Мировая политика
Правильная ссылка на статью:
Ильина Е.В., Чипизубова П.А. — Цифровизация на Ближнем Востоке: угроза региональной безопасности или инструмент ее поддержания? // Мировая политика. – 2023. – № 3. DOI: 10.25136/2409-8671.2023.3.38743 EDN: XRNYRT URL: https://nbpublish.com/library_read_article.php?id=38743

Цифровизация на Ближнем Востоке: угроза региональной безопасности или инструмент ее поддержания?

Ильина Елизавета Владимировна

студент, кафедра мировых политических процессов, Московский государственный институт международных отношений (университет) МИД Российской Федерации (МГИМО)

119454, Россия, город Москва, г. Москва, ул. Пр. Вернадского, 76, корп. В

ilinaelizaveta2002@gmail.com

Чипизубова Полина Андреевна

студент, кафедра мировых политических процессов, Московский государственный институт международных отношений (университет) МИД Российской Федерации (МГИМО)

119454, Россия, город Москва, г. Москва, ул. Вернадского, 76, корп. В

chip-polina2002@mail.ru

Статья из рубрики "Вьвовы и угрозы международной безопасности"

DOI:

10.25136/2409-8671.2023.3.38743

EDN:

XRNYRT

Дата направления статьи в редакцию:

09-09-2022

Дата публикации:

19-09-2023

Аннотация: В качестве предмета данного исследования выступают основные угрозы и преимущества, связанные с цифровизацией в ближневосточном регионе на современном этапе. В основе работы лежит исследовательский вопрос, какая сторона влияния цифровизации – положительная или деструктивная – превалирует на Ближнем Востоке, и какие перспективы ожидают этот регион в цифровой сфере. Анализируются интересы ключевых региональных игроков в киберсфере (Саудовской Аравии, ОАЭ, Турции, Ирана и др., а также антисистемных негосударственных акторов), а также

региональные и национальные инициативы в данной отрасли, среди которых "Щит полуострова", "Видение-2030" и другие. Научная новизна исследования заключается в неклассическом подходе к проблемам безопасности на Ближнем Востоке, а именно через призму цифровой сферы с учетом ее комплексности и множественности ее акторов. Теоретическая база исследования строится на неолиберальном подходе к мировой политике, в частности, на концепции комплексной взаимозависимости, поскольку авторы опираются на постулат, что мирополитическая сфера находится в неразрывной связи с другими, а также складывается из множества разнородных акторов и связей между ними. С точки зрения изучения региональной интеграции на Ближнем Востоке доминирующим подходом является неофункционализм, разработанный Э. Хаасом, в частности, теория «перелива» («spillover»). В качестве методов исследования используются описание, изучение официальных документов и статистических данных, ситуационный анализ, сравнительный анализ, что позволило дать оценку ключевым угрозам и перспективам для региональной безопасности и их соотношению. Авторы приходят к выводу, что ключевую угрозу для региона представляют разобщенность интересов акторов и связанная с этим возможность обострения политических противоречий. Тем не менее, цифровизация предоставляет Ближнему Востоку такие преимущества, как углубление региональной интеграции и включение в международную кооперацию, рост мягкой силы и потенциал диверсификации экономики.

Ключевые слова:

Цифровизация, Ближний Восток, кибербезопасность, антисистемные акторы, региональная интеграция, Щит полуострова, ССАГПЗ,мягкая сила, Иран, Саудовская Аравия

Введение. В начале XXI века американский политолог ливанского происхождения Николас Талеб разработал ***теорию «черного лебедя»***. «Черный лебедь», в его понимании, это некое переломное для истории событие, которое является, с одной стороны, беспрецедентным и трансформативным, а с другой – вполне рационально объяснимым в ретроспективе. Все события, изначально вызвавшие широкий общественный резонанс, будь то Арабская весна, война в Йемене, или запуск ядерной программы Ирана, со временем настолько прочно укоренились в нашем восприятии мира и получили столько логических объяснений, что теперь они представляются нам чуть ли не единственным возможным исходом череды событий и процессов, предшествовавших им. Этот удивительный феномен Талеб объясняет когнитивными искажениями, присущими человеческому мышлению, однако в связи с этим он приходит к неутешительному выводу: сколько бы предпосылок не находилось в поле нашего зрения, появление очередного «черного лебедя» крайне трудно «просчитать», как и его последствия, зачастую складывающиеся в бесконечный косяк новых лебедей.

Данная концепция представляет большой аналитический интерес с точки зрения ближневосточного региона: во-первых, данный регион за последние пару десятилетий принял на себя столько «черных лебедей», сколько ни один другой, а во-вторых, Ближний Восток представляет собой сложное хитросплетение различных факторов, которое, с одной стороны, является источником внутренней нестабильности в регионе, а с другой, причиной его относительной автономности и невосприимчивости к внешнему влиянию, поэтому любой «черный лебедь» неизбежно приобретает на Ближнем Востоке два параллельных измерения.

В числе «черных лебедей» Талеб выделяет изобретение Интернета и последовавшую за ним повсеместную **цифровизацию**. Понятие цифровизации, которое, как считается, было введено в 1995 г. Николасом Негропонте [1], неоднозначно и до сих пор трактуется по-разному как политиками, так и учеными. Так, М.М. Гоббл из Брукингского Института определила цифровизацию как «процесс использования цифровых технологий и информации для трансформации экономических, социальных, политических и др. процессов» [2]. Исследовательница из СПбГУ А.Н. Сытник предложила следующее определение: «продолжающийся переход на цифровые технологии во всех сферах жизни общества и датафикация, т.е. накопление больших данных в целях оптимизации, изучения и прогнозирования экономической и политической деятельности и социальных процессов» [3]. Её коллега из СПбГЭУ В.А. Плотников трактует это явление как «процесс внедрения цифровых технологий генерации, обработки, передачи, хранения и визуализации данных в различные сферы человеческой деятельности» [4]. Учитывая основные аспекты данных дефиниций, мы предлагаем более узкое определение цифровизации с мирополитической точки зрения, которое представляет это явление не как целенаправленную деятельность определенных акторов, а как более стихийный процесс, зависящий от множества факторов: ***«процесс усиления роли цифровых технологий во внутри- и внешнеполитической жизни государств, оказывающий влияние на взаимодействие её участников»***.

Глобализация открыла ей двери даже в самые обособленные и консервативные уголки земного шара. Не остался в стороне и Ближний Восток, для которого цифровизация выступает одновременно и двигателем прогресса, и источником немыслимых ранее угроз. В основе нашего исследования лежит ***вопрос***, какая сторона влияния цифровизации – положительная или деструктивная – все-таки превалирует на Ближнем Востоке, и какие перспективы ожидают этот регион в цифровой сфере.

Несмотря на вышеприведенные рассуждения по поводу проблематичности политического прогнозирования выше, Талеб не утверждает о его бессмысленности. Напротив, согласно его концепции, прогноз будет иметь существенную значимость, если не высчитывать вероятность тех или иных сценариев, опираясь на мелочи, а лишь ограничивать область возможного, руководствуясь общими тенденциями и анализируя ситуацию комплексно, что мы и планируем сделать в нашей работе.

Цифровизация как элемент ближневосточной реальности. В последние годы цифровизация на Ближнем Востоке обрела невиданные масштабы: по итогам 2020 года многие страны региона в рейтинге цифровизации Harvard Business Review были отнесены либо в группу лидеров, либо перспективных стран [5]. Количество пользователей Интернета в ближневосточном регионе за последние пять лет выросло на 59%, что сделало его лидером по темпам прироста пользователей [6]. Страны региона также уже не первый год возглавляют рейтинги по проникновению соцсетей [7]. Активно идет «арабизация» мировой паутины: за 10 лет процент контента на арабском языке от всего контента в Интернете вырос более, чем на 2500%. Такая краткая статистическая справка наглядно показывает масштабы цифровизации на Ближнем Востоке и её влияния на жизнь региона.

Первые плоды этих процессов оказались разрушительными: с одной стороны, волны политически мотивированных кибератак в начале века, вызванных «интифадой Аль-Акса» и терактом 11 сентября 2001 г. [8], с другой –Арабская весна, одним из ключевых факторов которой стали информационно-коммуникативные технологии. Во время

Арабской весны Ближний Восток впервые столкнулся с тем, что сейчас называется **информационной войной**, с присущими ей манипуляциями общественным мнением, фейковыми новостями, эмоциональными мифами. С тех пор эти явления сопровождали буквально каждый кризис в регионе. Событием, которое придало цифровой безопасности на Ближнем Востоке глобальное мирополитическое измерение, стала кибератака вируса нового поколения Stuxnet (разработанного, согласно экспертизе, Израилем совместно с США), который не только нанес существенный ущерб иранской ядерной программе, но и продемонстрировал, насколько деструктивное воздействие может иметь кибероружие в масштабах целых государств.

Так сложилось, что Ближний Восток, будучи одним из самых конфликтных регионов мира, стал еще и своеобразной ареной для ожесточенного цифрового противостояния, в которое оказались вовлечены самые разнообразные акторы, от традиционных региональных стран-антагонистов в лице, например, Ирана и Израиля, а также внешних игроков, таких как США, до неклассических субъектов, таких как кибертеррористы или хакерские группировки. Новообразовавшееся цифровое измерение ближневосточной безопасности не только унаследовало уже тянущиеся десятилетиями конфликты, но и «обогатилось» новыми, еще крепче затянув узел противоречий.

Страны Ближнего Востока далёки от формирования консолидированной позиции по вопросам кибербезопасности. С 2017 г. активизировались взаимные обвинения ОАЭ, Саудовской Аравии, Катара, Египта и других арабских стран в кибератаках и компьютерном шпионаже. В связи с эскалацией цифровой конфронтации в регионе происходит постепенное наращивание наступательных кибервооружений [9]. По данным Global Security Index, страны региона значительно рознятся по уровню киберзащищенности: лидеры Саудовская Аравия и ОАЭ заняли 2-е место 5-е места (наравне с Россией, между прочим) соответственно, на 20-х строчках расположились Египет, Оман, Катар, а такие страны, как Сирия и Йемен и вовсе замыкают рейтинг [10]. Поэтому стабильность в сфере кибербезопасности на Ближнем Востоке напрямую зависит от ключевых акторов, баланс интересов которых является единственным ключом к устойчивой архитектуре региональной цифровой безопасности, а его нарушение – верным путем к краху этой архитектуры. Исходя из этого, предлагаем перейти к детальному анализу крупнейших игроков на ближневосточной киберарене.

На региональном уровне выделяется ключевая диада киберпротивостояния Саудовской Аравии и Ирана, которые продвигают диаметрально противоположные видения архитектуры кибербезопасности в регионе, и это спровоцировало формирование своеобразных **блоков безопасности** вокруг данных полюсов. В арсенале Саудовской Аравии поддержка наиболее влиятельных стран региона, таких как ОАЭ и Израиль, а также внешних игроков преимущественно в лице США, тогда как на иранской стороне, помимо некоторых внерегиональных акторов, косвенно выступают множественные неклассические акторы цифровой безопасности. Рассмотрим сложившуюся систему акторов.

Саудовская Аравия. Саудовская Аравия является признанным лидером арабских стран и исламского мира в области кибербезопасности, менее чем за десять лет полностью трансформировав государственную политику в цифровой сфере и вырвавшись с 20-х позиций на вторую. Помимо совершенствования киберинститутов на национальном уровне, Саудовская Аравия взяла уверенный курс на международную кооперацию в данной области в рамках таких площадок, как МСЭ, специализированные группы ООН, ЛАГ, что позволило ей стать полноправным участником глобальных цифровых процессов,

но в то же время поставило в ситуацию взаимозависимости с развитыми странами, по большей степени с США. Опыт международного сотрудничества во многом был использован Саудовской Аравией для выстраивания собственного блока коллективной кибербезопасности под своим началом на Ближнем Востоке, который формируется в рамках Совета сотрудничества арабских государств Персидского залива (ССАГПЗ)[11]. В основе этого условного «блока» лежит скорее западное понимание цифровой безопасности, которое относится скорее к техническим аспектам киберугроз, нежели к их социально-политическим последствиям. Такое толкование информационной безопасности становится объектом существенных разногласий между странами ССАГПЗ и другими государствами региона. Однако успехи Королевства в цифровизации тем не менее позволили ему стать своеобразным региональным центром притяжения и привлечь таких союзников по цифровой проблематике, как ОАЭ, Кувейт, Бахрейн.

Значительную роль для Саудовской Аравии цифровой фактор сыграл в противостоянии с Йеменом. В 2015 г., в связи с вмешательством Королевства во внутренний конфликт, в Йемене резко радикализовались антисаудовские настроения, что вылилось в том числе в череду кибератак хакерской группировки, которая называла себя Йеменской киберармией. Среди преступлений Йеменской киберармии были масштабная кража данных у МИДа Саудовской Аравии, атака на государственные СМИ, передача государственных документов WikiLeaks [12]. Несмотря на то, что активность группировки прекратилась в тот же год, она спровоцировала множество дипломатических скандалов, в том числе по причине того, что ключевые заказчики и участники проекта так и не были идентифицированы; а также она стала катализатором экстренного укрепления системы национальной кибербезопасности Саудовской Аравии.

Израиль. Израиль, хотя и не является идейным единомышленником Саудовской Аравии, в цифровой сфере довольно часто выступает в роли ее неожиданного союзника по принципу общего покровителя – США – и общего противника – Ирана. На плодотворное развитие сотрудничества указывает также подписание «Авраамских соглашений» 2020 г., в которых арабские страны, в частности союзники Саудовской Аравии ОАЭ и Бахрейн, заявляют о нормализации отношений с Израилем, в том числе и в киберсфере. Также страны ССАГПЗ во многом зависимы от Израиля в цифровом секторе: у арабских стран заключены дорогостоящие контракты с известными израильскими киберкомпаниями, а некоторые госведомства работают на особом израильском софте [13].

В целом система национальной кибербезопасности Израиля крайне налажена и отточена, ее характерной чертой является огромное количество киберподразделений, интегрированных в государственные органы, которые создаются специально под различные проекты, и членов которых набирают в том числе из хакерских группировок [14]. Такие легальные хакерские подразделения получили название «**белые шляпы**».

Интересен факт израильского сотрудничества с Катаром в условиях их взаимного непризнания. **Катар** в целом играет довольно противоречивую роль в региональной кибербезопасности: с одной стороны, Катар является союзником Саудовской Аравии по ССАГПЗ и в поле публичной политики ведет активный пропалестинский курс, с другой стороны, Катар активно сотрудничает с Израилем в области цифровой безопасности, и параллельно выступает важным экономическим партнером Ирана – стратегического противника всех вышеперечисленных. Но что касается цифровой кооперации Израиля и Катара, Катар использовал модель, подобную аутсорсингу [15]. В первой половине 2010-х гг., когда Катар еще не обладал собственной развитой системой защиты от киберугроз, страна объявляла тендеры на укрепление цифровой безопасности, и большую их часть

заняли израильские компании (в частности, ClearSky Cyber Security). Израильские «белые шляпы» также неоднократно принимали участие в отражении кибератак на Катар: например, при атаке Ирана на нефтегазовые объекты с использованием вируса Shamoon в 2012 г. Со временем Катар наладил национальную систему киберзащиты, при этом сотрудничество с Израилем в данной сфере по инерции сохранилось, однако так и не выйдя на публичный уровень по политическим причинам: в официальных документах Катара Израиль выступает как «консультант» или «подрядчик».

Турция. Турция является еще одним претендентом на региональное лидерство в киберсфере [13], что делает ее скорее оппонентом для стран ССАГПЗ в силу совпадения зон интересов. Турция крайне серьезно подходит к вопросам цифровой безопасности: с 2012 г. в стране функционирует соответствующее ведомство, под началом которого находятся не менее 13 тыс. служащих «Турецкой киберармии» Türk Siber Ordusu, цифровая деятельность подкреплена национальными кибердоктринами [16]. Страна во многом перенимает опыт западных партнеров, нанимая зарубежных консультантов и принимая участие в международных киберучениях. В последнее время Турция активно наращивает свое наступательное кибервооружение и расширяет сотрудничество с хакерским сообществом, что провоцирует опасения Саудовской Аравии и ее сателлитов. Тем не менее, Турция вовсе не настроена на противостояние со странами Персидского Залива, скорее наоборот – на сотрудничество в интересах своих киберкомпаний. Во-первых, надежным союзником Турции также является Катар, и столкновение между Турцией и ССАГПЗ сорвало бы процесс нормализации отношений между ССАГПЗ и Катаром после дипломатического кризиса 2017 г. Во-вторых, страны Персидского залива все же не представляют для Турции угрозы, в отличие, например, от Египта или хакерских подразделений «Движения Гюлена» и «Рабочей партии Курдистана» [16].

Египет. С точки зрения кибер-мощи, Египет в целом выступает на равных со странами Персидского залива, и потому может позволить себе продвигать собственные интересы, зачастую идущие вразрез с интересами аравийских монархий, тем не менее, точек соприкосновения достаточно. В сфере кибербезопасности власти Египта больше заинтересованы во внутренней стабильности, нежели в региональных перипетиях, поэтому Египет большое внимание уделяет контролю СМИ, телевидения и национального Интернета, а в конфронтации с другими державами не заинтересован [17].

Иран. Иран – единственный игрок Ближнего Востока, политика которого может представлять глобальную угрозу, в связи с этим он также является самой частотной в регионе целью кибератак, принимая на себя 10% от всех кибератак в мире [18]. В 2010 г. Иран подвергся уже упомянутой разрушительной атаке Stuxnet, которая и стала катализатором активного развития национальной системы кибербезопасности в условиях учащающихся атак со стороны США и Израиля. При этом в цифровой сфере Иран сталкивается не только с внешними, но и с внутренними угрозами в связи со сложной внутриполитической обстановкой. В международных рейтингах кибербезопасности Иран не входит в число лидеров, однако это мало отражает реальную ситуацию, т.к. рейтинги не учитывают, к примеру, потенциал наступательного кибервооружения и устойчивые связи с хакерскими группировками. Западные исследователи относят Иран к группе из 6 стран с наиболее развитыми цифровыми компетенциями, наряду с США, РФ, Китаем, Израилем, Великобританией [19].

В начале 2000-х гг. кибератаки Ирана представляли собой скорее плохо скоординированные декларативные действия отдельных группировок, тогда как сейчас

проводятся тщательно проработанные масштабные операции по кибершпионажу, включающие детальный сбор данных с сайтов и внедрение вредоносных программ, причем с использованием ПК и личных аккаунтов лиц, аффилированных с Корпусом стражей исламской революции (КСИР). На сегодняшний день кибербезопасность Ирана обеспечивают преимущественно КСИР и Министерство разведки, регулируя соответствующие спецподразделения, сформированы также кибергруппы в составе сил спецназначения и военизированного ополчения.

Приоритетными целями иранских кибератак являются преимущественно США (и их западные союзники), Израиль и аравийский монархии. Однако в последнее время наблюдается тенденция снижения числа кибернападений и перехода преимущественно к разведке, а также переноса внимания с внешних противников на внутреннюю оппозицию, в связи с чем многие эксперты утверждают, что Иран постепенно уходит с позиций «глобальной киберугрозы».

Что касается союзников Ирана в сфере кибербезопасности, на официальном уровне их скорее нет. Некоторые эксперты считают таковыми Ирак, Ливан, Йемен, однако это сотрудничество не закреплено на государственном уровне, и уровень развития этих стран не позволяет им выйти на уровень полноценного союзника, скорее сателлита. Аравийские монархии, к примеру, заявляют, что Йеменская киберармия на самом деле была проектом Ирана, однако из-за специфики сферы проверить это очень сложно, и вряд ли когда-либо это будет установлено наверняка. Есть также категория «сочувствующих» Ирану стран, таких как Катар, который стремится придерживаться нейтралитета и не вступает в конфронтацию с Ираном, в частности, Катар отказался предоставлять Израилю данные о деятельности иранской прокси-группировки «Ливанский кедр» [15]. Но основной поддержкой Ирана в регионе выступают некоторые антисистемные хакерские группировки, которые связаны с негосударственными акторами, в том числе с различными террористическими группировками, такими как ИГИЛ* и Хезболла.

Антисистемные акторы. На ближневосточной кибераренe негосударственные акторы укоренились так же прочно, как и государственные. К сожалению, большинство из них оказывают деструктивное влияние на региональную безопасность, так как связаны с террористическими ячейками. Одними из первых в цифровом пространстве (2006-2007) проявили себя киберджихадистские группы «Аль-Каиды*», которых насчитывается более десяти, однако их деятельность ограничивалась в основном пропагандой и дефейсментом. Более решительной группировкой является «Объединенный киберхалифат ИГИЛ*», который своим возникновением обязан молодому британцу Джунаиду Хуссейну, известному благодаря взломам личных аккаунтов Цукерберга и Тони Блэра. Данная группировка совершила ряд атак на аккаунты госведомств и СМИ, однако сейчас специализируется на шпионаже на объектах энергетической инфраструктуры в странах Запада и угрожает глобальной кибератакой. К этой же группе относится уже упомянутый «Ливанский кедр», известный своей масштабной атакой на интернет-провайдеров и операторов связи в странах Запада, арабские страны, Израиль.

Совершенно особую роль играют акторы, которые находятся где-то между государственными и негосударственными, и ярким примером таких акторов является проект «**Кибермухи**». «Кибермух» сложно отнести к полноценным кибергруппировкам, они представляют собой скорее совокупность всех лояльных Саудовской Аравии хакеров, включая одиночных. У них нет четкой структуры или общего лидера, но долгое время их неформальным лидером считался первый советник наследного принца

Саудовской Аравии аль-Кахтани. Тем не менее, «Кибермухи» не относятся к аравийским «белым шляпам». С одной стороны, они, очевидно, сотрудничают с правительством, что отчетливо проявилось в ходе дипломатического кризиса с Катаром и конфликта с Йеменом. С другой стороны, координация, по-видимому, недостаточная: в 2021 г. «Кибермухи» атаковали министерство транспорта Ирана вскоре после заключения соглашений между Саудовской Аравией с Ираном, что значительно подорвало авторитет данных соглашений.

Разобщенность «Кибермух – это только одна из проблем их интеграции в госструктуру. Помимо этого, большую роль играет внутренний фактор, а именно общественное мнение: хакерство воспринимается многими мусульманами как серьезный грех, а Саудовская Аравия не может отказаться от своих претензий на лидерство в исламском мире. Также, как уже отмечалось, Саудовская Аравия сделала серьезную ставку на международную кооперацию в киберсфере, а открытое включение хакерской группировки в государственный штат могло бы пошатнуть ее международный имидж.

Интеграция как стабилизирующий фактор цифровизации на Ближнем Востоке. Внутренние и внешние угрозы вынуждают государства Ближнего Востока консолидировать свои усилия в целях эффективного обеспечения цифровой безопасности, что ведет к интенсификации регионального сотрудничества. Так называемый «Щит полуострова», созданный государствами-членами ССАГПЗ еще в далеком 1984 г. для сдерживания и реагирования на военную агрессию, со временем стал приобретать очертания щита информационного, призванного обеспечить киберзащиту региона [20]. В ходе тесного сотрудничества в области ИКТ странам ССАГПЗ удалось разработать устойчивую систему мер для противостояния киберугрозам, а построение стратегии коллективной кибербезопасности является одним из основных элементов интеграционных процессов в регионе.

Кроме того, цифровизация ведет к сглаживанию традиционных политических противоречий. В настоящий момент страны ССАГПЗ активно сотрудничают с Израилем по вопросам обеспечения кибербезопасности. По понятным причинам это сотрудничество не получает широкой огласки, однако оно является крайне плодотворным и имеет широкие перспективы. ОАЭ с начала 2000-х гг. ориентировались на ряд израильских проектов для построения собственной системы кибербезопасности, а приблизительно с 2008 г. ведется комплексное технологическое сотрудничество. Так, в 20082015 гг. модернизация систем наблюдения на важнейших нефтегазовых объектах ОАЭ фактически проходила под руководством израильской фирмы Logic Industries, хотя официальным подрядчиком являлась швейцарская корпорация AGT International. Кроме того, государственные органы ОАЭ взаимодействуют с профильными органами Израиля [21].

Стоит отметить и другие государства, сотрудничающие с Израилем в рамках вопросов информационных технологий и кибербезопасности. Саудовская Аравия поддерживает контакт с компанией IntuView, использующей технологии искусственного интеллекта для мониторинга закрытых каналов в социальных сетях в целях выявления террористических угроз. У Катара, как уже упоминалось, налажены взаимосвязи с ClearSky Cyber Security, которая оказывает услуги в сфере укрепления информационной защиты национальной критической инфраструктуры.

Помимо вышеуказанных стран ССАГПЗ сотрудничество с Израилем в информационной сфере осуществляют и Оман с Бахрейном, однако для них на первый план выходят вопросы не столько кибербезопасности, сколько цифровизации важнейших областей:

финансов, здравоохранения и образования. Так, в 2005 г. в Бахрейне началось внедрение программы по цифровизации высших и средних профессиональных учебных заведений, направленной на модернизацию методов обучения и формирование у учащихся знаний о современных информационных технологиях [22]. Для реализации проекта в Бахрейне была широко развернута электронная образовательная платформа EduWave от иорданской компании Integrated Technology Group, а осуществление программы и обучение пользователей проходило при поддержке израильских компьютерных экспертов.

В Омане, который старается балансировать между Ираном и Израилем [23] и поэтому в отличие от других стран-членов ССАГПЗ не готов к полноценной нормализации отношений с еврейским государством, при помощи израильских специалистов была разработана инициатива по внедрению и развитию интернет-банкинга, направленная на ускорение процесса регистрации клиентов и упрощение работы банковской системы в целом. Активное участие в этом процессе принимает и компания NNTC из ОАЭ, которая занимается разработками программного обеспечения [24].

Диверсификация экономики. Важным элементом развития коллективной кибербезопасности стало принятие странами ССАГПЗ во второй половине 2010-х гг. программ «Видение-2030», которые представляют собой долгосрочные стратегии по отходу от сырьевой составляющей национальных экономик и их диверсификации. Цифровизация всех сфер жизни государств при этом рассматривается в качестве главного драйвера развития региона. Несмотря на то, что большинство стран региона признают необходимость цифровой модернизации экономики, далеко не все из них успешно реализуют программу. Пожалуй, лучшим примером в этом отношении является Саудовская Аравия.

О внедрении программы «Saudi Vision 2030» [25] было объявлено в 2016 г., когда наблюдалось резкое снижение цен на нефть. Саудовская Аравия, как и многие страны Ближнего Востока, сильно зависима от добычи нефти и природного газа, поэтому правительству Королевства было необходимо принять экстренные меры для выхода из экономического кризиса, из-за которого страна погрязла в долгах, наблюдались рост безработицы и значительное снижение уровня жизни. Программа включает в себя ряд экономических реформ, направленных на снижение зависимости Саудовской Аравии от экспорта нефти и газа и на развитие других отраслей экономики.

Саудовская Аравия является одним из наиболее развитых в цифровом плане государств Ближнего Востока. На данный момент Саудовская Аравия добилась целого ряда успехов в рамках реализации программы «Видение-2030»: была создана программа электронного правительства Yesser, в 2019 г. была начата реализация Национальной стратегии развития Интернета вещей, в Саудовской Аравии регулярно повышается доверие граждан к онлайн-транзакциям и, как следствие, растет процент электронных платежей [26] (по состоянию на 2019 г. они составляли 36,2% всех платежей, что превысило целевой показатель программы) и происходит активное развитие электронной торговли (по состоянию на 2020 г. Королевство заняло 5 место среди развивающихся стран по этому показателю) [27].

Активно проходит цифровизация и в важнейших социальных сферах: здравоохранении и образовании. Большое количество граждан Саудовской Аравии использует для получения медицинских услуг электронную платформу Mawid, которая позволила Саудовской Аравии в 2020 г. сэкономить более 200 млн долларов. Электронная

образовательная платформа Noor объединяет все учебные заведения Королевства и активно используется учащимися по всей стране. Развивается в цифровом отношении и туристическая сфера: через электронную платформу туристических виз их было выдано более 250 тыс. Внедряют цифровые технологии даже в процесс организации и проведения хаджа и умры, что является спецификой цифровизации Саудовской Аравии [26].

Вероятность полной диверсификации экономики Саудовской Аравии к 2030 г. маловероятна, однако у страны есть огромный потенциал, и если руководство страны грамотно им воспользуется, Саудовская Аравия сможет стать одним из наиболее развитых в сфере цифровизации и кибербезопасности государств не только в регионе, но и во всем мире.

Как было сказано ранее, аналогичные программы были запущены и в других странах региона (ОАЭ, Бахрейн, Кувейт); во многих странах Ближнего Востока были приняты Национальные стратегии по цифровому развитию, разработаны проекты электронного правительства. Интересен тот факт, что в официальных документах по цифровизации почти каждая страна ставит целью выход на ведущие позиции в отношении кибербезопасности и уровню цифровизации в регионе [28].

Каково практическое влияние цифровой трансформации экономик стран Ближнего Востока на их развитие? Во-первых, наблюдается экономический рост, который обеспечивается за счет диверсификации экономики; во-вторых, благодаря современным технологиям страны Ближнего Востока становятся местами притяжения инвестиций; в-третьих, возникает большое количество рабочих мест, поскольку странам необходимы специалисты в сфере ИКТ (во многих из них реализуются различные проекты по цифровому образованию среди школьников и студентов).

Мягкая сила. Многие государства Ближнего Востока стремятся использовать цифровизацию в качестве мягкой силы, тем самым продвигая свои интересы на международной арене и оказывая влияние на мировые политические процессы. Для этого используется публичная дипломатия, которая, будучи реализуемой в интернет-пространстве, становится дипломатией цифровой, а социальные сети – ее главным инструментом.

В странах Ближнего Востока в целом растет уровень заинтересованности граждан в социальных сетях и пользовании интернетом: по данным на январь 2021 г. ОАЭ заняли первое место в мире по количеству людей, использующих интернет (99% населения), 8 место заняла Саудовская Аравия (95,7%), 23 строчку занял Израиль (88%) [29].

Одной из наиболее преуспевших в использовании цифровизации в качестве мягкой силы стран являются ОАЭ [30]. Во внутренней цифровой политике ОАЭ стремится к созданию умного, «безбумажного» правительства. В декабре 2021 г. правительство Дубая стало первым в мире, которое ввело полностью безбумажный документооборот [31]. Это важное решение уже позволило сэкономить 336 млн бумажных листов, что составляет около 14 млн часов человеческого труда и 353,8 млн долларов [32].

Что касается внешней сферы, в ОАЭ набирает популярность дипломатия социальных сетей: власти используют интернет-пространство для продвижения своих идей и национальных интересов, укрепления позиций страны в системе международных отношений, поддержания ее имиджа. Так, например, в 2017 г. премьер-министр ОАЭ стал

самым цитируемым политиком в Twitter [33], а его аккаунт насчитывает более 9 млн подписчиков (11-е место среди мировых лидеров). Кроме того, в ОАЭ есть специальные государственные органы, которые занимаются координацией деятельности внешнеполитических учреждений в интернете, например, Office of Public and Cultural Diplomacy. Все это продвигает национальный бренд ОАЭ (в 2021 г. ОАЭ заняли 17 место в рейтинге национальных брендов; на 2 строчки ниже расположилась Саудовская Аравия) [34].

Цифровизация – угроза региональной безопасности или инструмент ее поддержания? Какая сторона влияния «черного лебедя» в лице цифровизации окажется для Ближнего Востока превалирующей?

1). Значительную угрозу для Ближнего Востока в сфере кибербезопасности представляет сама множественность и существенная разобщенность интересов ее акторов. Региональные державы борются друг с другом за лидерство, что, в свою очередь, может привести к гонке кибервооружений и углублению пропасти в развитии между наиболее и наименее развитыми региональными державами. Параллельно действуют антисистемные хакерские группировки и другие неклассические акторы, интересы и структуру которых зачастую крайне трудно идентифицировать, и которые при этом способны значительно подорвать сложившийся баланс сил.

С другой стороны, конкуренция внутри региона в сфере кибербезопасности и цифровизации способствует общерегиональному развитию в данной сфере. Более того, несмотря на расхождения в национальных интересах, страны региона охотно идут на интеграцию в киберсфере. Активное сотрудничество, в свою очередь, повышает уровень их защищенности от внерегиональных угроз, а также ведет к стабилизации внутриполитической ситуации за счет цифровизации социально-ориентированных отраслей.

2). В линии регионального киберпротивостояния часто оказываются вовлечены внешние игроки, такие как США, развитые страны запада, Китай, Россия, КНДР, что создает угрозу превращения Ближнего Востока в арену кибер-проксиконфликтов. В то же время участие стран региона в специализированных международных организациях, а также посредничество американских и европейских цифровых компаний в отношениях стран ССАГПЗ с Израилем может послужить фундаментом большей интеграции стран Ближнего Востока в международное сообщество.

2). Учитывая нестабильную политическую ситуацию в регионе, киберпротиворечия в теории могут обострить уже существующие политические конфликты и стать поводом для новых. С другой стороны, уже сейчас наблюдается некий эффект «перетекания» («spillover») интеграции стран Ближнего Востока из информационной сферы в экономическую, культурную, и, главное, в политическую. Примеры Саудовской Аравии-Израиля, Катара-Ирана и др. показывают, что страны ищут пути в обход своих традиционных политических конфликтов для извлечения выгоды из сотрудничества в других сферах, в частности, в цифровой, что в значительной степени способствует снижению конфликтогенного потенциала в регионе.

3). Что касается изменения региональной позиции Ирана в киберсфере, согласно ряду прогнозов, его отход от роли главного «злодея» может расколоть региональное сообщество, так как, утратив сплочающую угрозу, они начнут искать ее друг в друге.

Однако эта же тенденция может, напротив, привести к построению обновленной

архитектуры кибербезопасности не по принципу общего противника, который характеризуется неустойчивостью, а на основе взаимных интересов стран Ближнего Востока.

4). Цифровизация является для Ближнего Востока источником качественно новых преимуществ, грамотное использование которых способно существенно укрепить международные позиции стран региона. Во-первых, цифровая отрасль – перспективная и вполне реализуемая возможность диверсификации экономики и спасения от «нефтяной иглы» для государств-экспортеров нефти, которых в регионе большинство. Кроме того, цифровая трансформация экономики может стать основой для внедрения стран Ближнего Востока в новые глобальные производственные цепочки.

Вторым ключевым преимуществом выступает использование цифровизации и цифровой дипломатии в качестве мягкой силы. С ее помощью страны Ближнего Востока продвигают свои интересы, формируют положительный национальный имидж, укрепляют позиции не только в цифровом, но и в политическом пространстве. Поскольку цифровизация на Ближнем Востоке с каждым годом только набирает обороты, а интернет-пользователей становится все больше, можно предположить, что уже в обозримом будущем регион станет одним из главных мировых цифровых центров, а его государства начнут оказывать куда большее влияние на мировое сообщество.

Ответ на вопрос, чем обернется цифровизация на Ближнем Востоке, неоднозначен, иначе бы мы изначально не включили цифровизацию в число «черных лебедей». Мы представили несколько возможных сценариев развития событий, вероятность реализации каждого из которых зависит от целого разброса случайных факторов, что лишает смысла более точные прогнозы. Нам представляется, однако, что на сегодняшний день позитивные аспекты все же превалируют, поскольку они не только создают способы нивелировать традиционные противоречия, давно зашедшие в тупик, но и предоставляют дополнительные импульсы к развитию. В любом случае, Ближний Восток, судя по всему, является для «черных лебедей» естественной средой обитания, что дает нам основания полагать, что и этот уж точно не станет фатальным.

* движения признаны террористическими и запрещены в РФ

Библиография

1. Коньков А.Е. Новые информационные технологии и международные отношения // Вестник Санкт-Петербургского университета. Международные отношения. 2020. Т. 3. Вып. 1. С. 47-68.
2. Semantic Scholar. [Электронный ресурс]. URL: https://www.semanticscholar.org/paper/Digital-Strategy-and-Digital-Transformation-Gobble/0f9d211b9ebab742b348a8800d04ab44b57353dd (дата обращения: 10.03.2022).
3. disserCat. [Электронный ресурс]. URL: https://www.dissercat.com/content/tsifrovizatsiya-i-bolshie-dannye-v-mezhdunarodnykh-otnosheniyakh-teoreticheskie-metodologich (дата обращения: 10.03.2022).
4. Плотников В.А. Цифровизация производства: теоретическая сущность и перспективы развития в российской экономике // Известия Санкт-Петербургского государственного экономического университета. 2018. № 4 (112). С. 16-24.
5. Самые цифровые страны мира: рейтинг 2020 года // Harvard Business Review. 2020. [Электронный ресурс]. URL: https://hbr-russia.ru/innovatsii/trendy/853688/ (дата

обращения: 11.03.2022).

6. Global Cybersecurity Index 2020 // ITU Publications. 2022. [Электронный ресурс]. URL: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E/ (дата обращения: 11.03.2022).
7. Вся статистика интернета на 2019 год – в мире и в России // WebCanape. 2019. [Электронный ресурс]. URL: https://www.web-canape.ru/business/vsya-statistika-interneta-na-2019-god-v-mire-i-v-rossii/ (дата обращения: 11.03.2022).
8. Валиахметова Г.Н. Исламский мир в условиях цифровых угроз XXI века // MINBAR. Islamic studies. 2019. Т. 12. № 1. С. 95-110.
9. How Prepared is Saudi Arabia for a Cyber War? // Institute for National Security Studies. 2019. [Электронный ресурс]. URL: https://www.inss.org.il/publication/how-prepared-is-saudi-arabia-for-a-cyber-war/ (дата обращения: 11.03.2022).
10. National cyber security index. [Электронный ресурс]. URL: https://ncsi.ega.ee/compare/ (дата обращения: 11.03.2022).
11. Цуканов Л.В. Система национальной кибербезопасности Саудовской Аравии: специфика и риски развития // Вестник Кемеровского государственного университета. Серия: политические, социологические и экономические науки. 2021. Т. 6. № 4. С. 435-443.
12. Цуканов Л.В. Йеменская киберармия: раунд второй? // Российский Совет по международным делам. 16.11.2021. [Электронный ресурс]. URL: https://russiancouncil.ru/analytics-and-comments/columns/middle-east/yemenskaya-kiberarmiya-raund-vtoroy/ (дата обращения: 12.03.2022).
13. Цуканов Л.В. Цифровые химеры Персидского залива: кто займет место Ирана? // Российский Совет по международным делам. 22.02.2022. [Электронный ресурс]. URL: https://clck.ru/eJdYR (дата обращения: 12.03.2022).
14. Кибербезопасность по-израильски // Независимое военное обозрение. 2019. [Электронный ресурс]. URL: https://nvo.ng.ru/armament/2019-09-27/1_1063_israel.html (дата обращения: 12.03.2022).
15. Цуканов Л.В. Сотрудничество Израиля и Катара в сфере кибербезопасности // Теории и проблемы политических исследований. 2021. Т. 10. № 5А. С. 28-36.
16. Турецкая киберармия: эра электронных янычаров // ПИР-Центр. 2020. [Электронный ресурс]. URL: http://www.pircenter.org/blog/view/id/426 (дата обращения: 12.03.2022).
17. Кутукова Е.А. Информационная политика Арабской Республики Египет // Век информации. 2018. [Электронный ресурс]. URL: https://clck.ru/eJMPH (дата обращения: 14.03.2022).
18. Кильченко В.С. Политика Исламской Республики Иран в сфере информационной безопасности // Сборник XIII Международной научно-практической конференции студентов, магистрантов, аспирантов, соискателей. Саратовский национальный исследовательский государственный университет имени Н.Г. Чернышевского. 2020. С. 91-93.
19. Хетагуров А.А. Кибермощь Ирана. Киберстражи Исламской Революции // Российский Совет по международным делам. 2019. [Электронный ресурс]. URL: https://russiancouncil.ru/cyberiran#rec93669097 (дата обращения: 14.03.2022).
20. Цуканов Л.В. Силы безопасности ССАГПЗ: цифровое измерение // Российский Совет по международным делам. 28.07.2021. [Электронный ресурс]. URL: https://russiancouncil.ru/analytics-and-comments/columns/middle-east/sily-bezopasnosti-ssagpz-tsifrovoe-izmerenie/ (дата обращения: 17.03.2022).

21. Цуканов Л.В. Страны ССАГПЗ и Израиль: да будет «цифровая солидарность»? // Российский Совет по международным делам. 30.09.2021. [Электронный ресурс]. URL: https://russiancouncil.ru/analytics-and-comments/analytics/strany-ssagpz-i-izrail-da-budet-tsifrovaya-solidarnost/ (дата обращения: 17.03.2022).
22. King Hamad launches EduWave for Future Schools // ITG Group. 2005. [Электронный ресурс]. URL: https://www.itgsolutions.com/king-hamad-launches-eduwave-for-future-schools/ (дата обращения: 17.03.2022).
23. Oman plays it safe on Israel // Middle East Institute. 2020. [Электронный ресурс]. URL: https://www.mei.edu/publications/oman-plays-it-safe-israel (дата обращения: 17.03.2022).
24. Oman Arab Bank использует технологии NNTC и Smart Engines для дистанционного открытия счетов // CNews. 2021. [Электронный ресурс]. URL: https://www.cnews.ru/news/line/2021-02-10_oman_arab_bank_ispolzuet_tehnologii (дата обращения: 17.03.2022).
25. Vision 2030. [Электронный ресурс]. URL: https://www.vision2030.gov.sa/ (дата обращения: 18.03.2022).
26. Рогожин А.А. ИКТ как направление диверсификации экономики Саудовской Аравии // Контуры глобальных трансформаций: политика, экономика, право. 2021. Т. 14. № 4. С. 122-141.
27. The UNCTAD B2C E-Commerce Index 2020: Spotlight on Latin America and the Caribbean // United Nations Conference on Trade and Development. 2021. [Электронный ресурс]. URL: https://unctad.org/system/files/official-document/tn_unctad_ict4d17_en.pdf (дата обращения: 18.03.2022).
28. Коровкин В.В. Национальные программы цифровой экономики стран Ближнего Востока // ARS ADMINISTRANDI. Искусство управления. 2019. Т. 11. № 1. С. 151-175.
29. Digital 2021: Global Overview Report // DataReportal. 2021. [Электронный ресурс]. URL: https://datareportal.com/reports/digital-2021-global-overview-report (дата обращения: 18.03.2022).
30. Цифровая дипломатия Объединенных Арабских Эмиратов // Центр стратегических оценок и прогнозов. 2019. [Электронный ресурс]. URL: http://csef.ru/ru/nauka-i-obshchestvo/445/czifrovaya-diplomatiya-obedinennyh-arabskih-emiratov-9048 (дата обращения: 19.03.2022).
31. Власти Дубая отказались от бумажного делопроизводства // ТАСС. 12.12.2021. [Электронный ресурс]. URL: https://tass.ru/obschestvo/13177849 (дата обращения: 19.03.2022).
32. Правительство Дубая стало полностью безбумажным // Русские Эмираты. 2021. [Электронный ресурс]. URL: https://russianemirates.com/news/uae-news/pravitel-stvo-dubaya-stalo-polnost-yu-bezbumazhnym/ (дата обращения: 19.03.2022).
33. Премьер-министр ОАЭ стал самым цитируемым политиком в сети Twitter // Русские Эмираты. 2017. [Электронный ресурс]. URL: https://russianemirates.com/news/uae-news/prem-yer-ministr-oae-stal-samym-tsitiruyemym-politikom-v-seti-twitter/ (дата обращения: 19.03.2022).
34. Nation Brands 2021. The annual report on the most valuable and strongest nation brands // Brand Finance. 2021. [Электронный ресурс]. URL: https://brandirectory.com/download-report/brand-finance-nation-brands-2021-preview.pdf (дата обращения: 19.03.2022).

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

Предметом рецензируемого исследования стал процесс цифровизации на Ближнем Востоке, а также те опасности и угрозы, которые порождаются этим процессом. В последние годы тема цифровизации современной политики и государственного управления привлекает всё более пристальное внимание исследователей: повсеместно внедряемые в процессы управления новые диджитал-технологии вызывают большой интерес специалистов и экспертов, результатом чего стал бурный рост научных и публицистических работ на эту тему. Поэтому практическая актуальность выбранной автором статьи темы исследования не вызывает ни малейших сомнений. Особую теоретическую значимость этой теме придаёт характерная для всякого нового и малоисследованного явления неоднозначность и размытость его концептуальных описаний, а также отсутствие парадигматического консенсуса в отношении методологического инструментария и терминологического аппарата. Тем любопытнее представляется предложенный автором подход, связывающий два относительно новых концепта – «чёрных лебедей» и «цифровизации» – для анализа ближневосточных реалий. К сожалению, определив концептуальную рамку своего исследования, автор ничего не говорит об использованном методологическом инструментарии. Из контекста можно понять, что в процессе исследования помимо общенаучных аналитических методов применялись элементы системного и институционального подходов, метод case study, а также вторичный анализ статистических данных. Такой методологический ход позволил автору получить результаты, обладающие признаками научной новизны. Прежде всего, научный интерес представляет попытка автора применить концептуальный аппарат теорий «чёрных лебедей» и «цифровизации» в анализе эмпирических данных ближневосточных государств – Саудовской Аравии, Израиля, Катара, Турции и др. В результате удалось выявить не только положительные последствия цифровизации (которые, в основном, и фиксируются в многочисленных исследованиях, посвящённых данной теме), но и те порождаемые ею эффекты, которые могут сыграть роль «чёрных лебедей» в политике исследованных государств. Любопытен также вывод о перспективах использования цифровизации в качестве одной из технологий «soft power» («мягкой силы», «мягкой власти»). Наконец, определённый теоретический интерес представляет предложенное автором «микрополитическое» определение феномена цифровизации, связывающее данный процесс не только с «большой» политикой (как внешней, так и внутренней) государств, но и с микровзаимодействиями политических акторов. В структурном плане статья также производит положительное впечатление: логика изложения достаточно последовательна, а структурные элементы рубрицированы. Во «Введении» ставятся задачи и определяется концептуальный дизайн исследования. В первом содержательном разделе «Цифровизация как элемент ближневосточной реальности» описываются основные направления процесса цифровизации в исследуемом регионе, которые затем конкретизируются на конкретных страновых кейсах. Далее рассматриваются деструктивные и стабилизирующие факторы региональной безопасности: деятельность антисистемных акторов, интеграционные процессы, диверсификация экономики, инструменты мягкой силы. В заключительном разделе «Цифровизация – угроза региональной безопасности или инструмент её поддержания?» резюмируются итоги проведённого исследования и намечаются перспективы дальнейших исследований этой темы. По стилю рецензируемую статью также можно квалифицировать как научную

работу, написанную достаточно грамотно, на хорошем научном языке, с корректным использованием научной терминологии. Библиография насчитывает 34 наименования, в том числе, работы на иностранных языках, и в должной мере репрезентирует состояние дел в исследуемой области. Хотя и могла бы быть расширена за счёт работ Н. Талеба, уж коли его концепция «чёрных лебедей» стала одним из ключевых элементов дизайна проведённого исследования. Тем более, что несколько работ этого автора переведены на русский язык. Апелляция к оппонентам имеет место в контексте обсуждения различных подходов к феномену цифровизации.

ОБЩИЙ ВЫВОД: представленную к рецензированию статью можно квалифицировать в качестве научной работы, соответствующей всем требованиям, предъявляемым к работам подобного рода. Полученные автором результаты будут интересны политологам, социологам, специалистам в области государственного управления, мировой политики и международных отношений, а также студентам перечисленных специальностей. В содержательном плане статья соответствует тематике журнала «Мировая политика» и рекомендуется к публикации.