Серия «Политология. Религиоведение»
2023. Т. 45. С. 49–58
Онлайн-доступ к журналу:
http://izvestiapolit.isu.ru/ru

ИЗВЕСТИЯ
Иркутского
государственного
университета

Научная статья

УДК 341.231+327.83+327.7
https://doi.org/10.26516/2073-3380.2023.45.49

Особенности формирования системы национальной кибербезопасности Государства Кувейт

Л. В. Цуканов*

Уральский федеральный университет им. первого Президента России Б. Н. Ельцина, г. Екатеринбург, Российская Федерация

Аннотация. Рассматривается актуальное состояние национальной системы кибербезопасности Государства Кувейт. С учетом стандартов кибербезопасности, разработанных Международным союзом электросвязи при ООН, раскрываются специфические черты формирования системы, среди которых поздний старт, десинхронизация институциональной и законотворческой работы, «селективный» подход к развитию государственно-частного партнерства и др., также определяется текущая степень вовлеченности Эль-Кувейта в международное сотрудничество в области цифровой защиты. Делается вывод, что национальная система кибербезопасности Кувейта по-прежнему развивается неравномерно, а многие решения направлены на купирование отдельных аспектов проблемы, а не на ее исправление в целом. Обращается внимание на двойственную позицию страны на международном треке, где, с одной стороны, лоббируется идея расширения внешних контактов путем активизации работы на ключевых региональных площадках, а с другой стороны, сохраняется определенная дистанцированность от международной кооперации в области цифровой безопасности. Дополнительное дестабилизирующее влияние на темпы сотрудничества оказывает антиизраильская позиция Кувейта, препятствующая налаживанию профильных связей с международными IT-компаниями, имеющими в Израиле свои представительства. По мнению автора, Эль-Кувейт нацелен на устранение указанных дисбалансов и в среднесрочной перспективе намерен выстроить более сбалансированную систему кибербезопасности с опорой на расширение международного сотрудничества. Однако для повышения эффективности этих усилий необходимо пересмотреть некоторые аспекты существующего подхода – в частности, выработать модель взаимодействия с цифровыми компаниями, поддерживающими деловые связи с Израилем.

Ключевые слова: Кувейт, кибербезопасность, стратегии цифрового развития, государственно-частное партнерство, международное сотрудничество, Совет сотрудничества арбских государств Персидского залива.

Для цитирования: Цуканов Л. В. Особенности формирования системы национальной кибербезопасности Государства Кувейт // Известия Иркутского государственного университета. Серия Политология. Религиоведение. 2023. Т. 45. С. 49–58. https://doi.org/10.26516/2073-3380.2023.45.49

*Полные сведения об авторе см. на последней странице статьи.
For complete information about the author, see the last page of the article.

Original article

Features of the Formation of the National Cybersecurity System of the State of Kuwait

L. V. Tsukanov*

Ural Federal University named after the First President of Russia, Yekaterinburg, Russian Federation

Abstract. The article is devoted to the analysis of the state of the national cybersecurity system of the State of Kuwait. Based on the cybersecurity standards of the International Telecommunication Union (a specialized UN agency responsible for coordinating international efforts to develop the digital sector) the author reveals the main specific features of the formation of the Kuwaiti cyber system, and also determines the level of the country's participation in the development of the international digital security system. The author comes to the conclusion that the digital system of Kuwait is formed with imbalances, and many decisions are aimed at "selective" relief of digital threats. In addition, the author draws attention to the existence of contradictions in the Kuwaiti model of international cooperation on cybersecurity issues: on the one hand, the country advocates more active participation in international processes, and, on the other hand, does not actively participate in the work of key international platforms. In addition, the sharp anti-Israeli position of the country has a certain negative impact on the Kuwaiti model of digital protection. The author notes that Kuwait is currently aimed at harmonizing the national cyber system and developing a more effective approach to international cooperation. However, to make these efforts more effective, some aspects of the existing approach need to be revisited, such as developing a model for interacting with digital companies that do business with Israel.

Keywords: Kuwait, cybersecurity, digital development strategies, public-private partnership, international cooperation, GCC.

For citation: Tsukanov L.V. Features of the Formation of the National Cybersecurity System of the State of Kuwait. *The Bulletin of Irkutsk State University. Series Political Science and Religion Studies,* 2023, vol. 45, pp. 49-58. https://doi.org/10.26516/2073-3380.2023.45.49 (in Russian)

Введение

В условиях продолжающейся цифровизации Ближнего Востока повышение уровня защищенности национальных государств в киберпространстве становится важным элементом обеспечения региональной стабильности. Особую активность на этом направлении проявляют аравийские монархии, рассматривающие цифровой фактор, с одной стороны, как основу комплексной трансформации собственных систем государственного управления, а с другой – как элемент наращивания геополитического веса.

Определенный интерес представляет кейс Кувейта. В отличие от большинства государств Совет сотрудничества арбских государств Персидского залива (ССАПГЗ)[1], Эль-Кувейт не делает ставку на форсированное наращивание кибермощи, а постепенно трансформирует отдельные элементы системы, что обусловливает его отставание от ведущих держав региона. Вместе с тем, несмотря на относительно невысокие позиции Кувейта в международных рейтингах киберготовности[2], эксперты отмечают серьезные каче-

[1] Помимо Кувейта, в Совет сотрудничества арабских государств Персидского залива (ССАПГЗ) входят также Саудовская Аравия, ОАЭ, Катар, Бахрейн и Оман.

[2] Согласно GCI-2020, занимает 9-е место среди стран Ближнего Востока и 65-е место в мире. См.: Global Cybersecurity Index 20120. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (date of access: 15.04.2023).

ственные изменения в его цифровой политике и прогнозируют дальнейший рост показателей при условии своевременной балансировки стратегии поведения в киберпространстве. Подобный расклад, в свою очередь, актуализирует ряд вопросов. Каковы специфические черты формирования кувейтской структуры кибербезопасности? Насколько эффективно выстраивается кооперация с другими цифровыми державами? В каких областях наблюдаются наибольшие проблемы?

Следует отметить, что в последние годы проблематика обеспечения кибербезопасности на Ближнем Востоке постепенно получает комплексное представление в научном поле. Как правило, на передний план выдвигаются вопросы, связанные с повышением уровня цифровой защищенности объектов критической инфраструктуры национальных государств [11], трансформацией подходов ключевых региональных акторов (включая переосмысление законодательных основ деятельности) [1; 4; 7] к обеспечению национальной киберзащиты и изменению ландшафта цифровой безопасности в регионе в целом [2; 5; 10].

Тем не менее, несмотря на рост числа публикаций по исследуемой тематике, значительную их часть по-прежнему составляют труды зарубежных авторов, в то время как в российском научном пространстве феномен кибербезопасности Ближнего Востока освещается реже, акцент делается на анализ кейсов стран, представляющих «цифровые полюсы» региона (Иран, Турция, Израиль, Саудовская Аравия). Кувейтский опыт формирования системы кибербезопасности пока не стал предметом отдельного исследования по причине меньшей вовлеченности страны в соперничество за статус регионального цифрового лидера. Данная работа призвана в определенной степени устранить указанный пробел. Научная новизна исследования заключается в том, что в работе производится систематизация данных о состоянии всех элементов кувейтской киберсистемы (включая смежные) и их взаимном влиянии друг на друга. Кроме того, автором по результатам самостоятельного анализа содержащихся в международных базах контрагентов данных приводится оценка текущей ситуации, складывающейся на цифровом рынке Кувейта, выявляются наиболее активные частные акторы. Это позволяет более полно оценить текущий потенциал страны в части повышения собственной киберготовности.

Источниковой основой исследования стали документы профильных министерств и ведомств Кувейта, отражающие концептуальные подходы страны к обеспечению национальной цифровой защиты; отчеты международных организаций, ведущих экспертных центров и IT-компаний, специализирующихся на вопросах кибербезопасности; материалы информационно-новостных ресурсов арабских стран.

В основу анализа специфики развития кувейтской системы кибербезопасности положены критерии, разработанные Международным союзом электросвязи (МСЭ) для определения степени цифровой защищенности государств: нормативно-правовая база и институты реализации киберполитики, технологические возможности, государственно-частное партнерство, международное сотрудничество, кадровый потенциал[3].

[3] Global Cybersecurity Index 2020 // ITU. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (date of access: 15.04.2023).

Обзор системы кибербезопасности Кувейта

Несмотря на то что Кувейт подключился к Глобальной сети еще во второй половине 1990-х гг. и по ключевым показателям относится к группе стран с высоким уровнем информатизации[4], профильное законодательство долгое время не удавалось сформировать из-за специфики национальной законодательной системы [4, p. 7][5], ввиду чего регулирование вопросов, связанных с киберпространством, осуществлялось в первую очередь с опорой на существующие прецеденты (включая юридическую практику других государств ССАГПЗ) [Там же, p. 14, 16], что не способствовало эффективному развитию национальной киберсистемы [3, p. 50]. Первым шагом к формированию *нормативно-правовой базы* можно считать Закон о телекоммуникациях (Telecoms Law, 2014 г.)[6], определявший права и обязанности как поставщиков телекоммуникационных услуг, так и рядовых пользователей. Годом позже был принят Закон об электронных транзакциях (ET Law, 2015 г.), заложивший основу для признания конфиденциальности ряда групп цифровых данных[7], а также повысивший безопасность электронных платежей [9].

Важным шагом стало принятие в 2015 г. Закона о борьбе с киберпреступностью (Cybercrime Law No. 63). Несмотря на то что закон подвергся критике со стороны международных правозащитных организаций, он стал первым национальным актом, в котором формулировались базовые юридические понятия («киберпреступление», «кибератака», «хакинг» и др.), а также предлагался механизм борьбы с противозаконной деятельностью в интернете[8]. В дальнейшем правовая база Кувейта в области обеспечения цифровой безопасности дополнилась рядом актов, регулирующих отдельные аспекты вопроса (Закон об электронных СМИ, 2017 г.[9], Закон о защите авторского права, 2019 г. и др.)[10], однако именно Закон о борьбе с киберпреступностью попрежнему составляет законодательную основу системы кибербезопасности.

---

[4] По состоянию на начало 2023 г. уровень проникновения интернета в Кувейте превышает 99 %. Кроме того, страна является одним из лидеров по использованию технологий 5G. См.: Kuwait Mobile Network Experience Report // Open Signal. URL: https://www.opensignal.com/reports/2023/02/kuwait/mobile-network-experience (date of access: 20.05.2023); Digital 2023: Kuwait. Data Reportal // Global Digital Insights. URL: https://datareportal.com/reports/digital-2023-kuwait#:~:text=Internet%20use%20in%20Kuwait%20in%202023 &text=Kuwait's%20internet%20penetration% 20rate%20stood,at%20the%20start%20of%202023 (date of access: 20.05.2023).

[5] Правовая система Кувейта имеет смешанный характер и сформирована на стыке британской и французской правовых школ, а также шариатского права. Несмотря на законодательные реформы 1980-х гг., многие аспекты общественной жизни (включая цифровую деятельность) по-прежнему остаются трудноурегулируемыми.

[6] Law № 37 (2014) on the Establishment of Communication and Information Technology Regulatory Authority // Communication and Information Technology Regulatory Authority. URL: https://citra.gov.kw/sites/en/LawofCITRA/Law%20No.%2037-%202014.pdf (date of access: 21.04.2023).

[7] Подразумеваются электронные записи, сообщения, а также иная информация, документы и подписи, относящиеся к гражданско-правовым, коммерческим и административным сделкам.

[8] Law № 63 (2015) on Combating Information Technology Crimes («Cybercrime Law № 63») // State of Kuwait Ministry of Interior. 07.07.2015. URL: https://www.e.gov.kw/sites/kgoenglish/Forms/CAITLawNo.63of2015 oncombatingInformationTechnologyCrimes.pdf (date of access: 21.04.2023).

[9] Kuwait applies the Electronic Media Law // Tamimi. 10.07.2017. URL: https://www.tamimi.com/law-update-articles/kuwait-applies-electronic-media-law/ (date of access: 22.04.2023).

[10] Kuwait: implementing regulations of the Copyright Law published // Saba IP Bulletin. 10.03.2019. URL: https://www.sabaip.com/news/kuwait-implementing-regulations-of-the-copyright-law-published/ (date of access: 18.04.2023).

Несмотря на то что стремление к формированию национального правового поля вокруг «якорного» нормативного правового акта в целом соответствует рекомендациям МСЭ и на данный момент является общей тенденцией для всех государств ССАГПЗ, кувейтский Закон о борьбе с киберпреступностью отличается размытыми формулировками и охватывает гораздо меньше сфер[11], чем аналогичные акты других аравийских монархий [6]. Это свидетельствует о недостаточных темпах трансформации нормативной базы страны.

Другой специфической чертой киберсистемы Кувейта можно считать «отложенный» формат *развития национальных институтов*. Хотя формирование профильных киберструктур в стране, как и в других государствах ССАГПЗ, шло по методу «замещающего конструирования»[12], Эль-Кувейту долгое время не удавалось выработать план реформ цифрового сектора, ввиду чего процесс получил бóльшую по сравнению с остальными аравийскими монархиями протяженность во времени [Там же]. По этой причине вплоть до принятия Закона о телекоммуникациях 2014 г. основную нагрузку по поддержанию цифровой стабильности в стране несло Центральное агентство информационных технологий (Central Agency for Information Technology, CAIT), созданное в 2006 г. В ведении Агентства, в частности, находились вопросы, связанные с разработкой национальной политики в области информационных технологий, а также осуществлением надзора за развитием внутриведомственных проектов в области цифровизации[13].

В ходе реформы системы государственных органов Кувейта в 2014 г. был создан Регуляторный орган связи и информационных технологий (Communication and Information Technology Regulatory Authority, CITRA), которому была передана часть функций CAIT (в частности, задачи по мониторингу ситуации в телекоммуникационном секторе и регулированию рынка услуг)[14]. Перераспределение полномочий усилило устойчивость национальной киберсистемы, поскольку позволило сформировать более гибкую систему реагирования на вызовы в гражданском секторе.

Тем не менее текущая конфигурация государственных институтов попрежнему не в полной мере позволяет реагировать на вызовы, исходящие из киберпространства, а сохраняющийся дисбаланс развития законодательства неизбежно ведет к формированию новых нерегулируемых зон[15]. В этой связи

---

[11] Например, не проработаны (или проработаны лишь частично) механизмы противодействия распространению противоправной информации, кибербуллингу, сексуальному насилию в Интернете и пр.

[12] В рамках данного метода шло формирование первичных институтов, под которые формулировалось профильное законодательство. В дальнейшем, по мере имплементации новых законов, создавались киберинституты «нового поколения», в то время как первичные, ввиду дублирования функций, упразднялись или серьезно реформировались. См.: Hakmeh J. Cybercrime Legislation in the GCC Countries. Fit for Purpose? // Chatham House. 18.07.2018. URL: https://www.chathamhouse.org/sites/default/files/publications/ research/2018-07-04-cybercrime-legislation-gcc-hakmeh-final.pdf (date of access: 21.04.2023).

[13] Central Agency for Information Technology // Kuwait Government Online Portal. URL: https://www.cait.gov.kw/?lang=en-US (date of access: 23.04.2023).

[14] About CITRA // Communication and Information Technology Regulatory Aithority. URL: https://www.citra.gov.kw/sites/en/Pages/Home.aspx (date of access: 21.04.2023).

[15] Например, в Кувейте долгое время отсутствовала модель регулирования обращения с криптовалютами, не был сформулирован подход к майнингу, отсутствовали органы, специализирующиеся на операциях с цифровыми активами и т. д. См.: Kuwait and Cryptocurrency // Freeman Law. 17.12.2021. URL: https://freemanlaw.com/cryptocurrency/kuwait/ (date of access: 16.04.2023).

в январе 2022 г. правительство Кувейта анонсировало новый комплекс реформ, нацеленных на актуализацию профильного законодательства и создание к 2024 г. Центра кибербезопасности и общественного порядка, нового ключевого звена национальной системы цифровой защиты[16].

Отдельно следует сказать о *технологических возможностях* Кувейта в части реагирования на компьютерные инциденты. Ввиду того что киберсистема страны не обладает значительным запасом прочности (в том числе вследствие продолжающихся комплексных преобразований), власти стремятся избежать перегрузки ответственных органов и распределяют функционал Компьютерных групп реагирования на чрезвычайные ситуации (CERT)[17] между несколькими специализированными агентствами. Так, в стране в настоящий момент функционируют Национальный центр кибербезопасности[18], осуществляющий мониторинг угроз в национальном сегменте киберпространства, и Центр сертификации (Kwt-Cert), отвечающий за оценку рынка поставщиков и их дальнейшую сертификацию[19]. Наличие постоянно действующей национальной CERT (пусть и представленной в «разделенном» виде) позволяет говорить о стремлении государства к повышению стандартов кибербезопасности и формированию безопасной среды для бизнеса.

Что касается мер по развитию *национального потенциала*, то здесь Кувейт, как и другие аравийские монархии, делает ставку на преодоление кадрового дефицита в национальном IT-секторе [8, p. 5]. Несмотря на то что в университетах страны по-прежнему реализуют сравнительно малое количество собственных образовательных программ, связанных с кибербезопасностью, данный недостаток частично компенсируется внедрением частных образовательных курсов, запущенных при участии американских и европейских некоммерческих организаций, – в первую очередь Ассоциации индустрии вычислительных технологий и Международного совета консультантов по электронной торговле[20]. Кроме того, в рамках развития государственно-частного партнерства (ГЧП) Эль-Кувейт делает ставку на привлечение внешних специалистов путем создания IT-кластеров, а также организации и проведения профильных мероприятий. В частности, на территории страны с 2019 г. регулярно проводятся крупные международные конференции – например, форумы Cyber Security Education and Research Conference (CERC)[21] и Women in Cyber Security Middle East (WICSME)[22]. Следует отме-

[16] Kuwait approves cyber security bill // Arab Times. 18.01.2022. URL: https://www.arabtimesonline.com/news/kuwait-approves-cyber-security-bill/ (date of access: 18.04.2023).

[17] Компьютерная группа реагирования на чрезвычайные ситуации (*Computer emergency response team, CERT*) – группа экспертов по компьютерной безопасности, создаваемая под эгидой МСЭ ООН и занимающаяся сбором информации об инцидентах в киберпространстве, их классификацией и нейтрализацией.

[18] Профильный департамент в составе Регуляторного органа связи и информационных технологий (CITRA).

[19] Cybersecurity and Emergency Response // Communication and Information Technology Regulatory. URL: https://www.citra.gov.kw/sites/en/Pages/cybersecurity.aspx (date of access: 21.04.2023).

[20] Cyber Security Certification Training in Kuwait // Mildain. URL: https://mildaintrainings.com/loc/cyber-security-training-in-kuwait/ (date of access: 21.04.2023).

[21] См., напр.: UK-Kuwait Cyber security Education & Research Conference // British Council. 24.11.2020. URL: https://www.britishcouncil.com.kw/en/events/UK-Kuwait-cyber-security-education-research-conference-2020 (date of access: 24.04.2023).

[22] WiCSME 2020 Virtual Conference: to empower and secure together // WiCSME. 15.11.2020. URL: https://www.womenincybersecurity.me/wicsme2020/?ref=infosec-conferences.com (date of access: 20.04.2023).

тить, что активная деятельность Эль-Кувейта по созданию конкурентных условий труда (в том числе в IT-секторе) позитивно сказывается на темпах «утечки мозгов» из страны. Так, к концу 2022 г. этот показатель удалось снизить до отметки в 2,7 индексных пункта (при показателе 3,9 и. п. на конец 2018 г.)[23] – в данном случае Кувейт несколько опережает некоторые аравийские монархии, в частности Бахрейн (3 и. п.) и Саудовскую Аравию (3 и. п.)[24].

С другой стороны, в части развития ГЧП-связей Кувейт несколько отстает от других держав ССАГПЗ. В настоящий момент в стране зарегистрировано около десятка компаний, специализирующихся на различных аспектах кибербезопасности[25], однако к государственным проектам фактически привлекаются только крупнейшие игроки рынка (Security Systems Company и SEEDiS), в то время как остальные не выходят за рамки консультирования бизнеса[26]. При этом основными инвесторами в кувейтский IT-сектор, суммарно обеспечивающими до 85 % потребностей внутреннего рынка, остаются американские (Booz Allen Hamilton, Lockheed Martin, Raytheon и др.), европейские (Ericsson) и китайские (Huawei) мегакорпорации. Как итог подобная модель сотрудничества хоть и обеспечивает приток иностранного капитала в национальный цифровой сектор, в определенной степени тормозит развитие потенциала Кувейта в части разработки собственных технологических решений.

Международное сотрудничество

В последние годы наблюдается заметная активизация усилий Кувейта по налаживанию международных связей в сфере цифровой безопасности. Так, Эль-Кувейт стал поддерживать инициативы по повышению уровня цифровой защищенности на пространстве Лиги арабских государств, Организации исламского сотрудничества и ССАГПЗ, а также в рамках Движения неприсоединения[27] [10, p. 99].

Расширяется сотрудничество и по линии Кувейт – НАТО. С 2017 г. в Эль-Кувейте функционирует Региональный центр подготовки Альянса, созданный в рамках программы «Наука ради мира и безопасности» и осуществляющий подготовку кадров в сфере кибербезопасности для кувейтского МВД, Минобороны и специальных служб[28]. Кроме того, в рамках координации региональных секьюритарных усилий в стране планируется к 2024 г.

---

[23] Kuwait: Human flight and brain drain // The Global Economy. URL: https://www.theglobaleconomy.com/Kuwait/human_flight_brain_drain_index/ (date of access: 15.05.2023).

[24] Human flight and brain drain – Country rankings // The Global Economy. URL: https://www.theglobaleconomy.com/rankings/human_flight_brain_drain_index/ (date of access: 15.05.2023).

[25] Подразумеваются в первую очередь IT-фирмы, созданные без участия иностранных инвесторов. Посчитано по: Kuwait Companies Database. См.: URL: https://www.globaldatabase.com/kuwait-companies-database (date of access: 21.04.2023).

[26] Cyber security companies in Kuwait List // Digital Marketing Deal. 15.01.2022. URL: https://digitalmarketingdeal.com/blog/cyber-security-companies-in-kuwait/ (date of access: 22.04.2023).

[27] Kuwait calls at NAM summit for new balanced world // KUNA. 26.10.2019. URL: https://www.kuna.net.kw/ArticleDetails.aspx?id=2829220 (date of access: 25.04.2023).

[28] Activities at NATO-Kuwait ICI Regional Center start // NATO. 11.10.2017. URL: https://www.nato.int/cps/en/natohq/news_147010.htm?selectedLocale=en (date of access: 25.04.2023).

создать Центр мониторинга, который будет заниматься экспертизой кибератак на пространстве ССАГПЗ[29].

В то же время, несмотря на достигнутые успехи, деятельность Кувейта на международном треке по-прежнему недостаточно сбалансирована. Так, Эль-Кувейт дистанцировался от участия в большинстве проектов Арабского регионального центра кибербезопасности МСЭ (ITU-ARCC)[30], а его национальные эксперты практически не включаются в рабочие группы ООН по кибербезопасности. В обоих случаях это можно объяснить отсутствием у кувейтских властей (несмотря на продолжающиеся реформы) сформулированных стратегий работы на указанных площадках.

На темпах развития сотрудничества, кроме того, негативно сказывается выраженная антиизраильская позиция Эль-Кувейта, транслируемая как на национальном уровне, так и в рамках региональных площадок (в первую очередь в ССАГПЗ). В результате на фоне агрессивной риторики, например, многие региональные IT-компании, имеющие деловые связи с Израилем, предпочитают не участвовать в кувейтских проектах[31], ввиду чего усилия Кувейта по созданию имиджа конкурентоспособной цифровой державы зачастую нивелируются.

Заключение

Национальная система кибербезопасности Кувейта в настоящий момент находится в стадии трансформации. Анонсированные правительством комплексные реформы, направленные на формирование новой информационно-технологической структуры, позволят в перспективе увеличить запас прочности системы, сбалансировав ее институциональные и правовые основы, а также повысить общий уровень технологической готовности государства. Подобные трансформации в целом укладываются в рамки долгосрочных планов Эль-Кувейта по превращению в один из региональных флагманов цифровизации.

Тактика развития международного сотрудничества в части обеспечения региональной и глобальной кибербезопасности, избранная кувейтскими властями, в целом позволяет решать ключевые задачи, стоящие перед страной в цифровой сфере, и обеспечивает доступ к передовым технологическим решениям, а также благоприятно сказывается на имидже страны.

В то же время переход национальной киберсистемы на более высокий уровень не видится возможным без пересмотра ряда характерных для кувейтского подхода черт. Прежде всего Эль-Кувейту необходимо уделить больше внимания разработке собственных технологических решений – во избежание попадания в зависимость от внешних партнеров (что приобретает

[29] NATO-ICI calls for greater exchange of expertise on cyber operations // KUNA. 15.09.2022. URL: https://www.kuna.net.kw/ArticleDetails.aspx?id=3054252&language=en# (date of access: 25.04.2023).

[30] За исключением проводимого под эгидой МСЭ на базе ITU-ARCC ежегодного регионального форума по стандартизации и IoT.

[31] Kuwait says it'll be 'last to normalize' with Israel, will stand by Palestinians // The Times of Israel. 16.08.2020. URL: https://www.timesofisrael.com/kuwaiti-officials-reject-israel-normalization-reaffirm-support-for-palestinians/ (date of access: 25.04.2023).

дополнительную актуальность в свете усиливающегося соперничества КНР и США за рынок высоких технологий стран Залива). Кроме того, частое апеллирование к «неприятию» сотрудничества с лояльными Израилю IT-фирмами в перспективе может привести к ослаблению деловых контактов с западными партнерами, в первую очередь с американскими корпорациями, что повлечет за собой снижение объемов инвестиций в кувейтский цифровой сектор и, как следствие, снизит темпы его развития.

Список литературы

1. *Мелкумян Е. С.* Развитие арабских монархий залива: прорыв в будущее // Азия и Африка сегодня. 2020. № 2. С. 37–42.

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

3. *Abu-Taieh E.* Cyber security crime and punishment: comparative study of the laws of Jordan, Kuwait, Qatar, Oman, and Saudi Arabia // International Journal of Cyber Warfare and Terrorism. 2018. N 3. P. 46–59.

4. *al-Mutairi N. H.* The Right to Privacy in the Digital Age as Expressed in a Muslim Country: A Case Study of Kuwait //Arab Law Quarterly. 2022. N 1. P. 1–28.

5. *Ashour S. M. K.* The regional security system in the Middle East in the context of international changes since 2011 // Iraqi Journal of Political Science. 2022. N 6. P. 1–15.

6. *Hakmeh J.* Cybercrime Legislation in the GCC Countries. Fit for Purpose? // Chatham House. 18.07.2018. URL: https://www.chathamhouse.org/sites/default/files/publications/research/2018-07-04-cybercrime-legislation-gcc-hakmeh-final.pdf (date of access: 21.04.2023).

7. *Hassib B., Shires J.* Cybersecurity in the GCC: From Economic Development to Geopolitical Controversy // Middle East Policy. 2022. Vol. 29, N 1. P. 90-103.

8. *Ko K.* An Analysis of Cybersecurity Threats and Countermeasures in the Kuwaiti Banking Sector // Kuwait Journal of Information Technology and Decision Sciences. 2023. Vol. 1, № 1. P. 1–8.

9. *Levac L.* Kuwait: Law regarding Electronic Transactions in force – introduction of a concept akin to data privacy // Global Compliance News. 11.12.2015. URL: https://www.globalcompliancenews.com/2015/12/11/kuwait-law-regarding-electronic-transactions-in-force-introduction-of-a-concept-akin-to-data-privacy/ (date of access: 25.04.2023).

10. *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, N 4. P. 96–101.

11. *Semsari M. C., Keskin O.* Threats to Energy Security and Energy Policies in Central Asia and the Middle East // Handbook of Research on Cyber Approaches to Public Administration and Social Policy. IGI Global, 2022. P. 343–364.

References

1. Melkumyan E.S. Razvitie arabskih monarhij zaliva: proryv v budushchee [The development of the Arab monarchies of the Gulf: a breakthrough into the future]. *Aziya i Afrika segodnya [Asia and Africa today],* 2020, no. 2, pp. 37-42. (in Russian)

2. Savel'ev A.G., Karasev P.A. Perspektivy regulirovaniya i snizheniya voennoj kiberugrozy [Prospects for regulation and reduction of the military cyber threat]. *Bulletin of the Moscow University. Series 12, Political Science*, 2018, no. 5, pp. 47-61. (in Russian)

3. Abu-Taieh E. Cyber security crime and punishment: comparative study of the laws of Jordan, Kuwait, Qatar, Oman, and Saudi Arabia. *International Journal of Cyber Warfare and Terrorism*, 2018, № . 3, pp. 46-59.

4. al-Mutairi N.H. The Right to Privacy in the Digital Age as Expressed in a Muslim Country: A Case Study of Kuwait. *Arab Law Quarterly,* 2022, no. 1, pp. 1-28.

5. Ashour S.M.K. The regional security system in the Middle East in the context of international changes since 2011. *Iraqi Journal Of Political Science,* 2022, no. 6, pp. 1-15.

6. Hakmeh J. Cybercrime Legislation in the GCC Countries. Fit for Purpose? Available at: https://www.chathamhouse.org/sites/default/files/publications/research/2018-07-04-cybercrime-legislation-gcc-hakmeh-final.pdf (date of access: 21.04.2023).

7. Hassib B., Shires J. Cybersecurity in the GCC: From Economic Development to Geopolitical Controversy. *Middle East Policy*, 2022, vol. 29, no. 1, pp. 90-103.

8. Ko K. An Analysis of Cybersecurity Threats and Countermeasures in the Kuwaiti Banking Sector. *Kuwait Journal of Information Technology and Decision Sciences*, 2023, vol. 1, no. 1, pp. 1-8.

9. Levac L. Kuwait: Law regarding Electronic Transactions in force – introduction of a concept akin to data privacy. Available at: https://www.globalcompliancenews.com/2015/12/11/kuwait-law-regarding-electronic-transactions-in-force-introduction-of-a-concept-akin-to-data-privacy/ (date of access: 25.04.2023).

10. 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, pp. 96-101.

11. Semsari M. C., Keskin O. Threats to Energy Security and Energy Policies in Central Asia and the Middle East. Handbook of Research on Cyber Approaches to Public Administration and Social Policy. *IGI Global*, 2022, pp. 343-364.

Сведения об авторе

Цуканов Леонид Вячеславович
аспирант, кафедра востоковедения, департамент (факультет) международных отношений
Уральский федеральный университет им. первого Президента России Б. Н. Ельцина
Российская Федерация, 620050, г. Екатеринбург, ул. Мира, 19
e-mail: leon.tsukanov@mail.ru
ORCID 0000-0001-6882-9841

Information about the author

Tsukanov Leonid Vyacheslavovich
Postgraduate, Department of Oriental Studies, Department (Faculty) of International Relations
Ural Federal University named after the First President of Russia B. N. Yeltsin
19, Mir st., Yekaterinburg, 620050, Russian Federation
e-mail: leon.tsukanov@mail.ru
ORCID 0000-0001-6882-9841.

Статья поступила в редакцию **03.05.2023**; одобрена после рецензирования **16.06.2023**; принята к публикации **21.08.2023**
The article was submitted **May, 03, 2023**; approved after reviewing **June, 16, 2023**; accepted for publication **August, 21, 2023**