




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

Research article / Научная статья

## 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>

## 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 Федерацияvgulnara@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 гло-

© Valiakhmetova G.N., Tsukanov L.V., 2022



This work is licensed under a Creative Commons Attribution 4.0 International License.

<https://creativecommons.org/licenses/by/4.0/>

бальную 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>

## Introduction

Digitalization, as a global megatrend, poses a number of threats common to all countries. At the same time, the regional context shapes the specifics of the digital challenge, encouraging countries to develop their own approaches and practices to overcome or reduce new risks. The Arab case is of particular academic and practical interest not only due to the high impact of the Arab world and, more broadly, the Greater Middle East,<sup>1</sup> on the global agenda. The interplay of global and regional trends in this part of the world is complex and contradictory, and regional developments can overtake as well as slow down or even counteract global trends, sometimes shaping the opposite direction and

<sup>1</sup> Within the framework of this study, the conventional term “Arab world” refers to the geopolitical space encompassing the 22 countries that are members of the League of Arab States (LAS), the main platform for inter-Arab cooperation. The Arab world is a system-forming element of the Middle East subsystem of international relations and, more broadly, the Greater Middle East (English equivalent to MENA, or Middle East and North Africa region), which in this article is understood as a geopolitical region consisting of Arab countries, Türkiye, Iran, and Israel.

nature (Baranovsky & Naumkin, 2018; Zvyagelskaya, Svistunova & Surkov, 2020b).

Scientific reflection on the development of the Middle East in a changing global context is accompanied by the development of new theoretical approaches and the research of the possibilities of their application to regional realities. The distinctive feature of academic publications by Russian experts in Middle Eastern and Arab studies is the combination of political or economic analysis with historical research methods, which allows creating predictive scenarios taking into account the historical specifics of the region (Filonik & Isaev, 2020; Melkumyan, 2020; Zvyagelskaya & Kuznetsov, 2017).

In this approach, Vladimir Baranovsky and Vitaly Naumkin reveal the specifics of the refraction of global megatrends in the Middle East, the formation of regional space and a common regional identity based on the Arab component. Since the formation of nationhood in the Arab countries took place during the colonial period, constant attributes of the region have become a constant lack of security, exclusivity (consolidation in opposition to common “foe,” which Türkiye, Israel, and now Iran are

considered to be), a high degree of involvement of global actors in regional affairs and the “habituation effect” to the presence of external interests in the region, as well as the permanently growing conflict against the background of the weakening of subregional integration (Baranovsky & Naumkin, 2018).

An analysis of the interaction in the Middle East of global and regional trends through the prism of the concept of “negative uncertainty” leads international researchers to similar conclusions about the deregionalization and fragmentation of the integration platforms available in the Arab world, about maintaining the region unity due to the high level of conflict. Signs of the contemporary Middle East political arena are also the growth of regional rivalry and the activity of regional powers seeking to use external interests to realize their own ambitions; a high degree of mistrust and suspicion; fragile bilateral relations and an increase in tactical (situational) alliances, including with external actors; a weakening of US and Western interest in the region and, as a result, a consequent desire to reduce their involvement in the regional agenda; a declining role of “soft power” and replacing it with “hard power” tools in the form of proxy wars and direct interventions (Shumilin, 2019; Zvyagelskaya, Svistunova & Surkov, 2020b).

The notion of “uncertainty” has also entered the scientific lexicon of socio-economic researchers of the Middle East realities. A variety of economic models, the presence of an impressive economic, technological and social gap between the Arab countries, which is intensified by the declining role of most Arab economies in the economy, create conditions for growing tension in the region and leave little space for integration initiatives. The diversity of economic models, the sizeable economic, technological and social gaps between Arab countries, which are exacerbated by the declining role of most Arab economies in the world economy, create conditions for growing tensions in the region and leave little room for integration initiatives (Filonik & Isaev, 2020; Melyantsev, 2020).

Russian researchers enrich the concepts developed in foreign scientific communities with

their own approaches. As part of the development of the neo-modernist approach, an alternative to modernism and postmodernism, Vasily Kuznetsov explores the problem of overcoming the socio-political fragmentation of Arab communities (Kuznetsov, 2019; 2020). The leading scholars of the IMEMO RAS systematize a vast layer of political identity concepts, identifying the factors for choosing foreign policy priorities for the Middle Eastern countries (Zvyagelskaya et al., 2020a). The phenomenon of permanently increasing conflict and the changing role of external actors in ensuring security in the Middle East is studied by Vitaly Naumkin based on the concepts of right-sizing and right-peopling (Naumkin, 2019) and the theory of deeply divided societies (Naumkin, 2015).

The empirical material of the Middle East allows a team of researchers from MGIMO University of the Russian Foreign Ministry to refute the theory of waves of democratization popular abroad, on the basis of which Western authors defend the thesis about the positive impact of information technology on the democratic choice of modern countries. Russian researchers convincingly argue that extrapolating the global trend of digitalisation to Arab countries, with their late subjectivity in the system of international relations, incomplete state-building, hybrid political systems combining traditional and modern elements, as well as numerous imbalances in institutional development, could generate a rollback of countries to authoritarianism and even archaism (Lebedeva et al., 2016). Another example of a critical approach to the analytical potential of Western concepts is the study by Elena Zinovieva (2018), whose scientific novelty is due to the use of methodological tools of the theory of social constructivism to study the mutual impact of the scientific and technological spheres and world political processes.

The problems of building a collective cybersecurity system in the Arab world have recently appeared on the political and scientific agenda and have so far been little studied both in Russia and abroad. In the Russian academic field, the digital issues of the region are

represented mainly by studies of the phenomenon of cyberterrorism and the role of information and communication technologies (ICT) in mobilizing a protest resource using the example of the Arab Spring. The country cases cover, as a rule, non-Arab countries of the Middle East — Iran, Israel and Türkiye. A similar picture is observed in foreign publications; however, representatives of the Western and Middle Eastern scientific communities are more actively turning to Arabic topics, expanding the empirical and analytical base of research on regional cybersecurity issues. In this context, there are studies on the digital security practices of individual Arab countries (Alaleeli & Alnajjar, 2020; El-Houssami & Rizk, 2020; Shat et al., 2013), the role of external actors (Liu, 2021; Mogielnicki, 2021) and Israel<sup>2</sup> in providing cybersecurity of the region's leading economies, as well as various aspects of the digital challenge requiring a collective Arab response (Alrawabdeh, 2009; Pöpper et al., 2021).

In general, despite the exceptional variety of approaches and research topics on the specifics of development trends in the Arab world, including in the context of information threats, the problems of reshaping the region into a single cybersecurity space are still fragmentarily presented in scientific publications. This article fills this gap to some extent by seeking to answer the question of whether the digital challenge can be a factor that enables the Arab world to overcome traditional divisions and come together to develop a collective response.

The general theoretical basis of the research is the fundamental scientific works of Manuel Castells (2002; 2010), the greatest researcher of the information age, which allowed us to consider the Arab world not only as an

<sup>2</sup> See: 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).

independent cluster, but also as part of a global digital society. The assessment of the current state of readiness of Arab countries to repel digital threats is carried out mainly based on the methodology of the Global Cybersecurity Index, a research mega-project of the International Telecommunication Union (ITU) of the United Nations.<sup>3</sup> When compiling the rating, ITU experts consider five criteria: the regulatory and legal system of national cyber defense, technical capabilities, organizational structure, capacity development measures and international cooperation. Within the framework of this research, these parameters will be considered through the problems of inter-Arab cooperation and the interaction of the Arab world with external actors. There used methods of structural, system and statistical analysis, event analysis, and forecasting scenario.

### **The Specifics of the Arab Digital Threats Space**

Digitalization processes started in the Arab world almost a decade later than in the countries of the Global North. The region saw explosive growth in Internet users in the 2000s, surpassing the global average in 2015 and reaching 62.96% in 2019.<sup>4</sup> Although the Arab component of the Global South still lags far behind the OECD countries in terms of Internet penetration (85.08%)<sup>5</sup>; in terms of the number of mobile cellular subscribers per 100 people, this gap is already insignificant (103.2 and 120.2 people, respectively<sup>6</sup>).

At the forefront of the movement towards a digital society are the Persian Gulf monarchies,

<sup>3</sup> Global Cybersecurity Index (hereinafter — 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).

<sup>4</sup> 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).

<sup>5</sup> Ibid.

<sup>6</sup> 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).

where the level of Internet penetration has doubled over the past decade and now stands at 95% and above, ahead of the leaders of the Global North in this parameter, and the United Arab Emirates (UAE) has become the first and so far the only country in the world with the number of Internet users at 100%.<sup>7</sup> At the opposite pole of the Arab world are the least developed and politically unstable countries with Internet penetration of 30% or less; in the “average” group of countries, this indicator varies in the range of 57.2—72%.<sup>8</sup> The growth of Internet activity increases the risk of cyberattacks, creating different types of threats in this heterogeneous and controversial region.

Due to the successful modernization, diversification and digitalization of their economies as part of the large-scale long-term “Vision” programs, the Gulf monarchies are the most rapidly increasing their presence in cyberspace. It is they who become the main targets for financially oriented cybercrime, the damage from which in these countries amounts to billions of dollars.<sup>9</sup>

At the same time, unlike other regions, in the Arab world, cyberattacks are focused mainly on access to commercial, technological and nation secrets (63.6%), rather than on the theft of financial (6.2%) and personal data (29.6%).<sup>10</sup>

<sup>7</sup> 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).

<sup>8</sup> Ibid.

<sup>9</sup> See: 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 Battlefield: Cyber Security across the GCC // Gulf International Forum. October 29, 2018. URL: <https://gulif.org/the-new-battlefront-cyber-security-across-the-gcc/> (accessed: 30.10.2021).

<sup>10</sup> 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](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). This specificity explains the impressive growth of cyber-attacks in the Gulf area during the preparation and holding of such major world events as Dubai Expo 2020 and Qatar World Cup

In terms of the number of cyberattacks, the regional rating has traditionally been led by the Gulf monarchies, but in recent years they have impressively strengthened their protection: in 2021, the Kingdom of Saudi Arabia (KSA) and the UAE dropped to 3rd and 4th places respectively in the Arab index (ranks 30 and 36 in the world).<sup>11</sup> Nevertheless, they, along with the United States, remain in the top three world leaders with the most expensive data breaches.<sup>12</sup> A critical asset for the Gulf monarchies is the oil and gas sector, which tends to be concentrated in narrow geographical areas, which greatly increases the damage from cyberattacks. Over the past decade, the Saudi oil and gas giant “Saudi Aramco” and the Qatari “RasGas” have been the victims of major attacks using sophisticated malware (2012, 2016, 2017) and drones (2019) multiple times. Such attacks have not only global economic consequences, from rising oil prices to cascading effects on various sectors of the world economy (Pöpper et al., 2021, pp. 96—97). We are talking about the use of so-called digital weapons, which are developed by countries, in connection with which such attacks are interpreted as an act of external aggression, creating the potential for a retaliatory cyber strike (Saveliev & Karasev, 2018).

2022. The experts of the Gulf International Forum note that “74% of CEOs in the region view the risk of breaches in data privacy as the most pertinent threat to stakeholder trust in the business, much higher than the global average of 55% determined by a global.” Cited by: The New Battlefield: Cyber Security across the GCC // Gulf International Forum. October 29, 2018. URL: <https://gulif.org/the-new-battlefront-cyber-security-across-the-gcc/> (accessed: 30.10.2021).

<sup>11</sup> As of the December 31, 2021. See: Kaspersky Cyberthreat Real-Time Map. URL: <https://cybermap.kaspersky.com/> (accessed: 31.12.2021).

<sup>12</sup> The elimination of the consequences of each of their similar violations, at an average cost of more than 5 million USD, can take several months and cause serious financial, economic, and reputational damage. See: 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).

The high degree of cyber threats from state actors in regional and global politics, as well as the relatively low level of readiness of the Arab countries to repel them, are another feature of the region.<sup>13</sup> The practice of using breakthrough digital technologies as a power component in interstate conflicts has become widespread in the Middle East after a cyber-attack on Iran's nuclear research center in 2010 using a new generation virus, Stuxnet, which was recognized as the first example of a cyber-weapon due to its colossal destructive potential. Large-scale cyber-weapon tests conducted in the Middle East in 2010—2012 presumably by the United States and Israel<sup>14</sup> drew Iran into the digital arms race and then other countries in the region.

In 2015, there emerged evidence that the governments of Bahrain, Egypt, the KSA, Lebanon, Morocco, Oman, Sudan, and the UAE, were involved in the purchase of spyware and other malicious digital tools from abroad.<sup>15</sup> Secret cooperation with Israel, one of the leaders in the global cyber-weapons market, has provided a number of Gulf monarchies with effective tools to counter Iran, fight terrorism and

control internal opposition.<sup>16</sup> The interstate confrontation in the cyberspace of the Middle East runs primarily along the lines of the KSA — Iran, Israel — Iran, the USA — Iran, and is also being implemented in the context of regional crises (Syrian, Yemeni, Qatari, etc.). At the same time, cyber weapons used, for example, in the Saudi-Iranian proxy conflict in Yemen, are used throughout the Middle East and beyond.<sup>17</sup> The use of ICT by Arab countries as an instrument of foreign and national policy significantly worsens the regional environment, increasing its already high conflict potential.

In addition to countries, the carriers of threats in the Arab digital space are non-systemic actors in regional politics in the form of cyber groups, allegedly sponsored at the governmental level, as well as hacktivists and lone hackers, whose activity also often goes far beyond the Middle East. Moreover, the globalization of cyber threats emanating from the region is due to the activities of numerous radical extremist and terrorist groups that conduct so called cyber jihad against the “infidels” in the Global Network.<sup>18</sup>

Thus, from the triad of cyber threats, in the context of which the UN defines the concept of “international information security,” for the Arab world, the threat of using ICT for military-political purposes, as a tool of interstate confrontation and interference in the internal affairs of sovereign countries is of paramount

<sup>13</sup> 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](https://www.internetsociety.org/wp-content/uploads/2020/04/Internet_Infrastructure_Security_Guidelines_for_Arab_states-EN.pdf) (accessed: 30.10.2021).

<sup>14</sup> Rayu K., Emm, D. Kaspersky Security Bulletin 2013: Evolution of Threats in 2013 [Раю К., Эмм Д. Kaspersky Security Bulletin 2013: Развитие угроз в 2013 году] // Securelist. December 11, 2013. (In Russian). URL: <https://securelist.ru/analysis/ksb/19140/kaspersky-security-bulletin-2013-razvitie-ugroz-v-2013-godu/> (accessed: 21.10.2021). Today, the means of conducting digital wars (cyber wars) range from relatively simple hacker programs to ICT equated to strategic offensive weapons, and serious material or political damage to the state can also be inflicted by technically poorly trained groups using widely available virus programs (for example, hacktivists in the framework of protest actions). See for example: (Kabernik, 2013).

<sup>15</sup> Unidentified People Hacked into the Network of a Spyware Supplier for Government Intelligence Agencies [Неизвестные взломали сеть поставщика шпионского ПО для правительственных спецслужб] // SecureLab. July 06, 2015. (In Russian). URL: <http://www.securitylab.ru/news/473587.php> (accessed: 21.11.2021).

<sup>16</sup> 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).

<sup>17</sup> From Shamoon to StoneDrill. Wiper-like Programs Attack Companies in Saudi Arabia and Beyond [От Shamoon к StoneDrill. Wiper-подобные программы атакуют компании в Саудовской Аравии и не только] // SecureList. March 6, 2018. (In Russian). URL: <https://securelist.ru/from-shamoon-to-stonedrill/30350/> (accessed: 21.11.2021).

<sup>18</sup> 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). See also: (Bunt, 2003).

importance. Countering this type of threat directly depends on the stabilization of the military-political situation and the settlement of numerous conflicts in the Middle East, which, in turn, requires the combined efforts of regional actors and support from the international community. Other types of threats — cybercrime and cyberterrorism — also form a common challenge for the Arab countries, prompting the development of cybersecurity not only at the national but also at the regional level.

### **Cybersecurity in the Arab World: Trends and Problems of Development**

In recent years, a number of Arab countries have significantly improved their positions in the ITU Global Cybersecurity Index. The most impressive results are in the KSA and the UAE, which in 2020 entered the top five world leaders; Qatar, Kuwait and Jordan also demonstrate a “sprint” approach.<sup>19</sup> Oman and Egypt,<sup>20</sup> Tunisia, Morocco, and Bahrain, which were the first of the Arab countries to start creating national cybersecurity systems, are characterized by a progressive type of development. In this regional top ten, the ITU index ranges from 99.5 (KSA) to 70.9 (Jordan). The rest of the Arab countries

<sup>19</sup> The KSA and the UAE moved up, respectively, from 46th and 47th positions in the global rankings in 2017 to 2nd and 5th places in 2020. Kuwait moved from 138th place in 2017 to 64th line in 2020 and from 17th to 9th place in the Arab ranking. See: GCI 2017. P. 59—64. URL: [https://www.itu.int/dms\\_pub/itu-d/otp/str/D-STR-GCI.01-2017-R1-PDF-E.pdf](https://www.itu.int/dms_pub/itu-d/otp/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/otp/str/D-STR-GCI.01-2021-PDF-E.pdf](https://www.itu.int/dms_pub/itu-d/otp/str/D-STR-GCI.01-2021-PDF-E.pdf) (accessed: 30.10.2021).

<sup>20</sup> Prior to 2020, Oman and Egypt led the Regional Cybersecurity Rankings by a wide margin, with Oman ranked among the top three global leaders in 2014 and ranked 4th in the world in 2017. In 2020, both countries moved down in the ITU Index by 21 and 23, respectively (3rd and 4th places in the Arab region), nevertheless, continuing to outperform a number of European states. See: GCI 2015. P. 1. URL: [https://www.itu.int/dms\\_pub/itu-d/otp/str/D-STR-SECU-2015-PDF-E.pdf](https://www.itu.int/dms_pub/itu-d/otp/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/otp/str/D-STR-GCI.01-2017-R1-PDF-E.pdf](https://www.itu.int/dms_pub/itu-d/otp/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/otp/str/D-STR-GCI.01-2021-PDF-E.pdf](https://www.itu.int/dms_pub/itu-d/otp/str/D-STR-GCI.01-2021-PDF-E.pdf) (accessed: 30.10.2021).

have a low level of cyber defense, ranking 104—182 in the global ranking with an index below 35.<sup>21</sup> In general, the analysis of ITU data indicates a “catching up” type of development of the national cybersecurity sector and the presence of a significant digital gap between the countries of the Arab world.

In the field of digital security regulation, most Arab countries have already taken serious steps: 17 countries have legislation on illegal access to information, 14 — on data protection legislation, 12 — on breach notification measures, 11 — on online harassment legislation.<sup>22</sup> According to this indicator, the Arab world shows trends similar to other regions: the presence of legal norms to prevent and counter criminal activity in cyberspace, as a rule, is typical for countries with high and medium levels of Internet penetration, stable economies and governments’ focus on digitalization.<sup>23</sup> At the same time, in the Arab world, where Islam regulates various spheres of life, the legislative process to one degree or another requires coordination with the norms of Sharia,<sup>24</sup> primarily with the norms of Islamic law (*fiqh*) (Syukiyainen, 2016; 2019).

Among other factors hindering the adaptation of the national legislations of the Arab countries to the realities of the digital age, one should note a certain inertia of the legal and regulatory sphere, a reactive approach to

<sup>21</sup> GCI 2020. P. 25—27. URL: [https://www.itu.int/dms\\_pub/itu-d/otp/str/D-STR-GCI.01-2021-PDF-E.pdf](https://www.itu.int/dms_pub/itu-d/otp/str/D-STR-GCI.01-2021-PDF-E.pdf) (accessed: 30.10.2021). The Maximum value of the ITU Index is 100.

<sup>22</sup> Ibid. P. 3—6.

<sup>23</sup> Ibid. P. 4—5.

<sup>24</sup> Thus, the KSA lacks a criminal code and a number of other attributes of the Romano-Germanic legal system. Since the country’s legislation is based on Islamic law, Sharia norms prevail in law enforcement practice, including in the field of regulation of the internet space. See: Kingdom of Saudi Arabia // Scientific and Technical Center of the Federal State Unitary Enterprise “GRFC” [Королевство Саудовская Аравия // Научно-технический центр ФГУП «ГРЦЦ»]. March 29, 2021. (In Russian). URL: <https://rdc.grfc.ru/2021/03/saudi-arabia/> (accessed: 21.11.2021). On the specifics of the perception of digitalization in the system of Islamic values see for example: (Faizi & Abubakar, 2021).

filling in the gaps in the legislation, stopping certain aspects of the problem instead of a comprehensive solution, excessive bureaucratization of the legislative process, etc. Overcoming these barriers will pave the way for the harmonization of Arab legislation and the formation of a regional cybersecurity system.<sup>25</sup>

The presence of Computer Incident Response Teams (CSIRTs), or Computer Emergency Response Teams (CERTs), is a key indicator for ITU's assessment of technical cybersecurity measures. The CSIRT model is based on the principles of openness and cooperation and assumes that technical and technological protection can be ensured not by "building moats and pulling up the drawbridge" around the Internet infrastructure but by creating an atmosphere of trust and conditions for a wide exchange of information and experience.<sup>26</sup>

National CSIRTs/CERTs operate in 17 Arab countries, exclusively as government agencies.<sup>27</sup> In a number of countries, their activities are not limited to traditional digital infrastructure protection or direct technical support to government authorities, but also include conducting awareness-raising campaigns and cyber exercises, accrediting cybersecurity experts and other activities to increase national cyber capacity, develop and deepen relations with various cybersecurity actors. In addition, 10 Arab countries have established sector-specific CSIRTs, mainly in the telecommunications or energy sectors.<sup>28</sup>

<sup>25</sup> 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/CIEM5\\_ESCWA2\\_en.pdf](https://unctad.org/system/files/non-official-document/CIEM5_ESCWA2_en.pdf) (accessed: 10.10.2021).

<sup>26</sup> 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](https://www.internetsociety.org/wp-content/uploads/2020/04/Internet_Infrastructure_Security_Guidelines_for_Arab_states-EN.pdf) (accessed: 30.10.2021).

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

<sup>28</sup> See: GCI 2020. P. 8. URL: [https://www.itu.int/dms\\_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf](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.

According to experts, CSIRTs have already played a key role in protecting Arab states' Internet structures, but their effectiveness is limited by a lack of finance, equipment, specialists and skills, a challenge faced not only by underdeveloped countries but also by advanced ones.<sup>29</sup> In addition, unlike other regions, the Arab national CSIRTs cooperate less with the private sector and other stakeholders.<sup>30</sup> Weak horizontal links of CSIRTs have so far prevented any Arab state from achieving the maximum ITU indicator for technical measures.<sup>31</sup>

However, there is a growing trend in the Arab world to develop public-private partnerships at the national level, especially with the emergence of sectoral CSIRTs. A number of countries are developing methods and practices for identifying and removing legal and other barriers to the interaction of various cybersecurity actors — government agencies, business structures, research communities,

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](https://www.internetsociety.org/wp-content/uploads/2020/04/Internet_Infrastructure_Security_Guidelines_for_Arab_states-EN.pdf) (accessed: 30.10.2021).

<sup>29</sup> Thus, CERT Bahrain was formed with the sponsorship of Washington, which was interested in strengthening the security of the largest US naval base in the Middle East, located in this sheikhdom. See: The New Battlefield: Cyber Security across the GCC // Gulf International Forum. October 29, 2018. URL: <https://gulrif.org/the-new-battlefront-cyber-security-across-the-gcc/> (accessed: 30.10.2021). Another example demonstrates the KSA, where, as part of the priority of cybersecurity of critical infrastructure, the authorities have taken a course for regular centralized purchases abroad (mainly in the USA) of software and other ready-made solutions. See: 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).

<sup>30</sup> 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](https://www.internetsociety.org/wp-content/uploads/2020/04/Internet_Infrastructure_Security_Guidelines_for_Arab_states-EN.pdf) (accessed: 30.10.2021).

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



ordinary Internet users, as well as non-system actors such as “white hats.”<sup>32</sup>

The obstacles to building a sustainable regional digital infrastructure are the traditional atmosphere of distrust in the Arab world and the managerial model of “top-down control” by the government. Under this approach, various state agencies and government-controlled CSIRTs, acting on national priorities (including in the interests of national intelligence services), face distrust from foreign colleagues.<sup>33</sup> In other words, there is a true demand for trust and strategic flexibility in the region.

Significant steps in this direction have already been taken. In 2012, the ITU Regional Center for Cybersecurity for the Arab Region (ITU-ARCC),<sup>34</sup> under the operational management of the Oman National CERT was established in Muscat. The latter is also responsible for coordinating the CERT of the Gulf monarchies.<sup>35</sup> Interaction also takes place on the sidelines of the Arab Regional Cybersecurity Summit<sup>36</sup> and the Organization of Islamic Cooperation (OIC).<sup>37</sup>

Arab countries also participate in global initiatives to deepen cybersecurity knowledge and build relationships at the intergovernmental and intersectoral levels. Thus, 7 Arab states (Egypt, Qatar, the KSA, Morocco, Oman, Tunisia, the UAE,) cooperate in the Global Forum of Incident Response and Security Teams (FIRST). The KSA and the UAE have the largest

representation among the Arab participating countries, respectively 9 and 5 government and industry groups.<sup>38</sup>

The third pillar of the ITU — organizational measures — includes mechanisms for managing and coordinating the cybersecurity sphere at the level of the executive branch, the private sector and civil society. The cornerstone of organizational measures is the existence and characteristics of the National Cybersecurity Strategy (NCS). Its evaluation is carried out according to a number of parameters: focus on the protection of critical infrastructure (available in 13 Arab countries); regular updates in the context of new threats and priorities (6 states); national cybersecurity audits performed at the national level and metrics for assessing cyberspace associated risk at the national level (9 countries), etc.<sup>39</sup> The dependence of the development of the national digital industry and cybersecurity on external assistance, primarily from the UN and the countries of the Global North, forms in the Arab world similar methodological approaches to the concept of “cybersecurity,” which is synonymous with the term “information security” and covers a wide range of problems related to technical and technological protection of information systems and networks.<sup>40</sup>

<sup>32</sup> 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](https://www.internetsociety.org/wp-content/uploads/2020/04/Internet_Infrastructure_Security_Guidelines_for_Arab_states-EN.pdf) (accessed: 30.10.2021).

<sup>33</sup> Ibid. P. 14.

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

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

<sup>36</sup> The 9th meeting was held in KSA in November 2021, along with the annual (13th) conference of the CERTs of the OIC member countries. See: CERTs in an Evolving Cybersecurity Landscape. URL: <https://www.oic-cert.org/event2021/> (accessed: 10.12.2021).

<sup>37</sup> 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).

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

<sup>39</sup> GCI 2020. P. 10–13. URL: [https://www.itu.int/dms\\_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf](https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf) (accessed: 30.10.2021). The last of these parameters is also implemented at the regional level on the online platform of the ITU-ARCC in Oman, where all Arab countries have the opportunity to assess their cyber risks in real time. See: About OCERT Services // Oman National CERT. URL: <https://cert.gov.om/services.aspx> (accessed: 10.12.2021).

<sup>40</sup> See for example: 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](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

Currently, only three Arab countries — the KSA, Oman and Egypt, have reached the maximum ITU indicator for organizational measures; the UAE and Qatar<sup>41</sup> also have a high index; the rest have yet to address serious gaps in the cyber defense management system. Sluggishness in the development of the NCS, institutionalization and centralization of cybersecurity on one platform in the Arab countries is due to a reactive rather than proactive approach to parrying threats, a “top-down” management model that gives rise to many government institutions with often duplicating functionality and a low level of interagency cooperation, as well as limited financial and human resources; weak horizontal links between various cybersecurity actors.<sup>42</sup> In addition, investments in cybersecurity are implemented mainly through programs to modernize the military potential and protect the most significant industries (energy, financial and ICT),<sup>43</sup> which is due to the economic and military-political specifics of the region.

According to researchers, the US played a key role in eliminating the fragmentation of the Saudi cybersecurity space, setting this task as one of the main components of the 2017 agreement on the modernization of the Saudi military forces worth 110 bln USD.<sup>44</sup> Increasing

---

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](https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/SaudiArabia_NISS_Draft_7_EN.pdf) (accessed: 15.12.2021).

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

<sup>42</sup> 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](https://www.internetsociety.org/wp-content/uploads/2020/04/Internet_Infrastructure_Security_Guidelines_for_Arab_states-EN.pdf) (accessed: 30.10.2021). See also: (Pöpper et al., 2021, p. 97).

<sup>43</sup> 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).

<sup>44</sup> See: 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->

cyber readiness to ensure the security of both their own and external partners is typical for those Arab countries that are of military-political and/or economic importance for non-regional actors. It explains the build-up of national cyber potential with the active participation of external forces not only in the advanced countries of the region, but also in the least developed ones, for example, in Somalia and Djibouti,<sup>45</sup> where foreign military bases are located.

Countries that are not of interest to external actors due to their economic backwardness or political instability cannot count on financial, technological and personnel assistance from outside. Thus, the decrease in the role of the Palestinian factor in the regional agenda (Naumkin, 2019, pp. 75—78; Shumilin, 2019, p. 116) led to a significant reduction in foreign assistance to Palestine in the formation of the national ICT and cyber defense sector and, as a result, a drop in the country’s rating in the ITU Global Index from 102 in 2017 to 122 in 2020.<sup>46</sup> In other words, the increasingly selective and pragmatic approach of external sponsors to support Arab digitalization and cybersecurity programs will have an increasing

---

saudi-arabia/ (accessed: 10.12.2021); The New Battlefield: Cyber Security across the GCC // Gulf International Forum. 2018. URL: <https://gulffif.org/the-new-battlefront-cyber-security-across-the-gcc/> (accessed: 30.10.2021).

<sup>45</sup> 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).

<sup>46</sup> See: 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](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](https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf) (accessed: 30.10.2021). For more information on foreign assistance programs to Palestine in the field of ICT development and cybersecurity, see: 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. See also: (Shat et al., 2013).

impact on the growing digital divide in the Arab world.

The fourth indicator of countries' readiness to repel cyber threats is capacity development measures which include the training of their own personnel, availability of specialized educational programs and research institutes, support for small and medium-sized businesses and the development of public-private partnerships. According to this parameter, only 4 states have the maximum ITU index — Qatar, the KSA, the UAE and Oman. Egypt also has a high indicator, for the rest of the Arab countries it is an area of potential growth.<sup>47</sup>

Despite the recognition of the importance of this group of measures by the Arab governments, they are implemented mainly at the suggestion and with the support of Western partners.<sup>48</sup> In addition, there is a serious imbalance in the geography of agreements in the field of public-private partnerships involving two or more Arab companies: such interaction is carried out mainly between the Gulf monarchies, while in the rest of the Arab world it is absent or limited to single episodes.<sup>49</sup>

The problem of “brain drain,” which is not new for the region, is also becoming a serious challenge for the Arab world,<sup>50</sup> but it has become especially acute with the launch of reforms in the field of digitalization. Despite the obvious success<sup>51</sup> in training their own personnel

(Alaleeli & Alnajjar, 2020), the outflow of professionals to Western countries continues, and for qualified personnel from Arab countries, even the leading economies of the region, represented by the Gulf states, are significantly inferior to such migration destinations in terms of their attractiveness like USA, EU and Canada.<sup>52</sup> Taking into account the outflow of the population from the turbulent zones of the region and the significant socio-economic gap between the Arab countries, including in the human development index (Melyantsev, 2020), the movement of human capital will increase technological inequality in the Arab world and hinder its integration.

### **International Cooperation of Arab Countries in the Field of Cybersecurity**

International cooperation is the cornerstone of national and regional cybersecurity, however, it is on this parameter that the positions of the Arab countries are the most vulnerable and indicate the presence of a significant “digital divide.”<sup>53</sup> As in other regions, in such a sensitive area as cybersecurity, Arab countries prefer to enter into multilateral agreements (12 countries) and other international formats of participation

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

<sup>48</sup> 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). See also: (Pöpper et al., 2021, pp. 98—100).

<sup>49</sup> The pattern was derived based on the analysis of data contained in the open databases of counterparties in the Arab countries of the Middle East, as well as the register of joint companies with Arab partners registered in the United States. See for example: Public Register // Qatar Financial Centre. URL: <https://eservices.qfc.qa/qfcpublicregister/publicregister.aspx> (accessed: 12.12.2021).

<sup>50</sup> 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).

<sup>51</sup> See for example: 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).

<sup>52</sup> 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).

<sup>53</sup> According to the ITU Index 2020, only the KSA, the UAE and Oman peaked; they are followed by states with a relatively high (Qatar, Egypt, Morocco, Tunisia) and an average level (Kuwait, Jordan, Bahrain) of intergovernmental cooperation; other countries have extremely low (Libya, Algeria, Somalia, Iraq, Lebanon, Comoros) and even zero scores (Djibouti, Yemen, Mauritania, Palestine, Syria, Sudan). See: GCI 2020. P. 71—82. URL: [https://www.itu.int/dms\\_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf](https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf) (accessed: 30.10.2021).

(14 countries) rather than bilateral forms of intergovernmental interaction (11 countries).<sup>54</sup>

The regional trend towards the demand for the active participation of external actors in the formation of the security system (Baranovsky & Naumkin, 2018, p. 13; Shumilin, 2019, p. 111—117) is also manifested in the digital protection segment, both national and collective. The countries of the Global North (the USA, the Great Britain, a number of EU countries, the Republic of Korea, Japan) are represented on the external tracks of interaction; along the South — South line, China and the Muslim countries of Southeast Asia act as partners of the Arab world.<sup>55</sup>

The American vision of collective cyber defense architecture in the Arab world, promoted by Washington since the early 2010s, is based on the concept of creating a sub-regional security system in the Persian Gulf that does not require a significant US presence. In this regard, Washington relies on its traditional regional allies — the KSA and the UAE, which it considers as drivers of the process of consolidating the Cooperation Council for the Arab States of the Gulf (Gulf Cooperation Council, GCC) to jointly counter digital threats with the subsequent transformation of this association into the integration core of the pan-Arab cybersecurity system (Alazab & Chong, 2015). This approach is implemented mainly within the framework of the US military cooperation with the Gulf monarchies and support for the GCC initiatives in the development of the military segment of digital defense (“Cyber Shield of the Peninsula”, etc.<sup>56</sup>).

<sup>54</sup> GCI 2020. P. 20—21. URL: [https://www.itu.int/dms\\_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf](https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf) (accessed: 30.10.2021). Thus, for example, the KSA is limited to only two bilateral agreements on cooperation in the field of cybersecurity — with the UAE and the UK. See: Saudi Arabia // UNIDIR. March, 2021. URL: <https://unidir.org/cpp/state-pdf-export> (accessed: 20.10.2021).

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

<sup>56</sup> See: 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->

China takes a more flexible approach, which is also based on the general principles of the country’s Middle East policy, allowing Beijing to focus on pursuing economic interests, while avoiding immersion in regional disputes (Liu, 2021). Accordingly, in matters of cybersecurity, the PRC adheres to multilateral formats of interaction with the Arab world, considering the Arab League as the main integration platform<sup>57</sup> and proposing regional technological cooperation projects within the framework of the “Belt and Road” and “Digital Silk Road” initiatives.<sup>58</sup> The priority areas of China’s cooperation with the Arab League countries are the development of digital infrastructure, FinTech and online trading,<sup>59</sup> and with the GCC countries, in addition, the promotion of blockchains, cryptocurrencies and other technologies that ensure financial security, including for cross-border payments,<sup>60</sup> as well as technological

security-and-the-kind-of-political-and-military-cooperation-with-the-united-states/ (accessed: 18.12.2021); The 5x5 — 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).

<sup>57</sup> 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).

<sup>58</sup> 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).

<sup>59</sup> 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](http://www.xinhuanet.com/english/2021-07/19/c_1310069392.htm) (accessed: 22.12.2021).

<sup>60</sup> See: 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 // Nikkei 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).

solutions in the field of optimizing public services and reducing wasteful spending (Mogielnicki, 2021, p. 173).

Thus, in relation to the Arab world, a certain balance of power has been achieved in the technological rivalry between the United States and China, since Washington and Beijing pursue different long-term goals and use different methods for their implementation. Moreover, a certain similar vision of ensuring stability in the Greater Middle East has emerged between the two powers, which, although based on different initial imperatives, comes down to the idea of the key participation of the Arab countries themselves in building a regional security system (Liu, 2021, pp. 81, 93—94; Mogielnicki, 2021, pp. 163, 173—174). Although the desire of leading external actors to reduce their involvement in the regional agenda is perceived very negatively in the GCC (Baranovsky & Naumkin, 2018, pp. 13—14) and does not meet the expectations of the Arab League,<sup>61</sup> it will give impetus to intra-regional integration processes, including in the field of cybersecurity.

The highest intensity of interaction in the field of digital security is observed on the GCC platform. Similar economic models and rates of development, including in the digital segment, the uniformity of political systems and the perception of key cyber threats,<sup>62</sup> combined with the presence of common approaches to ensuring security in the Gulf area, create favorable conditions for the formation of a “united digital front.” However, there is also a

certain technological gap among the Gulf monarchies, in connection with which the “lagging behind” GCC members believe that the Saudi Arabia and the UAE should make the main contribution to ensuring collective cybersecurity. Riyadh and Abu Dhabi, for their part, are not ready for such a “quota” of obligations in order to avoid excessive pressure on their cyber sector (which is fraught with increased vulnerability to external threats), therefore, they give priority to the development of national cybersecurity structures, on the basis of which flexible and sustainable system of collective response to digital challenges will be built.<sup>63</sup> But the main disintegrating factor for the GCC remains numerous contradictions between its members, expressed primarily in the Qatari diplomatic crisis, as well as the current lack of a common position on Iran and Israel (Baranovsky & Naumkin, 2018, p. 14; Pradhan, 2018; Shumilin, 2019, pp. 114—115; Zvyagelskaya, Svistunova & Surkov, 2020b, pp. 97—98).

The problems of joint digital protection have begun to appear more and more often on the agenda of the Arab League summits, and to a large extent under the impact of global institutions, primarily represented by the UN.<sup>64</sup> The League’s overall approach to collective cybersecurity is still under development, but generally suggests that countries with best practices, primarily the KSA, the UAE and Egypt, should assist the Arab “digital periphery” in building technical and human capacity. Arab countries have already taken serious steps in developing cooperation between national CSIRT/CERT<sup>65</sup> and public-private

<sup>61</sup> See: 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](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).

<sup>62</sup> 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).

<sup>63</sup> 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).

<sup>64</sup> Development and Harmonization of Cyber Legislation // *UNCTAD*. 2013. URL: [https://unctad.org/system/files/non-official-document/CIEM5\\_ESCWA2\\_en.pdf](https://unctad.org/system/files/non-official-document/CIEM5_ESCWA2_en.pdf) (accessed: 10.10.2021).

<sup>65</sup> 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](https://www.internetsociety.org/wp-content/uploads/2020/04/Internet_Infrastructure_Security_Guidelines_for_Arab_states-EN.pdf) (accessed: 30.10.2021).

partnerships,<sup>66</sup> training<sup>67</sup> and harmonization of relevant legislation.<sup>68</sup>

At the same time, the integration potential of the Arab League is seriously limited by enormous economic imbalances (Filonik & Isaev, 2020; Melyantsev, 2020), socio-political fragmentation of Arab societies (Kuznetsov, 2020; Melkumyan, 2020; Zvyagelskaya et al., 2020a) and the obvious decline in the interest of external actors and GCC countries in the Arab periphery, the digital development of which is associated with impressive economic costs and high political risks.<sup>69</sup> In this regard, in recent years, the Arab countries have been establishing interaction without the participation of the Gulf monarchies. Examples of such South-South cooperation include the exchange of innovative e-commerce practices between Egypt, Tunisia and Morocco (El-Houssami & Rizk, 2020), as well as the joint training activities of Jordan, Lebanon, Algeria, and Morocco.<sup>70</sup> However, such projects, as a rule, are isolated, have a narrow specialization and do not have sufficient integration potential.

Another platform for interaction between Arab countries is the OIC, within which national CSIRT/CERT<sup>71</sup> interact, the Cyber Security

Center to combat cyberterrorism (2017)<sup>72</sup> and the 5G Security Working Group (2021)<sup>73</sup> operate, and a number of other projects are being implemented. However, taking into account the geography of the participants in this association, which goes far beyond the Arab region, as well as the exceptional heterogeneity and inconsistency of the Islamic world itself, the OIC initiatives can a priori be of the most generalized nature and cover mainly the technical sphere. Therefore, cooperation with the OIC remains an important, but not the determining direction of integration processes in the Arab world, including in the field of cybersecurity.

A new regional trend was laid by the 2020 Abraham Agreements, which paved the way for the normalization of Israel's relations with the UAE and Bahrain and became the culmination of their informal interaction in the field of high technology and cybersecurity for many years. The readiness of Israel and a number of Arab countries to expand cooperation is motivated by the idea of joint opposition to Iran, as well as by a complex of other strategic and commercial interests.<sup>74</sup> In the field of cybersecurity, Israel is focused on cooperation with the Gulf monarchies, primarily the KSA, as well as with Egypt and Jordan, with which interdepartmental ties and public-private partnerships are actively developing, joint long-term digital development programs are being developed, and bilateral

<sup>66</sup> 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).

<sup>67</sup> 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). See also: (Alaleeli & Alnajjar, 2020).

<sup>68</sup> 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).

<sup>69</sup> Ibid.

<sup>70</sup> See for example: Qualls: Jordan Algeria Lebanon Morocco National CTF 2020 // Cyber Talents. July 9, 2020. URL: <https://cybertalents.com/competitions/qualls-jordan-lebanon-and-morocco-national-cyber-security-ctf-2020> (accessed: 10.12.2021).

<sup>71</sup> 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).

<sup>72</sup> 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](https://www.oic-oci.org/topic/?t_id=16023&t_ref=8082&lan=en) (accessed: 10.12.2021).

<sup>73</sup> 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).

<sup>74</sup> See: 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); Khorrani 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-Khorrani.pdf> (accessed: 30.10.2021).

specialized working groups are being created.<sup>75</sup> Countries that are less digitally advanced (Morocco, Sudan), which have also taken a course towards normalizing relations with Israel, are of predominantly commercial interest to the Israeli side, and therefore interaction with them is limited to short-term projects.<sup>76</sup>

According to experts, the tendency to nominate Israel to the role of a cybersecurity guarantor for part of the Arab world, is fraught with destabilization of the entire Middle East region, both in view of the ambiguous position of the Arab countries, including the GCC countries, towards Iran and Israel, and in the light of the reciprocal strengthening of Iran's offensive cyber potential.<sup>77</sup> In addition, according to observers, Israel, actively involved in the construction of a secure digital environment in a number of advanced Arab countries, expects to reduce the intensity of inter-Arab interaction, primarily with countries hostile to it, thereby accelerating their pushing to the periphery of weak and/or connected with Iran (Iraq, Syria, Yemen, etc.).<sup>78</sup>

<sup>75</sup> 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).

<sup>76</sup> 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).

<sup>77</sup> See: 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).

<sup>78</sup> 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).

Overall, the international cooperation of Arab countries in the field of cybersecurity encounters the same obstacles that limit the region's integration potential. These include the lack of a single economic basis, the crisis of pan-Arab identity, and the desire to preserve national sovereignty, which is characteristic of all countries with relatively late subjectivity in the system of international relations, even at the cost of abandoning the obvious benefits of cooperation (Baranovsky & Naumkin, 2018, p. 14; Lebedeva et al., 2016, pp. 23—24), including in the field of digitalization and cyber defense.

### Conclusion

The digital challenge creates for the Arab world a set of unique opportunities and, at the same time, risks for further development. Most Arab countries have recognized the ICT sector as an integral part of their economies and national security. Therefore, the Arab world as a whole is gaining momentum in building cyber defense, demonstrating development trends similar to global ones, but at the same time differing in a variety of strategies, practices, and dynamics for moving towards a secure digital environment. Despite traditional mistrust, there is a growing regional communication effort in the Arab world. There is a clear desire to deepen regional cooperation in the field of cybersecurity where it is appropriate and productive. Obviously, the center of such cooperation is located in the Gulf monarchies. However, even there, these efforts remain mostly reactive and fragmented, and the initiators and sponsors of unification processes are mainly global structures, primarily represented by the UN, as well as the leading economies of the world. In general, the digital factor reinforces the heterogeneity and inconsistency of the Arab world. Therefore, in the foreseeable future, it will not be able to give the necessary impetus to regional integration, despite certain trends towards consolidation.

Received / Поступила в редакцию: 19.01.2022

Revised / Доработана после рецензирования: 24.02.2022

Accepted / Принята к публикации: 18.04.2022

## References

- Alaleeli, S., & Alnajjar, A. (2020). The Arab digital generation's engagement with technology: The case of high school students in the UAE. *Journal of Technology and Science Education*, 1(10), 159—178. <https://doi.org/10.3926/jotse.756>
- Alazab, M., & Chon, S. (2015). Cyber security in the Gulf Cooperation Council. *Social Science Research Network Electronic Journal*, 1—13. <https://doi.org/10.2139/ssrn.2594624>
- Alrawabdeh, B. (2009). Internet and the Arab world: Understanding the key issues and overcoming the barriers. *International Arab Journal of Information Technology*, 1(6), 27—33.
- Baranovsky, V. G., & Naumkin, V. V. (2018). The Middle East in the changing global context: The key trends of centennial development. *World Economy and International Relations*, 3(62), 5—19. (In Russian). <https://doi.org/10.20542/0131-2227-2018-62-3-5-19>
- Bunt, G. (2003). *Islam in the digital age: E-jihad, online fatwas and cyber Islamic environments*. London and Sterling, Virginia: Pluto Press.
- Castells, M. (2002). *The Internet galaxy: Reflections on the Internet, business, and society*. Oxford, UK: Oxford University Press. <https://doi.org/10.1093/acprof:oso/9780199255771.001.0001>
- Castells, M. (2010). *The rise of the network society*. Oxford, UK: John Wiley & Sons. <https://doi.org/10.1002/9781444319514>
- El-Houssami, N., & Rizk, N. (2020). Innovation practices at makerspaces in Egypt, Tunisia and Morocco. *The African Journal of Information and Communication*, (26), 1—25. <https://doi.org/10.23962/10539/30357>
- Faizi, I., & Abubakar, A. (2021). The Internet of everything from Islamic perspective. *International Journal on Perceptive and Cognitive Computing*, 1(7), 66—71.
- Filonik, A. O., & Isaev, V. A. (2020). The Arab world: Merger into nation or increasing disengagement? (A note of theme). *Asia and Africa Today*, (3), 12—19. (In Russian). <https://doi.org/10.31857/S032150750008723-7>
- Kabernik, V. V. (2013). Approaches to cyber weapons classification problem. *MGIMO Review of International Relations*, 2(29), 72—78. (In Russian). <https://doi.org/10.24833/2071-8160-2013-2-29-72-78>
- Kuznetsov, V. A. (2019). From the Ocean to the Gulf: One region's identity in the context of neomodernity. *Moscow University Bulletin of World Politics*, (2), 9—38. (In Russian).
- Kuznetsov, V. A. (2020). Arab societies of neomodernity: Seeking for new unities. *Vostok (Oriens)*, (2), 28—40. (In Russian). <https://doi.org/10.31857/S086919080009104-1>
- Lebedeva, M. M., Kharkevich, M. V., Zinovieva, E. S., & Koposova, E. N. (2016). State archaization: The role of information technologies. *Polis. Political Studies*, (6), 22—36. (In Russian). <https://doi.org/10.17976/jpps/2016.06.03>
- Liu, L. (2021). China's policy and practice regarding the Gulf security. In L. Narbone & A. Divsallar (Eds.), *Stepping away from the abyss: A gradual approach towards a new security system in the Persian Gulf* (pp. 81—94). San Domenico di Fiesole: European University Institute. <https://doi.org/10.2870/39131>
- Melkumyan, E. S. (2020). Role of the Arab League in structuring the Arab regional space. *MGIMO Review of International Relations*, 5(13), 220—235. (In Russian). <https://doi.org/10.24833/2071-8160-2020-5-74-220-235>
- Melyantsev, V. A. (2020). Long-term trends in the socio-economic development of Arab countries. *MGIMO Review of International Relations*, 5(13), 194—219. (In Russian). <https://doi.org/10.24833/2071-8160-2020-5-74-194-219>
- Mogielnicki, R. (2021). Smart context-based investments in the Persian Gulf's economic security. In L. Narbone & A. Divsallar (Eds.), *Stepping away from the abyss: A gradual approach towards a new security system in the Persian Gulf* (pp. 163—174). San Domenico di Fiesole: European University Institute. <https://doi.org/10.2870/39131>
- Naumkin, V. V. (2015). Deeply divided societies in the Middle East: Conflict, violence, and foreign intervention. *Moscow University Bulletin of World Politics*, (1), 66—96. (In Russian).
- Naumkin, V. V. (2019). Right-sizing and right-peopling: The Middle East challenges. *Polis. Political Studies*, (6), 67—80. (In Russian). <https://doi.org/10.17976/jpps/2019.06.06>
- Pöpper, C., Maniatakos, M., & Di Pietro, R. (2021). Cyber security research in the Arab region: A blooming ecosystem with global ambitions. *Communications of the ACM*, 4(64), 96—101. <https://doi.org/10.1145/3447741>
- Pradhan, P. (2018). Qatar crisis and the deepening regional faultlines. *Strategic Analysis*, 4(42), 437—442. <https://doi.org/10.1080/09700161.2018.1482620>



- Saveliev, A. G., & Karasev, P. A. (2018). Prospects for the regulation and reduction of the military cyberthreat. *Moscow University Bulletin of World Politics*, (5), 47—61. (In Russian).
- Shat, F. J. F., Mousavi, A., & Pimenisis, E. (2013). Electronic government enactment in a small developing country — the Palestine authority’s policy and practice. In *E-Democracy, Security, Privacy and Trust in a Digital World. 5th International Conference. Revised Selected Papers, December 5—6, 2013* (pp. 83—92). Athens, Greece: Springer International Publishing. [https://doi.org/10.1007/978-3-319-11710-2\\_8](https://doi.org/10.1007/978-3-319-11710-2_8)
- Shumilin, A. I. (2019). Middle East: Window of opportunities or a trap for the Atlantists? *World Economy and International Relations*, 7(63), 111—120. (In Russian). <https://doi.org/10.20542/0131-2227-2019-63-7-111-120>
- Syukiyainen, L. R. (2016). Constitutional status of Sharia as main source of legislation in Arab countries. *Pravo. Zhurnal Vysshey Shkoly Ekonomiki*, (3), 183—205. (In Russian). <https://doi.org/10.17323/2072-8166.2016.4.205.222>
- Syukiyainen, L. R. (2019). Fikh as source of contemporary law in Arab countries. *Pravo. Zhurnal Vysshey Shkoly Ekonomiki*, (4), 222—245. (In Russian). <https://doi.org/10.17323/2072-8166.2019.4.222.245>
- Zinovieva, E. S. (2018). Conceptualization of the international cooperation in the field of science and technology. *MGIMO Review of International Relations*, 6(63), 242—254. (In Russian). <https://doi.org/10.24833/2071-8160-2018-6-63-242-254>
- Zvyagelskaya, I. D., & Kuznetsov, V. A. (2017). Statehood in the Middle East: The future which started yesterday. *International Trends*, 4(15), 6—19. (In Russian). <https://doi.org/10.17994/IT.2017.15.4.51.1>
- Zvyagelskaya, I. D., Bogacheva, A. S., Davydov, A. A., Ibragimov, I. E., Samarskaya, L. M., Svistunova, I. A., & Surkov, N. Y. (2020a). Political identity and its impact on the foreign policy of the states of the Middle East. *Vostok (Oriens)*, 2(64), 55—73. (In Russian). <https://doi.org/10.31857/S086919080009039-9>
- Zvyagelskaya, I. D., Svistunova, I. A., & Surkov, N. Y. (2020b). The Middle East at a time of “negative certainty”. *World Economy and International Relations*, 6(64), 94—103. (In Russian). <https://doi.org/10.20542/0131-2227-2020-64-6-94-103>

**About the authors:** Valiakhmetova Gulnara Nilovna — PhD, Dr. of Sc. (History), Associate Professor, Head of the Department of Oriental Studies, Faculty of International Relations, Ural Federal University named after the first President of Russia B.N. Eltsin; ORCID: 0000-0001-7199-7723; e-mail: [vgulnara@mail.ru](mailto:vgulnara@mail.ru)  
Tsukanov Leonid Vyacheslavovich — PhD Student, Department of Oriental Studies, Faculty of International Relations, Ural Federal University named after the first President of Russia B.N. Eltsin; ORCID: 0000-0001-6882-9841; e-mail: [leon.tsukanov@mail.ru](mailto:leon.tsukanov@mail.ru)