

Перспективы сотрудничества России и ОАЭ в области обеспечения информационной безопасности

© Хайруллин Т.Р.^{a,b,c,f}, Шелковников А.И.^{d,g}, Симбирцев Е.Д.^{e,h}, 2025

^a Институт Африки РАН

^b Финансовый университет при Правительстве РФ, Москва, Россия

^c СПбГУ, Санкт-Петербург, Россия

^d НИУ ВШЭ, Москва, Россия

^e РУДН им. Патриса Лумумбы

^f ORCID: 0000-0001-5418-2792; jumglaw16@yandex.ru

^g ORCID: 0000-0002-1630-0310; andyshelk68@gmail.com

^h ORCID: 0009-0000-7548-794X; 1132221920@pfur.ru

Резюме. В статье рассматриваются перспективы сотрудничества России и Объединенных Арабских Эмиратов (ОАЭ) в области обеспечения информационной безопасности. Выяснено, что данное сотрудничество является частью более широкого взаимодействия, нашедшего правовое закрепление в Декларации о стратегическом сотрудничестве от 1 июня 2018 г.

Успех ОАЭ в области развития информационных технологий и обеспечения информационной безопасности связан с устойчивым экономическим ростом, обеспечившим необходимый приток технологий и высококвалифицированных специалистов. Однако, несмотря на то, что оба государства объявили о намерении сотрудничать, а также совместно противодействовать киберугрозам, на деле произошло заметное замедление реализации заявленных проектов. Отчасти это связано с наличием внешних и внутренних проблем в России и в ОАЭ. Так, развитие российского сегмента информационных технологий было замедлено масштабным санкционным давлением последних лет. В свою очередь, ОАЭ географически находятся в нестабильном регионе, где, наряду с угрозой религиозного терроризма и экстремизма, растет число хакерских атак. В этой связи сотрудничество России и ОАЭ является важным аспектом в рамках международной кооперации. В статье приводятся практические рекомендации по повышению уровня сотрудничества в области обеспечения информационной безопасности на фоне активного внедрения в жизнь искусственного интеллекта.

Ключевые слова: Россия, ОАЭ, кибербезопасность, информационная безопасность, искусственный интеллект, новые технологии

Благодарность. Работа выполнена при поддержке СПбГУ, шифр проекта 116471555.

Для цитирования: Хайруллин Т.Р., Шелковников А.И., Симбирцев Е.Д. Перспективы сотрудничества России и ОАЭ в области обеспечения информационной безопасности. *Азия и Африка сегодня*. 2025. № 7. С. 37–46.
DOI: 10.31857/S0321507525070022

Prospects for Cooperation between Russia and the UAE in the Field of Information Security

© Timur R. Khayrullin^{a,b,c,f}, Andrey I. Shelkovnikov^{d,g}, Egor D. Simbirtsev^{e,h}, 2025

^a Institute for African Studies, Russian Academy of Sciences, Moscow, Russia

^b Financial University under the Government of the Russian Federation; Moscow, Russia

^c Saint-Petersburg State University, Saint Petersburg, Russia

^d HSE University, Moscow, Russia

^e Patrice Lumumba RUDN University, Moscow, Russia

^f ORCID: 0000-0001-5418-2792; jumglaw16@yandex.ru

^g ORCID: 0000-0002-1630-0310; andyshelk68@gmail.com

^h ORCID: 0009-0000-7548-794X; 1132221920@pfur.ru

Abstract. The article discusses the prospects of cooperation between Russia and the United Arab Emirates (UAE) in information security. This cooperation is part of broader interactions that were legally consolidated in the June 1, 2018

Declaration on Strategic Cooperation. The UAE's success in information technology and security is related to sustained economic growth, which has provided the necessary technology and highly qualified specialists. However, despite both states announcing their intention to cooperate and jointly counter cyber threats, there has been a noticeable slowdown in implementing the announced projects. This is partly due to external and internal issues in Russia and the UAE. For example, the development of Russia's information technology sector has slowed due to large-scale sanctions and the consequences of the financial and economic crisis in recent years. In turn, the UAE is located in an unstable region where religious terrorism and extremism pose a threat, and the number of hacker attacks is growing.

Keywords: Russia, UAE, cybersecurity, information security, artificial intelligence, new technologies

For citation: Khayrullin T.R., Shelkovnikov A.I., Simbirtsev E.D. Prospects for Cooperation between Russia and the UAE in the Field of Information Security. *Asia and Africa today*. 2025. № 7. Pp. 37–46. (In Russ.). DOI: 10.31857/S03215075 25070022

ВВЕДЕНИЕ

Стремительная реконфигурация международных отношений на Ближнем Востоке, связанная в т.ч. с ростом влияния таких игроков, как Саудовская Аравия, Иран, Катар, ОАЭ, открывает перед Россией новые возможности в деле выстраивания конструктивного диалога с ключевыми государствами региона. И здесь российско-эмиратские отношения являются одними из самых динамично развивающихся. В их основе лежит сотрудничество в целом ряде ключевых отраслей, таких как инвестиции, торговля, энергетика, информационные и передовые технологии и т.д. Являясь крупными производителями и экспортерами нефти, Россия и ОАЭ понимают важность сохранения сбалансированности мирового энергетического рынка и стремятся развивать взаимовыгодное сотрудничество как в традиционной, так и в «зеленой» энергетике.

По мере развития инновационных и информационных технологий, необходимость в обеспечении безопасности от киберугроз стала приобретать особую актуальность. Поэтому важным направлением сотрудничества между Москвой и Абу-Даби стало совместное «содействие обеспечению безопасного и мирного киберпространства...», нашедшее правовое закрепление в Декларации от 1 июня 2018 г. о стратегическом сотрудничестве между Россией и ОАЭ¹. Кроме того, оба государства в рамках Декларации запланировали запустить совместные исследовательские проекты, направленные на защиту критической инфраструктуры от кибератак, что позволит укрепить устойчивость цифровых систем². В сегодняшних реалиях активного развития технологии искусственного интеллекта обеспечение информационной безопасности выходит на передний план как внутри отдельных государств, так и на межгосударственном уровне [1]. Важным этапом в деле укрепления российско-эмиратских отношений стало вхождение ОАЭ в БРИКС 1 января 2024 г. на фоне председательства Москвы в организации.

ОАЭ КАК ПОТЕНЦИАЛЬНЫЙ ПАРТНЕР В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

С учетом стратегического партнерства успехи ОАЭ в области передовых технологий и защиты данных могли бы иметь теоретический и практический интерес для России. Успехам Эмиратов способствуют отсутствие санкционного давления, наличие устойчивого экономического роста (за исключением кратковременного спада в период пандемии *COVID-19*) и, как следствие, благоприятный инвестиционный климат [4]. На государственном уровне поддерживается развитие цифровой экосистемы, что приводит к росту цифровой экономики и большей зависимости от данных. В итоге информационное пространство Эмиратов регулярно подвергается киберугрозам. Согласно отчетам *Kaspersky Lab* и *DarkMatter*, на долю ОАЭ в 2019 г. приходилось 5% всех глобальных кибератак [5]. Между тем с первой половины 2023 г. по первую половину 2024 г. в ОАЭ произошло резкое снижение числа *DoS*-атак (кибератак)³ – с 58 538 до 2301⁴. Во многом это связано с тем, что ОАЭ активно развивают систему противо-

¹ Декларация о стратегическом партнерстве между Российской Федерацией и Объединенными Арабскими Эмиратами. 01.06.2018. <http://kremlin.ru/supplement/5309> (accessed 30.11.2024)

² Там же.

³ *DoS*-атака (от англ. *denial-of-service attack* – «отказ в обслуживании») – хакерская атака на вычислительную систему с целью довести ее до отказа, т.е. создание таких условий, при которых добросовестные пользователи системы не смогут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ будет затруднен (*прим. авт.*).

действия киберугрозам и поддержки информационной безопасности, принимая комплексные законодательные и организационные меры для защиты цифрового пространства⁵.

Кроме того, ОАЭ сосредоточились на создании мощной технологической инфраструктуры в области кибербезопасности с помощью новых совместных и партнерских проектов. Немаловажным аспектом здесь является предоставление Эмиратами иностранным специалистам широких возможностей для раскрытия своего потенциала. Приток высококвалифицированных специалистов во многом обеспечил ОАЭ возможность осуществить технологический рывок.

Уже в 2017 г. в Дубае была принята первая стратегия кибербезопасности – *Dubai Cyber Security Strategy*. Она стала скорее результатом деятельности в том же году первого на Ближнем Востоке Министерства искусственного интеллекта [1]. Этот документ фактически повлиял на дальнейшее государственное планирование в области информационной безопасности. Приоритетными направлениями стратегии Дубая стали обеспечение комплексной защиты от угроз киберпространства, поддержка инноваций в киберпространстве, а также его экономическое процветание. Стратегия была направлена на реализацию 5 основных направлений: умная с точки зрения цифровых технологий нация, инновационность, кибербезопасность, киберустойчивость, а также национальное и международное сотрудничество. Отметим, что другим важным результатом деятельности Министерства искусственного интеллекта стало принятие в 2017–2018 гг. Национальной стратегии в области искусственного интеллекта (ИИ) до 2031 г., согласно которой ОАЭ должны стать к указанному году мировым лидером в области ИИ. Эта цель согласуется с более масштабной и амбициозной задачей страны – стать к 2071 г. лучшей страной в мире. Согласно данной стратегии ОАЭ стремятся повысить конкурентоспособность в приоритетных секторах за счет внедрения ИИ, создать благоприятную экосистему для ИИ, внедрить ИИ в сферу обслуживания, привлечь мировой опыт применения ИИ⁶. Однако вернемся к проблеме кибербезопасности.

Принятие первой стратегии кибербезопасности именно в эмирате Дубай неслучайно. Данный эмират в связке с эмиратом Абу-Даби является локомотивом развития ОАЭ. Традиционно Дубай славился своей торговой предприимчивостью и наличием купеческих кланов, превратившихся впоследствии в экономическую элиту государства [6]. В свою очередь, Абу-Даби отличался доминированием военно-административных элит и представлял собой политико-административный центр, центр консолидации силовых и управленческих кадров. Неслучайно правитель Абу-Даби – президент, в то время как правитель Дубая – вице-президент, а также премьер-министр. Более того, оказание эмиратами помощи друг другу в критических ситуациях обеспечило процветание и экономический рост федерации [4]. Поэтому неудивительно, что на региональном уровне вторым эмиратом, принявшим стратегию кибербезопасности, был Абу-Даби.

Подчеркнем, что важность информационной безопасности осознается в ОАЭ на самом высоком уровне. Так позицию Эмиратов по этому вопросу прояснил премьер-министр ОАЭ и эмир Дубая Мохаммед бин Рашид Аль Мактум: «Наши границы в киберпространстве – это политические границы, которые нам всегда нужно защищать и укреплять их оборону» [7]. Такое восприятие объясняет высокую приоритетность информационной безопасности в современной политике ОАЭ и эмирата Дубай в частности. Отметим, что в 2023 г. стратегия кибербезопасности Дубая была обновлена, а в ее основу легли 4 основных принципа: кибербезопасное общество (содействие доступности кибербезопасности и развитию кибернавыков), город-инкубатор инноваций (продвижение исследований в области информационной безопасности), устойчивый цифровой город (расширение цифровой экосистемы и управления цифровым пространством) и активное цифровое сотрудничество (сотрудничество на локальном и международном уровне по противодействию угрозам и развитию цифровой среды)⁷.

⁴ UAE Cyber Security Council, CPX unveil Cybersecurity Report 2025.

⁵ В преддверии перехода ОАЭ к «правительству ИИ» киберпандемия ускорила цифровую трансформацию: руководитель службы кибербезопасности. 27.09.2021. <https://wam.ae/en/article/hszrd5e6-%D0%BF%D1%80%D0%B5%D0%B4%D0%B2%D0%B5%D1%80%D0%B8%D0%B8-%D0%BF%D0%B5%D1%80%D0%B5%D1%85%D0%BE%D0%B4%D0%B0-%D0%B%D0%B0%D1%8D-...> (accessed 30.11.2024)

⁶ The UAE National Strategy for Artificial Intelligence 2031. 2018. <https://ai.gov.ae/wp-content/uploads/2021/07/UAE-National-Strategy-for-Artificial-Intelligence-2031.pdf> (accessed 07.06.2025)

⁷ Dubai Cyber Security Strategy – Updated. 07.11.2023. <https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/government-services-and-digital-transformation/dubai-cyber-security-strategy> (accessed 21.02.2025)

Примечательно, что часть этих принципов сохранила свою редакцию из предыдущей версии 2017 г. Стратегию запустил наследный принц эмирата Дубай и председатель Исполнительного совета эмирата Хамдан бин Мохаммед Аль Мактум, который подчеркнул изменчивый характер угроз безопасности, на противодействие которым в том числе направлена стратегия: «Учитывая постоянно меняющиеся проблемы и риски, крайне важно продолжать уделять первостепенное внимание развитию кибербезопасности. Чтобы быть в курсе быстрых изменений и новых тенденций, требуются гибкость, инновации, активность и повышенная цифровая осведомленность»⁸.

В то же время стратегические документы в этой области стали принимать и на уровне других эмиратов. К примеру, в ноябре 2020 г. Исполнительный комитет Абу-Даби одобрил стратегию кибербезопасности для правительства эмирата, направленную на создание безопасной и защищенной киберсреды, соответствующей лучшим международным практикам⁹.

Стратегия кибербезопасности эмирата Дубай не только стала первым примером стратегического планирования в Эмиратах, но и подтолкнула к формированию стратегических документов на федеральном уровне. Уже в 2019 г. была принята первая редакция Национальной стратегии кибербезопасности с обязательством обновлять ее в последующие годы¹⁰. Основной целью национальной стратегии было заявлено формирование безопасной и устойчивой цифровой инфраструктуры в ОАЭ, которая позволила бы гражданам реализовать свои стремления и дала бы возможность бизнесу процветать. В рамках реализации стратегии планировалось мобилизовать всю экосистему для реализации более 60 инициатив по 5 основным направлениям: законы и регулирование цифровой безопасности; развитая экосистема цифровой безопасности; национальный план реагирования на цифровые инциденты; политика защиты критической информационной инфраструктуры; партнерство и сотрудничество. Важным направлением в осуществлении стратегии стали планы по подготовке компетентных кадров, готовых к эффективной работе в области информационной безопасности. В рамках стратегии планировалось обучить более 40 тыс. местных специалистов по цифровой и информационной безопасности.

Хотя первую национальную стратегию по обеспечению кибербезопасности разрабатывало и вводило Управление по регулированию телекоммуникаций, дальнейшая деятельность по обеспечению информационной и цифровой безопасности была поручена новому органу, которым стал Совет по кибербезопасности, созданный в ноябре 2020 г. Одной из главных задач Совета остается выработка политики и установление стандартов¹¹ для обеспечения защиты от кибератак, а также обеспечение готовности всех секторов к эффективному реагированию на чрезвычайные ситуации в области информационной безопасности [8].

Деятельностью Совета с 2020 г. руководит глава Службы кибербезопасности правительства Мохаммед Хамад Аль-Кувейти, имеющий мандат управляющего директора Национального центра данных при Верховном совете национальной безопасности, а также исполнительного директора Агентства радиотехнической разведки. Руководитель Совета по кибербезопасности – один из наиболее влиятельных людей в стране в области обеспечения информационной безопасности.

На базе Совета в 2023 г. был запущен и действует Национальный центр цифровой безопасности. Центр функционирует как центральный узел мониторинга и реагирования на киберугрозы. Он собирает данные из секторальных центров безопасности, обеспечивая обнаружение и управление инцидентами в режиме реального времени. Подобные инициативы особенно важны для оперативного реагирования на угрозы, снижения негативного влияния и последствий цифровых атак и демонстрируют высокий прикладной уровень развития направления в стране.

Последняя редакция национальной стратегии была разработана Советом по кибербезопасности ОАЭ и принята Кабинетом министров в начале февраля 2025 г.¹² Срок действия новой стратегии составит

⁸ Hamdan bin Mohammed launches second cycle of Dubai Cyber Security Strategy. 12.07.2023. <https://www.wam.ae/en/details/1395303176784> (accessed 21.02.2025)

⁹ Executive Committee approves a strategy for Abu Dhabi government cyber security. 05.11.2020. <https://www.wam.ae/en/details/1395302883894> (accessed 30.11.2024)

¹⁰ National Cybersecurity strategy 2019. 13.02.2024. <https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/strategies-plans-and-visions-until-2021/national-cybersecurity-strategy-2019#:~:text=The%20UAE's%20National%20Cybersecurity%20strategy,and%20empowers%20businesses%20to%20thrive> (accessed 30.01.2025)

¹¹ Cyber Security Council. 01.03.2025. <https://csc.gov.ae/en/about> (accessed 30.11.2024)

¹² <https://uaecabinet.ae/en/news/uae-cabinet-approves-national-cybersecurity-strategy-api-first-policy> (accessed 21.02.2025)

5 лет. Новая стратегия основана на 5 центральных принципах, каждый из которых направлен на достижение нескольких национальных целей: управление, достижимое путем создания эффективной структуры администрирования цифровой безопасности; защита через обеспечение безопасной, устойчивой и надежной цифровой среды; инновации, направленные на быстрое и безопасное внедрение инновационных механизмов; усиление и развитие потенциала для расширения национальных возможностей в области цифровизации и кибербезопасности; партнерство и сотрудничество, направленное на укрепление партнерских отношений как на национальном, так и на международном уровне для достижения целей ОАЭ в области кибербезопасности¹³.

Деятельность ОАЭ по обеспечению информационной безопасности не ограничивается разработкой стратегических планов. ОАЭ активно принимают стандарты обеспечения цифровой безопасности для государственных учреждений и рассматривают цифровое страхование как способ смягчения и реагирования на цифровые риски. Руководство страны также проводит реформирование законодательства, осуществляет подготовку институтов и кадров. 2 января 2022 г. в ОАЭ вступил в силу Федеральный указ № 34 от 2021 г., который укрепил законодательные меры по защите от киберугроз и киберпреступлений, совершаемых с использованием информационных технологий, сетей и платформ. Этот закон охватывает ключевые аспекты, такие как защита данных, противодействие кибератакам и распространению ложной информации, регулирует наказания за хакерские атаки на государственные и коммерческие системы (в частности, предусмотрены большие штрафы и тюремные сроки, особенно если атаки затрагивают критическую инфраструктуру). Также закон вводит жесткие наказания за нарушение конфиденциальности персональных данных и за взлом финансовых и коммерческих систем¹⁴.

В сентябре 2024 г. была запущена комплексная программа в рамках инициативы *Cyber Sniper*, направленная на повышение квалификации государственных служащих ОАЭ в области кибербезопасности¹⁵. Инициатива была организована Советом по кибербезопасности ОАЭ совместно с Федеральным управлением правительства по кадрам и реализуется ведущими международными партнерами по кибербезопасности (*SANS, EC-Council, Offsec* и *CyberGate Defense*). Руководитель Совета по кибербезопасности ОАЭ М.Х.Аль-Кувейти заявил, что в настоящее время Совет занимается разработкой новых стратегий для поддержки системы кибербезопасности страны. Эти стратегии направлены на укрепление позиций ОАЭ как глобального центра передовых технологий и искусственного интеллекта. Он отметил, что исполнительные положения для закона о шифровании, который устанавливает основные стандарты для обеспечения безопасности передачи данных с помощью квантовых систем, находятся на финальной стадии внедрения¹⁶.

В феврале 2025 г. Совет по кибербезопасности ОАЭ, Управление по закупкам в сфере обороны и безопасности ОАЭ (*Tawazun*) и американская военно-промышленная корпорация *Lockheed Martin* подписали письмо о намерениях с целью создания современного Центра передового опыта в области кибербезопасности¹⁷. Планируется, что Центр будет сосредоточен на проведении передовых исследований, специализированном обучении и отраслевом сотрудничестве. Центр нацелен на продвижение передачи знаний и инновационных решений для укрепления устойчивости кибербезопасности. Это очередной шаг в повышении эффективности местных специалистов, способных самостоятельно защищать жизненно важную инфраструктуру страны.

Согласно отчету Глобального индекса кибербезопасности (*Global Cybersecurity Index (GCI)*)¹⁸ за 2024 г., ОАЭ занимают лидирующие позиции¹⁹. Так, по всем 5 основным категориям оценивания

¹³ <https://csc.gov.ae/discover-csc> (accessed 21.02.2025)

¹⁴ الإلكترونية والجرائم الشائعات مكافحة بشأن بقانون مرسوم . 02.01.2022. <https://uaelegislation.gov.ae/ar/legislations/1526> (accessed 30.11.2024)

¹⁵ UAE's Cyber Sniper initiative continues developing government employees' knowledge, skills. 07.09.2024. <https://www.wam.ae/en/article/b52fjvs-uaes-cyber-sniper-initiative-continues-developing> (accessed 30.11.2024)

¹⁶ UAE to issue 3 new policies to boost cybersecurity by end of 2024: Cybersecurity Council Chairman. 27.07.2024. <https://www.wam.ae/en/article/141cc1n-uae-issue-new-policies-boost-cybersecurity-end> (accessed 30.11.2024)

¹⁷ IDEX 2025: UAE to establish Cybersecurity Centre of Excellence. 18.02.2025. <https://www.wam.ae/en/article/bi9jgsd-index-2025-uae-establish-cybersecurity-centre> (accessed 30.01.2025)

¹⁸ Глобальный индекс кибербезопасности (*GCI*) измеряет приверженность стран кибербезопасности на глобальном уровне. Поскольку кибербезопасность имеет широкую сферу применения, охватывающую многие отрасли и различные секторы, уровень развития или вовлеченности каждой страны оценивается по 5 основным направлениям: (1) правовые меры,

(«правовое обеспечение», «организационные меры», «техническое обеспечение», «развитие потенциала», «международная кооперация») были достигнуты максимальные показатели – 20 баллов из 20. Кроме того, ОАЭ планируют сохранить за собой лидирующие позиции в данной сфере. Так, в 2025 г. Эмираты объявили о выделении более \$2 млрд на развитие кибербезопасности и цифровой экосистемы²⁰. При этом в ОАЭ уже разработана федеральная сеть с общей инфраструктурой, которая обеспечивает взаимосвязь и обмен данными между местным и национальным уровнями. Она опирается на многоуровневую среду безопасности, которая обеспечивает сохранность шифрования информации по нескольким протоколам, снижая угрозы от киберпреступлений за счет минимизации уязвимостей.

Отметим, что ОАЭ рассматривают информационную безопасность как одно из важнейших, стратегических направлений в современном все более цифровизированном мире, усилия по укреплению которой могут оказывать позитивное влияние не только на государственном, но и на индивидуальном и организационном уровнях отдельных предприятий, содействуя их экономическому процветанию. Для ОАЭ развитие сильного национального цифрового потенциала необходимо для укрепления суверенитета и реализации идей превращения в международный цифровой центр. Поощряя инициативы по подготовке новых специалистов, деятельность бизнес-структур в области информационной безопасности, Эмираты стремятся создать основу для обеспечения цифрового суверенитета.

Несмотря на серьезные успехи в области обеспечения информационной безопасности, Эмираты сталкиваются с рядом трудностей: в стране, особенно в Дубае, наблюдается дефицит ИТ-специалистов, что обусловлено быстрым ростом технологической индустрии. Особенно актуален дефицит в таких областях, как разработка программного обеспечения, кибербезопасность, аналитика данных и облачные технологии. Цифровое пространство в ОАЭ характеризуется строгими правилами и ограничениями, особенно касающимися услуг связи и доступа к информации.

Кроме того, в последние годы в стране наблюдалось определенное замедление темпов экономического роста, отчасти из-за сокращения добычи нефти в рамках соглашений ОПЕК, продолжающейся корпоративной реструктуризации, сокращения государственных инвестиций и снижения цен на недвижимость. Внешние факторы также включают замедление мировой экономики, геополитическую напряженность, снижение спроса на энергоносители и пандемию *COVID-19*. Тем не менее в 2022 г. страна вернулась к устойчивому росту, чему способствовал сильный подъем туризма, строительства и деятельности, связанной со Всемирной выставкой в Дубае, а также рост добычи нефти. Цены на нефть, поддерживаемые на достаточно высоком уровне благодаря действиям ОПЕК+, обеспечивают высокие профициты бюджетного и внешнего балансов [10].

ИНИЦИАТИВЫ И ПРАКТИЧЕСКИЕ АСПЕКТЫ СОТРУДНИЧЕСТВА ОАЭ И РФ

На международном треке Россия с 1998 г. инициативно выступает за развитие сотрудничества в области обеспечения информационной безопасности как на региональном, так и на глобальном уровне, а также за адаптацию международного права к особенностям информационной сферы [2]. Еще в 2013 г. в документе «Основы государственной политики в области международной информационной безопасности на период до 2020 г.» Россия добавила к триаде угроз опасность вмешательства во внутренние дела суверенного государства посредством ИКТ²¹; нарушение общественной стабильности; разжигание межэтнической, межнациональной розни²². По сути, это стало реакцией России на события «арабской весны», когда социальные сети и блоги активно использовались для координации протестного движе-

(2) технические меры, (3) организационные меры, (4) развитие потенциала и (5) сотрудничество, а затем суммируется в общую оценку (*прим. авт.*).

¹⁹ Global Cybersecurity Index. 01.03.2025. <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx> (accessed 12.03.2025)

²⁰ UAE to launch National Cybersecurity Strategy. 11.02.2025. <https://www.wam.ae/en/article/bi5dfsr-uae-launch-national-cybersecurity-strategy> (accessed 30.01.2025)

²¹ ИКТ – информационно-коммуникационные технологии (*прим. авт.*).

²² Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. 01.08.2013. <http://www.scrf.gov.ru/documents/6/114.html> (accessed 30.11.2024)

ния [2]. С тех пор Россия активно работает над развитием ИТ-технологий и обеспечением информационной безопасности.

Согласно отчету Глобального индекса кибербезопасности (*Global Cybersecurity Index (GCI)*) за 2024 г., Россия занимает прочные позиции по всем 5 основным категориям оценивания²³. Так, в категориях «правовое обеспечение» и «организационные меры» достигнуты максимальные показатели – 20 баллов из 20, в то время как в остальных категориях еще необходимо расти: «техническое обеспечение» – 16,59; «развитие потенциала» – 18,77; «международная кооперация» – 16,77. Максимальные показатели по 3 критериям пока не достигнуты во многом из-за последствий продолжающегося финансово-экономического кризиса и крупномасштабной санкционной политики стран Запада в отношении России.

ОАЭ заинтересованы в активизации международного сотрудничества, понимая, что угрозы в информационной сфере эволюционируют гораздо быстрее, чем находятся решения по противодействию им. По словам главы Совета по кибербезопасности ОАЭ Мохаммеда Аль-Кувейти, Эмираты должны сохранять бдительность в области информационной безопасности, поддерживая высокий уровень взаимодействия и сотрудничества: «Поскольку мы стоим на пороге новой эры, основанной на новых технологиях, рост числа атак с использованием искусственного интеллекта и расширение кибервозможностей требуют большей бдительности для обеспечения безопасности будущего. Путь вперед требует международного сотрудничества, инноваций и приверженности. Вместе мы продолжим строить безопасные и процветающие цифровые ОАЭ, где процветают инновации, возможности, а наши системы остаются устойчивыми перед лицом любых вызовов»²⁴.

Одним из шагов на пути к реализации заключенных соглашений стал запуск в 2019 г. образовательной программы по защите критической информационной инфраструктуры и обучению этичному хакингу. Официальное представительство российской группы компаний *InfoWatch* на Ближнем Востоке (*InfoWatch Gulf*) занимается подготовкой специалистов из ОАЭ в области информационной безопасности. Проект включает обучающие программы, курсы и тренинги по информационной безопасности и предотвращению утечек данных, направленные на повышение цифровых компетенций специалистов и руководителей организаций ОАЭ, а также обучение школьников и студентов основам киберграмотности²⁵. Этот проект способствует не только приобретению полезных цифровых навыков в ОАЭ, но и укреплению партнерских связей между двумя странами в сфере цифровой безопасности благодаря участию российских экспертов, которые проводят обучение и разрабатывают учебные программы для подготовки специалистов в области информационной безопасности.

Еще одним значимым достижением в рамках сотрудничества стало открытие Российского центра цифровых инноваций и ИКТ (*Russian Centre of Digital Innovation & ICT*) в Дубае в 2019 г. при поддержке Министерства цифрового развития, связи и массовых коммуникаций России. Центр, расположенный в *Dubai Internet City*, в Минкомсвязи называли «трамплином» для российских компаний, работающих в области информационной безопасности, искусственного интеллекта и облачных технологий²⁶. Однако, несмотря на высокие ожидания, произошло свертывание работы Центра из-за пандемии *COVID-19* и последующих геополитических изменений²⁷.

Важным событием стала первая международная онлайн-конференция «День технологий России и ОАЭ», организованная 23 июня 2020 г. при поддержке *Tech Global*²⁸, Министерства связи России и На-

²³ Global Cybersecurity Index. 01.03.2025...

²⁴ UAE Cyber Security Council, CPX unveil Cybersecurity Report 2025.

²⁵ Россияне обучат информационной безопасности жителей ОАЭ. 01.09.2019. <https://rg.ru/2019/01/09/rossiane-obuchat-informacionnoj-bezopasnosti-zhitelej-uae.html> (accessed 30.11.2024)

²⁶ Российский центр цифровых инноваций открылся в Дубае. 01.03.2025. <https://digital.gov.ru/ru/events/39146/#:~:text=%D0%94%D1%83%D0%B1%D0%B0%D0%B9%2C%2021%20%D0%B8%D1%8E%D0%BD%D1%8F%202019%20%D0%B3%D0%BE%D0%B4%D0%B0,%D1%86%D0%B5%D0%BD%D1%82%D1%80%20%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D1%8B%D1%85%20%D0%B8%D0%BD%D0%BD%D0%BE%D0%B2%D0%B0%D1%86%D0%B8%D0%B9%20%D0%B8%20%D0%98%D0%9A%D0%A2.> (accessed 30.11.2024)

²⁷ Running in parallel, the Russian startup ecosystem in Dubai. *Wamda*. <https://www.wamda.com/2023/05/running-parallel-russian-startup-ecosystem-dubai> (accessed 02.05.2025)

²⁸ *Tech Global* – международный бренд, под которым российский государственный инвестиционный фонд АО «Росинфокоминвест» реализует проекты за рубежом.

циональной компьютерной корпорации ОАЭ. Очевидным результатом совместных усилий стало соглашение о совместном предприятии²⁹, подписанное в июне 2023 г. компанией *Omega.Future*, отечественным разработчиком ИТ-решений для цифровой трансформации правительства и бизнеса, и *Sinaha*, крупнейшей на Ближнем Востоке платформой электронной коммерции и маркетинга. Соглашение предусматривает строительство завода в Абу-Даби по производству 3D-принтеров и образовательных роботов [3]. Однако официальных публикаций и анонсов о реализации соглашения в открытых источниках не встречается.

В 2020 г. Россия и ОАЭ разделили 5-е место в рейтинге кибербезопасности *Global Cybersecurity Index*³⁰. Кроме того, обе страны подчеркивают значимость обеспечения кибербезопасности и совершенствования правовых основ сотрудничества, что подтверждается активным участием обеих сторон в международных дискуссиях о нормах и стандартах в сфере информационной безопасности.

В последние несколько лет российские вузы (Казанский федеральный университет, Московский физико-технический институт) активно сотрудничают с ведущим эмиратским Университетом науки и технологий Халифы³¹. В январе 2024 г. на базе этого вуза при содействии Совета по кибербезопасности ОАЭ была открыта Академия кибербезопасности Университета Халифа, которая предлагает комплексные программы сертификации и обучения на английском и арабском языках, обучая и сертифицируя частных лиц, студентов, компании и организации по вопросам цифровой безопасности³². Кроме того, рабочие группы из России и ОАЭ регулярно участвуют в профильных международных форумах и конференциях, посвященных защите данных и киберугрозам³³.

ЗАКЛЮЧЕНИЕ

Сотрудничество России и ОАЭ в области обеспечения информационной безопасности закреплено в Декларации от 1 июня 2018 г. о стратегическом сотрудничестве. Кроме того, оба государства осознают партнерский характер взаимодействия, основанного на понимании необходимости кооперации и обмена опытом в деле укрепления цифрового суверенитета. Однако в практической плоскости сотрудничество в данной области ограничено и требует пересмотра его методов и тактик. В частности, России и ОАЭ необходимо активнее развивать совместные инициативы, направленные на повышение цифровой безопасности, защиту критической инфраструктуры и подготовку квалифицированных специалистов. Сотрудничество в данном направлении становится все более актуальным из-за возрастающих угроз как для России, так и для ОАЭ.

В условиях развития передовых технологий перспективными направлениями более тесного сотрудничества могли бы стать совместное обучение ИТ-специалистов по программам двойных дипломов с последующей стажировкой, поддержка молодежных инициатив по разработке и продвижению инновационных технологий, выделение исследовательских грантов, поддержка стартапов, проведение регулярных конкурсов и соревнований в области кибербезопасности. Данные направления тесно связаны с успехами сотрудничества в торгово-экономической и инвестиционной сферах. Вхождение ОАЭ в январе 2024 г. в БРИКС, где Россия играет ведущую роль, могло бы укрепить сотрудничество между государствами. Приток инвестиций БРИКС в экономику ОАЭ может привести к реализации совместных инфраструктурных проектов, в т.ч. с участием российских компаний.

Российский сегмент передовых технологий продолжает сталкиваться с санкционным давлением в рамках глобального противостояния с коллективным Западом, а также с последствиями финансово-эко-

²⁹ <https://spbit.ru/news/IT-kompaniya-Omega-Future-otkroyet-v-OAE-proizvodstvo-3D-printerov-i-robototekhniki-274175> (accessed 12.03.2025)

³⁰ Global Cybersecurity Index 2020. 01.01.2020. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (accessed 30.11.2024)

³¹ <https://ku.ac.ae/ku-and-moscow-power-engineering-institute-sign-mou-on-research-partnership-and-long-term-collaboration>; <https://trade-house-rus-uae.com/ru/a/pri-sodeystvii-delovoy-rossii-sostoyalos-podpisanie-soglasheniya-o-sotrudnichestve-mezhdu-mfti-universitetom-halifa-i-mkc-for-power-solutions>

³² <https://www.ku.ac.ae/khalifa-university-cybersecurity-academy-inaugurated> (accessed 21.02.2025)

³³ Глава *InfoWatch Gulf* приняла участие в Восьмом заседании Межправительственной Российско-Эмиратской комиссии по торговому, экономическому и научно-техническому сотрудничеству. 11.07.2018. <https://www.infowatch.ru/company/presscenter/news/20573> (accessed 30.11.2024)

номического кризиса. В свою очередь, ОАЭ географически находятся в нестабильном регионе, где, наряду с угрозой религиозного терроризма и экстремизма, растет число хакерских атак [9]. Это вынуждает ОАЭ использовать многосторонний подход для обеспечения информационной безопасности, обеспечивая защиту критической информационной инфраструктуры, разрабатывая и внедряя новые элементы законодательства, содействуя инвестициям в повышение квалификации местных кадров в области кибербезопасности.

Позиции ОАЭ как одного из мировых лидеров в обеспечении информационной безопасности отражают долгосрочные цели и текущую политику государства. Вместе с тем изучение опыта Эмиратов в данном направлении становится необходимым и привлекательным.

На фоне роста кибератак, связанных в том числе с высоким уровнем геополитической напряженности и соперничества между глобальным и региональными игроками, партнерство между Россией и ОАЭ в области обеспечения информационной безопасности имеет большой потенциал для дальнейшего развития.

ЛИТЕРАТУРА / REFERENCES

1. Пашенцев Е.Н., Чебыкина В.А. Злонамеренное использование искусственного интеллекта и угрозы информационно-психологической безопасности в Объединенных Арабских Эмиратах. *Восток (Oriens)*. 2024. № 6. С. 107–117. DOI: 10.31696/S086919080032578-2
Pashentsev E.N., Chebykina V.A. 2024. Malicious Use of Artificial Intelligence and Threats to Information and Psychological Security in the United Arab Emirates. *Vostok (Oriens)*. № 6. Pp. 107–117. DOI: 10.31696/S086919080032578-2
2. Зиновьева Е.С. Международное сотрудничество по обеспечению информационной безопасности. *Право и управление. XXI век*. 2014. № 4 (33), с. 44–52.
Zinovieva E.S. 2014. International cooperation for information security. *Journal of Law and Administration*. № 4 (33). Pp. 44–52.
3. Matveev I. Russia and the UAE: An Outlook for Cooperation in High Technologies. 18.01.2024. <https://russian-council.ru/en/analytics-and-comments/analytics/russia-and-the-uae-an-outlook-for-cooperation-in-high-technologies/> (accessed 21.02.2025)
4. Хайруллин Т.Р., Коротаев А.В. ОАЭ в борьбе за региональное лидерство. *Азия и Африка сегодня*. 2023. № 9. С. 27–35. DOI: 10.31857/S032150750027592-3
Khayrullin T.R., Korotayev A.V. 2023. UAE in the Struggle for Regional Leadership. *Asia and Africa today*. № 9. Pp. 27–35. (In Russ.). DOI: 10.31857/S032150750027592-3
5. Chandra G.R., Sharma B.K., Liaqat I.A. 2019. UAE's Strategy Towards Most Cyber Resilient Nation. *International Journal of Innovative Technology and Exploring Engineering*. Vol. 8. № 12. Pp. 2803–2809. DOI: 10.35940/ijitee.L3022.1081219
6. Efthymiopoulos M.P. 2016. Cyber-security in smart cities: the case of Dubai. *Journal of Innovation and Entrepreneurship*. Vol. 5. Pp. 1–16. DOI: 10.1186/s13731-016-0036-x
7. Forster S. Sheikh Mohammed bin Rashid announces five-year budget for UAE. 12.10.2021. <https://thenationalnews.com/uae/government/2021/10/12/sheikh-mohammed-bin-rashid-announces-five-year-budget-for-uae/> (accessed 21.02.2025)
8. Хома В.С. Основные направления цифровизации экономики в ОАЭ. *Российский внешнеэкономический вестник*. 2023. № 7. С. 115–126.
Khoma V.S. 2023. The Main Areas of Digitalization of the UAE's Economy. *Russian Foreign Economic Journal*. № 7. Pp. 115–126.
9. Валиахметова Г.Н., Цуканов Л.В. Цифровой вызов для арабского мира: фактор интеграции или дифференциации? *Вестник Российского университета дружбы народов. Серия: Международные отношения*. 2022. № 2. С. 303–319. DOI: 10.22363/2313-0660-2022-22-2-303-319
Valiakhmetova G.N., Tsukanov L.V. 2022. Digital Challenge for the Arab World: Integration or Differentiation Factor? *Vestnik RUDN. International Relations*. № 2. Pp. 03–319. DOI: 10.22363/2313-0660-2022-22-2-303-319
10. Развитие объединения БРИКС в контексте мировой динамики: задачи и перспективы. Под ред. В.А.Садовниченко. М.: Изд-во Московского ун-та, 2024. 464 с. ISBN 978-5-19-012139-1
2024. Development of the BRICS association in the context of global dynamics: challenges and prospects. Ed. V.A.Sadovnichiy. Moscow. 464 p. ISBN 978-5-19-012139-1

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Хайруллин Тимур Радикович кандидат политических наук, старший научный сотрудник, Центр цивилизационных и региональных исследований, Институт Африки РАН; старший преподаватель кафедры политологии, Финансовый университет при Правительстве РФ, Москва, Россия; старший научный сотрудник СПбГУ, Санкт-Петербург, Россия.

Timur R. Khayrullin, PhD (Political Science), Senior Researcher, Center for Civilizational and Regional Studies, Institute for African Studies, Russian Academy of Sciences; Senior Lecturer, Department of Political Sciences, Financial University under the Government of the Russian Federation, Moscow, Russia; Senior Researcher, Saint-Petersburg State University, Saint Petersburg, Russia.

Шелковников Андрей Игоревич, выпускник аспирантуры Факультета мировой экономики и мировой политики НИУ ВШЭ; эксперт, Центр изучения Африки НИУ ВШЭ, Москва, Россия.

Andrey I. Shelkovnikov, Postgraduate of the Faculty of World Economy and International Affairs, HSE University; Expert, Center for African Studies, HSE University, Moscow, Russia.

Симбирцев Егор Дмитриевич, студент, РУДН им. Патриса Лумумбы, Москва, Россия.

Egor D. Simbirtsev, student, RUDN University, Moscow, Russia.

Поступила в редакцию
(Received) 27.03.2025

Доработана после рецензирования
(Revised) 12.05.2025

Принята к публикации
(Accepted) 10.06.2025