Vestnik RUDN. International Relations. ISSN 2313-0660 (print), ISSN 2313-0679 (online) 2022 Vol. 22 No. 2 303—319
Вестник РУДН. Серия: МЕЖДУНАРОДНЫЕ ОТНОШЕНИЯ http://journals.rudn.ru/international-relations

DOI: 10.22363/2313-0660-2022-22-2-303-319

Научная статья / Research article

Цифровой вызов для арабского мира: фактор интеграции или дифференциации?

Г.Н. Валиахметова ✉, Л.В. Цуканов

Уральский федеральный университет имени Первого Президента России Б.Н. Ельцина, Екатеринбург, Российская Федерация
✉vgulnara@mail.ru

Аннотация. По мере интеграции в глобальное цифровое пространство арабские страны разделяют его преимущества и риски, включаются в построение системы международной информационной безопасности. Учитывая значительное влияние арабского мира на формирование мировой политической повестки и глобальную систему безопасности, изучение специфики развития арабского цифрового кластера на современном этапе приобретает не только академическую, но и политическую актуальность. Статья посвящена исследованию текущего состояния, потенциала и пределов кооперации арабских стран в области цифровой защиты в рамках межарабского сотрудничества в многосторонних и двусторонних форматах, а также взаимодействия с мировыми лидерами технологической «гонки». Анализ основан на методологии Глобального индекса кибербезопасности, разработанной Международным союзом электросвязи ООН и включающей пять ключевых параметров оценки готовности современных государств к отражению киберугроз, таких как: нормативно-правовая система национальной киберзащиты, технические возможности, организационная структура, меры по развитию потенциала и международное сотрудничество. Оценивая «цифровой ландшафт» арабских государств, авторы отмечают, что политическая, финансово-экономическая и историко-культурная специфика арабских стран способствует формированию в регионе особой среды для противостояния киберугрозам и решения проблем кибербезопасности. С одной стороны, цифровой вызов побуждает арабские государства к преодолению некоторых разногласий, придавая определенный импульс интеграционным процессам. С другой стороны, «догоняющий» тип и скачкообразная динамика развития цифровой отрасли в регионе, а также присущая арабскому миру разнородность и противоречивость в совокупности с традиционно высокой степенью конфликтности в регионе и сильным влиянием внешних факторов создают гетерогенную и фрагментированную среду, препятствующую формированию коллективного ответа на вызовы цифровой эпохи.

Ключевые слова: арабские страны, Ближний Восток, киберугрозы, кибербезопасность, региональные международные отношения, интеграция

Для цитирования: *Валиахметова Г. Н., Цуканов Л. В.* Цифровой вызов для арабского мира: фактор интеграции или дифференциации? // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2022. Т. 22, № 2. С. 303—319. https://doi.org/10.22363/2313-0660-2022-22-2-303-319

Digital Challenge for the Arab World: Integration or Differentiation Factor?

Gulnara N. Valiakhmetova ✉, Leonid V. Tsukanov
Ural Federal University, Yekaterinburg, Russian Federation
✉vgulnara@mail.ru

Abstract. As Arab states integrate into the global digital space, they share its advantages and risks and are included in the construction of the international information security system. Considering the significant influence of the Arab world on the formation of the world political agenda and the global security system, the study of the specifics of the development of the Arab digital cluster at the present stage acquires not only academic but also political relevance. This article is devoted to the study of the current state, potential and limits of Arab countries cooperation in the field of digital security within the framework of inter-Arab cooperation in multilateral and bilateral formats, as well as interaction with the world leaders in the technological 'race'. The analysis was based on the methodology of the Global Cybersecurity Index developed by the UN International Telecommunication Union. It includes five key parameters for assessing the readiness of modern states to repel cyberthreats: the regulatory and legal system of national cyber defense, technical capabilities, organizational structure, capacity development measures and international cooperation. Assessing the 'digital landscape' of the Arab states, the authors note that the political, financial, economic, historical, and cultural specifics of the Arab countries contribute to the formation of a special environment in the region for countering cyber threats and solving cyber security problems. On the one hand, the digital challenge is forcing the Arab states to overcome some differences, giving a certain impetus to integration processes. On the other hand, the 'catch-up' type, and spasmodic dynamics of the digital industry development in the region, as well as the heterogeneity and inconsistency inherent in the Arab world, combined with the traditionally high degree of conflict and the strong influence of external factors, create a heterogeneous and fragmented environment that prevents the formation of a collective response to challenges of the digital age.

Key words: Arab states, the Middle East, cyber threats, cyber security, regional international relations, integration

For citation: Valiakhmetova, G. N., & Tsukanov, L. V. (2022). Digital challenge for the Arab world: Integration or differentiation factor? *Vestnik RUDN. International Relations*, 22(2), 303—319. https://doi.org/10.22363/2313-0660-2022-22-2-303-319

Введение

Цифровизация как глобальный мегатренд порождает общий для всех стран комплекс угроз. Вместе с тем региональный контекст формирует специфику цифрового вызова, побуждая государства нарабатывать собственные подходы и практики преодоления или снижения новых рисков. Арабский кейс представляет особый академический и практический интерес не только в связи с высоким влиянием арабского мира и шире — Большого Ближнего Востока[1] — на глобальную повестку. Взаимодействие общемировых и региональных трендов в этой части света носит сложный и противоречивый характер, причем развитие на региональном уровне может как обгонять, так и тормозить или даже противодействовать глобальным тенденциям, формируя порой противоположные им по направленности и характеру последствия (Барановский, Наумкин, 2018; Звягельская, Свистунова, Сурков, 2020b).

Научное осмысление особенностей развития Ближнего Востока в меняющемся глобальном контексте сопровождается разработкой новых теоретических подходов и изучением возможностей их применения к региональным реалиям. Отличительной чертой трудов российских востоковедов, ближневосточников и арабистов является сочетание политического или экономического анализа с методами

[1] В рамках данного исследования условный термин «арабский мир» обозначает геополитическое пространство, охватывающее 22 страны, входящие в состав Лиги арабских государств (ЛАГ), главной площадки межарабского сотрудничества. Арабский мир является системообразующим элементом ближневосточной подсистемы международных отношений и, в более расширительных трактовках, Большого Ближнего Востока (англоязычный аналог — регион MENA, Middle East and North Africa), под которым в данной статье понимается геополитический регион в составе арабских стран, Турции, Ирана и Израиля.

исторического исследования, что позволяет строить прогнозные сценарии с учетом исторической специфики региона (Звягельская, Кузнецов, 2017; Мелкумян, 2020; Филоник, Исаев, 2020).

В рамках данного подхода В.Г. Барановский и В.В. Наумкин раскрывают особенности преломления глобальных мегатрендов на реалии Ближнего Востока, формирования регионального пространства и общей региональной идентичности, базирующейся на арабском компоненте. Поскольку становление государственности в арабских странах пришлось на колониальный период, неизменными атрибутами региона стали постоянный дефицит безопасности, эксклюзивизм (консолидация в противостоянии «чужим», которыми в разное время считались Турция, Израиль, а в настоящее время Иран), высокая степень участия глобальных акторов в региональных делах и «эффект привыкания» к присутствию в регионе внешних интересов, а также перманентно растущая конфликтность на фоне ослабления субрегиональной интеграции (Барановский, Наумкин, 2018).

Анализ взаимодействия на Ближнем Востоке глобальных и региональных трендов через призму концепции «негативной неопределенности» приводит исследователей-международников к аналогичным выводам о дерегионализации и фрагментации имеющихся в арабском мире интеграционных площадок, о поддержании единства региона за счет высокого уровня конфликтности. Приметами современного ближневосточного политического ареала становятся также рост регионального соперничества и активности региональных держав, стремящихся использовать внешние интересы для реализации собственных амбиций; высокая степень недоверия и подозрительности, непрочность двусторонних отношений и расширение практики создания тактических альянсов (ситуативных союзов), в том числе с внешними акторами; ослабление интереса США и стран Запада к региону и, как следствие, их стремление к сокращению своего участия в региональной повестке; снижение роли «мягкой силы» и замещение ее инструментами «жесткой силы» в форме прокси-войн и прямых интервенций (Звягельская, Свистунова, Сурков, 2020b; Шумилин, 2019).

Понятие «неопределенность» также вошло в научный лексикон исследователей социально-экономического среза ближневосточных реалий. Разнообразие экономических моделей, наличие внушительного экономического, технологического и социального разрыва между арабскими странами, который усиливается снижающейся ролью большинства арабских экономик в мировом хозяйстве, создают условия для роста напряженности в регионе и оставляют мало места для интеграционных инициатив (Мельянцев, 2020; Филоник, Исаев, 2020).

Российские ученые обогащают собственными подходами концепции, разработанные в зарубежных научных сообществах. В рамках развития неомодернисткого подхода, альтернативного модернизму и постмодернизму, В.А. Кузнецов исследует проблему преодоления социально-политических фрагментаций арабских сообществ (Кузнецов, 2019; 2020). Ученые ИМЭМО РАН систематизируют обширный пласт концепций политической идентичности, выявляя факторы выбора внешнеполитических приоритетов для ближневосточных государств (Звягельская и др., 2020a). Феномен перманентно возрастающей конфликтности и меняющейся роли внешних акторов в обеспечении безопасности на Ближнем Востоке исследуется в трудах В.В. Наумкина на основе концептов территориального и демографического «упорядочивания» (Наумкин, 2019) и теории глубоко разделенных обществ (Наумкин, 2015).

Эмпирический материал Ближнего Востока позволяет коллективу исследователей из МГИМО МИД России опровергнуть популярную за рубежом теорию волн демократизации, на основе которой западные авторы отстаивают тезис о положительном влиянии информационных технологий на демократический выбор современных государств. Российские ученые убедительно доказывают, что экстраполяция глобального тренда цифровизации на арабские страны с их поздней субъектностью в системе международных отношений, незавершенностью нациестроительства, гибридностью политических систем, сочетающих традиционные и современные элементы, а также многочисленными дисбалансами

институционального развития способны породить откат государств к авторитаризму и даже архаизации (Лебедева и др., 2016). Другим примером критического подхода к аналитическому потенциалу западных концепций может служить исследование Е.С. Зиновьевой (Зиновьева, 2018), научная новизна которого обусловлена применением методологического инструментария теории социального конструктивизма для изучения взаимовлияния научно-технологической сферы и мирополитических процессов.

Проблемы построения в арабском мире коллективной системы кибербезопасности относительно недавно появились в политической и научной повестке и пока мало изучены как в России, так и за рубежом. В российском академическом поле цифровая проблематика региона представлена преимущественно исследованиями феномена кибертерроризма и роли информационно-коммуникационных технологий (ИКТ) в мобилизации протестного ресурса на примере событий «арабской весны». Страновые кейсы охватывают, как правило, неарабские государства Ближнего Востока — Иран, Израиль и Турцию. Схожая картина наблюдается в зарубежных публикациях, однако представители западных и ближневосточных научных сообществ активнее обращаются к арабской тематике, расширяя эмпирическую и аналитическую базу исследований по проблемам общерегиональной кибербезопасности. В данном контексте следует отметить труды, посвященные практикам цифровой защиты отдельных арабских стран (Alaleeli & Alnajjar, 2020; El-Houssami & Rizk, 2020; Shat et al., 2013), роли внешних акторов (Liu, 2021; Mogielnicki, 2021) и Израиля[2] в обеспечении кибербезопасности ведущих экономик региона, а также различным аспектам цифрового вызова, требующего от арабских стран коллективного ответа (Alrawabdeh, 2009; Pöpper et al., 2021).

В целом, несмотря на исключительное разнообразие подходов и тематик исследований по специфике трендов развития арабского мира, в том числе в контексте информационных угроз, проблемы переформатирования региона в единое пространство кибербезопасности пока фрагментарно представлены в научных публикациях. Данная статья позволяет в определенной степени восполнить указанный пробел в рамках поиска ответа на вопрос, сможет ли цифровой вызов стать тем фактором, который позволит арабскому миру преодолеть его традиционную противоречивость и объединиться для разработки коллективного ответа.

Общетеоретической основой исследования стали фундаментальные труды крупнейшего исследователя информационной эпохи М. Кастельса (Castells, 2002; 2010), что позволило рассматривать арабский мир не только как самостоятельный кластер, но и как часть глобального цифрового общества. Оценка текущего состояния готовности арабских стран к отражению цифровых угроз произведена преимущественно на основе методологии Глобального индекса кибербезопасности (Global Cybersecurity Index, GCI) — исследовательского мегапроекта Международного союза электросвязи (МСЭ) ООН[3]. При составлении рейтинга эксперты МСЭ принимали во внимание пять критериев: нормативно-правовую систему национальной киберзащиты, технические возможности, организационную структуру, меры по развитию потенциала, международное сотрудничество. В рамках данного исследования указанные параметры будут рассматриваться через призму проблематики межарабского сотрудничества и взаимодействия арабского мира с внешними акторами. В работе использованы методы структурного, системного и статистического анализа, ивент-анализа и сценарного прогнозирования.

[2] См.: El-Masry J. The Abraham Accords and Their Cyber Implications: How Iran is Unifying the Region's Cyberspace // Middle East Institute. June 9, 2021. URL: https://www.mei.edu/publications/abraham-accords-and-their-cyber-implications-how-iran-unifying-regions-cyberspace (accessed: 30.10.2021); Khorrami N. One Year On — Israel's Cybersecurity Cooperation with the GCC States // Middle East Institute. September, 2021. URL: https://mei.nus.edu.sg/wp-content/uploads/2021/09/Insight-266-Nima-Khorrami.pdf (accessed: 30.10.2021).

[3] Global Cybersecurity Index (далее — GCI) 2014—2020. Geneva: International Telecommunication Union (ITU), 2015—2021. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (accessed: 30.10.2021).

Специфика арабского пространства цифровых угроз

Процессы цифровизации стартовали в арабском мире почти на десятилетие позже, чем в странах Глобального Севера. В 2000-х гг. регион продемонстрировал взрывной рост численности интернет-пользователей, в 2015 г. превысил средние общемировые показатели и в 2019 г. достиг 62,96 %[4]. Хотя по степени проникновения Интернета арабский компонент Глобального Юга еще значительно отстает от государств Организации экономического сотрудничества и развития (ОЭСР) (85,08 %)[5], по численности абонентов мобильной сотовой связи на 100 человек этот разрыв уже незначителен (103,2 и 120,2 чел. соответственно[6]).

В авангарде движения к цифровому обществу находятся монархии Персидского залива, где уровень проникновения Интернета за последнее десятилетие удвоился и сейчас составляет от 95 % и выше, опережая по данному параметру лидеров Глобального Севера, а Объединенные Арабские Эмираты (ОАЭ) стали первым и пока единственным государством мира с численностью интернет-пользователей в 100 %[7]. На противоположном полюсе арабского мира расположены наименее развитые и политически нестабильные страны с уровнем проникновения Интернета от 30 % и ниже; в «средней» группе государств указанный показатель варьируется в диапазоне 57,2—72 %[8]. Рост интернет-активности увеличивает риск кибератак, формируя в этом разнородном и противоречивом регионе различные виды угроз.

Благодаря успешной модернизации, диверсификации и цифровизации своих экономик в рамках масштабных долгосрочных программ «Видение» наиболее быстро наращивают свое присутствие в киберпространстве аравийские монархии. Именно они становятся главными мишенями для финансово ориентированной киберпреступности, ущерб от которой в этих странах исчисляется миллиардами долларов[9]. Вместе с тем, в отличие от других регионов, в арабском мире кибератаки ориентированы преимущественно на доступ к коммерческим, технологическим и государственным секретам (63,6 %), нежели на похищение финансовых (6,2 %) и персональных данных (29,6 %)[10].

По количеству кибератак региональный рейтинг традиционно возглавляли монархии Залива, но в последние годы они значительно усилили свою защиту: в 2021 г. Королевство Саудовская Аравия (КСА) и ОАЭ опустились соответственно на 3-е и 4-е места в арабском индексе (30-я и 36-я строки в мировом)[11]. Тем не менее они наряду с США остаются в тройке

[4] Individuals Using the Internet (% of population) // Data Bank World Development Indicators. URL: https://data.worldbank.org/indicator/IT.NET.USER.ZS (accessed: 30.11.2021).

[5] Ibid.

[6] Mobile Cellular Subscription (per 100 people) // Data Bank World Development Indicators. URL: https://databank.worldbank.org/reports.aspx?source=2&series=IT.CEL.SETS.P2&country=VNM (accessed: 30.11.2021).

[7] Individuals Using the Internet (% of population) // Data Bank World Development Indicators. URL: https://data.worldbank.org/indicator/IT.NET.USER.ZS (accessed: 30.11.2021).

[8] Ibid.

[9] См.: El-Masry J. The Abraham Accords and Their Cyber Implications: How Iran is Unifying the Region's Cyberspace // Middle East Institute. June 9, 2021. URL: https://www.mei.edu/publications/abraham-accords-and-their-cyber-implications-how-iran-unifying-regions-cyberspace (accessed: 30.10.2021); The New Battlefront: Cyber Security across the GCC // Gulf International Forum. October 29, 2018. URL: https://gulfif.org/the-new-battlefront-cyber-security-across-the-gcc/ (accessed: 30.10.2021).

[10] Data Breach Report 2018. A Study of Data Leaks in the Middle East // InfoWatch Analytics Center, 2018. P. 4. URL: https://infowatch.com/sites/default/files/report/analytics/a_study_of_data_leaks_in_the_middle_east_in_2017-2018_.pdf (accessed: 30.10.2021). Этой спецификой объясняется внушительный рост кибератак в зоне Залива в периоды подготовки и проведения таких крупных мировых событий, как Dubai Expo 2020 и Qatar World Cup 2022. Эксперты Международного форума стран Персидского залива, отмечают, что «74 % руководителей предприятий региона рассматривают риск нарушений конфиденциальности данных как наиболее актуальную угрозу доверию заинтересованных сторон к бизнесу, что намного выше, чем в среднем по миру (55 %)». Цит. по: The New Battlefront: Cyber Security across the GCC // Gulf International Forum. October 29, 2018. URL: https://gulfif.org/the-new-battlefront-cyber-security-across-the-gcc/ (accessed: 30.10.2021).

[11] По состоянию на 31 декабря 2021 г. См.: Kaspersky Cyberthreat Real-Time Map. URL: https://cybermap.kaspersky.com/ (accessed: 31.12.2021).

мировых лидеров с самыми дорогостоящими утечками данных[12].

Критически важным активом аравийских монархий является нефтегазовый сектор, предприятия которого, как правило, сосредоточены в узких географических областях, что значительно увеличивает урон от кибератак. В последнее десятилетие саудовский нефтегазовый гигант Saudi Aramco и катарский RasGas неоднократно становились жертвами крупных нападений с использованием сложных вирусных программ (2012, 2016, 2017 г.) и беспилотников (2019 г.). Подобные атаки имеют не только глобальные экономические последствия — от повышения цен на нефть до каскадного воздействия на различные отрасли мировой экономики (Pöpper et al., pp. 96—97). Речь идет о применении так называемых цифровых вооружений, за разработкой которых стоят государства, в связи с чем такие атаки интерпретируются как акт внешней агрессии, создавая потенциал для ответного кибердара (Савельев, Карасев, 2018).

Высокая степень киберугроз со стороны государственных субъектов региональной и мировой политики, а также относительно низкий уровень готовности арабских стран к их отражению являются еще одной особенностью региона[13]. Практика применения прорывных цифровых технологий в качестве силовой компоненты в межгосударственных конфликтах получила широкое распространение на Ближнем Востоке после кибератаки на ядерный исследовательский центр Ирана в 2010 г. с использованием вируса нового поколения Stuxnet, который был признан первым образцом кибероружия в силу его колоссального разрушительного потенциала. Масштабные испытания кибероружия, проводившиеся на Ближнем Востоке в 2010—2012 гг. предположительно США и Израилем[14], втянули в гонку цифровых вооружений сначала Иран, а затем и другие страны региона.

В 2015 г. появились данные о причастности правительств Бахрейна, Египта, КСА, Ливана, Марокко, ОАЭ, Омана и Судана к покупке за рубежом шпионского программного обеспечения (ПО) и других вредоносных цифровых инструментов[15]. Тайное сотрудничество с Израилем, одним из лидеров глобального рынка кибервооружений, обеспечило ряд монархий Залива эффективными инструментами противодействия Ирану, борьбы с терроризмом и контроля за внутренней оппозицией[16]. Межгосударственное противостояние в киберпространстве Ближнего Востока пролегает прежде всего по линиям КСА — Иран, Израиль — Иран, США — Иран, а также реализуется в контексте региональных кризисов (сирийского, йеменского, катарского и т. д.). При этом цифровые вооружения, используемые, например, в саудовско-иранском прокси-конфликте в Йемене, применяются на всем Ближнем Востоке и за его пределами[17]. Использование арабскими странами ИКТ в качестве инструмента внешней и внутренней

[12] Устранение последствий каждого из подобных нарушений по стоимости составляет в среднем более 5 млн долл. США, может занять несколько месяцев и нанести серьезный финансово-экономический и репутационный ущерб. См.: Internet Infrastructure Security Guidelines for the Arab States // Internet Society. March 2020. P. 6. URL: https://www.internetsociety.org/wp-content/uploads/2020/04/Internet_Infrastructure_Security_Guidelines_for_Arab_states-EN.pdf (accessed: 30.10.2021).

[13] Ibid.

[14] Раю К., Эмм Д. Kaspersky Security Bulletin 2013: Развитие угроз в 2013 году // Securelist. 11.12.2013. URL: https://securelist.ru/analysis/ksb/19140/kaspersky-security-bulletin-2013-razvitie-ugroz-v-2013-godu/ (дата обращения: 21.10.2021). Сегодня средства ведения цифровых войн (кибервойн) варьируются от относительно несложных хакерских программ до ИКТ, приравненных к стратегическим наступательным вооружениям, причем серьезный материальный или политический ущерб государству может быть нанесен и технически слабо подготовленными, но массовыми группами, использующими широко доступные вирусные программы (например, хактивистами в рамках протестных акций). См., например: (Каберник, 2013).

[15] Неизвестные взломали сеть поставщика шпионского ПО для правительственных спецслужб // SecureLab. 06.07.2015. URL: http://www.securitylab.ru/news/473587.php (дата обращения: 21.11.2021).

[16] Khorrami N. One Year On — Israel's Cybersecurity Cooperation with the GCC States // Insights. 2021. No. 266. P. 1—2. URL: https://mei.nus.edu.sg/wp-content/uploads/2021/09/Insight-266-Nima-Khorrami.pdf (accessed: 30.10.2021).

[17] От Shamoon к StoneDrill. Wiper-подобные программы атакуют компании в Саудовской Аравии и не только // SecureList. 06.03.2018. URL: https://securelist.ru/from-shamoon-to-stonedrill/30350/ (дата обращения: 21.11.2021).

политики значительно ухудшает региональную среду, увеличивая ее и без того высокий конфликтный потенциал.

Помимо государств носителями угроз в арабском цифровом пространстве являются внесистемные игроки региональной политики в лице кибергрупп, предположительно спонсируемых на государственном уровне, а также хактивисты и хакеры-одиночки, активность которых тоже зачастую выходит далеко за рамки Ближнего Востока. Кроме того, глобализация киберугроз, исходящих из региона, обусловлена деятельностью многочисленных радикально-экстремистских и террористических группировок, которые ведут в Глобальной сети киберджихад против «неверных»[18].

Таким образом, из триады киберугроз, в контексте которой ООН определяет понятие «международная информационная безопасность», для арабского мира первостепенное значение имеет угроза использования ИКТ в военно-политических целях, в качестве инструмента межгосударственного противостояния и вмешательства во внутренние дела суверенных государств. Противодействие данному виду угроз напрямую зависит от стабилизации военно-политической обстановки и урегулирования многочисленных конфликтов на Ближнем Востоке, что, в свою очередь, требует объединения усилий региональных акторов и поддержки со стороны международного сообщества. Другие виды угроз — киберпреступность и кибертерроризм — также формируют общий для арабских стран вызов, побуждая развивать кибербезопасность не только на национальном, но и региональном уровне.

Кибербезопасность в арабском мире: тенденции и проблемы развития

В последние годы ряд арабских государств довольно внушительно усилили свои позиции в Глобальном индексе кибербезопасности МСЭ. Наиболее впечатляющие результаты — у КСА и ОАЭ, которые в 2020 г. вошли в пятерку мировых лидеров; «спринтерский» подход демонстрируют также Катар, Кувейт и Иордания[19]. Для Омана и Египта[20], Туниса, Марокко и Бахрейна, которые первыми из арабских стран приступили к созданию систем национальной кибербезопасности, характерен поступательный тип развития. В указанной региональной десятке лидеров индекс МСЭ варьируется от 99,5 (КСА) до 70,9 (Иордания). Остальные арабские государства имеют низкий уровень киберзащиты, занимая 104—182-ю строки глобального рейтинга с индексом ниже 35[21]. В целом анализ данных МСЭ свидетельствует о «догоняющем» типе развития национального сектора кибербезопасности и наличии значительного цифрового разрыва между странами арабского мира.

В сфере нормативно-правового обеспечения цифровой защиты большинство арабских стран уже сделали серьезные шаги: 17 государств имеют законы о несанкционированном доступе к информации, 14 — о защите данных, 12 — о мерах по уведомлению о нарушениях, 11 — об антиобщественном поведении в Интернете[22]. По данному показателю

[18] EU Terrorism Situation and Trend Report (TE-SAT) 2019. Hague : European Police Office, 2019. URL: https://www.europol.europa.eu/activities-services/main-reports/terrorism-situation-and-trend-report-2019-te-sat (accessed: 19.10.2021). См. также: (Bunt, 2003).

[19] КСА и ОАЭ поднялись соответственно с 46-й и 47-й позиций глобального рейтинга 2017 г. на 2-ю и 5-ю строки в 2020 г. Кувейт переместился с 138-го места в 2017 г. на 64-ю строку в 2020 г. и с 17-го на 9-е место в арабском рейтинге. См.: GCI 2017. P. 59—64. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf (accessed: 30.10.2021); GCI 2020. P. 25—27, 29. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (accessed: 30.10.2021).

[20] До 2020 г. Оман и Египет с большим отрывом лидировали в региональном рейтинге кибербезопасности, а Оман входил в тройку мировых лидеров в 2014 г. и занимал 4-е место в мире в 2017 г. В 2020 г. обе страны спустились в Индексе МСЭ соответственно на 21-е и 23-е места (3-я и 4-я позиции в арабском регионе), продолжая, тем не менее, опережать ряд европейских государств. См.: GCI 2015. P. 1. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf (accessed: 30.10.2021); GCI 2017. P. 59. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf (accessed: 30.10.2021); GCI 2020. P. 25—27, 29. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (accessed: 30.10.2021).

[21] GCI 2020. P. 25—27. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (accessed: 30.10.2021). Максимальное значение индекса МСЭ — 100.

[22] Ibid. P. 3—6.

арабский мир демонстрирует тренды, схожие с другими регионами: наличие правовых норм по предупреждению и противодействию преступной деятельности в киберпространстве, как правило, характерно для стран с высоким и средним уровнем проникновения Интернета, устойчивой экономикой и нацеленностью правительств на цифровизацию[23]. Вместе с тем в арабском мире, где ислам регулирует различные сферы жизни, законотворческий процесс в той или иной мере требует согласования с нормами шариата[24], прежде всего нормами мусульманского права (фикха) (Сюкияйнен, 2016; 2019). В числе других факторов, тормозящих адаптацию национальных законодательств арабских стран к реалиям цифровой эпохи, следует отметить определенную инертность нормативно-правовой сферы, реактивный подход к заполнению образующихся в законодательстве лакун, купирование отдельных аспектов проблемы вместо комплексного решения, излишнюю бюрократизацию законотворческого процесса и т. д. Преодоление указанных барьеров откроет путь к гармонизации арабских законодательств и формированию региональной системы кибербезопасности[25].

Наличие групп реагирования на компьютерные инциденты (Computer Incident Response Teams, CSIRT) или групп реагирования на компьютерные чрезвычайные ситуации (Computer Emergency Response Team, CERT) является ключевым показателем для оценки МСЭ технических мер развития кибербезопасности. Модель CSIRT базируется на принципах открытости и сотрудничества и предполагает, что технико-технологическая защита может быть обеспечена не возведением «высоких стен» вокруг интернет-инфраструктуры, но созданием атмосферы доверия и условий для широкого обмена информацией и опытом[26].

Национальные CSIRT/CERT действуют в 17 арабских государствах, причем исключительно в статусе правительственных учреждений[27]. В ряде стран их деятельность не ограничивается традиционной защитой цифровой инфраструктуры или оказанием прямой технической поддержки органам государственной власти, но также включает проведение информационно-просветительских кампаний и киберучений, аккредитацию экспертов по кибербезопасности и иные мероприятия по увеличению национального киберпотенциала, развитию и углублению отношений с различными субъектами кибербезопасности. В 10 арабских странах, кроме того, созданы отраслевые CSIRT, преимущественно в телекоммуникационном или энергетическом секторах[28].

По мнению экспертов, группы реагирования уже сыграли ключевую роль в защите интернет-структур арабских государств, однако их эффективность ограничивается нехваткой финансов, оборудования, специалистов и навыков, причем с такими проблемами сталкиваются не только слаборазвитые страны, но и передовые[29]. Кроме того, в отличие от

[23] GCI 2020. P. 4—5. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (accessed: 30.10.2021).

[24] Так, в КСА отсутствует уголовный кодекс и ряд других атрибутов романо-германской правовой системы. Поскольку законодательство страны базируется на исламском праве, в правоприменительной практике преобладают нормы шариата, в том числе в области регулирования интернет-пространства. См.: Королевство Саудовская Аравия // Научно-технический центр ФГУП «ГРЧЦ». 29.03.2021. URL: https://rdc.grfc.ru/2021/03/saudi-arabia/ (дата обращения: 21.11.2021). О специфике восприятия цифровизации в системе исламских ценностей см., например: (Faizi & Abubakar, 2021).

[25] Development and Harmonization of Cyber Legislation in the Arab Region. New York : Economic and Social Commission for Western Asia (ESCWA), 2013. URL: https://unctad.org/system/files/non-official-document/CIIEM5_ESCWA2_en.pdf (accessed: 10.10.2021).

[26] Internet Infrastructure Security. Guidelines for the Arab States // Internet Society. 2020. P. 1. URL: https://www.internetsociety.org/wp-content/uploads/2020/04/Internet_Infrastructure_Security_Guidelines_for_Arab_states-EN.pdf (accessed: 30.10.2021).

[27] GCI 2020. P. 7. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (accessed: 30.10.2021).

[28] См.: GCI 2020. P. 8. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (accessed: 30.10.2021); Internet Infrastructure Security. Guidelines for the Arab States // Internet Society. 2020. P. 7, 12. URL: https://www.internetsociety.org/wp-content/uploads/2020/04/Internet_Infrastructure_Security_Guidelines_for_Arab_states-EN.pdf (accessed: 30.10.2021).

[29] Так, CERT Бахрейна формировалась при спонсорском участии Вашингтона, заинтересованного в усилении безопасности крупнейшей на Ближнем Востоке военно-морской базы США, размещенной в этом шейхстве. См.: The New Battlefront: Cyber Security across the GCC // Gulf International Forum. October 29,

других регионов, арабские национальные CSIRT меньше сотрудничают с частным сектором и другими заинтересованными сторонами[30]. Слабость горизонтальных связей CSIRT пока не позволяет ни одному арабскому государству достичь максимального показателя МСЭ по техническим мерам[31].

Тем не менее в арабском мире наблюдается растущая тенденция к развитию государственно-частных партнерств на национальном уровне, особенно с появлением отраслевых CSIRT. Ряд стран нарабатывают методы и практики выявления и устранения правовых и иных барьеров для взаимодействия различных субъектов кибербезопасности — правительственных учреждений, бизнес-структур, исследовательских сообществ, рядовых интернет-пользователей, а также внесистемных акторов в лице, например, «белых хакеров»[32].

Препятствиями для создания устойчивой региональной цифровой инфраструктуры являются традиционная для арабского мира атмосфера недоверия и управленческая модель «нисходящего контроля» со стороны государства. При таком подходе различные госучреждения и подконтрольные правительствам CSIRT, действуя исходя из национальных приоритетов (в том числе в интересах национальных разведслужб), сталкиваются с недоверием со стороны зарубежных коллег[33]. Иными словами, в регионе имеется запрос на доверие и стратегическую гибкость.

Значительные шаги в этом направлении уже сделаны. В 2012 г. в Маскате был создан Региональный центр МСЭ по кибербезопасности для арабского региона[34] под оперативным управлением CERT Омана, который также отвечает за координацию CERT монархий Залива[35]. Взаимодействие также осуществляется на полях Регионального саммита по кибербезопасности для арабских государств[36] и Организации исламского сотрудничества (ОИС)[37]. Арабские страны, кроме того, участвуют в глобальных инициативах с целью углубления знаний в области кибербезопасности и выстраивания отношений на межгосударственном и межотраслевом уровнях. Так, 7 арабских государств (Катар, КСА, Египет, Марокко, ОАЭ, Оман, Тунис) сотрудничают в формате глобального Форума групп реагирования на инциденты и обеспечения безопасности. У КСА и ОАЭ — самое большое из арабских стран-участниц представительство — соответственно 9 и 5 правительственных и отраслевых групп[38].

Третий оценочный критерий МСЭ — организационные меры — включает механизмы управления и координации сферы кибербезопасности на уровне исполнительной власти, частного сектора и гражданского общества. Главным индикатором их эффективности является наличие и характеристики национальной стратегии кибербезопасности (НСК). Ее оценка осуществляется по ряду параметров:

2018. URL: https://gulfif.org/the-new-battlefront-cybersecurity-across-the-gcc/ (accessed: 30.10.2021). Другим примером служит КСА, где в рамках приоритета киберзащиты критической инфраструктуры власти взяли курс на постоянные централизованные закупки за рубежом (преимущественно в США) ПО и иных готовых решений. См.: Hathaway M., Spidalieri F., Alsowailm F. Kingdom of Saudi Arabia Cyber Readiness at a Glance // Potomac Institute for Policy Studies. September 2017. URL: https://www.belfercenter.org/sites/default/files/files/publication/cri-2.0-ksa.pdf (accessed: 17.10.2021).

[30] Internet Infrastructure Security. Guidelines for the Arab States // Internet Society. 2020. P. 7, 13—14. URL: https://www.internetsociety.org/wp-content/uploads/2020/04/Internet_Infrastructure_Security_Guidelines_for_Arab_states-EN.pdf (accessed: 30.10.2021).

[31] GCI 2020. P. 71—82. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (accessed: 30.10.2021).

[32] Internet Infrastructure Security. Guidelines for the Arab States // Internet Society. 2020. P. 14—16. URL: https://www.internetsociety.org/wp-content/uploads/2020/04/Internet_Infrastructure_Security_Guidelines_for_Arab_states-EN.pdf (accessed: 30.10.2021).

[33] Ibid. P. 14.

[34] ITU Arab Regional Cybersecurity Centre (ITU-ARCC). URL: https://arcc.om/?GetLang=en (accessed: 10.12.2021).

[35] About OCERT // Oman National CERT. URL: https://cert.gov.om/about.aspx (accessed: 10.12.2021).

[36] 9-я по счету встреча прошла в КСА в ноябре 2021 г. вместе с ежегодной (13-й) конференцией групп CERT стран — участниц ОИС. См.: CERTs in an Evolving Cybersecurity Landscape. URL: https://www.oic-cert.org/event2021/ (accessed: 10.12.2021).

[37] Online Tutoring — What It Is All about and How Much It Costs // OIC Tech Platform. September 2, 2018. URL: http://www.oic-cert.net/ (accessed: 10.12.2021).

[38] FIRST Members around the World // FIRST. URL: https://www.first.org/members/map (accessed: 10.12.2021).

— нацеленность на защиту критической инфраструктуры (имеется у 13 арабских стран);

— регулярные обновления в контексте новых угроз и приоритетов (6 государств);

— проведение национальных аудитов;

— наличие метрик для оценки рисков на национальном уровне (9 стран) и т. д.[39]

Зависимость развития национальной цифровой отрасли и кибербезопасности от внешней помощи, прежде всего в лице ООН и стран Глобального Севера, формирует в арабском мире схожие с ними методологические подходы к понятию «кибербезопасность», которое синонимично термину «информационная безопасность» и охватывает широкий круг проблем, связанных с технико-технологической защитой информационных систем и сетей[40].

Сегодня максимальный показатель МСЭ по организационным мерам достигнут только тремя арабскими государствами — КСА, Оманом и Египтом; высокий индекс также у ОАЭ и Катара[41], остальным странам еще предстоит устранять серьезные пробелы в системе управления киберзащитой. Пробуксовка в разработке НСК, институционализации и централизации кибербезопасности на одной платформе обусловлена в арабских странах реактивным, а не проактивным подходом к парированию угроз, «нисходящей» моделью управления, порождающей множество правительственных институтов с зачастую дублирующим функционалом и низкий уровень межведомственного взаимодействия, а также ограниченностью финансовых и кадровых ресурсов, слабостью горизонтальных связей между различными субъектами кибербезопасности[42] (Pöpper et al., 2021, p. 97). Кроме того, инвестиции в кибербезопасность реализуются преимущественно через программы модернизации военного потенциала и защиты наиболее значимых отраслей (энергетической, финансовой и ИКТ)[43], что обусловлено экономической и военно-политической спецификой региона.

По мнению исследователей, ключевую роль в устранении фрагментации саудовского пространства кибербезопасности сыграли США, заложив данную задачу в качестве одного из основных компонентов соглашения 2017 г. по модернизации вооруженных сил КСА стоимостью 110 млрд долл. США[44]. Повышение киберготовности для обеспечения безопасности, как собственной, так и внешних партнеров, характерно для тех арабских стран, которые имеют военно-политическую и/или экономическую значимость для внерегиональных акторов. Этим объясняется наращивание национального киберпотенциала при активном участии внешних сил не только в передовых государствах региона, но и в наименее

[39] GCI 2020. P. 10—13. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (accessed: 30.10.2021). Последний из указанных параметров реализуется также на региональном уровне на онлайн-платформе Регионального центра МСЭ в Омане, где все арабские страны имеют возможность произвести оценку своих киберрисков в режиме текущего времени. См.: About OCERT Services // Oman National CERT. URL: https://cert.gov.om/services.aspx (accessed: 10.12.2021).

[40] См., например: National Cybersecurity Strategy // UAE Telecommunication and Digital Government Regulatory Authority. URL: https://tdra.gov.ae/en/national-cybersecurity-strategy (accessed: 15.12.2021); Egypt National Cybersecurity Strategy (2017—2021) // Ministry of Communications and Information Technology. URL: https://www.mcit.gov.eg/Upcont/Documents/Publications_12122018000_EN_National_Cybersecurity_Strategy_2017_2021.pdf (accessed: 15.12.2021); Developing National Information Security Strategy for the Kingdom of Saudi Arabia // Kingdom of Saudi Arabia Ministry of Communications and Informational Technology. March 10, 2017. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/SaudiArabia_NISS_Draft_7_EN.pdf (accessed: 15.12.2021).

[41] GCI 2020. P. 71—82. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (accessed: 30.10.2021).

[42] Internet Infrastructure Security. Guidelines for the Arab States // Internet Society. 2020. P. 14—16. URL: https://www.internetsociety.org/wp-content/uploads/2020/04/Internet_Infrastructure_Security_Guidelines_for_Arab_states-EN.pdf (accessed: 30.10.2021).

[43] Cybersecurity Spending for Critical Infrastructure to Surpass US$105 Billion in 2021 // ABI Research. February 10, 2021. URL: https://www.abiresearch.com/press/cybersecurity-spending-critical-infrastructure-surpass-us105-billion-2021/ (accessed: 10.12.2021).

[44] См.: U.S. Security Cooperation with Saudi Arabia. Fact Sheet // U.S. State Department. January 20, 2021. URL: https://www.state.gov/u-s-security-cooperation-with-saudi-arabia/ (accessed: 10.12.2021); The New Battlefront: Cyber Security across the GCC // Gulf International Forum. 2018. URL: https://gulfif.org/the-new-battlefront-cyber-security-across-the-gcc/ (accessed: 30.10.2021).

развитых, например в Сомали и Джибути[45], где расположены иностранные военные базы.

Государства, не представляющие интереса для внешних акторов в силу своей экономической отсталости или политической нестабильности, не могут рассчитывать на финансовую, технологическую и кадровую помощь извне. Так, снижение роли палестинского фактора в региональной повестке (Шумилин, 2019, с. 116; Наумкин, 2019, с. 75—78) привело к существенному сокращению внешней помощи Палестине в формировании национального сектора ИКТ и киберзащиты и, как следствие, падению рейтинга страны в Глобальном индексе МСЭ с 102 позиции в 2017 г. на 122 строку в 2020 г.[46] Иными словами, все более проявляющийся избирательный и прагматичный подход внешних спонсоров к поддержке программ цифровизации и кибербезопасности арабских стран будет оказывать возрастающее влияние на увеличение цифрового разрыва в арабском мире.

Четвертый показатель готовности государств к отражению киберугроз — меры по развитию потенциала — включает подготовку собственных кадров, наличие профильных образовательных программ и исследовательских институтов, поддержку малого и среднего бизнеса, развитие государственно-частного партнерства. По данному параметру максимальный индекс МСЭ имеют только 4 государства — Катар, КСА, ОАЭ и Оман, высокий показатель также у Египта, для остальных арабских стран — это сфера потенциального роста[47].

Хотя арабские правительства и признают значимость данной группы мер, они реализуются преимущественно с подачи и при поддержке западных партнеров[48]. Кроме того, наблюдается серьезный дисбаланс в географии соглашений в области государственно-частного партнерства с участием двух и более арабских компаний: такое взаимодействие осуществляется главным образом между монархиями Залива, в то время как в остальной части арабского мира оно отсутствует либо ограничивается единичными эпизодами[49].

Серьезным вызовом для арабского мира становится также проблема «утечки мозгов», которая не нова для региона[50], однако именно с запуском реформ в области цифровизации она приобрела особую остроту. Несмотря на очевидные успехи[51] в подготовке собственных кадров (Alaleeli & Alnajjar, 2020), отток профессионалов в страны Запада продолжается, причем для квалифицированных кадров из арабских стран даже ведущие экономики региона в лице государств Залива по своей

[45] US, France, Djibouti Enhance Cyber Defense Interoperability // Dvids. February 23, 2021. URL: https://www.dvidshub.net/news/389582/us-france-djibouti-enhance-cyber-defense-interoperability (accessed: 12.12.2021).

[46] См.: GCI 2017. P. 59—64. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf (accessed: 30.10.2021); GCI 2020. P. 25—27. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (accessed: 30.10.2021). О программах внешней помощи Палестине в сфере развития ИКТ и кибербезопасности подробнее см.: Modernising the Public Administration. The Case of E-Government in the Palestinian Authority. OECD, 2011; Telecommunication Sector Note in the Palestinian Territories: Missed Opportunity for Economic Development. Note for the Palestinian Ministry of Telecommunications and Information Technology. World Bank Group, 2016. 63 p.; Shahwan M.A.M. Suggesting the Best Information Security Management System for Palestinian E-Government. Tallinn, 2015. 74 p. См. также: (Shat et al., 2013).

[47] GCI 2021. P. 71—82. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (accessed: 30.10.2021).

[48] Christidis O. Technology and Youth Drive the Future of Work in MENA // Middle East Institute. October 22, 2021. URL: https://www.mei.edu/publications/technology-and-youth-drive-future-work-mena (accessed: 22.10.2021). См. также: (Pöpper et al., 2021, pp. 98—100).

[49] Закономерность выведена на основе анализа данных, содержащихся в открытых базах контрагентов арабских стран Ближнего Востока, а также реестра совместных с арабскими партнерами компаний, зарегистрированных в США. См., например: Public Register // Qatar Financial Centre. URL: https://eservices.qfc.qa/qfcpublicregister/publicregister.aspx (accessed: 12.12.2021).

[50] Stop the Brain Drain from the Arab World // Gulf News. December 29, 2003. URL: https://gulfnews.com/uae/stop-the-brain-drain-from-the-arab-world-1.374254 (accessed: 14.12.2021).

[51] См., например: Shaneen S. By 2030, Every 100 Saudi Residents Will Have “One Programmer” // Leaders. August 27, 2021. URL: https://www.leaders-mena.com/by-2030-every-100-saudi-residents-will-have-one-programmer/ (accessed: 15.12.2021); Christidis O. Technology and Youth Drive the Future of Work in MENA // Middle East Institute. October 22, 2021. URL: https://www.mei.edu/publications/technology-and-youth-drive-future-work-mena (accessed: 22.10.2021).

привлекательности значительно уступают таким направлениям миграции, как США, ЕС и Канада[52]. С учетом оттока населения из турбулентных зон региона и существенного социально-экономического разрыва между арабскими странами, в том числе в индексе человеческого развития (Мельянцев, 2020), движение человеческого капитала будет усиливать технологическое неравенство в арабском мире и препятствовать его интеграции.

Международное сотрудничество арабских стран в области кибербезопасности

Международное сотрудничество является краеугольным камнем в системе обеспечения национальной и региональной кибербезопасности, однако именно по данному параметру позиции арабских стран наиболее уязвимы и свидетельствуют о наличии значительного «цифрового разрыва»[53]. Как и в других регионах, в такой деликатной сфере, как кибербезопасность, арабские страны предпочитают входить в многосторонние соглашения (12 стран) и иные международные форматы участия (14 стран), нежели в двусторонние формы межгосударственного взаимодействия (11 стран)[54].

Региональный тренд на востребованность активного участия внешних акторов в формировании системы безопасности (Барановский, Наумкин, 2018, с. 13; Шумилин, 2019, с. 111—117) проявляется и в сегменте цифровой защиты, как национальной, так и коллективной. На внешних треках взаимодействия представлены страны Глобального Севера (США, Великобритания, ряд государств ЕС, Республика Корея, Япония), по линии Юг — Юг партнерами арабского мира выступают Китай и мусульманские государства Юго-Восточной Азии[55].

Американское видение архитектуры коллективной киберзащиты в арабском мире, продвигаемое Вашингтоном с начала 2010-х гг., базируется на концепции создания в зоне Персидского залива субрегиональной системы безопасности, не требующей значительного присутствия США. В этой связи Вашингтон делает ставку на своих традиционных региональных союзников — КСА и ОАЭ, которых рассматривает в качестве драйверов процесса консолидации Совета сотрудничества арабских государств Персидского залива (ССАГПЗ) для совместного противостояния цифровым угрозам с последующим превращением данного объединения в интеграционное ядро общеарабской системы кибербезопасности (Alazab & Chon, 2015). Указанный подход реализуется преимущественно в рамках военного сотрудничества США с монархиями Залива и поддержки инициатив ССАГПЗ в развитии военного сегмента цифровой защиты («Киберщит полуострова» и др.[56]).

[52] Migration in the Middle East and North Africa // Konrad Adenauer Stiftung. March 1, 2021. URL: https://www.kas.de/documents/282499/282548/Migration+in+the+Middle+East+and+North+Africa+Report+KAS+PolDiMed+Survey.pdf/aec38c1f-bcf4-a58d-fe93-ae33db2d9228?version=1.0&t=1616675653756 (accessed: 17.12.2021).

[53] В Индексе МСЭ 2020 г. только КСА, ОАЭ и Оман достигли максимального показателя; за ними следуют государства с относительно высоким (Катар, Египет, Марокко, Тунис) и средним уровнем (Кувейт, Иордания, Бахрейн) межгосударственного сотрудничества; остальные страны (Ливия, Алжир, Сомали, Ирак, Ливан, Коморы) имеют крайне низкие и даже нулевые оценки (Джибути, Йемен, Мавритания, Палестина, Сирия, Судан). См.: GCI 2020. P. 71—82. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (accessed: 30.10.2021).

[54] GCI 2020. P. 20—21. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (accessed: 30.10.2021). Так, например, КСА ограничивается лишь двумя двусторонними соглашениями по сотрудничеству в области цифровой защиты — с ОАЭ и Великобританией. См.: Saudi Arabia // UNIDIR. March, 2021. URL: https://unidir.org/cpp/state-pdf-export (accessed: 20.10.2021).

[55] UNIDIR Cyber Policy Portal // The United Nations Institute for Disarmament Research. URL: https://cyberpolicyportal.org/en/ (accessed: 10.12.2021).

[56] См.: Abedi S. Omani National Security and the Kind of Political and Military Cooperation with the United States // Modern Diplomacy. July 15, 2019. URL: https://moderndiplomacy.eu/2019/07/15/omani-national-security-and-the-kind-of-political-and-military-cooperation-with-the-united-states/ (accessed: 18.12.2021); The 5×5 — The State of Cybersecurity in the Middle East // The Atlantic Council. June 15, 2021. URL: https://www.atlanticcouncil.org/content-series/the-5x5/the-5x5-the-state-of-cybersecurity-in-the-middle-east/ (accessed: 18.12.2021); Helou A. UAE, US Companies Partner to Provide Cyber Ranges in Gulf // C4isrnet. May 28, 2021. URL: https://www.c4isrnet.com/industry/2021/05/28/uae-us-companies-partner-to-provide-cyber-ranges-in-gulf/ (accessed: 18.12.2021).

Китай придерживается более гибкого подхода, который также базируется на общих принципах ближневосточной политики страны, позволяющих Пекину акцентировать внимание на реализации экономических интересов, избегая при этом погружения в региональные споры (Liu, 2021). Соответственно в вопросах кибербезопасности КНР придерживается многосторонних форматов взаимодействия с арабским миром, рассматривая в качестве главной интеграционной площадки Лигу арабских государств[57] и предлагая общерегиональные проекты технологического сотрудничества в рамках инициатив «Пояса и пути» и «Цифрового Шелкового пути»[58]. Приоритетными направлениями сотрудничества Китая со странами Лиги арабских государств становятся цифровая инфраструктура, финансовые технологии и онлайн-торговля[59], а с государствами ССАГПЗ, кроме того, — продвижение блокчейнов, криптовалют и иных технологий, обеспечивающих финансовую безопасность, в том числе для трансграничных платежей[60], а также технологических решений в области оптимизации государственных услуг и сокращения расточительных расходов (Mogielnicki, 2021, p. 173).

Таким образом, применительно к арабскому миру в технологическом соперничестве США и КНР достигнут определенный баланс сил, поскольку Вашингтон и Пекин преследуют разные долгосрочные цели и используют разные методы их реализации. Более того, между двумя державами наметилось некое схожее видение обеспечения стабильности на Большом Ближнем Востоке, которое, хотя и базируется на разных исходных императивах, сводится к идее ключевого участия самих арабских стран в построении региональной системы безопасности (Liu, 2021, pp. 81, 93—94; Mogielnicki, 2021, pp. 163, 173—174). Хотя стремление ведущих внешних акторов к снижению своей вовлеченности в региональную повестку воспринимается весьма негативно в ССАГПЗ (Барановский, Наумкин, 2018, с. 13—14) и не отвечает ожиданиям ЛАГ[61], оно придет импульс внутрирегиональным интеграционным процессам, в том числе в сфере кибербезопасности.

Наиболее высокая интенсивность взаимодействия в области цифровой защиты наблюдается на платформе ССАГПЗ. Схожие экономические модели и темпы развития, в том числе в цифровом сегменте, однотипность политических систем и восприятия ключевых киберугроз[62] в совокупности с наличием общих подходов к обеспечению безопасности в зоне Залива создают благоприятные условия для формирования «единого цифрового фронта». Однако определенный технологический разрыв имеется и среди аравийских монархий, в связи с чем «отстающие» участники ССАГПЗ считают, что основной вклад в обеспечение коллективной кибербезопасности следует внести КСА и ОАЭ. Эр-Рияд и Абу-Даби со своей стороны не готовы к подобному «квотированию» обязательств во избежание излишнего давления на свой киберсектор (что чревато

[57] Wu W. China Hails Arab Data Security Pact amid Battle for Cyber Influence // South China Morning Post. March 31, 2021. URL: https://www.scmp.com/news/china/diplomacy/article/3127795/china-hails-arab-data-security-pact-amid-battle-cyber (accessed: 20.12.2021).

[58] Zinser S. China's Digital Silk Road Grows with 5G in the Middle East // The Diplomat. December 16, 2020. URL: https://thediplomat.com/2020/12/chinas-digital-silk-road-grows-with-5g-in-the-middle-east/ (accessed: 18.12.2021).

[59] China, Arab League Hail Bilateral Ties, Pledge Further Cooperation // Xinhua. July 19, 2021. URL: http://www.xinhuanet.com/english/2021-07/19/c_1310069392.htm (accessed: 22.12.2021).

[60] См.: Central Banks of China and United Arab Emirates Join Digital Currency Project for Cross-Border Payments // BIS. February 23, 2021. URL: https://www.bis.org/press/p210223.htm (accessed: 20.12.2021); Kawate I. Thailand and UAE Join China's Global Digital Currency Push // Niikei Asia. February 25, 2021. URL: https://asia.nikkei.com/Business/Markets/Currencies/Thailand-and-UAE-join-China-s-global-digital-currency-push (accessed: 22.12.2021).

[61] См.: Olander E. China and the Arab League Publish Joint Statement That Showcases Beijing's Growing Geopolitical Ambitions // SupChina. July 20, 2021. URL: https://supchina.com/2021/07/20/china-and-the-arab-league-publish-joint-statement-that-showcases-beijings-growing-geopolitical-ambitions/ (accessed: 23.12.2021); China Challenges US Position as Most Important Partner for Middle East // Business Standard. June 14, 2021. URL: https://www.business-standard.com/article/international/china-challenges-us-position-as-most-important-partner-for-middle-east-121061400348_1.html (accessed: 25.12.2021).

[62] Cabral A.R. UAE Calls for United Front to Combat Global 'Cyber Pandemic' // The National News. November 15, 2021. URL: https://www.thenationalnews.com/business/2021/11/15/uae-calls-for-united-front-to-combat-global-cyber-pandemic/ (accessed: 21.12.2021).

повышением уязвимости к внешним угрозам), поэтому отдают приоритет развитию национальных структур кибербезопасности, на основе которых будет строиться гибкая и устойчивая система коллективного реагирования на цифровые вызовы[63]. Однако главным дезинтегрирующим фактором для ССАГПЗ остаются многочисленные противоречия между его участниками, выразившиеся, прежде всего, в катарском дипломатическом кризисе, а также нынешнем отсутствии единой позиции по Ирану и Израилю (Шумилин, 2019, с. 114—115; Звягельская, Свистунова, Сурков, 2020b, с. 97—98; Барановский, Наумкин, 2018, с. 14; Pradhan, 2018).

Проблемы совместной цифровой защиты стали все чаще появляться в повестке саммитов ЛАГ, причем в немалой степени под влиянием глобальных институтов, прежде всего в лице ООН[64]. Общий подход Лиги к вопросам коллективной кибербезопасности еще находится в стадии разработки, но в целом предполагает, что страны с передовыми практиками, в первую очередь КСА, ОАЭ и Египет, должны оказывать арабской «цифровой периферии» помощь в формировании технического и кадрового потенциала. Арабские страны уже сделали серьезные шаги в развитии сотрудничества национальных CSIRT/CERT[65] и государственно-частного партнерства[66], подготовки кадров[67] и гармонизации профильных законодательств[68].

Вместе с тем интеграционный потенциал ЛАГ серьезно ограничивается колоссальными экономическими диспропорциями (Мельянцев, 2020; Филоник, Исаев, 2020), социально-политической фрагментацией арабских обществ (Кузнецов, 2020; Звягельская и др., 2020a; Мелкумян, 2020) и очевидным снижением интереса внешних акторов и стран ССАГПЗ к арабской периферии, цифровое развитие которой сопряжено с внушительными экономическими издержками и высокими политическими рисками[69]. В этой связи в последние годы арабские страны налаживают взаимодействие без участия монархий Залива. Примерами такого сотрудничества по линии Юг — Юг могут служить обмен инновационными практиками в сфере онлайн-торговли между Египтом, Тунисом и Марокко (El-Houssami & Rizk, 2020), а также совместные мероприятия Иордании, Ливана, Алжира и Марокко по подготовке кадров[70]. Однако подобные проекты, как правило, единичны, имеют узкую специализацию и не обладают достаточным интеграционным потенциалом.

Еще одной платформой взаимодействия арабских стран является ОИС, в рамках которой взаимодействуют национальные CSIRT/CERT[71], функционируют Центр по противодействию кибертерроризму (создан в 2017 г.)[72] и Рабочая группа по безопасному

[63] Hakmeh J., Shires J. Is the GCC Cyber Resilient? // Chatham House. March 9, 2020. URL: https://www.chathamhouse.org/2020/03/gcc-cyber-resilient-0/summary (accessed: 19.10.2021).

[64] Development and Harmonization of Cyber Legislation // UNCTAD. 2013. URL: https://unctad.org/system/files/non-official-document/CIIEM5_ESCWA2_en.pdf (accessed: 10.10.2021).

[65] Internet Infrastructure Security. Guidelines for the Arab States // Internet Society. 2020. P. 7, 13—14. URL: https://www.internetsociety.org/wp-content/uploads/2020/04/Internet_Infrastructure_Security_Guidelines_for_Arab_states-EN.pdf (accessed: 30.10.2021).

[66] Arab League Inks Multi-Million Dollar Deal for Regional Data Hub in Bahrain // Arab Business. September 9, 2021. URL: https://www.arabianbusiness.com/industries/technology/468209-arab-league-inks-multi-million-dollar-deal-for-regional-data-hub-in-bahrain (accessed: 20.12.2021).

[67] Christidis O. Technology and Youth Drive the Future of Work in MENA // Middle East Institute. October 22, 2021. URL: https://www.mei.edu/publications/technology-and-youth-drive-future-work-mena (accessed: 22.10.2021). См. также: (Alaleeli & Alnajjar, 2020).

[68] Hakmeh J. Cybercrime Legislation in the GCC Countries Fit for Purpose? London : Chatham House, 2018. URL: https://www.chathamhouse.org/sites/default/files/publications/research/2018-07-04-cybercrime-legislation-gcc-hakmeh.pdf (accessed: 22.10.2021).

[69] Ibid.

[70] См. например: Quals: Jordan Algeria Lebanon Morocco National CTF 2020 // Cyber Talents. July 9, 2020. URL: https://cybertalents.com/competitions/quals-jordan-lebanon-and-morocco-national-cyber-security-ctf-2020 (accessed: 10.12.2021).

[71] Online Tutoring — What It Is All about and How Much It Costs // OIC Tech Platform. September 2, 2018. URL: http://www.oic-cert.net/ (accessed: 10.12.2021).

[72] OIC Will Soon Establish a Cyber Security Center to Combat Cyberterrorism // OIC. November 7, 2017. URL: https://www.oic-oci.org/topic/?t_id=16023&t_ref=8082&lan=en (accessed: 10.12.2021).

использованию технологий 5G (2021 г.)[73], также реализуется ряд других проектов. Однако с учетом географии участников данного объединения, которая выходит далеко за пределы арабского региона, а также исключительной разнородности и противоречивости самого исламского мира, инициативы ОИС априори могут иметь самый обобщенный характер и охватывать преимущественно техническую сферу. Поэтому сотрудничество с ОИС остается важным, но не определяющим направлением интеграционных процессов в арабском мире, в том числе в области кибербезопасности.

Новый региональный тренд заложили «Соглашения Авраама» 2020 г., открывшие путь к нормализации отношений Израиля с ОАЭ и Бахрейном и ставшие кульминацией их многолетнего неофициального взаимодействия в сфере высоких технологий и кибербезопасности. Готовность Израиля и ряда арабских государств к расширению сотрудничества мотивирована идеей совместного противостояния Ирану, а также комплексом иных стратегических и коммерческих интересов[74]. В сфере кибербезопасности Израиль ориентирован на кооперацию с монархиями Залива, прежде всего КСА, а также Египтом и Иорданией, с которыми активно развиваются межведомственные связи и государственно-частное партнерство, ведется разработка совместных долгосрочных программ цифрового развития, создаются двусторонние профильные рабочие группы[75]. Менее продвинутые в цифровом плане страны (Марокко, Судан), также взявшие курс на нормализацию отношений с Израилем, представляют для израильской стороны преимущественно коммерческий интерес, в связи с чем взаимодействие с ними ограничивается краткосрочными проектами[76].

Тенденция к выдвижению Израиля на роль гаранта кибербезопасности для части арабского мира, по мнению экспертов, чревата дестабилизацией всего Ближневосточного региона как ввиду неоднозначной позиции арабских стран, в том числе государств ССАГПЗ, в отношении Ирана и Израиля, так и в свете ответного усиления наступательного киберпотенциала Ирана[77]. Кроме того, по мнению обозревателей, Израиль, активно включаясь в строительство безопасной цифровой среды в ряде передовых арабских стран, рассчитывает на снижение интенсивности межарабского взаимодействия, прежде всего с враждебно настроенными к нему странами, тем самым ускоряя оттеснение на периферию слабых и/или связанных с Ираном государств (Ирака, Сирии, Йемена и др.)[78].

В целом международное сотрудничество арабских стран в сфере кибербезопасности наталкивается на те же преграды, которые ограничивают интеграционный потенциал региона. В их числе отсутствие единого экономического базиса, кризис общеарабской идентичности и свойственное всем государствам с

[73] Banda M. OIC-CERT Launch 5G Security Working Group at GISEC 2021 // Intelligent CIO. June 1, 2021. URL: https://www.intelligentcio.com/me/2021/06/01/oic-cert-launch-5g-security-working-group-at-gisec-2021/# (accessed: 15.12.2021).

[74] См.: El-Masry J. The Abraham Accords and Their Cyber Implications: How Iran Is Unifying the Region's Cyberspace // Middle East Institute. June 9, 2021. URL: https://www.mei.edu/publications/abraham-accords-and-their-cyber-implications-how-iran-unifying-regions-cyberspace (accessed: 30.10.2021); Khorrami N. One Year On — Israel's Cybersecurity Cooperation with the GCC States // Insights. 2021. No. 266. P. 1—2. URL: https://mei.nus.edu.sg/wp-content/uploads/2021/09/Insight-266-Nima-Khorrami.pdf (accessed: 30.10.2021).

[75] Israel Is Becoming a Cybersecurity Guarantor in the Middle East // Atlantic Council. November 18, 2021. URL: https://www.atlanticcouncil.org/blogs/menasource/israel-is-becoming-a-cybersecurity-guarantor-in-the-middle-east-heres-how/ (accessed: 26.12.2021).

[76] Zainabi M. Morocco — Israel: First Steps Towards Promising Joint Projects // The Jerusalem Post. February 11, 2021. URL: https://www.jpost.com/israel-news/morocco-israel-first-steps-towards-promising-joint-projects-658652 (accessed: 18.12.2021).

[77] См.: El-Masry J. The Abraham Accords and Their Cyber Implications: How Iran Is Unifying the Region's Cyberspace // Middle East Institute. June 9, 2021. URL: https://www.mei.edu/publications/abraham-accords-and-their-cyber-implications-how-iran-unifying-regions-cyberspace (accessed: 30.10.2021); Khorrami N. One Year On — Israel's Cybersecurity Cooperation with the GCC States // Insights. 2021. No. 266. P. 1—2. URL: https://mei.nus.edu.sg/wp-content/uploads/2021/09/Insight-266-Nima-Khorrami.pdf (accessed: 30.10.2021).

[78] Israel Is Becoming a Cybersecurity Guarantor in the Middle East // Atlantic Council. November 18, 2021. URL: https://www.atlanticcouncil.org/blogs/menasource/israel-is-becoming-a-cybersecurity-guarantor-in-the-middle-east-heres-how/ (accessed: 26.12.2021).

относительно поздней субъектностью в системе международных отношений стремление сохранить национальный суверенитет даже ценой отказа от очевидных благ кооперации (Лебедева и др., 2016, с. 23—24; Барановский, Наумкин, 2018, с. 14), в том числе в области цифровизации и киберзащиты.

Заключение

Цифровой вызов создает для арабского мира совокупность уникальных возможностей и в то же время рисков дальнейшего развития. Большинство арабских стран признали сферу ИКТ интегральной частью своих экономик и национальной безопасности. Поэтому арабский мир в целом набирает темпы в области создания киберзащиты, демонстрируя схожие с общемировыми тренды развития, но в то же время отличается разнообразием стратегий, практик и динамики продвижения к безопасной цифровой среде. Несмотря на традиционное недоверие, в арабском мире расширяются усилия в области региональной коммуникации, имеется явное стремление к углублению регионального взаимодействия в сфере кибербезопасности там, где это уместно и продуктивно. Очевидно, что центр такого сотрудничества расположен в монархиях Залива. Однако даже там эти усилия остаются в основном реактивными и фрагментарными, а инициаторами и спонсорами объединительных процессов преимущественно выступают глобальные структуры, прежде всего в лице ООН, а также ведущие экономики мира. В целом цифровой фактор усиливает разнородность и противоречивость арабского мира, поэтому в обозримой перспективе не сможет придать необходимый импульс региональной интеграции, несмотря на наличие определенных тенденций к консолидации.

Поступила в редакцию / Received: 19.01.2022
Доработана после рецензирования / Revised: 24.02.2022
Принята к публикации / Accepted: 18.04.2022

Библиографический список

Барановский В. Г., Наумкин В. В. Ближний Восток в меняющемся глобальном контексте: ключевые тренды столетнего развития // Мировая экономика и международные отношения. 2018. Т. 62, № 3 (62). С. 5—19. https://doi.org/10.20542/0131-2227-2018-62-3-5-19

Звягельская И. Д., Кузнецов В. А. Государство на Ближнем Востоке: будущее началось вчера // Международные процессы. 2017. Т. 15, № 4 (15). С. 6—19. https://doi.org/10.17994/IT.2017.15.4.51.1

Звягельская И. Д., Богачева А. С., Давыдов А. А., Ибрагимов И. Э., Самарская Л. М. и др. Политическая идентичность и ее влияние на внешнюю политику государств Ближнего Востока // Восток. Афро-азиатские общества: история и современность. 2020a. Т. 64, № 2. С. 55—73. https://doi.org/10.31857/S086919080009039-9

Звягельская И. Д., Свистунова И. А., Сурков Н. Ю. Ближний Восток в условиях «негативной определенности» // Мировая экономика и международные отношения. 2020b. № 6 (64). С. 94—103. https://doi.org/10.20542/0131-2227-2020-64-6-94-103

Зиновьева Е. С. Мирополитическая концептуализация международного научно-технического сотрудничества // Вестник МГИМО-Университета. 2018. № 6 (63). С. 242—254. https://doi.org/10.24833/2071-8160-2018-6-63-242-254

Каберник В. В. Проблемы классификации кибероружия // Вестник МГИМО-Университета. 2013. № 2 (29). С. 72—78. https://doi.org/10.24833/2071-8160-2013-2-29-72-78

Кузнецов В. А. Арабские общества эпохи неомодерна: поиск новых единств // Восток. Афро-азиатские общества: история и современность. 2020. № 2. С. 28—40. https://doi.org/10.31857/S086919080009104-1

Кузнецов В. А. От океана до Залива: идентичность одного региона в условиях неомодерна // Вестник Московского университета. Серия: Международные отношения и мировая политика. 2019. № 2. С. 9—38.

Лебедева М. М., Харкевич М. В., Зиновьева Е. С., Копосова Е. Н. Архаизация государства: роль современных информационных технологий // Полис. Политические исследования. 2016. №. 6. С. 22—36. https://doi.org/10.17976/jpps/2016.06.03

Мелкумян Е. С. Роль Лиги арабских государств в структурировании арабского регионального пространства // Вестник МГИМО-Университета. 2020. № 5 (13). С. 220—235. https://doi.org/10.24833/2071-8160-2020-5-74-220-235

Мельянцев В. А. Долгосрочные тренды социально-экономического развития арабских стран // Вестник МГИМО-Университета. 2020. № 5 (13). С. 194—219. https://doi.org/10.24833/2071-8160-2020-5-74-194-219

Наумкин В. В. Территориальное и демографическое «упорядочивание»: ближневосточные вызовы // Полис. Политические исследования. 2019. № 6. С. 67—80. https://doi.org/10.17976/jpps/2019.06.06

Наумкин В. В. Глубоко разделенные общества Ближнего и Среднего Востока: конфликтность, насилие, внешнее вмешательство // Вестник Московского университета. Серия: Международные отношения и мировая политика. 2015. № 1. С. 66—96.

Савельев А. Г., Карасев П. А. Перспективы регулирования и снижения военной киберугрозы // Вестник Московского университета. Серия 12: Политические науки. 2018. № 5. С. 47—61.

Сюкияйнен Л. Р. Конституционный статус шариата как источник законодательства в арабских странах // Право. Журнал Высшей школы экономики. 2016. № 3. С. 183—205. https://doi.org/10.17323/2072-8166.2016.4.205.222

Сюкияйнен Л. Р. Фикх — источник современного права в арабских странах // Право. Журнал Высшей школы экономики. 2019. № 4. С. 222—245. https://doi.org/10.17323/2072-8166.2019.4.222.245

Филоник А. О., Исаев В. А. Арабский мир: слияние в нацию или усиление разобщенности? (заметки по поводу) // Азия и Африка сегодня. 2020. № 3. С. 12—19. https://doi.org/10.31857/S032150750008723-7

Шумилин А. И. Ближний Восток: окно возможностей или западня для атлантистов? // Мировая экономика и международные отношения. 2019. Т. 63, № 7 (63). С. 111—120. https://doi.org/10.20542/0131-2227-2019-63-7-111-120

Alaleeli S., Alnajjar A. The Arab Digital Generation's Engagement with Technology: The Case of High School Students in the UAE // Journal of Technology and Science Education. 2020. Vol. 10, no. 1. P. 159—178. https://doi.org/10.3926/jotse.756

Alazab M., Chon S. Cyber Security in the Gulf Cooperation Council // Social Science Research Network Electronic Journal. 2015. P. 1—3. https://doi.org/10.2139/ssrn.2594624

Alrawabdeh B. Internet and the Arab World: Understanding the Key Issues and Overcoming the Barriers // International Arab Journal of Information Technology. 2009. Vol. 6, no. 1. P. 27—33.

Bunt G. Islam in the Digital Age: E-jihad, Online Fatwas and Cyber Islamic Environments. London and Sterling, Virginia : Pluto Press, 2003.

Castells M. The Internet Galaxy: Reflections on the Internet, Business, and Society. Oxford, UK : Oxford University Press, 2002. https://doi.org/10.1093/acprof:oso/9780199255771.001.0001

Castells M. The Rise of the Network Society. Vol. 1. Oxford, UK : John Wiley & Sons Ltd, 2010. https://doi.org/10.1002/9781444319514

El-Houssami N., Rizk N. Innovation Practices at Makerspaces in Egypt, Tunisia and Morocco // The African Journal of Information and Communication. 2020. Iss. 26. P. 1—25. https://doi.org/10.23962/10539/30357

Faizi I., Abubakar A. The Internet of Everything from Islamic Perspective // International Journal on Perceptive and Cognitive Computing. 2021. Vol. 7, no. 1. P. 66—71.

Liu L. China's Policy and Practice Regarding the Gulf Security // Stepping Away from the Abyss: A Gradual Approach Towards a New Security System in the Persian Gulf / ed. by L. Narbone, A. Divsallar. San Domenico di Fiesole : European University Institute, 2021. P. 81—94. https://doi.org/10.2870/39131

Mogielnicki R. Smart Context-Based Investments in the Persian Gulf's Economic Security // Stepping Away from the Abyss: A Gradual Approach Towards a New Security System in the Persian Gulf / ed. by L. Narbone, A. Divsallar. San Domenico di Fiesole : European University Institute, 2021. P. 163—174. https://doi.org/10.2870/39131

Pöpper C., Maniatakos M., Di Pietro R. Cyber Security Research in the Arab Region: A Blooming Ecosystem with Global Ambitions // Communications of the ACM. 2021. Vol. 64, no. 4. P. 96—101. https://doi.org/10.1145/3447741

Pradhan P. Qatar Crisis and the Deepening Regional Faultlines // Strategic Analysis. 2018. Vol. 42, iss. 4. P. 437—442. https://doi.org/10.1080/09700161.2018.1482620

Shat F. J. F., Mousavi A., Pimenisis E. Electronic Government Enactment in a Small Developing Country — The Palestine Authority's Policy and Practice // E-Democracy, Security, Privacy and Trust in a Digital World. 5th International Conference. Revised Selected Papers, December 5—6, 2013. Athens, Greece : Springer International Publishing, 2013. P. 83—92. https://doi.org/10.1007/978-3-319-11710-2_8

Сведения об авторах: *Валиахметова Гульнара Ниловна* — доктор исторических наук, доцент, заведующая кафедрой востоковедения департамента (факультета) международных отношений Уральского федерального университета имени Первого Президента России Б.Н. Ельцина; ORCID: 0000-0001-7199-7723; e-mail: vgulnara@mail.ru

Цуканов Леонид Вячеславович — аспирант кафедры востоковедения департамента (факультета) международных отношений Уральского федерального университета имени Первого Президента России Б.Н. Ельцина; ORCID: 0000-0001-6882-9841; e-mail: leon.tsukanov@mail.ru