Федеральное государственное автономное образовательное учреждение высшего образования «Уральский федеральный университет имени первого Президента России Б. Н. Ельцина»

На правах рукописи

Цуканов Леонид Вячеславович

Сотрудничество монархий Персидского залива в области кибербезопасности: особенности, проблемы, тенденции

Специальность 5.5.4 – Международные отношения, глобальные и региональные исследования

Автореферат
диссертации на соискание ученой степени
кандидата политических наук

Екатеринбург – 2024

Работа выполнена на кафедре востоковедения ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б. Н. Ельцина»

Научный руководитель: доктор исторических наук, доцент **Валиахметова Гульнара Ниловна**

Официальные оппоненты: **Зиновьева Елена Сергеевна**, доктор политических наук, профессор, ФГАОУ ВО «Московский государственный институт международных отношений (Университет) Министерства иностранных дел Российской Федерации», профессор кафедры мировых политических процессов

Кузнецов Василий Александрович, доктор политических наук, ФГБУН Институт востоковедения Российской Академии Наук (г. Москва), заведующий Центром арабских и исламских исследований

Козюлин Вадим Борисович, кандидат политических наук, ФГБОУ ВО «Дипломатическая академия Министерства иностранных дел Российской Федерации» (г. Москва), главный научный сотрудник Центра глобальных исследований и международных отношений

Защита состоится «24» июня 2024 г., в 13:00 на заседании диссертационного совета УрФУ 5.5.15.02 по адресу: 620000, г. Екатеринбург, пр. Ленина, 51, зал диссертационных советов, комн. 248.

С диссертацией можно ознакомиться в библиотеке и на сайте ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»: https://dissovet2.urfu.ru/mod/data/view.php?d=12&rid=5984

Автореферат разослан «___» мая 2024 г.

Ученый секретарь
диссертационного совета
кандидат политических наук, доцент  Наронская Анна Гегамовна

I. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Стремительное развитие информационно-коммуникационных технологий (ИКТ), как глобальный мегатренд, оказывает весьма противоречивое влияние на современное общество, усиливая взаимозависимость и уязвимость государств, трансформируя национальный суверенитет, расширяя субъектное поле мировой политики и экономики, меняя векторы их развития. Наряду с очевидным улучшением качества жизни человечества, информационная революция породила целый ряд новых вызовов и угроз безопасности (международной, национальной, индивидуальной), поставив в мировую повестку вопрос о создании комплексной системы защиты государств, народов и каждого индивида от деструктивного воздействия извне с использованием ИКТ. Поскольку ни одна страна мира не может в одиночку обеспечить надежную защиту своего информационного пространства, именно в рамках международного сотрудничества и объединения усилий всех участников мирового сообщества возможно формирование безопасной цифровой среды. Однако этот процесс осложняется множеством факторов, в первую очередь концептуальными разногласиями между государствами по широкому спектру проблем, подлежащих урегулированию на международном уровне.

Реалии информационной эпохи усилили социально-политическую и экономическую нестабильность Ближнего Востока, его и без того высокий конфликтный потенциал, втянув регион в разрушительные кибервойны и гонку кибервооружений. Каждый новый всплеск турбулентности на Ближнем Востоке крайне негативно отражается на его информационном пространстве, а носителями цифровых угроз все чаще выступают антисистемные акторы в лице радикально-экстремистских группировок. Ослабление базовых принципов Вестфальской системы и отсутствие международных механизмов противодействия угрозам, порождаемым ИКТ, способствуют неизбежной обратной трансляции деструктивных трендов развития Ближнего Востока с регионального на глобальный уровень.

Сегодня ближневосточные государства нарабатывают собственные практики и методы цифровой защиты, активно включаясь в формирование системы международной информационной безопасности. В авангарде этого процесса находятся арабские монархии Персидского залива. Необходимость адаптироваться к цифровым реалиям стала одной и главных причин запуска стратегических программ экономической диверсификации «Видение» и, как следствие, форсированного строительства национальных систем киберзащиты. Эта задача была решена в рекордно короткие исторические сроки, и сегодня сектор кибербезопасности обеспечивает аравийские монархии не только надежной цифровой защитой, но и эффективными инструментами продвижения к технологическому суверенитету, внешнеполитического влияния и выстраивания новой архитектуры региональной безопасности на Ближнем Востоке и в зоне Персидского залива.

Значительная роль в этих процессах отводится международному сотрудничеству. Сегодня среди партнеров аравийских монархий представлены самые разные акторы – от лидеров мировой технологической гонки в лице США, Китая, Индии, Японии, Республики Корея до наименее развитых стран арабского мира в лице Сомали и Джибути. Сотрудничество с Израилем в области кибербезопасности стало одной и главных причин отказа большинства монархий Залива от конфронтации с ним, вплоть до нормализации отношений в рамках «Соглашений Авраама» 2020 г. (ОАЭ, Бахрейн). Диверсификация внешних связей в секторе киберзащиты является залогом дальнейшей успешной реализации стратегических программ «Видения» и интеграции аравийских монархий в мировые экономические и политические процессы в качестве равноправных акторов. Вместе с тем наращивание киберпотенциала государствами Ближнего Востока сопровождается высоким уровнем соперничества и трансформирует геополитическое пространство региона, ведет к обострению ранних конфликтов и формированию новых узлов напряженности в зонах столкновения интересов.

Практики и опыт международного сотрудничества монархий Залива в области кибербезопасности требуют научного осмысления, которое позволит выявить алгоритмы и механизмы кооперации разнотипных акторов мировой политики, определить пути преодоления асимметрии цифрового развития современных государств и снижения конфликтного потенциала цифрового фактора на Ближнем Востоке, который сегодня в значительной степени формирует глобальную повестку.

Степень научной разработанности. Международное сотрудничество по обеспечению информационной безопасности уже более двух десятилетий остается предметом довольно острых академических и политических дискуссий, в связи с чем научная литература по данной проблематике весьма обширна и разнообразна.

Противоречивое влияние технологий, в том числе цифровых, на международные отношения и мировую политику стало предметом теоретического осмысления в фундаментальных трудах З. Бжезинского, А. Тоффлера, М. Кастельса, К. Шваба, Д. Херреры, Е.Б. Скольникова, П. Хааса, Д.Г. Балуева, М.М. Лебедевой, Е.С. Зиновьевой, М.В.Харкевич, Е.Н. Копосовой[1].

Одной из ключевых проблем, осложняющих объективный научный поиск, является чрезмерная политизация проблемы в связи с доктринальными разногласиями между ведущими акторами мировой политики, прежде всего в

[1] Brzezinski Z. Between two ages. America's role in the technetronic era. N.Y., 1970. 352 p.; Toffler A. Powershift: knowledge, wealth, and violence in the 21st century. N.Y., 1990. 640 p.; Castells M. The Internet galaxy: reflections on the Internet, business, and society. Oxford, 2002. 340 p.; Castells M. The rise of the network society. Oxford, 2011. 609 p.; Шваб К. Четвертая промышленная революция. М., 2017. 280 с.; Herrera G.L. Technology and international transformation. N.Y., 2007. 278 p.; Skolnikoff E.B. The elusive transformation: science, technology, and the evolution of international politics. Princeton, 1994. 336 p.; Haas P. Epistemic communities and international policy coordination // International Organization. 1992. № 1. P. 1–35; Балуев Д.Г. Информационная революция и современные международные отношения. Н. Новгород, 2001. 208 с.; Лебедева М.М., Харкевич М.В., Зиновьева Е.С., Копосова Е.Н. Архаизация государства: роль современных информационных технологий // Полис. Политические исследования. 2016. № 6. С. 22–36; Зиновьева Е.С. Мирополитическая концептуализация международного научно-технического сотрудничества // Вестник МГИМО-Университета. 2016. № 6. С. 242–254.

лице США и России, по вопросу о путях создания безопасной информационной среды на глобальном уровне. Политика России в области международной информационной безопасности в различных ее аспектах является магистральной темой исследований в российских экспертных сообществах и остается предметом острых дискуссий с представителями западных научных школ. Главными дискуссионными площадками России являются Национальная Ассоциация международной информационной безопасности (НАМИБ), РСМД, международный клуб «Валдай». Исследования по данному направлению ведутся в ИМЭМО РАН, РИСИ, МГИМО, МГУ, ПИР-Центре, Дипломатической академии МИД РФ и многих других научных и научно-образовательных учреждениях страны. Научное обоснование позиции, которую Россия при поддержке Китая и ряда стран Азии отстаивает в ООН и на других глобальных и региональных площадках международного взаимодействия, представлена в исследованиях ведущих российских экспертов-международников: А.В. Крутских, В.И. Булвы, М.Б. Алборовой, Н.П. Ромашкиной, О.А. Хлопова, Ю.А. Юдиной и др.[2]. Российские политологи и правоведы убедительно опровергают мнение западных коллег о том, что инициативы России, выдвинутые на глобальном, региональном и межрегиональном уровнях (ГА ООН, ОБСЕ, ШОС, ОДКБ, ЕАЭС, БРИКС, АСЕАН, «Группа 20» и т.д.) якобы имеют рамочный характер и не формируют комплексной системы международной информационной безопасности.

Другой не менее значимой исследовательской проблемой является отсутствие единого общепризнанного понятийного аппарата, в первую очередь речь идет о содержании и соотнесении базовых терминов «информационная безопасность» и «кибербезопасность» и смежных с ними категорий. Данный вопрос стал предметом анализа в трудах правоведов (А.Ю. Баландин, Л.М. Старкова), экономистов (А.В. Яковлева) и представителей технических специальностей (А.С. Алпеев)[3]. Исследователи сходятся во мнении о том, что кибербезопасность является интегральной частью информационной безопасности и имеет многоаспектный характер.

Использование ИКТ, в том числе технологий искусственного интеллекта, в военных целях – еще один восходящий тренд, который нашел отражение в работах О.В. Демидова, В. Каберника, П.А. Карасева, В.Б. Козюлина,

[2] Крутских А.В. Международная информационная безопасность: в поисках консолидированных подходов // Вестник РУДН: Международные отношения. 2022. № 2. С. 342–351; Международная информационная безопасность: подходы России / А.В. Крутских, Е.С. Зиновьева, В.И. Булва, М.Б. Алборова, Ю.А. Юдина. М., 2021. 32 с.; Ромашкина Н.П. Проблема международной информационной безопасности в ООН // Мировая экономика и международные отношения. 2020. № 12. С. 24–30; Хлопов О.А. Проблемы кибербезопасности в деятельности ООН // Системный анализ и синтез моделей научного развития общества. 2021. № 3. С. 65–73.

[3] Баландин А.Ю. Кибербезопасность и информационная безопасность. Демаркация правовых категорий // Правовая политика и правовая жизнь. 2023. № 3. С. 260–270; Старкова Л.М. Подходы к пониманию и нормативному определению категории «киберпреступность» и смежных понятий в практике региональных международных организаций // Московский журнал международного права. 2021. № 4. С. 123–135; Яковлева А.В. Кибербезопасность и ее правовое регулирование (зарубежный и российский опыт) // Социально-политические науки. 2021. № 4. С. 70–81; Алпеев А.С. Терминология безопасности: кибербезопасность, информационная безопасность // Вопросы кибербезопасности. 2014. № 5. С. 39–42.

Е.С. Черненко, А.А. Чирко, В.В. Ященкова[4]. Из зарубежных специалистов следует упомянуть таких авторов, как А. Арслан, Д. Деннинг, С. Икбал, Р. Кларк, М. Либицки, М. Малик, М. Михалка, Р. Нэйк, С. Раза, С. Ризви, О. Хайзлер, Дж. Шелдон[5]. Исследователи сходятся во мнении о том, что применение ИКТ-средств в межгосударственном противостоянии усиливает асимметричность современных международных конфликтов.

Исследованию кибервойн на Ближнем Востоке посвящены работы Г.Н. Валиахметовой, Р. Мугга, С. Чжиуа и др.[6]. Учитывая, что в качестве основного стратегического противника аравийских монархий в региональном киберпространстве зачастую позиционируется Иран, уместно также обратить внимание на публикации Г. Сибони, С. Кроненфельда и М. Базнера[7], где анализируется оборонительный и наступательный киберпотенциал Тегерана. Авторы подчеркивают, что использование ближневосточными государствами и их прокси-силами ИКТ в военно-политическом противостоянии усиливает и без того высокий конфликтный потенциал региона.

Анализ деятельности радикально-экстремистских и террористических группировок в информационной среде имеет особую важность при изучении ландшафта киберугроз на Ближнем Востоке. Радикалы довольно быстро наращивают свой деструктивный киберпотенциал, оказывая значительное влияние на формирование национальных подходов к обеспечению цифровой защиты. Результаты исследований различных проявлений кибертерроризма представлены в работах Л. Веста, Д. Коэна, М. Нэнс, А. Онирети, А. Ротбарта, Ч. Сампсона, Л. Тисуро[8], а также в публикациях российских экспертов

[4] Демидов О.В., Черненко Е.В. Грозный ум на страже кибербезопасности // Индекс безопасности. 2014. № 3. С. 150–161; Каберник В. Проблемы классификации кибероружия // Вестник МГИМО-Университета. 2013. № 2. С. 72–78; Карасев П.А. Эволюция национальных подходов к ведению кибервойны // Международная аналитика. 2022. № 2. С. 79–94; Карасев П.А., Ященков В.В. Многофакторный анализ стратегической стабильности в контексте угроз международной информационной безопасности // Вестник РГГУ: Информатика, информационная безопасность. 2019. № 3. С. 19–35; Козюлин В.Б. Многостороннее сотрудничество в области регулирования использования технологий искусственного интеллекта. М., 2021. 30 с.; Чирко А.А. Бот-генерал: чем грозит боевое применение нейросетей // Россия в глобальной политике. 26.07.2023. URL: https://globalaffairs.ru/articles/bot-general/ (дата обращения: 30.01.2024).

[5] Arslan A. Neorealist analysis of security dilemma in cyberspace: a quantitative study. Washington DC., 2023. 17 p.; Denning D. Information warfare and security. Washington DC., 1999. 544 p.; Iqbal S., Rizvi S., Malik M., Raza S. Artificial Intelligence in security and defense: explore the integration of AI in military strategies, security policies, and its implications for global power dynamics // International Journal of Human and Society. 2023. № 4. P. 341–353; Clarke R. A., Knake R. Cyber war. The next threat to national security and what to do about it. N.Y., 2010; Libicki M. Cyberdeterrence and cyberwar. Santa Monica, 2009; Mihalka M. Cooperative security in the 21st century // Connections: The Quarterly Journal. 2005. № 4. P. 113–122; Haizler O. The United States' cyber warfare history: implications on modern cyber operational structures and policymaking // Cyber, Intelligence, and Security. 2017. № 1. P. 31–45; Sheldon J. Deciphering cyberpower: strategic purpose in peace and war // Strategic Studies Quarterly. 2011. № 2. P. 95–112.

[6] Валиахметова Г.Н. Ближний Восток в цифровую эпоху: глобализация угроз региональной безопасности // Восток: Афро-азиатские общества. 2017. № 3. С. 6–15; Muggah R. Yemen's parallel war in cyberspace // Foreign Policy. 06.01.2022. URL: https://foreignpolicy.com/2022/01/06/yemen-war-internet-media-houthis-iran-saudi-arabia/ (accessed: 07.10.2023); Zhioua S. The Middle East under malware attack dissecting cyber weapons. Philadelphia, 2013.

[7] Siboni G., Kronenfeld S. Developments in Iranian cyber warfare 2013–2014 // Military and Strategic Affairs. 2014. № 2. P. 83–104; Baezner M. Iranian cyber-activities in the context of regional rivalries and international tensions. Zurich. 2019. 37 p.

[8] West L. #jihad: Understanding social media as a weapon // Security Challenges. 2016. № 2. P. 9–26; Siboni G., Cohen D., Rotbart A. The threat of terrorist organizations in cyberspace // Military and Strategic Affairs. 2013. № 3. P. 20–29; Nance M., Sampson Ch. Hacking ISIS: how to destroy the cyber jihad. N.Y., 2017. 320 p.; Onireti A. Cyber-terrorism: an appraisal of the dimensions of the new face of terrorism in a post-9/11 period. L., 2024. 196 p.; Teasuro L. The role

А.В. Манойло, Н.Х. Гафиатулиной, Д.М. Брусенцевой, А.В. Федорова[9]. Комплексные исследования ИКТ-угроз со стороны радикально-экстремистких группировок ведутся также в Центре оценки рисков Кембриджского университета, Европоле, Лаборатории Касперского и т.д.[10].

Большой пласт исследований посвящен взаимовлиянию цифровизации и мировых религий, в первую очередь, ислама. Актуальность обращения к данной проблематике обусловлена тем, что в монархиях Залива проблема адаптации традиционных религиозных установок к реалиям цифровой эпохи стоит особенно остро: здесь ислам не просто государственная религия, а основной закон, определяющий все сферы жизни государства и общества и оказывающий значительное влияние на принятие стратегически значимых для развития стран решений. В силу многоаспектного характера обозначенной проблемы исследования на данном направлении отличаются многообразием оценок и методологических подходов. В центре внимания исследователей – восприятие мусульманскими правоведами цифровизации и иных технологических нововведений (Л.Р. Сюкияйнен, А. Магайре)[11]; влияние интернета на повседневные религиозные практики мусульман (Б. Лоуренс, Дж. Шанцер, С. Миллер, Е.Н. Чеснова, З. Хабибулина, Э. Муратова, А.П. Забияко)[12], специфика цифровизации бизнес-среды в мусульманских странах (М. Навид, А. Шоаиб)[13].

Особенности Ближнего Востока оказывают существенное влияние на специфику экстраполяции на регион глобального мега-тренда цифровизации. Труды ведущих российских востоковедов (ближневосточников, арабистов, исламоведов), специализирующихся на исследовании регионального геополитического пространства, – академика РАН В.В. Наумкина, В.А. Кузнецова, И.Д. Звягельской, В.Г. Барановского[14] – отличаются

Al Qaeda plays in cyberterrorism // Small Wars Journal, 8.12.2018. URL: https://smallwarsjournal.com/jrnl/art/role-al-qaeda-plays-cyberterrorism (accessed: 30.12.2023).

[9] Манойло А.В. Модели «мягкой силы» сетевых террористических организаций в системе угроз национальной безопасности // Вестник Российской нации. 2016. № 2. С. 180–194; Гафиатулина Н.Х., Брусенцева Д.М. Медийное пространство как источник активности террористической организации // Гуманитарные, социально-экономические и общественные науки. 2017. № 6. С. 37–40; Федоров А.В. Супертерроризм: новый вызов нового века. М., 2022. 198 с.

[10] Cyber Terrorism: assessment of the threat to insurance. Cambridge, 2017. 48 p.; Online jihadist propaganda 2021. Luxembourg, 2022. 50 p.; Kaspersky Security Bulletin 2015. URL: https://securelist.ru/kaspersky-security-bulletin-2015-razvitie-ugroz-v-2015-godu/27466/ (accessed: 15.12.2023) и др.

[11] Сюкияйнен Л.Р. Глобализация и мусульманский мир: оценка современной исламской правовой мысли. М., 2012. 88 с.; Сюкияйнен Л.Р. Исламское право и диалог культур в современном мире. М., 2021. 684 с.; Maghaireh A. Shariah law and cyber-sectarian conflict: How can Islamic criminal law respond to cybercrime? // International Journal of Cyber Criminology. 2009. № 2. P. 337–445.

[12] Lawrence B. Allah on-line: the practice of global Islam in the information Age. N.Y., 2002. P. 237–253; Shanzer J., Miller S. Facebook fatwa: Saudi clerics, Wahhabi Islam, and social media. Washington DC., 2012. 103 p.; Чеснова Е.Н. Цифровизация религии: ислам // Гуманитарные ведомости ТГПУ. 2021. № 4. С. 71–82; Виртуальный ислам на постсоветском пространстве: киберсреда и религиозные авторитеты / под ред. Хабибулиной З., Муратовой Э. Баку, 2023. 259 с.; Забияко А.П. Киберрелигия: наука как фактор религиозных трансформаций. Благовещенск, 2012. 208 с.

[13] Naveed M., Shoaib A. The resilience of shariah-compliant investments: probing the static and dynamic connectedness between gold-backed cryptocurrencies and GCC equity markets // International Review of Financial Analysis. 2024. № 91. P. 113–145.

[14] Барановский В.Г., Наумкин В.В. Ближний Восток в меняющемся глобальном контексте: ключевые тренды столетнего развития // Мировая экономика и международные отношения. 2018. № 3. С. 5–19; Кузнецов В.А., Наумкин В.В. Глобальные и региональные тренды «столетия+» на Ближнем Востоке: новое прочтение // Вестник

многофакторным подходом и применением методов политических и исторических исследований. Особенности исторического и социокультурного развития ближневосточных стран включаются в анализ при разработке прогнозных сценариев развития военно-политической обстановки на Ближнем Востоке в исследованиях А.С. Богачевой, А.А. Давыдова, И.Э. Ибрагимова, Л.М. Самарской, И.А. Свистуновой, Н.Ю. Суркова[15]. Внутренняя и внешняя политика аравийских монархий получила всестороннее освещение в фундаментальных исследованиях ведущих российских специалистов по арабским странам Залива Г.Г. Косача и Е.С. Мелкумян[16]. Проблемы безопасности на Ближнем Востоке также представлены в публикациях таких зарубежных исследователей, как Ф. Гауб, Й. Гузански, С. Кук, К. Михаэль[17].

Изучению политики аравийских монархий в области кибербезопасности посвящены труды таких исследователей, как Д. Бродерс, М.А. Келло, А. Зибак, Н. Зильбер, А. Сукумар, Дж. Хакме, Б. Хассиб, Дж. Ширес[18]. Влияние геополитических факторов на решение технических проблем цифровой защиты в зоне Персидского залива исследовали Ф. Дузе, Л. Петинио, К. Саламатиан, Дж.-Л. Самаан[19]. Сравнительный анализ правовых подходов арабских стран в вопросах противодействия киберпреступности проведен Э. Абу-Тайи[20].

Развитие международного сотрудничества в области кибербезопасности является одним из приоритетов внешней политики монархий Залива, что побуждает представителей академических сообществ обращаться к данной тематике. Различные направления взаимодействия аравийских монархий с

Моск. ун-та: Международные отношения и мировая политика. 2023. № 1. С. 70–92; Наумкин В.В. Новые моменты в ближневосточной политике США // Проблемы национальной стратегии. 2022. № 5. С. 14–25; Наумкин В.В. Исламский радикализм в зеркале новых концепций и подходов. М., 2005; Naumkin V.V., Kuznetsov V.A. Non-State actors in the Middle East: towards a new typology // Russia in Global Affairs. 2020. № 4. P. 192–214; Кузнецов В.А. Арабские общества эпохи неомодерна: поиск новых единств // Восток. 2020. № 2. С. 28–40; Звягельская И.Д., Свистунова И.А., Сурков Н.Ю. Ближний Восток в условиях «негативной определенности» // Мировая экономика и международные отношения. 2020. № 6. С. 94–103.

[15] Звягельская И.Д., Богачева А.С., Давыдов А.А., Ибрагимов И.Э., Самарская Л.М., Свистунова И.А., Сурков Н.Ю. Политическая идентичность и ее влияние на внешнюю политику государств Ближнего Востока // Восток. 2020. № 2. С. 55–68.

[16] Косач Г.Г., Мелкумян Е.С. Совет сотрудничества арабских государств Залива как военно-политическая организация // Вестник Моск. ун-та: Международные отношения и мировая политика. 2012. № 4. С. 39–69; Мелкумян Е.С. Арабские монархии Залива в XXI веке. Региональные и глобальные аспекты внешней политики. М., 2023. 317 с.

[17] Gaub F. Stuck in the barracks: the Joint Arab Force. Brussel, 2015; Guzansky Y., Michael K. Revisiting the possibility of a regional military alliance // INSS Insight. 2022. № 1561. 5 p.; Cook S. Biden's Middle East strategy is ruthless pragmatism // Foreign Policy. 07.01.2022. URL: https://foreignpolicy.com/2022/01/07/biden-middle-east-saudi-arabia-syria-yemen-strategy/ (accessed: 06.10.2023).

[18] Sukumar A., Broeders D., Kello M. The pervasive informality of the international cybersecurity regime: geopolitics, non-state actors and diplomacy // Contemporary Security Policy. 2024. № 1. P. 7–44; Zibak A. Cyber (non)cooperation in the Gulf // CYJAX. 02.07.2020. URL: https://www.cyjax.com/cyber-noncooperation-in-the-gulf/ (accessed: 11.10.2023); Zilber N. Gulf cyber cooperation with Izrael: balancing threats and rights // The Washington Institute of Near East Policy. 17.01.2019. URL: https://www.washingtoninstitute.org/policy-analysis/gulf-cyber-cooperation-israel-balancing-threats-and-rights (accessed: 06.10.2023); Shires J., Hakmeh J. Is the GCC cyber resilient? L., 2020. 20 p.; Hassib B, Shires J. Cybersecurity in the GCC: from economic development to geopolitical controversy // Middle East Policy. 2022. № 29. P. 90–103.

[19] Douzet F., Pétiniaud L., Salamatian K., Samaan J.-L. Digital routes and borders in the Middle East: the geopolitical underpinnings of Internet connectivity // Territory, Politics, Governance. 2023. № 6. P. 1059–1080.

[20] 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.

отдельными внерегиональными и региональными партнерами по вопросам цифровизации и киберзащиты представлены в исследованиях К. Касапоглу, Н. Кожанова, Л. Лю, В.И. Михайленко, Т.А. Успенских, Р. Могильницки, А. Мосли, А. Салаха, а также исследовательского коллектива Института Буссола[21]. Вместе с тем практика заимствования за рубежом готовых технологических решений и профессиональных кадров порождает зависимость арабских стран от своих партнеров (прежде всего США и КНР) и способствует ослаблению их суверенитета, что трактуется рядом исследователей как проявление «цифрового колониализма» (М. Кросстон, М. Квет и др.)[22].

Среди региональных сюжетов в последние годы наибольшей дискуссионностью отличается тема развития кооперации по вопросам кибербезопасности в открытом и «дискретном» формате между монархиями Залива и Израилем. К этой теме, в частности, обращались А. Эл-Масри, Б. Букс, Д. Джиндаль, Н. Хоррами М. Солиман и др.[23]. Исследователи выявляют комплекс факторов, способствовавших сближению бывших стратегических противников, а также акцентируют внимание на возможных сценариях изменения баланса сил на Ближнем Востоке в случае выдвижения Израиля на роль гаранта региональной кибербезопасности.

В целом, можно констатировать, что проблематика международного сотрудничества в области кибербезопасности довольно широко представлена в современном научном поле и отличается разнообразием методологических подходов и направлений исследований. Вместе с тем следует признать, что ни зарубежными, ни российскими научно-экспертными сообществами пока не было предложено комплексной работы, в которой проводился бы анализ политики аравийских монархий в области обеспечения кибербезопасности через призму развития международного сотрудничества. Российские международники пока не занимались предметно вопросами информационной безопасности в зоне Залива, а российские востоковеды относительно недавно стали обращаться к исследованию данной проблематики. Имеющиеся к настоящему времени

[21] Kasapoglu C. Turkey's future cyber defense landscape. Ankara, 2016. 20 p.; Kozhanov N. Russia and the issue of a new security architecture for the Persian Gulf // London School of Economics and Political Science. 04.08.2021. URL: https://blogs.lse.ac.uk/mec/2021/08/04/russia-and-the-issue-of-a-new-security-architecture-for-the-persian-gulf/ (accessed: 06.10.2023); Liu L. China’s policy and practice regarding the Gulf security // Stepping away from the abyss. San Domenico di Fiesole, 2021. P. 81–94; Михайленко В.И., Успенских Т.А. Политика ЕС в отношении Совета сотрудничества арабских государств Персидского залива // Современная Европа. 2019. № 5. С. 35–45; Mogielnicki R. Smart context-based investments in the Persian Gulf’s economic security // Stepping away from the abyss. San Domenico di Fiesole, 2021. P. 163–174; Mosly A. Saudi-Canada relations: restoration of ties // Gulf Research Center. 31.07.2023. URL: https://www.grc.net/single-commentary/103 (accessed: 30.01.2024); Salah A. Realigning priorities: Egypt's strategic shift toward Qatar, Turkey, and Iran // Middle East Institute. 25.07.2023. URL: https://www.mei.edu/publications/realigning-priorities-egypts-strategic-shift-toward-qatar-turkey-and-iran (accessed: 30.01.2024); Euro-Gulf regional cybersecurity collaboration // Bussola. 16.09.2021. URL: https://www.bussolainstitute.org/euro-gulf-regional-cybersecurity-collaboration (accessed: 06.10.2023).

[22] Crosston M. Cyber colonization: the dangerous fusion of Artificial Intelligence and authoritarian regimes // Cyber, Intelligence, and Security. 2020. № 1. P. 149–171; Kwet M. Digital colonialism: US empire and the new imperialism in the Global South // Race & Class. 2019. № 4. P. 13–24.

[23] El-Masry A. The Abraham Accords and their cyber implications // Middle East Institute. 09.06.2021. URL: https://www.mei.edu/publications/abraham-accords-and-their-cyber-implications (accessed: 06.10.2023); Bouks B. Israel’s strategic threats and challenges: security, influence & cyber // Security Science Journal. 2023. № 1. P. 118–133; Jindal D., Soliman M. Understanding the growing Indo-Israeli strategic cyber partnership // Middle East Institute. 06.07.2023. URL: https://www.mei.edu/publications/understanding-growing-indo-israeli-strategic-cyber-partnership (accessed: 06.10.2023); Khorrami N. Israel’s cybersecurity cooperation with the GCC states. Singapore, 2021.

исследовательские наработки российских и зарубежных ученых формируют обстоятельную научную базу для проведения комплексного исследования ключевых трендов и особенностей развития международного сотрудничества монархий Персидского залива в области кибербезопасности.

Цель работы – выявление основных направлений и особенностей международного сотрудничества монархий Залива в сфере кибербезопасности.

Исходя из цели, сформулированы следующие **исследовательские задачи:**

– раскрыть содержание и соотношение понятий «информационная безопасность» и «кибербезопасность», определить подход аравийских монархий к обеспечению национальной и международной информационной безопасности;

– охарактеризовать ландшафт цифровых угроз в монархиях Залива, определить факторы, формирующие запрос на коллективные меры киберзащиты;

– выявить общие тренды и риски развития национальных систем кибербезопасности аравийских монархий, установить степень их готовности к отражению киберугроз;

– раскрыть основные направления профильной кооперации монархий Залива на региональных интеграционных площадках Совета сотрудничества арабских государств Залива (ССАГЗ), Лиги арабских государств (ЛАГ) и Организации исламского сотрудничества (ОИС); определить причины относительно низкой динамики продвижения проектов коллективной киберзащиты;

– выявить роль и место военного сотрудничества в формировании киберпотенциала аравийских монархий; раскрыть влияние цифрового фактора на трансформацию подходов к обеспечению региональной безопасности на Ближнем Востоке;

– провести сравнительный анализ вовлеченности региональных и внерегиональных акторов в формирование безопасной цифровой среды в монархиях Залива, обозначить особенности и диспропорции диверсификации их внешних связей по линии кибербезопасности;

– обозначить факторы, способствующие и препятствующие развитию совместных инициатив аравийских монархий в вопросах выработки коллективного ответа на цифровой вызов.

Объектом диссертационного исследования выступает политика монархий Персидского залива в сфере кибербезопасности.

Предметом исследования является международное сотрудничество аравийских монархий в области обеспечения кибербезопасности.

Хронологические рамки исследования включают период с конца 1990-х гг., когда монархиями Залива были предприняты первые шаги по регулированию национального информационного пространства и его цифровой защиты, до конца 2023 г., когда обозначенная группа государств прочно укрепилась на лидирующих позициях в области кибербезопасности среди стран Ближнего Востока и арабского мира. Выбор верхней хронологической границы обусловлен, кроме того, наличием статистических материалов по исследуемой

проблематике, а также кардинальными изменениями геополитической ситуации на Ближнем Востоке в связи с эскалацией конфликта между Израилем и ХАМАС в Секторе Газа в октябре 2023 г., что напрямую отразилось на международном сотрудничестве аравийских монархий в области кибербезопасности.

Географические рамки исследования охватывают шесть аравийских монархий – Бахрейн, Катар, Кувейт, Объединенные Арабские Эмираты (ОАЭ), Оман, Саудовскую Аравию. Данная группа государств расположена в зоне Персидского залива (субрегион Ближнего Востока), является интегральной частью арабского мира и мусульманского историко-культурного ареала. Указанные страны объединяют схожие тренды экономического и социально-политического развития, а также взаимодействие в рамках созданной ими региональной организации – Совета сотрудничества арабских государств Залива (ССАГЗ).

Методология и методы исследования. Методологическую основу данного исследования составляют *положения теорий неореализма*: «дилеммы безопасности» К. Уолтца, «гегемонистской стабильности» Р. Гилпина, «баланса угроз» С. Уолта, секьюритизации Б. Бузана и О. Вейвера, наступательного реализма Дж. Миршаймера, «гегемонии нового типа» и «технотронного общества» З. Бжезинского. Выбор методологических рамок определяется тем, что в условиях цифровой эпохи ключевыми акторами международных отношений остаются государства, которые ориентированы на защиту национальных интересов и обеспечение безопасности, а главным средством достижения обозначенных целей является сила и межгосударственное сотрудничество. Общетеоретической основой исследования, кроме того, стали фундаментальные труды крупнейшего исследователя информационной эпохи М. Кастельса, что позволило рассматривать Ближний Восток и регион Персидского залива как отдельный кластер в составе глобального «сетевого общества».

В рамках *принципа научной объективности* события и явления рассматривались как феномены объективной действительности во всей ее многогранности и противоречивости. Беспристрастное отношение к информации, отраженной в источниках и научной литературе, обеспечивалось применением *метода критического анализа*. *Системный подход и структурно-функциональный анализ* позволили исследовать цифровую плоскость международных отношений на Ближнем Востоке как целостную систему, обладающую сложной структурой и состоящую из совокупности элементов, каждый из которых находится в отношениях и связях с другими элементами, выполняет специфические функции, направленные на удовлетворение соответствующих потребностей системы. Базовым при работе над диссертацией также стал *сравнительно-сопоставительный метод*, что позволило выявить общие и отличительные характеристики международного сотрудничества монархий Залива в области кибербезопасности.

Оценка готовности аравийских монархий к отражению киберугроз производилась на основе методологии «Глобального индекса кибербезопасности», исследовательского мега-проекта под эгидой

Международного союза электросвязи (МСЭ), специализированного института ООН по ИКТ[24]. Индекс предусматривает 5 ключевых критериев национальных систем цифровой защиты: нормативно-правовая база, технический, организационный и кадровый потенциал, международное сотрудничество. Последний из указанных критериев включает межгосударственное и межведомственное взаимодействие в двусторонних и многосторонних форматах, государственно-частное партнерство международного уровня и поддержку малого и среднего бизнеса; партнерские отношения между профильными агентствами, фирмами и странами; наличие механизмов обмена технической информацией; сотрудничество в области развития цифрового потенциала, в том числе в рамках создания совместных исследовательских институтов и платформ, специализированных образовательных программ и т.д.

В процессе работы также применялись такие методы исследования международных отношений, как SWOT-анализ и сценарное прогнозирование. Ряд сюжетов диссертации исследовался в рамках *исторического подхода* с применением *проблемно-хронологического, историко-генетического и сравнительно-исторического методов*. Для обработки статистических данных применялись *методы статистического анализа*. Кроме того, были использованы *общенаучные методы* – анализ и синтез, сравнение и аналогия, систематизация и обобщение материала.

Источниковую базу исследования составили:

– международные договоры, конвенции, совместные декларации, в том числе Будапештская конвенция по борьбе с киберпреступлениями, Арабская конвенция о борьбе с преступлениями в области информационных технологий, декларации по итогам саммитов ССАГЗ, совместные декларации ССАГЗ и его отдельных участников с США, Евросоюзом, двусторонние соглашения аравийских монархий с внешними партнерами;

– документы и материалы международных организаций – ООН и МСЭ, ССАГЗ, ЛАГ, ОИС, Международной организации по стандартизации, Европейского агентства по сетевой и информационной безопасности, а также международных правозащитных, правоохранительных и мониторинговых организаций;

– нормативно-правовые акты, составляющие основу регулирования информационного пространства в монархиях Залива;

– национальные стратегии и программы развития: национальные и отраслевые стратегии кибербезопасности аравийских монархий и США, Доктрина информационной безопасности РФ, Основы государственной политики РФ в области международной информационной безопасности, программы долгосрочного экономического развития «Видение» монархий Залива и т.д.;

– отчеты и пресс-релизы органов государственной власти аравийских монархий, США (Госдепартамента, Министерства обороны, Центрального командования), национальных групп реагирования на компьютерные инциденты

[24] Global Cybersecurity Index 2014–2020. Geneva: ITU, 2015– 2021.

монархий Залива (CERT) и ряда других государств, оказывающих заметное влияние на развитие ландшафта кибербезопасности на Ближнем Востоке;

– отчеты и материалы IT-компаний, вовлеченных в развитие национальных систем киберзащиты аравийских монархий или осуществляющих системную оценку результатов их профильной деятельности: CISCO, IBM, Microsoft, CYJAX, Kaspersky, Proofpoint, InfoWatch, C4ISRNET, ABI и др.;

– статистические отчеты и базы данных о развитии сектора телекоммуникаций и рынка кибербезопасности на Ближнем Востоке публикуемые Всемирным банком, Лабораторией Касперского, Statista, Markets&Markets, PWC и т.д.;

– официальные заявления и интервью государственных деятелей и дипломатов Саудовской Аравии, ОАЭ, США по вопросам международного сотрудничества стран ССАГЗ;

– материалы СМИ: арабских стран (Al Arabiya, Al Khaleej, Doha News, Zawya), западных (The New York Times, The Washington Post, CNN, BBC, Reuters и др.) и российских (РБК, Газета.ru).

Научная новизна исследования. Анализ политики монархий Залива в области кибербезопасности через призму развития международного сотрудничества проводится в России впервые. Научная новизна исследования обусловлена совокупностью привлеченных к анализу методологических концепций, а также разнообразных по характеру источников и научной литературы, что позволило выявить ключевые тренды и особенности развития взаимодействия аравийских монархий с региональными и внерегиональными акторами по вопросам создания безопасной цифровой среды в зоне Персидского залива и на Ближнем Востоке в целом.

Научной новизной обладают конкретные результаты исследования:

– определен комплекс угроз национальной безопасности монархиям Залива, исходящих из информационного пространства и побуждающих к разработке коллективного ответа на цифровой вызов;

– раскрыты особенности подхода аравийских монархий к решению проблем национальной и международной информационной безопасности, обоснована целесообразность многовекторного развития их внешнеполитических связей в области противодействия ИКТ-угрозам;

– выявлены факторы, ограничивающие динамику и направления кооперации монархий Залива в вопросах кибербезопасности на платформе ССАГЗ, а также их взаимодействия со странами арабского и исламского мира на интеграционных площадках ЛАГ и ОИС;

– раскрыта роль внерегиональных и региональных (ближневосточных) акторов в формировании и развитии национальных систем кибербезопасности аравийских монархий, выделены ключевые критерии выбора внешнеполитических партнеров и особенности выстраивания диалога по вопросам цифровой защиты;

– раскрыты причины преимущественной ориентации монархий Залива на формат двустороннего сотрудничества с США в вопросах развития военного

сектора кибербезопасности; определены факторы, препятствующие реализации проектов создания на Ближнем Востоке региональной системы кибербезопасности под эгидой США;

– предложены возможные сценарии дальнейшей кооперации монархий Залива в вопросах создания общей безопасной цифровой среды с учетом влияния на этот процесс внешних и внутренних факторов, а также в контексте развития военно-политической обстановки на Ближнем Востоке.

Положения, выносимые на защиту:

1. Монархии Персидского залива формально придерживаются «западной» концепции обеспечения национальной и международной информационной безопасности, акцентируя внимание на технико-технологической защите информационного пространства. Однако на практике указанные государства дополняют свою политику в сфере кибербезопасности социально-политическими аспектами, что сближает их видение с российским подходом.

2. Из триады ИКТ-угроз для монархий Залива первостепенное значение имеет фактор применения цифровых технологий в военно-политических целях государственными акторами ближневосточной политики и их прокси. В совокупности с ИКТ-угрозами со стороны преступных сообществ и террористических группировок это стимулирует рассматриваемые страны к развитию систем киберзащиты. С принятием стратегических программ «Видение», где ИКТ отводится роль одного из драйверов социально-экономических преобразований, работа по совершенствованию национальных систем кибербезопасности приобрела комплексный и динамичный характер. Это позволило монархиям войти в число ближневосточных и общеарабских лидеров по уровню готовности к отражению киберугроз, а Саудовской Аравии и ОАЭ – в мировой топ-5. Вместе с тем ни одна из стран пока не достигла показателя абсолютной киберготовности ввиду системного характера большинства имеющихся проблем развития национальных секторов киберзащиты, что требует дальнейшей работы, а также формирует запрос на создание совместной безопасной среды.

3. Проекты коллективной киберзащиты продвигаются на площадках регионального взаимодействия ССАГЗ, ЛАГ и ОИС, где формируется правовая и институциональная основа профильного взаимодействия, но отсутствуют высокая динамика и серьезные подвижки в решении проблемы. Это обусловлено незавершенностью процесса создания национальных систем кибербезопасности стран – участниц обозначенных организаций, а также внутренней разнородностью и противоречивостью как арабского, так и мусульманского мира. В этой связи монархии Залива отдают предпочтение более гибким форматам двустороннего сотрудничества между собой и с членами ЛАГ и ОИС.

4. Участие внерегиональных акторов в развитии сектора кибербезопасности аравийских монархий мотивировано экономическими интересами (внушительная емкость местного рынка ИКТ и защитных цифровых технологий), а также тесно связано с проводимой ими на Ближнем Востоке политикой. Сотрудничество реализуется в двустороннем формате

(межгосударственное взаимодействие, государственно-частное партнерство), который является доминирующим, а также на платформе ССАГЗ. Монархии Залива стремятся к диверсификации профильных международных контактов для расширения доступа к новейшим ИКТ, поэтому при выборе внешних партнеров отдают предпочтение мировым лидерам технологической гонки, прежде всего в лице США и Китая, а также государствам и объединениям, с которыми установлены отношения стратегического партнерства (Европейский союз, Индия, Республика Корея, Япония и т.д.).

5. Традиционно высокий конфликтный потенциал Ближнего Востока побуждает монархии Залива уделять повышенное внимание развитию военного сектора национальной кибербезопасности, которое реализуется преимущественно в рамках двустороннего военного сотрудничества с США. Кибербезопасность также играет важную роль в формировании подходов к обеспечению безопасности на Ближнем Востоке. Однако стремление США, Израиля и ряда стран ССАГЗ заложить в основу региональной системы кибербезопасности довольно неоднозначную идею «иранской перманентной угрозы», разногласия по вопросу о допустимости и возможных пределах сотрудничества с Израилем, а также нежелание подписывать многосторонние соглашения военно-политического характера затрудняют практическую реализацию подобных проектов с участием аравийских монархий.

6. Текущий тренд на объединение усилий на платформе ССАГЗ следует трактовать как постепенное сближение стран-участниц в контексте поиска эффективных инструментов противодействия киберугрозам. Однако в обозримой перспективе можно ожидать, что монархии Залива продолжат отдавать приоритет развитию национальных систем кибербезопасности, делая ставку на наращивание международного сотрудничества в двустороннем формате, вне прямой зависимости от интенсивности профильного взаимодействия в рамках ССАГЗ.

Теоретическая и практическая значимость исследования. Теоретическая значимость диссертационного исследования заключается в расширении научных знаний об особенностях сотрудничества аравийских монархий в области развития национального киберпотенциала и создания безопасной цифровой среды в зоне Персидского залива. Основные положения и выводы работы могут быть использованы в дальнейших исследованиях по проблемам цифровой безопасности стран арабского мира и Ближнего Востока.

Практическая значимость исследования состоит в том, что его материалы могут быть востребованы ответственными государственными структурами при подготовке экспертных заключений и принятии внешнеполитических решений касательно развития профильного сотрудничества с монархиями Залива. Кроме того, результаты диссертационного исследования могут найти практическое применение при разработке и чтении учебных курсов для студентов, обучающихся по направлениям подготовки «Международные отношения», «Политология», «Востоковедение», «Зарубежное регионоведение».

Достоверность результатов проведенного исследования обеспечена опорой на принципы научной объективности и системности, критическим подходом к анализу разнообразного по характеру корпуса эмпирического материала и научной литературы с учетом достижений и методологических наработок зарубежных и российских научных школ, специализирующихся на проблемах международной информационной безопасности и ближневосточных исследованиях.

Апробация результатов работы. Основные положения и результаты исследования отражены в 35 публикациях общим объемом 14 п.л., в том числе в 5 статьях в рецензируемых научных изданиях, определенных ВАК РФ и Аттестационным советом УрФУ. Основные положения и выводы обсуждались на 35 всероссийских и международных научных конференциях. В их числе: XVI конференция арабистов «Чтения И.М. Смилянской» (Москва, 2021 г.), V международный конкурс научно-аналитических работ по ближневосточной проблематике им. Е.М. Примакова (Москва, 2022 г.), VIII международный научно-экспертный форум «Примаковские чтения» (Москва, 2022 г.), экспертная сессия международного клуба «Триалог» (ПИР-Центр) «Иран, Израиль и страны Персидского Залива. Новые тренды в условиях изменения геополитического ландшафта» (Звенигород, 2023 г.), экспертный семинар «По обе стороны Персидского залива: развитие высокотехнологичного бизнеса в регионе и интересы России»» (Москва, 2023 г.) и др. Ряд положений и выводов диссертационного исследования, кроме того, был представлен в программе повышения квалификации «Научно-технологическая политика стран Африки южнее Сахары и государств Персидского залива», реализованной МГИМО МИД России совместно с АНО «Политические исследования России» (ПИР-Центр) в рамках программы стратегического академического лидерства «Приоритет-2030» 20-27 ноября 2023 г. (г. Москва).

Структура диссертации. Работа состоит из введения, трех глав, заключения, списка источников и литературы, приложений (таблицы, схемы, список сокращений). Общий объем работы – 245 стр.

II. ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **Введении** обоснована актуальность темы; раскрыта степень ее научной разработанности; определены цель и задачи исследования, его объект, предмет, хронологические и географические рамки, теоретико-методологические основы, методы и источниковая база; сформулированы основные положения, выносимые на защиту; раскрыта научная новизна, теоретическая и практическая значимость; представлены сведения об апробации результатов работы.

В **первой главе «Концептуальные подходы к исследованию международной информационной безопасности»** раскрывается суть академических дискуссий по вопросам содержания и методов обеспечения международной информационной безопасности, а также роли и места

международного сотрудничества в процессе создания безопасной цифровой среды на национальной, региональном и глобальном уровнях.

В *параграфе 1.1* «*Кибербезопасность как предмет политического анализа»* подчеркивается высокая степень дискуссионности рассматриваемой проблематики, что обусловлено ее относительной новизной и многоаспектным характером, несформированностью научно-терминологического аппарата, доктринальными разногласиями между государствами, а также разницей концептуальных подходов, принятых в тех или иных научных школах.

Автор выделяет три ключевых подхода к определению содержания и соотношению базовых терминов «информационная безопасность» и «кибербезопасность». В рамках первого, «западного» подхода (США, Канада, страны Европы, ряд государств Азии), указанные термины выступают в качестве синонимов и охватывают широкий круг проблем, связанных с технико-технологической защитой информационных сетей и систем, а также соблюдением законности и правопорядка в телекоммуникационной сфере. Второй, «не-западный», расширительный подход (Россия, Китай, большинство стран Азии и Африки) ранжирует информационную безопасность в соответствии с видами угроз и разделяет ее на два направления – технико-технологическое (кибербезопасность) и политико-идеологическое (защита общества от деструктивного информационного воздействия извне, нацеленного на подрыв социальной стабильности и международного авторитета государства; противодействие использованию ИКТ в качестве инструмента вмешательства во внутренние дела суверенных государств, разжигания межэтнической и межконфессиональной розни и т.д.). Третий подход представлен позицией ООН, которая была сформулирована в 1999 г. на основе российских инициатив и учитывает специфику двух обозначенных выше подходов. ООН определяет содержание понятия «международная информационная безопасность» в контексте «триады угроз» – использование ИКТ в военно-политических целях (межгосударственных конфликтах), преступных и террористических.

Диссертант отмечает, что рост численности, типов и форм вредоносной деятельности в информационном пространстве, а также тенденция к размыванию традиционных границ между ними способствуют расширению предметного поля академических и политических дискуссий, порождая множество неологизмов с приставкой «кибер-» и прилагательными «информационный», «цифровой», «электронный», «виртуальный» и т.п.

Автор резюмирует, что кибербезопасность охватывает информационно-технологическую сферу и является одним из направлений информационной безопасности, которая, в свою очередь, играет ключевую роль в обеспечении международной и национальной безопасности. Трансграничный характер кибербезопасности требует разработки комплекса мер по борьбе с киберугрозами на различных уровнях – технологическом, экономическом, политическом, правовом, управленческом, военном и т.д. Международное сотрудничество является краеугольным камнем в обеспечении национальной и международной кибербезопасности, может реализовываться в формате

двустороннего и многостороннего, а также формального и неформального взаимодействия.

В *параграфе 1.2 «Методологические основы исследования»* обосновывается целесообразность применения методологического инструментария неореалистского подхода для комплексного анализа особенностей и трендов развития международного сотрудничества монархий Залива в сфере кибербезопасности.

ИКТ обеспечили современные государства, остающиеся главными акторами международных отношений, принципиально новыми инструментами для наращивания силовой компоненты и отстаивания своих основополагающих приоритетов, в число которых, согласно неореалистам, входят защита национальных интересов, обеспечение безопасности и сохранение статус-кво. Диссертант отмечает, что трансформация международных отношений на Ближнем Востоке под влиянием цифрового фактора формирует богатый эмпирический материал для научного осмысления и дальнейшего развития базовых идей ведущих представителей неореализма – К. Уолтца, Дж. Грико, Р. Гилпина, С. Уолта, Б. Бузана и О. Вейвера, Дж. Миршаймера, З. Бжезинского. Вместе с тем автор подчеркивает, что даже между исследователями, проводящими анализ взаимовлияния цифровых технологий и международных отношений в рамках неореализма, имеется ряд существенных разногласий (например, по вопросу о воздействии технологий искусственного интеллекта на «дилемму безопасности» и т.п.).

Диссертант обосновывает положение о том, что в условиях информационной эпохи государствам отводится ведущая, координирующая роль в многоуровневом взаимодействии всех субъектов кибербезопасности, а ключевым форматом кооперации остается межправительственное сотрудничество. Соответственно именно неореализм остается базовым для анализа международного сотрудничества в сфере кибербезопасности, что, однако, не исключает возможности его дополнения отдельными теоретическими наработками других методологических подходов. В рамках данного исследования была привлечена концепция «сетевого общества» М. Кастельса, что позволило рассматривать регион Персидского залива не только как самостоятельный кластер с динамично развивающимися структурами киберзащиты в общей системе безопасности Ближнего Востока, но и как часть глобального цифрового общества, задающего тренды развития.

Вторая глава «Тренды развития национальных систем кибербезопасности монархий Залива» посвящена анализу эволюции национальных секторов цифровой защиты аравийских монархий, определению их эффективности, выявлению особенностей и рисков их развития.

В *параграфе 2.1 «Аравийские монархии в условиях цифрового вызова»* выявляются три группы угроз, исходящих из цифрового пространства зоны Персидского залива и Ближнего Востока и формирующих цифровой вызов для монархий Залива: киберпреступность, кибертерроризм и применения ИКТ в военно-политических целях.

С точки зрения национальной безопасности из указанной триады угроз наиболее значимой для монархий Залива является ширящаяся практика использования цифровых средств и инструментов в межгосударственном противостоянии, прежде всего по линии противостояния Ирану, а также в региональных конфликтах, которые в той или иной степени затрагивают интересы аравийских монархий и где представлены иранские прокси (сирийский, йеменский, палестино-израильский и др.). Соответственно ключевым источником киберугроз в зоне Залива выступают государственные акторы, которые имеют практически неограниченные возможности в сфере развития национального киберпотенциала, причем не только оборонительного, но и наступательного, и для которых цифровые технологии становятся одним из ключевых элементов национальной силовой компоненты.

Помимо государств, носителями угроз в киберпространстве Персидского залива и Ближнего Востока являются внесистемные акторы – кибергруппы, предположительно спонсируемые государствами; политически мотивированные хактивисты и хакеры-одиночки, которые, как правило, руководствуются теми или иными идеологическими парадигмами, а также радикально-экстремистские и террористические группировки. Киберпреступность и кибертерроризм также формируют общий для монархий Залива цифровой вызов, побуждая совершенствовать национальные системы кибербезопасности и актуализируя вопрос о необходимости развивать международное сотрудничество и вырабатывать коллективные меры цифровой защиты.

В *параграфе 2.2 «Уровень готовности к отражению киберугроз»* на основе методологии МСЭ ООН проводится анализ структуры национальных систем киберзащиты монархий Залива по пяти ключевым критериям: нормативно-правовая система, технический потенциал, организационная структура, меры по развитию потенциала, международное сотрудничество.

Автор выделяет три периода в процессе эволюции национальных систем кибербезопасности монархий Залива: первый (конец 1990-х – 2006 гг.) характеризуется формированием институциональных и правовых основ регулирования национального информационного пространства; второй (2007–2015 гг.) – развитием внешних связей и адаптацией к местным реалиям зарубежного опыта в области цифровой защиты (технического, правового, организационного, образовательного, научно-исследовательского и т.д.), совершенствованием инструментов и механизмов координации развития профильной отрасли; на третьем этапе (с 2016 г. по настоящее время) под влиянием программ «Видение» началось форсированное строительство комплексных систем национальной киберзащиты, что актуализировало вопрос о диверсификации международных связей. К настоящему времени развитие систем кибербезопасности аравийских монархий характеризуется динамичностью и имеет восходящий вектор. За относительно короткое время государствам удалось выстроить, в целом, эффективную структуру цифровой защиты и достичь лидирующих позиций в мировых и региональных (ближневосточных и общеарабских) рейтингах готовности к отражению

киберугроз. В то же время ни одна из монархий пока не достигла показателя абсолютной киберготовности, хотя их работа по повышению эффективности национальных систем киберзащиты стала более комплексной и последовательной. Для всех стран в той или иной степени характерны проблемы с наращиванием технического потенциала, требуют доработки нормативно-правовая сфера, институциональная структура и стратегические программы развития цифровой защиты, далеко не в полной мере используются возможности международного сотрудничества.

В *параграфе 2.3 «Запрос на коллективные меры киберзащиты»* выявляется комплекс факторов, формирующих тренд на объединение усилий монархий Залива в области создания совместной безопасной цифровой среды.

Для коммуникационной структуры Ближнего Востока, включая зону Персидского залива, характерны относительно низкая устойчивость к внешним воздействиям (цифровым и физическим), недостаточное количестве точек обмена интернет-трафиком и неравномерность в их географическом размещении. Однако трансформация ИКТ-инфраструктуры реализуется каждой из монархий самостоятельно и строго с ориентацией на национальные приоритеты кибербезопасности, совместные инициативы пока не получили должной поддержки даже на уровне ССАГЗ.

Запрос на коллективные меры цифровой защиты обусловлен не только техническими аспектами проблемы, но и комплексом экономических, политических, социальных и иных факторов. Все рассматриваемые государства в той или иной степени испытывают схожие проблемы с актуализацией законодательств и приведением их в соответствие с реалиями цифровой эпохи, стратегическим планированием, оптимизацией институциональной структуры отрасли, высокой степенью зависимости от внешних партнеров в вопросах доступа к новейшим технологиям и готовым технологическим решениям, формированием собственного кадрового потенциала и т.д. Это порождает запрос на координацию действий и закладывает основу и для расширения многостороннего сотрудничества, прежде всего на региональных интеграционных площадках ССАГЗ, ЛАГ, ОИС.

Важнейшим стимулом к развитию сотрудничества в сфере кибербезопасности является запрос на снижение конфликтного потенциала региона и стратегическую гибкость. Присущая Ближнему Востоку атмосфера недоверия порождает широкий спектр рисков развития национальных систем кибербезопасности монархий Залива – слабую развитость горизонтальных связей и отсутствие координации между различными субъектами цифровой защиты (органами госуправления, правоохранительными, силовыми и бизнес-структурами, спецслужбами, техническими государственными агентствами, научно-исследовательскими институтами и пр.). Наиболее негативное влияние на ситуацию оказывает обострившееся соперничество между военным и гражданским секторами кибербезопасности на фоне усложнения военно-политической обстановки на Ближнем Востоке. Использование монархиями Залива цифровых технологий не только в интересах социально-экономической

модернизации и обеспечения национальной кибербезопасности, но также в качестве инструментов для реализации внешнеполитических амбиций и купирования внутренних проблем развития серьезно осложняет и ухудшает военно-политическую ситуацию в регионе, увеличивая его и без того высокий конфликтный потенциал.

В **третьей главе «Основные направления международного сотрудничества монархий Залива в области кибербезопасности»** рассматриваются многосторонние и двусторонние форматы взаимодействия по вопросам реагирования на цифровой вызов, выявляются факторы, определяющие выбор монархиями Залива внешних партнеров в вопросах развития национальных систем кибербезопасности и совместных профильных проектов.

Параграф 3.1 «Региональные площадки взаимодействия: ССАГЗ, ЛАГ, ОИС» посвящен анализу взаимодействия аравийских монархий в сфере кибербезопасности со странами арабского и мусульманского мира в рамках региональных объединений.

Автор отмечает, что декларируемый монархиями Залива курс на развитие коллективной системы кибербезопасности на платформе ССАГЗ еще далек от реализации на практике, несмотря на серьезные подвижки в вопросах профильной кооперации: в Совете действуют профильные структуры (Комитет CERT, Постоянный комитет по кибербезопасности, Министерский комитет по электронному правительству и др.), ответственные за разработку и реализацию совместных инициатив. Однако дисбалансы в развитии национальных систем киберзащиты, атмосфера взаимного недоверия и нежелание делиться с партнерами чувствительными технологиями, внутренние противоречия в организации детерминируют сравнительно низкую динамику кооперации по проблемам кибербезопасности. Монархии продолжают отдавать предпочтение более гибкому формату сотрудничества – на двусторонней основе, а достижения такого диалога зачастую позиционируются как результат совместной работы членов ССАГЗ.

Трансграничный характер ИКТ-угроз вынуждает монархии Залива расширять географические контуры совместных проектов, интегрируя в свою повестку кибербезопасности вопросы межарабского сотрудничества. ЛАГ имеет определенные наработки в области коллективной цифровой защиты, однако большинство инициатив пока не удалось перевести в практическую плоскость ввиду внутренней разнородности и противоречивости арабского мира. Схожим образом ситуация развивается и в ОИС, где совместные проекты сосредоточены преимущественно на обмене информацией в рамках технических групп реагирования на компьютерные инциденты (CERT) и продвижении профильных образовательных программ. В этой связи аравийские монархии предпочитают развивать взаимодействие с отдельными членами ЛАГ и ОИС в двустороннем формате. Вместе с тем автор подчеркивает, что в силу геополитического веса Лиги, представляющей на международной арене интересы всех арабских государств, а также наличия широко спектра механизмов межарабского

взаимодействия и воздействия на отдельные государства, профильные рабочие группы и иные структуры ЛАГ, как правило, куда чаще служат площадкой для выработки первичных договоренностей между монархиями Залива в области коллективной киберзащиты.

В *параграфе 3.2 «Военное сотрудничество и кибербезопасность»* раскрывается значимость военного направления международного сотрудничества монархий Залива в области киберзащиты и влияние цифрового фактора на вопросы обеспечения региональной безопасности.

Ключевую роль в формировании оборонительного и наступательного киберпотенциала аравийских монархий играют США, их главный стратегический союзник. Военное сотрудничество с Вашингтоном в области кибербезопасности развивается по линии взаимодействия с ССАГЗ, где усилия сосредоточены преимущественно на противодействии кибертеррористической угрозе. Но наибольшая интенсивность контактов характерна для двустороннего взаимодействия, особенно по линии США – Саудовская Аравия.

Проблемы цифровой защиты оказывают прямое влияние на формирование подходов к обеспечению региональной безопасности, о чем свидетельствуют проекты Ближневосточного стратегического альянса (MESA) и «Негевской инициативы» с участием США и Израиля. Однако указанные военно-политические проекты не вышли на уровень практической реализации, так как заложенная в них идея «перманентной иранской угрозы» не получила поддержки со стороны большинства аравийских монархий, возродив между ними, кроме того, разногласия по вопросу о целесообразности и допустимых пределах участия Израиля в цифровой защите арабских стран.

В *параграфе 3.3 «Роль внерегиональных акторов в формировании безопасной цифровой среды в аравийских монархиях»* раскрывается внушительный вклад внешних акторов в развитие систем кибербезопасности монархий Залива.

В области киберзащиты в качестве ключевых внерегиональных партнеров (внешних по отношению к региону Ближнего Востока) монархий Залива выступают США, КНР, Индия, страны ЕС, Великобритания, Канада, Япония, Республика Корея. Важная роль также отводится таким внерегиональным акторам (внешним по отношению к ближневосточным субрегионам в границах зоны Персидского залива и арабского мира), как Израиль и Турция. Интерес внерегиональных партнеров обусловлен значительной емкостью местного рынка ИКТ и технологий цифровой защиты, а также императивами их ближневосточной политики. Сотрудничество реализуется как на платформе ССАГЗ, так и в двустороннем формате, преимущественно в рамках межгосударственного взаимодействия и государственно-частного партнерства.

В свою очередь монархии Залива при выборе внешних партнеров отдают предпочтение мировым лидерам технологической гонки, прежде всего в лице США и Китая. Более высокая интенсивность профильных связей, кроме того, характерна для тех внерегиональных акторов, отношения с которыми вышли на уровень стратегического партнерства: в случае с США и Евросоюзом – по линии

ССАГЗ и в двустороннем межгосударственном формате, в случае с КНР, Индией, Республикой Корея, Японией – на уровень партнерств с отдельными монархиями. Данный тренд в совокупности с готовностью увеличить число своих стратегических партнеров обусловлен стремлением монархий Залива диверсифицировать свои внешнеполитические связи для обеспечения надежной цифровой защиты и расширения доступа к новейшим технологиям.

Вместе с тем высокий уровень конфликтности на Ближнем Востоке и ухудшающиеся региональные реалии актуализируют взаимодействие со стратегическими союзниками, прежде всего США, что сужает поле для открытой конкуренции и ограничивает каждую из монархий Залива в выборе внешних партнеров для развития сектора кибербезопасности и цифровизации в целом.

В параграфе 3.4 «Перспективы и риски развития кооперации по вопросам кибербезопасности в рамках ССАГЗ» представлена характеристика зарождающейся в регионе Персидского залива коллективной системы кибербезопасности. С использованием метода SWOT-анализа выявляются сильные стороны и уязвимости ее внутренней среды, определяется влияние на ее развитие внешних факторов – возможностей и угроз. Приводятся прогнозные сценарии дальнейшего развития тренда на кооперацию монархий Залива в области кибербезопасности.

Автор отмечает, что в рамках наиболее вероятного сценария аравийские монархии будут придерживаться комплексного подхода к обеспечению кибербезопасности, признаки формирования которого можно наблюдать в настоящее время. Сохраняя приоритет развития национальных киберсистем и приверженность двусторонним форматам сотрудничества (в первую очередь с передовыми технологическими державами), государства ССАГЗ также будут проявлять интерес к разработке совместных профильных проектов, которые способны увеличить их геополитический вес и влияние, а также ускорить продвижение к технологическому суверенитету.

В целом, анализ взаимодействия монархий Залива по вопросам кибербезопасности на региональных площадках ССАГЗ, ЛАГ и ОИС, в рамках координации действий на военном направлении, а также развития двусторонних и многосторонних связей с внерегиональными и ближневосточными партнерами позволяет автору сделать вывод о значимой роли международного сотрудничества в создании безопасной цифровой среды в зоне Персидского залива и на Ближнем Востоке в целом. Многовекторный характер кооперации аравийских монархий обусловлен комплексом объективных внутренних и внешних факторов, которые не позволяют продвигать профильные интеграционные инициативы форсированными темпами. В этой связи тренд на разработку и реализацию совместных проектов цифровой защиты в рамках ССАГЗ можно трактовать скорее как постепенное, осторожное сближение и «притирку» государств в контексте поиска эффективных инструментов противодействия киберугрозам. Соответственно активизация международного сотрудничества, ставку на которое сделали все без исключения монархии Залива в вопросах обеспечения национальной и региональной кибербезопасности,

создает благоприятные условия для развития совместных инициатив и выработку на платформе ССАГЗ коллективного ответа на цифровой вызов.

В **Заключении** подведены итоги работы, сформулированы основные выводы, намечены перспективы дальнейшего исследования проблемы.

III. ПУБЛИКАЦИИ АВТОРА ПО ТЕМЕ ДИССЕРТАЦИИ

а) статьи, опубликованные в рецензируемых научных журналах и изданиях, определенных ВАК РФ и Аттестационным советом УрФУ:

1. Цуканов Л.В. Сотрудничество Израиля и Катара в сфере кибербезопасности // Теории и проблемы политических исследований. 2021. № 5А. С. 28–36 / 0,7 п.л.
2. Цуканов Л.В. После А. аз-Завахири: изменится ли «кибердоктрина» «Аль-Каиды»? // Известия Иркутского государственного университета. Серия Политология. Религиоведение. 2022. Т. 42. С. 61–69 / 0,6 п.л.
3. Цуканов Л.В. «Цифровой тандем» ОАЭ – Израиль: сценарии и пределы сотрудничества // Вестник ученых-международников. 2022. № 4 (22). С. 77–84 / 0,5 п.л.
4. Цуканов Л.В., Валиахметова Г.Н. Цифровой вызов для арабского мира: фактор интеграции или дифференциации? // Вестник РУДН. Серия: международные отношения. 2022 Т. 22. № 2. С. 303–319 / 1 п.л. / 0,5 п.л..
5. Цуканов Л.В. Особенности формирования системы национальной кибербезопасности Государства Кувейт // Известия Иркутского государственного университета. Серия Политология. Религиоведение. 2023. Т. 45. С. 49–58 / 0,7 п.л.

б) другие публикации по теме исследования:

6. Цуканов Л.В. «Школы будущего короля Хамада» как фактор модернизации королевства Бахрейн // Мир Евразии: от древности к современности: сборник материалов Всероссийской научно-практической конференции. Уфа. 2020. С. 316–320 / 0,7 п.л.
7. Цуканов Л.В. Лига киберсправедливости: как Арабский мир видит коллективную кибербезопасность? // ПИР-Центр. 22.12.2020. URL: https://pircenter.org/editions/liga-kiberspravedlivosti-kak-arabskij-mir-vidit-kollektivnuju-kiberbezopasnost/ / 0,3 п.л.
8. Цуканов Л.В. Система национальной кибербезопасности Саудовской Аравии: специфика и риски развития // Вестник Кемеровского университета. 2021. № 4 (22). С. 435–443 / 0,5 п.л.
9. Цуканов Л.В. Силы безопасности ССАГПЗ: цифровое измерение // РСМД. 28.07.2021. URL: https://russiancouncil.ru/analytics-and-comments/columns/middle-east/sily-bezopasnosti-ssagpz-tsifrovoe-izmerenie/ / 0,3 п.л.

10. Цуканов Л.В. Страны ССАГПЗ и Израиль: да будет «цифровая солидарность»? // РСМД. 30.06.2021. URL: https://russiancouncil.ru/analytics-and-comments/analytics/strany-ssagpz-i-izrail-da-budet-tsifrovaya-solidarnost/ / 0,3 п.л.
11. Цуканов Л.В. Цифровая дипломатия России на Ближнем Востоке: настоящее и будущее // Современные международные отношения глазами студентов и аспирантов Урала: сборник лучших эссе. 2021. С. 53–56 / 0,2 п.л.
12. Цуканов Л.В., Валиахметова Г.Н. «Сумма всех ресурсов страны»: специфика израильского подхода к обеспечению национальной кибербезопасности // Уральское востоковедение: международный альманах. 2021. № 11. С. 23–35. / 1 п.л. (50%).
13. Цуканов Л.В. «Кибермухи отдельно»: будущее хакерского движения в Саудовской Аравии // РСМД. 29.10.2021. URL: https://russiancouncil.ru/analytics-and-comments/analytics/kibermukhi-otdelno-budushchee-khakerskogo-dvizheniya-v-saudovskoy-aravii/ / 0,3 п.л.
14. Цуканов Л.В. Коллективная кибербезопасность: позиция ССАГПЗ // Сборник материалов международной конференции 5-й молодежный Конвент УрФУ «Трансформация реальности: стратегии и практики», 25–27 марта 2021 г. С. 218–221 / 0,2 п.л.
15. Цуканов Л.В. Политика ОАЭ в области регулирования криптовалют на современном этапе // Евразийский журнал региональных и политических исследований. 2021. № 1. С. 49–55 / 0,5 п.л.
16. Цуканов Л.В. Политика Королевства Бахрейн в сфере цифровизации образования // Вестник Омского университета. Серия «Исторические науки». 2022. Т. 9. № 3 (35). С. 185–191 / 0,5 п.л.
17. Цуканов Л.В. Цифровые химеры Персидского залива: кто займет место Ирана? // РСМД. 22.02.2022. URL: https://russiancouncil.ru/analytics-and-comments/columns/middle-east/tsifrovye-khimery-persidskogo-zaliva-kto-zaymet-mesto-irana/ / 0,3 п.л.
18. Цуканов Л.В. «Арабское НАТО»: даешь новый заход? // РСМД. 24.03.2022. URL: https://russiancouncil.ru/analytics-and-comments/analytics/arabskoe-nato-daesh-novyy-zakhod/ / 0,3 п.л.
19. Цуканов Л.В. Проиранские хакеры: «пояс безопасности» Тегерана? // РСМД. 04.07.2022. URL: https://russiancouncil.ru/analytics-and-comments/analytics/proiranskie-khakery-poyas-bezopasnosti-tegerana/ / 0,3 п.л.
20. Цуканов Л.В. Ирано-албанский кризис отношений: куда ведет цифровой след? // РСМД. 13.09.2022. URL: https://russiancouncil.ru/analytics-and-comments/analytics/irano-albanskiy-krizis-otnosheniy-kuda-vedet-tsifrovoy-sled/ / 0,3 п.л.
21. Цуканов Л.В. Делийская декларация: шаг к победе над цифровым террором // ПИР-Центр. 03.11.2022. URL: http://pir.dfagency.ru/editions/delijskaja-deklaracija-shag-k-pobede-nad-cifrovym-terrorom/ / 0,3 п.л.
22. Цуканов Л.В. «Киберянычары»: пять лет на службе Турции // РСМД. 08.12.2022. URL: https://russiancouncil.ru/analytics-and-comments/analytics/kiberyanychary-pyat-let-na-sluzhbe-turtsii/ / 0,3 п.л.

23. Цуканов Л.В. Идем в 2023-й: ландшафт киберугроз на Ближнем Востоке // ПИР-Центр. 15.12.2022. URL: https://pircenter.org/editions/strong-idem-v-2023-j-landshaft-kiberugroz-na-blizhnem-vostoke-strong/ / 0,3 п.л.
24. Цуканов Л.В. Тонкости дружбы в кулуарах арабо-израильского киберальянса // РСМД. 26.01.2023. URL: https://russiancouncil.ru/analytics-and-comments/analytics/tonkosti-druzhby-v-kuluarakh-arabo-izrailskogo-kiberalyansa/ / 0,3 п.л.
25. Цуканов Л.В. Арабо-израильский «Киберкупол» // РСМД. 14.03.2023. URL: https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/arabo-izrailskiy-kiberkupol/ / 0,3 п.л.
26. Цуканов Л.В. Перспективы возвращения группировки ИГИЛ* к тактике «цифрового джихада» // Восточный курьер. 2023. С. 158-169 / 1 п.л.
27. Цуканов Л.В. Сирия и «арабская семья»: цифровой аспект возвращения // РСМД. 17.05.2023. URL: https://russiancouncil.ru/analytics-and-comments/columns/middle-east/siriya-i-arabskaya-semya-tsifrovoy-aspekt-vozvrashcheniya/ / 0,4 п.л.
28. Цуканов Л.В. Никто не знает о персидских котах: группировка «Charming Kitten» и стратегия безопасности Тегерана // РСМД. 08.08.2023. URL: https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/nikto-ne-znaet-o-persidskikh-kotakh-gruppirovka-charming-kitten-i-strategiya-bezopasnosti-tegerana/ / 0,3 п.л.
29. Цуканов Л.В. «Цифровой шторм» Аль-Акса: штрихи к противостоянию Израиля и ХАМАС // РСМД. 18.01.2024. URL: https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/tsifrovoy-shtorm-al-aksa-shtrikhi-k-protivostoyaniyu-izrailya-i-khamas/ / 0,4 п.л.
30. Цуканов Л.В. Взлеты и падения «киберхалифата»: Аль-Каида* и ИГИЛ* в цифровом пространстве / Ред. Е.Г. Чобанян. М.: ПИР-Пресс, 2022. 39 с. (Индекс Безопасности – Научные записки). ISBN 978-5-6048679-2-1 / 1,3 п.л.
31. Цуканов Л.В. Технологический ренессанс в Африке южнее Сахары: вызовы и возможности для России // Доклады ПИР-Центра. № 37. М.: ПИР-Центр, 2023. - 80 с. / 3,2 п.л.
32. Цуканов Л.В. «По обе стороны Персидского залива»: развитие высокотехнологичного бизнеса в регионе и интересы России // Доклады ПИР-Центра. № 38. М.: ПИР-Центр, 2023. - 76 с. / 3,2 п.л.
33. Цуканов Л.В. Facebook[25]-оборона: как Израиль видит ландшафт безопасности в соцмедиа? // ПИР-Центр. 14.02.2024. URL: https://pircenter.org/editions/facebook-oborona-kak-izrail-vidit-landshaft-bezopasnosti-v-socmedia/ / 0.3 п.л.
34. Tsukanov L. An ‘Elephant’ in the digital space: How does India operate in the cyberspace of the Middle East? // Trends. 29.09.2023. URL: https://trendsresearch.org/insight/an-elephant-in-the-digital-space-how-does-india-operate-in-the-cyberspace-of-the-middle-east/ / 0.9 п.л. (англ. язык).

[25] Деятельность Facebook признана экстремистской и запрещена в России.

35. Tsukanov L. Cyber factor in France Middle Eastern policy // Trends. 29.01.2024. URL: https://trendsresearch.org/research.php?id=1076 / 0.7 п.л. (англ. язык).