭ ООН, в двух из них (2014–15 и 2019–21 годов[2]) ее представитель был председателем группы. Во многом благодаря проявленной им гибкости, в 2015 году был согласован знаковый доклад ГПЭ ООН с нормами ответственного поведения, инициатива разработки которых принадлежит России [15]. Кроме этого, представитель Бразилии является одним из вице-председателей в Специальном комитете ООН по разработке всеобъемлющей конвенции по противодействию информационной преступности[3].

В декабре 2021 года после быстрого процесса и непродолжительных публичных дебатов Бразилия стала шестой южноамериканской страной, подписавшей Будапештскую конвенцию о киберпреступности. Ранее позиция Бразилии заключалась в том, чтобы воздерживаться от подписания этого документа, поскольку страна не участвовала в его разработке. Внезапный разворот и смещение в сторону западноцентричного подхода в вопросах безопасности стал следствием, среди прочего, американо-китайских разногласий по поводу безопасности ИКТ. Президент Бразилии Жаир Болсонару выступил против Huawei, в то время как министр экономики выступал за более либеральный подход [16]. В итоге возобладал нейтральный подход, и Бразилия не запретила Huawei или любой другой компании участвовать в аукционе по сетям связи 5G, проводимом Агентством связи Бразилии, но решение было принято слишком поздно, чтобы помириться с Пекином и одновременно вызвало негативную реакцию Вашингтона.

Несмотря на то, что Бразилия подписала Будапештскую конвенцию, страна «полностью привержена идее универсальной конвенции» и «активно участвует в переговорах по всеобъемлющей конвенции по противодействию информационной преступности. Это уникальная возможность установить общие стандарты сотрудничества в решении такой, по сути, транснациональной проблемы, опираясь на лучшие традиции и практику в этом отношении» [17].

---

2 Группа 2014–15 годов созвана в соответствии с пунктом 4 резолюции 68/243 Генеральной Ассамблеи ООН, Группа 2019–2021 годов создана в соответствии с пунктом 3 резолюции 73/266 Генеральной Ассамблеи ООН.

3 Специальный комитет создан в соответствии с резолюцией Генеральной Ассамблеи ООН A/Res/74/247 от 27 декабря 2019 года «Противодействие использованию информационно-коммуникационных технологий в преступных целях», https://www.unodc.org/documents/Cybercrime/AdHocCommittee/N1944028.pdf

В Организации американских государств Бразилия является участником Комплексной межамериканской стратегии по борьбе с угрозами кибербезопасности (принята в 2004 году)[18]. В Союзе южноамериканских наций, до того как Бразилия покинула эту организацию в 2018 году, она продвигала идею обще регионального сотрудничества в области киберзащиты [19].

Федеральное правительство Бразилии официально не поддержало Парижский призыв к доверию и безопасности в киберпространстве, но это самостоятельно сделали 17 национальных корпораций, неправительственных организаций, государственных органов, а также штат Сан-Паулу [20].

Бразилия имеет прочные отношения с Европейским Союзом благодаря множеству соглашений по вопросам киберпространства. Например, в 2010 году начался Диалог Бразилия-ЕС по вопросам информационного общества и цифровой экономики, а в 2017 году был дан старт Кибердиалогу ЕС-Бразилия [21].

Следует отметить, что правовой основы для сотрудничества между Россией и Бразилией в рассматриваемой сфере сформировать не удалось. В мае 2010 года было подписано Соглашение между Правительством Российской Федерации и Правительством Федеративной Республики Бразилии о сотрудничестве в области обеспечения международной информационной и коммуникационной безопасности. Оно ратифицировано российским правительством, но в силу не вступило.

6. Возможные приоритеты в сфере обеспечения информационной безопасности и международной информационной безопасности в рамках БРИКС

По некоторым свидетельствам [22], бразильские дипломаты в дебатах о нормах ответственного поведения государств характеризуют свою страну как посредника или строителя стратегических мостов между различными лагерями и подчеркивают, что баланс между обоими лагерями служит поддержанию независимости внешней политики.

Во время первого президентства Лулы да Силвы Бразилия стремилась укрепить связи с Глобальным Югом, в том числе продвигать интересы в региональных и других механизмах, таких как Форум IBSA (Индия, Бразилия и Южная Африка). Президент Дилма Руссефф обеспечила некоторую преемственность этого подхода. Во время ее президентства в контексте БРИКС начали появляться новые и более конкретные направления сотрудничества в области кибербезопасности, например, поддержана инициатива создания Рабочей группы БРИКС по вопросам безопасности в сфере использования информационно-коммуникационных технологий. Правительство Болсонару отличалось парадоксальностью, но

при этом не всегда выступало против сотрудничества в области кибербезопасности. Недавние примеры включают ряд двусторонних соглашений и диалогов с Финляндией, Великобританией и Суринамом.

Бразилия считает, что международное право, в т.ч. международное гуманитарное право и международное право прав человека, в целом применимо в киберпространстве [23]. В то же время, это не следует понимать как легитимизацию превращения киберсреды в сферу военного противоборства. Это понимание должно заставить все государства проявлять сдержанность и способствовать поддержанию безопасной, надежной, стабильной и процветающей среды информационных и коммуникационных технологий [24].

Бразилия в 2021 году выразила поддержку предложению о принятии в средне- и долгосрочной перспективе юридически обязательного инструмента для предотвращения милитаризации киберпространства, а в 2005 году поддержала позицию России относительно создания международного режима контроля над информационным оружием [25].

7. Список использованной литературы

1. Население Бразилии, численность, занятость, безработица, гендерный состав // BDEX, https://bdex.ru/naselenie/brazil/?ysclid=lpejmdm3nh394737224
2. Brazil Data // World Bank, https://data.worldbank.org/country/brazil
3. Pesquisa sobre o uso das Tecnologias de Informação e Comunicação nas empresas brasileiras // TIC Empresas, 2017, https://www.cetic.br/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-nas-empresas-brasileiras-tic-empresas-2017/
4. Facilities and Data Centers in Brazil // DataCenterJournal, https://www.datacenterjournal.com/data-centers/brazil/
5. Infrastructures for Brazil's digital economy. Going Digital in Brazil // OECD iLibrary, https://www.oecd-ilibrary.org/sites/2f42e299-en/index.html?itemId=/content/component/2f42e299-en
6. Global Cybersecurity Index 2020, https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E
7. Internet Organised Crime Threat Assessment (IOCTA) 2018, https://www.europol.europa.eu/cms/sites/default/files/documents/iocta2018.pdf
8. Sergiu Gatlan Brazil's court system under massive RansomExx ransomware attack, November 5, 2020, https://www.bleepingcomputer.com/news/security/brazils-court-system-under-massive-ransomexx-ransomware-attack/
9. Brazil's Eletrobras says nuclear unit hit with cyberattack // Reuters, February 4, 2021, https://www.reuters.com/article/us-eletrobras-cyber-idUSKBN2A41JN
10. Vazamento expõe CPF de 220 milhões de brasileiros //Olhar Digital, 20.01.2021, https://olhardigital.com.br/en/2021/01/20/seguranca/vazamento-de-banco-de-dados-expoe-cpf-de-quase-toda-a-populacao-do-brasil/
11. The National Defense Strategy, https://www.files.ethz.ch/isn/154868/Brazil_English2008.pdf
12. National Information Security Policy// PNSI, 2021, https://www.gov.br/gsi/pt-br/dsic/legislacao/dec_9637_traducao_19_nov_2021_limpa.pdf
13. Summary of the Brazilian Artificial Intelligence Strategy //EBIA 2021, https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ebia-summary_brazilian_4-979_2021.pdf
14. «Право на неприкосновенность личной жизни в цифровой век», A/RES/68/167, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/449/49/PDF/N1344949.pdf?OpenElement
15. Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности/ Записка Генерального секретаря A/70/174 от 22 июля 2015 года, https://documents.un.org/doc/undoc/gen/n15/228/37/pdf/n1522837.pdf?token=jCSfcHccTVOrITLDdE&fe=true

16. Oliver Stuenkel Brazilian 5G: The Next Battleground in the U.S.-China Standoff // Americas Quarterly, January 15, 2020, https://www.americasquarterly.org/article/brazilian-5g-the-next-battleground-in-the-u-s-china-standoff/
17. Brazilian Government's position regarding the objectives, scope and structure of an international convention on countering the use of information and communications technologies for criminal purposes //Permanent Mission of the Federative Republic of Brazil, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/Brazil_AHC_Brazilian_Position.pdf
18. Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity// Inter-American Telecommunication Commission, Organization of American States, July 2004, http://www.oas.org/en/citel/infocitel/julio-04/ult-ciberseguridad_i.asp
19. Brazil Asks South American Nations to Join Cyber Treaty // The BRICS Post, 25 November 2013, http://www.thebricspost.com/brazil-asks-south-american-nations-to-join-cyber-treaty/#.X66JJsj7SUk
20. Supporters — Paris Call, https://pariscall.international/en/supporters
21. Hannes Ebert and Louise Marie Hurel, 'Brazil–EU Cyber Cooperation: Swinging Bridges on the Road to Stability in 28 The International Institute for Strategic Studies Cyberspace', Council on Foreign Relations, 25 March 2020, https://www.cfr.org/blog/brazil-eu-cyber-cooperation-swinging-bridges-road-stability-cyberspace
22. Hannes Ebert and Laura Groenendaal Brazil's Cyber Resilience and Diplomacy: The Place for Europe // The German Marshall Fund of the United States, April 2020, https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/2IbYw_1n/brazil_digital-dialogue_eucd_he.pdf
23. Официальный сборник добровольно представляемых национальных материалов по вопросу о том, как международное право применяется к использованию информационно-коммуникационных технологий государствами, предоставленных участвующими правительственными экспертами, входящими в Группу правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности, созданную в соответствии с резолюцией 73/266 Генеральной Ассамблеи, A/76/136* от 13 июля 2021 года, https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf
24. Norms, rules and principles // Digital Watch Observatory, 11 Feb 2020, https://dig.watch/event/open-ended-working-group-oewg-second-substantive-session/norms-rules-and-principles
25. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Доклад Генерального секретаря. Добавления, A/60/95/Add.1, 21 September 2005, C.4, https://digitallibrary.un.org/record/558279?v=pdf

Южно-Африканская Республика


Официальное название: Южно-Африканская Республика

Столица: Претория (административная), Кейптаун (законодательная), Блумфонтейн (судебная).

Официальный язык: английский, африкаанс, венда, зулу, коса, южный ндебеле, свати, северный сото, сесото, тсвана, тсонга, южноафриканский жестовый язык.

Территория: Площадь ЮАР является 24 мире и составляет 1 221 037 км². Государство расположено на южной оконечности Африки. Длина береговой линии составляет 2 798 км. Омывается водами Индийского и Атлантического океанов. Высшая точка ЮАР — гора Нджесути в Драконовых горах. Граничит со странами: Ботсвана, Лесото, Мозамбик, Намибия, Свазиленд, Зимбабве.

Население: На 1 декабря 2023 года численность населения (постоянных жителей) ЮАР составила 54 956 900 человек, что является 24 показателем в мире [1].

Государственное устройство: ЮАР является унитарным государством. Территория страны поделена на 9 провинций. ЮАР — президентско-парламентская республика. Двухпалатный парламент состоит из Национального совета провинций (верхняя палата, 90 членов) и Национальной ассамблеи (400 членов). Члены нижней палаты избираются по пропорциональной системе голосования: половина депутатов идут по общенациональным спискам, половина — по провинциальным. Каждая провинция, независимо от численности населения, посылает в Национальный совет провинций десять членов. Выборы проходят каждые пять лет. Правительство формируется в нижней палате, а лидер партии, получившей в ней большинство, становится президентом, сейчас этот пост занимает Сирил Рамафоса.

Экономика: По данным Всемирного банка за 2022 год показатели Валового внутреннего продукта (ВВП) по паритету покупательной способности (ВВП по ППС в текущих ценах):

Итого: 953 млрд долл. США (32 место в мире).

На душу населения: 15 905 долл. США (92 место в мире).

Показатели ВВП (по номинальному значению, в текущих ценах):

Итого: 406 млрд долл. (37 место в мире).

На душу населения: 6 777 долл. США (92 место в мире) [2].

Дипломатические отношения с Российской Федерацией были установлены 28 февраля 1992 года.

1. Уровень развития информатизации страны и ИКТ-инфраструктуры, системы обеспечения информационной безопасности

По данным МСЭ на 2021–2022 годы, 72,3% населения ЮАР пользовались сетью Интернет, что выше общемирового уровня в 66,3%, и почти вдвое превышает показатель по африканскому Континенту [3].

В 2016 году была принята **Национальная комплексная белая книга по политике в области ИКТ**. В ней определены сферы, в которых имеются пробелы в плане инфраструктуры и услуг, и способы устранения этих пробелов и сокращения цифрового разрыва с помощью инвестиций со стороны правительства и частного сектора. В документе 2013 года **Соединим Южно-Африканскую Республику** [4] сформулирована политика в области широкополосной связи. Общая цель заключается в достижении к 2030 году средней скорости широкополосной связи на уровне 100 Мбит/с, при этом заданы промежуточные целевые показатели для домохозяйств, школ, медицинских учреждений и правительства.

В ЮАР несколько точек обмена международным трафиком[1] и корневой сервер доменных имен сети Интернет (DNS). Страна подключена к более чем шести подводным волоконно-оптическим системам на нескольких станциях выхода подводного кабеля на берег.

Подвижная телефонная связь получила практически повсеместное распространение, в 2016 году мобильные телефоны имелись у 87% домохозяйств. Более трех четвертей населения находятся в пределах зоны действия сигнала подвижной широкополосной связи (4G), что является наиболее высоким уровнем охвата в странах Африки к югу от Сахары.

В ЮАР имеется 15 центров обработки данных, которыми управляют восемь организаций: Internet Solutions ZA имеет наибольшее присутствие с четырьмя объектами, а другие организации включают Teraco Data Environments, Africa Data Centers и Bunker One Management. В число городов, где имеются центры обработки данных, входят Йоханнесбург, Дурбан и Кейптаун [5].

ЮАР, наряду с Нигерией, Египтом и Кенией, обеспечивают 50% ключевых цифровых индикаторов Африки. Именно эти страны обладают потенциалом быстрой отдачи от вложенных в их цифровую экономику денег. В ЮАР наибольшее число африканских разработчиков программного обеспечения (около 120 тыс.)[2].

Согласно Индексу сетевой готовности (NRI) 2023 года, страна занимает 74 место из 134, но по Африке она на втором месте [6]. Одновременно от-

1 В стране функционируют две точки обмена международным трафиком IXP: INX с одноранговыми центрами и NAP Africa, действующие в Йоханнесбурге, Кейптауне и Дурбане.
2 Accenture/IFC Google 2020

мечается, что показатели ЮАР лишь немного ниже стран с сопоставимым уровнем дохода.

Недостатком является низкая доступность услуг связи — по данным 2022 года стоимость интернет-данных в ЮАР относительно высока. Страна заняла 27 место из 49 по доступности данных в регионе к югу от Сахары [7].

Развитие цифровой экономики является приоритетом для правительства, при этом обеспечение необходимой ИКТ-инфраструктуры является частью **Национального плана развития до 2030 года**, который был представлен в 2012 году [8]. В середине 2021 года правительство вместе с заинтересованными сторонами также разработало **Генеральный план цифровой экономики** [9].

ЮАР также является одной из ведущих стран на континенте по развитию искусственного интеллекта (ИИ) и занимает 70 место в глобальном рейтинге из 160 стран [10]. Правительство учредило Президентскую комиссию по четвертой промышленной революции, что можно считать шагом к созданию национальной стратегии ИИ. Комиссия рекомендовала основать Институт искусственного интеллекта (создан в ноябре 2022 года) и развивать сотрудничество с южноафриканскими университетами для развития цифровых навыков [11]. В 2023 году создана Южноафриканская ассоциация искусственного интеллекта для продвижения развития ответственного ИИ [12].

В Глобальном индексе кибербезопасности МСЭ 2020 года ЮАР заняла 59 место в общем рейтинге и 8 место среди стран Континента [13]. По данным компании Accenture, в 2020 году Южно-Африканская Республика находилась на третьем месте в мире по количеству жертв киберпреступлений, а потери составили около 120 млн долл. США [14]. Эти статистические данные коррелируют с Отчетом Интерпола об оценке киберугроз в Африке за 2021 год [15], согласно которому в период с января 2020 по февраль 2021 года в стране зафиксировано 230 млн атак, из которых 219 млн связаны с электронной почтой. Согласно тем же данным, ЮАР больше всего пострадала от целенаправленных атак программ-вымогателей. При этом, киберугрозам все чаще подвержены объекты критически важной инфраструктуры. В июле 2021 года компания Transnet, которая управляет национальной железнодорожной, портовой и трубопроводной инфраструктурой, подверглась крупной кибератаке, которая привела к серьезным нарушениям в работе морской инфраструктуры [16]. В том же году атакам подверглись Министерство юстиции и конституционного развития и Южноафриканское национальное космическое агентство [17]. Рост числа компьютерных преступлений во время пандемии привел к срочному принятию **Закона о киберпреступлениях** в декабре 2021 года [18].

В секторе телекоммуникаций директивным органом является Министерство связи и цифровых технологий (Department of Communications and Digital

Technologies). За регулирование в отраслях электросвязи, радиовещания и почтовых служб отвечает Независимое управление связи ЮАР (Independent Communications Authority of South Africa, ICASA). Управление было создано в июле 2000 года в результате слияния Южноафриканского регуляторного органа электросвязи и Независимого управления радиовещания.

2. Основные документы стратегического планирования в сфере развития ИКТ, обеспечения национальной и международной информационной безопасности

В связи с высоким уровнем компьютерной преступности и уязвимостью информационных сетей, основной задачей правительства является противодействие этим угрозам и формирование соответствующей государственной политики.

2.1. **Стратегия исследований, разработок и инноваций в области ИКТ для Южной Африки** (2007)

Цель Стратегии (Information and Communication Technology (ICT) Research and Development (R&D) and Innovation Strategy for South Africa [19]) состоит в том, чтобы создать благоприятную основу для систематической поддержки исследований, разработки и инноваций в области ИКТ. Она устанавливает план и рамки для максимального увеличения вклада исследований, разработок и инноваций в науку и технологии в ЮАР; при этом обеспечивает последовательный, систематический подход, который будет способствовать улучшению качества жизни и повышению экономической конкурентоспособности. Заложенное видение развития ИКТ к 2015 году предполагало построение инклюзивного информационного общества, в котором процветают инновации на основе ИКТ. Это видение поставило задачу достижения следующих результатов:

- глобальное лидерство в определенных ключевых научных и технологических областях;
- разработка междисциплинарных технологий, навыков и методологий для решения проблем, которыми пренебрегает рынок, особенно для искоренения цифрового разрыва;
- собственный сектор ИКТ, который является развитым, растущим, инновационным и конкурентоспособным;
- разумное распространение ИКТ в других секторах экономики.

Стратегия реализуется посредством последовательной, интегрированной и хорошо управляемой системы партнерств, финансирования, процессов, политики и инфраструктуры. В основе стратегии лежат три стратегические и четыре вспомогательные задачи.

Стратегические задачи:

- целенаправленные исследования мирового уровня: сосредоточить и усилить исследовательскую деятельность в высших учебных заведениях и научно-исследовательских институтах для создания в стране признанных исследовательских компетенций мирового уровня;
- сильная и надежная инновационная цепочка, которая должна привести к увеличению количества патентов в области ИКТ, улучшению показателей цифрового неравенства и динамичной высокотехнологичной отрасли ИКТ для малых, средних и микро-предприятий;
- развитый потенциал человеческих ресурсов: добиться заметного увеличения базы передовых навыков в области ИКТ, чтобы улучшить способность к освоению ИКТ и тем самым обеспечить целенаправленные исследования и инновации.

Вспомогательные задачи:

- создать мощную исследовательскую инфраструктуру, поддерживающую целенаправленные исследования и сотрудничество на национальном и международном уровнях;
- создать прочные связи в области НИОКР со странами, которые являются ведущими игроками в области ИКТ;
- внедрить эффективную политику и другие структуры поддержки в Министерстве науки и технологий, его агентствах и вузах;
- обеспечить ресурсами системы НИОКР и инноваций в области ИКТ.

2.2. Рамочная национальная политика в области кибербезопасности (2012)

В 2010 году по указанию Агентства государственной безопасности Министерство связи[3] начало разработку Рамочной национальной политики в области кибербезопасности (National Cybersecurity Policy Framework, NCPF [20]). После доработки, в марте 2012 года проект был утвержден Кабинетом министров ЮАР. В документе дана оценка угроз национальной безопасности в киберпространстве и поставлена задача противодействия им. Политика предназначена для формирования целостного подхода к кибербезопасности всех акторов, а её реализация обеспечивается Национальным планом реализации кибербезопасности, который было поручено разработать силовому блоку органов юстиции, охраны правопорядка и обеспечения безопасности (JCPS Cluster) с привлечением соответствующих заинтересованных сторон. Политикой определены роли и обязанности акто-

3 Название до 2014 года, после — Министерство телекоммуникаций и почтовых услуг, с 2019 года — Министерство связи и цифровых технологий.

ров, сроки, конкретные показатели эффективности, а также механизмы мониторинга и оценки. Рамочная национальная политика в области кибербезопасности соответствует мандату и обязательствам Силового блока.

В этом отношении рамочная Политика направлена на развитие мер по устранению киберугроз национальной безопасности, мер по содействию борьбе с киберпреступностью. по укреплению доверия к безопасному использованию ИКТ; разработку, обзор и обновление существующих норм материального и процессуального права для обеспечения их согласованности.

Согласно документу, ключевыми целями национальной политики являются:

- централизация процесса координации действий в сфере кибербезопасности, в том числе путем создания соответствующих структур, политических механизмов и стратегий, направленных на борьбу с киберпреступностью, решение задач национальной безопасности и развитие информационного общества и экономики, основанной на знаниях;
- развитие сотрудничества и координации между правительством, частным сектором и гражданским обществом путем стимулирования и поддержания тесной взаимосвязи между политикой, законодательством, общественным одобрением и технологиями;
- развитие международного сотрудничества;
- развитие необходимых навыков и научно-исследовательского потенциала;
- продвижение культуры кибербезопасности;
- содействие соблюдению необходимых технических и эксплуатационных стандартов кибербезопасности.

В документе отмечается, что в списке международных, а также национальных угроз безопасности злонамеренное использование киберпространства и ИКТ стоит на первом месте, и проблемы киберугроз необходимо решать, как на глобальном, так и на национальном уровне. NCPF формулирует и решает следующие задачи:

- разработка и реализация последовательного и комплексного правительственного подхода к обеспечению кибербезопасности и устранению угроз кибербезопасности;
- создание в JCPS специализированного органа по разработке политики, стратегий и принятию решений — Комитета реагирования на угрозы кибербезопасности (Cybersecurity Response Committee, CRC) для определения приоритетных областей противодействия киберугрозам. Комитет возглавляется генеральным директором Агентства государственной безопасности (SSA), а Центр кибербезопасности Агентства (Cybersecurity Centre) оказывает Комитету оперативную поддержку;
- наращивание возможностей по эффективной координации ресурсов департаментов для достижения общих целей кибербезопасности и защи-

щенности (включая планирование, координацию реагирования, а также мониторинг и оценку);
- эффективная борьба с киберпреступностью посредством продвижения скоординированных подходов и планирования, а также подготовки необходимого персонала и инфраструктуры;
- координация продвижения мер кибербезопасности всеми акторами (государством, частным сектором, гражданским обществом и группами с особыми интересами) совместно с Узловым центром кибербезопасности (Cybersecurity Hub, который создан в Министерстве связи и цифровых технологий и представляет собой государственный CSIRT[4] с расширенными полномочиями);
- усиление сбора разведывательной информации, расследований, судебного преследования и судебных процессов для предотвращения и борьбы с киберпреступностью, кибертерроризмом и кибервойнами;
- обеспечение защиты национальной критической информационной инфраструктуры;
- продвижение культуры кибербезопасности и соблюдение базовых стандартов безопасности;
- создание государственно-частного партнерства для реализации национальных планов и планов действий в соответствии с NCPF;
- обеспечение всеобъемлющей правовой базы, регулирующей киберпространство.

2.3. **Национальный план развития до 2030 года** (2012)

Национальный план развития (National Development Plan 2030. Our Future-make it work [21]) является всеобъемлющим документом, затрагивающим большинство сфер человеческой деятельности, конечная цель которого — к 2030 году устранить бедность и сократить неравенство. Этому должно способствовать, в том числе, решение ряда задач в сфере ИКТ. Непосредственной политической целью является обеспечение того, чтобы национальные структуры ИКТ адекватно поддерживали потребности экономики, позволяя участвовать в процессе сторонам, не входящим в государственный сектор.

В Плане говорится, что для достижения целей в области ИКТ ЮАР должна иметь скоординированную стратегию и план в области ИКТ. Ключевыми аспектами этого должны стать:

- национальная электронная стратегия, охватывающая все государственные ведомства и сектора;

4 Computer Security Incident Response Team, группа реагирования на инциденты компьютерной безопасности.

- стимулирование инноваций через государственные и частные инвестиции в ИКТ, особенно для модернизации и расширения сетей, а также разработки приложений и местного контента;
- создание общей операторской сети, возможно, путем структурного отделения магистральных операций Telkom от розничных услуг;
- развитие институционального потенциала для обеспечения соответствия политики уровню развитию сектора и эффективности регулирования;
- стимулирование спроса путем продвижения электронной грамотности, введения скидок и стимулов в области ИКТ и разработки приложений ИКТ в таких секторах, как здравоохранение и образование, а также в инфраструктуре и учреждениях;
- эффективное вовлечение различных учреждений, в том числе глобальных агентств по управлению ИКТ, таких как Международный союз электросвязи и Всемирная торговая организация, по вопросам региональной интеграции и гармонизации.

2.4. **Политика ЮАР в области широкополосной связи** (2013)

В ответ на развивающиеся глобальные тенденции и в целях удовлетворения разнообразных потребностей народа Южной Африки в Политике широкополосной связи [22] применяется всеобъемлющий подход. Политика предполагает устранение ограничений, влияющих на рост конкурентоспособности рынка широкополосной связи, при этом Независимое управление связи Южной Африки (ICASA) проводит политику единого строительства, оказывает поддержку инфраструктурным проектам и поощряет совместное использование инфраструктуры. Политика установила, что правительство через Министерство связи[5] осуществляет координацию развертывания широкополосной связи, опираясь на успехи, достигнутые на областном и муниципальном уровнях. Для удовлетворения потребностей государственного сектора в широкополосной связи и с целью облегчения закупок была организована программа South Africa Connect. Политикой также предусмотрено введение программ электронной готовности в школах и клиниках, развитие навыков, а также проведение кампаний по повышению осведомленности и цифровой грамотности.

2.5. **Обзор обороны ЮАР** (2015)

Этот Обзор обороны (South African Defence Review [23]) является вторым по счету в Южно-Африканской Республике (первый был осуществлен в 1998 году),

5 См. сноску 3.

в нем обозначены направления развития обороны на следующие 20–30 лет. Относительно положения дел в сфере ИКТ, в обзоре сказано, что ЮАР требуется защита национального киберпространства посредством комплексного потенциала ведения информационной войны, интегрированного в ее разведывательные информационные системы, на международном, национальном и ведомственном уровнях. Для обеспечения безопасности критически важных сетей необходимо усилить возможности как на уровне ведомства, так и государства в целом.

В Обзоре выделено четыре вида ИКТ-угроз:

- кибершпионаж, в том числе негласный сбор секретной информации без разрешения владельца информации;
- киберпреступления, в том числе использование вредоносного ПО, вирусов, кража личных данных, преднамеренный и несанкционированный доступ, изменение и/или перехват компьютерных данных или программ, компьютерное вымогательство, мошенничество и подлог;
- кибервойна, в том числе наступательные информационные операции;
- кибертерроризм, в том числе атаки через Интернет в рамках террористической деятельности отдельных лиц и групп.

Особо отмечается, что социальные сети все чаще используются злоумышленниками для мобилизации человеческого ресурса как на национальном, так и на международном уровнях. Эти технологии позволяют радикальным группировкам вербовать людей, а также планировать и финансировать террористические акты в различных странах. Поскольку национальные экономики все больше основываются на цифровых данных, серьезной угрозой становится использование технологий информационных войн.

В соответствии с рассмотренной выше Рамочной национальной политикой в области кибербезопасности (2012), Министерство обороны решает следующие задачи:

- устранение угроз национальной безопасности в киберпространстве;
- противодействие угрозам, в том числе кибервойне и киберпреступности;
- разработка, пересмотр и обновление существующего материального и процессуального законодательства для обеспечения их согласованности;
- укрепление доверия к использованию ИКТ и их безопасности.

Кроме этого, общая ответственность Министерства обороны за координацию, подотчетность и реализацию мер киберзащиты в ЮАР является неотъемлемой частью его мандата национальной обороны, поэтому ведомство возглавляет разработку соответствующих политик, стратегий и систем.

2.6. Белая книга национальной комплексной политики в области ИКТ (2016)

В Белой книге (National Integrated ICT Policy White Paper [24]) изложены всеобъемлющие политические механизмы по преобразованию ЮАР в инклюзивное и инновационное общество, основанное на цифровых технологиях и знаниях. В основе документа заложена идея конвергенции. Признается, что негативные изменения в традиционных секторах требуют адаптации всеобъемлющих политических подходов, чтобы облегчить, в том числе, всеобщий доступ к ИКТ, а также трансформацию почтового сектора и рост ИКТ-отрасли. Также признается, что политика должна учитывать потребности таких секторов, как образование, юстиция, здравоохранение и социальное обеспечение, чтобы цифровые технологии могли способствовать их целям развития, учитывая при этом, что конвергенция создает новые угрозы реализации прав на безопасность и неприкосновенность частной жизни.

Белая книга содержит: подход правительства к обеспечению лидерства и содействию участию многих заинтересованных сторон в рамках инклюзивной цифровой трансформации в ЮАР (Глава 4); меры по усилению честной конкуренции и содействию инновациям в конвергентной среде, включая подходы к решению проблемы горизонтальной и вертикальной интеграции в цепочке создания стоимости (Глава 6); рассмотрение вопросов ИКТ и конвергенции (Глава 7); политику защиты открытого Интернета (Глава 8). Также перечислены меры по содействию цифровой трансформации общества: политика устранения цифрового разрыва и обеспечения доступности ИКТ для всех (Глава 5); подходы к решению проблем со стороны предложения и развертыванию инфраструктуры, включая управление дефицитными ресурсами, меры по содействию открытому доступу и быстрому развертыванию инфраструктуры, а также структура лицензирования ИКТ (Глава 9) и политика решения проблем спроса с целью содействия инклюзивной цифровой трансформации в ЮАР (Глава 10).

При разработке подходов и политики, принятых в Белой книге, учитывался ряд принципов: политика, основанная на правах человека; целостность политики; общеправительственный подход; участие многих заинтересованных сторон; обеспечение гибкости и уверенности; ответственность правительства за обеспечение устойчивого развития.

2.7. Национальная стратегия и дорожная карта электронного правительства (2017)

Целью документа (National e-Government Strategy and Roadmap [25]) является цифровая трансформация государственного управления ЮАР в инклюзивное цифровое общество, где все граждане могут извлечь выгоду из возможностей, предлагаемых цифровыми технологиями, для улучшения качества своей жизни. Этот документ определяет обновленный подход и программу действий, которые радикально улучшат ситуацию с электронным правительством. Министерство связи и цифровых технологий, которое ответственно за реализацию Стратегии, координирует работу с другими правительственными ведомствами, оказывающими услуги населению. Новый подход и программа действий не подменяют существующие политику и структуры электронного правительства. Министерство ставит задачу поддержки Государственного агентства информационных технологий (SITA), которое должно создать благоприятную ИКТ-среду для предоставления электронных услуг гражданам ЮАР. Реализации Стратегии должно способствовать решение следующих задач:

- создание структуры и институционального механизма для надзора за реализацией программ электронного правительства;
- создание нормативно-правовой базы, поддерживающей принятие и внедрение электронного правительства;
- создание структуры, способствующей эффективному и действенному взаимодействию граждан с правительством, внутри правительства, правительства с бизнесом и правительства с сотрудниками;
- внедрение безопасной, надежной и совместимой инфраструктуры электронного правительства;
- использование ИКТ в эффективной среде электронного правительства для достижения приоритетных целей социально-экономического развития;
- стимулирование активного и прямого участия частного сектора во внедрении электронного правительства;
- разработка центрального портала услуг электронного правительства;
- интеграция услуг электронного правительства;
- разработка программ развития потенциала и навыков;
- создание центров обработки звонков для электронного правительства.

2.8. Национальная стратегия цифровых навыков и навыков будущего (2020)

Разработанная Министерством связи и цифровых технологий Стратегия (National Digital and Future Skills Strategy South Africa [26]) представляет собой

структурированный ряд инициатив, призванных способствовать расширению возможностей южноафриканцев решать проблемы, возникающие в результате продолжающегося внедрения цифровых технологий с учетом того, что цифровая революция происходит в контексте более широкой четвертой промышленной революции. В совокупности эти факторы оказывают существенное влияние на сферу труда, образования и исследований. Элементы стратегии реализуются рядом заинтересованных сторон, включая правительство, частный сектор и образовательные учреждения. В Стратегии представлено восемь взаимосвязанных элементов, в каждом из которых свой набор действий, всего 28 пунктов. Первые четыре элемента связаны с взаимоотношениями между государством, промышленностью, трудовыми сообществами, университетами и учебными заведениями: цифровые основы — базовые и промежуточные цифровые навыки; цифровое будущее и мастерство — развитие передовых цифровых навыков; навыки для Индустрии 4.0; создание общества 4.0 и устранение разрыва в цифровых навыках.

Остальные четыре элемента Стратегии носят сквозной характер: повышение осведомленности о цифровых навыках; исследования и мониторинг цифровых навыков; координация между правительством, промышленностью, профсоюзами и другими группами заинтересованных сторон; приобетения цифровых навыков.

2.9. **Генеральный план по ИКТ и цифровой экономике** (2021)

Генеральный план (ICT and Digital Economy Masterplan for South Africa [27]) представляет собой инструмент, позволяющий правительству мобилизовать социальных партнеров и двигаться к реализации своей политики. Он разработан в результате тщательного исследования и обширных консультаций с заинтересованными сторонами в государственном, частном и гражданском секторах. В нем изложено амбициозное видение того, что в течение следующих пяти лет цифровая экономика может дать ЮАР, а также практический план действий по реализации этого видения. Головным исполнителем намеченных действий является Министерство связи и цифровых технологий. Оно играет роль ведущего координатора в тех случаях, где требуется привлечение других государственных ведомств, частного сектора или гражданского общества. Министр созывает Исполнительный комитет по надзору (Executive Oversight Committee, EOC), в состав которого входят высокопоставленные представители правительства, частного сектора и профсоюзов, которые консультируют министра по вопросам реализации Генерального плана и осуществляют надзор за его реализацией.

3. Состояние нормативно-правовой базы в сфере развития ИКТ и передовых технологий, обеспечения национальной информационной безопасности

Согласно данным МСЭ, за 2023 год в ЮАР сформирована развитая система правового регулирования цифровой экономики[6].

Основным законом страны является Конституция Южно-Африканской Республики (вступила в силу 4 февраля 1997 года), определяющая ЮАР как демократическую, независимую республику, основанную на принципах защиты достоинства, прав человека и верховенства закона. Как и предыдущая, Временная конституция (1994–97 гг.), она предусматривает создание многорасового демократического государства.

В сфере противодействия компьютерным преступлениям действующее законодательство включает принятый в 2021 году Закон о киберпреступлениях, основанный на законопроекте «О киберпреступлениях и кибербезопасности» 2015 года, а также Закон об электронных коммуникациях и транзакциях, Закон о регулировании перехвата сообщений и предоставлении соответствующих данных, Закон о защите персональных данных, Закон о защите критической инфраструктуры [28,29,30,31].

Полиция ЮАР с 2012 года ведет базу данных жертв компьютерных преступлений (VOCS), что позволяет оценивать характер, распространённость и модели нападений, прогнозировать риски и уведомлять о них пользователей и разработчиков средств защиты, формировать понимание о работе правоохранительной системы, частью которой является взаимодействие полиции с провайдерами.

В ЮАР функционирует несколько Интернет-порталов, предоставляющих возможность конфиденциально сообщить о компьютерном преступлении[7], компьютерных атаках,[8] угрозах критическим инфраструктурам[9], распространении спама[10], нарушении авторских прав[11], мошенничестве и фишинге [32].

---

6 По методике G5 Benchmark, включающей оценку регулирования телекоммуникационного сектора, ИКТ-отрасли и цифровой политики, правовых и регуляторных рамок, ЮАР получила 69,29 балла, что обеспечило ей попадание в группу развитых государств (индекс от 60 до 80 баллов). Источник: Benchmark for Fifth Generation Digital Collaborative Regulation/ G5 Benchmark, ITU, https://app.gen5.digital/benchmark/concepts.

7 Сайт полицейских служб — SAPS.gov.za, сайт компании Primedia — Crimeline.co.za, сайт независимой организации — Reportacrime.co.za.

8 Сайт Центра компьютерной безопасности университета Йоханнесбурга, созданного при участии МСЭ — UJ.ac.za

9 Национальный оперативный центр — noc@ssa.gov.za. Агентство государственной безопасности — ecs-csirt@e-comsec.com.

10 Сервис компании ISPA — ISPA.org.za, сервис компании WASPA- SMScode.co.za.

11 Сервис компании Microsoft — HowToTell.com.

3.1. Закон об электронных коммуникациях и транзакциях (2002)

Основными целями Закона (Electronic Communications and Transactions Act [33]) являются:

- облегчение и регулирование электронных коммуникаций и транзакций;
- разработка Национальной электронной стратегии;
- содействие всеобщему доступу к электронным коммуникациям и транзакциям, а также использованию электронных транзакций малым и средним бизнесом;
- развитие человеческих ресурсов в области электронных транзакций;
- предотвращение злоупотреблений информационными системами;
- поощрение использования электронных государственных услуг.

Закон также предписывает создание на предприятиях должностных позиций «инспектор по кибербезопасности», которые должны действовать в интересах национальной безопасности. Важно отметить, что на данный момент это слабо реализуется ввиду кадрового дефицита.

В соответствии с главой IX, должны предприниматься и/или изыскиваться меры по защите критической информационной инфраструктуры (КИИ) от компьютерных атак. Статьи 53, 54, 55 определяют должностных лиц, на которых возложено право разработки таких мер, в том числе определение данных, которые должны быть засекречены в интересах национальной безопасности, защиты экономики и благополучия граждан, правила регистрации и управления КИИ. В частности, процедура регистрации включает предоставление полного имени, адреса и контактных данных администратора критической базы данных, местоположение КИИ или ее компонентов, краткое описание хранящейся информации.

Правила управления КИИ должны включать порядок доступа и обработки информации, правила и процедуры обеспечения целостности и безопасности КИИ, резервного копирования, планы действий в чрезвычайных ситуациях, включая вывод из строя отдельных компонент КИИ, восстановление системы и обеспечение непрерывности управления.

Статья 55(2) определяет, что процедуры и механизмы управления КИИ, находящиеся в управлении государственных органов, должны быть согласованы с членами Кабинета министров (Министерства обороны, Полиции и Агентства государственной безопасности). Это гарантирует, что будут применяться принципы управления рисками, разработанные ОЭСР.

3.2. Закон о регулировании перехвата сообщений и предоставлении соответствующих данных (2002)

Закон (Regulation of Interception of Communications and Provision of Communication-related Information Act) призван:

- регулировать перехват определенных сообщений, осуществлять мониторинг сигналов и радиочастотных спектров и предоставлять соответствующие данные;
- регулировать подачу заявок и выдачу распоряжений, разрешающих перехват сообщений и предоставление данных при определенных обстоятельствах;
- регулировать исполнение сотрудниками правоохранительных органов указаний и ордеров, а также оказание поставщиками почтовых услуг, поставщиками телекоммуникационных услуг и держателями ключей шифрования содействия при выполнении таких указаний и ордеров;
- запретить предоставление телекоммуникационных услуг, которые не могут быть перехвачены;
- предусмотреть покрытие некоторых расходов, которые должны нести определенные поставщики телекоммуникационных услуг;
- предусмотреть создание центров перехвата, Управления центров перехвата и Фонда помощи Интернет-провайдерам;
- запретить производство, сборку, владение, продажу, покупку или рекламу определенного оборудования;
- криминализировать соответствующие преступления и установить наказание за них.

3.3. Закон о защите персональных данных (2013)

Целью Закона (The Protection of Personal Information Act) является:

- реализация конституционного права на неприкосновенность частной жизни путем защиты личной информации при ее обработке ответственной стороной, с учетом оправданных ограничений, которые направлены на:
- поддержание баланса между правом на неприкосновенность частной жизни и другими правами, в частности правом на доступ к информации;
- защиту важных интересов, включая свободный поток информации внутри страны и за рубежом;
- регулирование способов обработки личной информации путем установления условий в соответствии с международными стандартами, которые предписывают минимальные пороговые требования для законной обработки личной информации;

- предоставление владельцам персональных данных права и средств защиты их личной информации от обработки, не соответствующей настоящему Закону;
- принятие добровольных и обязательных мер, включая учреждение регулятивного органа для обеспечения уважения, продвижения, обеспечения соблюдения и реализации прав, защищаемых настоящим Законом.

3.4. **Закон о защите критической инфраструктуры** (2019)

Принятый в 2019 году Закон (Critical Infrastructure Protection Act [34]) призван:
- защитить критически важную инфраструктуру от угроз;
- гарантировать конфиденциальность информации, касающейся мер безопасности, применимых к критически важной инфраструктуре;
- обеспечить разработку объективных критериев для идентификации, объявления и защиты критически важной инфраструктуры;
- обеспечить государственно-частное партнерство в выявлении и защите критически важной инфраструктуры;
- обеспечить безопасность критически важной инфраструктуры путем создания условий, в которых обеспечивается общественная безопасность, общественное доверие и основные государственные услуги;
- посредством реализации мер, направленных на обеспечение безопасности критически важных инфраструктур, путем снижения рисков для них через оценку уязвимостей и реализацию соответствующих мер;
- содействовать сотрудничеству и культуре совместной ответственности между различными участниками, чтобы обеспечить междисциплинарный подход к решению вопросов защиты критически важной инфраструктуры;
- повысить коллективный потенциал акторов, отвечающих за защиту критически важной инфраструктуры, для смягчения возможных рисков безопасности;
- гарантировать, что каждый объект критической инфраструктуры соответствует нормам защиты от ИКТ-угроз;
- определить полномочия и обязанности лиц, контролирующих критически важную инфраструктуру;
- поддерживать интеграцию и координацию функций различных сторон, участвующих в обеспечении безопасности критически важной инфраструктуры.

Кроме этого, Законом предусмотрено создание Совета критической инфраструктуры, регламентированы функции Верховного комиссара полиции, который осуществляет общий контроль над исполнением Закона.

Совет критической инфраструктуры:

- рассматривает любое заявление об объявлении инфраструктуры критической и дает рекомендации по такому заявлению Министру полиции;
- утверждает руководящие принципы относительно: оценки заявления; внедрения системы отнесения критически важной инфраструктуры к категории низкого, среднего или высокого риска; политик, протоколов и стандартов по любым вопросам, необходимым для достижения целей Закона; содействия сотрудничеству государственного и частного секторов в вопросах защиты критически важной инфраструктуры;
- выполняет любые другие функции, которые могут быть возложены на Совет Министром полиции.

Верховный комиссар полиции должен:

- создавать и поддерживать административные системы и процедуры, необходимые для реализации и обеспечения соблюдения настоящего Закона;
- поддерживать Совет по критической инфраструктуре и Министра полиции в исполнении настоящего Закона;
- осуществлять сотрудничество между Полицейской службой Южной Африки, другими государственными органами и частным сектором в той мере, в какой это касается защиты критически важной инфраструктуры.

Функции Верховного комиссара полиции также заключаются в разработке единых стандартов, руководств и протоколов для утверждения Советом в отношении:

- способов, согласно которым:
- инфраструктура должна быть определена, классифицирована и объявлена критически важной;
- проводится любая оценка физической безопасности критической инфраструктуры и потенциальной критической инфраструктуры;
- информация, которая может иметь отношение к защите критически важной инфраструктуры, передается между соответствующими заинтересованными сторонами;
- функционируют и отчитываются любые релевантные комитеты или форумы;
- структур и механизмов, способствующих координации и обеспечению защиты критически важной инфраструктуры.

3.5. **Закон о киберпреступлениях** (2021)

Данный закон (Cybercrimes Act [35]) основан на более раннем законопроекте 2015 года, принят в 2020 году, и вступил в силу в 2021 году. Он призван:

- криминализировать правонарушения, имеющие отношение к киберпреступности;
- ввести уголовную ответственность за разглашение сообщений с вредоносным контентом и предусмотреть временные охранные приказы;
- развить регулирование юрисдикции в отношении киберпреступлений;
- развить регулирование полномочий по расследованию киберпреступлений;
- развить регулирование различных аспектов взаимной помощи в расследовании киберпреступлений;
- обеспечить создание должности назначенного контактного лица;
- обеспечить фиксацию доказательств определенных фактов посредством письменных показаний;
- установить обязательства сообщать о киберпреступлениях;
- обеспечить наращивание потенциала;
- предусмотреть возможность для исполнительной власти заключать соглашения с иностранными государствами для содействия мерам, направленным на обнаружение, предотвращение, смягчение последствий и расследование киберпреступлений.

4. Государственные органы, входящие в систему обеспечения информационной безопасности и форматы государственно-частного партнерства

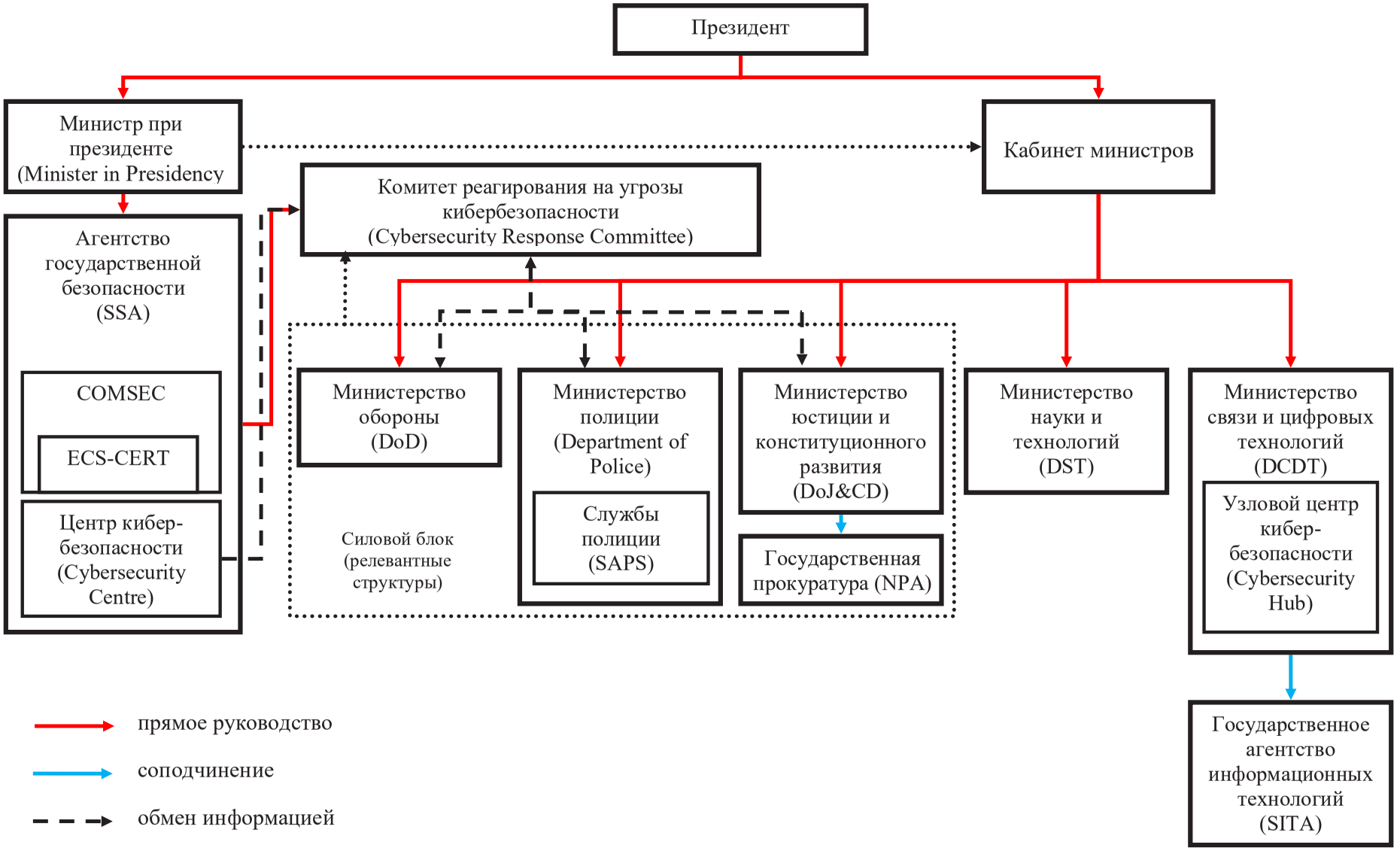
4.1. Агентство государственной безопасности (SSA)

Агентство государственной безопасности (State Security Agency) де-факто руководит обеспечением кибербезопасности, поскольку директор Агентства возглавляет Комитет реагирования на угрозы кибербезопасности (Cybersecurity Response Committee), который координирует деятельность в сфере кибербезопасности Силового блока органов юстиции, охраны правопорядка и обеспечения безопасности. Агентство также ответственно за разработку стратегии в области криптографии и стратегии защиты критической информационной инфраструктуры (КИИ). **Центр кибербезопасности** (Cybersecurity Centre) Агентства осуществляет операционную поддержку деятельности Комитета.

В рамках Агентства также функционирует структура радиоэлектронной разведки — **Национальный центр связи** (National Communication Centre). Его основными функциями являются:

- содействие оперативной координации действий по реагированию на инциденты кибербезопасности, касающиеся национальной разведки, национальной обороны и киберпреступности;

Рисунок 1. Структура управления информационной/ кибербезопасностью в ЮАР — основные элементы



- разработка мер для решения вопросов кибербезопасности, влияющих на национальную безопасность;
- содействие анализу инцидентов, тенденций, уязвимостей в области кибербезопасности, обмену информацией, обмену технологиями в области национальной безопасности и угроз для улучшения координации технического реагирования;
- руководство идентификацией, защитой и обеспечением безопасности национальной критической информационной инфраструктуры;
- обеспечение регулярной оценки и тестирования национальных критически важных информационных инфраструктур, включая оценку уязвимости, оценку угроз и рисков, а также тестирование на проникновение;
- обеспечение координации и руководства в отношении корпоративной безопасности и разработки политики; управления рисками и нормативно-правового соответствия; управления идентификацией и безопасностью; управления информацией о безопасности и событиями (SIEM) и цифровой криминалистики, касающейся вопросов кибербезопасности в государственных органах;
- разработка протоколов управления скоординированным реагированием на инциденты кибербезопасности и взаимодействия с различными заинтересованными сторонами;
- обеспечение проведения аудитов кибербезопасности, оценок и учений по обеспечению готовности, а также давать консультации по разработке национальных планов реагирования;
- осуществление функций Секретариата, необходимых для работы Комитета реагирования на угрозы кибербезопасности.

Государственно-частная компания COMSEC, являющаяся частью Агентства государственной безопасности, в первую очередь отвечает за защиту правительственной информации посредством обеспечения безопасности критически важной инфраструктуры и сетей электронных коммуникаций. В ее обязанности входит разработка, закупка, установка и обслуживание государственных систем электронной связи, в том числе, для Южно-Африканских национальных сил обороны; защита национальной критически важной инфраструктуры; предоставление криптографических услуг; а также проведение исследований, обучение и консультации по использованию ИТ-продуктов. COMSEC уполномочена обеспечивать безопасность государственных электронных услуг. Группа реагирования на инциденты компьютерной безопасности в информационной инфраструктуре государственных органов (ECS-CSIRT) фактически является частью компании.

4.2. **Комитет реагирования на угрозы кибербезопасности** (CRC)

Функционал Комитета (Cybersecurity Response Committee) включает:

- обеспечение достижения целей Рамочной национальной политики в области кибербезопасности;
- координацию деятельности в сфере кибербезопасности и осуществление функций центрального контактного пункта по всем вопросам кибербезопасности, имеющим отношение к национальной безопасности (национальная оборона, национальная разведка и киберпреступность);
- продвижение, определение направления и координация деятельности, направленной на улучшение мер кибербезопасности со стороны всех акторов, в том числе расширение сбора разведывательной информации и повышение потенциала государства по расследованию, судебному преследованию и борьбе с киберпреступностью, кибертерроризмом, кибершпионажем, кибервойной;
- любыми иными угрозами, связанными с кибербезопасностью;
- осуществление контроля и руководства работой Центра кибербезопасности, Cybersecurity Hub, Правительственной группы реагирования на инциденты компьютерной безопасности (ECS-CSIRT) и любым другим CSIRT, созданным в ЮАР;

Продвижение и руководство процессом разработки и реализации:

- плана защиты национальной критической информационной инфраструктуры;
- ситуационного анализа и кампании по повышению осведомленности о рисках безопасности киберпространства;
- культуры кибербезопасности и соблюдения минимальных стандартов безопасности;
- государственно-частных партнерств для национальных планов и планов действий в соответствии с Рамочной национальной политикой в области кибербезопасности;
- технических и эксплуатационных стандартов кибербезопасности;
- программ обучения, образования, исследований и разработок в области кибербезопасности, а также программ развития навыков;
- международного сотрудничества;
- содействия взаимодействию как на национальном, так и на международном уровне, в том числе посредством международного членства в таких организациях, как Форум групп реагирования на инциденты компьютерной безопасности (FIRST), и разработке руководящих принципов политики для информирования о таком взаимодействии;

- создания отраслевых, региональных и континентальных CSIRT; комплексной правовой базы, регулирующей киберпространство.

4.3. **Министерство связи и цифровых технологий** (DCDT)

Министерство связи и цифровых технологий (Department of Communications and Digital Technologies, DCDT) было сформировано в 2019 году в результате слияния Министерства связи и Министерства телекоммуникаций и почтовых услуг.

Основной мандат новой структуры — возглавлять цифровую трансформацию страны, что предполагает укрепление доверия и уверенности в безопасном использовании ИКТ. Министерство развивает политику, регуляторные нормы и отраслевые стандарты, обеспечивает взаимодействие с провайдерами и производителями в целях создания безопасности и доверия к использованию ИКТ. Оно также несет значительную ответственность за ряд аспектов национальной кибербезопасности. Главный директор DCDT по операциям в области кибербезопасности руководит национальной группой реагирования на инциденты компьютерной безопасности, также известной как **Cybersecurity Hub**. Основанная в 2015 году, группа взаимодействует с государственными ведомствами, частным сектором и гражданским обществом в целях выявления и противодействия киберугрозам, включая содействие созданию отраслевых CSIRT.

В структуре Министерства также действует **Национальный консультативный совет по кибербезопасности** (National Cyber security Advisory Council, NCAC), созданный для консультирования правительства по киберполитике и техническим вопросам. В состав Совета входят представители научных кругов и промышленности, юристы и исследователи.

4.4. **Государственное агентство информационных технологий** (SITA)

Роль Агентства (State Information Technology Agency, SITA) заключается в консолидации и координации информационных ресурсов государства для достижения экономии средств за счет масштабирования, увеличения возможностей доставки и улучшения функциональной совместимости. SITA стремится использовать информационные технологии в качестве стратегического ресурса для правительства, управляя процессом закупок и поставок ИТ, чтобы гарантировать, что правительство ЮАР получает лучшее соотношение цены и качества и повышенную производительность; качественные решения, услуги и продукты; и использует передовые ИТ-подходы при модернизации и предоставлении услуг всем гражданам. Агентство предлагает комплексные решения по всему спектру

ИТ-услуг многочисленным национальным, провинциальным и местным правительственным организациям. Министерство связи и цифровых технологий осуществляет контроль над деятельностью Агентства.

4.5. **Службы полиции** (SAPS)

Службы полиции (South Africa Police Services) находятся в подчинении Министерства полиции и занимаются предотвращением и борьбой с компьютерными преступлениями на основе положений Уголовного кодекса [36]. С этой целью наращиваются национальные возможности к расследованию компьютерных преступлений. Активно реализуются программы подготовки оперативных работников и следователей, в том числе при сотрудничестве с США.

SAPS разрабатываются методы противодействия массированным атакам по типу отказ в обслуживании, кражам персональных данных, распространению детской порнографии. Развивается сотрудничество с национальными и международными партнерами (ГПЭ ООН, МСЭ), трансграничное взаимодействие правоохранительных органов, партнерство с частным сектором.

4.6. **Министерство обороны** (DoD)

В рамках своих полномочий Министерство (Department of Defence) обеспечивает защиту собственных информационных систем и гражданских ведомств. В своем отчете за 2014–2015 годы, Министерство объявило о планах разработать в течение трех лет стратегию кибервойны и создать штаб киберкомандования. Однако нехватка финансирования, а также отсутствие навыков и опыта препятствовали достижению этих целей в установленные сроки. Стратегия находится в процессе утверждения ведомством, а киберкомандование еще не достигло полной оперативной готовности.

Что касается оборонных исследований и разработок, созданный в 1945 году Совет по научным и промышленным исследованиям (Council for Scientific and Industrial Research, CSIR) уполномочен разрабатывать стратегические технологии и возможности, в том числе для киберзащиты и безопасности. Он обеспечивает НИОКР и экспертные знания для Силового блока органов юстиции, охраны правопорядка и обеспечения безопасности.

4.7. **Министерство науки и технологий** (DST)

Министерство (Department of Science and Technology) отвечает за разработку, координацию и применение национальных программ развития, научных ис-

следований по кибербезопасности. Участвует в реализации Стратегии исследований, разработок и инноваций в области ИКТ Южной Африки.

4.8. Министерство юстиции и конституционного развития (DoJ&CD)

Роль Министерства юстиции (Department of Justice and Constitutional Development) в системе обеспечения информационной безопасности ЮАР заключается, прежде всего, в содействии разработке соответствующего законодательства. Кроме этого, соподчиненная Министерству Государственная прокуратура (National prosecuting authority) осуществляет судебное преследование противоправных действий в ИКТ-среде согласно соответствующему законодательству.

4.9. Государственно-частное партнерство в сфере реагирования на компьютерные инциденты

Рамочная национальная политика в области кибербезопасности реализует задачу формирования единой национальной системы групп реагирования на компьютерные инциденты с иерархической структурой. Четыре южноафриканских CERT участвуют в Глобальном форуме групп реагирования на инциденты и обеспечения безопасности (FIRST). Отраслевой CERT есть у Ассоциации Интернет-провайдеров [37], а Южноафриканская национальная исследовательская сеть создала группу реагирования на инциденты, связанные с компьютерной безопасностью. Кроме этого, с 2011 года ЮАР участвует в работе региональной группы реагирования AfricaCERT.

Как уже упоминалось, с целью защиты правительственного сектора в структуре Агентства государственной безопасности образован ECS-CSIRT. Координацию всех отраслевых CERT в ЮАР осуществляет Cybersecurity Hub, через него Министерство также контролирует создание и функционирование отраслевых групп CSIRT, определяя их роль и функции. Cybersecurity Hub поручено содействовать развитию государственно-частного партнерства, обмену информацией и технологиями, а также привлекать общественность к повышению осведомленности об угрозах безопасности. В апреле 2017 года он запустил форум для координации деятельности существующих и создаваемых отраслевых CERT.

Cybersecurity Hub имеет каналы связи и стандартные процедуры обмена информации с полицейскими службами и другими группами реагирования в критически важных секторах экономики (банковского сектора — SABRIC [38], телекоммуникационного сектора — ISPA[12], ITA [13] и др.).

12 Internet service Providers Association.
13 Information Technology Association.

5. Участие в международном сотрудничестве с ООН и другими международными и региональными организациями в области формирования системы международной информационной безопасности

Организация Объединенных Наций

Некоторые экспертные оценки приписывают ЮАР статус пассивного «колеблющегося государства» в вопросах глобального киберуправления [39]. Так, 2016 году она проголосовала против резолюции Совета ООН по правам человека «О поощрении, защите и осуществлении прав человека в Интернете», встав на сторону Китая, России и Саудовской Аравии [40]. Однако в 2018 году по аналогичной резолюции Южно-Африканская Республика проголосовала «за». В то же время очевидно, что по ряду вопросов страна выдвигает некоторые инициативы и не может считаться «пассивным» актором.

В июле 2019 года министр государственной безопасности ЮАР призвал ООН создать в киберпространстве «арбитражный орган для разрешения конфликтов, агрессии и злонамеренных обвинений, и предотвращения эскалации напряженности» [41].

ЮАР принимала участие в работе трех Групп правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности — в 2004–2005 годах, 2009–2010 годах и 2019–2021 годах. Будучи членом Группы правительственных экспертов ООН по продвижению ответственного поведения государств в киберпространстве в контексте международной безопасности, страна проголосовала в поддержку предложенной Россией Рабочей группы ООН открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (РГОС). ЮАР также внесла свой вклад в проект итогового отчета РГОС, подчеркнув важность преодоления цифрового и гендерного разрыва, а также участия всех заинтересованных сторон в сфере ИКТ [42].

Международное сотрудничество

В рамках Сообщества развития Юга Африки (САДК) ЮАР возглавила усилия по наращиванию потенциала безопасности и исследовательской деятельности через Кейптаунский университет, в котором находится Центр наращивания потенциала кибербезопасности для Южно-Африканской Республики. В марте 2022 года центр запустил первое исследование САДК по зрелости кибербезопасности, чтобы оценить готовность стран Сообщества реагировать на цифровые угрозы [43].

Страна была разработчиком Европейской конвенции по борьбе с киберпреступностью и подписала ее в 2001 году, но не ратифицировала. Кроме этого, ЮАР участвовала в работе над проектом «Конвенции Африканского союза по кибербезопасности и защите персональных данных» [44], который включает развитие национального уголовного законодательства по борьбе с киберпреступлениями и другими противоправными действиями с использованием ИКТ. Несмотря на то, что документ был принят в 2014 году, ЮАР подписала его только в феврале 2023 года, и по состоянию на начало 2024 года не ратифицировала [45].

В 2019 году создана Группа экспертов по кибербезопасности Африканского союза (African Union Cyber Security Expert Group, AUCSEG), которая осуществляет координацию экспертного сообщества и консультирует комиссию Африканского союза по всему спектру вопросов обеспечения информационной безопасности на континенте. Основной задачей AUCSEG является ускорение ратификации и имплементации в национальном праве Конвенции Африканского союза о кибербезопасности и защите персональных данных. Также предполагается, что группа должна исследовать и предложить комиссии обоснованную позицию по возможным последствиям для национальной безопасности африканских государств признания киберпространства пятым театром военных действий. В настоящее время только ЮАР имеет концепцию преобразований национальных вооруженных сил (Revolution in Military Affairs), предполагающую разработку новых доктрин, стратегий, тактик и технологий, которые будут необходимы в войне будущего.

Некоторая активность по тематике информационной и кибербезопасности наблюдается в рамках трехстороннего диалога Индия-Бразилия-ЮАР (IBSA). В частности, в итоговом документе Десятого заседания Трехсторонней министерской комиссии IBSA, в сентябре 2022 года, было подчеркнуто, что «международное сотрудничество поможет в формировании общего понимания ответственного поведения государств в киберпространстве и принесет пользу государствам в содействии экономическому росту и инновациям» [46]. Также зафиксировано установление сотрудничества IBSA в этой области.

Российская Федерация

В двустороннем формате в 2017 году ЮАР подписала Межправительственное соглашение с Россией о сотрудничестве в области обеспечения международной информационной безопасности. Помимо обязательств по совместному реагированию на киберугрозы и сотрудничеству в расследовании киберпреступлений, соглашение позволяет обеим странам координировать свои подходы к проблематике МИБ на международной арене, включая такие площадки, как ООН, БРИКС и Международный союз электросвязи [47]. Курс на дальнейшее развитие сотруд-

ничества в сфере информационной безопасности был зафиксирован в 2018 году в Совместном заявлении о стратегическом партнерстве Российской Федерации и Южно-Африканской Республики. Во-первых, стороны отметили необходимость укрепления многостороннего взаимодействия в сфере международной информационной безопасности. При этом стороны подчеркнули ключевое значение принципов международного права, в частности принципов неприменения силы или угрозы силой, суверенного равенства государств, невмешательства во внутренние дела государств, а также принципов политической независимости, территориальной неприкосновенности, уважения прав и основных свобод человека. Во-вторых, стороны отметили необходимость активизации международного сотрудничества в борьбе с использованием ИКТ в преступных целях и поддержали инициативу выработки под эгидой ООН обязательного для всех нормативно-правового документа по противодействию использованию ИКТ в преступных целях. В-третьих, стороны признали важность установления основы сотрудничества между странами-участницами БРИКС в сфере обеспечения безопасного использования ИКТ и в связи с этим договорились работать с целью подготовки межправительственного соглашения между странами БРИКС в этой сфере. Помимо этого, стороны выступили за усиление координации их приоритетов на международном уровне по вопросам глобального управления сетью Интернет в рамках ООН.

Иран

В 2017 году ЮАР было подписано двустороннее соглашение с Ираном об инвестициях в ИКТ, спутники, электронную коммерцию, кибербезопасность.

Франция

В 2017 году были подписаны Меморандум о взаимопонимании и совместное заявление с Францией, которое предполагает создание Специального следственного подразделения и сотрудничество в правоохранительной сфере.

Великобритания

В сентябре 2021 года ЮАР стала одним из организаторов первого двустороннего кибердиалога по ИКТ. Государства обменялись мнениями о киберпреступности, будущем процессов ООН, касающихся ответственного поведения государств в киберпространстве, а также усилиях по наращиванию киберпотенциала в ЮАР [48].

Нидерланды

В 2022 году Южно-Африканская Республика провела двусторонний кибердиалог с Нидерландами, в ходе которого две страны обсудили различные во-

просы, включая борьбу с киберпреступностью и продвижение международных норм [49].

6. Возможные приоритеты в сфере обеспечения информационной безопасности и международной информационной безопасности в рамках БРИКС

В сентябре 2016 года был принят План совместных действий стран БРИКС в области ИКТ [50]. В него входит обмен информацией и передовым опытом в борьбе с киберпреступностью, развитие сотрудничества между техническими и правоохранительными органами, совместные исследования и разработки в области кибербезопасности, а также наращивание потенциала. Это позволило ЮАР внести свой вклад в укрепление потенциала борьбы с киберугрозами и активно участвовать в учебных программах других стран БРИКС.

Южно-Африканская Республика является членом экспертной рабочей группы БРИКС, созданной в 2015 году для развития практического сотрудничества в области безопасности ИКТ и обмена информацией о политике и программах в области ИКТ. Группа подтвердила свою приверженность расширению обмена информацией о киберпреступности между техническими и правоохранительными органами, а также исследованиям в области кибербезопасности.

В 2018 году в Дурбане (ЮАР) состоялась встреча высоких представителей стран БРИКС, курирующих вопросы безопасности, на которой была достигнута договоренность о проведении единой политики в области международной информационной безопасности. Сообщалось, что участники встречи не только одобрили результаты деятельности Рабочей группы БРИКС по вопросам безопасности в сфере использования ИКТ, которой удалось выработать «дорожную карту» взаимодействия в этой сфере, но и признали необходимость подвести под это сотрудничество прочную международно-правовую базу и стремиться к выработке пятистороннего межправительственного соглашения о сотрудничестве в области обеспечения международной информационной безопасности [51]. В том же году это стремление было зафиксировано на заседании Совета министров иностранных дел БРИКС [52].

В 2023 году на мероприятии BRICS-Africa Outreach и диалоге с партнерами BRICS+ президент ЮАР Сирил Рамафоса высказал несколько тезисов, которые можно интерпретировать как приоритет для стран Африки и ЮАР: «Хотя во многих странах Глобального Юга наблюдается значительный прогресс в индустриализации, технологическом развитии, инновациях и цифровой экономике, они не в полной мере пользуются экономическими выгодами. Работая вместе, обмениваясь навыками и возможностями, мобилизуя ресурсы, мы сможем придать

новый импульс глобальному росту и устойчивому развитию. Нам необходимо выйти за рамки выражения солидарности и перейти к инклюзивности и взаимовыгодному экономическому сотрудничеству». Из этого можно сделать вывод, что от сотрудничества в рамках БРИКС, в том числе по линии международной информационной безопасности ЮАР ожидает практических результатов.

На полях Второго саммита Россия-Африка, который прошел 27–28 июля 2023 года в Санкт-Петербурге, советник по кибербезопасности президента ЮАР Джозеф Пу заявил, что страна намерена развивать с Россией сотрудничество в области кибербезопасности, а также предложил странам БРИКС поработать над совместными документами по кибербезопасности [53].

Можно утверждать, что ЮАР вносит стратегический вклад в сотрудничество БРИКС. Есть мнение, что в некоторых аспектах кибербезопасности она следует за странами объединения, а в других она если не лидирует, то стратегически может стать лидером [54].

7. Список использованной литературы

1. BDEX, https://bdex.ru/naselenie/south-africa/
2. The World Bank, https://data.worldbank.org/country/south-africa
3. ITU Data Hub, https://datahub.itu.int/data/?e=ZAF&c=701&i=11624
4. South Africa Connect: Creating Opportunities, Ensuring Inclusion. South Africa's Broadband Policy, 20 Nov. 2013, https://www.gov.za/sites/default/files/gcis_document/201409/37119gon953.pdf
5. Data Center Journal, https://www.datacenterjournal.com/data-centers/south-africa/
6. Network Readiness Index 2023 – South Africa // Portulans Institute, https://download.networkreadinessindex.org/reports/countries/2023/south-africa.pdf.
7. Worldwide Mobile Data Pricing 2022 // Cable.co.uk, 2022, https://www.cable.co.uk/mobiles/worldwide-data-pricing/.
8. National Development Plan 2030 // South African Government, 2012, https://www.gov.za/issues/national-development-plan-2030.
9. ICT and Digital Economic Masterplan for South Africa // Ellipsis, 31 August 2021, https://www.ellipsis.co.za/ict-and-digital-economic-masterplan-for-south-africa/.
10. Government AI Readiness Index 2022 // Oxford Insights, 2022, p. 8, https://static1.squarespace.com/static/58b2e92c1e5b6c828058484e/t/639b495cc6b59c620c3ecde5/1671121299433/Government_AI_Readiness_2022_FV.pdf
11. Report of the Presidential Commission on the Fourth Industrial Revolution // Presidency of the Republic of South Africa, August 2020, p. 180, https://www.ellipsis.co.za/wp-content/uploads/2020/10/201023-Report-of-the-Presidential-Commission-on-the-Fourth-Industrial-Revolution.pdf
12. South Africa Launches Artificial Intelligence Industry Association // Benjamindada.com, 18 July 2023, https://www.benjamindada.com/south-african-artificial-intelligence-association/
13. Global Cybersecurity Index 2020 // ITU, https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E
14. Insight into the cyber threat landscape in South Africa, May 27, 2020, https://www.accenture.com/za-en/insights/security/cyberthreat-south-africa
15. INTERPOL report identifies top cyberthreats in Africa, 21 October 2021, https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-identifies-top-cyberthreats-in-Africa
16. Denys Reva 'Cyber Attacks Expose the Vulnerability of South Africa's Ports' // Institute for Security Studies, 29 July 2021, https://issafrica.org/iss-today/cyber-attacks-expose-the-vulnerability-of-south-africas-ports
17. Luke Feltham 'Basic Web Lessons for South Africa: Government Hacks Point to Systematic Security Issues' // Mail & Guardian, 19 September 2021, https://mg.co.za/news/2021-09-19-basic-web-lessons-for-south-africa-government-hackspoint-to-systematic-security-issues/

18. Act No. 19 of 2020: Cybercrimes Act // Republic of South Africa Government Gazette, 1 June 2021, https://www.gov.za/sites/default/files/gcis_document/202106/44651gon324.pdf
19. Information and Communication Technology (ICT) Research and Development (R&D) and Innovation Strategy for South Africa, http://www.ist-africa.org/home/files/RSA_ICTResearchDevelopmentInnovationStrategy_Final.pdf
20. State Security Agency: National Cybersecurity Policy Framework (NCPF), 4 December 2015, https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf
21. National Development Plan 2030. Our Future-make it work, https://www.gov.za/sites/default/files/gcis_document/201409/ndp-2030-our-future-make-it-workr.pdf
22. South Africa Connect: Creating Opportunities, Ensuring Inclusion. South Africa's Broadband Policy, 20 Nov. 2013, https://www.gov.za/sites/default/files/gcis_document/201409/37119gon953.pdf
23. South African Defence Review 2015, https://static.pmg.org.za/170512review.pdf
24. National Integrated ICT Policy White Paper, 28 September 2016, https://www.dcdt.gov.za/documents/legislations/white-papers/file/109-the-national-integrated-ict-poli
25. National e-Government Strategy and Roadmap, https://www.gov.za/sites/default/files/gcis_document/201711/41241gen886.pdf
26. National Digital and Future Skills Strategy South Africa, https://www.gov.za/sites/default/files/gcis_document/202009/43730gen513.pdf
27. Digital-Economy-Masterplan, https://www.ellipsis.co.za/wp-content/uploads/2021/08/Digital-Economy-Masterplan-22-Feb-2021v1_updated.pdf
28. Electronic Communications and Transactions Act No 25 of 2002 // Republic of South Africa Government Gazette, https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf
29. Regulation of Interception of Communications and Provision of Communication-related information Act No 70 of 2002// Republic of South Africa Government Gazette, https://www.gov.za/documents/regulation-interception-communications-and-provision-communication-related-information--13
30. Protection of Personal Information Bill of 2010 (Acts, 2012) // Republic of South Africa Government Gazette, https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013popi.pdf
31. Act No. 8 of 2019: Critical Infrastructure Protection Act, 2019 // Republic of South Africa Government Gazette, https://www.gov.za/sites/default/files/gcis_document/201911/4286628-11act8of2019criticalinfraprotectact.pdf
32. Cybercrime.org.za, http://cybercrime.org.za/reporting
33. Electronic Communications and Transactions Act No 25 of 2002 // Republic of South Africa Government Gazette, https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf
34. Act No. 8 of 2019: Critical Infrastructure Protection Act, 2019 // Republic of South Africa Government Gazette, https://www.gov.za/sites/default/files/gcis_document/201911/4286628-11act8of2019criticalinfraprotectact.pdf
35. Act No. 19 of 2020: Cybercrimes Act, 2020 // Republic of South Africa Government Gazette, https://www.gov.za/sites/default/files/gcis_document/202106/44651gon324.pdf
36. Criminal Procedures Act 51, 1997
37. Republic of South Africa Department of Telecommunications and Postal Services, 'Cybersecurity Briefing to Portfolio Committee', PowerPoint presentation, slide 13, 22 August 2017, https://slideplayer.com/slide/12695097/
38. South African inter-Banking CSIRT, www.sabric.co.za
39. Cyber Capabilities and National Power. Volume 2, https://www.iiss.org/research-paper/2023/09/cyber-capabilities-national-power-volume-2/
40. The promotion, protection and enjoyment of human rights on the Internet, https://www.icnl.org/wp-content/uploads/A_HRC_RES_32_13.pdf
41. Minister Ayanda Dlodlo: State Security Agency Dept Budget Vote 2019/20 // South African Government, 18 July 2019, https://www.gov.za/speeches/minister-state-security-ms-ayanda-dlodlo-18-jul-2019-0000
42. Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security – Third Substantive Session // United Nations General Assembly, 25 March 2021, pp. 72–73, https://front.un-arm.org/wp-content/uploads/2021/04/AAC.290-2021-INF-2.pdf; и United Nations Office for Disarmament Affairs, 'Statement by South Africa statement 140 The International Institute for Strategic Studies at the Informal OEWG', 22 February 2021, https://front.un-arm.org/wp-content/uploads/2021/02/South-Africastatement-OEWG-Final.pdf
43. C3SA to Launch the First SADC Study on Cybersecurity Maturity // University of Cape Town, 22 March 2022, https://www.news.uct.ac.za/article/-2022-03-22-c3sa-to-launch-thefirst-sadc-study-on-cybersecurity-maturity

44. African Union Convention on Cyber Security and Personal Data Protection, https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf.
45. List of Countries which have Signed, Ratified/Acceded to The African Union Convention On Cyber Security and Personal Data Protection, 19.09.2023, https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION_0.pdf
46. INDIA-BRAZIL-SOUTH AFRICA DIALOGUE FORUM 10th IBSA Trilateral Ministerial Commission Meeting 21 September2022, https://www.gov.br/funag/en/content-centers/news/india-brazil-south-africa-dialogue-forum-10th-ibsa-trilateral-ministerial-commission-meeting-21-september2022
47. О подписании Соглашения между Правительством Российской Федерации и Правительством Южно-Африканской Республики о сотрудничестве в области обеспечения международной информационной безопасности // МИД России, 04.09.2017 https://www.mid.ru/en/foreign_policy/international_safety/1551693/?lang=ru
48. Republic of South Africa Department of International Relations and Cooperation, 'South Africa and the United Kingdom Co-hosted the Inaugural SA–UK Dialogue', 28 September 2021, https://www.dirco.gov.za/blog/2021/09/28/south-africa-and-the-united-kingdom-co-hosted-theinaugural-sa-uk-dialogue/
49. Joint Statement South Africa and the Netherlands: Cyber Policy Dialogue // Government of the Netherlands, 6 April 2022, https://www.government.nl/documents/diplomaticstatements/2022/04/06/south-africa-netherlands-cyber-policydialogue-joint-statement.
50. Принят план совместных действий стран БРИКС в области ИКТ // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации, 11.11.2016, https://digital.gov.ru/ru/events/36049
51. Страны БРИКС готовят соглашение в информационной безопасности // РИА Новости, 29.06.2018, https://ria.ru/20180629/1523671244.html?ysclid=ls06vvjw5z944943719
52. Лавров: страны БРИКС выступают за разработку совместного соглашения по кибербезопасности // Рамблер новости, 04.06.2018, https://news.rambler.ru/other/40018752
53. В ЮАР заявили о намерении развивать сотрудничество с РФ в кибербезопасности// Известия, 30.07.2023, https://iz.ru/1551729/2023-07-30/v-iuar-zaiavili-o-namerenii-razvivat-sotrudnichestvo-s-rf-v-kiberbezopasnosti
54. Positioning South Africa in the BRICS cybersecurity context: a strategic perspective // Mitrovic, Zoran&Thakur, Surendra (2019) p.8, https://www.researchgate.net/profile/Zoran-Mitrovic-5/publication/331438637_Positioning_South_Africa_in_the_BRICS_cybersecurity_context_a_strategic_perspective/links/5c865423458515831f9b5a02/Positioning-South-Africa-in-the-BRICS-cybersecurity-context-a-strategic-perspective.pdf?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19

4. Международная информационная безопасность в БРИКС: общее понимание и синергия усилий

На фоне существующих расхождений в подходах к решению многих вопросов информационной и кибер- безопасности и, одновременно, наличия запроса на преодоление новых вызовов и угроз при использовании и развитии ИКТ-средств, новую актуальность приобретает взаимодействие на региональном и межрегиональном уровне. Объединение БРИКС обладает значительным потенциалом эффективного решения многих проблем от пандемии до финансовых кризисов, и повестка международной информационной безопасности не является исключением.

История обсуждения тематики международной информационной безопасности (МИБ) в БРИКС насчитывает не один год. Впервые она была затронута в итоговом документе III саммита БРИКС, где страны выразили «приверженность сотрудничеству в укреплении международной информационной безопасности», а также высказали намерение уделить «особое внимание борьбе с киберпреступностью»[1]. По итогам V саммита БРИКС страны-участники объединения отметили, среди прочего, «исключительно важную позитивную роль, которую играет Интернет в мире в плане содействия экономическому, социальному и культурному развитию», а также подчеркнули, что «безопасность при использовании информационных и коммуникационных технологий с применением универсально признанных норм, стандартов и практик имеет первостепенную важность»[2].

На рубеже 2013–2014 гг. произошел качественный скачок в обсуждении тематики МИБ в БРИКС, и итоговые декларации объединения стали гораздо более субстантивными на этом направлении. Стоит вспомнить, что именно летом 2013 года в публичном дискурсе стали доступны секретные материалы о тотальной слежке спецслужб США с использованием ИКТ, раскрытые Эдвардом Сноуденом — бывшим сотрудником американской разведки. Эта информация подтвердила точку зрения, что США используют свое технологическое доминирование и глобальную сеть Интернет для продвижения собственных национальных интересов, не считаясь с интересами других государств, даже собственных союзников. В итоговой декларации VI саммита БРИКС страны решительно осудили «акты массовой электронной слежки и сбора данных о частных лицах по всему миру, а также нарушение суверенитета государств и прав человека,

1 Пункт 11 Саньянской декларации III саммита БРИК (г. Санья, о. Хайнань, КНР, 14 апреля 2011 года) // Саммиты и документы, НКИ БРИКС Россия, https://nkibrics.ru/pages/summit-docs.

2 Пункт 34 Этеквинской декларации V саммита БРИКС (г. Дурбан, ЮАР, 27 марта 2013 года) // Саммиты и документы, НКИ БРИКС Россия, https://nkibrics.ru/pages/summit-docs.

и права на неприкосновенность частной жизни»[3]. Принципиально важной стала выработка общего видения стран БРИКС по вопросам развития ИКТ и обеспечения безопасности ИКТ-среды. В Декларации VI Саммита было отмечено, что, во-первых, ИКТ «должны служить инструментом поощрения устойчивого экономического прогресса и социальной интеграции». Во-вторых, «использование и развитие ИКТ на основе международного сотрудничества и общепризнанных норм и принципов международного права имеют первостепенное значение для обеспечения мирного, безопасного и открытого цифрового и Интернет-пространства». В-третьих, «необходимо сохранять ИКТ, и, в частности, Интернет, как инструмент мира и развития и не допускать их использования в качестве оружия». Кроме того, в практическом плане страны обязались «сотрудничать друг с другом в выявлении возможностей для осуществления совместных действий по решению общих проблем безопасности в сфере использования ИКТ»[4]. Также было заявлено о создании группы экспертов стран БРИКС, которая будет заниматься выработкой практических предложений, касающиеся основных областей сотрудничества, и будет координировать позиции на международных форумах. Направления работы группы более подробно раскрыты в итоговой декларации VII Саммита БРИКС: «обмен информацией и передовой практикой в вопросах безопасности в сфере использования ИКТ; эффективная координация мер противодействия киберпреступности; выделение уполномоченных по связям в государствах-участниках; сотрудничество между странами БРИКС с использованием существующих групп реагирования на компьютерные инциденты в области информационной безопасности (CSIRT); совместные проекты в области НИОКР; укрепление потенциала; а также разработка международных норм, принципов и стандартов»[5]. С учетом осуществлявшихся в тот момент активных попыток интернационализации управления Интернетом, этим вопросам также было уделено особое внимание, и выработано общее понимание, что «Интернет является международным ресурсом и что государства должны в равной степени участвовать в его развитии и функционировании, принимая во внимание необходимость привлечения соответствующих заинтересованных сторон в определенном качестве и с определенными обязательствами». Страны БРИКС поддержали «развитие механизма управления Интернетом… на основе открытого и демократического процесса, не подверженного влиянию решений, принятых в одностороннем порядке»[6].

---

3 Пункт 49 Форталезской декларации VI саммита БРИКС (г.Форталеза, Бразилия, 15 июля 2014 года) // Саммиты и документы, НКИ БРИКС Россия, https://nkibrics.ru/pages/summit-docs.
4 Там же, пп. 49, 50.
5 Пункт 34 Уфимской декларации VII саммита БРИКС (г. Уфа, Российская Федерация, 9 июля 2015 года) // Саммиты и документы, НКИ БРИКС Россия , https://nkibrics.ru/pages/summit-docs.
6 Там же, п 33.

Активными действиями против ИГИЛ[7] как на земле, так и в информационном пространстве ознаменовался 2016 год. Декларация VIII саммита БРИКС («Декларация Гоа») призвала все страны придерживаться всеобъемлющего подхода в борьбе с терроризмом, который должен включать «противодействие злоупотреблению террористическими структурами Интернетом, включая социальные сети, используя последние разработки в области ИКТ»[8].

С 2017 года наметились значимые подвижки в плане развития практического сотрудничества. Так, в итоговой Декларации IX саммита БРИКС был отмечен прогресс, достигнутый Рабочей группой экспертов государств БРИКС по вопросам безопасности в сфере использования ИКТ; принято решение «развивать сотрудничество в соответствии с Дорожной картой практического сотрудничества БРИКС в обеспечении безопасности в сфере использования ИКТ и любыми другими согласованными механизмами»; подтверждено, что страны БРИКС «продолжат совместную работу при помощи существующего механизма в целях обеспечения безопасного, открытого, мирного и совместного использования ИКТ на основе равноправного участия международного сообщества в управлении им», а также отмечена инициатива Российской Федерации «о межправительственном соглашении БРИКС по сотрудничеству в вопросах безопасности в сфере использования ИКТ»[9].

В Йоханнесбургской декларации X саммита БРИКС была подтверждена «важность разработки под эгидой ООН правил, норм и принципов ответственного поведения государств в информационном пространстве для обеспечения безопасности в сфере использования ИКТ»; подтверждена «важность международного сотрудничества в борьбе с использованием ИКТ в террористических и преступных целях» и «необходимость выработки под эгидой ООН универсального, юридически обязывающего нормативно-правового документа по противодействию использованию ИКТ в преступных целях»; признана «значимость создания правовых рамок для сотрудничества между участниками БРИКС в области обеспечения безопасности в сфере использования ИКТ». В этой связи государства объединения договорились продолжить работу по рассмотрению и разработке соответствующего межправительственного соглашения[10].

В Московской Декларации XII саммита БРИКС[11] (состоялся в режиме видеоконференции) вновь содержались решения, способствующие укреплению

---

7 Прежнее название «Исламского государства», террористической группировки, запрещённой в России.

8 Пункт 59 Декларации Гоа VIII саммита БРИКС (Гоа, Индия 16 октября 2016 года) // Саммиты и документы, НКИ БРИКС Россия, https://nkibrics.ru/pages/summit-docs.

9 Пункты 54, 55 Саньянской декларации III саммита БРИК (г. Санья, о. Хайнань, КНР, 14 апреля 2011 года) // Саммиты и документы, НКИ БРИКС Россия, https://nkibrics.ru/pages/summit-docs.

10 Пункты 37, 38 Йоханнесбургской декларации X саммита БРИКС (г. Йоханнесбург, ЮАР, 26 июля 2018 года) // Саммиты и документы, НКИ БРИКС Россия, https://nkibrics.ru/pages/summit-docs.

11 Пункт 40 Московской декларации XII саммита БРИКС (г. Москва, Россия, 17 ноября 2020 года) // Саммиты и документы, НКИ БРИКС Россия, https://nkibrics.ru/pages/summit-docs.

МИБ. В Декларации акцентирована необходимость всеобъемлющего и сбалансированного подхода к развитию и обеспечению безопасности в сфере использования ИКТ, в том числе в контексте технического прогресса и развития бизнеса, обеспечения безопасности государств и защиты их интересов, а также уважения права на неприкосновенность частной жизни; была подчеркнута ведущая роль ООН в развитии диалога — без ущерба для деятельности других международных площадок — по достижению общего понимания в отношении безопасности ИКТ и их использования и разработки под эгидой ООН общепризнанных норм, правил и принципов ответственного поведения государств в сфере использования ИКТ; особо была отмечена важность международного права и принципов, применяемых в данной сфере, и приветствовалась деятельность Рабочей группы ООН открытого состава и Группы правительственных экспертов (ГПЭ) ООН по международной информационной безопасности. В Московской Декларации была также подчеркнута «важность формирования нормативно-правовой базы для сотрудничества стран БРИКС в обеспечении безопасности в сфере использования ИКТ» и отмечены усилия Рабочей группы экспертов (РГЭ) БРИКС по вопросам безопасности в сфере использования ИКТ»[12]. Также приветствовалось «создание центральными банками стран БРИКС специального Канала по информационной безопасности для осуществления обмена данными и опытом государств объединения в области противодействия киберугрозам в финансовой сфере»[13].

В Декларации XIII саммита БРИКС в Нью-Дели[14] вновь было подтверждена приверженность созданию открытой, безопасной, стабильной, доступной и мирной среды для использования ИКТ; отмечена необходимость всеобъемлющего и сбалансированного подхода к развитию и обеспечению безопасности в сфере использования ИКТ, в том числе в контексте технического прогресса и развития бизнеса, обеспечения безопасности государств и защиты их интересов, а также уважения права на неприкосновенность частной жизни; подчеркнута ведущая роль ООН в развитии диалога — без ущерба для деятельности других профильных международных площадок — по достижению общего понимания в отношении безопасности ИКТ и их использования и разработки под эгидой ООН общепризнанных норм, правил и принципов ответственного поведения государств в сфере использования ИКТ. В Декларации приветствовалось успешное завершение работы Рабочей группы ООН открытого состава (РГОС) и Группы правительственных экспертов (ГПЭ) по международной информационной безопасности, а также запуск новой РГОС по вопросам безопасности в сфере использования ИКТ

12 Там же.

13 Там же, п. 63.

14 Декларация XIII саммита БРИКС — Нью-Дели (г. Нью-Дели, Индия, 9 сентября 2021 года) // Саммиты и документы, НКИ БРИКС Россия, https://nkibrics.ru/pages/summit-docs.

и самих ИКТ 2021–2025. Среди прочего, в этом документе отмечена публикация «Электронного справочника регуляторных актов стран БРИКС в сфере информационной безопасности и Сборника лучших практик по надзору и контролю за рисками информационной безопасности, рассматривая их в качестве комплексных документов, содержащих правила и передовые практики, используемые в рамках специального Канала БРИКС по информационной безопасности»[15].

Сегодня проблематика МИБ неизменно стоит в повестке дня заседаний с участием глав государств-участников БРИКС и регулярно находит отражение в итоговых документах саммитов объединения. Также успешно продолжается формирование общих позиций и по новым вопросам, связанным с использованием ИКТ. Так, XIV Саммит БРИКС (Пекин, КНР, 23–24 июня 2022 г.) сформировал позицию по вопросам, связанным с искусственным интеллектом (ИИ). В Пекинской декларации было отмечено, что «прорывы в применении цифровых технологий таких как, например, большие данные и искусственный интеллект, могут играть важную роль в обеспечении устойчивого развития»[16]. В декларации подчеркнута «необходимость сотрудничества в интересах укрепления доверия и безопасности, а также прозрачности и подотчетности в развитии надежного ИИ, чтобы максимально использовать его потенциал во благо общества и человечества в целом, с особым акцентом на маргинализированные и уязвимые группы населения»[17]. Отмечено, что нужно работать над устранением озабоченностей, связанных с рисками и этическими дилеммами, «обмениваться передовым опытом, проводить сравнительные исследования по этому вопросу для разработки общего подхода к управлению, которое будет служить руководством для стран БРИКС в отношении этического и ответственного использования искусственного интеллекта, способствуя развитию технологий ИИ»[18].

В 2023 году на XV саммите БРИКС в Йоханнесбурге председатель КНР Си Цзиньпин заявил, что «искусственный интеллект — это новая область человеческого развития, которая может принести большие возможности, но и риски и вызовы»[19]. Он также сказал, что необходимо «продолжить расширять сотрудничество в области искусственного интеллекта, усилить обмен информацией и техническое сотрудничество, совместно работать по предотвращению рисков, на основе широкого консенсуса сформировать структуру управления искусственным интеллектом и стандартов»[20].

---

15 Там же, п. 60.

16 Пункт 57 Пекинской Декларации XIV саммита БРИКС (г. Пекин, Китай, 23 июня 2022 года) // Саммиты и документы, НКИ БРИКС Россия, https://nkibrics.ru/pages/summit-docs.

17 Там же.

18 Там же.

19 Си Цзиньпин призвал БРИКС сформировать общую структуру управления ИИ // РИА Новости, 23 августа 2023 года, https://ria.ru/20230823/tszinpin-1891759909.html.

20 Там же.

В декларации XV саммита БРИКС[21] вновь была подтверждена приверженность созданию открытой, безопасной, стабильной, доступной и мирной среды, подчеркнута важность достижения общего понимания и активизации сотрудничества в использовании ИКТ и Интернета. Саммит поддержал ведущую роль ООН в развитии конструктивного диалога по теме обеспечения безопасности ИКТ, в том числе в рамках Рабочей группы ООН открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ в 2021–2025 гг., а также разработке общепризнанных нормативно-правовых рамок в этой области. Положения Декларации подтверждают последовательность БРИКС в стремлении к всеобъемлющему, сбалансированному и объективному подходу к разработке и обеспечению безопасности продуктов и систем ИКТ. XV Саммит вновь обозначил необходимость развития практического сотрудничества в рамках БРИКС посредством осуществления «дорожной карты» практического сотрудничества БРИКС в обеспечении безопасности в сфере использования ИКТ и в рамках деятельности Рабочей группы БРИКС по вопросам безопасности в сфере использования ИКТ»[22].

Положения Декларации XV саммита БРИКС в части, касающейся использования ИКТ, как и декларации предыдущих саммитов БРИКС, показывают общность подходов государств-участников объединения к выбору механизмов и средств противодействия глобальным вызовам и угрозам, возникающих при использовании ИКТ, обеспечению безопасности и стабильности глобальной цифровой среды, и это способствует формированию и укреплению системы МИБ.

***

Мир стоит на пороге перемен, и выработка общей позиции на основе инклюзивности, уважения суверенитета и национальных особенностей государств очень важна. Чем более четко и осмысленно будет звучать позиция БРИКС по актуальным вопросам международной повестки — как альтернатива гегемонии, тем большее число стран присоединятся к ней.

БРИКС — это больше, чем простая сумма частей. Синергия научно-образовательного, финансового и промышленного потенциала стран-участников при сохранении общих подходов может в значительной степени стать драйвером преодоления существующих и новых вызовов МИБ: от проблем цифрового разрыва, достижения и поддержания технологического суверенитета до рисков, сопровождающих внедрение передовых технологий, прежде всего искусственного интеллекта.

---

21 Йоханнесбургская декларация-II XV саммита БРИКС (г. Сэндтон, ЮАР, 23 августа 2023 года) // http://static.kremlin.ru/media/events/files/ru/ls471x8ogLBhjRQx05ufVB2uzMFo1kWs.pdf.

22 Там же, п. 24.

5. О некоторых аспектах председательства России в БРИКС в контексте обеспечения безопасности использования информационно-коммуникационных технологий

Межгосударственное объединение Бразилии, России, Индии, Китая и ЮАР (БРИКС), созданное по инициативе российского руководства, выдвинутой в 2006 году[1], стало влиятельным фактором мировой политики и драйвером развития экономики, одновременно олицетворяя набирающую силу тенденцию к формированию полицентричного мира. Вектор на всемерное укрепление БРИКС, заложенный в Концепции внешней политики Российской Федерации и в концепции участия нашей страны в данном объединении, определен одним из приоритетов внешней политики России.

Целью Российской Федерации в БРИКС и, соответственно, генеральной задачей председательства в объединении является постепенная, последовательная и устойчивая трансформация БРИКС в полноформатный механизм стратегического, оперативного и текущего взаимодействия в области политики и безопасности, экономики и финансов, культуры и гуманитарных связей.

Основные способы достижения данной цели — последовательное расширение спектра направлений сотрудничества, всё более активное продвижение общих интересов стран БРИКС на региональном уровне и международной арене, создание разветвленной системы механизмов взаимодействия и их институционализации, в первую очередь в финансово-экономической сфере. Другим важным направлением развития сотрудничества в рамках объединения становится **область обеспечения безопасности в сфере использования ИКТ**.

Всё это призвано вывести БРИКС на уровень важнейшего элемента системы глобального управления XXI века.

1. Основные итоги председательства России в межгосударственном объединении в 2009, 2015 и 2020 годах

На первом саммите глав государств и правительств БРИК (Екатеринбург, Россия, 16 июня 2009 г.) особое внимание было уделено вопросам глобального экономического кризиса, продовольственной безопасности, стратегиям развития и дальнейшему усилению стран БРИК, а также реформированию ООН.

1 Инициатива высказана в рамках Петербургского международного экономического форума (ПМЭФ) с участием министров экономики Бразилии, России, Индии, Китая. 12 ноября 2010 г. на саммите G20 в Сеуле ЮАР выразила желание присоединиться к БРИК.

Подписано два документа: Совместное заявление лидеров стран БРИК, а также Совместное заявление стран БРИК по глобальной продовольственной безопасности.

В 2011 году Фондом «Русский мир» совместно с РАН при поддержке МИДа России был создан «Национальный комитет по исследованию БРИКС» с целью организации и проведения исследований о роли и месте стран БРИКС и других «восходящих держав» в мировой политике и экономике. Деятельность НКИ БРИКС способствовала формированию единого информационного поля в области отечественных исследований БРИКС и продвижению российской позиции и экспертных оценок на международной арене; координации деятельности ведущих научно-исследовательских организаций и экспертов в интересах межгосударственного объединения, уделяя внимание проблемам информационной безопасности.

В 2012 году на базе Факультета государственного управления МГУ имени М.В. Ломоносова создается Межфакультетский координационный совет МГУ по исследованию проблем БРИКС. Целями деятельности Совета определяются научно-исследовательская и просветительская работа, посвященная изучению проблем стран-участниц БРИКС. К важным аспектам деятельности Совета отнесено объединение российских экспертов, привлечение к работе молодых специалистов, содействие их творческой и научной деятельности, активное взаимодействие с профильными ВУЗами, выстраивание партнерских отношений с университетскими структурами стран БРИКС.

Ключевым событием Председательства России в БРИКС (апрель 2015 г. – февраль 2016 г.) стал **VII саммит** в г. Уфе 8–9 июля 2015 г. под девизом «Партнерство стран БРИКС — мощный фактор глобального развития». Были приняты Уфимская декларация, Уфимский план действий и Стратегия экономического партнерства БРИКС, определившие основные задачи и направления дальнейшего развития БРИКС. Главы профильных ведомств пяти стран подписали Соглашение о сотрудничестве в сфере культуры и Меморандум о взаимопонимании о создании совместного интернет-сайта БРИКС. Российская сторона инициировала подготовку Дорожной карты торгово-экономического и инвестиционного сотрудничества на период до 2020 года.

В ходе саммита обсуждено создание «Банка развития БРИКС», ратификацию соглашения о котором в марте 2015 года утвердил Президент Российской Федерации.

Важными достижениями стал фактический запуск Нового банка развития и Пула условных валютных резервов.

Созданы постоянно действующие Рабочие группы по вопросам безопасности в сфере использования ИКТ, в антикоррупционной сфере, в области борьбы с наркотиками.

В ходе заседания Рабочей группы по вопросам безопасности в сфере использования ИКТ участники обменялись мнениями по проблематике международной информационной безопасности (МИБ) и обсудили вопросы эффективного взаимодействия в области противодействия преступности и терроризму в информационном пространстве. Подчеркнули важность совместных усилий и ключевую роль ООН в сфере выработки универсальных правил, норм, принципов поведения государств в информационном пространстве. Делегации договорились разработать план действий в целях укрепления практического сотрудничества. Российская сторона представила проект межправительственного соглашения БРИКС о сотрудничестве в области обеспечения безопасности в сфере использования ИКТ.

В БРИКС сформировался эффективно действующий механизм диалога на уровне высоких представителей государств-участников по вопросам национальной безопасности. В период российского председательства также решалась задача выведения БРИКС на позиции коллективного лидера в мировом сообществе в вопросах укрепления международной информационной безопасности, интернационализации управления сетью Интернет и выработки правил ответственного поведения государств в информационном пространстве. Тематика МИБ являлась одним из ключевых элементов российского председательства. Прилагались усилия по переводу взаимодействия стран БРИКС в данной области в практическую плоскость с подведением под него правовой базы в форме межправительственного соглашения государств БРИКС о сотрудничестве в сфере МИБ. Реализация данной задачи предусматривалась в рамках деятельности Рабочей группы экспертов БРИКС по безопасности в сфере использования ИКТ.

Открыто принципиально новое для БРИКС направление сотрудничества — в миграционной сфере с акцентом на использование возможностей современных информационно-коммуникационных технологий.

Российское председательство способствовало укреплению позиций нашей страны в БРИКС, развитию межцивилизационного диалога, продвижению общих ценностей стран БРИКС на мировой арене. Использована возможность сотрудничества в данной сфере для усиления позиций российской культуры и русского языка в крупнейших странах мира, каковыми являются участники БРИКС. Кроме того, вовлечение в деятельность БРИКС политических сил и организаций гражданского общества стран-участниц увеличило внутреннюю базу поддержки этого межгосударственного объединения.

В период председательства России в БРИКС реализованы меры, направленные на качественное улучшение распространения информации с использованием возможностей ИКТ о деятельности этой структуры в странах БРИКС и в международном сообществе.

По инициативе стран-участниц объединения БРИКС в 2017 году в России была создана международная сеть TV BRICS.

Введено в регулярную практику «на полях» встреч лидеров и министров государств БРИКС проведение мероприятий в формате «аутрич» с участием руководителей крупных развивающихся стран, международных и региональных организаций за счет использования возможностей современных ИКТ.

Таким образом, проведенные в этот период мероприятия позволили странам БРИКС сделать большой шаг вперед по пути интенсификации, диверсификации и институционализации их сотрудничества. БРИКС упрочил свои позиции в мире в качестве влиятельного фактора международной жизни, эффективного механизма согласования позиций пяти стран по актуальным вызовам современности. В объединении получила дальнейшее совершенствование разветвленная система механизмов сотрудничества, призванных на практике работать на повышение стабильности и надежности мировой финансовой системы, укрепление торгово-экономического и инвестиционного сотрудничества между странами БРИКС и с другими странами. Венцом совместных усилий в этой сфере стал старт операционной деятельности финансовых институтов БРИКС. Совместными усилиями пяти стран был придан импульс отладке механизмов «мягкой силы» в рамках объединения.

По итогам **XII саммита** глав-государств БРИКС под девизом «Партнерство БРИКС в интересах глобальной стабильности, общей безопасности и инновационного роста»), состоявшегося 17 ноября 2020 г.[2] в Москве, были обозначены общие позиции по укреплению архитектуры контроля над вооружениями, ситуации на Ближнем Востоке и в районе Персидского Залива, конфликту в Нагорном Карабахе и многим другим ключевым сюжетам мировой политики.

В результате саммита были приняты три документа: Стратегия экономического партнерства БРИКС до 2025 года, Антитеррористическая стратегия БРИКС и Московская декларация.

В Московской декларации отмечается необходимость всеобъемлющего и сбалансированного подхода к развитию и обеспечению безопасности в сфере использования ИКТ, в том числе в контексте технического прогресса и развития бизнеса, обеспечения безопасности государств и защиты их интересов, а также уважения права на неприкосновенность частной жизни. Подчеркивается ведущая роль Организации Объединенных Наций в развитии диалога — без ущерба для деятельности других международных площадок — по достижению общего понимания в отношении безопасности ИКТ и их использования и разработки под эгидой ООН общепризнанных норм, правил и принципов ответственного

2 Саммит ранее был запланирован на 21–23 июля, в мае из-за пандемии коронавируса мероприятие было перенесено и проведено в формате видеоконференции 17 ноября 2020 г.

поведения государств в сфере использования ИКТ. Особо отмечается важность международного права и принципов, применяемых в данной сфере. В этой связи приветствуется деятельность Рабочей группы ООН открытого состава и Группы правительственных экспертов и отмечается прогресс в обсуждениях. Подчеркивается также важность формирования нормативно-правовой базы для сотрудничества стран БРИКС в обеспечении безопасности в сфере использования ИКТ.

Отмечаются усилия Рабочей группы экспертов БРИКС по вопросам безопасности в сфере использования ИКТ и приветствуется работа по рассмотрению и подготовке соответствующих предложений, в том числе о разработке межправительственного соглашения БРИКС о сотрудничестве в области обеспечения безопасности в сфере использования ИКТ и двусторонних соглашений между странами объединения.

Заявляется о важности расширения сотрудничества в рамках «пятерки», в том числе посредством рассмотрения соответствующих инициатив и реализации Дорожной карты практического сотрудничества стран БРИКС в обеспечении безопасности в сфере использования ИКТ.

Справочно. «Дорожная карта» включает следующие области сотрудничества:

- *активизацию обмена подходами к политическим вопросам безопасности в сфере использования ИКТ (оценка событий на международной арене; развитие диалога о нормах, принципах и правилах, обеспечивающих открытую, безопасную, стабильную, доступную и мирную ИКТ-среду в рамках ООН; выработка общей позиции государств-участников БРИКС по ключевым вопросам проблематики; координация позиций на различных международных площадках);*
- *создание сети сотрудничества между национальными центрами (группами) реагирования на компьютерные инциденты (экстренной готовности к компьютерным инцидентам);*
- *углубление практического сотрудничества между уполномоченными ведомствами, отвечающими за безопасность в сфере использования ИКТ;*
- *проведение совместных исследований и разработок;*
- *создание механизма научного и исследовательского обмена между государствами БРИКС.*

Подчеркивая колоссальный потенциал цифровой революции для роста и развития, признается проблема, связанных с ней новых возможностей для преступных действий и угроз. Выражается обеспокоенность в связи с увеличением числа и растущей сложностью случаев использования ИКТ в преступных целях, а также отсутствием многосторонней базы для противодействия использованию ИКТ в преступных целях.

Признается также, что для противодействия новым вызовам и угрозам в данной сфере необходимо сотрудничество и обсуждение на международном уровне возможностей формирования нормативно-правовых основ, включая потребность в разработке под эгидой ООН всеобъемлющей международной конвенции по борьбе с использованием ИКТ в преступных целях, и отмечается учреждение специального Межправительственного комитета экспертов открытого состава под эгидой ООН в соответствии с резолюцией ГА ООН 74/247 от 27 декабря 2019 года.

Выражается беспокойство все более острой проблемой защиты детей от сексуальной эксплуатации в интернете и другого онлайн-контента, вредного для их здоровья и развития, что обуславливает необходимость укрепления сотрудничества между странами БРИКС в области разработки инициатив по обеспечению безопасности детей в Интернете.

Московская декларация XII саммита БРИКС закрепила создание Канала по информационной безопасности для сотрудничества стран БРИКС в области борьбы с киберугрозами в финансовой сфере.

Пандемия коронавируса и переход в онлайн привели к резкой активности киберпреступников, что определило приоритетным направлением проблематику кибербезопасности. В 2020 году прошел II Международный онлайн-тренинг Cyber Polygon 2020 — проект Центра кибербезопасности Всемирного экономического форума, Группы Сбербанка и компании BI.ZONE при поддержке Интерпола. Представители 120 крупнейших российских и международных организаций из 29 стран отработали действия при таргетированной атаке, нацеленной на кражу конфиденциальных данных и нанесение репутационного ущерба компании. Более пяти миллионов людей из 57 стран смотрели трансляцию форума.

Россия, несмотря на непростую ситуацию в мире, не отказалась от запланированных мероприятий и была вынуждена создавать новые форматы их проведения. При подведении итогов председательства России в 2020 году лидеры стран БРИКС отметили первый в истории БРИКС виртуальный саммит, который позволил сделать более доступной информацию о всех принимаемых решениях.

Среди значимых итогов председательства России в БРИКС в 2020 году следует отметить следующие: приняты Договоренности БРИКС по содействию инвестициям, Руководящие принципы по содействию эффективному участию малогго бизнеса в международной торговле, Дорожная карта энергетического сотрудничества стран БРИКС. Значимым событием российского председательства в части укрепления Нового банка развития БРИКС, как нового неподконтрольного США института международного развития, стало открытие Евразийского регионального центра Нового банка развития (НБР) в Москве. В рамках председательства России в БРИКС 16 ноября 2020 г. принят Меморандум, ко-

торый закрепляет правила и принципы финансирования институтов развития, а также механизмы межбанковского сотрудничества.

В 2020 году НБР были одобрены четыре кредитные программы для Бразилии, Индии, Китая и Южной Африки для ликвидации экономических последствий, связанных с пандемией. Всего НБР выделил на борьбу с пандемией 10 миллиардов долларов. России в сентябре 2020 года также было выделены три кредита: один — Черноморскому банку торговли и развития на развитие российской портовой транспортной инфраструктуры обновления флота, наращивание объемов торговли и пассажиропотока; два других — Евразийскому банку развития на строительство платных дорог и на программу модернизации водоснабжения и водоочистки. Также два кредита были выделены Индии.

В сфере политики и безопасности Россия выступила с позиций необходимости ведения дипломатических переговоров и решения спорных вопросов только мирными средствами, с учетом международной практики и международного права, «без войн и санкций». Страны БРИКС выступили единым фронтом по многим вопросам международной безопасности, включая конфликты в Сирии, Афганистане, Ливии, Нагорном Карабахе и др. Общая позиция просматривается и по таким вопросам, как контроль над вооружениями, милитаризация космоса (где актуализируется «срочная необходимость согласования юридически обязывающего многостороннего инструмента», который запрещал бы размещать оружие в космическом пространстве), биологическое оружие, использование ИКТ в военных интересах.

Особое значение имеет принятие Антитеррористической стратегии БРИКС в целях укрепления сотрудничества в сфере предотвращения угрозы терроризма и разработки методов борьбы с ней. Страны БРИКС еще раз указали на недопустимость использования террористических группировок, а также проблематики противодействия международному терроризму и экстремизму для достижения политических целей; отказ от двойных стандартов в противодействии терроризму и экстремизму. Определено, что представители стран объединения, курирующие вопросы безопасности, должны регулярно отчитываться перед главами стран БРИКС о ходе выполнения данной Стратегии, включая разработку плана действий БРИКС по борьбе с терроризмом.

В сфере информационных технологий рассматривался вопрос о сбалансированности и безопасности использования ИКТ, особенно в условиях цифровизации стран БРИКС. Рабочей группе БРИКС по вопросам безопасности в сфере использования ИКТ было поручено разработать план по развитию сотрудничества в данной области.

В сфере социально-гуманитарного и культурного сотрудничества Россия выступила с инициативой проведения ежегодного Молодежного энергетического

саммита БРИКС, который должен объединить исследовательскую работу талантливых и перспективных ученых (проект «Молодежный энергетический прогноз БРИКС» BRICS Youth Energy Outlook 2020).

Уточнены Концепция функционирования и Дорожная карта Сетевого университета стран БРИКС, на базе которого регулярно реализуется Школа БРИКС с участием молодых специалистов.

Одним из измерений сотрудничества 2020 году в рамках БРИКС явилось празднование 75-летия окончания Второй мировой войны. В параде Победы на Красной площади в Москве вместе с российскими военнослужащими участвовали военные расчеты из стран БРИКС. Важность Победы над фашизмом нашла свое отражение в основополагающих документах, принятых по итогам проведенных мероприятий. Акцентировано внимание на использовании ИКТ в интересах противодействия фальсификации истории, учитывая влияние этой деятельности на обеспечение информационной безопасности.

Важно отметить, что в «Концепции участия Российской Федерации в объединении БРИКС» в числе основных целей в области сотрудничества по вопросам международной безопасности заявлены:

- сотрудничество в интересах обеспечения международной информационной безопасности, использование возможностей БРИКС для продвижения инициатив в этом направлении в рамках различных международных форумов и организаций, прежде всего ООН;
- укрепление в формате БРИКС сотрудничества в области противодействия использованию ИКТ в военно-политических, террористических и криминальных целях, а также в целях, противоречащих обеспечению международного мира, стабильности и безопасности.

Подобное целеполагание в рассматриваемой области разделяется всеми государствами-участниками БРИКС и зафиксировано во всех итоговых декларациях саммитов объединения.

Результаты российского председательства в 2009, 2015 и 2020 годах способствовали дальнейшему укреплению взаимного доверия и понимания, конструктивному и эффективному сотрудничеству, дружбе между народами.

2. Факторы, оказывающие влияние на председательство России в БРИКС в 2024 году

Будущее межгосударственного объединения БРИКС зависит от ряда факторов.

Во-первых, от того, насколько успешно будет развиваться дальнейшее практическое сотрудничество между основоположниками объединения Бразилией, Россией, Индией, Китаем и ЮАР. Для этого сделало немало: заложены основы

для углубления взаимодействия БРИКС в энергетике, налогообложении, здравоохранении, космосе, противодействии терроризму и киберугрозам.

Во-вторых, от того, как БРИКС будет интегрировать новых членов межгосударственного объединения, углублять взаимодействие и партнерство с дружественными странами-единомышленниками, разделяющими базовые ценности. В этом контексте предпочтительным вариантом явится поэтапное присоединение новых членов объединения к различным экспертным и консультативным форматам межгосударственного взаимодействия в БРИКС.

XV саммит лидеров БРИКС в Йоханнесбурге (ЮАР) в 2023 году обозначил новую ступень развития объединения и его влияния на мир. Достигнуты договоренности по трем направлениям взаимодействия: политическому, экономическому и гуманитарному.

Расширение с 1 января 2024 г. БРИКС за счет новых стран-участников требует их полноценного подключения ко всем процессам интеграции в рамках объединения в период российского председательства. Данный фактор учитывается в контексте потребности рассмотрения значительного количества полученных официальных заявок от других стран на вступление в объединение.

Сообщается, что официальных заявок на вступление в БРИКС подано более двадцати. Таким образом, определяется важность выработки формата и параметров взаимодействия с перспективными государствами-партнерами БРИКС. В условиях формирования многополярного мира важным фактором является задача вовлечения мирового большинства в БРИКС после первой волны расширения.

В-третьих, российской стороне в период своего председательства в БРИКС, необходимо будет учитывать ранее задекларированные задачи, а также вновь поступившие предложения участников объединения.

Так, 30 января – 1 февраля в Москве состоялась первая встреча шерп/сушерп стран БРИКС в рамках российского председательства с участием представителей стран, ставших полноформатными членами объединения с 1 января 2024 г. В ходе заседания ряд участников высказали свои пожелания.

Шерпа Китая в БРИКС сообщил, что КНР считает необходимым использовать национальные валюты в расчетах между странами. «Мы должны укреплять наше практическое сотрудничество, поддерживать активную работу и содействовать развитию Нового банка развития (НБР) БРИКС», — заявил Ма Чжаосюй.

По его словам, власти Китая также рассматривают возможность запуска центра БРИКС по сотрудничеству в сфере развития технологий искусственного интеллекта. Данное направление работы государств БРИКС становится одним из наиболее важных в рамках группы.

Свое согласие с китайским коллегой выразил Мехди Сафари, шерпа Ирана в БРИКС. Он отметил, что Тегеран тоже рассчитывает на активизацию перехода к расчетам в национальных валютах в период председательства России в объединении.

Еще одна важная тема — сотрудничество стран-участниц в сфере здравоохранения. Представитель МИД Индии, шерпа страны в объединении Абишек Сингх выступил с предложением создать общий депозитарий лекарств БРИКС. Он также сообщил о том, что в 2024 году Индия планирует добиться прогресса в реализации проекта онлайн-архива базы данных БРИКС. По-мнению Индии, такой архив станет прекрасной возможностью для получения доступа к аутентичным документам БРИКС.

В ходе встречи замглавы МИД Египта Раги Этреби заявил о готовности страны проявлять активность во всем, что касается развития связей в сферах торговли, информационно-коммуникационных технологий, морского транспорта и логистики. Кроме того, Египет надеется на содействие России, как председателя БРИКС, в решении проблем продовольственной и энергетической безопасности. При этом египетская сторона считает, что этому будет способствовать плавная интеграция и полноценное включение новых членов в работу.

Представитель МИД ОАЭ Ахмед аль-Бадави сообщил, что Объединенные Арабские Эмираты намерены делиться с коллегами опытом в сфере цифровой экономики. По его мнению, такое взаимодействие поможет достичь целей БРИКС по цифровой трансформации.

Шерпа ЮАР в БРИКС Анил Суклал заявил о необходимости учета многократного роста интереса к объединению со стороны большей части развитых стран и государств глобального Севера, что «свидетельствует о доверительном отношении к тому, чем занимается объединение, к тем принципам, которые мы исповедуем, и к тем целям, которые мы ставим перед собой»[3].

Другой базовый фактор связан с одной из ключевых задач, стоящих перед объединением в интересах экономического развития государств, что требует выработки решения по запуску собственного платежного инструмента БРИКС с использованием достижений в ИКТ-сфере, а также справедливого реформирования международной валютно-финансовой системы через повышение возможностей голоса стран мирового большинства.

Актуальность решения задачи по обеспечению стабильности и предсказуемости торговли и инвестиций БРИКС определяется текущей санкционной политикой Запада по отношению к целому ряду стран БРИКС и объективной потребностью обеспечения независимого и неподконтрольного органам США финансового и торгово-экономического развития.

3 https://finance.rambler.ru/economics/52181977/?utm_content=finance_media&utm_medium=read_more&utm_source=copylink

Страны-участники БРИКС объединяет их политическое, экономическое и цивилизационное противостояние с индустриально развитыми странами Запада. государства, входящие в G7, не допускают страны БРИКС в круг избранных и предпочитают вырабатывать дальнейшую стратегию мирового финансово-экономического развития в узком составе, чтобы учитывать лишь собственные интересы и диктовать свои условия.

БРИКС превращается в основной фактор стабилизации в финансовой сфере, что в частности, определяет необходимость разработки антикризисных мер перед угрозой распада еврозоны и утери лидерства доллара.

Страны БРИКС уже выступают практически как единомышленники при рассмотрении серьезных проблем в ООН и на других форумах, включая экономическую G20. Очевидно и возрастание роли БРИКС в Совете Безопасности ООН.

БРИКС получил импульс к осуществлению реального перехода к новому справедливому миропорядку. Именно 2024 год покажет, справились ли Россия как председатель и весь БРИКС с этой сверхзадачей.

3. О председательстве Российской Федерации в БРИКС в 2024 году

В 2024 году Российская Федерация выполняет председательскую функцию в БРИКС и одновременно в СНГ. Двойное председательство России происходит на фоне сложной международной обстановки. Развитие турбулентности в межгосударственных отношениях и глобальной неопределенности, возникновение новых вызовов и угроз международной безопасности усугубляется глубокими противоречиями между коллективным Западом и большинством государств мирового сообщества. США и его западные партнеры определили Россию и Китай не как оппонентов и конкурентов, а в качестве стратегических противников. В этих условиях для Москвы и Пекина особое значение приобретает сотрудничество в рамках БРИКС.

В настоящий момент объединение находится на новой стадии своего развития, требующей повышения уровня координации действий расширенного состава стран-участниц и конкретизации планов развития. В данном контексте важнейшим приоритетом является не только экономическое, но и политическое направление. Перспективными направлениями представляются развитие свободной торговли БРИКС, укрепление потенциала Нового банка развития НБР БРИКС, взаимодействие сторон в области безопасности, прежде всего в сфере качественного улучшения методов антитеррористического противодействия, усовершенствование механизма совместного противодействия угрозам в информационной сфере.

Несмотря на прозвучавшие призывы к объединению стран мирового большинства для решения общих задач, председательство России в БРИКС все же стартовало в атмосфере некоторой неопределенности в связи с форматом участия Саудовской Аравии в первой московской встрече шерп/су-шерп стран БРИКС.

По заявлению Президента Российской Федерации В.В. Путина тема председательства 2024 года определена как «Укрепление многосторонности для справедливого глобального развития и безопасности», что будет включать в себя как вопросы развития преемственности в рамках ранее обсуждавшейся проблематики, так и направления, по которым у России накоплен значительный передовой опыт.

Вполне очевидно, что в центре внимания окажется развитие экономических связей в БРИКС.

Объединению под председательством России предстоит решить ряд сложных задач, связанных с сохранением эффективности БРИКС в расширенном составе, полноценном подключении новых участников ко всем уже согласованным проектам и механизмам, без снижения темпов углубления взаимодействия и интеграции, обеспечения финансовой и внутриполитической устойчивости для БРИКС.

Кроме того, важно консенсусом определить порядок председательствования с учетом новых членов. Прогнозируется, что в Казани будет положено начало новому порядку ротации с учетом региональных, политических и экономических принципов.

Запуск полноценной работы БРИКС в новом составе может стать стратегическим ориентиром на пути реформирования существующей системы международных и экономических отношений.

В период российского председательства следует ожидать решения ряда вопросов в области энергетики, что предусматривается Йоханнесбургской декларацией, в которой задекларировано право использования странами оптимального баланса источников энергии с учетом национальных запросов и возможностей. В свою очередь, это нацеливает на полноформатное концептуальное оформление принципов справедливого энергоперехода стран мирового большинства в рамках предстоящего председательства. На этом направлении запущенная по инициативе России Платформа энергетических исследований БРИКС, а также включение в объединение новых энергетических акторов позволят организовать более тесное взаимодействие в этой сфере и, возможно, рассмотреть вопрос создания Энергетического агентства БРИКС.

В рамках российского председательства необходима комплексная работа над новой стратегией экономического партнерства БРИКС, так как реализация второй Стратегии завершается в 2025 году. Ожидается, что одним из приоритетов

в новой стратегии должна стать составляющая транспортной взаимосвязанности и развития инфраструктуры БРИКС, в том числе в контексте объявленного Президентом В.Путиным предложения об организации комиссии по транспортным вопросам и создания новых устойчивых транзитных артерий как на пространстве Большой Евразии, так и в мировом масштабе. Реализация данной задачи должна быть обеспечена и мероприятиями, направленными на налаживание сотрудничества в области информационной безопасности.

Запланировано провести около 200 мероприятий более чем в десяти городах нашей страны.

При этом проведение встречи БРИКС на высшем уровне намечено в октябре 2024 года в Казани.

По заявлению Президента Российской Федерации В.В.Путина приоритетами председательства России в БРИКС определены: расширение круга участников объединения, плотная координация с партнерами по внешнеполитическому досье; борьба с терроризмом и с отмыванием денег.

«Будем способствовать дальнейшей комплексной реализации Стратегии экономического партнерства БРИКС до 2025 года и выработке новых долгосрочных ориентиров сотрудничества», — отметил В. Путин. В том числе речь пойдет о расширении использования национальных валют, развитии гуманитарных связей. Будучи председателем, Россия намерена конструктивно взаимодействовать с партнерами по «пятерке», укреплять роль и авторитет БРИКС»

В соответствии с решением Йоханнесбургского саммита пристальное внимание в 2024 году будет уделено органичному встраиванию новых участников БРИКС в архитектуру многостороннего сотрудничества. Планируется также доработать модальности новой категории «государств-партнеров» объединения.

Среди других подтвержденных приоритетов — наращивание внешнеполитической координации в формате БРИКС, прежде всего на ключевых международных площадках, укрепление взаимодействия по вопросам борьбы с терроризмом, отмыванием денег, международной информационной безопасности, включая использование технологий искусственного интеллекта. а также возвращения активов, полученных преступным путем.

Что касается развития сотрудничества в области обеспечения международной информационной безопасности стран-членов БРИКС, представляется целесообразным задействовать специализированные НКО и другие профильные структуры акторов межгосударственного объединения в целях наращивания усилий Рабочей группы экспертов БРИКС по вопросам безопасности в сфере использования ИКТ. Для координации взаимодействия научно-академических кругов, исследовательских институтов и НПО, продвижения российских интересов в формате БРИКС является востребованным научный потенциал Национальной Ассоциации междуна-

родной информационной безопасности (НАМИБ). Данный вопрос был предложен российской стороной к рассмотрению в апреле т.г. в ходе 10-го заседания рабочей группы БРИКС по вопросам безопасности в сфере использования ИКТ.

Важным направлением работы российского председательства будет комплексная реализация Стратегии экономического партнерства БРИКС до 2025 года и Плана действий по инновационному сотрудничеству на 2021–2024 гг.

Особый акцент будет сделан на повышении роли государств БРИКС в международной валютно-финансовой системе, развитии межбанковской кооперации с акцентом на наращивание расчетов в национальных валютах.

Страны БРИКС по весу в глобальной экономике уже обошли G7 и снижают зависимость от прежней финансовой инфраструктуры, наращивая расчеты в национальных валютах и создавая собственные платформы. В год председательства России в БРИКС ЦБ намерен придерживаться принципа преемственности и развития инициатив, которые предложили партнеры в предыдущие годы. Среди них четыре ключевых.

Первое — это развитие платежной сферы. Есть экспертная группа, которая обсуждает различные вопросы, включая цифровые валюты и взаимодействие платежных систем. Предполагается сделать больший фокус на расчеты в национальных валютах.

Вторая тема — кибербезопасность в финансовой сфере, что интересует многие центральные банки. Здесь, важно совершенствовать обмен данными о киберрисках. Кроме того, предусматривается проведение трансграничных киберучений. Этот вопрос был вынесен на обсуждение в феврале на Уральском форуме по кибербезопасности.

Так, Банк России в феврале 2024 г. сообщил о проведении первых совместных трансграничных киберучений, которые позволят определить оперативную готовность центральных банков стран БРИКС к реагированию на трансграничные компьютерные атаки. Сценарий киберучений обсуждался на первой встрече Канала БРИКС в сфере информационной безопасности (BRICS Rapid Information Security Channel) с участием представителей центральных банков и регуляторов финансового рынка стран-участников БРИКС, в том числе новых. На повестке стояли вопросы обмена данными о компьютерных атаках и киберугрозах, необходимости обновления справочника нормативно-правовых актов стран БРИКС в сфере кибербезопасности, а также отдельные аспекты функционирования внутренних систем обеспечения защиты организаций кредитно-финансовой сферы. Участники встречи решили продолжать выпускать сборники лучших практик стран БРИКС в области обеспечения информационной безопасности финансового сектора. Следующая встреча участников БРИКС в дистанционном формате — во втором квартале 2024 года.

Канал БРИКС — экспертная площадка подразделений по вопросам информационной безопасности центральных банков и групп реагирования на компьютерные инциденты стран БРИКС. Встречи Канала БРИКС проходят 3–4 раза в год, а взаимодействие осуществляется по четырем основным направлениям: предупреждение, идентификация, реагирование и восстановление.

Третье направление — развитие финансовых технологий путем автоматизации систем трансграничной идентификации, что позволит людям быстрее получать финансовые услуги в другой стране БРИКС. Также планируется обсудить использование искусственного интеллекта в финансах.

Четвертое направление — повестка устойчивого развития и адаптация экономик к климатическим изменениям. Страны БРИКС этим очень интересуются, и тему эту Россия намерена активно продвигать путем обсуждения проблемы выработки механизма интеграции климатических рисков в финансовое регулирование, а также развития стандартов для зеленых и адаптационных облигаций.

В числе новых инициатив определены следующие направления:

- продвижение тем взаимного признания рейтингов, что важно для взаимной торговли и инвестиций, включая создание наднациональных рейтинговых агентств;
- противодействие отмыванию сомнительных доходов. У России есть хороший опыт создания антиотмывочной платформы «Знай своего клиента», которым готовы делиться. Необходимо изучить какие общие платформенные решения в этой области можно развивать на уровне БРИКС, что упростило бы сотрудничество бизнеса стран-участниц объединения;
- выстраивание расчетно-депозитарной инфраструктуры;
- создание общей для стран-участниц БРИКС платформы для обучения и обмена опытом (планируется на базе Университета Банка России).

Главной задачей является обеспечение независимости от международной системы обмена финансовыми сообщениями SWIFT и совершенствование собственных инструментов стран БРИКС. Получен опыт интеграции подобных систем России и Ирана. У нашей страны есть своя Система передачи финансовых сообщений (СПФС), которая является альтернативой SWIFT, к которой предлагается подключаться странам БРИКС. Уже 159 иностранных участников из 20 стран присоединились. Аналогичная инфраструктура есть и у некоторых других стран. Ведутся дискуссии о взаимодействии таких платформ с учетом интереса и технической готовности наших партнеров.

Банком России рассматривается в перспективе проведение пилотов по трансграничным платежам в цифровых валютах. Многие страны сейчас думают о введении цифровых валют центральных банков. При создании платформы цифрового рубля заложена возможность ее интеграции с аналогичными зарубеж-

ными платформами. Сейчас проводятся консультации, переговоры со многими дружественными странами и, конечно, со странами БРИКС, по трансграничным расчетам через цифровые валюты. В перспективе они будут развиваться.

В России поддерживается применение криптовалют во внешней торговле, но законопроект, который дает такую возможность, еще обсуждается в Государственной думе[4].

Должное внимание будет уделено дальнейшему углублению диалога и взаимодействия в области культуры, спорта, молодежных обменов.

Летом в Казани будут организованы также спортивные Игры БРИКС, в том числе киберсоревнования.

Что касается скорости дальнейшего расширения БРИКС, то она будет зависеть от того, какой вектор сотрудничества станет приоритетным — экономический или политический. Ожидается, что эта тема станет одной из главных в повестке саммита в Казани. Тем более, что в течение председательства России планируется определиться с тем, как и по каким критериям будет осуществляться дальнейший прием новых членов. Ведь рост их числа несет в себе как новые возможности, так и новые риски.

Наглядный пример — подчеркнуто критический настрой нового президента Аргентины Хавьера Милея по отношению к БРИКС, в который страна была приглашена на саммите в Йоханнесбурге. Еще во время предвыборной кампании он неоднократно заявлял, что не намерен продвигать отношения с Бразилией, Китаем и Россией из-за несогласия с их политикой, но в то же время утверждал, что не будет мешать частному бизнесу вести дела с ними.

Самим странам БРИКС придется понять, что за расширение их рядов придется заплатить свою цену: больший численный состав и большее разнообразие внутри объединения затруднят достижение консенсуса по многим важным вопросам (опыт ШОС после принятия Индии и Пакистана — тому подтверждение).

30 января – 1 февраля т.г. в Москве состоялась первая встреча шерп/су-шерп стран БРИКС в рамках российского председательства с участием представителей стран, ставших полноформатными членами объединения с 1 января 2024 г.

В ходе заседания представители российских министерств и ведомств выступили с развернутыми брифингами по ключевым направлениям сотрудничества. Отмечена важность реализации ряда российских инициатив, в частности, запуска Комплексной системы раннего реагирования на риски возникновения массовых инфекционных заболеваний, учреждения Центра промышленных компетенций на базе ЮНИДО, Медицинской ассоциации БРИКС и профильного журнала, укрепления сотрудничества в сфере транспорта и туризма.

4 https://ria.ru/20240130/

В рамках выполнения поручений лидеров стран БРИКС по итогам XV саммита объединения (Йоханнесбург, 22–24 августа 2023 г.) продолжено обсуждение модальностей категории государств-партнеров БРИКС, а также повышения роли национальных валют и платежных инструментов в трансграничных операциях стран «десятки». Всеми участниками заседания подтверждена нацеленность на дальнейшую конструктивную работу в рамках трех «корзин» стратегического партнерства БРИКС: в области политики и безопасности, экономики и финансов, культуры и гуманитарных связей.

В 2024 году России как первому председателю БРИКС в расширенном составе необходимо обеспечить интеграцию новых стран-участниц в работу объединения. В интересах этого БРИКС нуждается в развитии неформальных инициатив академических, экспертных и гражданских сообществ, которые взаимодействуют с государственными институтами.

В связи с этим во исполнение поручения Правительства РФ по инициативе МИДа России и Минфина России в Высшей школе экономики в феврале 2024 г. создан «Экспертный совет по вопросам участия Российской Федерации в объединении БРИКС». Совет будет заниматься экспертно-аналитической и научной деятельностью по актуальным вопросам политического, социально-экономического и гуманитарного сотрудничества в объединении.

В этом году совет проведет ряд экспертных мероприятий для сбора рекомендаций лидерам государств БРИКС по развитию всеобъемлющего сотрудничества стран-участниц объединения. Главные итоги работы экспертного трека будут представлены на Академическом и Гражданском форумах БРИКС, которые пройдут в Москве 22–24 мая и 3–4 июля соответственно.

Очередным важным решением Президента России В. Путина по итогам заседания Совета при президенте по науке и образованию является поручение Российскому союзу ректоров, Российской академии наук (РАН) и Российской академии образования (РАО) подготовить предложения по рейтингу университетов стран БРИКС[26]. Кроме того, предусматривается также сформировать в рамках БРИКС общественно-консультативный совет по академическому лидерству. Его цель — консолидировать усилия по повышению уровня конкурентоспособности университетов и научных организаций стран-участниц, определить правила конкуренции. Предлагается создать систему рейтингования ВУЗов стран БРИКС на основе Московского международного рейтинга «Три миссии университета», в котором сегодня участвует 2000 университетов из 112 стран.

Впереди сотни мероприятий, организуемых Россией, направленных во благо стран-участниц БРИКС.

Основные источники:

1. Московская декларация XII саммита БРИКС (г. Москва, Россия, 17 ноября 2020 года) // Саммиты и документы, НКИ БРИКС Россия, https://nkibrics.ru/pages/summit-docs
2. Сайт российского председательства в БРИКС, https://brics-russia2020.ru/allnews/
3. Andrey Kortunov BRICS: between broadening and deepening, Global Times, Aug 21, 2023, https://www.globaltimes.cn/page/202308/1296683.shtml
4. В. Петровский БРИКС в 2024: дилемма расширения и развития, Журнал «Международная жизнь», 25.12.2023, https://interaffairs.ru/news/show/43919
5. Опубликован План действий Медиафорума высокого уровня стран БРИКС на 2022–2023 гг. // Агентство Синьхуа, 9.07.2022, https://russian.news.cn/20220709/d249f481a9b44010a2e1af12e5400207/c.html
6. Andrey Kortunov BRICS: between broadening and deepening, Global Times, Aug 21, 2023, https://www.globaltimes.cn/page/202308/1296683.shtml
7. В. Петровский БРИКС в 2024: дилемма расширения и развития, Журнал «Международная жизнь», 25.12.2023, https://interaffairs.ru/news/show/43919
8. Д. Каверин, Утвержден план мероприятий в рамках председательства России в БРИКС // Газета.ru, 25.12.2023, https://turbo.gazeta.ru/politics/news/2023/12/25/22002313.shtml
9. Итоги заседания Организационного комитета по подготовке и обеспечению председательства Российской Федерации в объединении БРИКС в 2024 году// Росконгресс, 25.12.2023, https://roscongress.org/news/itogi-zasedanija-organizatsionnogo-komiteta-po-podgotovke-i-obespecheniju-predsedatelstva-rossijskoj/?ysclid=lv3jz3n1y095988248
10. Ю. Паниев БРИКС шире откроет двери глобальному Югу // Независимая газета 24.12.2023, https://www.ng.ru/dipkurer/2023-12-24/9_11_8910_brics.html
11. Об участии заместителя Министра иностранных дел России С.А. Рябкова в заседании шерп/су-шерп стран-членов БРИКС // МИД России, 3.12.2023, https://www.mid.ru/ru/foreign_policy/news/1918749/
12. В. Панова Россия на пути к председательству в БРИКС // Международный дискуссионный клуб «Валдай», 1.09.2023, https://ru.valdaiclub.com/a/highlights/rossiya-na-puti-k-predsedatelstvu-v-briks/?ysclid=lv3k68u1qa303719370
13. Г.Карасин Роль России в БРИКС: влияние и перспективы // Tvbrics 20.03.23, https://tvbrics.com/news/rol-rossii-v-briks-vliyanie-i-perspektivy/?ysclid=lpodtpao48148450525
14. «Стратегия развития БРИКС и приоритеты для России». Материалы доклада НИУ ВШЭ 2020 г., Стратегия_развития_БРИКС-на_сайт-29.05.pdf (hse.ru)
15. Концепция участия Российской Федерации в объединении БРИКС (утверждена Президентом РФ 09.09.2013) // МИД России, 21.03.2013, https://www.mid.ru/ru/foreign_policy/news/1744621/
16. Гришаева Л.Е. БРИКС и новая роль России в глобальном партнерстве, https://cyberleninka.ru/article/n/briks-i-novaya-rol-rossii-v-globalnom-partnerstve?ysclid=lv3l82lhw0683773966
17. Об участии заместителя Министра иностранных дел России С.А.Рябкова в заседании шерп/су-шерп стран-членов БРИКС // МИД России, 3.12.2023, https://www.mid.ru/ru/foreign_policy/news/1918749/
18. Итоги заседания Организационного комитета по подготовке и обеспечению председательства Российской Федерации в объединении БРИКС в 2024 году// Росконгресс, 25.12.2023, https://roscongress.org/news/itogi-zasedanija-organizatsionnogo-komiteta-po-podgotovke-i-obespecheniju-predsedatelstva-rossijskoj/?ysclid=lv3jz3n1y095988248
19. Там же.
20. Соловьева О. Набиуллина сфокусирует страны БРИКС на новых формах расчетов // Независимая газета, 30.01.2024, https://www.ng.ru/economics/2024-01-30/4_8935_problems.html?ysclid=lv3lg9ryjo70390104
21. https://ria.ru/20240130/
22. Бойко С.М. Проблематика международной информационной безопасности на площадках ШОС и БРИКС // Журнал «Международная жизнь», 23.01.2019, https://interaffairs.ru/news/show/21480
23. В МИД РФ рассказали о сотрудничестве БРИКС по кибербезопасности, 2.06.2023, https://namib.online/2023/06/v-mid-rf-rasskazali-o-razvitii-sotrudnichestva-v-briks-po-kiberbezopasnosti/
24. ЦБ сообщил о первых совместных трансграничных киберучениях БРИКС, 19.02.2024, https://d-russia.ru/cb-soobshhil-o-pervyh-sovmestnyh-transgranichnyh-kiberuchenijah-briks.html
25. В НИУ ВШЭ начал работу Экспертный совет по вопросам участия России в БРИКС, 29.02.2024, https://www.hse.ru/news/expertise/900899058.html?ysclid=lt8jw0qqx7243995209
26. Путин поручил подготовить к 15 апреля рейтинг университетов стран БРИКС // ИА Регнум, 26.03.2024, https://regnum.ru/news/3877150?ysclid=lufnq95crk141632167

Соглашения Российской Федерации с государствами-участниками БРИКС в области использования ИКТ, обеспечения их безопасности и международной информационной безопасности

1. Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности.
   Подписано 6.06.2009, вступило в силу 5.01.2012, распространяется на членов ШОС — Индию, Иран, КНР, Российскую Федерацию, https://docs.cntd.ru/document/902289626.
2. Соглашение между Правительством Российской Федерации и Правительством Федеративной Республики Бразилии о сотрудничестве в области обеспечения международной информационной и коммуникационной безопасности.
   Подписано 14.05.2010, ратифицировано Распоряжением Правительства Российской Федерации от 13.05.2010 № 721-р, в силу не вступило, https://www.mid.ru/ru/foreign_policy/international_contracts/international_contracts/2_contract/44973/.
3. Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности.
   Подписано 08.05.2015, вступило в силу 10.08.2016, https://www.mid.ru/ru/foreign_policy/international_contracts/international_contracts/2_contract/43921/?ysclid=luuy8hw86j689302764.
4. Соглашение между Правительством Российской Федерации и Правительством Республики Индии о сотрудничестве в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий.
   Подписано 15.10.2016, ратифицировано Распоряжением Правительства Российской Федерации от 13.10.2016 № 2157-р, вступило в силу 22.01.2017, https://www.mid.ru/ru/foreign_policy/international_contracts/international_contracts/2_contract/51667/.
5. Соглашение между Правительством Российской Федерации между Правительством Российской Федерации и Правительством Южно-Африканской Республики о сотрудничестве в области обеспечения международной информационной безопасности.
   Подписано 04.09.2017, в силу не вступило, https://www.mid.ru/ru/foreign_policy/international_contracts/international_contracts/2_contract/52469/.

6. Соглашение между Правительством Российской Федерации и Правительством Исламской Республики Иран о сотрудничестве в области обеспечения информационной безопасности.
   Подписано 26.01.2021, одобрено меджлисом Ирана в декабре 2023, в силу не вступило, https://www.mid.ru/ru/foreign_policy/international_contracts/international_contracts/2_contract/59914/.
7. Соглашение о свободной торговле между Евразийским экономическим союзом и его государствами-членами, с одной стороны, и Исламской Республикой Иран, с другой стороны.
   Подписано и вступило в силу для Российской Федерации.
   25.12.2023, https://www.mid.ru/ru/foreign_policy/international_contracts/international_contracts/multilateral_contract/62376/?ysclid=luuy45kdx335332844.
8. Соглашение между Правительством Российской Федерации и Правительством Федеративной Демократической Республики Эфиопия о взаимной охране результатов интеллектуальной деятельности и защите интеллектуальной собственности в ходе двустороннего военно-технического сотрудничества.
   Подписано 24.08.2021, одобрено парламентом Эфиопии в декабре 2023, в силу не вступило, https://www.mid.ru/ru/foreign_policy/international_contracts/international_contracts/2_contract/60376/.
9. Соглашение между Правительством Российской Федерации и Правительством Федеративной Демократической Республики Эфиопии о сотрудничестве в области обеспечения международной информационной безопасности.
   Подписано 28.07.2023, в силу не вступило, https://www.mid.ru/ru/foreign_policy/international_contracts/international_contracts/2_contract/62201/.
10. Соглашение о создании Инвестиционного фонда в сфере высоких технологий в размере 1 миллиард долларов, предусматривающее инвестиции Публичного инвестиционного фонда Саудовской Аравии и Российского фонда прямых инвестиций.
    Подписано 5.10.2017, http://www.kremlin.ru/supplement/5236.
11. Меморандум о взаимопонимании между Министерством связи и массовых коммуникаций Российской Федерации и Министерством связи и информационных технологий Королевства Саудовская Аравия о сотрудничестве в области связи и информационно-коммуникационных технологий.
    Подписан 5.10.2017, http://www.kremlin.ru/supplement/5236.

12. Дорожная карта торгово-экономического и научно-технического сотрудничества между Российской Федерацией и Королевством Саудовская Аравия на среднесрочную перспективу.
    Подписана 5.10.2017 года, http://www.kremlin.ru/supplement/5236.
13. Меморандум о взаимопонимании между Министерством связи и массовых коммуникаций Российской Федерации и Министерством связи и информационных технологий Арабской Республики Египет о сотрудничестве в области электросвязи, почтовой связи и информационных технологий.
    Подписан в марте 2016, https://digital.gov.ru/ru/activity/directions/723/.

Совместные заявления о стратегическом партнерстве

1. Совместное заявление о стратегическом партнерстве Российской Федерации и Южно-Африканской Республики от 26.07.2018, http://www.kremlin.ru/supplement/5325.
2. Совместное заявление Российской Федерации и Китайской Народной Республики о развитии отношений всеобъемлющего партнерства и стратегического взаимодействия, вступающих в новую эпоху от 5.06.2019, http://www.kremlin.ru/supplement/5413.
3. Декларация о стратегическом партнерстве между Российской Федерацией и Республикой Индией. Подписано 3 октября 2000 г., https://www.mid.ru/tv/?id=1732761&lang=ru.

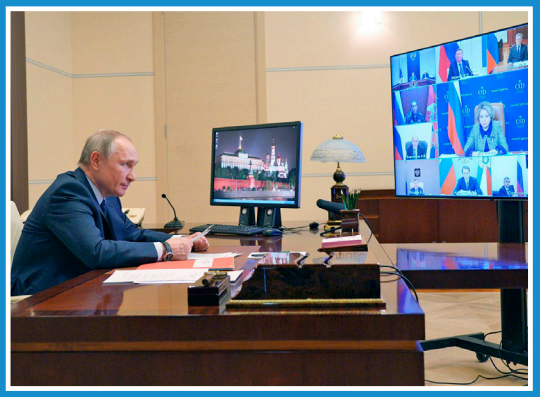
НАЦИОНАЛЬНАЯ АССОЦИАЦИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (НАМИБ)

Образована 10 апреля 2018 года

Заседание Совета Безопасности России 26 марта 2021 года

...в эффективной реализации государственной политики, обозначенной в новой редакции «Основ государственной политики в области международной информационной безопасности», надо активнее использовать возможности научных и экспертных кругов, делового сообщества, в том числе, конечно, Национальной ассоциации международной информационной безопасности.

В.В. Путин



Б.Н Мирошников

Президент Национальной Ассоциации международной информационной безопасности

В.В. Соколов

Генеральный директор Национальной Ассоциации международной информационной безопасности

В.П. Шерстюк

Научный руководитель Национальной Ассоциации международной информационной безопасности, Председатель Международного исследовательского консорциума информационной безопасности (объединяет 28 организаций из 18 стран)

Приглашаем Вас к сотрудничеству с Ассоциацией и Консорциумом. Добро пожаловать на наши международные мероприятия по информационной безопасности.

УСТАВ

Национальная Ассоциация международной информационной безопасности (далее — Ассоциация) является основанным на добровольном участии корпоративным объединением юридических и физических лиц, созданном для координации деятельности членов Ассоциации по содействию реализации государственной политики Российской Федерации в области международной информационной безопасности.

Цель

содействие формированию системы обеспечения устойчивого функционирования глобальной и национальной информационных инфраструктур, безопасного использования информационных и коммуникационных технологий во всех сферах жизни общества и управления государством.

Учредители

- Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный университет имени М.В. Ломоносова».
- Федеральное государственное автономное образовательное учреждение высшего образования «Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации».
- Федеральное государственное бюджетное образовательное учреждение высшего образования «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации».
- Федеральное государственное бюджетное образовательное учреждение высшего образования «Дипломатическая академия Министерства иностранных дел Российской Федерации».
- Публичное акционерное общество «Горно-металлургическая компания «Норильский никель».
- Федеральное государственное бюджетное учреждение Редакция журнала «Международная жизнь».

Члены Наблюдательного Совета

ХРАМОВ Олег Владимирович, Председатель Наблюдательного Совета, Заместитель Секретаря Совета Безопасности Российской Федерации.

ВОЛОБУЕВ Николай Анатольевич, заместитель Генерального директора Государственной корпорации «Ростех».

ГАСУМЯНОВ Владислав Иванович, директор Автономной некоммерческой организации «Национальный институт исследований и развития проектов в сфере межнациональных, межконфессиональных, межэтнических, межкультурных и межстрановых коммуникаций».

ЗОРИН Виктор Михайлович, советник ректора РАНХиГС при Президенте Российской Федерации.

ИСМАИЛОВ Рашид Рустам оглы, член Наблюдательного Совета НАМИБ.

КУЗНЕЦОВ Станислав Константинович, заместитель председателя правления ПАО «Сбербанк России».

СОКОЛОВ Игорь Анатольевич, декан факультета вычислительной математики и кибернетики МГУ имени М.В. Ломоносова.

Члены Президиума

МИРОШНИКОВ Борис Николаевич, Президент НАМИБ, вице-президент ГК «ГАРДА».

СОКОЛОВ Владимир Викторович, Генеральный директор НАМИБ, заместитель руководителя научного центра «ИПИБ» факультета вычислительной математики и кибернетики МГУ имени М.В. Ломоносова.

БОЙКО Сергей Михайлович, референт аппарата Совета Безопасности Российской Федерации.

ГРИГОРЬЕВ Дмитрий Игоревич, вице-президент НАМИБ, Генеральный директор АНО «КОМИБ».

КРУТСКИХ Андрей Владимирович, директор Центра международной информационной безопасности и научно-технологической политики МГИМО МИД России.

ЛЮКМАНОВ Артур Рушанович, специальный представитель Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности, директор департамента международной информационной безопасности МИД России.

ОГАНЕСЯН Армен Гарникович, главный редактор журнала «Международная жизнь».

ПЕРЕЛЫГИН Александр Станиславович, старший советник Председателя Правления, Управляющий директор Инвестиционной компании «Ренессанс Капитал».

СТРЕЛЬЦОВ Анатолий Александрович, вице-президент НАМИБ, ведущий научный сотрудник факультета вычислительной математики и кибернетики МГУ имени М.В. Ломоносова.

Основные направления деятельности

- осуществляет проработку в упреждающем режиме проблемных вопросов обеспечения МИБ в интересах формирования переговорных позиций государственных органов;
- участвует в составе российских делегаций в подготовке и проведении экспертных консультаций по вопросам формирования системы МИБ в формате международных организаций (ООН, ОБСЕ, ШОС, СНГ, ОДКБ, БРИКС, АТЭС, «Группы двадцати» и других), а также двусторонних, многосторонних и региональных консультаций Российской Федерации с другими государствами;
- совместно с федеральными органами исполнительной власти и заинтересованными организациями готовит предложения по укреплению международного сотрудничества, направленного на содействие успешному осуществлению программы «Цифровая экономика Российской Федерации» в части вопросов информационной безопасности.

Основные мероприятия

Международный форум «Партнерство государства, бизнеса и общества при обеспечении международной информационной безопасности» (в контексте обеспечения гармишевского процесса).

Международная конференция по проблемам обеспечения системы международной информационной безопасности (по плану Международного исследовательского консорциума информационной безопасности).

Проведение совместно с зарубежными экспертами исследовательских проектов по международной информационной безопасности.

Поддержка проектов по проработке в упреждающем режиме проблемных вопросов обеспечения МИБ в интересах формирования переговорных позиций государственных органов.

Участие в составе межведомственных делегаций и самостоятельно в консультациях и различных международных конференциях и форумах.
Содействие деятельности российских компаний-разработчиков средств и услуг в области информационной безопасности по продвижению их продукции на зарубежные рынки.

Деятельность некоммерческой организации НАМИБ обеспечивается финансовой и материальной поддержкой государственных корпораций и структур, заинтересованных в обеспечении информационной безопасности страны.

Полное Наименование	Национальная ассоциация международной информационной безопасности
Сокращенное наименование	НАМИБ
Юридический адрес	119192 г. Москва, пр-т Мичуринский, д.1, пом.4
Почтовый адрес	119192 г. Москва, пр-т Мичуринский, д.1, пом.4
Телефон/факс	тел. 8-916-304-30-00
ИНН/КПП	9729271968/ 772901001
ОГРН	1187700009606
Расчётный счет	40703810638000009576
Корреспондентский счет	30101810400000000225
БИК банка	044525225
Банк	ПАО «Сбербанк» г. Москва
Классификаторы в статистическом регистре	
ОКПО	28693418
ОКАТО	45268584000
ОКТМО	45325000000
ОКОГУ	4210014
ОКФС	41
ОКОПФ	20600
ОКВЭД	94.12
Генеральный директор	Соколов Владимир Викторович
E-mail	sokolov46@yandex.ru

АНО КОМИБ

Автономная некоммерческая организация

«ЦЕНТР КООРДИНАЦИИ ГОСУДАРСТВЕННО-ЧАСТНОГО ПАРТНЕРСТВА В ОБЛАСТИ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Слоган: ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РОССИИ:
СУВЕРЕНИТЕТ, ПРОВЕРЕННЫЙ ВРЕМЕНЕМ

создана в 2023 году
Национальной Ассоциацией
международной информационной безопасности

Москва, Комсомольский пр-т, 42, стр.1
Тел.: +7 985 464 31 10
mail@komib.ru

Генеральный директор АНО КОМИБ – вице-президент НАМИБ

ГРИГОРЬЕВ ДМИТРИЙ ИГОРЕВИЧ

Исполнительный директор АНО КОМИБ

КУЛЬПИН АНДРЕЙ АЛЕКСЕЕВИЧ

АНО КОМИБ создана при поддержке Аппарата Совета Безопасности Российской Федерации для содействия коммерческим компаниями информационной безопасности в организации экспортной деятельности и в их работе с зарубежными партнерами.

Деятельность АНО КОМИБ в формате G2B ориентирована на потребности и интересы операторов связи, провайдеров, поставщиков ИТ-услуг, а также производителей товаров и услуг в сфере информационной безопасности.

Для российских компаний информационной безопасности АНО КОМИБ выполняет следующие функции:

- обеспечивает помощь, предоставляет консультации по ведению бизнеса;
- представляет интересы предпринимателей в отношениях с органами власти;
- оказывает помощь в формировании правовой среды и инфраструктуры предпринимательства;
- оказывает помощь российским предпринимателям в установлении деловых связей с иностранными партнёрами.

Для зарубежных партнеров АНО КОМИБ:

- консультирует иностранных партнеров при формировании программ создания комплексных систем информационной безопасности на базе решений, предлагаемых российскими компаниями;
- рекомендует релевантные российские компании для выполнения проектов информационной безопасности по обращениям иностранных партнеров;
- обеспечивает необходимые для выполнения международных проектов информационной безопасности согласования.

АНО КОМИБ — это команда профессионалов:

- имеющих многолетний опыт обеспечения информационной безопасности крупных промышленных холдингов;
- обладающих серьезной экспертизой в области международных отношений;
- профессионально понимающих текущую ситуацию на рынках информационной безопасности стран-партнеров и имеющих сложившиеся рабочие контакты с лицами, принимающими решения в ряде этих стран.

В апреле 2024 года в рамках XII Международной встречи высоких представителей, курирующих вопросы безопасности АНО КОМИБ по поручению руководства Совета Безопасности Российской Федерации организовала и провела выставку отечественных продуктов и услуг информационной безопасности. АНО КОМИБ обеспечила в едином замысле консолидированную презентацию профильных российских компаний потенциальным зарубежным покупателям.

АНО КОМИБ — это эффективный инструмент государственно-частного партнерства формирования и развития справедливой и устойчивой системы МИБ

Международные командные соревнования по кибербезопасности «BRICS+ CTF»

«У народной дипломатии, у молодежной дипломатии большое будущее: студенческие контакты, прямые связи между учебными заведениями — это то, что мы будем поддерживать как ведомство, делали это раньше, будем наращивать эти усилия по МИДовской линии и впредь» [1].

Сергей Рябков, заместитель Министра иностранных дел, шерпа России в БРИКС

Соревнования «Взятие флага» (англ. Capture the Flag, CTF) — один из самых популярных форматов практико-ориентированных конкурсов для команд компьютерной безопасности. Задача каждой из них захватить «флаг» соперника, для чего необходимо оперативно решать разнообразные задачи, в том числе, связанные с поиском уязвимостей и защитой, сетевой безопасностью, цифровой криминалистикой, криптографией, реверс инжинирингом, искусственным интеллектом. В CTF могут принять участие как начинающие, так и профессиональные команды. Соревнования способствуют повышению профессиональных знаний, отработке навыков слаженной работы в команде, укреплению психологической устойчивости, что является важным компонентом повышения квалификации специалистов в сфере кибер- и информационной безопасности.

Страны-участницы БРИКС и их партнеры БРИКС+ заинтересованы в повышении защищенности национального информационного пространства и повышении кадрового потенциала, в том числе через проведение международных соревнований «BRICS+ CTF», главными целями которых являются:

1. Обеспечение квалифицированными кадрами в сфере информационных технологий.

2. Формирование среди участников системного видения проблем обеспечения информационной безопасности.

3. Глубокое осознание природы возникновения угроз информационной безопасности и практической реализации мероприятий по их предотвращению.

---

1 Председательство в Программе «Народы БРИКС выбирают жизнь» перешло от Индии к Бразилии в МГИМО МИД России // BRICS Мир традиций, https://bricsmt.ru/index.php/zhurnal/153-predsedatelstvo-v-programme-narody-briks-vybirayut-zhizn-pereshlo-ot-indii-k-brazilii-v-mgimo-mid-rossii#:~:text=И%20надеждой%20на%20-успех%2С%20прозвучали,по%20МИДовской%20линии%20и%20впредь».

4. Повышение уровня теоретических знаний и совершенствование практических навыков участников в организации и обеспечении эффективного функционирования систем информационной безопасности.

5. Установление и развитие профессиональных и научных связей между специалистами из стран БРИКС.

В рамках работы Сетевого Университета БРИКС[2] международные соревнования студентов и специалистов в области защиты информации направлены на сближение стран, взаимную интеграцию и сотрудничество в таких наукоёмких областях, как информационная и кибербезопасность.

Впервые «BRICS+ CTF» были проведены в 2019 году. Соревнования были организованы Санкт-Петербургским национальным исследовательским университетом информационных технологий, механики и оптики (Университет ИТМО). В отборочном онлайн-туре участвовали 1188 команд из 71 страны, в том числе из всех стран-участниц БРИКС. Финальный этап проходил очно одновременно в Бразилии, России, Индии, Китае и Южной Африке, что позволило из 22 наиболее сильных команд выявить трех победителей.

В 2020 и 2021 годах из-за пандемии Covid-19 соревнования проводились в один тур и онлайн. В 2023 году ограничения были сняты, и в «BRICS+ CTF» приняли участие 992 человека из 91 страны. Финал мероприятия был приурочен к V Международному муниципальному форуму БРИКС+. Соревнования «BRICS+ CTF» получили широкую известность и завоевали авторитет далеко за пределами Российской Федерации, что способствует расширению состава организаторов[3], отраслевых[4] и информационных партнеров[5]. Российская Ассоциация руководителей служб информационной безопасности (АРСИБ) присоединилась к команде в 2023 году.

Эффективность формата соревнований «BRICS+ CTF» для повышения внимания к проблематике информационной безопасности и подготовки кадров по

2 Сетевой университет БРИКС создан в 2016 году. От Российской Федерации в него вошли 12 вузов: МГИМО (У) МИД России, МГУ им. М.В. Ломоносова, МФТИ, МИСиС, Томский политехнический университет, НИУ ВШЭ, МЭИ, Томский государственный университет, РУДН, СПбГУ, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики (ИТМО) и Уральский федеральный университет.

3 Всероссийское общественное движение наставников детей и молодежи *«Наставники России»*.

4 RDP, EdgeЦентр, XCTF League, Positive Technologies, Федерация спортивного программирования.

5 Журналы Хакер и Международная жизнь, Форум информационной безопасности Codeby.

различным направлениям указанной специальности высоко оценена. Движение по поддержке и продвижению соревнований расширяется. В рамках IV Всероссийского форума «Сильные идеи для нового времени» проведение «BRICS+ CTF» вошло в ТОП100 самых интересных инициатив для формирования стратегии развития страны[6].

Растет международный интерес и география участников «BRICS+ CTF», особенно среди стран Глобального Юга. В 2024 году соревнования удостоены включения в **программу «Народы БРИКС выбирают жизнь»**. Под ее эгидой запущен научно-исследовательский IT-проект «Молодежь БРИКС — за кибербезопасность», реализация которого будет важным вкладом в развитие научно-технического и практического сотрудничества БРИКС в сфере обеспечения информационной безопасности.

6 Определен топ-100 проектов IV форума «Сильные идеи для нового времени» // Сильные идеи для нового времени- 2024, https://идея.росконгресс.рф/news/139812.

Список основных используемых сокращений

АС — Африканский союз

АСЕАН — Ассоциация государств Юго-Восточной Азии

АТЭС — Азиатско-Тихоокеанское экономическое сотрудничество

ВВУИО — Всемирная встреча на высшем уровне по вопросам информационного общества

ВВП — Валовой внутренний продукт

ВТО — Всемирная торговая организация

ЕАЭС — Евразийский экономический союз

ЕС — Европейский союз

ГА ООН — Генеральная Ассамблея Организации Объединенных Наций

ГПЭ ООН — Группа правительственных экспертов ООН:
в 2004–2017 годах по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности
в 2019–2021 годах по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности

ЕС — Европейский союз

ИИ — Искусственный интеллект

ИКТ — Информационно-коммуникационные технологии

ИТ — Информационные технологии

КИИ — Критическая информационная инфраструктура

МИБ — Международная информационная безопасность

МСЭ — Международный союз электросвязи

НАТО — Организация Североатлантического договора

НИОКР — Научно-исследовательские и опытно-конструкторские разработки

ОБСЕ — Организация по безопасности и сотрудничеству в Европе

ООН — Организация Объединенных Наций

ПД — Персональные данные

ПО — Программное обеспечение

РГОС ООН — Рабочая группа ООН открытого состава:
в 2019–2021 годах по достижениям в сфере информатизации

и телекоммуникаций в контексте международной безопасности в 2021–2025 годах по вопросам безопасности в сфере использования ИКТ и самих ИКТ

ССАГПЗ — Совет сотрудничества арабских государств Персидского залива

УК — Уголовный кодекс

ЦОД — Центр обработки данных /Дата-центр

ШОС — Шанхайская организация сотрудничества

ЮНИДИР — Институт Организации Объединенных Наций по исследованию проблем разоружения

3G/ 4G/ 5G — Поколения подвижной (мобильной) связи

AfCFTA — African Continental Free Trade Area / Африканский рынок свободной торговли

API — Application Programming Interface / Программный интерфейс для приложений

CERT/CERTs — Computer Emergency Response Team / Группа/группы реагирования на компьютерные чрезвычайные ситуации

CSIRT/CSIRTs — Computer Security Incident Response Team /Группа/группы реагирования на инциденты информационной безопасности

GCI — Global Cyber Security Index / Глобальный индекс кибербезопасности

GDPR — General Data Protection Regulation / Общий регламент безопасности данных ЕС

IEC — International Electrotechnical Commission / Международная электротехническая комиссия

ITU — International Telecommunication Union / Международный союз электросвязи

ISO — International Organization for Standardization / Международная организация по стандартизации

ISOCs — Information Security Operation Centers / Операционные центры информационной безопасности (отраслевые)

MENA — Middle East and North Africa / Регион Ближнего Востока и Северной Африки

PKI — Public Key Infrastructure / Инфраструктура открытых ключей

VPN — Virtual private network / Виртуальная персональная сеть

ОСОБЕННОСТИ ПОЛИТИКИ ГОСУДАРСТВ-УЧАСТНИКОВ БРИКС В СФЕРЕ РАЗВИТИЯ ИКТ, ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ И МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Подписано в печать 14.05.2024. Гарнитура Times.
Формат 60x84/8. Объем 46.97 усл. печ. л.
Тираж 200 экз.