УДК 32 **DOI: 10.34670/AR.2021.52.23.003**

Сотрудничество Израиля и Катара в сфере кибербезопасности

Цуканов Леонид Вячеславович

Аспирант,
Уральский гуманитарный институт,
Уральский федеральный университет им. первого Президента России Б.Н. Ельцина,
620002, Российская Федерация, Екатеринбург, ул. Мира, 19;
e-mail: leon.tsukanov@mail.ru

Аннотация

В статье рассматривается сотрудничество Государства Израиль и Катара по вопросам обеспечения национальной и международной кибербезопасности. Автор раскрывает специфику взаимодействия двух государств в условиях отсутствия дипломатических связей, выявляет основные формы и направления их сотрудничества. Анализируя влияние «Соглашений Авраама» (2020 г.) на развитие диалога Катара и Израиля в сфере кибербезопасности, автор указывает на формирующийся дуализм катарской политики – с одной стороны, предпочтение по-прежнему отдается «буферному» сотрудничеству (где главным посредником в диалоге выступают ОАЭ), а, с другой стороны, намечается тенденция к развитию прямых контактов. Также автор акцентирует внимание на ряде региональных факторов, влияющих на характер и динамику взаимодействия Израиля и Катара – вовлеченность Дохи в качестве посредника в палестино-израильский диалог, ее нейтралитет в асимметричном конфликте с Ираном и т. д. Автор приходит к выводу, что Катар намерен и дальше использовать передовой опыт израильских частных компаний для укрепления национальной системы кибербезопасности, ввиду чего будет постепенно легитимизировать наработанные до 2020 г. контакты. Вместе с тем Доха стремится сохранить региональный статус-кво, а потому не намерена в краткосрочной перспективе форсированно наращивать сотрудничество с Израилем.

Для цитирования в научных исследованиях

Цуканов Л.В. Сотрудничество Израиля и Катара в сфере кибербезопасности // Теории и проблемы политических исследований. 2021. Том 10. № 5А. С. 28-36. DOI: 10.34670/AR.2021.52.23.003

Ключевые слова

Катар, Израиль, кибербезопасность, международное сотрудничество, государственно-частное партнерство, стратегии цифрового развития.

Введение

Фактор кибербезопасности в последние годы играет все более ощутимую роль в глобальных и региональных политических процессах. Не стал исключением и Ближний Восток, где уровень цифровой защищенности оказывает прямое влияние на геополитический вес ведущих региональных держав. На фоне начавшегося в последние годы процесса нормализации отношений между отдельными государствами Персидского залива и Израилем наметился тренд на более глубокую вовлеченность последнего в обеспечение национальной и коллективной цифровой безопасности аравийских монархий [Rahman, 2021, www].

В этой связи особый научный и практический интерес представляет опыт Государства Катар. Несмотря на то, что Доха в последние годы существенно ослабила позиции в Глобальном рейтинге кибербезопасности, опустившись с 5 места (2014 г.) [Global Cybersecurity Index, 2014, www] на 27 место (2020 г.) [Global Cybersecurity Index, 2020, www], эксперты обращают внимание на качественные изменения катарской цифровой сферы, прежде всего, на разработку и утверждение стратегии кибербезопасности (2014 г.) [Qatar National Cyber Security Strategy, 2014, www], ускоренное развитие национальных институтов, связанных с обеспечением цифровой безопасности [Abu-Taieh, 2018, 52-53], а также на появление в стране большого количества частных фирм с международным участием [Milton-Edwards, 2020, 52]. Израиль сыграл на этом этапе важную роль [Abu-Taieh, 2018, 55]. Подобный расклад, в свою очередь, актуализирует ряд вопросов. Каким образом строилось сотрудничество Израиля и Катара по вопросам кибербезопасности в условиях взаимного непризнания? Изменился ли вектор этих отношений после нормализации рядом стран Персидского залива отношений с Израилем в 2020 г.? Почему Доха не идет на активное сближение с Израилем?

Проблематика взаимодействия Израиля и аравийских монархий представлена в современном научном поле значительным количеством исследований. Как правило, ведущие эксперты (как отечественные, так и зарубежные) рассматривают влияние израильского фактора на региональную политику различных государств Персидского залива [Косач, Мелкумян, 2012, 53-54, 63-65], в том числе Катара [Егоров, 2020, 367; Касаев, 2013, 91; Сарсембаев, 2020, 3624]. Довольно много работ посвящено проблемам, связанным с меняющейся ролью Дохи в палестино-израильском противостоянии, в том числе в контексте ее отношений с ХАМАС [Керимов, Рабайа, 2021, 97-99]. Вместе с тем следует признать, что израильско-катарское взаимодействие в сфере цифровой безопасности пока не стало предметом отдельного исследования, хотя определенные наработки имеются в трудах израильских экспертов [Michael, Guzansky, 2020, www]. Данная статья позволяет в определенной степени восполнить указанный пробел.

Источниковой основой исследования стали документы профильных министерств и ведомств Катара, отчеты ведущих экспертных центров и IT-компаний, специализирующихся на вопросах цифровой безопасности, материалы информационно-новостных ресурсов, базы данных контрагентов.

Специфика становления и развития связей Катара и Израиля в цифровой сфере

Первые контакты между Катаром и Израилем по вопросам кибербезопасности относятся к 2012 г., когда под влиянием событий «арабской весны» катарские власти объявили тендер на

разработку продуктов для укрепления цифровой защиты объектов критической инфраструктуры страны, а также на модернизацию систем видеонаблюдения [Qatar 2012. Promoting Online Safety and Cyber Ethics in the Middle East, 2012, www]. Несмотря на то, что официально исполнителями этого тендера в документах значатся германские, американские и швейцарские компании, среди субподрядчиков и консультантов проектов можно встретить немало израильских фирм (ClearSky Cyber Security, IntuView и др.), большинство из которых – с государственным участием.

Кроме того, израильские «белые хакеры» несколько раз участвовали в отражении массированных кибератак на инфраструктуру Катара: в 2012 г. (атака на объекты катарского нефтегазового конгломерата RasGas с использованием вируса Shamoon [Qatari Gas Company Hit With Virus in Wave of Attacks on Energy Companies, 2012, www]), в 2016 г. (массированный удар по банковскому сектору страны [Qatar National Bank allegedly hacked, data of 1,200 entities leaked, 2016, www]), 2017 г. (атака вируса WannaCry [WannaCry: A historic cyberattack, 2017, www]) и в 2019 г. (серия DDoS-атак на правительственные сайты и официальные страницы катарских компаний [DDoS Attacks that Hit the Headlines in 2019, 2020, www]). Эксперты подчеркивают, что именно поддержка со стороны израильских компьютерных экспертов позволила Катару существенно снизить ущерб от атак [Zilber, 2019, www]. Также аналитики полагают, что израильские частные IT-компании внесли серьезный вклад в подготовку реформ экономической модернизации Катара «Видение 2030» (Qatar National Vision 2030), в частности, выступили консультантами при разработке проекта умного города TASMU [Rahman, 2021, www].

Вместе с тем, несмотря на наличие значительного количества эпизодов взаимодействия, сотрудничество между Израилем и Катаром (как в контексте кибербезопасности, так и в целом) не вышло на официальный уровень ввиду нежелания Дохи отходить от своего открыто пропалестинского курса во внешней политике. Тем не менее два государства нашли способ коммуницировать без риска для собственного политического имиджа. Так, соглашения по развитию проектов в области кибербезопасности (включая их экспертное сопровождение) заключались с европейскими и американскими фирмами (реже – с арабскими фирмами-однодневками), которые позже привлекали израильские компании в качестве соисполнителя для проведения соответствующих работ (это, в свою очередь, объясняет обилие израильских фирм со статусом «субподрядчик» или «консультант» в отчетных документах европейских фирм, с которыми сотрудничал Катар [Koka, 2021, www]). Подобный способ взаимодействия (в Израиле получивший название «дискретный» [Koka, 2021, www]) решал сразу несколько задач: в первую очередь, позволял Дохе получать цифровые продукты высокого качества с минимальной наценкой и при этом не противоречить собственной внешнеполитической риторике. С другой стороны, такая модель сотрудничества зачастую не позволяла израильским специалистам оперативно вмешиваться в процесс модернизации систем цифровой безопасности (поскольку каждый эпизод масштабного обновления программного обеспечения требовал заключения нового «дискретного» контракта), а также обеспечивать постоянный мониторинг уязвимостей, ввиду чего атаки предположительно иранских и ливанских хакеров на катарские цифровые системы нередко заканчивались успехом [The New Battlefront: Cyber Security Across the GCC, 2018, www].

«Соглашения Авраама» и их роль в развитии двустороннего сотрудничества

После подписания в сентябре 2020 г. трехстороннего (ОАЭ, Израиль, Бахрейн) договора о нормализации отношений («Соглашения Авраама») начался новый этап в сотрудничестве государств – членов Совета сотрудничества арабских стран Персидского Залива (ССАГПЗ) и Израиля. Бахрейн и ОАЭ, стремясь легитимизировать свои контакты с израильскими IT-компаниями, официально заявили о готовности привлекать специалистов из этой страны для разработки и реализации проектов в области национальной и коллективной цифровой безопасности (в том числе в рамках развития цифровой составляющей объединенных сил быстрого реагирования «Щит полуострова») [Sakka, Akyar, 2021, 55-57].

Кроме того, изменился и подход к развитию сотрудничества. Так, в феврале 2021 г. стало известно, что израильская фирма с государственным участием Quali, ранее специализировавшаяся на создании систем тестирования в рамках оборонных проектов, в партнерстве с BEACON RED (ОАЭ) будет заниматься разработкой аналогичных продуктов в интересах стран ССАГПЗ (позже эту информацию официально подтвердили представители эмиратских деловых кругов) [CEO: UAE's Beacon Red Boosts Cyber Resilience in Mideast, 2021, www]. Учитывая, что это уже не первый случай коллаборации израильских и эмиратских компаний после подписания «Соглашений», можно предположить, что именно ОАЭ в дальнейшем станет ключевым посредником в израильско-катарском диалоге по вопросам цифровой безопасности и обеспечит более тесное взаимодействие специалистов двух стран.

На фоне «оттепели» в арабском мире Доха также предпринимает самостоятельные шаги по активизации прямых контактов с Израилем в области кибербезопасности. Так, за прошедший год доля катарских частных фирм, специализирующихся на цифровых проектах, выросла более чем на 35% [Companies in Qatar (Cybersecurity solutions), 2021, www]. Примечательно, что значительная доля созданных в этот период фирм либо поддерживает постоянный контакт с представителями израильского экспертного сообщества, либо аффилирована с международными корпорациями, где среди учредителей присутствуют израильские бизнесмены[1]. Кроме того, в ноябре 2020 г. власти Катара подписали крупный контракт с израильской фирмой Sdema Group на обслуживание цифровых систем, а также обеспечение комплексной безопасности киберпространства в ходе Чемпионата мира по футболу 2022 г., который пройдет в Катаре [Doha, like Abu Dhabi, also hooked on Israeli technology, 2021, www]. По сути, это первый опыт коммуникации специалистов двух стран без привлечения «дискретных» контор. Тем не менее эксперты склонны полагать, что это скорее частный случай, обусловленный удачным стечением внешних обстоятельств [Koka, 2021, www].

Препятствия на пути к двустороннему сотрудничеству в киберсфере

Несмотря на то, что в первой половине 2021 г. Катар рассматривался представителями экспертных сообществ мира как один из наиболее вероятных участников нового раунда

[1] Закономерность выведена на основе проверки данных, содержащихся в открытых базах контрагентов Катара и Израиля, а также реестра компаний, зарегистрированных в США. См., напр.: Public Register // Qatar Financial Centre. URL: https://eservices.qfc.qa/qfcpublicregister/publicregister.aspx (accessed: 23.09.2021).

расширения «Соглашений Авраама», власти страны так и не предприняли решительных шагов по нормализации отношений с Израилем. Подобная сдержанность Дохи объясняется в том числе влиянием палестинского фактора: Катар традиционно поддерживает тесные связи с довольно разнородными политическими силами современной Палестины и опасается ухудшения отношений с ними на фоне своего возможного сближения с Израилем. По этой же причине представители властных структур Катара воздерживались от оценочных высказываний по поводу беспорядков в Иерусалиме в мае и августе 2021 г. (в том числе относительно развернутой в соцсетях антиизраильской кампании), а также отказались передавать Израилю данные о палестинских акциях в киберпространстве, зафиксированных во время проведения операции «Страж стен» в мае 2021 г. [Dekel, 2021, www].

Кроме того, Катар понимает, что сближение с Израилем неизбежно вызовет негативную реакцию со стороны Ирана. На данный момент Доха вовлечена в ассиметричный конфликт с Тегераном куда меньше, чем Эр-Рияд и Абу-Даби, и открытая кооперация по вопросам кибербезопасности может положить начало серии масштабных ударов по цифровой инфраструктуре Катара со стороны иранских хакеров, а также иных лояльных Тегерану вне- и антисистемных кибергруппировок Ближнего Востока. Учитывая, что цифровая инфраструктура Катара уже подвергается сверхплановой нагрузке в преддверии Чемпионата мира по футболу 2022 г., высока вероятность, что подобные атаки увенчаются успехом и нанесут стране значительный урон (физический, экономический и имиджевый). По этой причине Катар также не принимает участия в «охоте» за иранскими прокси-группировками, работающими в киберпространстве: в частности, спецслужбы Катара не предоставили Израилю данные о деятельности хакерской группировки «Ливанский кедр» (предположительно связано с ливанским шиитским движением Хезболла), в отличие от своих коллег из Саудовской Аравии и ОАЭ [Israel targeted by Hezbollah hacker group, remained unnoticed for 5 years, 2021, www]. Оценки этого эпизода в экспертном сообществе крайне разнятся: одни исследователи считают, что Доха, на данный момент не обладающая достаточным технико-технологическим обеспечением, не смогла отследить аккаунты руководителей «Ливанского кедра» [Levitt, 2021, www]. Другие же, напротив, подчеркивают, что Катар намеренно не стал предоставлять данные, чтобы сохранить статус нейтрального игрока в ассиметричном конфликте с Ираном [Farmanfarmaian, Mans, 2021, www; Бязров, 2020, 31].

Заключение

В целом, отношения Катара и Израиля в сфере обеспечения цифровой безопасности можно охарактеризовать как стабильные, за время кооперации сторонам удалось выработать гибкий подход, позволяющий решать поставленные задачи без урона для собственной репутации.

«Соглашения Авраама», несмотря на их позитивное влияние на арабо-израильский политический диалог, не привели к существенному пересмотру модели катарско-израильских отношений в сфере кибербезопасности. В отличие от ОАЭ, которые твердо намерены использовать израильский опыт для превращения в цифрового лидера среди стран Персидского залива (а в перспективе – и в одного из лидеров мировых рейтингов кибербезопасности), Катар, вероятнее всего, в обозримом будущем сосредоточится на закреплении имеющихся с Израилем контактов с постепенным переходом от «дискретного» сотрудничества к системе аффилированных фирм.

В краткосрочной перспективе ожидать от Катара серьезных шагов не приходится: власти

страны в целом удовлетворены текущим уровнем взаимодействия с Израилем, поскольку, в отличие от своих соседей – Саудовская Аравии и ОАЭ, – не стремятся к статусу цифровой сверхдержавы и, соответственно, не ставят в приоритет задачу форсированного развития системы национальной кибербезопасности. Кроме того, Доха избегает обострения конфликта с Палестиной или Ираном, в связи с чем предпочитает занять нейтральную позицию в вопросах создания, в том числе при участии Израиля, системы коллективной кибербезопасности в зоне Залива, которые в последние годы все активнее продвигают в региональную повестку Эр-Рияд и Абу-Даби.

Библиография

1. Бязров А.В. Движение «Хезболла» в контексте военно-политических интересов Ирана на Ближнем Востоке // Вестник Северо-Осетинского государственного университета имени К.Л. Хетагурова. 2020. № 3. С. 27-35.
2. Егоров И.С. Катар в Совете сотрудничества арабских государств Персидского залива: развитие дипломатического кризиса // Социально-гуманитарные знания. 2020. № 5 С. 364-370.
3. Касаев Э.О. Перспективные направления экономического развития Катара // Мировая экономика и международные отношения. 2013. № 8. С. 86-94.
4. Керимов А.А., Рабайа Ф. Роль движения ХАМАС в создании Палестинского государства: идеология и практика // Известия Саратовского университета. 2021. № 1. С. 95-101.
5. Косач Г.Г., Мелкумян Е.С. Совет сотрудничества арабских государств залива как региональная военно-политическая организация // Вестник Московского университета. 2012. № 4. С. 39-69.
6. Сарсембаев Н.В. Региональные аспекты сирийского конфликта // Вопросы политологии. 2020. № 12. С. 3619-3627.
7. 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. P. 46-59.
8. CEO: UAE's Beacon Red Boosts Cyber Resilience in Mideast. URL: https://breakingdefense.com/2021/07/ceo-uaes-beacon-red-boosts-cyber-resilience-in-mideast/
9. Companies in Qatar (Cybersecurity solutions). URL: https://www.qataronlinedirectory.com/160295/company-list/companies-qatar/CYBER-SECURITY-SOLUTIONS
10. DDoS Attacks that Hit the Headlines in 2019. URL: https://www.link11.com/en/blog/threat-landscape/ddos-attacks-hit-headlines-2019/
11. Dekel U. Operation Guardian of the Walls: Envisioning the End. URL: https://www.inss.org.il/publication/operation-ending/
12. Doha, like Abu Dhabi, also hooked on Israeli technology. URL: https://www.intelligenceonline.com/government-intelligence/2021/08/26/doha-like-abu-dhabi-also-hooked-on-israeli-technology,109602026-evg
13. Farmanfarmaian R., Mans J. In the Middle East, War Is Going Digital. URL: https://foreignpolicy.com/2021/02/22/in-the-middle-east-war-is-going-digital/
14. Global Cybersecurity Index 2014. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/WP-GCI-101.pdf
15. Global Cybersecurity Index. 2020. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
16. Israel targeted by Hezbollah hacker group, remained unnoticed for 5 years. URL: https://jpost.com/breaking-news/israel-targeted-by-hezbollah-cyber-attack-657064
17. Koka A. The Next Front? Assessing Israel-Gulf Cybersecurity Cooperation. URL: https://www.egic.info/israel-gulf-cyber-cooperation
18. Levitt M. Hezbollah's Regional Activities in Support of Iran's Proxy Networks. URL: https://www.mei.edu/publications/hezbollahs-regional-activities-support-irans-proxy-networks
19. Michael K., Guzansky Y. Might Qatar Join the Abraham Accords? URL: https://www.inss.org.il/publication/the-abraham-accords-and-qatar/
20. Milton-Edwards B. The blockade on Qatar: Conflict management failings // The International Spectator. 2020. № 2. P. 34-48.
21. Public Register. URL: https://eservices.qfc.qa/qfcpublicregister/publicregister.aspx
22. Qatar 2012 – Promoting Online Safety and Cyber Ethics in the Middle East. URL: https://www.fosi.org/events/online-safety-and-cyber-ethics-middle-east
23. Qatar National Bank allegedly hacked, data of 1,200 entities leaked. URL: https://www.middleeasteye.net/fr/news/qatar-national-bank-allegedly-hacked-data-1200-entities-leaked-online-1642830110

24. Qatar National Cyber Security Strategy // Qatar Ministry of transport and communications. URL: https://www.motc.gov.qa/sites/default/files/national_cyber_security_strategy.pdf
25. Rahman O. The emergence of GCC-Israel relations in a changing Middle East. URL: https://www.brookings.edu/research/the-emergence-of-gcc-israel-relations-in-a-changing-middle-east/
26. Qatari Gas Company Hit with Virus in Wave of Attacks on Energy Companies. URL: https://www.wired.com/2012/08/hack-attack-strikes-rasgas/
27. Sakka C., Akyar M. What are the reasons behind the blockade on the State of Qatar by its neighboring Gulf countries and Egypt? And what are the implications of the imposed blockade now and beyond? // Journal of Humanities and Social Science. 2021. № 4. P. 59-67.
28. The New Battlefront: Cyber Security Across the GCC. URL: https://gulfif.org/the-new-battlefront-cyber-security-across-the-gcc/
29. WannaCry: A historic cyberattack. URL: https://www.qdsnet.com/2017/05/wannacry-a-historic-cyberattack/
30. Zilber N. Gulf Cyber Cooperation with Israel: Balancing Threats and Rights. URL: https://www.washingtoninstitute.org/policy-analysis/gulf-cyber-cooperation-israel-balancing-threats-and-rights

Israel-Qatar Cybersecurity Cooperation

Leonid V. Tsukanov

Postgraduate,
Ural Institute of Humanities,
Ural Federal University named after the first President of Russia B.N. Yeltsin,
620002, 19, Mira str., Yekaterinburg, Russian Federation;
e-mail: leon.tsukanov@mail.ru

Abstract

The growing cooperation between Qatar and Israel on cybersecurity issues is an important regional trend that requires detailed study. Analyzing the specifics of the interaction between Doha and Jerusalem, the author notes that in the absence of diplomatic ties between the two states, the main form of cooperation has become the involvement of Israeli private firms specializing in cybersecurity issues as subcontractors for the implementation of projects in Qatar. The author emphasizes that such a strategy, in general, is characteristic of all Arabian monarchies. The author also draws attention to the fact that the normalization of relations with Israel by a number of Arab states in 2020 led to the formation of a dual approach in Qatari foreign policy: on the one hand, Doha still prefers «buffer» cooperation (and the main mediator in the dialogue with Israel is UAE), and, on the other hand, is gradually moving to the development of direct contacts. In addition, the author notes that the pace of development of Qatari-Israeli cooperation on cybersecurity is given serious attention by the Palestinian and Iranian factors. The author concludes that Qatar, like other Arabian monarchies, intends to continue to use the best practices of Israeli private companies to strengthen its own cybersecurity system, which will gradually legitimize the contacts developed by 2020. Nevertheless, the author emphasizes that Doha is currently striving to maintain the regional status quo, and therefore will not forcefully increase cooperation in the short term.

For citation

Tsukanov L.V. (2021) Sotrudnichestvo Izrailya i Katara v sfere kiberbezopasnosti [Israel-Qatar Cybersecurity Cooperation]. *Teorii i problemy politicheskikh issledovanii* [Theories and Problems of Political Studies], 10 (5A), pp. 28-36. DOI: 10.34670/AR.2021.52.23.003

Keywords

Qatar, Israel, cybersecurity, international cooperation, public-private partnerships, digital development strategies.

References

1. Abu-Taieh E. (2018) 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*, 3, pp. 46-59.
2. *CEO: UAE's Beacon Red Boosts Cyber Resilience in Mideast.* Available at: https://breakingdefense.com/2021/07/ceo-uaes-beacon-red-boosts-cyber-resilience-in-mideast/ [Accessed 11/11/2021]
3. Byazrov A.V. (2020) Dvizhenie «Khezbolla» v kontekste voenno-politicheskikh interesov Irana na Blizhnem Vostoke [Hezbollah movement in the context of Iran's military-political interests in the Middle East]. *Vestnik Severo-Osetinskogo gosudarstvennogo universiteta imeni K.L. Khetagurova* [Bulletin of the North Ossetian State University], 3, pp. 27-35.
4. *Companies in Qatar (Cybersecurity solutions).* Available at: https://www.qataronlinedirectory.com/160295/company-list/companies-qatar/CYBER-SECURITY-SOLUTIONS [Accessed 11/11/2021]
5. *DDoS Attacks that Hit the Headlines in 2019.* Available at: https://www.link11.com/en/blog/threat-landscape/ddos-attacks-hit-headlines-2019/ [Accessed 11/11/2021]
6. Dekel U. *Operation Guardian of the Walls: Envisioning the End.* Available at: https://www.inss.org.il/publication/operation-ending/ [Accessed 11/11/2021]
7. *Doha, like Abu Dhabi, also hooked on Israeli technology.* Available at: https://www.intelligenceonline.com/government-intelligence/2021/08/26/doha-like-abu-dhabi-also-hooked-on-israeli-technology,109602026-evg [Accessed 11/11/2021]
8. Egorov I.S. (2020) Katar v Sovete sotrudnichestva arabskikh gosudarstv Persidskogo zaliva: razvitie diplomaticheskogo krizisa [Qatar in the Cooperation Council of the Arab States of the Persian Gulf: Development of the Diplomatic Crisis]. *Sotsial'no-gumanitarnye znaniya* [Social and Humanitarian Knowledge], 5, pp. 364-370.
9. Farmanfarmaian R., Mans J. *In the Middle East, War Is Going Digital.* Available at: https://foreignpolicy.com/2021/02/22/in-the-middle-east-war-is-going-digital/ [Accessed 11/11/2021]
10. *Global Cybersecurity Index 2014.* Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/WP-GCI-101.pdf [Accessed 11/11/2021]
11. *Global Cybersecurity Index. 2020.* Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx [Accessed 11/11/2021]
12. *Israel targeted by Hezbollah hacker group, remained unnoticed for 5 years.* Available at: https://jpost.com/breaking-news/israel-targeted-by-hezbollah-cyber-attack-657064 [Accessed 11/11/2021]
13. Kasaev E.O. (2013) Perspektivnye napravleniya ekonomicheskogo razvitiya Katara [Perspective directions of economic development of Qatar]. *Mirovaya ekonomika i mezhdunarodnye otnosheniya* [World Economy and International Relations], 8, pp. 86-94.
14. Kerimov A.A., Rabaia F. (2021) Rol' dvizheniya KhAMAS v sozdanii Palestinskogo gosudarstva: ideologiya i praktika [The role of the Hamas movement in the creation of a Palestinian state: ideology and practice]. *Izvestiya Saratovskogo universiteta* [News of the Saratov University.], 1, pp. 95-101.
15. Koka A. *The Next Front? Assessing Israel-Gulf Cybersecurity Cooperation.* Available at: https://www.egic.info/israel-gulf-cyber-cooperation [Accessed 11/11/2021]
16. Kosach G.G., Melkumyan E.S. (2012) Sovet sotrudnichestva arabskikh gosudarstv zaliva kak regional'naya voenno-politicheskaya organizatsiya [Cooperation Council for the Arab States of the Gulf as a Regional Military-Political Organization]. *Vestnik Moskovskogo universiteta* [Moscow University Bulletin], 4, pp. 39-69.
17. Levitt M. *Hezbollah's Regional Activities in Support of Iran's Proxy Networks.* Available at: https://www.mei.edu/publications/hezbollahs-regional-activities-support-irans-proxy-networks [Accessed 11/11/2021]
18. Michael K., Guzansky Y. *Might Qatar Join the Abraham Accords?* Available at: https://www.inss.org.il/publication/the-abraham-accords-and-qatar/ [Accessed 11/11/2021]
19. Milton-Edwards B. (2020) The blockade on Qatar: Conflict management failings. *The International Spectator*, 2, pp. 34-48.
20. *Public Register*. Available at: https://eservices.qfc.qa/qfcpublicregister/publicregister.aspx [Accessed 11/11/2021]
21. *Qatari Gas Company Hit with Virus in Wave of Attacks on Energy Companies.* Available at: https://www.wired.com/2012/08/hack-attack-strikes-rasgas/ [Accessed 11/11/2021]
22. *Qatar 2012 – Promoting Online Safety and Cyber Ethics in the Middle East.* Available at: https://www.fosi.org/events/online-safety-and-cyber-ethics-middle-east [Accessed 11/11/2021]
23. *Qatar National Bank allegedly hacked, data of 1,200 entities leaked.* Available at: https://www.middleeasteye.net/fr/news/qatar-national-bank-allegedly-hacked-data-1200-entities-leaked-online-1642830110

24. *Qatar National Cyber Security Strategy // Qatar Ministry of transport and communications.* Available at: https://www.motc.gov.qa/sites/default/files/national_cyber_security_strategy.pdf [Accessed 11/11/2021]
25. Rahman O. *The emergence of GCC-Israel relations in a changing Middle East.* Available at: https://www.brookings.edu/research/the-emergence-of-gcc-israel-relations-in-a-changing-middle-east/ [Accessed 11/11/2021]
26. Sakka C., Akyar M. (2021) What are the reasons behind the blockade on the State of Qatar by its neighboring Gulf countries and Egypt? And what are the implications of the imposed blockade now and beyond? *Journal of Humanities and Social Science*, 4, pp. 59-67.
27. Sarsembaev N.V. (2020) Regional'nye aspekty siriiskogo konflikta [Regional aspects of the Syrian conflict]. *Voprosy politologii* [Questions of political science], 12, pp. 3619-3627.
28. *The New Battlefront: Cyber Security Across the GCC*. Available at: https://gulfif.org/the-new-battlefront-cyber-security-across-the-gcc/ [Accessed 11/11/2021]
29. *WannaCry: A historic cyberattack*. Available at: https://www.qdsnet.com/2017/05/wannacry-a-historic-cyberattack/ [Accessed 11/11/2021]
30. Zilber N. *Gulf Cyber Cooperation with Israel: Balancing Threats and Rights*. Available at: https://www.washingtoninstitute.org/policy-analysis/gulf-cyber-cooperation-israel-balancing-threats-and-rights [Accessed 11/11/2021]