Федеральное государственное автономное учреждение
высшего образования «Уральский федеральный университет имени
первого Президента России Б. Н. Ельцина»
Уральский гуманитарный институт
Кафедра востоковедения

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

Диссертация
на соискание ученой степени кандидата политических наук

Научный руководитель:
доктор исторических наук, доцент
Валиахметова Гульнара Ниловна

Екатеринбург – 2024

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

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 и 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-технологий. 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, продвигающих идеи исламистской альтернативы существующему мировому порядку. 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 в области защитных цифровых технологий с Израилем стало одной и главных причин отказа большинства монархий Залива от конфронтации с этим государством вплоть до нормализации отношений с ним ОАЭ и Бахрейном в рамках «Соглашений Авраама» 2020 г. 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.

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 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 – Университете, 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. 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). Исследователи сходятся во мнении о том, что кибербезопасность является одним из направлений информационной безопасности и, по сути, охватывает информационно-технологическую сферу, обеспечивая разработку комплекса мер по борьбе с ИКТ-угрозами на различных уровнях – технологическом, экономическом, политическом, правовом, управленческом, военном и т.д.

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, Е.С. Черненко, А.А. Чирко, В.В. Ященкова. Из зарубежных специалистов, работающих над указанной проблематикой, 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. 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. 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, посвященные анализу оборонительного и наступательного киберпотенциала 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 в зоне Персидского залива и на Ближнем Востоке в целом. Радикалы довольно быстро наращивают свой деструктивный киберпотенциал, оказывая значительное влияние на формирование национальных подходов к обеспечению комплексной цифровой защиты. Результаты исследований различных проявлений кибертерроризма представлены в работах Л. Веста, Д. Коэна, М. Нэнс, А. Онирети, А. Ротбарта, Ч. Сампсона, Л. Тисуро, а также в публикациях российских экспертов А.В. Манойло, Н.Х. Гафиатулиной, Д.М. Брусенцевой, А.В. Федорова. Комплексные исследования ИКТ-угроз со стороны радикально-экстремистких

группировок ведутся также в Центре оценки рисков Кембриджского университета, Европоле, Лаборатории Касперского и др.

Довольно 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); влияние интернета на повседневные религиозные практики мусульман (Б. Лоуренс, Дж. Шанцер, С. Миллер, Е.Н. Чеснова, З. Хабибулина, Э. Муратова, А.П. Забияко), специфика цифровизации бизнес-среды в мусульманских странах (М. Навид, А. Шоаиб).

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 – отличаются 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. Внутренняя и внешняя

политика аравийских монархий получила всестороннее освещение в фундаментальных исследованиях главных российских специалистов по арабским странам Залива и ССАГЗ – Г.Г. Косача и Е.С. Мелкумян. Проблемы безопасности на Ближнем Востоке также представлены в публикациях таких зарубежных исследователей, как Ф. Гауб, Й. Гузански, С. Кук, К. Михаэль.

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. Влияние геополитических факторов на решение технических проблем цифровой защиты в зоне Персидского залива исследовали Ф. Дузе, Л. Петинио, К. Саламатиан, Дж.-Л. Самаан. Сравнительный анализ правовых подходов арабских стран в вопросах противодействия киберпреступности проведен Э. Абу-Тайи.

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 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. Вместе с тем практика заимствования за рубежом готовых технологических решений и профессиональных кадров порождает зависимость арабских стран от своих партнеров (США и КНР) и способствует ослаблению их суверенитета, что трактуется рядом исследователей (М. Кросстон, М. Квет) как проявление «цифрового колониализма».

Среди региональных сюжетов в последние годы наибольшей дискуссионностью отличается тема развития кооперации по вопросам кибербезопасности в открытом и «дискретном» формате между монархиями Залива с Израилем. К этой теме, в частности, обращались А. Эл-Масри,

Б. Букс, Д. Джиндаль, Н. Хоррами М. Солиман и др. 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 на Ближнем Востоке, а российские востоковеды относительно недавно стали обращаться к исследованию данной проблематики. Имеющиеся к настоящему времени 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, в том числе в

сфере 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 кардинальным изменением 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 – Катар, Кувейт, Бахрейн, Саудовскую Аравию, Объединенные Арабские Эмираты (ОАЭ), Оман, – которые демонстрируют схожие тренды экономического и социально-политического развития. Данная группа государств расположена в зоне Персидского залива (субрегион Ближнего Востока[1]), является интегральной частью арабского мира и мусульманского историко-культурного ареала. Указанные страны объединяет, кроме того, взаимодействие в рамках созданной ими региональной организации – Совет сотрудничества арабских государств Залива (ССАГЗ), способствуя формированию у них сходных приоритетов в области национального развития, в том числе в сфере международной информационной безопасности.

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 обозначенных методологических рамок обусловлен тем, что в условиях цифровой эпохи ключевыми акторами международных отношений остаются государства,

[1] Субрегионы Ближнего Востока // Международный дискуссионный клуб “Валдай». URL: https://ru.valdaiclub.com/multimedia/infographics/subregiony-blizhnego-vostoka/ (дата обращения: 15.01.2024).

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 не только 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 имеет определенное значение, играет определенную роль, 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 провести классификацию и типологию, выявить общие и отличительные признаки и свойства международного сотрудничества монархий Залива в области кибербезопасности.

Оценка готовности аравийских монархий к отражению киберугроз производилась на основе методологии Глобального индекса кибербезопасности Международного союза электросвязи (МСЭ), специализированного института ООН по ИКТ[2]. Индекс предусматривает 5 ключевых критериев национальных систем цифровой защиты: нормативно-

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

правовая база, технический, организационный и кадровый потенциал, международное сотрудничество. Последний из обозначенных 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 и историко-генетического методов*. Они позволили в динамике рассмотреть эволюцию внешнеполитических стратегий и приоритетов аравийских монархий в вопросах создания безопасной цифровой среды в зоне Персидского залива, а также выявить комплекс факторов, которые обусловили специфику национальных подходов и практик в сфере кибербезопасности. *Сравнительно-исторический метод*, предполагающий сравнение и обобщение однородных исторических явлений, позволил раскрыть общность и разнонаправленность национальных интересов монархий Залива на разных этапах развития их национальных систем киберзащиты.

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 США, Евросоюза, двусторонние соглашения аравийских монархий с внешними партнерами (США – Саудовская Аравия, Бахрейн – Япония и пр.).

– документы и материалы международных организаций – ООН, 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» и т.д.;

– отчеты и пресс-релизы органов государственной власти аравийских монархий, США (Госдепартамента, Министерства обороны, Центрального командования), национальных групп реагирования на компьютерные инциденты монархий Залива (CERT), Ирана, Канады и ряда других государств, оказывающих заметное влияние на развитие ландшафта кибербезопасности на Ближнем Востоке в целом;

– 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: данные о развитии сектора телекоммуникаций и рынка кибербезопасности на Ближнем Востоке и в зоне Персидского залива, динамике развития гражданского и военного секторов

кибербезопасности (Национальный индекс кибермощи, Рейтинг совокупной военной мощи и др.);

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

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

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 неоднозначного влияния на этот процесс внешних и внутренних факторов, а также в контексте развития военно-политической обстановки на Ближнем Востоке в целом.

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 как на платформе ССАГЗ, так и в двустороннем формате межгосударственного взаимодействия и государственно-частного партнерства, который является доминирующим. 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 формате 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 использованы в дальнейших исследованиях по проблемам цифровой безопасности стран арабского мира и Ближнего Востока.

Практическая значимость исследования состоит в том, его материалы могут быть востребованы профильными 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», а также в профессиональной деятельности – в том числе при подготовке экспертных заключений, а также при принятии внешнеполитических решений и выработке мер ответственными профильными структурами.

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.

ГЛАВА 1
КОНЦЕПТУАЛЬНЫЕ ПОДХОДЫ К ИССЛЕДОВАНИЮ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Кибербезопасность как предмет политического анализа

С момента своего создания в начале 1990-х гг. Интернет трансформировался из платформы обмена информацией в «сеть сетей» и ключевую информационную инфраструктуру современного мира. IT-технологии являются основополагающими в процессе перехода к информационному обществу и формирования постиндустриального технологического уклада в рамках «четвертой промышленной революции»[3]. Глобальные изменения, обусловленные взаимодействием физического и виртуального миров, «оказывают синергетический эффект на современное общество, трансформируя сложившиеся связи и отношения в сфере экономики, политики, общественной жизни, в том числе на международном уровне»[4]. В этой связи технологический потенциал становится одним из определяющих факторов обеспечения суверенитета и геополитического веса государств, а цифровые технологии – стратегическим ресурсом в социально-экономическом развитии и борьбе за глобальное и региональное лидерство.

Вместе с тем преобразовательный потенциал ИКТ и их роль катализатора экономического и социального развития ограничиваются их уязвимостью перед деструктивным воздействием извне. Кроме того, возрастающая в геометрической прогрессии численность новых ИКТ-устройств, сетей и баз данных (в среднем на 8,2 тыс. элементов ежесуточно[5]) ведет к тому, что роль человека начинает меняться с исполнителя на наблюдателя и появляется риск утраты «ручного» контроля над технологиями.

---

[3] Шваб К. Четвертая промышленная революция. М., 2017. С. 180.

[4] Зиновьева Е.С. Мирополитическая концептуализация международного научно-технического сотрудничества // Вестник МГИМО-Университета. 2018. № 6. С. 245.

[5] CISCO Annual Internet Report. San Jose, 2020. P. 18.

Глобальное информационное пространство трансформируется в поле многочисленных угроз, формирующих цифровой вызов международной и национальной безопасности. Это ставит в мировую повестку вопрос о консолидации усилий международного сообщества в деле защиты цифровой среды на глобальном, региональном и национальном уровнях. Однако развитие международного взаимодействия на данном направлении наталкивается на целый ряд препятствий и остается предметом довольно острых академических и политических дискуссий. Объективный научный поиск эффективных путей и форм международного сотрудничества по обеспечению информационной безопасности осложнен не только чрезмерной политизацией проблемы, но также отсутствием общепризнанного понятийного аппарата. Прежде всего речь идет о содержании базовых терминов «информационная безопасность» и «кибербезопасность».

Представляется возможным выделить три основополагающих подхода к определению содержания обозначенных терминов. В рамках первого, «западного» подхода, которого придерживаются США, Канада, страны Европы, ряд государств Азии (Республика Корея, Япония и др.), термины «информационная безопасность» и «кибербезопасность» 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 (синонимично термину «кибербезопасность») и политико-идеологическое, тем самым принимая в расчет дестабилизирующий потенциал ИКТ в социально-политической сфере[6]. Политико-идеологическое направление информационной безопасности предусматривает защиту

[6] Зиновьева Е.С. Международное сотрудничество в области обеспечения информационной безопасности // Право и управление. 2014. № 4. С. 45.

общества от деструктивного информационного воздействия извне, нацеленного на подрыв социальной стабильности и международного авторитета государства, а также включает противодействие использованию ИКТ в качестве инструмента вмешательства во внутренние дела суверенных государств, разжигания межэтнической и межконфессиональной розни и т.д. Данный подход отражен в базовых государственных документах России – Доктрине информационной безопасности РФ 2016 г.[7] и Основах государственной политики РФ в области международной информационной безопасности 2013 г. и 2021 г.[8].

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. Соответствующие резолюции принимаются ГА ООН ежегодно, расширяя и дополняя направления международного сотрудничества в области информационной безопасности с учетом развития ИКТ и порождаемых ими угроз[9]. Выработанный ООН при участии России новый термин «безопасность в сфере использования ИКТ», по сути, является компромиссным и позволяет обозначить точки соприкосновения, необходимые для взаимодействия государств, придерживающихся разных подходов. Сегодня он активно применяется в документах международных площадок профильного взаимодействия (ООН, АСЕАН, БРИКС, ШОС и др.)[10].

Вместе с тем США и их союзники, хотя и принимают компромиссные инициативы ООН, продолжают акцентировать внимание на технико-

---

[7] Доктрина информационной безопасности РФ. М., 2016. С. 2.

[8] Основы государственной политики РФ в области международной информационной безопасности от 12.04.2021. URL: http://www.scrf.gov.ru/security/information/document114/ (дата обращения: 15.06.2022).

[9] Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: Резолюция ГА ООН A/RES/76/19 от 8.12.2021 г.

[10] Международная информационная безопасность: подходы России. М., 2021. С. 6.

технологическом измерении информационной безопасности, в связи с чем термины «информационная безопасность» и «кибербезопасность» продолжают использоваться в качестве синонимов, причем не только сторонниками «западного» подхода, но и международными организациями (например, Международным союзом электросвязи – специализированным учреждением ООН по ИКТ). В этой связи в международных и национальных документах триада информационных угроз ООН также может быть представлена в терминах с приставкой «кибер-»: киберпреступность, кибертерроризм, межгосударственное киберпротивостояние и т.п.

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.

В мировом экспертом сообществе нет единства и в вопросе о содержании терминов «информационная война», «кибервойна», «цифровая война», «боевые действия в киберпространстве», под которыми в целом понимается стратегическое межгосударственное противостояние в информационном пространстве[11]. Оно может принимать формы разведывательной, электронной, хакерской, кибернетической, экономической и психологической войны, а также борьбы с системами управления противника[12]. Милитаризация цифрового пространства является следствием незавершенности перехода к новому миропорядку, сопровождающемуся ростом конфликтности, который, в свою очередь, побуждает государства наращивать как оборонительный, так и наступательный киберпотенциал[13].

---

[11] Denning D. Information Warfare and Security. Washington, 1999; Clarke R.A., Knake R. Cyber War. N.Y., 2010; Карасев П.А. Эволюция национальных подходов к ведению кибервойны // Международная аналитика. 2022. № 2. С. 79–94.

[12] Libicki M. Cyberdeterrence and Cyberwar. Santa Monica, 2009.

[13] Манойло А.В. Информационная война и новая политическая реальность // Вестник МГОУ. 2021. № 2. С. 135–148.

Соответственно военно-политические угрозы международной безопасности создают наибольшие риски для устойчивости мировой системы и стратегической стабильности[14].

Практика применения прорывных технологий в качестве силовой компоненты в межгосударственных конфликтах также породила в экспертной среде дискуссии о содержании терминов «информационное оружие», «кибероружие», «цифровые вооружения», которыми обозначаются сверхсложные вредоносные компьютерные программы, разработанные по инициативе и при прямом финансовом участии государств и предназначенные для нанесения технологического, информационного и материального ущерба государству-противнику[15]. Концепция кибероружия как инструмента ведения кибервойн, позволяющая провести четкую грань между кибервооружениями и обычными вредоносными ИКТ-средствами, используемыми, например, киберпреступниками в целях незаконного обогащения, по-прежнему окончательно не сформулирована. Хотя большинство государств признают, что в современных условиях кибероружие постепенно занимает нишу ядерного (что априори требует формирования особого режима международного контроля) и призывают к поиску «глобального киберконсенсуса», концепт мультидоменного цифрового сдерживания[16], предлагаемый на международных площадках, по-прежнему сталкивается с критикой и противодействием на национальном уровне.

Поскольку использование ИКТ в военно-политической сфере неизбежно усиливает асимметричность современных международных конфликтов, перед научными сообществами встает задача выработки критериев для определения способности государств эффективно вести оборонительные и наступательные действия в информационном пространстве, в связи с чем научный лексикон

---

[14] Карасев П., Ященков В.В. Многофакторный анализ стратегической стабильности в контексте угроз международной информационной безопасности // Вестник РГГУ: Информатика. 2019. № 3. С. 19–35.
[15] Каберник В.В. Проблемы классификации кибероружия // Вестник МГИМО-Университета. 2013. № 2. С. 74.
[16] Демидов О.В., Черненко Е.В. Грозный ум на страже кибербезопасности // Индекс безопасности. 2014. № 3. С. 157.

международной информационной безопасности пополнился термином «кибермощь». Авторитетный американский исследователь кибервойн Дж. Шелдон понимает под ним совокупность всех доступных кибернетических средств, определяющих способность государства воздействовать на киберпространство и отстаивать в нем свои интересы. Вместе с тем политолог признает, что данное понятие весьма условно, так как не может быть презентовано в конкретном количественном формате, что затрудняет сопоставление показателей кибермощи двух или более акторов[17].

Более актуальную, с точки зрения сравнительного анализа, трактовку понятия предлагают специалисты Белфер-центра Гарвардской школы Кеннеди: в соответствии с их подходом, «кибермощь» – это совокупный потенциал и возможности государства, позволяющие ему успешно противостоять угрозам из киберпространства со стороны государственных и негосударственных акторов. «Национальный индекс кибермощи» Белфер-центра выводится на основе 8 критериев и оценивает способность государства использовать ИКТ-средства в наступательных и оборонительных целях, а также для сдерживания противника. При этом ИКТ-инструменты выступают лишь одним из способов отстаивания национальных интересов и нередко реализуются в связке с «классическими» средствами (военными, дипломатическими и экономическими). Это, в свою очередь, делает понятие «кибермощь» составной частью более широкого понятия «мощь государства». В 2022 г. исследование охватывало 30 стран: рейтинг самых сильных (с точки зрения кибермощи) стран возглавили США, Китай и Россия. Значительно усилила свои позиции Саудовская Аравия (единственная из монархий Залива, включенная в исследование), переместившись с 27 строки рейтинга 2020 г. на 21 место в 2022 г.[18]. Следует отметить, что результаты подобного рода исследований (к настоящему времени насчитывается более десятка различных кибериндексов) нередко подвергаются критике из-за ограниченного охвата

[17] Sheldon J. Deciphering cyberpower // Strategic Studies Quarterly. 2011. № 2. P. 97.
[18] National Cyber Power Index 2022. Cambridge, 2022. P. 17–21.

государств, сложности с верификацией данных и политической ангажированности экспертных коллективов.

Спектр угроз международной информационной безопасности расширяется за счет использования ИКТ антисистемными акторами в лице транснациональных радикально-экстремистских группировок исламистского толка, которые в различных формах ведут в глобальной сети Интернет так называемый «киберджихад» против «неверных». Активизация радикалов в информационном пространстве порождает дискуссии относительно трактовки таких новых понятий, как «кибертерроризм», «киберджихад» («цифровой / электронный джихад»), «медиа-джихад», «киберхалифат» («цифровой халифат»), «радикальная метавселенная» и др. Академические разногласия обусловлены многоаспектным характером обозначенных феноменов, изучение которых лежит на стыке различных научных дисциплин (политологии, исламоведения, истории, компьютерных наук, психологии и т.д.), а оценки зачастую зависят от направлений исследований и традиций научной школы, к которой принадлежит исследователь[19]. При этом следует учесть, что, например, типологизация негосударственных акторов мировой и региональной политики представляет собой отдельную методологическую проблему[20].

Так, например, западные исследователи разводят понятия «медиа-джихад» (совокупность мер, предпринимаемых радикальными исламистами для продвижения своих идей на платформах социальных медиа) и «киберджихад» (преднамеренные, политически мотивированные кибератаки со стороны террористических группировок исламистского толка на ИКТ-инфраструктуру «неверных»), трактуя их как составные элементы более широкого термина «кибертерроризм»[21]. Российские исследователи склонны

[19] Наумкин В.В. Исламский радикализм в зеркале новых концепций и подходов. М.: КомКнига, 2005.
[20] 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.
[21] West L. #jihad: Understanding social media as a weapon // Security Challenges. 2016. № 2. P. 9–26; Siboni G., et. al. The threat of terrorist organizations in cyberspace // Military and Strategic Affairs. 2013. № 3. P. 20–29.

рассматривать оба понятия в связке[22], мотивируя это тем, что агитационная и вербовочная работа является одной из ключевых форм деятельности радикалов и поэтому попадает под понятия «киберджихад» и «кибертерроризм», которые в рамках case-studies могут быть взаимозаменяемы. В свою очередь термин «кибертерроризм» также может получать расширительные трактовки и рассматриваться в качестве составного элемента «супертерроризма» (использования радикалами передовых вооружений и технологий, позволяющих нанести государству либо группе государств существенный экономический, социально-политический или имиджевый ущерб)[23]. По сути, при любой интерпретации угрозы со стороны кибертерроризма затрагивают в равной степени и технико-технологический, и социально-политический аспекты международной информационной безопасности, приобретая форму угрозы стратегического характера. Однако разница концептуальных подходов затрудняет практическое сотрудничество государств в сфере противодействия ИКТ-угрозам, генерируемым антисистемными участниками информационных войн.

Различные методики определения деструктивного киберпотенциала радикально-экстремистских организаций и критерии оценки исходящих с их стороны киберугроз были разработаны в Центре исследования рисков Кембриджского университета[24], Лаборатории Касперского[25], Европоле[26], Министерстве обороны США[27], а также отдельными экспертами[28]. И, хотя результаты проведенных исследований во всех случаях приводят к выводу о том, что в среднесрочной перспективе «цифровой джихад» не способен трансформироваться в серьезную угрозу международной безопасности,

---

[22] Манойло А.В. Модели «мягкой силы» сетевых террористических организаций в системе угроз национальной безопасности // Вестник Российской нации. 2016. № 2. С. 184–188; Гафиатулина Н.Х., Брусенцева Д.М. Медийное пространство как источник активности террористической организации // Гуманитарные, социально-экономические и общественные науки. 2017. № 6. С. 39.

[23] Федоров А.В. Супертерроризм: новый вызов нового века. М., 2022. С. 93, 95.

[24] Cyber Terrorism: assessment of the threat to insurance. Cambridge, 2020.

[25] Ready... Or not? Balancing future opportunities with future risks. Moscow, 2021. P. 5, 8.

[26] Online Jihadist Propaganda 2021. Luxembourg, 2022.

[27] FM 3-12: Cyberspace and electromagnetic warfare. Washington, 2021.

[28] Onireti A. Cyber-Terrorism. L., 2024. P. 47, 49.

специалисты признают, что технические возможности террористов быстро растут, и приход физической террористической кибератаки является лишь вопросом времени.

Противоречивое влияние цифровизации на мировые религии также вызывает определенные опасения в экспертной среде. Религиозное информационное пространство характеризуется как «особое измерение реальности, созданное посредством компьютерных технологий и существующее в искусственно созданной компьютерными программами среде», а появление феномена «виртуальных религий» («киберрелигий») – как закономерное следствие научно-технического прогресса[29]. В данном контексте религиозная сфера жизни современного человека требует защиты от негативного воздействия с использованием ИКТ-средств и, соответственно, попадает в объектное поле международной информационной безопасности.

Исследования феномена «виртуального ислама» и влияния цифровых технологий на ислам отличаются многообразием оценок и методологических подходов к анализу таких проблем, как трансформация идентичности мусульман и роли института религиозных авторитетов в цифровую эпоху, специфика проведения виртуальных ритуалов и практик, и т.п.[30]. Мусульмане все чаще используют Интернет для поиска ответов на важные религиозные вопросы, что, с одной стороны, упрощает им доступ к рекомендациям религиозных авторитетов по возникающим вопросам (*фетвам*) и побуждает мусульманское духовенство более активно взаимодействовать с общиной через информационную среду, а с другой, создает угрозу распространения «ложных фетв»[31].

Российские и западные специалисты сходятся во мнении о том, что постепенная «виртуализация» ислама является закономерным результатом перехода в информационное общество, который формирует не только угрозы,

[29] Забияко А.П. Киберрелигия: наука как фактор религиозных трансформаций. Благовещенск, 2012. С. 7.
[30] Виртуальный ислам на постсоветском пространстве. Баку, 2023. С. 15–16, 19, 21–22.
[31] Чеснова Е.Н. Цифровизация религии: ислам // Гуманитарные ведомости ТГПУ. 2021. № 4. С. 75.

но и потенциальные точки роста. Так, по мнению американского исламоведа Б. Лоуренса, несмотря на цифровизацию всех сфер жизни мусульманских сообществ и общую размытость границ «виртуального ислама», его «столповые ориентиры» в виде священных текстов (Коран, Сунна), личностей (Пророк Мухаммед и его сподвижники) и закона (нормы шариата) сохраняют свою ключевую значимость[32]. Ведущий российский специалист по исламскому праву Л.Р. Сюкияйнен подчеркивает, что мусульманская правовая школа способна успешно адаптироваться к реалиям меняющегося мира в случае, если перемены не угрожают умме потерей религиозной и культурной идентичности[33]. При соблюдении данных условий исламское право способно эффективно регулировать цифровые аспекты жизни современных мусульман без введения существенных ограничений на использование ИКТ-сервисов.

В случае с монархиями Персидского залива вопрос гармоничного сочетания цифровых технологий и традиционных религиозных учений стоит особенно остро в силу того, что здесь ислам не просто государственная религия, а основной закон, определяющий структуру и все области жизни государства, включая его внутреннюю и внешнюю политику. Кроме того, например, Саудовская Аравия позиционирует себя в качестве главного защитника интересов глобальной уммы (мирового сообщества мусульман). Сегодня в аравийских монархиях в целом достигнут компромисс по вопросу внедрения цифровых технологий, однако время от времени власти этих государств подвергаются критике со стороны консервативных мусульманских богословов за социально-экономическую политику, «не соответствующую истинному учению»[34].

По этой причине вопросы, связанные с цифровизацией и обеспечением международной и национальной информационной безопасности, остаются для монархий Залива крайне чувствительными, а профильные инициативы,

[32] Lawrence B. Allah On-Line: the practice of global Islam in the information age // Practicing religion in the age of media. N.Y., 2002. P. 240.
[33] Сюкияйнен Л.Р. Исламское право и диалог культур в современном мире. М., 2021. С. 197–247.
[34] Shanzer J., Miller S. Facebook Fatwa: Saudi clerics, wahhabi Islam, and social media. Washington, 2012. P. 45, 48.

исходящие от внешних акторов (в лице международных организаций или стратегических союзников), далеко не всегда находят поддержку и понимание, особенно если дело касается гармонизации правового поля и восполнения правовых лакун, образовавшихся в связи с внедрением новых ИКТ-сервисов (финтех, блокчейн, криптовалюты и т.п.) и необходимостью их киберзащиты.

В научной литературе и нормативно-правовой документации международного и национального характера отсутствует единство в применении термина «киберпреступность», который может заменяться терминами «новые формы преступности», «информационная / компьютерная преступность», «атаки против информационных систем», «преступления в сфере компьютерной информации / информационных технологий», «использование ИКТ в преступных целях» и т.д. Термин «киберпреступность» широко применяется с странах Северной Америки, Европы, Африки, в ряде государств Азии, в том числе в арабских монархиях Персидского залива. В правовой практике и научных сообществах России приняты термины «преступления в сфере ИКТ / компьютерной информации» и «информационные преступления», что обусловлено согласованием понятийного аппарата с национальным подходом к обеспечению национальной и международной информационной безопасности, закрепленным в соответствующих стратегических документах страны.

Вместе с тем отечественные исследователи юридического профиля признают, что используемая в российском правовом и научном поле терминология избыточно широкая, в связи с чем возникают проблемы с ее применением на практике. По этой причине целесообразно ввести термин «киберпреступность», так как он включает и преступления в информационном пространстве, где в качестве *объекта правонарушения* выступает конфиденциальность, целостность, доступность (триада информационной безопасности, или триада КЦД), и преступления с использованием ИКТ-

инструментов, где последние являются *средством* совершения криминальных действий[35].

В рамках правового подхода аналогичным образом представляется возможным соотнести понятия «информационная безопасность» и «кибербезопасность». Сравнительный анализ нормативно-правовых актов РФ и других стран (США, Евросоюз, Китай) приводит российских правоведов к выводу о том, что в зарубежном правовом поле кибербезопасность (информационно-технологическая безопасность) – это самостоятельное направление национальной безопасности, тогда как в России она является составной частью информационной безопасности, которая, в свою очередь, выступает базовым компонентом национальной безопасности. Так, например, российский исследователь А.Ю. Баландин дает следующее авторское определение: «Кибербезопасность является одним из элементов информационной безопасности, характеризующимся спецификой цифровой среды распространения угроз, применением программно-аппаратного элемента при проведении атак и противодействия таковым, проявлением негативных последствий подобных атак как в компьютерно-цифровой среде, так и в иных сферах, а также инструментами, способами и методами противодействия таковым»[36].

Актуализация понятийного аппарата и инструментов, регулирующих отношения в сфере ИКТ, востребована не только в юридической, но также в экономической и технической областях, о чем свидетельствуют результаты исследований представителей указанных научных направлений, которые пришли к аналогичным выводам[37].

---

[35] Старкова Л.М. Подходы к пониманию и нормативному определению категории «киберпреступность» // Московский журнал международного права. 2021. № 4. С. 123–135.

[36] Баландин А.Ю. Кибербезопасность и информационная безопасность. Демаркация правовых категорий // Правовая политика и правовая жизнь. 2023. № 3. С. 267.

[37] См., напр.: Яковлева А.В. Кибербезопасность и ее правовое регулирование // Социально-политические науки. 2021. № 4. С. 70–81; Алпеев А.С. Терминология безопасности: кибербезопасность, информационная безопасность // Вопросы кибербезопасности. 2014. № 5. С. 39–42; What is cyber security // Kaspersky. URL: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security (accessed: 21.06.2023); Стратегии кибербезопасности // InfoWatch. URL: https://www.infowatch.ru/sites/default/ files/publication_file/analiticheskiy-otchet-strategii-kiberbezopasnosti.pdf (accessed: 21.06.2023).

Действительно, о многовекторности информационной безопасности и, как следствие, комплексном характере данного понятия свидетельствуют профильные стратегические документы РФ – Доктрина информационной безопасности 2016 г.[38] и Основы государственной политики в области международной информационной безопасности 2021 г.[39]. Обозначенные в указанных документах ИКТ-угрозы допустимо *дифференцировать по принципу, объекту и способу воздействия*. При таком подходе деструктивная информация, определяемая как информационно-психологическая угроза, оказывает воздействие на сознание человека (объект информационной атаки), а во внешней среде, в том числе цифровой, не идентифицируется. При компьютерных атаках (кибератаках), которые формируют комплекс информационно-технологических угроз (киберугроз), объектом деструктивного воздействия выступают информационные системы (программное обеспечение, технико-технологические элементы цифровых структур и т.п.), средством – вредоносное программное обеспечение, а принципом – распространение данных в цифровой (внешней) среде, т.е. без прямого воздействия на человека.

Дифференцированный характер деструктивных воздействий в разных средах (сознание человека – цифровая среда) на разные объекты (человек – ИКТ-системы) выявляется также при анализе целей, задач и направлений обеспечения информационной безопасности, закрепленных в Доктрине и Основах государственной политики РФ: например, «противодействие угрозе использования ИКТ в террористических целях, в том для пропаганды терроризма и привлечения к террористической деятельности новых сторонников»[40]. Это позволяет в рамках политического анализа выделить цифровую составляющую (кибербезопасность) из общего контекста информационной безопасности.

---

[38] Доктрина информационной безопасности РФ. М., 2016. С. 2.

[39] Основы государственной политики РФ в области международной информационной безопасности от 12.04.2021. URL: http://www.scrf.gov.ru/security/information/document114/ (дата обращения: 15.06.2022).

[40] Там же.

Аналогичный подход представлен и в документах ряда международных организаций и государств. Так, например, независимая неправительственная Международная организация по стандартизации (International Organization for Standartization, ISO), объединяющая профильные национальные органы 171 страны, определяет задачи информационной безопасности в контексте триады КЦД – «сохранение конфиденциальности, целостности и доступности информации», а кибербезопасность – как «безопасность киберпространства, сохранение конфиденциальности, целостности и доступности информации в киберпространстве». В свою очередь, киберпространство определяется как «сложная среда, возникающая в результате взаимодействия людей, программного обеспечения и услуг в Интернете и поддерживается распределенными по всему миру физическими устройствами ИКТ и подключенными сетями»[41].

Схожих принципов придерживаются монархии Персидского залива. К примеру, Стратегия кибербезопасности эмирата Дубай (ОАЭ) определяет кибербезопасность как «безопасность киберпространства и внедрение средств управления и контроля для защиты конфиденциальности, целостности и доступности данных для государственного и частного секторов и отдельных лиц» и «киберустойчивость – обеспечение непрерывности функционирования информационно-телекоммуникационных систем и их доступности в киберпространстве»[42].

Министерство обороны США определяет киберпространство как «глобальную область в информационной среде, состоящую из взаимозависимых сетей ИКТ-инфраструктуры и данных, включая Интернет, телекоммуникационные сети, компьютерные системы, а также встроенные процессоры и контроллеры»[43]. Министерство обороны РФ придерживается расширительного подхода, оперируя понятием «информационное

[41] ISO/IES 27032:2023. Cybersecurity. URL: https://www.iso.org/ru/standard/76070.html (accessed: 21.06.2023).
[42] Dubai cybersecurity strategy. URL: https://u.ae/en/dubai-cyber-security-strategy (accessed: 19.01.2024).
[43] Department of Defense: Cyber Strategy 2023 // U.S. Dept. of Defense. URL: https://media.defense.gov/2023/299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF (accessed: 11.12.2023).

пространство», в котором кибербезопасность, по сути, представлена в качестве его составной части: «сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие, в т. ч. на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию»[44].

Европейское агентство по сетевой и информационной безопасности (The European Union Agency for Network and Information Security, ENISA) определяет кибербезопасность как совокупность 5 областей защиты[45]:

– безопасность коммуникаций: защита от деструктивного воздействия на техническую инфраструктуру цифровых систем, которое может привести к нарушению или изменению задач и действий, изначально заложенных в них владельцами, разработчиками или пользователями;

– безопасность операций: защита от преднамеренного искажения рабочих процессов, которые могут привести к результатам, не предусмотренным владельцами, разработчиками или пользователями;

– безопасность информации: защита от кражи, удаления или изменения хранящихся и передаваемых данных в цифровых системах (киберсистемах);

– военно-политическая безопасность: защита от кибератак на системы связи и промышленную инфраструктуру, а также иных угроз в киберпространстве, в результате которых злоумышленники могут получить доступ к физическим и цифровым активам и приобрести тем самым политические, военные или стратегические выгоды или преимущества;

– физическая безопасность: защита киберсистем от физических угроз, в том числе предотвращение физического доступа злоумышленников к серверам с целью их повреждения, внедрения вредоносных программ либо принуждение к этому пользователей;

---

[44] Концептуальные взгляды на деятельность ВС РФ в информационном пространстве. М., 2011. С. 5.
[45] Definition of cybersecurity. Attiki, 2015.

Наиболее комплексное определение кибербезопасности представлено, на наш взгляд, в «Руководстве по разработке национальной стратегии кибербезопасности», подготовленном Международным союзом электросвязи в партнерстве с 12 организациями, представляющими структуры ООН, государственный и частный секторы, научно-исследовательские и общественные организации. В данном документе кибербезопасность определяется как «набор средств, стратегии, руководящие принципы, подходы к управлению рисками, действия, профессиональная подготовка, передовой опыт, гарантии и технологии, которые могут быть использованы для защиты доступности, целостности и конфиденциальности ресурсов в соединенной инфраструктуре, используемой государственными органами, частными организациями и гражданами; такие ресурсы включают соединенные компьютерные устройства, персонал, инфраструктуру, приложения, услуги, системы электросвязи и данные в киберсреде»[46]. В свою очередь обеспечение кибербезопасности рассматривается МСЭ как «комплексная задача со множеством различных управленческих, политических, эксплуатационных, технических и правовых аспектов»[47].

Следуя резолюциям ГА ООН, «Руководство» возлагает ответственность за обеспечение кибербезопасности на государства, в обязанности которых входит разработка и реализация политики в рассматриваемой сфере на основе согласованной деятельности глав государств, правительств, министерств иностранных дел, телекоммуникаций и связи, промышленности и торговли, юстиции, обороны, внутренних дел, а также специализированных государственных органов и институтов, непосредственно связанных с вопросами цифровой защиты и взаимодействием с ее негосударственными участниками в лице бизнес-структур, научно-исследовательских и образовательных учреждений[48].

---

[46] Руководство по разработке национальной стратегии кибербезопасности. Женева, 2018. С. 13.
[47] Там же. С. 8.
[48] Там же. С. 30, 49.

Государственная политика в сфере кибербезопасности, согласно «Руководству» МСЭ, должна основываться на 9 принципах[49]:

– наличие национальной стратегии кибербезопасности, базирующейся на четкой концепции и учитывающей интересы и мнения государства и общества во всей их полноте;

– всеобъемлющий подход и ориентированность на конкретные особенности и приоритеты страны, поскольку кибербезопасность – это не просто техническая проблема, а «комплексный многогранный вопрос, различные аспекты которого затрагивают не только экономическое и социальное процветание, но и другие области, такие как правоприменение, национальная и международная безопасность, международные отношения, торговые переговоры, устойчивое развитие и др.»;

– открытость для всех: активное участие всех заинтересованных сторон с учетом их потребностей и обязательств;

– экономическое и социальное процветание: кибербезопасность не является самоцелью, она должна вносить максимальный вклад в устойчивое развитие и социальную интеграцию;

– основополагающие права человека: права, которые человек имеет в офлайн-среде, должны также защищаться и в онлайн-среде;

– управление рисками и устойчивость: обеспечение экономической и социальной устойчивости, непрерывность процесса управления инцидентами и рисками;

– надлежащий набор политических инструментов: имеющиеся в распоряжении правительств различные рычаги и политические инструменты: законодательство, регулирование, стандартизация, программы и механизмы стимулирования и обмена информацией, образовательные программы, обмен передовым опытом, определение ожидаемых норм поведения, построение сообществ, основанных на доверии;

---

[49] Там же. С. 29–33.

– четкое определение руководства, функций и распределение ресурсов: правительство ответственно за распределение соответствующих функций и обязанностей между всеми субъектами кибербезопасности, а также выделение достаточных людских, материальных и финансовых ресурсов;

– доверительная среда: создание национальной цифровой экосистемы, в которой защищаются права и интересы граждан и делового сообщества.

Для оценки готовности современных государств к реагированию на угрозы, порождаемые ИКТ, в 2013 г. под эгидой МСЭ ООН был запущен исследовательский мега-проект «Глобальный индекс кибербезопасности». В состав экспертного коллектива вошли представители передовых технологических государств мира (США, Россия, Китай, страны Евросоюза и др.) и развивающихся стран, в том числе 4 из 6 монархий Залива – Саудовская Аравия, ОАЭ, Бахрейн и Оман. К настоящему времени опубликованы результаты 4-х исследований (2015, 2017, 2018, 2021 гг.)[50], последнее из которых охватывает 194 государства мира. Проект МСЭ является, на наш взгляд, наиболее авторитетным и объективным источником данных о состоянии и трендах развития международной и национальной кибербезопасности ввиду максимально широкого странового охвата и представительства ведущих государств мира, имеющих концептуальные разногласия по вопросам о путях строительства безопасной цифровой среды на глобальном уровне (Россия, Китай – США, Евросоюз). Кроме того, к участию в проекте присоединилось большинство аравийских монархий, что свидетельствует о том, что они разделяют подходы и принципы обеспечения кибербезопасности на глобальном, региональном и национальном уровнях, разработанные в рамках проекта.

В ходе реализации проекта экспертами была разработана методология оценки рисков развития национальной цифровой среды и определения уровня киберготовности государств (готовности к отражению киберугроз), на основе

[50] Global Cybersecurity Index 2014–2020. Geneva: ITU, 2015– 2021 (далее по тексту – GCI).

которых формируются рекомендации правительствам по укреплению устойчивости и развитию национальных систем кибербезопасности. В рамках данного подхода каждое исследуемое государство оценивается по пяти критериям[51]:

– *правовые меры:* наличие национальной законодательной базы в области обеспечения кибербезопасности и отраслевых нормативно-правовых актов и регламентов, регулирующих деятельность в цифровом пространстве и создающих благоприятные условия для гармонизации практики на международном уровне и повышения эффективности международной борьбы с киберпреступностью;

– *технические меры:* наличие общенациональных (Computer Emergency Response Team, CERT) и отраслевых (например, Fin-CERT) агентств по реагированию на чрезвычайные ситуации, степень развитости системы вспомогательных групп компьютерной безопасности по реагированию на инциденты (Computer Security Incident Response Services, CSIRT), национальных Центров управления безопасностью (Security operations center, SoC), а также иных структур с мониторингово-аналитическим функционалом, участие в региональных и глобальных инициативах по совершенствованию технических систем в сфере кибербезопасности;

– *организационные меры:* наличие стратегии национальной кибербезопасности (информационной безопасности) и профильных институтов с четким разграничением функционала, ответственных за разработку, реализацию и оценку результатов стратегии;

– *меры по развитию потенциала*: наращивание кадрового потенциала путем поддержки профильных научно-исследовательских проектов и образовательных программ, проведения регулярных кампаний по повышению уровня цифровых знаний представителей государственного и частного

[51] GCI 2017. Geneva, 2018. P. 4–11; GCI 2020. Geneva, 2021. P. 3–24, 130–136.

секторов, широких слоев населения; развитие государственно-частного партнерства в вопросах кибербезопасности;

– *меры по развитию международного сотрудничества*: наличие подписанных и ратифицированных соглашений на двусторонней и многосторонней основе вне зависимости от того, являются ли они юридически обязательными; географический охват и формы международных связей между всеми субъектами кибербезопасности – межправительственные и межведомственные контакты, международные связи по линиям государственно-частного партнерства, научно-исследовательских и образовательных учреждений, национальных и отраслевых групп реагирования на компьютерные инциденты и т.п.

Международное сотрудничество является краеугольным камнем обеспечения кибербезопасности на национальном, региональном и глобальном уровнях, охватывая все пять столпов киберготовности государств – нормативно-правовую и организационно-институциональную системы, технический и кадровый потенциал, внешнюю политику. МСЭ и его партнеры подчеркивают исключительную значимость многоуровневого сотрудничества, поскольку «кибербезопасность играет все более важную роль во множестве различных областей международных отношений, включая права человека, экономическое развитие, торговлю, коммерческую деятельность, контроль над вооружениями, безопасность, стабильность, поддержание мира и разрешение конфликтов»[52]. В этой связи «Руководство по разработке национальной стратегии кибербезопасности» МСЭ рекомендует государствам строить сотрудничество в области кибербезопасности на следующих принципах[53]:

– признание кибербезопасности одним из приоритетов внешней политики;

[52] Руководство по разработке национальной стратегии кибербезопасности. С. 48.
[53] Там же. С. 48–50.

– учет особенностей политического, общественного, культурного и экономического устройства страны в процессе развития регионального и международного сотрудничества;

– участие в международных обсуждениях по вопросам кибербезопасности на площадках региональных и международных организаций, а также объединений государственного и/или частного сектора, в рамках межправительственных дискуссий, задействуя в том числе традиционные отлаженные механизмы кооперации;

– поощрение официального и неофициального сотрудничества в международных инициативах, связанных с разработкой законодательных и политических мер, охраны правопорядка, реагирования на инциденты, обмена информацией, в том числе информацией о киберугрозах;

– приверженность обеспечению согласованности национальных и международных усилий по обеспечению кибербезопасности, ориентация на передовые методы работы, стремление внести вклад в достижение единообразия и сближение подходов в вопросах создания безопасной цифровой среды на региональном и глобальном уровнях.

На международном уровне ведущая роль в содействии диалогу между государствами по вопросу об использовании ИКТ играет ООН, что закреплено в резолюциях ГА ООН[54]. По инициативе России на платформе ООН с 1998 г. ведется комплексная работа, направленная на повышение уровня глобальной цифровой безопасности и устойчивости национальных государств к информационным угрозам[55]. На регулярной основе собираются группы правительственных экспертов (ГПЭ, с 2004 г.) и Рабочие группы открытого состава (РГОС, с 2018 г.), чья ключевая задача – формирование комплексного видения актуальных глобальных угроз, исходящих из информационного

[54] Достижения в сфере информатизации: Резолюция ГА ООН A/RES/76/19 от 8.12.2021 г.

[55] Крутских А.В. Международная информационная безопасность // Вестник РУДН. Международные отношения. 2022. № 2. С. 342–351; Козюлин В.Б. Потенциал российских инициатив в сфере международной информационной безопасности // Вестник ученых-международников. 2022. № 2. С. 34–55.

пространства, и выработка предложений по борьбе с ними[56]. Несмотря на то, что группы представляют разное видение принципов международного сотрудничества в области информационной безопасности (и возглавляются США и РФ соответственно), эксперты, как правило, выделяют три общих приоритета их деятельности:

– обеспечение механизмов применимости норм международного права по отношению к информационному пространству;

– разработка «Кодекса правил поведения» в информационном пространстве;

– работа по укреплению взаимного доверия в ИКТ-среде[57].

Особую важность для ГПЭ и РГОС, по мнению исследователей, приобретает работа по созданию единого хранилища информации о позиции государств по вопросам применения международного права в контексте международной ИКТ-безопасности и практике их адаптации на национальном уровне. При этом эксперты обращают внимание на то, что для повышения эффективности деятельности рабочих площадок ООН работа по адаптации государств к цифровому вызову должна вестись и в рамках региональных форматов сотрудничества, на полях международных организаций и объединений (СНГ, ОДКБ, ШОС, АСЕАН, ОБСЕ, БРИКС и др.)[58].

Несмотря на позитивные подвижки, работа по формированию международных правил поведения государств в киберпространстве, по мнению исследователей, по-прежнему далека от завершения, характеризуется прерывистой динамикой и зачастую реализуется в рамках более крупных переговорных процессов, связанных с обеспечением стратегической стабильности[59]. Определенное влияние оказывает и фактор отсутствия четких

---

[56] ГПЭ по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Нью-Йорк, 2013.
[57] Ромашкина Н.П. Проблема международной информационной безопасности в ООН // МЭМО. 2020. № 12. С. 28–29.
[58] Международная информационная безопасность: подходы России. С. 24–32.
[59] Хлопов О.А. Проблемы кибербезопасности в деятельности ООН // Системный анализ и синтез моделей научного развития общества. 2021.№ 3. С. 69.

разграничений между национальным и международным сегментами Интернета. Нередко международные проекты, продвигаемые под эгидой глобальных акторов (прежде всего, РФ и США), содержат противоположное видение будущего развития мировой системы информационной безопасности и, фактически, ведут к разделению позиций стран – членов ООН. Аналогично обстоит дело и в экспертной среде: несмотря на то, что параллельное функционирование ГПЭ и РГОС призвано ускорить разработку рекомендаций для ООН и сгладить разногласия, фрагментация по фундаментальным вопросам сохраняется, что вкупе с наращиванием большинством государств мира наступательных киберсредств создает опасный тренд, повышая общемировую конфликтность.

Немаловажную роль в пробуксовке международных инициатив в области киберзащиты играют опасения государств утратить свой информационно-технологический суверенитет – право самостоятельно формировать национальную политику в области ИКТ (включая контроль над информационными потоками и их вектором), а также определять допустимую степень вовлеченности других акторов в национальную киберповестку.

Так, например, широко распространенная сегодня практика заимствования за рубежом готовых цифровых решений с целью повышения общего уровня технологического развития и быстрого наращивания собственных позиций в мировой экономике, фактически, порождает зависимость от передовых держав мира, ведет к размыванию суверенитета развивающихся стран и может трактоваться как одно из проявлений «цифрового колониализма»[60]. Другим примером, подтверждающим данный тезис, может служить феномен «импорта мозгов» – привлечения иностранных специалистов в чувствительные отрасли экономики вместо развития национального кадрового потенциала[61]. В этой связи лояльность аравийских монархий к импорту западных технологий, в том числе в сфере

[60] Kwet M. Digital colonialism // Race & Class. 2019. № 4. P. 13–15.
[61] Schneider N. Governable stacks against digital colonialism // Communication & Critique. 2022. № 1. P. 30.

кибербезопасности, подвергается критике в трудах исследователей[62]. Алармистские суждения сторонников идеи «цифрового колониализма» разделяют далеко не все исследователи, считая, что международное сотрудничество в области кибербезопасности возможно без взаимного ущемления национальных интересов, поскольку государства свободны в выборе своих партнеров и определении степени своего участия в технологическом взаимодействии, а для продвижения профильной кооперации им следует развивать «цифровое доверие»[63].

Европейские исследователи считают, что сложившийся к настоящему времени международный режим кибербезопасности, в рамках которого государства уклоняются от формального многостороннего сотрудничества, а необязательный характер соглашений об «ответственном поведении» стал нормой, символизирует рост неформальности в современном глобальном управлении. Это обусловлено в первую очередь переходом мировой системы к многополярности, что серьезно осложняет формальное сотрудничество. Другая причина связана со значительным расширением субъектного поля международной кибербезопасности и увеличением количества негосударственных акторов, прежде всего в лице профильных бизнес-структур, которые включаются в цифровые международные отношения преимущественно в качестве неформальных участников, а их технические стандарты де-факто становятся стандартами управления[64].

Придать позитивный импульс международному сотрудничеству в области кибербезопасности, по мнению российских экспертов, способна постепенная унификация правовых, институциональных, технологических и иных аспектов цифровой деятельности[65]. Преодоление разночтений позволит ускорить продвижение профильных инициатив на региональном и глобальном

---

[62] Douzet F. Pétiniaud L., et. al. Digital routes and borders in the Middle East // Territory, Politics, Governance. 2023. №6. P. 1076-1077.
[63] Веселов Ю. В. Доверие в цифровом обществе // Вестник СПбГУ. Социология. 2020. № 2. С. 129–143.
[64] Sukumar A., Broeders D., et. al. The pervasive informality of the international cybersecurity regime // Contemporary Security Policy. 2024. № 1. P. 7–11, 25–26, 32–34.
[65] Международная информационная безопасность: подходы России. С. 30.

уровнях, а также будет способствовать эффективному противодействию угрозам из киберпространства.

Таким образом, исследовательское поле международной информационной безопасности, интегральной частью которой является кибербезопасность, характеризуется высоким уровнем дискуссионности, что обусловлено относительной новизной тематики и ее многоаспектным характером, несформированностью научно-терминологического аппарата, доктринальными разногласиями между государствами, а также разницей концептуальных подходов, принятых в тех или иных научных школах.

В целом можно резюмировать, 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 кибербезопасности на национальном и международном уровнях и может реализовываться в формате двустороннего и многостороннего, а также формального и неформального взаимодействия. В рамках данного исследования в качестве системы координат приняты методологические материалы ООН (как наиболее проработанные и в целом поддерживаемые ведущими государствами мира, прежде всего в лице России и США, а также аравийскими монархиями) – концепция «триады ИКТ-угроз» и оценочная система МСЭ касательно уровня готовности современных государств к реагированию на цифровой вызов.

1.2. Методологические основы исследования

Теоретической основой данного исследования стали концепции *неореализма (структурного реализма)*. Неореалистская парадигма базируется на идее о том, что государство является главным актором международных отношений, которые существуют в состоянии перманентной анархии, а в основе политики любого актора неизменно лежит сила. Цифровые технологии обеспечили современные государства 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[66]. Трансформация международных отношений под влиянием цифрового фактора предоставляет богатый эмпирический материал для научного осмысления и дальнейшего развития идей основоположников неореализма.

В условиях цифровой эпохи международные отношения остаются в состоянии «перманентной анархии», которое, как подчеркивал К. Уолтц, не тождественно хаосу и означает скорее отсутствие иерархии (управления), а понятие «сила» не ограничивается только военно-политической составляющей и подразумевает иные возможности влияния государства на других акторов (территория, население, индустриальные ресурсы, экономический потенциал, политическая стабильность и т.д.). Цифровое измерение приобретает и «дилемма безопасности» К. Уолтца, в контексте которой увеличение безопасности одного государства неизбежно снижает уровень защищенности других. Для анализа международного сотрудничества в области кибербезопасности весьма продуктивна также концепция относительной (ожидаемой) выгоды К. Уолтца: даже в случае взаимовыгодного сотрудничества (абсолютной выгоды) каждая из сторон

[66] Munawar S., Afzal S., et. al. Realism: revisiting the concept of power in the age of information // Global Strategic & Security Studies Review. 2021. № 6. P. 128–137.

будет опасаться, что другая воспользуется полученными преимуществами для нанесения урона своему партнеру[67].

Проблема влияния анархии на международное сотрудничество получила развитие в трудах Дж. Грико. Согласно концепции автора, анархичная природа международных отношений накладывает жесткие ограничения на поведение государств, ставя их в условия выживания. Это значительно затрудняет международную кооперацию, ограничивая ее рамками безопасности, где ключевая роль отводится фактору силы. При этом относительная выгода государства трактуется Дж. Грико как препятствие к тому, чтобы другие акторы получили преимущества, поэтому главным структурным элементом международных отношений является конфликт, а международная кооперация реализуется преимущественно в военно-политической сфере[68].

Концепция «гегемонистской стабильности» Р. Гилпина развивает идею многомерности понятия «сила», а именно возможности перераспределения силового ресурса в другие сферы, прежде всего экономические. Для исследования международных отношений на цифровом треке, в том числе в сегменте кибербезопасности, важны следующие теоретические положения концепции Р. Гилпина:

– конечным «арбитром» в мировой политике является силовой фактор, который определяется не только военными, но экономическими возможностями (ресурсами) государства;

– политическое влияние актора определяется в том числе его интегрированностью в мировые экономические процессы;

– международная экономическая стабильность может рассматриваться как относительная выгода (общее благо), но ее системообразующим элементом может стать только государство-гегемон либо группа государств, претендующих на лидерство;

---

[67] Waltz K. Theory of international politics. Reading, 1979.
[68] Grieco J. M. Anarchy and the limits of cooperation // International Organization. 1988. № 3. P. 485–507.

– в отсутствии гегемона государства сосредоточены на обеспечении национальной безопасности и политическом соперничестве, что ведет к экономической нестабильности[69].

Для монархий Залива и других стран арабского мира подобный подход к сотрудничеству, с одной стороны, видится наиболее уместным и эффективным: он не требует уступок части государственного суверенитета во имя «общего блага» и не препятствует наращиванию национального военного потенциала. Он также предусматривает развитие международного сотрудничества с различными субъектами международной безопасности, и при этом наличие формальных соглашений и институтов не является обязательным, поэтому взаимодействие может осуществляться в формате гибкого диалога. Диверсификация экономик в рамках стратегических программ «Видение», где цифровизации отводится роль одного из ключевых драйверов социально-экономических преобразований, позволяет аравийским монархиям интегрироваться в мировые экономические процессы в качестве сильных игроков. Это способствует увеличению геополитического веса рассматриваемой группы государств и выводит их в число лидеров Ближнего Востока и арабского мира.

С другой стороны, международная кооперация на Ближнем Востоке и в зоне Персидского залива представляет собой довольно непростую задачу. Прежде всего, сохраняющаяся зависимость от технологической, кадровой и иной помощи извне предопределяет преимущественную ориентацию внешнеэкономических связей аравийских монархий на технологически более развитых внерегиональных партнеров, сужая поле для взаимодействия с другими арабскими странами. Кроме того, процесс сближения в области безопасности (особенно в такой чувствительной области, как кибербезопасность) осложнен чрезвычайно высоким конфликтным

[69] Gilpin R. The political economy of international relations. New Jersey, 2016.

потенциалом региона[70], порождающим атмосферу взаимной подозрительности и недоверия[71], тогда как концепция Р. Гилпина базируется на идее открытости и готовности государств к сотрудничеству.

Данное противоречие представляется возможным устранить в рамках обращения к теории «баланса угроз» С. Уолта, которая расширяет и дополняет теорию «баланса сил». В соответствии с подходом С. Уолта, безопасность государства достигается только при условии наличия у актора ресурсов, достаточных для доминирования над другими игроками. При этом доминирование не исключает возможности заключения союзов между государствами, которые, напротив, рассматриваются как способ укрепления собственных позиций на мировой арене и увеличения своего геополитического веса. При этом, согласно концепции «баланса угроз», государства стремятся к объединению не против наиболее сильного, как считал К. Уолтц, а против наиболее опасного, с их точки зрения, противника, а уровень угроз определяется его географической близостью, наступательным потенциалом и степенью заинтересованности в эскалации конфликта. Исходя из оценки рисков, государство выбирает одну из двух возможных стратегий поведения – «балансирования» (объединение с целью защиты от более сильного противника) или «примыкания» (сближение с державой, представляющей наибольшую опасность)[72].

Теория «баланса угроз» С. Уолта обеспечивает методологическим инструментарием исследование целого ряда сюжетов, связанных с развитием систем национальной кибербезопасности монархий Залива и кооперации государств перед лицом общих угроз, исходящих из цифрового пространства. В первую очередь речь идет о так называемой «иранской киберугрозе»: данный конструкт базируется на идее о том, что стремящийся к статусу

[70] Барановский В.Г., Наумкин В.В. Ближний Восток в меняющемся глобальном контексте: ключевые тренды столетнего развития // МЭМО. 2018. № 3. С. 5–19.
[71] Звягельская И.Д., Свистунова И.А. и др. Ближний Восток в условиях «негативной определенности» // МЭМО. 2020. № 6. С. 94–103.
[72] Walt S. The origins of alliance. N.Y., 1987. P. 147–167.

регионального лидера Иран быстрыми темпами наращивает свой наступательный потенциал (кибервооружения) и активно использует его для разрушительных атак на объекты критической инфраструктуры монархий Залива, а также в противостоянии со своими оппонентами (Саудовская Аравия, Катар, ОАЭ, Израиль, США и др.) в киберпространстве Ближнего Востока. Противодействие «иранской угрозе» стало одним из ключевых стимулов к сближению ОАЭ и Бахрейна с Израилем, завершившемуся подписанием «Соглашений Авраама» в 2020 г., которые, в свою очередь, позволили его участникам перевести сотрудничество в сфере цифровой защиты (в ее гражданском и военном сегментах) в открытый формат. Попытки использовать «иранскую киберугрозу» в качестве консолидирующей идеи предпринимались некоторыми аравийскими монархиями в процессе разработки ряда совместных проектов в области кибербезопасности, в том числе на платформе ССАГЗ, а также военных проектов с участием США и Израиля.

В рамках концепции «баланса угроз» С. Уолта представляется возможным выявить не только факторы активизации международного сотрудничества монархий Залива по вопросах кибербезопасности, но и комплекс причин, ограничивающих эффективность совместных форматов взаимодействия. Так, с одной стороны, стремление аравийских монархий развивать двусторонние и многосторонние связи с целью обеспечения международной кибербезопасности обусловлено схожим восприятием значимости консолидации усилий в противодействии триаде киберугроз – со стороны кибертерроризма, киберпреступности, а также государств-оппонентов и их прокси-сил, использующих ИКТ в качестве демонстрации своей силовой компоненты.

С другой стороны, эта схожесть подходов к определению круга киберугроз и их градации имеет свои пределы. Так, между аравийскими монархиями имеются разногласия по целому кругу вопросов. Например, какие именно исламистские группировки следует считать террористическими? Не

станет ли создание антииранского киберфронта стимулом для Ирана форсированно наращивать свой наступательный киберпотенциал и наносить ответные удары по критической инфраструктуре своих арабских оппонентов? В итоге монархиям Залива пока не удается достичь «баланса угроз» даже в рамках переговорного процесса на площадке ССАГЗ, а с выходом на другие региональные форматы сотрудничества, ЛАГ или ОИС, спектр мнений кратно возрастает. Более выпукло эти разногласия проявляются, когда речь заходит о формировании тактических альянсов с участием неарабских региональных игроков, в первую очередь Израиля. Показательным примером может служить американский проект «Ближневосточного стратегического альянса», который породил серьезные дискуссии в ССАГЗ по вопросу о допустимых пределах сотрудничества с Израилем в части обеспечения безопасности на Ближнем Востоке, в том числе безопасности регионального цифрового пространства.

Тем не менее, несмотря на наличие многочисленных разногласий, процесс строительства безопасной цифровой среды на Ближнем Востоке и в арабском мире демонстрирует в целом положительную динамику. Это свидетельствует о том, что региональные игроки все же способны найти точки соприкосновения в вопросах обеспечения безопасности. В данном ракурсе при анализе проблем кооперации монархий Залива продуктивным будет обращение к концепции секьюритизации Б. Бузана и О. Уэйвера. Преимущество их подхода состоит в том, что в основе анализа международного сотрудничества лежит концепт безопасности, а субъектное поле исследования расширяется за счет негосударственных акторов (системных и внесистемных). В вопросах градации угроз безопасности предложен секторальный принцип: военный сектор, экономический, политический, социальный, экологический. Авторы выделяют 4 типа региональных комплексов безопасности. Ближний Восток отнесен к стандартному типу: он имеет анархичную основу, системообразующим фактором выступает военно-политическая сфера, а отношения между ведущими региональными державами (дружба – вражда) являются

определяющими для малых и средних игроков, а также принимаются в расчет внерегиональными акторами[73].

При экстраполяции данного подхода на проблемы кибербезопасности монархий Залива угрозы «высшего порядка» также обнаруживаются в военно-политической сфере. В военном секторе – это гонка кибервооружений и использование ИКТ в военном конфликте. В политическом секторе определяющими выступают угрозы размывания суверенитета под влиянием цифрового фактора и потери суверенитета в случае отставания в глобальной технологической гонке. В экономическом кластере ландшафт угроз охватывает, в первую очередь, критически значимые отрасли экономики аравийских монархий (нефтегазовый сектор, финансовый, ИКТ и т.д.). В социальном секторе угрозы связаны с проецированием на виртуальный мир проблем, имеющих религиозную или социальную подоплеку, а также постепенным уходом различных социальных групп и индивидов в «ИКТ-идентичность»[74], где последние приобретают гораздо б*о*льшие свободы в сравнении с физическим миром и получают возможность игнорировать физические границы и правовые нормы государств. И, наконец, угрозы экологического характера могут возникнуть, например, в результате кибердиверсий на нефтегазовых и иных объектах критической инфраструктуры.

В ближневосточном комплексе безопасности определяющими для региональных и внерегиональных акторов являются отношения по линии Саудовская Аравия – Иран, арабский мир – Израиль, Иран – Израиль, а в качестве ключевой общей угрозы выступают высокий уровень конфликтности и военно-политическая нестабильность. Однако неоднократные попытки выстроить на Ближнем Востоке систему региональной безопасности путем продвижения идеи единства перед лицом общей угрозы неизменно заканчивались неудачей ввиду исключительного социально-экономического,

[73] Buzan B., Waever O. Regions and powers. Cambridge, 2003.
[74] Carter M., Grover V. Me, My Self, and I(T) // MIS Quarterly. 2015. № 4. P. 931–932.

политического и этноконфессионального разнообразия и внутренней противоречивости региона[75].

В рамках анализа роли внешних акторов в развитии международного сотрудничества монархий Залива в области кибербезопасности весьма продуктивно обратиться к концепции наступательного реализма Дж. Миршаймера[76]. Аравийские монархии, будучи рациональными акторами международных отношений, действуют эгоистически, исходя из своих национальных интересов («операциональных целей»), которые (по Дж. Миршаймеру) сводятся к увеличению национального благосостояния (на что, собственно, и нацелены стратегические программы «Видение» и цифровизации, и, соответственно, создание высокоэффективных систем национальной киберзащиты) и повышению своего регионального статуса, в том числе за счет силовой компоненты (высокотехнологичные вооружения, включая кибервооружения). При этом для реализации своих национальных интересов («операциональных целей») аравийские монархии пытаются идти как по пути сохранения статус-кво на региональной и глобальной аренах, продолжая накапливать свой силовой ресурс, так и по пути продвижения к региональному лидерству («локальная гегемония»). В этих процессах значимая роль отводится «внешним стабилизаторам» («offshore balancers»). В число последних уместно включить США, КНР, Индию, страны Европейского союза, Республику Корея, Японию, вносящих внушительный вклад в развитие национального киберпотенциала монархий Залива, а также Россию, отношения с которой в последние годы приобретают восходящий вектор развития.

В ходе исследования системы сдержек и противовесов на Ближнем Востоке, которые неизменно проецируются на сферу международного сотрудничества монархий Залива в области кибербезопасности,

---

[75] Звягельская И.Д., Богачева А.С. и др. Политическая идентичность и ее влияние на внешнюю политику государств Ближнего Востока // Восток. 2020. № 2. С. 55–68; Кузнецов В.А. Арабские общества эпохи неомодерна // Восток. 2020. № 2. С. 28–40.

[76] Mearsheimer J. The tragedy of great power politics. N.Y., 2001.

продуктивным видится обращение к концепции «гегемонии нового типа» З. Бжезинского[77]. Несмотря на то, что она отражает американское видение проблем глобальной безопасности, данная концепция позволяет довольно эффективно определять внешнеполитические интересы монархий Залива, так как они, по сути, стремятся к сохранению текущего глобального баланса сил.

С течением времени геополитическая борьба выходит за рамки противостояния «атлантистов» и «континенталистов» (в более широком смысле – приморских и сухопутных держав), а акценты в геостратегических подходах смещаются в сторону попыток «проецирования» успешно работающих региональных проектов на глобальный уровень. Это ведет к формированию нового миропорядка, воспроизводящего в мировом масштабе черты наиболее эффективной системы управления процессами безопасности (сам З. Бжезинский подразумевает американскую и евроатлантическую модели) и постепенно распространяющего его на все региональные подсистемы. В условиях продолжающейся цифровизации информационное пространство (как общемировое, так и его отдельные сегменты) постепенно превратилось в один из уровней комплексной системы безопасности, требующий выработки особых методов регулирования.

Поскольку монархии Залива стремятся сохранить имеющуюся на Ближнем Востоке систему сдержек и противовесов, «антигегемонистская коалиция» (Китай, Россия, Иран, а также Турция, претендующая на роль регионального лидера и полюса силы), возможность создания которой З. Бжезинский считал одной из наиболее серьезных угроз для американского внешнеполитического доминирования, не отвечает их национальным интересам. С целью не допустить формирования геополитической оси «Россия – Китай – Иран – Турция» (в том числе в киберпространстве) аравийские монархии диверсифицируют свои внешнеполитические связи, расширяя сотрудничество в двусторонних и многосторонних форматах с Китаем,

[77] Бжезинский З. Великая шахматная доска. М., 2009.

Турцией и Россией, в том числе в рамках создания тактических альянсов (например, по линии Катар – Турция).

В рамки американской «стратегии балансирования» укладываются многочисленные инициативы США по повышению цифровой безопасности монархий Залива, своих ключевых региональных союзников. Вместе с тем при выстраивании архитектуры безопасности на Ближнем Востоке США проявляют определенную непоследовательность: подталкивая Саудовскую Аравию к нормализации отношений с Израилем и присоединению к «Соглашениям Авраама», Вашингтон, по сути, создает в регионе серьезный дисбаланс сил, который будет воспринят Тегераном как продолжающееся строительство антииранского фронта, что грозит новым витком напряженности, в том числе в киберпространстве.

Говоря о теоретико-методологических наработках З. Бжезинского, следует также упомянуть сформулированную им концепцию «технотронного общества», в основе которой лежат идеи «всемирности» и «всеохватности» передовых технологий[78]. Концепция базируется на идее возрастающего влияния технологий на международные отношения и мировую политику, в связи с чем их умелое использование позволит добиваться значительных геополитических успехов при меньших экономических затратах. Подход Бжезинского во многом заложил основу американского видения роли цифровых технологий (в дальнейшем – инструментов обеспечения кибербезопасности) как в вопросах позиционирования США на международной арене, так и в выстраивании диалога со своими стратегическими союзниками на Ближнем Востоке, что довольно ярко проявилось в период президентства Б. Обамы (2009–2017 гг.), Д. Трампа (2017–2021 гг.) и Дж. Байдена (2017 – наст. вр.).

Аравийские монархии, по сути, разделяют идеи «технотронного общества», признавая ведущую роль передовых технологий в формировании

[78] Brzezinski Z. Between two ages. America's role in the technetronic era. N.Y., 1970.

современного общества во всех его аспектах (экономических, политических, социальных, культурных, психологических и т.д.). Об этом свидетельствует тот факт, что идеи технологического лидерства, цифровизации и построения «защищенного цифрового общества» интегрированы в национальные стратегии долгосрочных экономических преобразований «Видение» в качестве базовых элементов[79].

Вместе с тем монархии Залива с большим опозданием включились в глобальную технологическую гонку, и по этой причине в вопросах реализации своих масштабных программ диверсификации национальных экономик делают ставку на международное сотрудничество и помощь извне. Это формирует зависимость от передовых технологических держав, прежде всего США и КНР, которые, в свою очередь, реализуют в странах Персидского залива собственные национальные интересы (используя при этом принципиально разные стратегии) и не заинтересованы в технологическом суверенитете своих аравийских партнеров.

Неравномерность в распределении ИКТ, включая технологии кибербезопасности, ведет к образованию цифрового разрыва, прежде всего по линии Глобальный Север – Глобальный Юг, а отношения между ведущими технологическими державами и оказавшимися у них в технологической зависимости странами все более начинают напоминать отношения между метрополией и колонией, что позволяет исследователям ввести в политический лексикон термин «цифровой колониализм»[80]. В данном контексте представляется возможным рассматривать монархии Залива в качестве объекта «цифрового колониализма» США и КНР, которые с большим отрывом лидируют на рынках ИКТ арабских стран Персидского залива. Однако расширяющееся сотрудничество с арабским миром и странами

[79] См., напр.; Saudi Vision 2030. Riyadh, 2016; Bahrain Economic Vision 2030. Manama, 2008; Kuwait Vision 2035. El Kuwait, 2019, и др.

[80] Crosston M. Cyber colonization // Cyber, Intelligence, and Security. 2020. № 1. P. 149–171; Карасев П. Цифровой колониализм vs цифровое неприсоединение // РСМД. 8.11.2021. URL: https://russiancouncil.ru/analytics/tsifrovoy-kolonializm-tsifrovoe-neprisoedinenie/ (дата обращения: 21.01.2022).

Африки, большинство из которых только начинаю погружаться в цифровые реалии, свидетельствует о том, что и сами аравийские монархии, экспортируя ИКТ в государства Глобального Юга, трансформируются в субъект «цифрового колониализма».

В целом, следует отметить, что влияние цифровых технологий на мировую политику изучается преимущественно в рамках теорий международных отношений, базирующихся на парадигме технологического детерминизма, которая рассматривает технологии не только как движущий, но и независимый, автономный фактор общественных трансформаций, в том числе в сфере международных отношений и внешней политики (см., например, труды А. Тоффлера, Е.Б. Скольникова, Д.Г. Балуева и др.)[81], а также области военного сотрудничества[82].

Вместе с тем даже между исследователями, проводящих анализ в рамках неореалистской парадигмы, имеется ряд существенных разногласий по вопросу о роли информационных технологий в процессе трансформации международных отношений и политического развития современных государств. Примером может служить дискуссия о влиянии технологии искусственного интеллекта на «дилемму безопасности», когда усиление киберпотенциала одного актора неизбежно воспринимается другими игроками как угроза. Ряд исследователей считает, что в случае повсеместного внедрения в силовую компоненту современных государств ИИ-технологий, которые не ограничены рамками морали при принятии решений, угроза «цифровой Хиросимы» (применения кибервооружений, чей кумулятивный эффект может быть сопоставим с ядерным ударом) из гипотетической может перейти в разряд реальных[83]. Другие, напротив, рассматривают

---

[81] Toffler A. Powershift: knowledge, wealth, and violence in the 21st century. N.Y., 1990; Skolnikoff E.B. The elusive transformation: science, technology, and the evolution of international politics. Princeton, 1994; Балуев Д.Г. Информационная революция и современные международные отношения. Н. Новгород, 2001.

[82] Козюлин В.Б. Многостороннее сотрудничество в области регулирования использования технологий искусственного интеллекта. М., 2021; Mihalka M. Cooperative Security in the 21st Century // Connections. 2005. № 4. P. 113–122; Iqbal S., Rizvi S., et. al. Artificial Intelligence in security and defense // International Journal of Human and Society. 2023. № 4. P. 341-353.

[83] Ibid.

искусственный интеллект как инструмент взаимного сдерживания ввиду его способности смоделировать и продемонстрировать разрушительные последствия подобного столкновения для всех его участников[84]. Не менее показательный пример – дискуссия о деструктивном влиянии информационных технологий на трансформацию Вестфальской системы международных отношений и развитие экономически отсталых либо погруженных во внутренние конфликты государств, в первую очередь стран Ближнего Востока и Африки[85].

В дискуссии о взаимовлиянии цифровых технологий и международных отношений главным оппонентом неореализма выступает социальный конструктивизм. В отличие от технологического детерминизма, конструктивистский подход позволяет выявить социальный контекст преобразовательного потенциала технологий, влияние на них социальных отношений и структур, в том числе во внешнеполитическом измерении[86].

Применительно к теориям международных отношений аналитический и эвристический потенциал социального конструктивизма обусловлен возможностью изучать влияние политической сферы на научно-технический прогресс, теоретически обосновать тезис о том, что технологии не являются политически нейтральными и со временем сами становятся предметом политического соперничества (в том числе на международном уровне), которое, в свою очередь, способно корректировать и даже ограничивать динамику и направления технологического развития, а также определять внешнеполитический выбор государств в вопросах международного сотрудничества в сфере цифровых технологий[87]. В рамках конструктивистского подхода представляется возможным включить в анализ международного сотрудничества в области информационной безопасности

---

[84] Arslan A. Neorealist analysis of security dilemma in cyberspace. Washington, 2023. P. 34, 41, 54.

[85] См.: напр.: Лебедева М.М., Зиновьева Е.С. и др. Архаизация государства: роль современных информационных технологий // Полис. 2016. № 6. С. 22–36.

[86] Herrera G.L. Technology and international transformation. N.Y., 2007.

[87] Haas P. Epistemic communities and international policy coordination // International Organization. 1992. № 1. P. 1–35.

форматы многоуровневой дипломатии, которая предполагает участие не только государств, но также бизнеса, гражданского общества, научно-академических сообществ[88].

Вместе с тем следует признать, что современная международная система сохраняет свои этатистские характеристики, ввиду чего государствам отводится ведущая, координирующая роль и в многоуровневом взаимодействии всех субъектов информационной безопасности, 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 нашем случае речь идет о трудах М. Кастельса, одного из крупнейших исследователей информационной эпохи и проблем новой экономики. Опора на его концепцию «сетевого общества»[89] позволяет 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. Концепт «сетевого общества» (в том числе положение о том, что децентрализация организованных экономических структур за счет автономных филиалов и электронных рынков позволяет провести эффективный охват экономического пространства[90]), раскрывается при анализе программ развития «Видение», отражая их суть и задавая ключевые параметры, к соответствию которым стремятся монархии Залива (создание инновационных сред, децентрализация финансовых потоков, формирование сетевых предприятий и пр.)[91].

---

[88] Зиновьева Е.С. Мирополитическая концептуализация международного научно-технического сотрудничества. С. 242–254.
[89] Castells M. The rise of the network society. Oxford, 2011.
[90] Ibid. P. 302-304, 311-312; Castells M. The Internet galaxy. Oxford, 2002.
[91] См., напр.: The UAE Vision. Abu Dhabi, 2023; Oman Vision 2040. Muscat, 2021; Qatar National Vision 2030. Doha, 2008.

При этом особенности социально-экономического и историко-культурного развития «цифрового кластера» монархий Залива в некоторой степени предопределяют «догоняющий» тип развития его систем национальной кибербезопасности и отставание от лидеров глобальной технологической гонки. Так, медленная адаптация традиционных социальных структур к реалиям цифровой эпохи ведет к формированию специфических механизмов обеспечения киберзащиты, когда, например, киберполиция не только сосуществует, но и тесно взаимодействуют с шариатскими судами[92].

Таким образом, для комплексного анализа особенностей и трендов развития международного сотрудничества монархий Залива в сфере кибербезопасности наиболее эффективным, на наш взгляд, методологическим инструментарием располагает неореалистский подход. Он позволяет исследовать широкий спектр проблем, связанных с формированием цифрового измерения международной безопасности и трансформацией международных отношений под влиянием информационных технологий. Глобальная повестка, прежде всего разногласия между Россией и Западом о путях создания коллективной системы информационной безопасности, оказывают серьезное влияние на позиции стран Ближнего Востока и выбор ими внешнеполитических ориентиров. Эти разногласия обусловлены не только разными доктринальными и правовыми подходами к решению обозначенной проблемы, но также логикой развития современного мирополитического процесса, характерной чертой которого является соперничество ведущих государств мира за глобальное и региональное лидерство, неизбежное в условиях незавершенности перехода системы международных отношений в качественно новое состояние.

[92] Maghaireh A. Shariah law and cyber-sectarian conflict // Intern. Journal of Cyber Criminology. 2009. № 2. P. 340.

ГЛАВА 2
ТРЕНДЫ РАЗВИТИЯ НАЦИОНАЛЬНЫХ СИСТЕМ КИБЕРБЕЗОПАСНОСТИ МОНАРХИЙ ЗАЛИВА

2.1. Аравийские монархии в условиях цифрового вызова

Одной из характерных черт развития систем кибербезопасности монархий Залива является их относительно поздний старт. Это обусловлено тем, что процессы цифровизации здесь начались лишь в конце 1990-х гг., почти на десятилетие позже, чем в государствах Глобального Севера. Тем не менее аравийские монархии довольно быстро включились в глобальную технологическую «гонку», однако интеграция в глобальное цифровое пространство породила комплекс новых угроз и вызовов национальной и международной безопасности.

Сегодня монархии Залива находятся в авангарде движения к цифровому обществу. За последнее десятилетие средний показатель проникновения Интернета в данной группе стран удвоился и по состоянию на 2023 г. составил 99,3%, превысив средний показатель государств Глобального Севера (96,8%); в ОАЭ, Саудовской Аравии, Катаре и Бахрейне численность интернет-пользователей достигла 100% населения, Кувейт и Оман близки к «точке максимума» (99,7% и 96,3% соответственно)[93]. Примечательно, что еще в 2022 г. ОАЭ были единственной страной мира с абсолютным показателем по данному параметру. Взрывной рост демонстрирует также показатель численности пользователей услуг мобильной Интернет-связи, который на конец 2023 г. составил 90 млн человек (см.: *Приложение I, Таблица 1*).

Повышение уровня проникновения Интернета, повсеместное распространение мобильных устройств, рост интернет-активности пользователей стимулировали развитие телекоммуникационного сектора и

[93] Individuals using the Internet // The World Bank. URL: https://data.worldbank.org/indicator/it.NET.user.ZSmost (accessed: 11.12.2023).

цифровой инфраструктуры аравийских монархий, одновременно поставив вопрос об их защите от кибератак. Мощный импульс развитию мобильного сектора кибербезопасности и совершенствованию инструментов реагирования на атаки злоумышленников в секторе связи, кроме того, придали пандемия COVID-19 и массовое внедрение технологий 5G[94].

Значимой вехой в развитии ландшафта кибербезопасности монархий Залива стало принятие в 2010-х гг. национальных стратегий «Видение» («Vision»), направленных на постепенную (к 2030–2040 гг.) диверсификацию экономик, прежде всего путем развития наукоемких отраслей. Масштабные преобразования ожидаемо оказали заметное влияние на трансформацию внешнеполитических приоритетов аравийских монархий, что нашло отражение в форсированном расширении связей с передовыми технологическими державами мира, прежде всего США, КНР, Республикой Корея и др.[95].

Цифровизация стала одним из ключевых драйверов социально-экономических преобразований в рамках «Видений», что стимулировало форсированное развитие национальных секторов кибербезопасности, прежде всего путем участия в глобальном профильном проекте Международного союза электросвязи под эгидой ООН. О тесной взаимосвязи между запуском масштабных программ социально-экономических трансформаций и стремительным развитием национальных систем цифровой защиты свидетельствует пример Саудовской Аравии и ОАЭ, которые после принятия стратегических программ «Видение» в 2016 г. (в случае с ОАЭ речь идет об обновлении стратегии 2010 г.) в период 2017–2020 гг. резко усилили свои позиции в мировом рейтинге готовности к отражению киберугроз, переместившись соответственно с 46 и 47 строчек на 2 и 5 (*см.: Приложение I, Таблица 2*).

[94] Annual Security Report 2023. Dubai, 2023. P.10, 14.
[95] Мелкумян Е.С. Арабские монархии Залива в XXI веке. М., 2023. С. 43–52.

Впечатляющие результаты экономической модернизации и цифровизации позволили монархиям Залива довольно быстро интегрироваться в глобальное цифровое пространство, однако при этом они стали мишенью для киберпреступного сообщества.

Согласно исследованию, проведенному специалистами Международного форума стран Залива в 2018 г., 74% предприятий стран – участников форума в качестве ключевой угрозы для бизнеса рассматривают угрозу незаконного доступа к чувствительной информации, тогда как среднемировой показатель не превышает 55%[96]. По данным IBM, к августу 2023 г. общая стоимость утечек ближневосточных компаний превысила отметку в 8 млрд долларов (самый большой показатель за прошедшее десятилетие), и свыше половины этой стоимости (4,4 млрд долларов) составили совокупные финансовые потери аравийских монархий[97].

Среди инструментов, используемых киберпреступниками, следует отметить программы-вымогатели и сложносоставное программное обеспечение, доля применения которых значительно возросла. Так, по состоянию на октябрь 2023 г., каждая четвертая атрибутированная атака на Ближнем Востоке содержит следы использования «программ-шантажистов», созданных в том числе с применением технологий искусственного интеллекта[98].

Актуальной угрозой для цифровой среды стран Залива остается фишинг – вид Интернет-мошенничества, целью которого является захват конфиденциальных пользовательских данных (паролей, логинов, контрольных и проверочных кодов и пр.). Международное консалтинговое агентство Proofpoint (США) фиксирует внушительный рост частоты фишинговых атак на пользовательскую мобильную инфраструктуру на глобальном уровне: так, если в 2022 г. злоумышленники совершали в среднем

[96] The new battlefront: cyber security across the GCC. Report. Washington, DC, 2018. P. 5.
[97] IBM Cost of a data breach. Report 2023. N.Y., 2023. P. 11, 14.
[98] Cybersecurity threatscape in the Middle East: 2022-2023. Moscow, 2023. P.7.

300 тыс. фишинговых атак ежедневно[99], то в 2023 г. – уже порядка 350 тыс. атак, а прогнозируемый экспертами показатель на 2024 г. варьируется от 370 до 450 тыс. мобильных кибератак[100]. Более того, доля успешных атак по сравнению с 2021 г. возросла в среднем на 76% (что, среди прочего, объясняется использованием злоумышленниками новых подходов к рассылке фишинговых материалов и более совершенного программного обеспечения), обусловив кратное увеличение совокупных прямых финансовых потерь пользователей и бизнеса[101].

В случае с монархиями Залива данный риск имеет наиболее выраженный характер, поскольку данная группа стран лидирует как на мировом, так и на ближневосточном уровне по темпам цифровизации, распространения технологий мобильной связи и прироста пользователей мобильного Интернета[102]. Вполне естественно, что государственные институты, отвечающие за разработку и реализацию политики национальной кибербезопасности, а также бизнес-структуры стремятся своевременно реагировать на этот вызов.

Специалисты IBM обращают внимание, что уровень осведомленности пользователей из аравийских монархий об основных способах кражи чувствительных данных злоумышленниками значительно возрос по сравнению со второй половиной 2010-х гг.[103]. Это обусловлено как влиянием фактора пандемии COVID-19, так и расширением практики проведения кампаний по повышению цифровой грамотности населения. Соответствующие инициативы запущены во всех монархиях Залива и реализуются с активным привлечением бизнес-структур из сферы кибербезопасности. По данным международной корпорации GBM, единственного официального представителя IBM в зоне Персидского залива,

---

[99] 2023 State of the Phish. Sacramento, 2023. P.19.
[100] 2024 State of the Phish. Sacramento, 2024. P. 19,22.
[101] Ibid, P.27.
[102] Mobile internet usage in MENA // Statista. URL: https://www.statista.com/topics/8710/mobile-internet-usage-in-MENA/topicOverview (accessed: 20.12.2023).
[103] 2024 State of the Phish. P. 38.

уже в первый год пандемии порядка 60% государственных и частных организаций аравийских монархий пересмотрели приоритеты в области защиты от несанкционированного доступа к своим данным и выразили готовность инвестировать в собственную кибербезопасность, а в 2022 г. их доля выросла до 84%[104].

Нефтегазовый сектор имеет критическое значение для экономик аравийских монархий и является наиболее уязвимым с точки зрения киберугроз. Учитывая, что предприятия по добыче и переработке нефти и газа, как правило, сосредоточены в узких географических областях, урон от возможных кибератак против них кратно возрастает. В последнее десятилетие саудовский нефтегазовый гигант Saudi Aramco и катарский RasGas неоднократно становились жертвами крупных нападений с использованием сложносоставных вирусных программ (2012, 2016, 2017, 2018, 2021 г.), нацеленных на нарушение производственного цикла или выведение из строя отдельных элементов цифрового периметра. Важно отметить, что в случае с монархиями Персидского залива нефтегазовый сектор имеет государственный статус. Поэтому нападения на производственные мощности Saudi Aramco или RasGas неизменно трактуются как угроза критической инфраструктуре и национальной безопасности, в связи с чем цифровая защита подобного рода объектов возлагается на государственные институты, а не на частные бизнес-структуры.

По состоянию на начало 2024 г. лидерами по числу кибератак (как отраженных, так и атрибутированных) являются Саудовская Аравия (2,23 тыс. кибернападений в месяц), ОАЭ (2,1 тыс.), Катар (1,4 тыс.) и Бахрейн (1,25 тыс.)[105]. Рост количества кибернападений, как правило, наблюдается в периоды подготовки и проведения крупных международных мероприятий (например, Dubai Expo 2020 и 2023, Чемпионат мира по футболу 2022 в Катаре

[104] Annual Security Report 2022. P. 19.
[105] По состоянию на 10.01.2024. См.: Kaspersky cyberthreat real-time map. URL: https://cybermap.kaspersky.com/ (accessed: 10.01.2024).

и т.п.). Несмотря на значительные усилия по наращиванию уровня национальной цифровой защищенности, Саудовская Аравия и ОАЭ продолжают возглавлять мировой рейтинг стран с наиболее дорогостоящими утечками данных[106], что связано не только с ростом количества кибернападений, но и кратным увеличением размеров выкупа, требуемого злоумышленниками за возвращение украденных данных[107].

По подсчетам экспертов, мероприятия по преодолению последствий кибератак в зоне Персидского залива занимают несколько месяцев, а средняя стоимость восстановительных работ для каждого из подвергшихся атаке объектов превышает 5 млн долларов[108]. Помимо серьезного финансово-экономического ущерба кибернападения наносят значительный репутационный урон.

Систематизация и анализ общего массива данных монархий Залива по типу утечек и хищений с использованием цифровых инструментов в 2023 г. позволяет выявить наиболее значимые для киберпреступников и иных злоумышленников сферы. Это материалы, связанные с государственными секретами (30%), коммерческими данными и деятельностью бизнес-структур (25,6%), персональными данными пользователей сети Интернет (19,8%), финансовыми данными (14,2%) и технологическими секретами (*см. Приложение II, Схема 1*).

Разумеется, большая часть подобных акций, в силу несовершенства используемых цифровых инструментов и зачастую относительно невысокой квалификации исполнителей, отражается системами киберзащиты объектов критической информационной инфраструктуры и не наносит им значительного ущерба. Однако риск проведения атаки «высшей степени сложности» полностью не исключается: подобные кибератаки несут в себе не только катастрофические финансовые последствия в виде повышения цен на

---

[106] Microsoft Digital Defense Report. Redmond, 2023. P. 51-52.
[107] UAE ransomware attacks decline but payout size grows // AGBI. 19.01.2024. URL: https://www.agbi.com/articles/uae-ransomware-attacks-decline-but-payout-size-grows/ (accessed: 30.01.2024).
[108] Internet infrastructure security guidelines for the Arab states. Washington, 2020. P. 6.

нефть и негативного каскадного воздействия на мировую экономику в целом, но и актуализируют угрозу применения цифровых вооружений, повышая и без того значительный конфликтный потенциал Ближнего Востока.

Вместе с тем скоординированные атаки «грубой силы» («brute force»), несмотря на кажущуюся примитивность используемых инструментов, в случае достижения ими критической массы, могут нарушить работу систем киберзащиты и нанести внушительный урон объектам критической инфраструктуры. Примером тому могут служить DDoS-атаки, чья основная цель – превысить предельную пропускную способность сети за счет генерации ложных запросов. По данным компании StormWall, специализирующейся на оказании услуг в области информационной безопасности, самая мощная DDoS-атака в 2023 г. достигла показателя 1,4 терабита в секунду на пиковой точке (т.е. порядка 400 млн запросов в секунду), что сопоставимо с суммарным среднесуточным объемом интернет-трафика Бахрейна или Кувейта[109]. Наличие подобной угрозы в совокупности с ростом доли координируемых атак на фоне очередного военно-политического кризиса на Ближнем Востоке вынуждает аравийские монархии активнее совершенствовать систему противодействия угрозе DDoS-атак.

Практика применения передовых цифровых технологий в межгосударственных конфликтах в качестве ударного средства получила распространение в начале 2010-х гг. после резонансной атаки с использованием сложного боевого компьютерного вируса нового поколения Stuxnet на ядерный сектор Ирана, осуществленной предположительно киберподразделениями США и Израиля с целью срыва иранской ядерной программы. Отсутствие в международном правовом поле прецедентов и соответственно практики выявления и наказания агрессора, а также оказания помощи жертвам атак с использованием киберсредств, приравненных к стратегическим наступательным вооружениям, вынудило Иран включиться в

[109] Отчет StormWall о DDoS-атаках за 2023 г. М., 2024. С. 9.

гонку кибервооружений и в короткие сроки выстроить комплексную систему национальной кибербезопасности с эффективными структурами и инструментами кибероборонны и проведения наступательных операций в киберпространстве[110].

Сегодня Ирану приписывается проведение серии масштабных кибератак на саудовский «Saudi Aramco» и катарский «RasGas» с применением боевого вируса Shamoon, разработанного на базе Stuxnet, и беспилотников, кибернападение на Управление электроэнергетики и водоснабжения Бахрейна, а также организация многочисленных хакерских акций, осуществленных контролируемой Тегераном так называемой иранской «киберармией»[111]. Широко применяемая Тегераном тактика нанесения масштабных ударов и «булавочных уколов» с использованием цифровых технологий вновь актуализировалась в связи с переходом противостояния Израиля и ХАМАС в вооруженную стадию осенью 2023 г., вынуждая монархии Залива держать национальные системы кибероборонны в состоянии повышенной готовности и расходовать внушительные финансовые средства на обеспечение стабильной работы ключевых объектов инфраструктуры, поскольку практически каждая успешная кибератака со стороны Ирана или его прокси-сил наносит существенный материальный, финансовый и имиджевый урон.

Несмотря на то, что, согласно последним исследованиям МСЭ ООН, по степени развитости киберсистемы Иран уступает большинству монархий Залива (за исключением Бахрейна и Кувейта), занимая 54 место в мировом рейтинге кибербезопасности и 8 место в ближневосточном[112], именно фактор «перманентной иранской угрозы» стал одним из основных стимулов для форсированного строительства национальных систем киберзащиты арабских

---

[110] Siboni G., Kronenfeld S. Developments in Iranian Cyber Warfare 2013–2014 // Military and Strategic Affairs. 2014. №. 2. P. 83–104.
[111] Baezner M. Iranian cyber-activities in the context of regional rivalries. Zurich, 2019. P. 6–15; Валиахметова Г.Н. Ближний Восток в цифровую эпоху // Восток. 2017. № 3. С. 7.
[112] GCI 2020. P. 26, 88.

монархий и приложения усилий в решении вопроса о создании форматов коллективного противодействия Ирану в киберпространстве, в том числе на площадке ССАГЗ[113]. Выдвижение Ирана на роль главного стратегического киберпротивника монархий Залива, кроме того, обусловлено длительной историей противостояния сторон, в основе которого лежат преимущественно политико-идеологические расхождения[114].

Хотя с момента атаки Stuxnet прошло почти 14 лет, работа по ее атрибутированию продолжается и затрагивает новых акторов, ранее не упоминавшихся в расследованиях. В частности, в 2024 г. стало известно, что Генеральная служба разведки и безопасности Нидерландов по просьбе спецслужб США еще в 2007 г. под видом подрядчика установила на иранском ядерном объекте в Натанзе оборудование со сниженным уровнем защиты, что впоследствии позволило внедрить вирус в систему управления. Примечательно, что, согласно опубликованным данным, содействие голландским агентам также оказывали представители ОАЭ[115]. Это косвенно подтвердило предположения о причастности монархий Залива к масштабному тестированию кибервооружений на Ближнем Востоке, которое осуществлялось предположительно США и Израилем в 2010–2012 гг.

В последующие годы практика нанесения ударов в киберпространстве в качестве элемента асимметричного конфликта получила на Ближнем Востоке значительное развитие. Наиболее известны эпизоды с применением боевых вирусов DuQu (2011 г.), Gauss (2012 г.), Flame (2012 г.), и Shamoon (2012 г., 2016 г.) против Ирана, Саудовской Аравии, Катара, Йемена, Израиля и ряда других стран[116]. Важно также отметить, что в зависимости от конкретной

---

[113] El-Masry A. The Abraham Accords and their cyber implications. URL: https://www.mei.edu/publications/abraham-accords-and-their-cyber-implications-how-iran-unifying-regions-cyberspace (accessed: 17.10. 2023); Baezner M. Iranian cyber-activities. P. 16–18.

[114] Косач Г.Г., Мелкумян Е.С. ССАГЗ как военно-политическая организация // Вестник Моск. ун-та. Сер. МОиМП. 2012. № 4. С. 52–58.

[115] Sabotage in Iran: een missie in duisternis // Volkskrant. 08.01.2024. URL: https://www.volkskrant.nl/kijkverder/v/2024/sabotage-in-iran-een-missie-in-duisternis/ (accessed: 20.01.2024).

[116] Zhioua S. The Middle East under malware attack dissecting cyber weapons. P. 1–6; От Shamoon к StoneDrill. Wiper-подобные программы атакуют компании в Саудовской Аравии и не только // SecureList. 06.03.2018. URL: https://securelist.ru/from-shamoon-to-stonedrill/30350/ (дата обращения: 21.10.2023).

задачи вредоносное ПО использовалось как для выведения из строя объектов критической инфраструктуры, так и для сбора чувствительной информации. Подобные атаки, как правило, интерпретируются как акт внешней агрессии и увеличивают вероятность ответного удара в киберпространстве[117].

Важно отметить, что в зависимости от сложности состава конкретного средства цифровой войны урон от его потенциального использования можно одновременно оценить и как незначительный, и как масштабный, характерный для случаев применения стратегических средств борьбы. Это обусловлено тем, что серьезный материальный и имиджевый ущерб государству можно нанести с использованием простого, но массового продукта – за счет перегрузки цифровой инфраструктуры атакуемого объекта (например, посредством DDoS-атак)[118]. По этой причине аравийские монархии не склонны определять дополнительную градацию ИКТ-вооружений, предпочитая рассматривать их в качестве единого, совокупного риска[119].

Другое направление развития силовой компоненты – программное обеспечение для кибершпионажа (в классификации НАТО – средств наступательной киберразведки). Аравийские монархии проявляют к данному типу ПО повышенный интерес, рассматривая его в качестве инструмента решения не только внешнеполитических, но и внутренних задач. Еще в 2015 г. появились первые сведения о причастности правительств Саудовской Аравии, Бахрейна, ОАЭ и Омана к закупке вредоносных цифровых инструментов и технологий шпионажа за рубежом[120], а в 2021 г. – свидетельства об использовании этих средств для проведения разведывательных операций на Ближнем Востоке. По мнению IT-экспертов, сегодня все государства Персидского залива в той или иной степени используют шпионское ПО для реализации своей внутренней и внешней политики, однако наиболее широко

---

[117] Демидов О.В., Черненко Е.В. Грозный ум на страже кибербезопасности. С. 155.
[118] Каберник В.В. Проблемы классификации кибероружия // Вестник МГИМО. 2013. №. 2. С.74.
[119] Cybersecurity threatscape in the Middle East. Moscow, 2023. P. 7-8.
[120] Неизвестные взломали сеть поставщика шпионского ПО для правительственных спецслужб // SecureLab. 06.07.2015. URL: http://www.securitylab.ru/news/473587.php (дата обращения: 21.12.2023).

эти технологии при решении государственных задач применяют ОАЭ и Саудовская Аравия. При этом значительная часть технологий, составляющих разведывательный цифровой инструментарий аравийских монархий, по оценкам экспертов, имеет иностранное происхождение[121]; о разработке собственных решений в настоящее время ничего не известно.

Сегодня лидером в разработке и поставках разведывательных кибертехнологий и иных цифровых средств защиты на Ближнем Востоке выступает Израиль, чья профильная индустрия во второй половине 2010-х гг. получила дополнительный импульс к развитию в свете краха иранской «ядерной сделки». В силу исторической специфики отношений с монархиями Залива передача технологий и инструментов обеспечения кибербезопасности долгое время осуществлялась Израилем через посредников преимущественно в лице европейских IT-компаний. С подписанием в 2021 г. «Соглашений Авраама» сотрудничество ОАЭ и Бахрейна на этом направлении расширилось, в то время как остальные арабские государства Залива (за исключением Кувейта) продолжили взаимодействие в кулуарном формате[122]. В целом сближение с Израилем в рамках развития национальных систем киберзащиты обеспечило большинство монархий Залива эффективными инструментами противодействия внешним оппонентам, борьбы с терроризмом и дискредитации диссидентов.

Относительно новым направлением развития модели применения киберсредств в военном деле можно считать использование технологий искусственного нейронного интеллекта (так называемая «нейросеть») для ускорения принятия оперативно-тактических решений. Прежде всего речь идет о возможности внедрения в систему управления смертоносными автономными системами (САС) бот-программ с генеративным искусственным интеллектом, которые в режиме реального времени способны анализировать боевой потенциал выявляемых угроз и моделировать способы

[121] Cybersecurity threatscape in the Middle East. P. 8.
[122] Bouks B. Israel’s strategic threats and challenges: security, influence & cyber // SSJ. 2023. № 1. P. 120.

противодействия им. По мнению разработчиков, это позволяет существенно сократить количество тактических ошибок, обусловленных влиянием человеческого фактора, а также повысить общую эффективность применения передовых ударных средств[123].

Следует отметить, что феномен «боевых нейросетей» пока не получил комплексной оценки в военной и экспертной среде монархий залива, но отдельные предложения по внедрению передовых практик в системы управления национальной обороны высказывались саудовскими и эмиратскими экспертами в рамках Глобального саммита по искусственному интеллекту «AI 2020» (2021 г.)[124].

Концепция «искусственного советника» также продвигается западными технологическими концернами (в первую очередь, американской «Palantir Technologies», специализирующейся на технологиях киберразведки и безопасности данных) и позиционируется как закономерный элемент развития национальных систем обороны, а отдельные решения напрямую тестируются на Ближнем Востоке. Так, например, «Palantir Technologies» с началом эскалации конфликта вокруг Сектора Газа в октябре 2023 г. заметно нарастила поставки программного обеспечения Израилю для повышения оперативных возможностей ЦАХАЛ, прежде всего в части ведения аэроразведки. Разработчики считают, что демонстрация военного потенциала искусственного интеллекта в условиях реальных боевых действий позитивно скажется на темпах его дальнейшего распространения, в том числе в странах Персидского залива[125]. С учетом общего для всех аравийских монархий стремления к повышению эффективности национальных вооруженных сил (в первую очередь, за счет наукоемких вооружений и цифровых решений)

---

[123] 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).

[124] AI militarization will be ‘force multiplier’ for UAE, Saudi Arabia // CISRNET. 24.02.2021. URL: https://www.c4isrnet.com/artificial-intelligence/2021/02/24/ai-militarization-will-be-force-multiplier-for-uae-saudi-arabia/ (accessed: 30.01.2024).

[125] Palantir supplying Israel with new tools since Hamas war started // Bloomberg. 10.01.2024. URL: https://www.bloomberg.com/articles/2024-01-10/palantir-supplying-israel-with-new-tools (accessed: 01.02.2024).

практика разработки и внедрения технологий искусственного интеллекта в качестве мультипликатора совокупной национальной военной мощи может стать более распространенной уже в среднесрочной перспективе.

Вместе с тем следует признать, что полноценный переход к использованию «боевых нейросетей» (даже в рамках отдельных командно-штабных учений, проводимых в монархиях Залива под эгидой НАТО) потребует существенной доработки национальных законодательств. Несмотря на то, что курс на внедрение технологий искусственного интеллекта закреплен в национальных стратегиях «Видение» в качестве одного из приоритетных направлений социально-экономического развития и довольно успешно реализуется на практике в последнее десятилетие, тем не менее механизмы нормативно-правового регулирования сферы нейросетей пока не проработаны или же затронуты только отдельные ее аспекты. Отсутствуют юридически обязывающие нормы регулирования боевого применение искусственного интеллекта и на глобальном уровне.

Другим важным фактором, ограничивающим возможности усиления военного потенциала современных государств за счет «боевых нейросетей», является проблема этичности их использования, которая отличается высокой степенью дискуссионности и неизбежно обостряет споры о «пределах допуска» искусственного интеллекта к процессу принятия решений. В случае со странами Залива данная проблематика дополняется вопросом о соответствии подобного рода новейших технологий этическим нормам ислама в целом[126]. В этом контексте аравийские монархии в случае внедрения технологий искусственного интеллекта в военную сферу могут не найти понимания в мусульманском мире, что чревато репутационными издержками и негативным влиянием на развитие сотрудничества с внешними партнерами в области кибербезопасности.

[126] Сюкияйнен Л.Р. Глобализация и мусульманский мир. М., 2012. С. 49–67.

Помимо государств, носителями угроз в киберпространстве Персидского залива и Ближнего Востока являются внесистемные акторы – кибергруппы, предположительно спонсируемые государствами или отдельными политическими группами; политически мотивированные хактивисты и хакеры-одиночки, которые, как правило, руководствуются теми или иными идеологическими парадигмами.

Особый исследовательский интерес представляет деятельность так называемых «киберармий» – хакерских команд, решающих оперативные задачи какого-либо государства (реже – группы государств) по нанесению урона оппонентам в киберпространстве, но отрицающих свои связи с государственными институтами. Одной из первых арабоязычных «киберармий» является команда «Соколы пустыни» («Desert Falcons»), которая проводила операции по кибершпионажу в период с 2013 по 2015 г. Набор ее цифровых инструментов, включающих в том числе уникальное многосоставное программное обеспечение, свидетельствовал о высоком уровне подготовки ее участников и наличии значительных финансовых ресурсов. Это позволило экспертам предположить, что за данной киберкомандой может стоять одно из арабских государств Залива[127].

Действительно, следует признать, что аравийские монархии проявляют к формату «киберармий» повышенный интерес, поскольку видят в них эффективный инструмент проведения внешней политики и борьбы за региональное влияние. Сегодня известно о деятельности как минимум трех группировок, на системной основе отстаивающих интересы Саудовской Аравии («Кибермухи»), ОАЭ («Цифровая армия ОАЭ») и Бахрейна («Цифровая армия Бахрейна»). С высокой долей вероятности аналогичные группировки созданы и другими странами Залива.

Из перечисленных выше «киберармий» особого внимания заслуживает предположительно саудовская хакерская команда «Кибермухи», которая была

[127] Kaspersky Security Bulletin 2015. URL: https://securelist.ru/kaspersky-security-bulletin-2015-razvitie-ugroz-v-2015-godu/27466/ (дата обращения: 15.12.2023).

создана в 2012 г. и стала не только первым подобного рода проектом, успешно реализованным в зоне Персидского залива, но и единственным, в котором наиболее полно представлено было политико-идеологическое измерение кибербезопасности. Так, при реализации операций против оппонентов Саудовской Аравии «Кибермухи», как правило, сочетают кибератаки (DDoS-атаки, туннелирование DNS, использование программ-вымогателей, взлом аккаунтов и пр.) с запуском комплексных информационно-психологических операций (сбор и развитие правительственных ботоферм, создание DeepFake-контента, «посев» позитивной или дискредитирующей повестки в социальных медиа и др.), в результате чего удается максимизировать эффект от проводимой акции и добиться информационного преобладания над оппонентом[128].

«Кибермухи» показали высокую эффективность в период катарского дипломатического кризиса 2017–2021 гг., реализовав несколько многосоставных операций против Катара и тем самым ухудшив его переговорные позиции. Отдельные дискредитирующие конструкты, созданные и раскрученные в рамках деятельности этой хакерской группировки (например, «посев» результатов «журналистского расследования» о вскрытии деятельности сети контролируемых государством каналов по отмыванию незаконных активов с помощью криптовалюты на территории Катара), по-прежнему оказывают негативное влияние на международный имидж Дохи и продолжают создавать определенные проблемы в вопросах его внутреннего развития (например, препятствуют либерализации национального законодательства в области торговли цифровыми активами)[129].

Несмотря на наличие комплексного подхода и его относительно высокую эффективность в рамках операций «Кибермух», другие страны

[128] Saudi Arabia seeks to tame powerful cyber armies // MENA. 08.07.2020. URL: https://menafn.com/1100598791/ (accessed: 20.01.2024).
[129] Ibid.

Залива на данный момент не проявляют интереса к тому, чтобы перенимать опыт Саудовской Аравии в области создания подобного рода группировок. Деятельность «киберармий», находящихся предположительно под контролем других аравийских монархий, как правило, ограничена проведением кибератак с использованием обычного хакерского инструментария или сотрудничеством с властями в вопросах выявления уязвимостей в системе национальной цифровой обороны с целью их дальнейшего устранения (например, в рамках программы взаимодействия с «белыми» хакерами «Bug Bounty»). Это объясняется как объективными причинами (нехватка профильных кадров, отсутствие специализированного программного обеспечения и пр.), так и субъективными факторами (страх перед «обратным эффектом» от информационных операций). Более того, большинство стран Залива постепенно ужесточает подход к регулированию работы социальных сетей и мессенджеров[130], что заметно усложняет проведение информационных акций даже в национальных интересах отдельных государств. В то же время аравийские монархии проявляют повышенный интерес к технологиям кибербразведки (функционал которых также позволяет проводить эффективные дискредитирующие мероприятия при меньших финансовых и иных издержках), ввиду чего вектор деятельности «киберармий» постепенно смещается в сторону получения доступа к чувствительной информации без использования инструментов социальных медиа.

Например, в 2016 г. стало известно о деятельности в ОАЭ проправительственной кибергруппировки «Соколы-невидимки» («Stealth Falcon»), атаковавшей аккаунты эмиратовских диссидентов и оппозиционных журналистов, а также правозащитников[131]. В отличие от упомянутых ранее саудовских «Кибермух», делавших ставку на работу с соцмедиа, проправительственные хакеры ОАЭ более активно использовали технологии

[130] Freedom on the Net. Berlin, 2023. P. 16, 23, 27, 29.
[131] Stealth Falcon group uses custom spyware, fake journalists to target UAE dissidents // CSO. 30.05.2016. URL: https://www.csoonline.com/article/3076178/stealth-falcon-group-uses-custom-spyware.html (accessed: 30.01.2024).

социальной инженерии и макровирусов (вредоносного кода, «вшитого» в текстовый документ, изображение или гиперссылку), что позволяло им проводить точечные и эффективные атаки без задействования социального ресурса («посев» в социальных сетях и мессенджерах). Кроме того, «Соколы» не объясняли свою деятельность патриотическими мотивами и отрицали какую-либо связь с государством (хотя де-факто руководствовались теми же целями, что и группировки, работавшие под эгидой оборонного «Project Raven»)[132].

Кроме того, в отличие от команды «Кибермухи», деятельность «Соколов-невидимок» имела несистемный характер, а эффект от проводимых атак и их периодичность стремительно снижались, что и обусловило ее «уход в тень» во второй половине 2010-х гг. и последующее вероятное поглощение другими сетевыми киберподразделениями (предположительно «Цифровой армией ОАЭ»). В то же время ряд экспертов допускает, что кибергруппировка продолжила свою деятельность в ограниченном формате и сосредоточилась на распространении вредоносного ПО в интересах ОАЭ – например, алгоритмов несанкционированного доступа (так называемый «бэкдор») «Deadglyph», обнаруженных на устройствах ряда ближневосточных оппозиционеров и журналистов в сентябре 2023 г.[133].

В рамках рассмотрения комплекса цифровых угроз в зоне Персидского залива особого внимания требует феномен кибертерроризма. Радикально-экстремистские и террористические группировки не оставляют попыток укрепить позиции в глобальном киберпространстве и используют цифровые инструменты для дестабилизации отдельных стран Ближнего Востока (так называемый «киберджихад»). Примером системных усилий джихадистов в киберпространстве можно считать их деятельность в период с 2015 по 2019 гг., когда в составе двух крупнейших радикальных группировок – ИГИЛ и Аль-

[132] Stealth Falcon // MITRE. URL: https://attack.mitre.org/groups/G0038/ (accessed: 01.02.2024).
[133] Deadglyph: new advanced backdoor with distinctive malware tactics // The Hacker News. 23.09.2023. URL: https://thehackernews.com/2023/09/deadglyph-new-advanced-backdoor-with.html (accessed: 30.01.2024).

Каиды – были сформированы киберподразделения («Объединенный киберхалифат» и «Цифровой батальон Ан-Немра» соответственно), специализировавшиеся на проведении кибератак, пропаганде и привлечении в свои ряды высококвалифицированных хакеров.

Сравнительные характеристики организационной структуры и деятельности киберподразделений указанных радикально-экстремистских группировок представлены в *Приложении I* (*Таблица 3*). Их анализ позволяет сделать вывод о том, что хотя деятельность киберподразделений ИГИЛ и Аль-Каиды была сосредоточена на достижении схожих стратегических целей (превращение киберпространства в полноценную арену борьбы с дальнейшим нанесением поражения противникам «халифата»), а радикальные хакеры использовали схожий набор приемов (отдавая предпочтение DDoS-атакам и краже чувствительных данных), круг их компетенций отличался. Так, например, хакеры ИГИЛ, будучи встроенными в организационную структуру группировки, имели прямой доступ к финансовым потокам, контролируя добычу и оборот цифровых активов, в то время как боевики «Цифрового батальона» использовались исключительно как ударная сила и де-факто действовали независимо от других структур Аль-Каиды. Кроме того, лояльные Аль-Каиде хакеры были заинтересованы во взаимодействии с другими кибергруппировками радикального толка, при поддержке которых им удавалось проводить более масштабные, по сравнению с ИГИЛ, кибератаки. Важно подчеркнуть, что, несмотря на открытый конфликт между ИГИЛ и Аль-Каидой, их киберподразделения не проводили ударных акций друг против друга. Пропагандисты обеих группировок в своих воззваниях к хакерскому сообществу многократно подчеркивали недопустимость обмена кибердарами до победы над «врагами ислама»[134].

В целом, можно заключить, что несмотря на идеологические расхождения (даже концепция «киберджихада» остается крайне

[134] Online Jihadist Propaganda 2021. P. 12, 15, 25.

дискуссионной в радикально-экстремистских кругах) и наработку собственных стратегий ведения борьбы в цифровом пространстве, киберподразделения террористических группировок все же предпринимают попытки сформировать «тактический альянс» для повышения общей эффективности проводимых ими кибераций. Кроме того, технические возможности и профессионализм участников «киберджихада» пока остаются в целом на относительно невысоком уровне, все же они демонстрируют устойчивую тенденцию к росту[135]. В этой связи аравийские монархии включают кибертерроризм в число наиболее значимых угроз национальной безопасности.

Хактивизм – политически мотивированные протестные акции с использованием информационно-коммуникационных технологий – также рассматриваются монархиями Залива в качестве серьезной угрозы, исходящей из цифрового пространства. Под влиянием событий «арабской весны» такая форма протеста получила значительное распространение в странах Ближнего Востока; тогда же сформировались и наиболее известные общеарабские хактивистские сообщества (например, «Arab Warriors Team» и «Moroccan Black Cyber Army»), которые действуют по сей день. Учитывая, что деятельность хактивистов в период «арабской весны» была сосредоточена во многом на критике действий правящих режимов монархий Залива, в некоторых из них (в частности, в Бахрейне) подобные хактивистские акции были оценены как социально опасное явление и в конечном итоге отнесены к разряду уголовно наказуемых деяний.

Тем не менее, по оценкам экспертов, степень влияния хактивистов на политику монархий Залива в области кибербезопасности, несмотря на предпринимаемые государственными структурами меры, продолжает расти: если в 2013 г. на их долю приходилось порядка 45% совершаемых

[135] Cyber Terrorism: Assessment of the Threat to Insurance. Cambridge, 2017. P. 13–15.

кибераций[136], то по итогам 2023 г. показатель вырос примерно на 14%, а атаки приобрели более комплексный характер, затронув в том числе банковский и медиасектор[137].

Серьезный всплеск активности хактивистов в цифровом пространстве аравийских монархий был зафиксирован в конце 2023 г. в связи с эскалацией конфликта вокруг Сектора Газа. С началом операции ЦАХАЛ против ХАМАС в октябре 2023 г. политически мотивированные хакерские группы и хакеры-одиночки объявили о своей готовности «бороться за справедливость»: в общей сложности, на начальном этапе конфликта к протестным акциям присоединились по меньшей мере 50 хактивистских команд и около 100 хакеров-одиночек (подавляющее большинство выступили с пропалестинских позиций)[138]. Атакам хактивистов подвергся не только Израиль (порядка 80% от атрибутированных кибератак), но и его союзники по «Соглашениям Авраама» (ОАЭ, Бахрейн)[139].

Усиление нагрузки на цифровую инфраструктуру ряда монархий Залива в связи с очередным всплеском хактивизма вновь актуализировало вопрос о совершенствовании методов киберзащиты. Кроме того, деятельность хактивистов в контексте кризиса в Секторе Газа негативно сказалась на отношениях аравийских монархий и Ирана, поскольку ряд участников протестных акций («Cyber Av3ngers», «Hizbullah Cyber Team» и др.) ранее были уличены в сотрудничестве с проиранскими киберкомандами[140]. Несмотря на то, что Тегеран отвергает выдвинутые против него обвинения, продвигаемая (прежде всего, с подачи США) информация о причастности

---

[136] Hacktivism the motivator of cyberattacks in Middle East // Gulf Business. 06.06.2013. URL: https://www.thenationalnews.com/business/hacktivism-the-motivator-of-cyber-attacks-in-middle-east (accessed: 24.01.2024).

[137] Cybersecurity threatscape in the Middle East. P.8.

[138] Pro-Hamas cyber groups target social media with disinfo designed to incite antisemitism // Polygraph. 18.10.2023. URL: https://www.polygraph.info/a/7315940.html (accessed: 27.01.2024).

[139] Hacktivists stoke Israel-Gaza conflict online // Reuters. 11.10.2023. URL: https://www.reuters.com/world/middle-east/hacktivists-stoke-israel-gaza-conflict-online-2023-10-11/ (accessed: 20.01.2024).

[140] Iranian hacktivist proxies escalate activities beyond Israel // CPB. 04.12.2023. URL: https://checkpoint.com/research/shift-in-cyber-warfare-tactics-iranian-hacktivist-proxies-extend-activities-beyond-israel/ (accessed: 20.01.2024).

Ирана к хактивистским акциям против монархий Залива в связи с палестино-израильским противостоянием в Секторе Газа снижает и без того невысокий уровень взаимного доверия между государствами по обе стороны Персидского залива и тормозит наметившуюся было ранее «цифровую разрядку» на Ближнем Востоке.

Таким образом, представляется возможным выявить три группы угроз, исходящих из цифрового пространства зоны Персидского залива и Ближнего Востока и формирующих цифровой вызов для аравийских монархий: киберпреступность, кибертерроризм и применения информационно-коммуникационных технологий 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.

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.

2.2. Уровень готовности к отражению киберугроз

Согласно методологии, разработанной экспертами ООН в рамках международного научно-исследовательского проекта «Глобальный индекс кибербезопасности», ключевыми критериями для оценки эффективности национальных систем цифровой защиты современных государств являются: нормативно-правовая система, технический потенциал, организационная структура, меры по развитию потенциала, международное сотрудничество. В рамках данного раздела обозначенные параметры будут рассматриваться также в контексте проблем развития сотрудничества аравийских монархий с внешними партнерами на двусторонней основе и в многосторонних форматах.

Нормативно-правовая система монархий Залива в сфере кибербезопасности. Выбор экспертами ООН нормативно-правовой системы в качестве основополагающего критерия оценки киберготовности государств обусловлен тем, что именно в законодательной плоскости закладывается модель реагирования страны на цифровой вызов, которая оказывает определяющее влияние на эффективность других важных составляющих национальных систем кибербезопасности.

Процесс развития правовых систем монархий Залива в разрезе реагирования на цифровой вызов представляется возможным условно разделить на несколько этапов.

Первый этап охватывает конец 1990-х гг. – 2006 г., когда закладывались основы правого регулирования цифрового пространства путем принятия нормативно-правовых актов по отдельным отраслям экономики (сектор телекоммуникаций, электронная торговля и др.).

Второй период – с 2007 г. по 2015 г. – ознаменовался включением в нормативно-правовую сферу социальных аспектов цифровой защиты и попытками адаптации зарубежного профильного опыта к местным реалиям ввиду стремительного внедрения цифровых технологий в различные сферы жизни общества и индивида и взрывного роста числа Интернет-пользователей.

Начало третьему этапу – с 2016 г. по настоящее время – было положено запуском программ «Видение», которые стимулировали процесс принятия «якорных» нормативно-правовых актов, в первую очередь, национальных законов о борьбе с киберпреступлениями, о несанкционированном доступе к информации, о защите персональной пользовательской информации, о мерах по уведомлению о нарушениях, об антиобщественном поведении в Интернете и т.д. (*см. Приложение I, Таблица 4*). Именно в данный период значительно активизировалось сотрудничество между монархиями Залива в сфере кибербезопасности (включая ее правовые аспекты) в двустороннем формате и на площадке ССАГЗ.

Согласно текущим оценкам МСЭ, все аравийские монархии, за исключением Кувейта, вышли на максимальные показатели по нормативно-правовому критерию (*см.: Приложение I, Таблица 5; Приложение II, Схема 2*), запустив после 2016 г. процесс адаптации национального законодательства к реалиям цифровой эпохи. Относительное отставание Кувейта от своих соседей по Заливу обусловлено тем, что нормотворческий процесс в области цифровой защиты стартовал лишь в 2014 г. в силу ряда причин внутреннего характера[141].

Вместе с тем следует констатировать, что, несмотря на высокие позиции в мировом рейтинге МСЭ ООН по нормативно-правовому обеспечению сектора кибербезопасности, подходы монархий Залива к регулированию цифрового пространства весьма разнятся, что препятствует формированию единого правового поля в рамках ССАГЗ. Позиции государств далеко не всегда совпадают даже в вопросах трактовки содержания базовых понятий и терминов и имеют ряд существенных отличий от юридической практики западных стран. Так, например, ряд монархий включает в понятие «киберпреступность» такие виды деятельности, как призывы к критике действий властей, координация массовых протестов и т.п.

[141] Abu-Taieh E. Cyber security crime and punishment: comparative study of the laws of Jordan, Kuwait, Qatar, Oman, and Saudi Arabia // IJCWT. 2018. № 3. P. 49.

Иллюстрацией к данному тезису может служить нормотворческий опыт Омана. Национальный Закон о киберпреступности (Королевский указ 12/2011), принятый в Султанате в 2011 г., ввел в правовой оборот сразу два смежных понятия – «киберпреступление» и «преступление, совершенное с использованием информационных технологий». К киберпреступлениям, согласно позиции оманских законодателей, относятся следующие типы деяний: цифровое мошенничество, посягательство на кредитные карты и иные платежные средства, распространение порнографических материалов в Интернете, посягательство на частную жизнь, незаконный доступ к закрытым порталам и веб-сайтам, кибертерроризм, вымогательство, организация незаконных торговых каналов в Интернете, совершение атак на критическую информационную инфраструктуру Султаната. К группе «преступлений, совершенных с использованием информационных технологий» были отнесены оскорбления религиозных или общественных ценностей, нарушение авторских и смежных прав, нарушение прав объектов промышленной собственности (в первую очередь, промышленный саботаж), антиправительственная пропаганда[142].

Подобное разделение не характерно для «Законов о киберпреступности» других монархий Залива, которые, в отличие от Омана, предпочитают оперировать максимально обобщенными, не конкретизированными формулировками. В этой связи любые попытки обсуждения коллективных мер борьбы с киберпреступностью на пространстве ССАГЗ априори обречены на неудачу.

Нет единства среди аравийских монархий и по вопросу о регулировании сектора цифровых валют, ввиду чего позиция законодателей варьируется от страны к стране (*см.: Приложение I, Таблица 6*). Так, например, во всех странах ССАГЗ уже сформирована первичная нормативно-правовая база, позволяющая регулировать оборот криптоактивов (закон «Об электронных

[142] The Cyber Crime Law (Royal Decree 12/2011). Muscat, 2011. P. 6, 8.

транзакциях», «О банковской деятельности», «О регулировании телекоммуникационного сектора» и др.). При этом более комплексный подход (подразумевающий, помимо непосредственного контроля за оборотом токенов, определение порядка регистрации и лицензирования майнинговой деятельности, функционирования профильных бирж, центров майнинга и пр.) выработан только тремя странами – ОАЭ, Бахрейном и Оманом. Создание национальных криптовалют, по состоянию на начало 2024 г., санкционировано лишь одной страной – ОАЭ. В двух государства – Кувейте и Катаре – работа с цифровыми активами все еще относится к категории уголовно наказуемых деяний.

С 2019 г. монархии Залива предприняли ряд шагов по преодолению имеющихся разногласий. В частности, в целях развития единого рынка на пространстве ССАГЗ страны-участницы выразили готовность перейти на использование «стейблкоинов» – стабилизированных криптовалютных активов, курс которых привязан к стоимости биржевых товаров или традиционных валют и характеризуется меньшей степенью непредсказуемости[143]. Хотя данная мера и выглядит перспективной, на практике она едва ли станет решением проблемы без выработки единой позиции по цифровым активам в рамках ССАГЗ.

Аналогично обстоят дела и с противодействием террористической угрозе в киберпространстве. Ввиду того, что у каждой страны существует собственный список запрещенных группировок (который также не унифицирован в рамках ССАГЗ) и собственный подход к борьбе с кибертерроризмом, попытки достигнуть консенсуса раз за разом терпели неудачу. По этой же причине сторонам не удалось договориться относительно используемых инструментов для поддержания стабильности в киберпространстве, а также выработать единый подход к проблеме кибертерроризма, что проявилось в ходе обсуждения проекта российской

[143] Naveed M., Shoaib A. The resilience of Shariah-compliant investments: probing the static and dynamic connectedness between gold-backed cryptocurrencies and GCC equity markets // IRFA. 2024. № 91. P. 117,123.

Концепции коллективной безопасности в зоне Персидского залива в 2019 г. в рамках заседаний ССАГЗ[144].

Серьезным препятствием к гармонизации правовой сферы в области кибербезопасности на пространстве ССАГЗ являет то, что все входящие в это объединение государства продолжают придерживаться преимущественно реактивного, а не проактивного подхода к развитию национальной нормативно-правовой базы. Это выражается, в первую очередь, в склонности к купированию последствий кибератак и иных нарушений в работе цифровой инфраструктуры вместо поэтапной разработки комплексного ответа, предполагающего принятие мер на опережение.

Другая причина связана с определенным дистанцированием монархий Залива от международного нормотворческого процесса в области цифровой защиты. С одной стороны, они принимают участие в реализации комплексных проектов кибербезопасности под эгидой МСЭ, а также сотрудничают с ООН в рамках специализированных Рабочих групп и ГПЭ, что дает возможность корректировать предлагаемые инициативы под нужды региона.

С другой стороны, инициативы ООН и других международных профильных экспертных площадок далеко не всегда являются руководством к действию для аравийских монархий, которые неизменно принимают в расчет ситуацию в арабском мире в целом. Так, например, рекомендации по гармонизации законодательства в области кибербезопасности, разработанные ЮНКТАД для арабских стран в 2013 г.[145], в большинстве своем так и остались на бумаге. Схожая судьба постигла и проект международной профессиональной организации «Internet Society», занимающейся вопросами развития Интернета и создания безопасной цифровой среды[146].

---

[144] Kozhanov N. Russia and the issue of a new security architecture for the Persian Gulf // LSE. 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).

[145] Development and harmonization of cyber legislation in the Arab region. N.Y., 2013. P. 7–14.

[146] Internet infrastructure security guidelines for the Arab states. P. 16–18.

Кроме того, аравийские монархии, как правило, не представлены на международных площадках, находящихся вне структур ООН (например, Консорциум по изучению угроз информационной безопасности[147] (РФ, КНР) или консультативная группа в рамках «Counter-Ransomware Initiative»[148] (США), что ведет к неизбежному отставанию от глобальных трендов в вопросах контроля над киберпространством.

По сути, стимулом к активизации нормотворческой деятельности в монархиях Залива выступают крупные кибератаки на объекты критической инфраструктуры, новые цифровые реалии социально-экономического развития либо инициативы внешних акторов в лице ООН, США и т.д. Схожая ситуация прослеживается в вопросах создания общего правового пространства ССАГЗ. Одна из последних попыток стимулировать этот процесс была предпринята Вашингтоном в конце 2018 г., когда в рамках проекта «Ближневосточного стратегического альянса» (Middle East Strategic Alliance, MESA) США выдвинули идею создания коллективного киберкомандования и предложили аравийским монархиям было разработать модульный закон, который в перспективе должен был стать основой для коллективного договора; однако (с приходом к власти в США администрации Джо Байдена проект был свернут[149]. Проект MESA будет предметно рассмотрен в Главе 3 (раздел 3.2) данной работы.

Разумеется, представители экспертных сообществ монархий Залива признают наличие «концептуального разрыва» в подходах к обеспечению кибербезопасности (включая правовые аспекты проблемы) и необходимость его преодоления. Однако они считают, что адаптация правового поля аравийских монархий к общемировой практике невозможна без гармонизации

---

[147] Россия и Китай начинают партнерство в области кибербезопасности // Газета.ru. 06.05.2015. URL: https://www.gazeta.ru/tech/2015/05/06/6670173/Russia_China_infobezopasnost.shtml (дата обращения: 17.10.2023).

[148] Update on the International Counter-Ransomware Initiative // US Dept. of State. 15.11.2021. URL: https://www.state.gov/briefings-foreign-press-centers/update-on-the-international-counter-ransomware-initiative (accessed: 06.10.2023).

[149] 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).

профильного законодательства в рамках всего арабского мира, а этот процесс неизменно наталкивается на множество препятствий по причине «нормотворческих разногласий» внутри арабского сообщества[150].

В целом, можно резюмировать, что если в вопросах формирования национальной правовой базы обеспечения кибербезопасности монархии Залива добились впечатляющих результатов, то в области продвижения к общему правовому полю в рамках ССАГЗ им предстоит решить довольно большой комплекс проблем.

Технические возможности, в соответствии с методологией МСЭ ООН, являются важным показателем при оценке цифровой готовности государств, поскольку отражают способность актора адаптироваться к усложнению угроз, исходящих из киберпространства (за счет совершенствования структуры отраслевой безопасности), а также готовность обеспечить высокоуровневую защиту критической инфраструктуры и уязвимых слоев населения. Аравийские монархии в последние годы демонстрируют на данном направлении значительное улучшение показателей.

Во всех рассматриваемых государствах к настоящему моменту созданы национальные компьютерные группы реагирования на чрезвычайные ситуации (Computer Emergency Response Team, CERT), ведется активная работа по комплексному укреплению «цифрового периметра». Так, в двух странах (Катар, Оман) помимо общенациональных созданы отраслевые группы реагирования (в нефтегазовом и финансовом секторах), еще в двух государствах (Саудовская Аравия, Бахрейн) вопрос находится в стадии проработки. Также в четырех странах (ОАЭ, Катар, Оман, Кувейт) учреждены специализированные центры, занимающиеся аналитикой по профилю кибербезопасности и учитывающие в своей деятельности передовые практики профильных структур НАТО. Почти все монархии демонстрируют стремление к интеграции в общенациональную систему цифровой защиты

[150] Experts call for 'Geneva Convention' for cybersecurity at Abu Dhabi Strategic debates // India Times. 15.11.2021. URL: https://indiatimes.com/news/experts-call-for-geneva-convention (accessed: 06.10.2023).

дополнительных защитных механизмов за счет привлечения частных кибергрупп, осуществляющих мониторинг и атрибуцию цифровых угроз. Исключение составляет Оман, где данная деятельность распределена между национальными отраслевыми группами и профильными аналитическими центрами (*см.: Приложение I, Таблица 7*).

Вместе с тем при анализе технических показателей обнаруживается общая для всех монархий определенная инерционность действий на рассматриваемом направлении. Несмотря на то, что монархии Залива присоединились к международному проекту CERT еще в 2000-х гг., развитие системы реагирования на чрезвычайные ситуации в цифровом пространстве, в целом, сохраняет скачкообразный и несистемный характер, особенно в вопросе создания отраслевых мониторинговых групп. Как правило, повышенное внимание к вопросу формирования отраслевых CERT, нацеленных на защиту критической инфраструктуры, уделяют те страны, которые либо уже становились жертвами крупных кибератак в прошлом (Саудовская Аравия, Катар), либо подвержены этой угрозе на данный момент (ОАЭ).

Эффективность национальных и отраслевых CERT государств Залива ограничивается, кроме того, по причине недостатка финансовых средств, специализированного оборудования, высококвалифицированных кадров и опыта, в том числе в области генерации собственных IT-решений. Так, например, процесс формирования CERT Бахрейна проходил по инициативе и при финансовом и организационном участии Вашингтона в рамках мероприятий по наращиванию мер безопасности военно-морской базы США, размещенной в данном государстве[151]. Специализированное оборудование и программное обеспечение монархии Залива предпочитают приобретать за рубежом, преимущественно в США и странах НАТО[152].

[151] The new battlefront. P. 12.
[152] Kingdom of Saudi Arabia cyber readiness. Arlington, 2017. P. 20-21.

Эксперты также отмечают ориентированность арабских CERT, в том числе профильных групп из аравийских монархий, на взаимодействие с правительственными структурами своих государств, а также их относительно низкую (по сравнению с другими регионами мира) заинтересованность в развитии горизонтальных связей (с CERT других стран) и сотрудничества с частными бизнес-структурами и другими субъектами кибербезопасности. В числе причин подобного положения дел специалисты указывают доминирование управленческой модели «нисходящего государственного контроля» и в определенной степени обоснованную подозрительность в отношении подконтрольных правительствам CERT других стран по поводу их действий в интересах национальных разведслужб[153].

Кроме того, как и в случае с гармонизацией правового поля, в сфере развития технического потенциала также наблюдается определенная дистанцированность монархий Залива от передового мирового опыта. Так, например, на площадке глобального Форума групп реагирования на инциденты и обеспечения безопасности (*Forum of Incident Response and Security Teams, FIRST*), в рамках которого разрабатываются и реализуются проекты, связанные с расширением знаний в области кибербезопасности и способствующие развитию отношений на межправительственном и межотраслевом уровнях, представлены CERT всего трех из шести монархий Залива: Саудовской Аравии (национальная группа и 8 отраслевых), ОАЭ (1 и 5 соответственно) и Омана (правительственная CERT)[154].

Совокупность вышеуказанных факторов (нехватка финансовых ресурсов, кадровые проблемы, слабость горизонтальных связей CERT, общерегиональная атмосфера недоверия и т.п.) обусловила тот факт, что ни одна из монархий Залива не вышла на максимальный показатель МСЭ ООН по параметру технической готовности к отражению киберугроз (*см.: Приложение I, Таблица 5; Приложение II, Схема 2*), несмотря на довольно

[153] Internet infrastructure security. P. 7, 13–14.
[154] FIRST members around the world // FIRST. URL: https://www.first.org/members/map (accessed: 10.12.2023).

внушительные успехи на данном направлении развития национального киберпотенциала.

Организационные меры. Совершенствование институтов и механизмов управления политикой в области цифровой защиты на уровне органов исполнительной власти, частного сектора и гражданского общества, а также своевременные разработка и обновление национальных стратегий кибербезопасности являются неотъемлемой частью развития систем кибербезопасности государств. В случае с монархиями Залива развитие организационной структуры шло, фактически, параллельно с совершенствованием законодательного поля.

Так, первичная структура институтов, ответственных за управление национальным киберсектором, сложилась в рассматриваемых государствах уже к 2006 г. (*см.: Приложение I, Таблица 8*). К этому же периоду относится и формирование первых профильных департаментов в составе ключевых органов исполнительной власти (Минобороны, МВД, МИД, Таможенная служба и др.), ответственных за координацию цифровой защиты на подотчетных их направлениях.

С 2016 г., после официального принятия стратегических программ «Видение», начался процесс комплексной реорганизации системы государственного управления в сфере кибербезопасности, в ходе которого в Саудовской Аравии, Катаре и Бахрейне (2017 г.), ОАЭ (2018 г.), Омане и Кувейте (2019 г.) были сформированы специализированные институты, ответственные за регулирование сферы киберзащиты на общенациональном уровне Новые институты стали «ядром» национальных систем управления кибербезопасностью. Кроме того, был перераспределен функционал ряда структур, ранее выполнявших основные регулирующие и надзорные функции, что позволило устранить дублирование полномочий и добиться разгрузки системы управления в целом.

Одновременно начала развиваться система вспомогательных агентств в структуре управления кибербезопасностью – консультационных групп

высокого уровня, призванных способствовать более взвешенному принятию стратегических решений. Соответствующие единицы появились в Саудовской Аравии (Консультационная группа при Совете министров, Группа кибербезопасности проекта «NEOM» и др.), ОАЭ (Национальный совет по кибербезопасности) и Омане (Консультационная группа при Совете министров Султаната).

Отдельное направление развития оргструктуры кибербезопасности было связано с разработкой и обновлением стратегий национальной кибербезопасности. Системность и своевременность реализации мер на этом направлении является важным критерием оценки эффективности механизма управления и координации сферы цифровой защиты. Сегодня во всех монархиях в том или ином виде сформулированы стратегии национальной кибербезопасности (*см.: Приложение I, Таблица 8*). Большинство из них приняты в первый год после запуска «Vision» и ориентированы преимущественно на обеспечение безопасности объектов критической инфраструктуры.

В контексте рассмотрения практик монархий Залива в области разработки долгосрочных программ развития сектора кибербезопасности особого внимания заслуживает опыт ОАЭ. Помимо общенациональной стратегии цифровой защиты 2019 г.[155], ведется работа и на уровне отдельных эмиратов. Собственная стратегия кибербезопасности имеется в эмирате Дубай (принята в 2017 г., обновлена в 2023 г.)[156], в ней сделан акцент на усиление цифровой защиты смарт-городов и цифровой инфраструктуры. В Абу-Даби разработана стратегия кибербезопасности для сектора здравоохранения[157], в настоящее время ведется разрабатывается программа защиты бизнес-структур[158]. В эмирате Фуджейра работа над стратегией кибербезопасности

[155] UAE National Cybersecurity strategy 2019. Abu Dhabi, 2019.
[156] Dubai cybersecurity strategy. URL: https://u.ae/en/dubai-cyber-security-strategy (accessed: 19.01.2024).
[157] Abu Dhabi Healthcare Information and Cybersecurity strategy. Abu Dhabi, 2020.
[158] How Abu Dhabi plans to build up its cybersecurity defences // Arabian Business. 08.01.2022. URL: https://www.arabianbusiness.com/how-abu-dhabi-plans-to-build-up-its-cybersecurity-defences (accessed: 19.10.2023).

ведется с 2020 г., ее краеугольным камнем стала цифровая защита финансовой отрасли[159].

С учетом стремительно меняющихся реалий цифровой среды и исходящих из нее угроз ОАЭ сделали еще один важный шаг к укреплению цифрового периметра страны. В сентябре 2023 г. глава Совета по национальной кибербезопасности Мохаммед Аль-Кувейти заявил о планах разработать и представить до конца 2024 г. стратегию комплексного развития цифровой сферы «Видение кибербезопасности» (*«Cybersecurity Vision»*), рассчитанную до 2071 г. Стратегия затронет различные отрасли инновационного развития (технологии искусственного интеллекта, квантовых вычислений, дополненной реальности, биоинженерии, высокотехнологичного производства и пр.), а предложенные в ней шаги позволят уже к 2050 г. (промежуточная точка реализации «Cybersecurity Vision») кратно повысить эффективность цифровой защиты и закрепить технологическое лидерство ОАЭ как на региональном, так и на глобальном уровнях[160]. Учитывая острый дух соперничества за статус лидера между монархиями Залива (в первую очередь, между ОАЭ и Саудовской Аравией) не исключено, что новые документы стратегического планирования в обозримом будущем представят и другие страны.

Вместе с тем в рейтинге МСЭ ООН по параметру «организационные меры» только две страны – Саудовская Аравия и Оман – получили высший балл; ОАЭ и Катар близки к максимальному показателю; Бахрейн и Кувейт значительно уступают своим соседям по данному критерию (*Приложение I, Таблица 5; Приложение II, Схема 2*).

Одна из причин заключается в том, что действующие в настоящее время стратегии национальной безопасности официально приняты только в двух

---

[159] National Bank of Fujairah: building a robust cybersecurity strategy // Gulf News. 23.02.2022. URL: https://gulfnews.com/gn-focus/national-bank-of-fujairah-building-a-robust-cybersecurity-strategy (accessed: 21.10.2023).

[160] UAE plans Cybersecurity Vision for next 50 years // The National News. 20.09.2023. URL: https://www.thenationalnews.com/business/technology/2023/09/20/uae-plans-cybersecurity-vision-for-next-50-years/ (accessed: 30.01.2024).

государствах – Бахрейне и ОАЭ, в Саудовской Аравии этот документ остается в статусе проекта и постоянно корректируется, в Катаре и Кувейте действие стратегии формально истекло, в Омане указанная программа все еще находятся в разработке (*см.: Приложение I, Таблица 8*).

Кроме того, системная работа по своевременной адаптации стратегий национальной кибербезопасности к меняющимся цифровым реалиям (проведение национальных аудитов, выработка метрик оценки рисков на национальном уровне и пр.) проводится только тремя странами (Оман, Катар, Саудовская Аравия), в то время как другие ограничиваются реализацией отдельных мер или принимают их со значительной задержкой (*см.: Приложение I, Таблица 9*).

Институциональная структура сектора кибербезопасности монархий Залива также нуждается в доработке. Ее вертикальный формат обеспечивает государству статус основного регулятора (на практике, зачастую, единственного), препятствуя тем самым формированию специализированных институтов на уровне других субъектов кибербезопасности в лице деловых кругов, научно-исследовательских и образовательных центров, обычных пользователей, а также тормозя развитие горизонтальных связей между ними. В числе других причин исследователи указывают незавершенность процесса реорганизации системы управления киберсектором, что приводит к сохранению в различных профильных государственных ведомствах дублирующего функционала; относительно низкий уровень взаимодействия между различными институтами; определенную ограниченность финансирования и кадровых ресурсов[161].

Особенности экономических и военно-политических приоритетов формируют еще одну специфическую черту организационной структуры монархий Залива в сфере кибербезопасности: инвестиции в указанный сектор в большинстве своем реализуются через программы модернизации военного

[161] Internet infrastructure security. P. 14–16.

потенциала и обеспечения цифровой защиты наиболее значимых объектов критической инфраструктуры (как правило, это такие отрасли, как энергетика, финансы, телекоммуникации)[162].

Более того, немаловажную роль в выработке и реализации организационных мер в сфере кибербезопасности играют внешние стратегические партнеры монархий. В качестве иллюстрации можно привести пример соглашения между Саудовской Аравией и США 2017 г., в котором в качестве одного из базовых условий оказания Вашингтоном помощи в модернизации вооруженных сил Королевства общей стоимостью 110 млрд. долларов фигурирует задача преодоления фрагментации управления сектора кибербезопасности[163].

Меры по развитию потенциала. Данный параметр предусматривает, в первую очередь, развитие человеческого потенциала – комплексного совокупного показателя многообразных явных и скрытых свойств населения страны, который отражает уровень развития ее граждан, их производственные, социальные, экономические и иные возможности, а также служит одним из ключевых критериев при оценке уровня их жизни. С точки зрения кибербезопасности указанный критерий включает меры по поощрению осведомленности населения о цифровых угрозах и методах их парирования; наличие профильных научно-исследовательских центров и образовательных программ; привлечение в отрасль и поддержку со стороны государства малого и среднего бизнеса; развитие государственно-частного партнерства (ГЧП), проведение кампаний по повышению уровня цифровых знаний на общенациональном и отраслевом уровнях, а также на уровне деловых кругов и профильных учреждений (государственных, образовательных, научно-исследовательских и др.).

---

[162] Cybersecurity spending for critical infrastructure to surpass US$105 billion in 2021 // ABI Research. 10.02.2021. URL: https://www.abiresearch.com/press/cybersecurity-spending-critical-infrastructure-surpass-us105-billion-2021/ (accessed: 12.11.2023).

[163] U.S. security cooperation with Saudi Arabia. Fact Sheet // U.S. State Department. January 20, 2021. URL: https://www.state.gov/u-s-security-cooperation-with-saudi-arabia/ (accessed: 12.11.2023); The new battlefront. P. 7.

Все монархии Залива активно развивают профильную научную и образовательную среду, однако привлекают к работе не только национальные государственные и частные структуры, но также ведущие зарубежные исследовательские и образовательные центры и международные корпорации. Как правило, ставка делается на создание в рамках ГЧП специализированных образовательных центров, действующих под эгидой крупных IT-компаний: подобные учреждения открыты в большинстве стран, и их число постоянно растет. Например, в ОАЭ в рамках ГЧП за последнее десятилетие запущено более 100 краткосрочных курсов от ведущих IT-компаний мира (американских, европейских, азиатских), направленных на развитие профессиональных компетенций в области искусственного интеллекта и цифровой безопасности, а также созданы программы профессиональной переподготовки государственных служащих (например, на базе частного образовательного центра «Hippo Cyber Institute»)[164]; значительная часть проектов реализуется в сотрудничестве с международной организаций Cyber Management Alliance (CMA), штаб-квартира которой располагается в Лондоне. Аналогичные по содержанию и направленности проекты реализуются в Саудовской Аравии, Катаре и Омане. Именно эти площадки в большинстве случаев выступают платформой для проведения мероприятий, направленных на оттачивание практических навыков молодых специалистов.

Следует отметить, что соотношение государственных и частных площадок в монархиях Залива находится в относительном балансе за счет наращивания количества профильных образовательных программ во второй половине 2010-х гг. и введения в ряде стран (Саудовская Аравия, ОАЭ, Бахрейн) дополнительных мер поддержки для обучающихся. Тем не менее доля частных платформ по-прежнему преобладает во всех рассмотренных странах без исключения (*см.: Приложение II, Схема 3*). Особенно это заметно на примере Кувейта, где доля частного сектора достигает отметки в 78%, а

[164] NCSC-Certified cyber incident planning and response // CMA. URL: https://www.cm-alliance.com/cyber-incident-response-training-dubai-uae (accessed: 13.10.2023).

образовательное пространство сформировано преимущественно из программ американских и европейских IT-фирм и НКО[165].

Важно подчеркнуть, что усилия монархий в настоящий момент сосредоточены преимущественно на работе со старшим звеном обучающихся (студенты выпускных курсов технических ВУЗов и молодые специалисты), в то время как программы поддержки одаренных школьников на системной основе реализуются только в трех странах – Саудовской Аравии, ОАЭ и Бахрейне. Определенные шаги на этом направлении также предпринимает Катар, однако его усилия имеют скорее реактивный характер.

Наибольшую эффективность, с точки зрения итогового практического результата, имеют меры поддержки, реализуемые ОАЭ. Так, национальное Управлением разведки сигналов (*National Electronic Security Authority, NESA*) с 2014 г. на регулярной основе проводит проектные смены инициативы «CyberQuest», ориентированной на старшеклассников и студентов, чья проектная и исследовательская деятельность связана с вопросами кибербезопасности[166]. Кроме того, в стране постоянно проводятся образовательные форумы, мастер-классы, открытые лекции и хакатоны; наиболее известным и престижным из них считается «Hackathon 4.0», который проводится под эгидой правительства ОАЭ и служит дополнительным источником для пополнения национального кадрового резерва[167]. Подобный комплексный подход позволил ОАЭ существенно повысить интерес к теме цифровой безопасности среди молодежи и обеспечить приток кадров в отрасль. Не исключено, что в среднесрочной перспективе аналогичные меры предпримут и другие монархии.

Еще одной общей специфической чертой киберсистем монархий Залива является ставка на иностранных специалистов, доля которых в цифровом

---

[165] Cyber Security certification training in Kuwait // Mildain. URL: https://mildaintrainings.com/loc/cyber-security-training-in-kuwait/ (accessed: 10.10.2023).
[166] National electronic Security Authority CyberQuest // NESA. URL: https://www.actionimpact.com/national-electronic-security-authority-cyber-quest-case-study (accessed: 16.10.2023).
[167] About the Hackathon 4.0 // Hackathon 4.0. URL: https://hackathon.ae/en/About (accessed: 06.10.2023).

сегменте, в зависимости от страны, варьируется от 64% до 89% (*см.: Приложение II, Схема 4*) и реализуется преимущественно в рамках ГЧП. Такой подход обусловлен как недостатком собственных кадров, усугубляемым «утечкой мозгов», так и стремлением в короткие сроки получить готовые цифровые продукты зарубежного производства. Несмотря на декларативные заявления увеличить долю собственных предприятий в сегменте цифровой безопасности, достичь паритета отечественных и зарубежных компаний в краткосрочной перспективе вряд ли удастся, хотя спрос со стороны профессионального сообщества фиксируется во всех рассматриваемых странах.

Примечательно, что монархии Залива не только не воспринимают преобладание внешних IT-специалистов в отрасли в качестве проблемы, но, напротив, проявляют живой интерес к расширению связей в области кибербезопасности с иностранными компаниями, позиционируя данный подход как наиболее эффективный в вопросе своевременного достижения целей, анонсированных в «Видениях»[168]. Вместе с тем следует признать, что ставка на иностранных специалистов в вопросах реализации группы мер по развитию национального потенциала в сфере кибербезопасности со временем неизбежно сформирует комплекс новых проблем, даже несмотря на успешность мероприятий по подготовке собственных кадров.

Указанные риски усугубляются в свете уже обозначившейся в странах Залива проблемы «утечки мозгов», которая имеет «двухуровневый характер»: с одной стороны, налицо приток иностранных кадров в экономику, цифровую отрасль и сектор кибербезопасности аравийских монархий (в том числе из других арабских стран), но в то же время уже начался отток собственных специалистов на Запад[169]. Сохранение подобного тренда объективно будет

[168] Mohammed bin Salman interview on Vision 2030 // Al-Arabiya. 28.04.2021. URL: https://www.youtube.com/watch?v=xqXl0L3lL8w (accessed: 15.11.2023).
[169] Migration in the Middle East and North Africa. Tunis: Konrad Adenauer Stiftung, 2021. P. 1–6.

ослаблять позиции монархий в технологической «гонке» и вопросах обеспечения национальной цифровой защиты.

Определенный негативный отпечаток на реализацию мер по развитию потенциала в киберсекторе наложила и пандемия COVID-19. Снижение темпов развития экономики на фоне ограничительных мер привело к закрытию ряда малый цифровых проектов, не входящих непосредственно в орбиту национальных программ «Видение» и сокращению масштабов государственно-частного партнерства. Вместе с тем пандемия COVID-19 способствовала ускоренной апробации некоторых технологических решений и более эффективному внедрению цифровых сервисов в повседневную жизнь аравийских монархий[170].

Несмотря на ряд вышеуказанных проблем максимальный индекс МСЭ ООН по развитию потенциала присвоен четырем из шести монархий Залива – Саудовской Аравии, ОАЭ, Оману и Катару (*Приложение I, Таблица 5; Приложение II, Схема 2*). При этом все без исключения аравийские монархии продемонстрировали внушительный качественный рост по сравнению с периодом, предшествовавшим принятию стратегических программ «Видение» и концепций национальной кибербезопасности[171].

Международное сотрудничество в сфере кибербезопасности нацелено на гармонизацию минимальных мер безопасности, обмен информацией и передовым опытом, а также кодификацию норм поведения в цифровом пространстве. Оно охватывает двусторонний и многосторонний формат межгосударственного взаимодействия (включая межведомственный уровень), в том числе на полях глобальных и региональных международных организаций и иных интеграционных площадках; коллаборацию профильных бизнес-структур различных стран, в том числе государственно-частное партнерство; сотрудничество по линии научно-исследовательских, образовательных и общественных институтов.

---

[170] PWC: leveraging public private partnerships in the GCC post COVID-19. L., 2021. P. 8.
[171] GCI 2018. P. 27, 33, 57.

Аравийские монархии рассматривают международный трек как один из драйверов развития национальных киберсистем, и потому уделяют ему повышенное внимание. Вместе с тем по данному параметру Глобального индекса кибербезопасности максимальные показатели имеются только у трех государств – Саудовской Аравии, ОАЭ и Омана, относительно высокий рейтинг имеет Катар, а Кувейт и Бахрейн занимают средние строки рейтинга (*Приложение I, Таблица 5; Приложение II, Схема 2*).

Подобный расклад обусловлен рядом факторов. Прежде всего, монархии Залива участвуют в многосторонних форматах международного сотрудничества (между тремя или более сторонами) только в случаях, когда подобные соглашения не затрагивают такие чувствительные сферы, как нормативно-правовое поле и национальные законодательства, критическую инфраструктуру, военную отрасль, вопросы государственного устройства и политической культуры. Как правило, многосторонне взаимодействие осуществляется в области обмена информацией, передовым опытом и новыми подходами к борьбе с киберугрозами, а также развития потенциала в рамках участия в международных мероприятиях (конференциях по кибербезопасности, семинаров по повышению квалификации и т.п.). Согласно исследованию МСЭ ООН, данный тренд характерен для большинства государств мира ввиду особо деликатного характера сферы кибербезопасности[172]. В случае с монархиями Залива действие обозначенного фактора усугубляется традиционно высокой степенью конфликтности и недоверия на Ближнем Востоке[173].

В силу указанных причин монархии Залива проявляют больший к международному сотрудничеству под эгидой ООН, прежде всего по линии групп реагирования на компьютерные чрезвычайные ситуации. В 2012 г. по инициативе МСЭ ООН в Маскате под оперативным управлением CERT Омана

[172] GCI, 2020. P. 20–21.
[173] Звягельская И.Д., Свистунова И.А. и др. Ближний Восток в условиях «негативной определенности». С. 94–103.

был учрежден Арабский региональный центр кибербезопасности (*ITU Arab Regional Cyber Security Center, ITU-ARCC*) для мониторинга киберрисков в режиме текущего времени, координации деятельности CERT стран арабского мира и разработке коллективных решений в целях гармоничного развития систем цифровой защиты стран арабского мира. Национальная группа реагирования Омана, кроме того, координирует деятельность совместную в рамках ССАГЗ группу реагирования, а Маскат возглавляет специализированный Комитет CERT Совета сотрудничества (Gulf Cooperation Council CERT Committee)[174].

Группы CERT аравийских монархий также взаимодействуют с группами реагирования других стран мира на полях Форума групп реагирования на инциденты и обеспечения безопасности (FIRST), Лиги арабских государств (Региональный саммит по кибербезопасности для арабских государств) и Организации исламского сотрудничества[175]. Три государства – ОАЭ, Катар и Кувейт – поддерживают глобальные общественные инициативы, связанные с вопросами «цифровой разрядки» (например, «Парижский призыв к доверию и безопасности в киберпространстве» 2018 г.[176]), выступая за прекращение гонки кибервооружений.

Несмотря на расширяющееся международное сотрудничество в многосторонних форматах, все монархии Залива, как и большинство стран мира, предпочитают развивать свой киберпотенциал в рамках двусторонних отношений. Однако соглашения о сотрудничестве во всех сферах аспектах кибербезопасности на двусторонней основе заключаются редко. Так, согласно данным МСЭ ООН, Оман подписал всего 4 двусторонних соглашения по сотрудничеству в области цифровой защиты – с Эстонией, Малайзией, Сингапуром и Южной Кореей (самый высокий показатель среди стран

[174] About ARCC // ITU Arab Regional Cybersecurity Centre (ITU-ARCC). URL: https://arcc.om/?GetLang=en (accessed: 10.12.2023).
[175] Vision & Mission Statement // OIC-CERT. URL: https://www.oic-cert.org/en/missionstatement.html# (accessed: 10.12.2023).
[176] Paris Call: 12.11.2018. URL: https://pariscall.international/en/call (accessed: 06.10.2023).

ССАГЗ); у ОАЭ и Кувейта таких договоров по одному (с Саудовской Аравией и Великобританией[177] соответственно), у Саудовской Аравии всего два – с Великобританией и ОАЭ[178].

Как правило, двусторонние соглашения ориентированы на развитие отдельных компонентов сектора кибербезопасности – обмен информацией о киберугрозах, либо поставки специализированного оборудования и программного обеспечения, некоторые меры по развитию потенциала (технического или кадрового), инвестиции в ту или иную профильную отрасль, обмен опытом и т.д. Более того, зачастую кибербезопасность не является центральным пунктом двустороннего договора о сотрудничестве, а ее правовые аспекты никогда не становятся областью межгосударственного взаимодействия.

Наиболее активно двусторонняя кооперация в вопросах обеспечения кибербезопасности, особенно в ее военном сегменте, развивается между странами, которых связывают отношения стратегического партнерства и длительный исторический опыт сотрудничества. В случае с монархиями Залива это США, их главный стратегический союзник, а также страны Евросоюза. Большую роль при выборе внешнего партнера в вопросах развития национальных киберсистем играет технологическая мощь страны и ее готовность оказать профильную помощь. Этим объясняется значительное наращивание сотрудничества аравийских монархий с новыми внерегиональными акторами на Ближнем Востоке – Китаем, Республикой Корея и Японией. Обозначенные тренды предметно будут рассмотрены в Главе 3 данной работы.

Отраслевые и межведомственные соглашения между монархиями Залива и иностранными государствами, как правило, заключаются в форме

---

[177] Kuwait, Britain sign deal on cybersecurity coop // Kuna. 30.08.2023. URL: https://www.kuna.net.kw/ArticleDetails.aspx?id=3107460&language=en# (accessed: 12.12.2023).
[178] Saudi Arabia // UNIDIR, March 2021. URL: https://unidir.org›cpp›state-pdf-export (accessed: 20.10.2021).

меморандумов о взаимопонимании[179]. Они направлены на развитие сотрудничества в отдельных секторах кибербезопасности – безопасность данных и электронных банковских платежей; образование и подготовка кадров и т.д. Данные о сотрудничестве аравийских монархий в двустороннем формате по линии профильных министерств и ведомств представлены в *Приложении I (Таблица 10)*. Из этих данных следует, что все монархии Залива имеют профильные отраслевые и межведомственные соглашения с США, своим стратегическом партнером, а наиболее активно данную форму взаимодействия продвигают Саудовская Аравия, ОАЭ и Бахрейн. Примечательно, что на внутрирегиональном уровне (в границах зоны Персидского залива) подобная форма сотрудничества развита относительно слабо, государства Залива предпочитают кооперироваться со своими соседями в рамках государственно-частного партнерства.

Страны Залива также сотрудничают с представителями частного сектора других стран в форме государственно-частного партнерства; данная сфера международной кооперации представлена в *Приложении I (Таблица 10)*. ГЧП позволяет аравийским монархиям более широко вовлечься в экосистему кибербезопасности путем заключения контрактов с мировыми гигантами индустрии цифровой защиты[180], создания специализированных научных и технологических парков, разработки и внедрения совместных образовательных программ и курсов повышения квалификации, проведения конференций и семинаров, где могут встречаться представители частного и государственного секторов разных стран.

---

[179] См,, напр.: Saudi National Cybersecurity Authority and U.S. Department of Homeland Security Sign MoU to Promote Cybersecurity Cooperation // Saudi Press. 16.07.2022. URL: https://www.spa.gov.sa/2370312 (accessed: 12.12.2023); Saudi Arabia, Four Countries Sign Cybersecurity MoUs // Asharq Al-Aswat. 03.11.2023. URL: https://english.aawsat.com/business/4645086-saudi-arabia-four-countries-sign-cybersecurity-mous (accessed: 12.12.2023).

[180] См, напр.: Oman: MTC signs agreement to promote cybersecurity start-ups // Data Guidelines. 09.01.2020. URL: https://www.dataguidance.com/news/oman-mtc-signs-agreement-promote-cybersecurity-start-ups (accessed: 12.12.2023); Beyon Cyber signs strategic agreement to launch Cyber Security Solutions for Bahrain's SMEs during AICS 2023 // BNA. 06.12.2023. URL: https://www.bna.bh/en/BeyonCybersignsstrategicagreementtolaunchCybersecuritySolutionsforBahrainsSMEsduringAICS2023.aspx?cms=q8FmFJgiscL2fwIzON1%2BDpsmkryoGUibbCpfxbm%2FFkU%3D (accessed: 12.12.2023).

Монархии Залива также уделяют значительное внимание имиджевым аспектам сотрудничества в области кибербезопасности и совместными усилиями уверенно продвигаются к статусу «региональной площадки цифрового диалога». Проведение международных мероприятий по вопросам киберзащиты, в том числе под эгидой ССАГЗ, способствует укреплению цифрового имиджа государств- участников Совета сотрудничества и самого объединения, а также позволяет развивать новые направления взаимодействия с внешними партнерами. Сегодня развитие системы имиджевых площадок находится в числе приоритетов всех стран ССАГЗ, однако наиболее активно действуют Саудовская Аравия и ОАЭ, принимающие более десяти мероприятий ежегодно (см.: *Приложение II, Схема 5*).

«Дискретная» форма сотрудничества (через посредников) в области кибербезопасности была характерна для всех монархий Залива (кроме Кувейта) по линии взаимодействия с Израилем ввиду отсутствия официальных дипломатических связей. После подписания «Соглашений Авраама» в 2020 г. два арабских участника договора – ОАЭ и Бахрейн – нормализовали отношения с Израилем, что позволило им изменить формат кооперации. Саудовская Аравия, Катар и Оман продолжают взаимодействие с Израилем «дискретно» (см.: *Приложение I, Таблица 10; Приложение II, Схема 6*). Подробнее указанная форма сотрудничества будет рассмотрена в Главе 3 (раздел 3.3) данной работы.

Таким образом, все монархии Залива демонстрируют относительно высокий уровень готовности к отражению цифровых угроз (*Приложение I, Таблица 5; Приложение II, Схема 2*). Лидирующие позиции среди стран ССАГЗ занимают Саудовская Аравия и ОАЭ, которые в течение 5 лет после принятия программ «Видение» (2016–2020 гг.) форсированными темпами сумели выстроить комплексную систему национальной цифровой защиты и вошли в мировой топ-5 Глобального индекса кибербезопасности МСЭ ООН. К числу «спринтеров» также можно отнести Кувейт, который за указанный период поднялся в мировом рейтинге с 138 строки на 64, а в региональном

арабском индексе – соответственно с 17 на 9 место (см.: *Приложение I, Таблица 2*).

Остальные монархии Залива, также взявшие курс на диверсификацию и цифровизацию своих экономик, предпочитают динамичное, но размеренное и поступательное продвижение к безопасной цифровой среде, демонстрируя при этом передовые практики. Наиболее показателен в этом отношении кейс Омана, где процессы цифровизации и, как следствие, строительства национальной системы кибербезопасности начались практически десятилетием раньше других монархий Залива, что позволило Султанату прочно удерживаться в топ-5 мирового рейтинга кибербезопасности в 2014–2018 гг. По этой же причине в 2012 г. именно Оман был выбран МСЭ ООН в качестве координационного центра развития кибербезопасности в арабском мире[181]. С 2020 г. Султанат переместился на 21 строчку Глобального индекса, пропустив вперед не только аравийских, но также европейских и азиатских «спринтеров», что, однако, не помешало ему сохранить за собой место в тройке лидеров арабского мира (вместе с Саудовской Аравией и ОАЭ) и в пятерке мусульманских стран с наиболее комплексной системой цифровой защиты.

Вместе с тем следует признать, что ни одна из монархий Залива не достигла абсолютных показателей МСЭ ООН, несмотря на высокие результаты развития национального сектора кибербезопасности. Для всех стран в той или иной степени характерны проблемы с наращиванием технического потенциала, требуют доработки институциональная структура и стратегические программы развития цифровой защиты, далеко не в полной мере используются возможности международного сотрудничества и объединения усилий в противодействии угрозам, прежде всего на площадке ССАГЗ.

[181] GCI 2015. P. 360.

2.3. Запрос на коллективные меры киберзащиты

Специфика развития Интернет-пространства такова, что обеспечение кибербезопасности со временем становится не конечной целью, а скорее неотъемлемым инструментом экономической и социальной деятельности акторов в глобальном цифровом мире. Учитывая децентрализованный формат управления киберпространством, его безопасность не может поддерживаться только одним актором и требует принятия коллективных мер. Не исключение и пространство Ближнего Востока, где ведущая роль в развитии регионального сектора кибербезопасности отводится аравийским монархиям в силу их наиболее высокой степени готовности к отражению цифровых угроз.

Переходя к анализу комплекса факторов, формирующих запрос на коллективные меры киберзащиты, в первую очередь следует остановиться на *технических аспектах проблемы*. С точки зрения технической составляющей важным показателем устойчивости региональной системы кибербезопасности является система точек обмена Интернет-трафиком (*Internet Exchange Point, IXP*), бесперебойная работа которых служит для обеспечения устойчивости Интернет-инфраструктуры и снижения уязвимости национальных сетей за счет стабилизации каналов переадресации[182].

В случае с Ближним Востоком можно говорить о недостаточном количестве точек обмена интернет-трафиком: по состоянию на начало 2024 г. их общее количество составляет 29, что значительно ниже показателей других регионов мира. Кроме того, очевидна неравномерность в их географическом расположении: большинство локализуется в Турции (11 точек IXP, из которых 9 расположены в районе Стамбула и европейской части страны); в монархиях Залива имеется 9 точек, остальные расположены в Иране (3 точки), Египте (2 точки), Израиле, Иордании, Палестине (Западный берег реки Иордан) и Ливане – по одной точке[183].

[182] Internet Infrastructure Security. P. 9.
[183] Internet exchange map. URL: https://www.internetexchangemap.com/#/ (accessed: 21.02.2024).

Относительно низкая численность точек IXP несет в себе серьезный риск того, что целые группы ближневосточных государств могут оказаться жертвами крупной согласованной кибератаки. Так, например, эксперты международной организации «Internet Society» фиксируют в странах арабского мира возрастающее количество инцидентов, связанных преднамеренным захватом Интернет-маршрутов с целью перенаправления трафика или шпионажа за ним, причем за атаками подобного рода с высокой долей вероятности стоят государственные акторы из других регионов. По мнению специалистов, данный риск может быть существенно снижен путем расширения системы IXP[184].

Первыми из монархий Залива к системе точек обмена интернет-трафиком присоединились Саудовская Аравия и ОАЭ (2020 г.), сегодня в этих государствах имеется соответственно три и две точки IXP, в остальных странах на постоянной основе функционирует по одной точке[185]. Это самый высокий показатель для субрегионов арабского мира и Ближнего Востока, что позволяет говорить о не только о высоких темпах развития интернет-инфраструктуры в аравийских монархиях, но также о наличии у них значительных возможностей для выдвижения общерегиональных инициатив по оптимизации сетевых структур, в том числе путем увеличения числа точек обмена интернет-трафиком.

Однако трансформация инфраструктуры IXP на данный момент реализуется каждой из монархий Залива самостоятельно и строго с ориентацией на национальные приоритеты кибербезопасности, инициативы по коллективной оптимизации соответствующей инфраструктуры пока не получили должной поддержки даже на уровне ССАГЗ.

Обеспечение физической защиты объектов информационной инфраструктуры также требует коллективных усилий. Еще одним из ключевых элементов систем кибербезопасности является коммуникационная

[184] Internet Infrastructure Security. P. 9.
[185] Internet exchange map. URL: https://www.internetexchangemap.com/#/ (accessed: 21.02.2024).

инфраструктура – физические активы, необходимые для функционирования Интернета, в том числе система кабелей (волоконно-оптические, медные, широкополосные) и связи (беспроводная и проводная); здания и объекты, где, например, размещаются центры обработки данных или посадочные точки для подводных кабелей; системы электроснабжения, охлаждения и физической безопасности, и т.д. Поскольку Интернет является «сетью сетей», акцент на устойчивости исключительно национальных сетей не обеспечивает постоянного подключения, необходима устойчивость Интернета на региональном уровне. При этом надежность региональной интернет-инфраструктуры определяется количеством физических путей для Интернет-трафика: если есть только один физический путь для входа и выхода трафика из страны или региона, соответственно существует и единая точка отказа из-за атаки, стихийного бедствия, человеческой ошибки или иных инцидентов[186].

Устойчивость коммуникационной структуры Ближнего Востока, включая зону Персидского залива, к внешним воздействиям можно отнести к разряду относительно низких. На данный момент ближневосточный Интернет-трафик проходит преимущественно через подводную инфраструктуру оптоволоконных кабелей (см. *Приложение II, Схема 7*), которая, несмотря на повсеместное развитие систем спутниковой связи, остается ведущей. По этой причине любая нештатная ситуация грозит сбоями и замедлением скорости передачи данных на всем Ближнем Востоке, что ярко проявилось в ходе аварий на подводной интернет-инфраструктуре в Средиземном (2008 г., 2013 г.)[187] и Красном (2024 г.)[188] морях. Учитывая, что в случае с аравийскими монархиями сохранение стабильности и высокой скорости интернет-соединения во многом определяет эффективность и темпы национальной цифровой трансформации в рамках стратегических программ

[186] Internet Infrastructure Security. P. 8–9.
[187] Undersea internet cables off Egypt disrupted as navy arrests three // The Guardian. 28.05.2013. URL: https://www.theguardian.com/technology/2013/mar/28/egypt-undersea-cable-arrests (accessed: 20.01.2024).
[188] Red Sea cables have been damaged, disrupting internet traffic // CNN. 28.02.2024. URL: https://edition.cnn.com/2024/03/04/business/red-sea-cables-cut-internet/index.html (accessed: 28.02.2024).

«Vision», обеспечение физической безопасности инфраструктуры является одним из приоритетов сотрудничества в области кибербезопасности.

Вопрос защиты объектов информационной инфраструктуры от негативного физического воздействия для монархий Залива и стран Ближнего Востока в настоящее время приобрел исключительную актуальность. В начале 2024 г. проиранская группировка «Ансар Аллах» (хуситы) в ответ на участившиеся удары американо-британских сил по инфраструктуре группировки в Йемене пригрозила повредить межконтинентальный оптоволоконный кабель, проложенный по дну Красного моря[189]. Данная линия служит каналом связи между Европой, Африкой и Ближним Востоком, и по ней проходит значимая часть трафика аравийских монархий.

Несмотря на то, что красноморская оптоволоконная линия не является единственной и по пропускной способности данных серьезно уступает трансатлантическим каналам связи, ее повреждение может на какое-то время нарушить передачу данных, что негативно скажется на глобальных финансовых процессах (в частности, на скорости проведения банковских платежей и обработке международных транзакций) и информационной безопасности ближневосточного региона в целом. Учитывая, что для аравийских монархий стабильность цифровых сервисов имеет основополагающее значение, вопрос о возможном повышении защищенности оптоволоконных каналов постепенно переходит в разряд основных.

Угрозы «Ансар Аллах» изначально трактовались экспертами как элемент информационной борьбы, поскольку факт наличия у группировки технологий, необходимых для проведения диверсии такого уровня, вызывал сомнение, а угрозы нанести урон критической инфраструктуре связи звучали и ранее, например, в 2019 г.[190]. Однако в конце февраля 2024 г. в

---

[189] Why Yemen’s Houthi rebels welcome conflict with the US // CNN. 01.02.2024. URL: https://edition.cnn.com/2024/02/01/middleeast/houthi-reputation-red-sea-attacks-gaza-mime-intl/index.html (accessed: 03.02.2024).

[190] Who are the Houthis and how closely linked are they to Iran? // the Washington Post. 16.09.2019. URL: https://washingtonpost.com/world/2019/09/16/why-iran-is-getting-blame-an-attack-saudi-arabia-claimed-by-yemens-houthis/ (accessed: 30.01.2024)

территориальных водах Йемена в результате диверсии было повреждено от 8 до 15 подводных кабелей[191]. Несмотря на то, что хуситы отрицают свою причастность к инциденту, они препятствуют проведению восстановительных работ, требуя, например, чтобы европейские подрядчики получить у них официальное разрешение на ремонт. Задержки с проведением работ вкупе с растущей угрозой уцелевшим оптоволоконным магистралям свидетельствуют о необходимости объединения усилий монархий Залива и ближневосточных стран в целом в вопросах физической защиты коммуникационной инфраструктуры региона.

Запрос на коллективные меры цифровой защиты обусловлен не только техническими аспектами проблемы, но и комплексом экономических, политических, социальных и иных факторов.

В первую очередь следует отметить *необходимость преодолеть зависимость от внешней помощи* в вопросах развития как цифровой отрасли в целом, так и сферы кибербезопасности. Аравийские монархии продолжают отдавать предпочтение заимствованию за рубежом готовых политико-правовых и технологических решений и адаптации их под национальные реалии. Отчасти это можно объяснить поздним (относительно стран Глобального Севера) стартом процессов цифровизации и развития сектора цифровой защиты. Однако следует признать, что объединение уже имеющихся национальных потенциалов (технико-технологического, политического, организационного, научно-исследовательского, кадрового и т.п.) будет способствовать преодолению этой зависимости, которая вынуждает монархии Залива придерживаются «догоняющей» модели развития, несмотря на их высокие позиции в Глобальном индексе кибербезопасности.

Запрос на коллективные действия в сфере развития кибербезопасности также обусловлен *необходимостью развития собственного кадрового*

[191] Red Sea cables have been damaged, disrupting internet traffic // CNN. 24.02.2024. URL: https://edition.cnn.com/2024/02/27/business/red-sea-cables-cut-internet/ (accessed: 28.02.2024).

потенциала. «Утечка мозгов» является еще одной общей для всех монархий Залива проблемой. Несмотря на то, что отток человеческого капитала из рассматриваемых стран по-прежнему значительно меньше, чем из других государств арабского мира, его объем за последние несколько лет вырос[192]. При сохранении данного тренда профильная отрасль аравийских монархий со временем может столкнуться с проблемой кадрового «голода», что усилит зависимость от внешних факторов в сфере цифровой защиты. Развитие единого образовательного пространства, в первую очередь в рамках ССАГЗ, и выработка общих механизмов, гарантирующих возвращение на родину национальных специалистов после завершения обучения за рубежом, могли бы способствовать укреплению всех стран-участниц Совета сотрудничества.

В рамках коллективных усилий представляется возможным *преодолеть* и другой фактор, ограничивающий эффективность национальных секторов цифровой защиты монархий Залива, а именно *инертность законодательной сферы*. Данная проблема не является уникальной для рассматриваемых стран, она характерна для всех современных государств: на фоне стремительной трансформации цифрового пространства и национальное, и международное правовое поле не успевают своевременно адаптироваться к новым угрозам, что ведет к появлению законодательных пробелов и усложняет регулирование[193]. Конечно, в данном контексте необходимо учитывать специфику национальных правовых систем аравийских монархий. Кроме того, зачастую разъяснения по нововведениям поступают в профильные учреждения и ведомства с опозданием в несколько месяцев ввиду традиционной для монархий Залива управленческой модели «нисходящего контроля» со стороны государства и общего уровня бюрократизации системы управления.

В числе стимулов, которые должны побуждать монархии Залива к совместному преодолению преград на пути формирования общего

[192] Christidis O. Technology and youth drive the future of work in MENA. P. 1.
[193] GCI 2020. P. 4–5.

безопасного цифрового пространства, следует отметить *необходимость снижения роли религиозного фактора в принятии стратегически значимых для развития стран решений*. В целом, современные мусульманские правоведы одобряют заимствования достижений неисламского мира в области научно-технического прогресса, если они не нарушают нормы шариата и социокультурные традиции ислама[194]. Тем не менее каждая новая технология, которая практически ежедневно пополняет реалии современного цифрового мира, в исламских странах неизменно вызывает богословские споры на предмет их соответствия исламским ценностям. Отсутствие единого мнения в богословской среде перерастает в столкновение взаимоисключающих подходов, что ведет к формированию некоего дуализма восприятий.

С одной стороны, исламские богословы, ввиду терпимости большинства школ ислама к допустимым нововведениям (*бида*), не оказывают серьезного противодействия государственным институтам, отвечающим за развитие технологий кибербезопасности, а в вопросах трактовки нововведений зачастую придерживаются позитивных или нейтральных позиций. Укоренению такого компромиссного подхода поспособствовало продвижение исламской доктрины «Аль-Васатыя», разработанной в середине 2000-х гг. ведущими духовными авторитетами стран мусульманского мира при значительном участии кувейтских государственных институтов (в частности, Министерства вакфов и исламских дел) и духовенства. В соответствии с данной доктриной, процесс вынесения решений при трактовке и оценке тех или иных событий и понятий предполагает соблюдение принципа умеренности, что позволяет избегать как излишнего идеализма (выраженного в слепом отстаивании классических постулатов), так и крайнего прагматизма (стремления к постоянным переменам «ради перемен»)[195].

С другой стороны, в цифровом мире существует достаточное число явлений, которые сложно объяснить с точки зрения исламских норм даже с

[194] Сюкияйнен Л.Р. Глобализация и мусульманский мир. С. 49–67.
[195] Мелкумян Е.С. Власть и ислам в Кувейте: поле взаимодействия. С. 92–104.

опорой на принцип «серединности». Это касается, например, хакерских атак на содержащие антиисламский контент сайты, которая может оцениваться по-разному – и как благо (отстаивание чести *уммы*), и как зло (уподобление отступникам). Другой весьма показательный пример – многочисленные дискуссии вокруг феномена децентрализованных хешированных активов (криптовалют)[196]. Ряд мусульманских богословов считает, что использование цифровых активов нарушает ключевые заповеди исламского банкинга, а операции с фьючерсами криптовалют противоречат принципу *мусавама* (фиксированной цены), поскольку курс цифровой валюты характеризуется крайней нестабильностью и не гарантирует полное покрытие издержек со стороны продавца в случае резкого ценового скачка[197]. По этой причине практика создания «халяльных» токенов, а также попытки сертифицировать деятельность «криптобирж по шариату» пока не привела к серьезным изменениям в отрасли. Феномен «отступничества», в свою очередь, дополнительно раскручивается оппозиционными деятелями и радикальными пропагандистами, что способствует появлению серьезных проблем – например, активизации «цифрового джихада».

С необходимостью гармонизировать законодательное регулирование сети Интернет связана и другая «болевая точка», характерная для всех монархий Залива и требующая коллективных усилий, – *проблема гражданских прав и свобод*. Так, ведущие международные правозащитные организации («Amnesty International», «Freedom House» и др.) неоднократно обращали внимание на излишне жесткую, с их точки зрения, политику аравийских монархий в области цифрового регулирования. По мнению правозащитников, события «арабской весны» привели к формированию в монархиях Залива убежденности в наличии постоянной скрытой угрозы, исходящей из глобальных соцсетей (что в дальнейшем нашло отражение в

[196] См., напр.: Is Crypto Haram or Halal? Reasons & Opinion of Islamic Scholars // AIMS. URL: https://aims.education/is-bitcoin-halal-or-bitcoin-haram/ (accessed: 12.10.2023).
[197] Is Crypto Haram or Halal? Reasons & Opinion of Islamic Scholars // AIMS. URL: https://aims.education/is-bitcoin-halal-or-bitcoin-haram/ (accessed: 12.10.2023).

законодательных актах рассматриваемых стран), а также в необходимости бороться с ней всеми доступными средствами. В этой связи, по мнению западных правозащитников, под прикрытием противодействия терроризму и киберпреступности в государствах Залива, по сути, ведется борьба с инакомыслием[198].

Свою лепту в развитие темы «шпиономании» в регионе вносят глобальные и западные медиа. Так, например, в начале 2022 г. издание «New York Times» опубликовало масштабное расследование о распространении шпионского ПО «Pegasus» (производится израильской IT-корпорацией «NSO Ltd.») и его использовании в странах Залива. Издание отмечает, что софт использовался представителями аравийских спецслужб для слежки за диссидентами (в частности, за саудовскими оппозиционными журналистами Джамалем Хашогги и Ганемом Альмасариром), в том числе на территории других государств[199].

Примечательно, что данная тема поднимается не впервые: в центре международных скандалов на регулярной основе оказываются проекты ОАЭ («Project Raven»), Саудовской Аравии (кампания по массовой слежке с использованием «Pegasus» и ряда аналогичных программ), Бахрейна (слежка за пользователями через приложение «BeAware Bahrain»), Катара (отслеживание местоположения пользователей в реальном времени с помощью приложения «Etheraz») и т.д. Расследование вопросов цифрового шпионажа за гражданами в очередной раз возродило дискуссии о праве на частную жизнь и соблюдении этики поведения государств в киберпространстве.

Неоднозначно влияет на сферу цифровой защиты и *проблема цензуры* в государствах ССАГЗ. С одной стороны, жесткие рамки, установленные национальным законодательством, упрощают регулирование цифровой

---

[198] Amnesty International Report 2020/21. P. 76, 218, 277, 298, 309, 376; Freedom on the Net. P. 16, 23, 27, 29.

[199] Israeli companies aided saudi spying despite Khashoggi killing // The NYT. 17.07.2021. URL: https://www.nytimes.com/2021/07/17/world/middleeast/israel-saudi-khashoggi (accessed: 06.10.2023).

среды, а также дают возможность эффективно противодействовать пропагандистской деятельности, которую представители радикально-экстремистских группировок пытаются вести на Аравийском полуострове. С другой стороны, предписания накладывают серьезные ограничения на деятельность общественных организаций, научно-аналитических и дискуссионных площадок, независимых СМИ и блогеров, фактически, выводя их деятельность под жесткий государственный контроль (без возможности трансляции мнений, отличающихся от общепринятых), что также, по оценкам правозащитников, нарушает право на свободу слова.

Подчас жесткие цензурные рамки не идут на пользу и самим аравийским монархиям. Примером служит Королевство Бахрейн, где ряд учебно-методических пособий, разработанных при участии израильских специалистов и рекомендованных к использованию в рамках совместных онлайн-программ под эгидой проекта «Школы будущего короля Хамада», по-прежнему находятся в списке запрещенных[200], несмотря на формальную нормализацию бахрейно-израильских отношений после подписания «Соглашений Авраама» в 2020 г. По этой причине обучающиеся не имеют возможности полноценно работать с пособиями, публичный доступ к которым заблокирован властями, ввиду чего итоговая эффективность цифровых образовательных проектов заметно снижается. Кроме того, национальные провайдеры (не только в Бахрейне, но и, например, в Кувейте) автоматически блокируют доступ к некоторым крупным образовательным платформам (Coursera, MIT Open Courseware и др.) или размещенным на них отдельным курсам (EdX), маркируя их как «потенциально опасный контент»[201], что существенно ограничивает развитие профильного образования и формирования собственного кадрового потенциала в монархиях Залива.

[200] Bahrain: dreams of reform crushed 10 years after uprising // Amnesty International. 11.02.2021. URL: https://www.amnesty.org.2021/02/bahrain-dreams-of-reform-crushed (accessed: 06.10.2023).
[201] Self-Censorship in Arab Higher Education: an untold problem // Al-Fanar. 18.04.2021. URL: https://www.al-fanarmedia.org/2021/04/self-censorship-in-arab-higher-education (accessed: 14.10.2023).

Важнейшим стимулом к развитию сотрудничества в сфере создания безопасного цифрового пространства на Ближнем Востоке, в том числе в зоне Персидского залива, 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 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.

На сегодняшний день наблюдается рост милитаризации ряда аравийских монархий (в первую очередь, Саудовской Аравии, ОАЭ и Катара), что в значительной степени обусловлено возросшими региональными амбициями этих держав. Бахрейн, Кувейт и Оман, хотя и не продвигаются вверх в международных рейтингах милитаризации, все же сохраняют довольно высокий уровень военных расходов и иных показателей военной мощи[202]. Учитывая, что военная сфера одной из первых берет на вооружение новейшие прорывные технологии, а специалисты военных ведомств и спецслужбы, как правило, неподотчетны гражданским органам, в рамках государств возникает параллельная система цифровой защиты, судить об уровне развития которой не позволяет дефицит находящейся в публичном доступе информации.

Как итог, слабое взаимодействие между «публичной» и «скрытой» частями киберсистемы ведет к разбалансировке между военным и гражданским регулированием. Кроме того, участившиеся информационные спекуляции представителей военного сектора на теме «скрытой иранской угрозы» (исходящей, в том числе, из киберпространства), призванные

[202] 2023 military strength ranking // Global Firepower. URL: https://www.globalfirepower.com/countries-listing.php (accessed: 06.11.2023).

привлечь в военные проекты дополнительные субсидии (в том числе внешние), на деле увеличивают дисбаланс между двумя частями национальных систем кибербезопасности монархий залива и усложняют региональное сотрудничество.

Значимость данного риска подтверждают многолетние дискуссии о превращении Ближнего Востока в «полигон» для цифровых вооружений. Некоторые исследователи полагают, что в 2010–2012 гг. американской стороной были проведены масштабные испытания кибероружия на Ближнем Востоке (атака с использованием вируса Stuxnet), которые в итоге положили начало «гонке цифровых вооружений» в регионе[203]. Сегодня монархии Залива в качестве главного источника киберугроз рассматривают Иран, который, по их мнению, неоднократно использовал цифровые средства для проведения разрушительных кибераакций против своих арабских соседей по Персидскому заливу, а для достижения кумулятивного эффекта привлекал к реализации масштабных кибердударов по объектам критической инфраструктуры многочисленные лояльные Тегерану группировки хакеров[204].

Впрочем, в последние годы аравийские монархии научились не только предупреждать крупные кибератаки со стороны Ирана, но и наносить эффективные контрудары по его инфраструктуре. Примером подобных контракций в иранском цифровом пространстве считается кибератака на систему распределения топлива на заправочных станциях страны (октябрь 2021 г.), в результате которой из строя были одновременно выведены до 5,5 тыс. объектов, что стало самой масштабной за последние годы кибератакой на Ближнем Востоке и повлекло за собой локальный топливный кризис и беспорядки. Несмотря на то, что никто из участников цифрового противостояния в зоне Залива (в лице государственных и внесистемных акторов) не взял на себя ответственность за нанесение этого удара, некоторые

[203] Kaspersky Security Bulletin 2013. URL: https://securelist.ru/kaspersky-security-bulletin-2013-razvitie-ugroz-v-2013-godu/19140/ (accessed: 06.10.2023).
[204] The new battlefront. P. 3.

эксперты склонны полагать, что за акцией может стоять хакерская группировка, действующая в интересах Саудовской Аравии или ОАЭ (при этом не исключается, что в группировку входили и иранские граждане)[205]. Факт возможного присутствия в составе группировки, ответственной за топливный кризис (а также причастной к некоторым более ранним атакам на инфраструктуру ИРИ), иранских граждан, поддерживавших эмигрантское националистическое движение «Тондар»[206], позволяет выдвинуть гипотезу, что аравийские монархии официально приняли формат резидентур HumInt в качестве инструмента воздействия на Иран изнутри, что серьезно меняет конфигурацию асимметричного конфликта.

Хакерские группировки создают множество рисков для национальных систем киберзащиты монархий Залива. В отличие от Ирана и Турции, где хакерское сообщество частично интегрировано в систему национальной кибербезопасности (турецкий кейс для примера представлен в *Приложении II, Схема 8*), аравийские монархии пока не смогли выработать комплексную модель взаимодействия с хакерами, хотя попытки сделать это предпринимали как минимум три страны – Саудовская Аравия, ОАЭ и Катар. Как показывает практика, они предпочитают сотрудничать преимущественно с легальными специалистами в области компьютерной безопасности (так называемыми «белыми» хакерами), в то время как местные «серые» хакеры привлекаются для решения отдельных задач (чаще всего имиджевых) или не привлекаются к взаимодействию вовсе[207]. В результате патриотично настроенные хакерские группировки (в том числе объединенные в рамках тех или иных «киберармий»), хоть и действуют в интересах своей страны, определяют направление атаки самостоятельно, что нередко идет вразрез с долгосрочными планами государства, интересы которого они стремятся отстаивать.

---

[205] Iran blames foreign country for cyberattack on petrol stations // BBC. 27.10.2021. URL: https://www.bbc.com/news/world-middle-east-59062907 (accessed: 11.10.2023).
[206] Intelligence Ministry arrests second man of Tondar terrorist group // Iran Government. 02.02.2022. URL: https://irangov.ir/detail/379412 (accessed: 22.10.2023).
[207] Internet infrastructure security. P. 7, 12.

Представляется возможным обозначить три варианта потенциальной интеграции хакерских групп в систему национальной кибероборонs аравийских монархий с учетом успешного опыта других региональных кибердержав – «турецкий», «иранский» и «израильский».

«Турецкий» вариант предполагает пошаговое включение хакеров-патриотов в систему национальной кибербезопасности с последующим их разделением на группы – «ядро» (более сильные и профессиональные киберкоманды») и вспомогательные силы (хакеры средней и низкой квалификации). Подобная система позволит расширить штат государственных киберспециалистов за счет сотрудничества с так называемыми «белыми хакерами», однако может снизить общий эффект от проведения операций в силу особенностей целеполагания и быстрой бюрократизации системы управления. Кроме того, в случае с аравийскими монархиями формирование «ядра» может потребовать пересмотра отдельных элементов национального законодательства (например, отмены законодательного запрета на хакерскую деятельность в Кувейте).

В рамках «иранского» варианта можно предположить сохранение зонтичной структуры и формальной независимости хакеров-патриотов от государственных институтов, однако контроль за их деятельностью, в случае внедрения данной модели, будет централизован и кратно усилен за счет включения в состав основных кибергрупп «посредников» из числа государственных служащих и представителей силовых структур. Учитывая, что деятельность «киберармий» в данном случае будет подчинена профильным государственным институтам монархий Залива, а любые попытки действовать самостоятельно непременно будут жестко пресекаться, высок риск отказа большинства хакеров от такого формата сотрудничества с властями, что напрямую скажется на «ударном потенциале» аравийских монархий в киберпространстве.

Наиболее эффективным, на наш взгляд, мог бы стать «израильский» вариант, где находящиеся в ведении национальных правительств

кибергруппировки будут играть роль «тренировочных юнитов» – структур, в которых поступающие на службу специалисты в области компьютерной безопасности проходят первичную подготовку и отбор для последующего зачисления в государственные подразделения, участвующие в выстраивании цифровой обороны (по аналогии с израильским «Подразделением 8200»). При этом данный вариант предполагает, что зона ответственности включенных в систему киберкоманд будет разграничена (наступательные, оборонительные, разведывательные операции и т.д.), а концепт патриотично настроенных хакеров в его текущем смысловом наполнении будет вытеснен из государственной повестки образом хакера на государственной службе. Однако переход к «израильской» модели взаимодействия с хакерами потребует значительной предварительной подготовки – в первую очередь, перестройки существующей структуры ответственных за кибербезопасность военных и гражданских институтов, создания профильных образовательных учреждений и запуска программ непрерывной кадровой подготовки (по содержанию аналогичных израильским программам «Тальпийот» и «Хавацалот»). Однако очевидно, что пока аравийские монархии готовы к подобного рода реформированию институциональной системы сектора кибербезопасности.

В свете вышеуказанного можно ожидать, что формат отношений между представителями хакерских сообществ и властными структурами монархий Залива в обозримой перспективе вряд ли претерпит существенные изменения, а хакерская активность останется в числе серьезных рисков развития цифрового пространства рассматриваемых государств.

Таким образом, 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 на Ближнем Востоке, увеличивая его и без того

высокий конфликтный потенциал. Однако ни одно из государств Персидского залива не готово пожертвовать национальными интересами и безопасностью для разрядки обстановки. Как результат, противостояние в киберпространстве сегодня пролегает, в первую очередь, по линии региональных кризисов, где затронуты интересы аравийских монархий, Ирана и их прокси-сил (палестино-израильский, сирийский, йеменский и др.).

Развитие национальных систем кибербезопасности монархий Залива в настоящий момент характеризуется динамичностью и имеет восходящий вектор. За относительно короткое время государствам удалось выстроить, в целом, эффективную структуру цифровой защиты и достигнуть лидирующих позиций в мировых и региональных (ближневосточных и общеарабских) рейтингах готовности к отражению киберугроз. Вместе с тем национальный киберсектор всех аравийских монархий сохраняет жесткую зависимость от внешних поставщиков технологий цифровой защиты и готовых решений. Это не позволяет рассматриваемым странам выйти за пределы модели «догоняющего» развития как в сфере цифровизации, так и в вопросах создания безопасной цифровой среды.

Большинство проблем, с которыми сталкиваются монархии Залива, имеют системный характер и не могут быть решены без комплексного пересмотра государственной политики в области кибербезопасности. Это, в свою очередь, формирует запрос на выработку коллективных мер цифровой защиты, координацию усилий и расширение многостороннего сотрудничества.

ГЛАВА 3
ОСНОВНЫЕ НАПРАВЛЕНИЯ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА МОНАРХИЙ ЗАЛИВА В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

3.1. Региональные площадки взаимодействия: ССАГЗ, ЛАГ, ОИС

Совет сотрудничества арабских государств Залива (ССАГЗ) – региональная организация, объединяющая все шесть арабских монархий, расположенных в зоне Персидского залива: Бахрейн, Катар, Кувейт, ОАЭ, Оман и Саудовскую Аравию. Все они отличаются высокой степенью политической стабильности, их связывают отношения стратегического партнерства. В рамках Совета сотрудничества государства-члены принимают активное участие в решении региональных проблем и совместными усилиями защищают свои национальные интересы. К настоящему времени ССАГЗ считается единственным эффективным политическим и экономическим объединением на Ближнем Востоке и в арабском мире.

Вместе с тем интеграция государств на данной платформе имеет свою специфику. С момента своего создания в 1981 г. Совет сотрудничества в качестве интеграционного ориентира принял практику Европейского союза: приоритет экономической интеграции на начальных этапах становления, развитие торгово-экономические связей (2001 г.), частичное снятие тарифов во взаимной торговле (2003 г.), общий рынок труда (2008 г.), таможенный союз (2011 г.). Однако на политическом направлении адаптация интеграционного опыта Евросоюза, предложенная в 2013 г. Саудовской Аравией, продвигается с большими трудностями[208]. С 2011 г. Совет сотрудничества декларирует курс на повышение уровня интеграции, трансформацию из площадки многофункционального сотрудничества в полноценное интеграционное объединение с общей политикой в сфере

[208] Wahba M. GCC: a force for regional stability // AGSIW. 21.02.2017. URL: https://agsiw.org/gcc-force-regional-stability/ (accessed: 06.10.2023).

экономики и обеспечения безопасности, а также общей оборонной политикой[209]. В этой связи стала активно развиваться институциональная система ССАГЗ, дополняя новыми органами кооперации базовую структуру организации в лице Высшего совета (в составе глав государств), Министерского совета (министры иностранных дел стран – участниц), Генерального секретариата и ряда специализированных комитетов[210].

Рост геополитического веса ССАГЗ в мире и на Ближнем Востоке обусловлен быстрыми (относительно других сран арабского мира) темпами социально-экономического развития, что во многом стало возможным благодаря наличию крупнейших на планете запасов нефтегазовых ресурсов и запуском с 2016 г. стратегических программ диверсификации экономик «Видение». Технологическое сотрудничество вносит внушительный вклад в продвижение интеграционных процессов в ССАГЗ: оно ориентировано на кооперацию усилий стран-участниц в создании цифровой экономики, взят курс на разработку соответствующей единой стратегии и программы совместных мероприятий по ее реализации. С этой целью в 2016 г. было создано Управление по делам экономического развития (Economic Development Affairs Authority), подотчетное Высшему совету ССАГЗ. 34-й саммит Совета сотрудничества (2022 г.) поручил данному институту активизировать усилия по завершению экономической интеграции (единый рынок, таможенный союз, гармонизация экономических законодательств и т.д.), продвижению совместных инициатив в области разработки и внедрения новых технологий (включая технологии искусственного интеллекта), альтернативных источников энергии, проектов в области туризма и т.д. Кроме

[209] King Abdullah Statement to the 33rd Summit of the GCC Supreme Council in Bahrain, 24.12.2011. URL: https://www.saudiembassy.net/statements/king-abdullah-statement-33rd-summit-gcc-supreme-council-bahrain (accessed: 10.04.2023).

[210] About GCC // Cooperation Council for the Arab States of Gulf. URL: https://www.gcc-sg.org/en-us/AboutGCC/Pages/OrganizationalStructure.aspx (accessed: 10.04.2023).

того был принят ряд общих законов касательно регулирования сфер промышленности и сельского хозяйства[211].

Однако для Совета сотрудничества характерна внутренняя противоречивость, связанная со стремлением более развитых государств к проведению самостоятельной внешней политики, исходя из собственных национальных, а не коллективных интересов. Прежде всего речь идет о Саудовской Аравии, стремящейся к статусу ближневосточного лидера и сохранению своих ведущих позиций в ССАГЗ, а также об ОАЭ и Катаре. Кроме того, в Совете отсутствует единство мнений касательно архитектуры региональной безопасности и ситуации, сложившейся на Ближнем Востоке и в зоне Персидского залива после «арабской весны»; имеются разногласия по тактике выстраивания контактов с исламистскими организациями; между некоторыми странами не урегулированы территориальные споры и т.д. [212].

Проблемы кибербезопасности появились в национальной повестке монархий Залива в начале 2000-х гг., когда значительно возросла активность политически мотивированных групп хакеров и хактивистов, проводивших протестные акции (преимущественно в форме дефейсмента сайтов) в связи с развернувшейся на палестинских территориях «интифадой Аль-Акса» (2000–2004 г.), терактами в США 11 сентября 2001 г. и военной кампанией США в Ираке (март 2003 г.). По мере роста профессиональных навыков хакерского сообщества жертвами нападений с использованием информационно-коммуникационных средств, стали объекты критической инфраструктуры.

Это побудило государства ССАГЗ в 2006 г. принять решение о запуске своего первого совместного CERT, но этот проект был реализован лишь в 2012 г., причем по инициативе МСЭ ООН, на базе CERT Омана и в формате общеарабского регионального центра кибербезопасности (ITU-ARCC). Группа реагирования Омана стала также главным центром обмена

---

[211] GCC Supreme Council release final communique after 43rd summit // Saudi Gazette. 09.12.2022. URL: https://saudigazette.com.sa/article/627828 (accessed: 12.10.2023).
[212] Мелкумян Е.С. Арабские монархии Залива в XXI веке. С. 53–81.

информацией и координации действий для стран – участниц Совета сотрудничества, поэтому именно Оман возглавил созданный в дальнейшем Комитет CERT ССАГЗ (GCC CERT Committee). Комитет стал инициатором ряда значимых проектов, реализуемых сегодня на пространстве ССАГЗ: так, например, в июле 2020 г. была запущена специализированная платформа для выявления вредоносного ПО в странах – участницах ССАГЗ[213].

С целью улучшение координации коллективных усилий по борьбе с киберугрозами с 2016 г. CERT ССАГЗ проводят регулярные совместные учения по кибербезопасности на базе групп реагирования государств – членов. Наиболее высокий уровень кооперации CERT стран Совета сотрудничества продемонстрировали в период подготовки и проведения ЭКСПО в Дубае (2020–2021 гг.) и Чемпионата мира по футболу 2022 в Катаре, а также в период пандемии COVID-19[214].

Помимо Комитета CERT на площадке ССАГЗ действуют Постоянный комитет по кибербезопасности (Standing Committee for Cyber Security), Министерский комитет по электронному правительству (GCC eGovernment Ministerial Committee), Организация по разработке стандартов кибербезопасности (GCC Standardization Organization) и ряд других структур, ответственных за разработку и реализацию инициатив в области коллективной кибербезопасности[215].

Несмотря на очевидные подвижки в деле создания общей безопасной цифровой среды, Совет сотрудничества еще очень далек от создания эффективной архитектуры коллективной безопасности, что обусловлено комплексом факторов. Прежде всего следует отметить, что страны – участницы ССАГЗ приступили к планомерному форсированному строительству национальных систем национальной кибербезопасности, по сути, лишь во второй половине 2010-х гг., в условиях хаотизации

[213] Hassib B, Shires J. Cybersecurity in the GCC // MEP. 2022. № 29. P. 98.
[214] 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).
[215] Ibid.: Hassib B, Shires J. Cybersecurity in the GCC. P. 98–99.

общемировой системы международных отношений и ослабления глобальных структур безопасности, резкого ухудшения военно-политической ситуации на Ближнем Востоке и нарастающей атмосферы недоверия в регионе[216]. Соответственно каждая из монархий Залива делала ставку преимущественно на собственные силы, а не ССАГЗ, создавая собственные киберинфраструктуры и самостоятельно определяя требуемый для себя уровень киберготовности.

В этой связи между участниками Совета сотрудничества сразу возникли разногласия по условиям кооперации. Малые государства считают, что их вклад должен определяться исходя из национальных возможностей и не быть равнозначным с более сильными игроками; иными словами, основную нагрузку (финансовую, технологическую, организационную) должны взять на себя передовые страны в лице Саудовской Аравии и ОАЭ, имеющие продвинутые системы киберзащиты и входящие в мировой топ-5 по уровню готовности к отражению цифровых угроз. Такая модель кооперации не устраивает Эр-Рияд и Абу-Даби, поскольку требует от них значительных финансовых вливаний и чревата многократным увеличением нагрузки на национальный киберсектор[217].

Подобное расхождение позиций отчасти обусловлено тем, что, несмотря на совпадение приоритетов долгосрочного развития, конкретные, тактические задачи участников ССАГЗ отличаются в силу разницы экономического потенциала и имеющихся финансовых, технико-технологических, человеческих и иных ресурсов, как в сфере кибербезопасности, так и в вопросах социально-экономического развития в целом. Поэтому стратегические цели и задачи, которые ставят перед собой (в том числе в рамках «Видений») Саудовская Аравия, ОАЭ и Катар, более амбициозны и

[216] Кузнецов В.А., Наумкин В.В. Глобальные и региональные тренды «столетия+» на Ближнем Востоке // Вестник Моск. ун-та. Сер. МОиМП. 2023. №.1. С. 85–89.
[217] Shires J., Hakmeh J. Is the GCC cyber resilient? London, 2020. P. 5, 7-8.

масштабны по сравнению с теми, на которые ориентируются Оман, Кувейт и Бахрейн[218].

Внутренняя противоречивость ССАГЗ наиболее наглядно проявилась в период Катарского дипломатического кризиса 2017–2021 гг. Примечательно, что начало кризиса было спровоцировано наступательной кибероперацией, которую провела просаудовская хакерская команда «Кибермухи», разместив на сайте Катарского информационного агентства сфабрикованные проиранские комментарии. При этом на состоявшемся 4 месяцами ранее первом заседании только что созданного Постоянного комитета по кибербезопасности ССАГЗ участники встречи подчеркнули значимость кооперации и доверия в вопросах развития безопасной цифровой среды[219].

Источником противоречий внутри ССАГЗ стал и конструкт о «перманентной иранской угрозе», который, по сути, является одним из системообразующих элементов выстраиваемой монархиями Залива архитектуры коллективной кибербезопасности. Оман и Катар, например, не находятся с Ираном в постоянной конфронтации и убеждены, что эскалация противостояния с Ираном может мотивировать его на ответное форсированное наращивание наступательного киберпотенциала[220].

Тегеран умело использует разногласия внутри ССАГЗ с целью разобщения членов Совета и предотвращения создания единого антииранского цифрового фронта. Так, в период катарского дипломатического кризиса Тегеран намеренно снизил частоту кибератак по объектам Катара, усилив при этом давление на киберсистемы ключевых оппонентов Дохи в лице Саудовской Аравии и ОАЭ. Эр-Рияд и Абу-Даби расценили это как признак наличия между Катаром и Ираном неких тайных договоренностей, что

[218] Мелкумян Е.С. Арабские монархии Залива в XXI веке. С. 11, 43.
[219] Zibak A. Cyber (non)cooperation in the Gulf. URL: https://www.cyjax.com/cyber-noncooperation-in-the-gulf/ (accessed: 11.10.2023).
[220] El-Masry A. The Abraham Accords and their cyber implications. URL: https://www.mei.edu/publications/abraham-accords-and-their-cyber-implications-how-iran-unifying-regions-cyberspace (accessed: 17.10.2023).

усилило разобщение в рамках ССАГЗ[221]. Кроме того, именно умением играть на противоречиях объясняется тот факт, что на ирано-саудовских переговорах по снижению региональной напряженности Тегеран, фактически, диктовал Эр-Рияду свои условия. Поэтому после формальной нормализации двусторонних отношений в марте 2023 г. фактор иранской киберугрозы не утратил своей значимости.

Отсутствие единства мнений имеется и по вопросу о целесообразности сотрудничества с Израилем. Несмотря на многолетнее взаимодействие с Израилем в вопросах доступа к новейшим технологиям, в том числе технологиям цифровой защиты, а также подписание ОАЭ и Бахрейном «Соглашений Авраама», далеко не все страны ССАГЗ готовы принять Израиль в качестве гаранта кибербезопасности даже для части арабского мира, поскольку это может обернуться очередной дестабилизацией Ближнего Востока. Наиболее жесткую позицию в этом отношении демонстрирует Кувейт, который единственный из монархий Залива воздержался от взаимодействия с Израилем даже в «дискретном» формате[222].

Противоречия внутри ССАГЗ, нараставшие в течение последнего десятилетия, укрепили убежденность монархий Залива в том, что создание системы коллективной безопасности только в рамках ССАГЗ имеет мало шансов на успех без запуска аналогичных процессов во всех арабских странах. Однако на платформе *Лиги арабских государств (ЛАГ)*, главной интеграционной площадки арабского мира, участниками которой также являются монархии Залива, реализация идей коллективной цифровой защиты наталкиваются на еще большее количество преград.

В первую очередь речь идет о наличии «концептуального разрыва» в подходах к обеспечению кибербезопасности как внутри ССАГЗ и ЛАГ, так и по отношению арабского мира к имеющейся международно-правовой

---

[221] Bahrain uncovers Iran and Qatar cyber terrorism network // Gulf News. 20.05.2019. URL: https://gulfnews.com/world/gulf/bahrain/bahrain-uncovers-iran-and-qatar-cyber-terrorism-network (accessed: 18.10.2023).

[222] Khorrami N. Israel’s cybersecurity cooperation with the GCC states. Singapore, 2021. P. 12–14.

практике. Наглядным примером может служить Арабская конвенция о борьбе с преступлениями в области информационных технологий[223], принятая ЛАГ в декабре 2010 г. и ставшая первым региональным (в рамках арабского мира) соглашением по кибербезопасности (в данном случае – одного из ее ключевых элементов – о борьбе с киберпреступностью). Конвенция ЛАГ была подписана и ратифицирована всеми монархиями Залива, за исключением Саудовской Аравии, которая подписала этот документ, но воздержалась от его ратификации.

Арабская конвенция, по сути, является калькой с Будапештской конвенции о киберпреступности, принятой Советом Европы в 2001 г., однако между двумя документами имеется ряд существенных отличий (развернутое сравнение Будапештской и Арабской конвенций представлено в *Приложении I, Таблица 11*). Так, например, статья 12 Конвенции ЛАГ дает расширенное определение «киберпреступности», включая в него распространение «непристойного» контента, но при этом не обозначая четких параметров понятия «непристойности». Статья 14 декларирует право на неприкосновенность частной жизни, но в ней отсутствуют какие-либо строгие правила, обязывающие подписантов соблюдать конфиденциальность. Статья 21 позволяет государствам вводить жесткие наказания за онлайн-активизм и выражение мнений. По мнению экспертов ООН, размытость формулировок и неопределенность критериев атрибуции правонарушений в цифровой среде, заложенная в Конвенции ЛАГ, создает благоприятные условия для нарушения гражданских прав и свобод в арабских странах[224].

Хотя Арабская конвенция легла в основу разработанных и принятых в дальнейшем в странах ССАГЗ и ряде других арабских государств национальных законов о кибербезопасности, она до сих остается предметом острых дискуссий не только в арабских политических и экспертных кругах, но

[223] Arab Convention on Combating Information Technology Offences. Cairo, 2010.
[224] Development and harmonization of cyber legislation in the Arab region. P. 7–14.

и на площадке ЛАГ[225]. С учетом довольно быстро меняющихся реалий цифровой эпохи документ требует доработки по целому ряду направлений[226]. Например, в нем отсутствуют механизмы классификации и пресечения ряда преступлений, доля которых в Интернете в последнее время выросла: в их числе проявления расизма, ксенофобии, оправдание геноцида и преступлений против человечности, подстрекательство, кибербуллинг, цифровой харассмент и т.д. Также не представлена такая важная с точки зрения цифровой защиты группа параметров, как персональная ответственность и ответственность поставщиков телекоммуникационных услуг, и т.п.[227].

В ноябре 2021 г. ЛАГ утвердила «дорожную карту» разработки и согласования нового общеарабского закона в области защиты и повышения кибербезопасности с целью поддержки усилий по разработке всеобъемлющей правовой базы для борьбы с киберпреступлениями, усиления защиты технических систем и их компонентов[228]. Данная инициатива призвана модернизировать Арабскую конвенцию 2010 г., однако к настоящему времени она остается на стадии согласования общих ориентиров. На последних саммитах ССАГЗ 2021–2023 гг. страны-участницы также ограничились декларативными заявлениями поддержки указанного проекта ЛАГ, не предложив каких-либо конкретных мер и шагов по его реализации[229].

В сентябре 2023 г. новый импульс к развитию получил процесс институциализации формируемой в арабском мире коллективной системы

---

[225] بلتقييس المعني العربي العمل لفريق العاشر الاجتماع (X заседание Арабской рабочей группы по стандартизации). Cairo, 2016. P. 3–11.

[226] محاربة أخطار الفضاء السيبراني تبدأ ببنية تشريعية قوية. (Борьба с опасностями киберпространства начинается с сильной законодательной структуры) // Al-Arab. 07.03.2021. URL: https://alarab.co.uk/إنشاء-يقترح-والقانون-السيبرانية-كتاب-السيبراني-بالأمن-للتخصص-عالمية-منظمة (accessed: 06.10.2023).

[227] Cybercrime Laws in Arab Countries. Washington DC, 2021. P. 15, 45, 56.

[228] اقرار أول قانون عربي استرشادي لحماية الأمن السيبراني بالدول العربية (Принятие первого руководящего арабского закона о защите кибербезопасности в арабских странах) // Addustour. 03.11.2021. URL: http://www.addustour.com/articles/1249438 (accessed: 06.10.2023).

[229] قمة الرياض تؤكد وحدة الصف والتكامل الاقتصادي (Саммит в Эр-Рияде подтверждает идею единства и экономической интеграции) // Al Khaleej. 15.12.2021. URL: https://www.alkhaleej.ae/2021-12-15/قمة-الرياض-تؤكد-وحدة-الصف-والتكامل-الاقتصادي/أخبار-من-الإمارات/أخبار-الدار (accessed: 12.10.2023); GCC Supreme Council release final communique after 43rd summit // Saudi Gazette. 09.12.2022. URL: https://saudigazette.com.sa/article/627828 (accessed: 12.10.2023); Doha Declaration of the 44th Session of the Supreme Council of the Gulf Cooperation Council (Doha Summit) // Secretariat General of the GCC. 5.12.2023. URL: https://www.gcc-sg.org/en-us/MediaCenter/NewsCooperation/News/Pages/news2023-12-5-1.aspx (accessed: 12.01.2024).

кибербезопасности. В дополнение к уже имеющимся профильным структурам ЛАГ (Арабский региональный центр кибербезопасности ITU-ARCC, Арабская рабочая группа по стандартизации и др.) по инициативе Саудовской Аравии был создан Совет министров арабских стран по кибербезопасности (Council of Arab Ministers of Cybersecurity), включающий в себя Генеральный секретариат и Исполнительный офис[230]. Тот факт, что штаб-квартира нового института ЛАГ размещена в Эр-Рияде, свидетельствует о признании арабским миром лидирующей роли Саудовской Аравии в вопросах кибербезопасности и ожидании от нее дальнейших инициатив по активизации регионального сотрудничества в борьбе с киберугрозами.

В феврале 2024 г. Саудовская Аравия представляла ЛАГ в Специальном комитете ООН по борьбе с киберпреступностью, на базе которого разрабатывается Международная конвенция о киберпреступности, которую планируется представить на утверждение Генеральной Ассамблее ООН[231]. Данное событие примечательно и с точки зрения того, что до недавнего времени Саудовская Аравия, как и другие страны ССАГЗ и ЛАГ, довольно неохотно включалась в дискуссии по вопросу заключения международных соглашений о киберпреступности, а также избегала обсуждения проблем применимости к киберпространству международного права о вооруженных конфликтах[232].

Помимо проблем гармонизации законодательного поля в области кибербезопасности и приведения его в соответствие с международно-правовыми практиками, предметом серьезных дискуссий в ЛАГ стал вопрос о выборе модели интеграции киберпотенциала государств-членов. В первую очередь речь идет о так называемой «арабской периферии», к которой относятся экономически слаборазвитые и политически нестабильные страны,

---

[230] Arab League announces establishment of Council of Ministers for Cybersecurity // Arab News. 11.09.2023. URL: https://www.arabnews.com/node/2371501/ (accessed: 22.01.2024).

[231] Saudi Arabia engages in UN cybercrime convention negotiations in New York // KSA.com. 2.02.2024. URL: https://www.ksa.com/saudi-arabia-engages-in-un-cybercrime-convention-negotiations-in-new-york (accessed: 10.02.2024).

[232] Hassib B, Shires J. Cybersecurity in the GCC. P. 100.

с низким уровнем цифровизации и практически отсутствующим сектором киберзащиты (Йемен, Ливия, Джибути, Сомали, Мавритания и др.[233]).

Большинство государств ЛАГ поддерживают предложенную Египтом и Иорданией модель «гармоничного со-развития» арабского кибермира, которая предусматривает помощь «периферийным» странам со стороны государств с передовыми практиками цифровой защиты, прежде всего Саудовской Аравии, ОАЭ и Египта. Данная позиция исходит из того, что «цифровая периферия» генерирует внушительную долю угроз, прежде всего в форме кибертерроризма[234].

До недавнего времени страны ССАГЗ продвигали иной формат арабской цифровой кооперации на площадке ЛАГ, в рамках которого предлагалось временно исключить из проекта коллективной кибербезопасности «периферийные» страны (например, Ливию) ввиду высоких политических рисков и необходимости внушительных финансовых и иных дотаций в их цифровизацию и защиту[235]. Избирательный подход членов ССАГЗ к формированию коллективной киберзащиты в рамках ЛАГ подвергался серьезной критике со стороны политических кругов и общественности других арабских стран, особенно «проблемных». Тем не менее Совет сотрудничества продолжал отстаивать свою позицию. Более того, монархии Залива стали воплощать его в жизнь путем наращивания двустороннего сотрудничества с наиболее влиятельными арабскими государствами с развитым сектором кибербезопасности.

Наибольший интерес в данном случае представляют *Арабская Республика Египет* и *Иорданское Хашимитское Королевство*. Обе страны занимают важное место в структуре региональных альянсов, выстраиваемых под эгидой США (и имеют статус внеблоковых партнеров НАТО), а также

---

[233] GCI, 2020. P. 29.

[234] Cybercrime Laws in Arab Countries. P. 40-46; "الإلكتروني الإرهاب .. هل يتحول لمصدر التهديد الأول للعالم؟ ("Кибертерроризм»: превратится ли он в первостепенный источник угрозы миру?) // Al Khaleej. 05.04.2016. URL: https://alkhaleej.net/علوم-وتكنولوجيا/الإرهاب-الإلكتروني-هل-يتحول-لمصدر-التهديد-الأول-للعالم؟ (accessed: 06.10.2023).

[235] 8th Abu Dhabi Strategic Debate // EPC. 15.11.2021. URL: https://www.youtube.com/m-X3rpZVSMw (accessed: 19.10.2023).

прилагают значительные усилия по продвижению инициатив в области коллективной кибербезопасности под эгидой ЛАГ.

Египет занимает довольно высокие позиции в глобальном рейтинге киберготовности МСЭ ООН (23 место) и среди арабских стран (4 место после Саудовской Аравии, ОАЭ и Омана)[236]. Каир, как и Эр-Риядом с Абу-Даби, делает ставку на цифровизацию (что закреплено в его стратегии развития «Vision»[237]) и активно продвигает на платформе ЛАГ собственное видение системы общеарабской кибербезопасности.

Египет не имеет профильных соглашений ни с одной из стран ССАГЗ, но тесное сотрудничество по отдельным направлениям кибербезопасности (например, в энергетическом секторе) развивается с Саудовской Аравией и Бахрейном; взаимодействие с ОАЭ и Оманом осуществляется по торговле криптовалютными активами и противодействию киберпреступности. С Катаром у Египта сохраняется некоторое взаимное недоверие, обусловленное последствиями Катарского дипломатического кризиса (2017–2021 гг.), что ограничивает потенциал их сотрудничества. Однако Каир и Доха предпринимают существенные усилия по нормализации деловых отношений, главным образом за счет активизации бизнес-контактов в секторе связи и телекоммуникаций, энергетики и туризма[238].

Положение *Иордании* в рейтингах МСЭ ООН в сравнении с Египтом несколько скромнее (10 место среди арабских стран и 71 место в мире)[239], однако страна демонстрирует тенденцию к укреплению позиций за счет наращивания темпов международного сотрудничества и постепенного превращения в региональный хаб кибербезопасности. Так, в сентябре 2023 г. в Аммане прошел «Dot Cyber Summit», организованный Национальным центром кибербезопасности и Ассоциацией информационно-

[236] GCI 2020. P. 25, 29.
[237] Egypt Vision 2030. Cairo, 2018. 37 p.
[238] Salah A. Realigning priorities: Egypt's strategic shift toward Qatar, Turkey, and Iran // MEI. 25.07.2023. URL: https://www.mei.edu/publications/realigning-priorities-egypts-strategic-shift-toward-qatar-turkey-and-iran (accessed: 30.01.2024).
[239] GCI 2020. P. 26, 29.

коммуникационных технологий Иордании. Мероприятие было посвящено вопросам развития межарабского сотрудничества в условиях глобализации цифровых угроз и стало первым в истории страны форумом, полностью организованным иорданскими институтами кибербезопасности[240]. В работе «Dot Cyber Summit» приняли участие представители всех монархий Залива, что свидетельствует о высоком уровне данной площадки взаимодействия.

Как и в случае с Египтом, в отсутствие профильных межгосударственных соглашений взаимодействие между Иорданией и государствами ССАГЗ динамично развивается в частном секторе. Монархии Залива в большинстве своем склонны рассматривать Иорданию как перспективный рынок для расширения деятельности своих IT-компаний. За последнее десятилетие присутствие в Иордании заметно нарастили саудовский, эмиратский и катарский технологический бизнес, увеличилось число киберфирм, созданных гражданами Кувейта и Омана; активизировалось сотрудничество частных образовательных учреждений Иордании и Бахрейна в области разработки проектов EdTech. Ярким примером взаимовыгодного сотрудничества в области EdTech является цифровая образовательная платформа «Little Thinking Minds» (LTM), разработанная одноименной иорданской стартап-компанией. Платформа ориентирована на повышение уровня грамотности обучающихся и интеграцию в образовательный процесс передовых методик преподавания. По состоянию на начало 2024 г., к платформе подключено более 500 образовательных учреждений (включая школы всех аравийских монархий), суммарная аудитория платформы составляет более чем 200 тыс. пользователей; официальные представительства LTM открыты в двух странах ССАГЗ (Саудовская Аравия, ОАЭ), а сам проект пользуется поддержкой профильных государственных институтов[241].

---

[240] Jordan's first Cyber Security Summit to kick off next Monday // Ammon News. 23.09.2023. URL: https://en.ammonnews.net/article/68169 (accessed: 30.01.2024).

[241] Little Thinking Minds (EdTech Platform). URL: https://www.littlethinkingminds.com/en/about-us/ (accessed: 30.01.2024).

Следует также отметить, что Египет и Иордания, будучи первыми арабскими странами, подписавшими мирный договор с Израилем, были вовлечены (на уровне местных киберфирм) в качестве посредников в дистрибуцию программного обеспечения израильского производства на рынок региона (в первую очередь, в страны Персидского залива[242]) и тем самым внесли свой вклад в развитие национальных систем кибербезопасности некоторых стран ССАГЗ.

Что касается других арабских стран, занимающих относительно высокие позиции в региональном рейтинге кибербезопасности (Тунис, Марокко), взаимодействие с ними по вопросам реагирования на цифровой вызов не является приоритетным для монархий Залива и носит несистемный характер (за исключением взаимодействия в рамках ЛАГ и ОИС, а также рабочих площадок ООН).

В последние годы государства – члены ССАГЗ пересмотрели свою позицию касательно «периферийных» стран арабского мира и присоединились к участию в создании там безопасной цифровой среды, но без прямого финансирования проектов. Так, например, Саудовская Аравия с 2019 г. вовлечена в формирование профильных институтов в Сомали и Джибути (используя для этих целей в том числе площадку Совета стран Красного моря и Аденского залива)[243]; ОАЭ способствует формированию первых элементов кибербезопасности у органов Южного переходного совета (ЮПС) в Йемене[244].

В заключение следует сказать об *Организации исламского сотрудничества* как потенциальной площадки развития кооперации в сфере кибербезопасности на Ближнем Востоке. сотрудничества аравийских монархий в области кибербезопасности. С одной стороны, в рамках ОИС

---

[242] How Israeli spyware was sold to Egypt and pitched to Qatar and Saudi Arabia // Haaretz. 05.10.2023. URL: https://www.haaretz.com/israel-news/security-aviation/2023-10-05/how-israeli-spyware-was-sold-to-egypt-and-pitched-to-qatar-and-saudi-arabia/ (accessed: 30.01.2024).

[243] Шмелева Т. К вопросу о создании Совета арабских и африканских государств // ИБВ. 08.01.2020. URL: http://www.iimes.ru/?p=65692 (дата обращения: 11.10.2023).

[244] 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).

созданы специализированные структуры, позволяющие объединить усилия мусульманских государств в области цифровой защиты. В их числе Центр по противодействию кибертерроризму (с 2017 г.)[245] и Рабочая группа по безопасному использованию 5G-технологий (с 2021 г.)[246]. Кроме того, постоянной площадкой для обмена мнениями и опытом в рамках ОИС является формат Ежегодных конференций OIC-CERT, проводимых с 2009 г.

Вместе с тем ввиду разнородности и противоречивости самого исламского мира инициативы ОИС, как правило, имеют самый общий характер и сосредоточены преимущественно на подготовке профильного кадрового потенциала и обмене информацией в рамках деятельности групп CERT. Более того, значительная часть инициатив, реализуемых на платформе ОИС, носит рекомендательный характер и ориентирована на немедленную имплементацию в национальный киберсектор стран-участниц. В этой связи сотрудничество с ОИС по линии кибербезопасности остается для монархий Залива важным, но не ключевым направлением.

В целом можно резюмировать, что декларируемый монархиями Залива курс на развитие коллективной системы кибербезопасности в рамках ССАГЗ еще далек от реализации его на практике, несмотря на серьезные подвижки в вопросах профильной кооперации по линии национальных групп реагирования на чрезвычайные ситуации (CERT) и строительство институциональной структуры взаимодействия. Монархии Залива продолжают отдавать предпочтение более гибкому формату сотрудничества – на двусторонней основе, а достижения такого диалога зачастую позиционируются как результат совместной работы членов ССАГЗ.

Отсутствие высокой динамики в разработке и продвижении проектов коллективной киберзащиты в значительной степени обусловлено наличием внутренних противоречий в ССАГЗ, порождающих атмосферу недоверия и

---

[245] OIC will soon establish a Cyber Security Center to combat cyberterrorism // OIC. 7.11.2017. URL: https://www.oic-oci.org/topic/?t_id=16023&t_ref=8082&lan=en (accessed: 10.12.2021).

[246] OIC-CERT launch 5G Security Working Group at GISEC 2021 // Intelligent CIO. 1.06.2021. URL: https://www.intelligentcio.com/oic-cert-launch-5g-security-working-group (accessed: 15.12.2021).

подозрительности, а также незавершенностью процесса формирования собственных национальных систем кибербезопасности стран – участниц. Кроме того, с учетом глобализации угроз, исходящих из цифрового пространства, идея создания отдельно взятой зоны «цифрового благополучия», особенно в таком высоко конфликтном регионе, как Ближний Восток, очевидно, имеет целый ряд концептуальных уязвимостей. В этой связи государства ССАГЗ вынуждены расширять географические контуры проектов коллективной кибербезопасности и включать в свою повестку вопросы развития межарабского сотрудничества на данном направлении.

Лига арабских государств сегодня выступает ключевой площадкой взаимодействия, в рамках которой формулируется общая для всех арабских стран повестка кибербезопасности. Однако, как и в случае с ССАГЗ, несмотря на уже имеющиеся в ЛАГ довольно серьезные наработки по продвижению инициатив коллективной цифровой защиты, внутренняя разнородность и противоречивость арабского мира (безусловно, несравнимая с внутренним конфликтным потенциалом ССАГЗ) ограничивает динамику и темпы кооперации. Вместе с тем следует признать, что в силу геополитического веса Лиги, представляющей на международной арене интересы всех арабских государств, в том числе монархий Залива, 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.

Одна из ключевых причин пробуксовки идей совместного обеспечения цифровой безопасности на площадках ССАГЗ и ЛАГ, кроме того, заключается в том, что имеющийся на Ближнем Востоке запрос на снижение конфликтного потенциала побуждает государства региона уделять повышенно внимание развитию военного сектора национальных систем кибербезопасности. В этой связи представляется целесообразным рассмотреть проекты кооперации стран

– участниц ССАГЗ по вопросам обеспечения цифровой защиты в рамках их военного сотрудничества.

3.2. Военное сотрудничество и кибербезопасность

Военное сотрудничество является одним из ключевых направлений деятельности ССАГЗ практически с момента создания этой организации. Оно нацелено на охрану суверенитета и территориальной целостности государств-членов, предотвращение внешней агрессии, защиту от действий радикально-экстремистских и террористических группировок, обеспечение региональной безопасности в зоне Персидского залива[247].

С 2004 г. государства ССАГЗ входят в состав международной антитеррористической коалиции, с 2006 г. на площадке Совета действует постоянная антитеррористическая комиссия. Все страны-участницы на двусторонней основе имеют оборонные соглашения с США, Великобританией и Францией. Взаимодействие с НАТО реализуется с 2004–2005 гг. в рамках Стамбульской инициативы по сотрудничеству (Istanbul Cooperation Initiative, ICI), к ней присоединились все члены ССАГЗ, за исключением Саудовской Аравии и Омана, которые, тем не менее, принимают участие в отдельных направлениях деятельности ICI. Для расширения кооперации по линии ССАГЗ – НАТО с 2017 г. в Кувейте действует Региональный центр НАТО.

Совместные вооруженные силы «Щит полуострова» (Peninsula Sield) были сформированы в 1984 г., спустя всего три года после создания ССАГЗ; в 2014 г. их численность составляла порядка 30 тыс. человек. «Щит» включает сухопутные, военно-воздушные и военно-морские подразделения, которые в составе международных коалиций принимали участие в ряде военных операций (Ирак, 1991 г.), в том числе по линии сотрудничества с НАТО – в Афганистане (2001 г.), Ливии (2011 г.) и Аденском заливе (2012 г.), а также

[247] Косач Г.Г., Мелкумян Е.С. ССАГЗ как военно-политическая организация // Вестник Моск. ун-та. Сер. МОиМП. 2012. № 4. С. 39–69.

были введены в Бахрейн (2011 г.) для обеспечения безопасности этого государства в связи с «арабской весной». В рамках ССАГЗ разработана Совместная оборонная стратегия, имеется единая система ПВО «Щит мира», сформированы Высший оборонный совет и Объединенное военное командование, действуют центры по защите от нападений с воздуха и моря, ведется подготовка собственных кадров в Военной академии, регулярно проводятся совместные военные учения (Joint Peninsula Shield Military Drill, Peninsula Shield Force Drill «Takamul»). В январе 2021 г. на саммите глав государств – членов ССАГЗ в г. Аль-Ула (Саудовская Аравия) было принято решение о повышении уровня интеграции в военной сфере и согласован ряд инициатив по его реализации[248].

Учитывая, что из триады киберугроз наибольшую опасность в зоне Персидского залива представляет использование ИКТ-инструментов в военных целях, развитие цифровой компоненты «Щита полуострова» является логичным шагом. Однако в силу того, что речь идет о военной сфере, подобного рода материалов в публичном доступе крайне мало, а в случае с киберпространством дополнительные ограничения накладывает и «чувствительный» характер искомой информации. Тем не менее о наличии тренда на развитие в рамках «Щита» цифровых инструментов проведения военных оборонительных операций можно судить по косвенным признакам. Так, например, в ОАЭ технологии искусственного интеллекта активно внедряются в планирование военных операций и учебное моделирование, а отработка навыков киберзащиты проводится во всех родах войск (сухопутных, воздушных и морских силах)[249]. Обмен передовыми практиками в области совместной обороны и безопасности проводится в рамках совместных военных учений «Щита полуострова», которые, как правило, проходят при непосредственном участии иностранных советников (США, Великобритании,

[248] Мелкумян Е.С. Арабские монархии Залива в XXI веке. С. 90–101, 196.

[249] Artificial intelligence in UAE military // Times Aerospace. 19.02.2023. URL: https://www.timesaerospace.aero/news/defence/artificial-intelligence-in-uae-military (accessed: 10.02.2024).

НАТО и др.) и свидетельствуют о значимой роли внешних акторов в развитии силовой компоненты монархий Залива.

Главным стратегическим и военным союзником стран ССАГЗ являются США. Эти отношения проверены временем и базируются на совпадении стратегических интересов – поддержании стабильности в зоне Персидского залива, а также на схожей позиции касательно путей урегулирования региональных конфликтов. Последнее десятилетие в качестве общих стратегических противников выступают Иран и терроризм, а в свете развернувшихся на Ближнем Востоке кибервойн повестка военного сотрудничества дополнилась вопросами обеспечения кибербезопасности, в том числе киберсдерживания Ирана и противодействия кибертерроризму. Стремление стран ССАГЗ к сотрудничеству с Вашингтоном по проблемам цифровой защиты, кроме того, обусловлено абсолютным мировым лидерством США в данной сфере[250].

Подход США к обеспечению цифровой защиты (включая ее внешний контур) изложен в Национальной стратегии кибербезопасности, которая, как правило, регулярно обновляется и актуализируется. Согласно последней версии этого документа (март 2023 г.), Белый дом выделяет 5 ключевых направлений политики США в сфере кибербезопасности: защита критической инфраструктуры, противодействие киберпреступности и кибертерроризму, развитие системы рыночных стимулов повышения культуры кибербезопасности (безопасность «интернета вещей»), инвестиции в наукоемкие отрасли (защита информации в постквантовом будущем) и развитие международного сотрудничества в области кибербезопасности[251].

В 2023 г. также была обновлена Стратегия кибербезопасности министерства обороны США, согласно которой основная угроза США в киберпространстве исходит от государственных акторов в лице Китая, России, Ирана и КНДР, а также со стороны радикально-экстремистских группировок

[250] GCI 2020. P. 25.
[251] National Cybersecurity Strategy, March 2023. Washington, 2023. P. 7–33.

и транснациональной преступности. Среди приоритетных направлений деятельности в киберпространстве Пентагон выделяет защиту критической инфраструктуры путем своевременного совершенствования моделей реагирования и обеспечения оборонительных и наступательных возможностей (проактивная оборона); интеграцию кибероперaций в долгосрочное военное планирование; развитие комплексного диалога с союзниками по вопросам цифровой защищенности (расширение круга партнеров и форматов сотрудничества, участие в развитии военного киберпотенциала партнеров США); совершенствование национальной культуры кибербезопасности и повышение общей осведомленности вооруженных сил о цифровой угрозе[252].

В целом, оба документа нацелены на решение общей стратегической задачи – комплексную защиту интересов США и их ключевых союзников от угроз со стороны государственных и негосударственных акторов в киберпространстве. Кроме того, и общенациональная, и военная стратегии схожим образом определяют круг угроз и предполагают значительную ставку на международное сотрудничество (включая вовлечение Вашингтона в развитие систем национальной киберзащиты своих ключевых союзников), что довольно полно проявляется в рамках стратегического диалога между США и монархиями Залива.

За поддержание стабильности на Ближнем Востоке и в зоне Персидского залива несет ответственность Центральное командование США (CENTCOM). Регион также входит в сферу особого внимания американского Киберкомандования (USCYBERCOM), которое проводит наступательные и оборонительные операции в киберпространстве США и их союзников, а также осуществляет защиту их критической инфраструктуры и военных объектов[253]. О проведении Киберкомандованием США военных операций в цифровом

[252] Department of Defense: Cyber Strategy 2023. URL: https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF (accessed: 11.12.2023).
[253] Haizler O. The United States' cyber warfare history // Cyber, Intelligence, and Security. 2017. № 1. P. 38–41.

пространстве Ближнего Востока стало известно в феврале 2016 г. в связи с заявлением главы Пентагона Эштона Картера о начале полномасштабной кибервойны против ИГИЛ (запрещена в РФ) в форме кибератак на финансовые и логистические сервисы группировки, а также ее аккаунты в соцсетях для предотвращения вербовки и распространения пропаганды. Из заявления американского министра обороны, кроме того, следовало, что ранее Киберкомандование было сосредоточено преимущественно на противодействии Ирану[254].

Страны ССАГЗ также обеспечивают непосредственное военное присутствие США в Персидском заливе. В Бахрейне уже более 70 лет базируется Пятый флот США, в Катаре располагается крупнейшая военная база США за рубежом. Другие страны ССАГЗ, предоставляют свои военно-воздушные и военно-морские базы для американских вооруженных сил на период осуществления конкретных военных операций на Ближнем Востоке. В этой связи Бахрейн, Кувейт и Катар имеют статус «главного союзника США вне НАТО». В рамках усиления безопасности своих военных баз в Персидском заливе США инициируют участие военных специалистов стран ССАГЗ в программах по отработке навыков противодействия цифровым угрозам[255].

США внесли внушительный вклад в повышение обороноспособности государств – членов ССАГЗ путем поставок вооружений, активного участия в реализации проектов Совместной оборонной стратегии Совета сотрудничества, подготовки кадров и проведения совместных военных учений с силами «Щита» и вооруженными силами монархий Залива (например, многосторонние военные учения «Eagle Resolve 23», где моделирование тактики отражения киберугроз военными структурами было вынесено в отдельный тематический блок[256]). Военное сотрудничество с США

---

[254] Пентагон начал кибервойну против «Исламского государства» // РБК. 26.02.2016. URL: https://www.rbc.ru/politics/26/02/2016/56d04aca9a794756469e1f94 (дата обращения: 12.07.2022).

[255] U.S. security cooperation with Bahrain // US Department of State. 14.06.2021. URL: https://www.state.gov/u-s-security-cooperation-with-bahrain/ (accessed: 06.10.2023)

[256] Eagle Resolve 23 - Field Training Exercise // CENTCOM. 29.05.2023. URL: https://www.centcom.mil/Press-Release-View/Article/3409929/eagle-resolve-23-exercise-with-saudi-arabia/ (accessed: 10.02.2024).

реализуется, кроме того, в форме участия стран ССАГЗ в обеспечении морской безопасности в составе трех американских Объединенных оперативных групп Combined Task Forces, CTF) – CTF 151 (борьба с пиратством), CTF 152 (зона Персидского залива) и CTF 153 (Красное море, пролив Баб-эль-Мандеб и Аденский залив). В рамках развития стратегического партнерства Вашингтона и Эр-Рияда в 2022 г. США передали Саудовской Аравии командование CTF 150 (Оманский залив и северная часть Аравийского моря). Военно-морские силы стран ССАГЗ также принимают участие в морских учениях Пятого флота США Task Force, в рамках которых отрабатываются практические задачи применения высокотехнологичных морских вооружений, в том числе с использованием искусственного интеллекта[257].

Координация действий в военной сфере, по вопросам урегулирования региональных кризисов на Ближнем Востоке и обеспечения цифровой защиты ведется, кроме того, на площадках Форума стратегического сотрудничества США – ССАГЗ (с 2011 г.), в рамках которого действует совместная комиссия по безопасности, и саммитов США – ССАГЗ (с 2015 г.).

На полях первого саммита США – ССАГЗ, состоявшегося в Кэмп-Дэвиде в мае 2015 г., было принято решение об организации на регулярной основе совместных крупномасштабных военных учений по противодействию асимметричным угрозам со стороны террористических организаций, а также кибератакам и иным средствам ведения гибридных войн. Кроме того, США предложили направить в столицы стран – участниц ССАГЗ военную группу для обсуждения и принятия решения о путях активизации военного сотрудничества и обучения сил специальных операций в борьбе с терроризмом[258]. На втором саммите стороны согласовали ряд инициатив по

[257] Мелкумян Е.С. Арабские монархии Залива в XXI веке. С. 194–235.
[258] Annex to U.S.-GCC Camp David Joint Statement, May 14, 2015 // The White House. URL: https://obamawhitehouse.archives.gov/the-press-office/annex-us-gcc-joint-statement (accessed: 14.10.2023).

расширению военного сотрудничества, в том числе в вопросах обеспечения кибербезопасности в зоне Персидского залива[259].

При президенте Д. Трампе (2017–2021 гг.) военное сотрудничество вышло на качественно новый уровень. О значимости стран ССАГЗ во внешней политике США свидетельствовал визит Д. Трампа в Саудовскую Аравию 20–21 мая 2017 г., который стал первым в серии зарубежных турне нового главы Белого дома и был полон важных событий.

На полях третьего саммита США – ССАГЗ обсуждались вопросы совместных действий в области кибербезопасности, было принято решение о создании Совместной рабочей группы по противодействию терроризму, военным угрозам и угрозам, исходящим из киберпространства[260]. Призыв к консолидации исламского мира в борьбе против терроризма в военной, информационной и финансовой сферах также прозвучал в итоговой декларации саммита арабских и исламских стан и США, где были представлены 55 мусульманских государств[261].

Президент Д. Трамп и саудовский король Сальман бен Абдель Азиз приняли участие в торжественной церемонии открытия в Эр-Рияде Глобального центра по борьбе с экстремистской идеологией (Global Center for Combating Extremism Ideology, GCCEI). США и страны ССАГЗ также создали совместный Центр по противодействию финансированию терроризма (Terrorist Financial Target Center, TFTC) под руководством Вашингтона и Эр-Рияда. В задачи новой структуры входит выявление, отслеживание и обмен информацией о сетях финансирования терроризма и связанной с ними деятельности, представляющей взаимный интерес; координация совместных подрывных акций; помощь в наращивании потенциала для противодействия

---

[259] U.S. – GCC 2nd Summit Leaders Communique, April 21, 2016 // The White House. URL: https://obamawhitehouse.archives.gov/the-press-office/us-gcc-second-summit-communique (accessed: 14.10.2023).
[260] US, GCC Summit Communique condemns Iran's regional interferences // Al-Arabiya news. 22.05.2017. URL: https://english.alarabiya.net/News/gulf/US-GCC-Summit-communique (accessed: 14.10.2023).
[261] Riyadh Declaration. Arab-Islamic-American Summit // Saudi Press Agency, 21.05.2017. URL: https://www.spa.gov.sa/w410192 (accessed: 14.10.2023).

финансированию терроризма и связанных с ним рисков[262]. Американский президент, кроме того, анонсировал запуск проекта «Арабского НАТО» (данная инициатива будет рассмотрена ниже).

Решения, принятые в ходе визита Д. Трампа, по сути, стали очередным практическим шагом к реализации обозначившегося при Б. Обаме курса на сокращение прямого участия США в ближневосточных делах и передачи основных полномочий по обеспечению безопасности ведущим региональным акторам. По этой причине визит американского президента придал мощный импульс развитию двусторонних отношений между странами ССАГЗ и США. Это привело к внушительному росту военного потенциала стран ССАГЗ и укреплению двусторонних связей с США[263]. Наиболее показателен в данном контексте пример Саудовской Аравии.

Американо-саудовское военное сотрудничество в сфере кибербезопасности активно развивается с 2012 г.[264]. 20 мая 2017 г. США и Саудовская Аравия подписали соглашение о стратегическом партнерстве, которое в первую очередь было нацелено на обеспечение безопасности в зоне Персидского залива и предусматривало значительное расширение военного сотрудничества, прежде всего в области противодействия терроризму[265]. Декларацию дополнил крупный оружейный контракт на сумму 110 млрд долларов, который также затрагивал вопросы кооперации в сфере кибербезопасности[266]. В данном контексте следует отметить, что Саудовская Аравия является самым крупным покупателем американских вооружений[267].

Взаимодействие по вопросам кибербезопасности в рамках военного сотрудничества Вашингтона и Эр-Рияда получило дальнейшее развитие в ходе

---

[262] TFTC: History // Terrorist Financial Target Center. URL: https://www.tftc-istehdaf.org/history (accessed: 14.10.2023).
[263] Мелкумян Е.С. Арабские монархии Залива в XXI века. С. 207–212.
[264] Kingdom of Saudi Arabia cyber readiness. P. 19–20.
[265] Joint Strategic Vision Declaration for the USA and Kingdom of Saudi Arabia, May 20, 2017 // The White House. URL: https://trumpwhitehouse.archives.gov/statements/joint-strategic-vision-declaration (accessed: 14.10.2023).
[266] U.S. security cooperation with Saudi Arabia. Fact Sheet // U.S. State Department. January 20, 2021. URL: https://www.state.gov/u-s-security-cooperation-with-saudi-arabia/ (accessed: 12.11.2023).
[267] US dominates global arms sales, with Saudi Arabia the top customer // Axios. 16.03.2021 URL: https://www.axios.com/2021/03/16/global-arms-exports-us-russia-saudi-arabia-weapons (accessed: 12.11.2023).

визита нового президента США Дж. Байдена в Саудовскую Аравию 15–16 июля 2022 г. В итоговом коммюнике стороны подчеркнули значимость сотрудничества в сфере кибербезопасности «для защиты жизненно важных интересов и национальной безопасности обеих стран» и обязались «укреплять обмен информацией в режиме реального времени, наращивать человеческий и технический потенциал, а также развивать индустрию кибербезопасности»[268].

Кроме того, в рамках визита Дж. Байдена Национальное управление кибербезопасности Саудовской Аравии, с одной стороны, Министерство внутренней безопасности и Агентство кибербезопасности и защиты инфраструктуры США, с другой, подписали Меморандум о взаимопонимании в области кибербезопасности. Документ был нацелен на «дальнейшее укрепление лидирующих позиций двух стран на международном уровне путем развития интеграции и создания механизмов сотрудничества для достижения безопасного и надежного киберпространства»[269].

В рамках указанных соглашений в сентябре 2022 г. стартовал совместный проект Саудовской Аравии и Центрального командования США (CENTCOM) – Интегрированный испытательный центр «Красные пески» (Red Sands Integrated Experimentation Center, RSIEC). Новый военный центр базируется в Эр-Рияде и нацелен на тестирование различных методов электронной войны на больших открытых пространствах, апробацию инновационных подходов к обучению кадрового состава и повышению боеготовности вооруженных сил. Первая стадия проекта ориентировала на отработку тактики борьбы с беспилотными летательными аппаратами (БПЛА) как одной из ключевых форм противостояния Ирану, являющемуся крупнейшим в зоне Персидского залива производителем и экспортером боевых и разведывательных дронов. Испытания новых технологий в

---

[268] The Jeddah Communique, 15.07.2022 // White House. URL: https://www.whitehouse.gov/statements-releases/2022/07/15/the-jeddah-communique-a-joint-statement (accessed: 20.01.2023).

[269] Saudi National Cybersecurity Authority and U.S. Department of Homeland Security sign MoU to promote cybersecurity cooperation // Saudi Press Agency, 16.07.2022. URL: https://www.spa.gov.sa/2370312 (accessed: 14.10.2023).

противодействии растущей угрозе со стороны БПЛА позволит значительно усилить боеспособность сил ССАГЗ «Щит полуострова», действующих совместно с базирующими в Заливе американскими вооруженными силами[270].

Пример проекта «Красные пески» свидетельствует о том, что несмотря на доминирование формата двусторонних связей в ближневосточной политике Дж. Байдена, закрепленного в новой Стратегии национальной безопасности 2022 г.[271], США сохранили заинтересованность в интеграции ССАГЗ и усилении его военной мощи, в первую очередь в секторе военной кибербезопасности. Данный тезис подтверждают также итоги заседания Рабочей группы по Ирану саммита ССАГЗ – США, состоявшего в Эр-Рияде в феврале 2023 г. Стороны выразили приверженность стратегическому партнерству ССАГЗ – США и намерение расширять оборонное сотрудничество с целью противодействия Ирану, который обвинялся в дестабилизации обстановки на Ближнем Востоке, поддержке терроризма, а также использовании БПЛА, баллистических ракет и кибероружия и передаче их государственным и внесистемным акторам региональной политики[272].

Вместе с тем важно принять во внимание тот факт, что спустя месяц после столь серьезных обвинений в адрес Тегерана Саудовская Аравия и Иран достигли договоренностей о нормализации отношений, завершив двухлетние переговоры при посредничестве КНР, Омана и Ирака. Столь неожиданный шаг Эр-Рияда можно объяснить его недовольством политикой США после избрания Дж. Байдена, в рамках которой, несмотря на стратегической партнерство с ССАГЗ, Вашингтон не поддержал ряд инициатив Саудовской Аравии и ОАЭ (в отношении Ирана, Йемена и др.), а также стал активнее перекладывать на арабские страны ответственность за обеспечение

---

[270] Red Sands facility brings innovation, collaboration to counter-drone technology // Citadel. 31.08.2023. URL: https://centcomcitadel.com/en_GB/articles/ssc/features/2023/08/31/feature-03 (accessed: 21.11.2023).

[271] US National Security Strategy. October 2022 // The White House. URL: https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf (accessed: 21.11.2023).

[272] Joint statement by U.S. and GCC members on Iran, February 16, 2023 // The U.S. Department of States. URL: https://www.state.gov/joint-statement-by-the-united-states-and-gulf-cooperation-council-members-on-iran (accessed: 21.11.2023).

региональной безопасности[273]. Другой причиной стал провал попыток создать на Ближнем Востоке систему коллективной безопасности, которые были предприняты ЛАГ и США при поддержке стран ССАГЗ.

Первой и пока единственной попыткой сформировать общеарабский военный альянс является амбициозный проект *Объединенных арабских сил быстрого реагирования (ОАСБР),* обсуждавшийся в 2015 г. в ЛАГ по инициативе Египта. Формальной юридической основой альянса должен был стать Договор о совместной обороне ЛАГ 1950 г., а целью – поддержание региональной безопасности путем противодействия терроризму и проведения миротворческих операций. В составе ОАСБР предполагалось сформировать сухопутные, военно-воздушные и военно-морские подразделения, а также подразделения специального назначения общей численностью 40 тыс. человек. Штаб-квартиру ОАСБР планировалось разместить в Каире, общее командование возложить на Саудовскую Аравию, а финансирование проекта – на страны ССАГЗ. Несмотря на то, что готовность составить «костяк» коллективных вооруженных сил выразили ряд арабских стран, в том числе Саудовская Аравия, ОАЭ и Кувейт, процесс забуксовал уже в августе 2015 г., спустя 8 месяцев с начала обсуждения, когда Эр-Рияд при поддержке Бахрейна, Катара, Кувейта и ОАЭ воздержался от подписания протокола о создании ОАСБР.

Поводом к решению взять паузу в реализации проекта стали разногласия между Эр-Риядом и Каиром по вопросу размещения ОАСБР в Ливии, которая заявила о своем намерении сразу после создания сил обратиться в ЛАГ за помощью в подавлении на своей территории сети террористических группировок во главе с ИГИЛ (запрещена в РФ). Это сразу породило опасения, что ОАСБР могут быть использованы для вооруженного вмешательства в дела суверенных арабских государств, а не для поддержания безопасности. Стало очевидно, что идея военного арабского альянса еще «сырая» и требует

[273] Мелкумян Е.С. Арабские монархии Залива в XXI веке. С. 216.

тщательной проработки. Прежде всего необходимо было определиться с концепцией и соответственно правовым полем проекта – будет ли это договор о коллективной обороне по образцу НАТО, либо прототип системы коллективной безопасности ООН, либо следует пойти по пути Европейского союза и создать надгосударственные органы межарабского сотрудничества в области безопасности. И как борьба с терроризмом будет вписываться в функционал подобного рода структур с учетом неспособности арабских стран договориться о том, что собой представляет терроризм? Готовы ли арабские государства пожертвовать частью своего суверенитета в интересах коллективной обороны и безопасности?[274] В силу обозначенных причин проект ОАСБР оказался изначально нежизнеспособен.

В мае 2017 г. на смену ему пришел новый проект коллективной арабской обороны – *Ближневосточный стратегический альянс* (*Middle East Strategic Alliance, MESA*), неофициально именуемый «Арабское НАТО» за схожесть моделей управления с Североатлантическим блоком[275]. В отличие от проекта ОАСБР, который создавался по инициативе и на платформе ЛАГ, имел преимущественно оборонительный характер и нацеленность на борьбу с терроризмом, проект MESA был инициирован ключевым внерегиональным актором (США), имел ярко выраженную антииранскую направленность и был ориентирован на развитие партнерства между ведущими странами арабского мира (в лице государств ССАГЗ, Египта и Иордании) с Израилем, который должен был присоединиться к альянсу в качестве «intelligence state», т.е. взаимодействовать с блоком через США и исключительно по линии спецслужб.

Спустя всего две недели после того, как Д. Трамп на полях саммита США – ССАГЗ анонсировал проект MESA, разразился Катарский кризис. 5 июня 2017 г. три государства ССАГЗ – Саудовская Аравия, Бахрейн и ОАЭ,

[274] Gaub F. Stuck in the barracks: the Joint Arab Force. Brussel, 2015. P. 1–4.
[275] Guzansky Y., Michael K. Revisiting the Possibility of a Regional Military Alliance // INSS Insight. 2022. № 1561. P. 3–5.

а также Египет разорвали дипломатические отношения с Катаром. В 2019 г. США предприняли неудачную попытку перезагрузить проект, при этом в числе причин важности его возрождения Пентагон указывал на необходимость совместного противодействия возрастающей угрозе со стороны кибертерроризма[276].

Инициатором следующего проекта коллективной безопасности выступил Израиль, пригласив к его обсуждению министров иностранных дел ОАЭ, Бахрейна, Марокко и Египта в кибуц Сде-Бокер (Южный округ Израиля, пустыня Негев) в марте 2022 г. Тот факт, что представители Белого дома приняли участие в Негевском саммите в статусе приглашенных гостей должен был подчеркнуть внутрирегиональный характер встречи. Ключевая идея *«Негевской инициативы»* заключалась в продвижении процесса нормализации отношений Израиля с арабскими странами путем создания интеграционного блока с государствами, заключившими с ним мирный договор, а в качестве объединяющей идеи была предложена формула коллективной безопасности и объединения усилий в противостоянии «иранской угрозе». Однако попытка Израиля развить успехи арабо-израильской нормализации 2020–2021 гг. и стать полноправным интегрированным игроком на ближневосточном геополитическое поле закончилась неудачей. Участники встречи в Сде-Бокере разошлись во взглядах на суть «иранской угрозы». Кроме того, ввиду очередной пробуксовки палестино-израильского урегулирования от участия в Негевском саммите воздержались Иордания, имеющая мирный договор с Израилем, и Саудовская Аравия, которая, казалось бы, была готова последовать примеру ОАЭ и Бахрейна и вывести из тени свое многолетнее сотрудничество с Израилем, нормализовав отношения с ним. Судан, четвертый из подписантов «Соглашений Авраама», отсутствовал по причине

[276] Middle East Security Still Critical to U.S. // U.S. Department of Defense, 30.04.2019. URL: https://www.defense.gov/News/News-Stories/Article/Article/1829813/middle-east-security-still-critical-to-us/ (accessed: 21.11.2023).

внутреннего кризиса[277]. Провал «Негевской инициативы» свидетельствовал о том, что даже те арабские страны, которые развивали отношения с Израилем, пока не готовы принять «новую нормальность».

Несмотря на неудачу, Израиль предпринял новую попытку продвинуть идею обеспечения региональной безопасности на Ближнем Востоке со своим участием, но на этот раз под «брендом» кибербезопасности. В декабре 2022 г. на полях первой Арабской международной выставки-конференции по кибербезопасности, проходившей в Бахрейне, Израиль предложил арабским подписантам «Соглашений Авраама» (за исключением Судана) совместный проект *«Железный киберкупол» («Iron Cyber Dome»)*, в котором обыгрывалось название израильской системы противоракетной обороны дальнего действия «Железный купол». Проект был нацелен на защиту критической информационной инфраструктуры стран-участниц и кооперацию в вопросах выявления и реагирования на киберугрозы[278].

Новая инициатива также потерпела неудачу под влиянием палестинского фактора и разногласий между ОАЭ, Бахрейном и Марокко касательно допустимых пределов участия Израиля в обеспечении кибербезопасности арабских стран. Исключение Судана из киберпроектов Израиля объясняется сохраняющимся в стране внутриполитическим кризисом и низким уровнем развития национальной системы кибербезопасности (102 место в индексе МСЭ ООН[279]). Отсутствие интереса Израиля к включению кибербезопасности в сферу взаимодействия с Суданом может быть обусловлено, кроме того, уклонением Хартума от участия в расследовании киберинцидентов (в том числе кибератаки против израильской критической

[277] The Negev Summit furthers Arab-Israeli normalization // The U.S. Institute of Peace. 31.03.2022. URL: https://www.usip.org/publications/2022/03/negev-summit-furthers-arab-israeli-normalization (accessed: 14.10.2023).

[278] סייבר ברזל כיפת": המדפיסות ערב ומדינות "ישראל" של משותף פרויקט («Железный киберкупол»: совместный проект Израиля и арабских стран) // Tasnim. 15.12.2022. URL: https://www.tasnimnews.com/he/news/2022/12/15/2822055/ (accessed: 20.01.2024).

[279] GCC 2020. P. 26.

информационной инфраструктуры[280]), ответственность за которые предположительно несет хакерская группировка «Anonymous Sudan», якобы состоящая из граждан этой страны.

Финальная (на сегодняшний день) попытка создать на Ближнем Востоке региональную систему кибербезопасности была предпринята в январе 2023 г. на полях международной выставки «Cybertech Global 2023» в Тель-Авиве. Министерство внутренней безопасности США и Национальное управление кибербезопасности Израиля обратились к подписантам «Соглашений Авраама» в лице ОАЭ, Бахрейна и Марокко с предложением создать совместную систему цифровой защиты *«Региональный киберкупол»*, ориентированную, в первую очередь, на противодействие растущим киберугрозам со стороны Ирана. Проект предусматривал формирование конкретных механизмов оперативного сотрудничества между правительствами стран-участниц и продвижения государственно-частного партнерства в сфере кибербезопасности. Концептуальное отличие новой инициативы от всех предыдущих проектов, предусматривавших различного рода экономические выгоды и привилегии для участников, состояло в том, что она базировалась исключительно на приоритете императивов безопасности. Обосновывая новый подход США и Израиля к обеспечению региональной кибербезопасности на Ближнем Востоке, экс-директор ЦРУ Дэвид Х. Петреус заявил: «За последнее десятилетие геополитика резко трансформировалась из мира благоприятной глобализации, в котором экономика определяет геополитику, в мир возобновленного соперничества великих держав, в котором геополитика все больше определяет, что возможно с точки зрения экономических инвестиций, торговли и т. д.»[281].

---

[280] Mossad targeted in major cyber-attack by Sudanese hackers // Mehr. 25.04.2023. URL: https://en.mehrnews.com/news/199880/Mossad-targeted-in-major-cyber-attack-by-Sudanese-hackers (accessed: 20.01.2024).

[281] 'We are expanding the Abraham Accords to cybersecurity,' US Homeland Security Official says // Media Line. 31.01.2023. URL: https://themedialine.org/life-lines/we-are-expanding-the-abraham-accords-to-cybersecurity-us-homeland-security-official-says/ (accessed: 20.01.2024).

В рамках продвижения проекта ближневосточного *«Регионального киберкупола»* в мае 2023 г. двухпартийной группой сенаторов США был разработан проект «Закона о сотрудничестве со странами – участницами “Соглашений Авраама” в области кибербезопасности» (The Abraham Accords Cybersecurity Cooperation Act), который базировался на идее коллективной защиты от общих киберугроз и имел ярко выраженную антииранскую направленность[282].

Однако и эта инициатива не получила развития в свете участившихся в арабском мире шпионских скандалов с участием израильских киберфирм[283], а начавшийся процесс эскалации палестино-израильского конфликта (сначала на Западном берегу реки Иордан в июне 2023 г., а затем в Секторе Газа в октябре 2023 г.) привел к окончательной заморозке проекта.

Таким образом, кибербезопасность является одним из ключевых направлений международного сотрудничества монархий Залива в военной сфере, которое в последние годы развивается преимущественно в формате двусторонних отношений монархий Залива с США. Кибербезопасность также играет важную роль в формировании подходов к обеспечению региональной безопасности на Ближнем Востоке. Однако высокий уровень взаимного недоверия, стремление США, Израиля и ряда стран ССАГЗ заложить в основу системы коллективной кибербезопасности довольно неоднозначную идею «перманентной угрозы» со стороны Ирана, отсутствие комплексного осмысления причин заморозки прежних проектов, а также зависимость от позиции США (ключевого внерегионального модератора всех перечисленных ранее инициатив) обуславливают проблемы с их практической реализацией. Кроме того, неготовность стран ССАГЗ подкреплять запускаемые ими проекты документально (то есть подписывать многосторонние договоры и

[282] New bill aims to boost cybersecurity cooperation between U.S., Abraham Accords nations // Axios. 31.05.2023. URL: https://www.axios.com/2023/05/31/bill-cybersecurity-cooperation-abraham-accords-nations (accessed: 30.07.2023).
[283] Israeli spy company attempted hacking phones of Qatar residents, investigation reveals // Doha News. 10.03.2023. URL: https://dohanews.co/israeli-spy-company-attempted-hacking-phones (accessed: 10.01.2024).

соглашения) ради сохранения пространства для маневра закладывает весьма скромные пределы развития коллективных инициатив и ведет к их постепенному демонтажу.

3.3. Роль внерегиональных акторов в формировании безопасной цифровой среды в аравийских монархиях

Международное сотрудничество в сфере кибербезопасности приобретает исключительную значимость для монархий Залива с учетом «догоняющего» развития их национальных секторов цифровой защиты, ставки на технико-технологическую и кадровую помощь извне, а также приоритета императивов безопасности в деятельности ССАГЗ. В области киберзащиты в качестве ключевых внерегиональных партнеров (внешних по отношению к региону Ближнего Востока) для государств – членов ССАГЗ 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.

Соединенные Штаты Америки. На рынках цифровых технологий стран ССАГЗ доминируют американские компании (*см.: Приложение I, Таблица 12*), прежде всего ведущие игроки мировой IT-индустрии в лице Microsoft, IBM, Cisco, McFree, Oracle и др. Они также осуществляют поставки программного обеспечения (включая технологии защиты от компьютерных вирусов) для гражданского сектора кибербезопасности. Начиная с первой половины 2000-х гг. данный сегмент ближневосточного рынка постоянно растет – с 44,31 млн долларов в 2002 г.[284] до 14,8 млрд долларов в 2022 г.[285], и основным потребителем услуг остаются именно монархии Залива, чьи системы

[284] Security software booms in the Gulf // Edge. 24.08.2003. URL: https://www.edgemiddleeast.com/news/476981-security-software-booms-in-the-gulf (accessed: 10.02.2024).
[285] Middle East Cyber Security Market Size & Share. URL: https://www.marketsandmarkets.com/Market-Reports/middle-east-cyber-security-market-121119697.html (accessed: 20.02.2024).

цифровой защиты требуют постоянной подпитки технологиями. Это позволяет США контролировать значительную часть технологических цепочек и влиять на вектор развития национальных систем кибербезопасности аравийских монархий.

Текущий уровень вовлеченности США в развитие гражданского сектора кибербезопасности стран ССАГЗ можно охарактеризовать как высокий. США вносят колоссальный вклад в наращивание технологического и кадрового потенциала монархий Залива (в качестве элемента стабилизации национальных систем цифровой защиты), а также в развитие индустрии кибербезопасности в целом, оказывая помощь в решении широкого круга профильных проблем – от совместной защиты банковских данных[286] до обмена информацией о киберугрозах в режиме реального времени. Соответствующие договоренности достигнуты со всеми странами ССАГЗ.

Особое внимание США уделяют развитию кадрового потенциала. В качестве примера можно привести деятельность SANS Institute – частной американской компании, специализирующейся на подготовке специалистов в области информационной безопасности, включая противодействие кибератакам в гражданском секторе и повышение эффективности реагирования на компьютерные инциденты[287]. Специалисты SANS Institute на регулярной основе проводят мероприятия в каждой из монархий Залива, а в конце 2023 г. ими был организован первый общий формат для ССАГЗ[288], ставший крупнейшим мероприятием в сфере кибербезопасности в регионе Персидского залива, устроенным частным подрядчиком. Следует также отметить, что компания SANS Institute имеет в своем портфолио и разработки оборонного спектра (в частности, интерактивную утилиту NetWars, предназначенную для моделирования сценариев кибератак и используемой в

[286] Treasury Announces Cyber Security Cooperation MoU with the United Arab Emirates // Dept. of the Treasury. 16.10.2023. URL: https://home.treasury.gov/news/press-releases/jy1808 (accessed: 20.01.2024).
[287] Cybersecurity training in the Middle East // SANS Institute. URL: https://www.sans.org/mlp/middle-east-turkey-africa/ (accessed: 23.01.2024).
[288] SANS Institute to host the GCC region’s largest cybersecurity training event // Gulf News. 26.10.2023. URL: https://gulfnews.com/sans-institute-to-host-the-gcc-largest-cybersecurity-training-event (accessed: 10.01.2024).

вооруженных силах США), что значительно расширяет взаимодействие монархий Залива с данным центром подготовки.

Поддержка цифровизации и развития сектора безопасности монархий Залива осуществляется США также в рамках двустороннего межгосударственного сотрудничества. Так, в мае 2017 г. в ходе визита Д. Трампа в Эр-Рияд в связи с установлением стратегического партнерства США и Саудовская Аравия, помимо крупного оружейного контракта, включающего сферу кибербезопасности, подписали соглашения о взаимных инвестициях на сумму 250 млрд долларов[289], в том числе в секторе кибербезопасности[290]. В июле 2022 г. на полях визита Дж. Байдена в Эр-Рияд было подписано 18 соглашений, нацеленных на реализацию саудовской программы «Видение» и превращение страны в технологический и инновационный хаб Ближнего Востока и Северной Африки, а также на подготовку к приему World Expo in 2030 в Саудовской Аравии и Чемпионата мира по футболу 2026 в США[291]. В частности, Министерство связи и информационных технологий Саудовской Аравии подписало два соглашения – с Национальным управлением телекоммуникаций и информации США о взаимодействии в сфере разработки и внедрения технологий 5G и 6G, а также с компанией IBM об обучении в США по профильным программам 100 тыс. молодых саудовцев в течение следующих 5 лет[292].

Таким образом, доминирующее положение США на рынках цифровых технологий и в секторе кибербезопасности монархий Залива обусловлено глобальным технологическим лидерством страны, стратегическим характером отношений с Советом сотрудничества и его членами, а также сохраняющимся за Вашингтоном статусом одного из главных архитекторов системы

---

[289] Трамп на выезде: почему президент США начал с Саудовской Аравии // РБК. 21.05.2017. URL: https://www.rbc.ru/politics/21/05/2017/5921892d9a79476dcf9d1117 (дата обращения: 12.10.2022).

[290] Kingdom of Saudi Arabia cyber readiness. P. 18–20.

[291] The Jeddah Communique, 15.07.2022. URL: https://www.whitehouse.gov/statements-releases/2022/07/15/the-jeddah-communique-a-joint-statement (accessed: 20.01.2023).

[292] Saudi Arabia, US ink 18 agreements in energy, space, ICT, healthcare // Gulf Business.16.07.2022. URL: https://gulfbusiness.com/saudi-arabia-us-ink-18-agreements-in-energy-space-ict-healthcare/ (accessed: 11.10.2022).

региональной безопасности на Ближнем Востоке и в зоне Персидского залива. Внушительный приток американских инвестиций в кибербезопасность монархий Залива осуществляется преимущественно в двустороннем формате на уровне межгосударственного взаимодействия, государственно-частного партнерства и сотрудничества бизнес-структур.

Китайская Народная Республика (КНР). Китайские IT-компании занимают второе (после американских конкурентов) место на рынках цифровых технологий, готовых решений и ПО монархий Залива (*см.: Приложение I, Таблица 12*), что объясняется комплексом причин. Для Китая исходным мотивом для активного продвижения в зону Персидского залива в 1970–1990-е гг. была заинтересованность в энергоресурсах региона, и по мере расширения торгово-экономического сотрудничества повестка развития отношений с аравийскими монархиями объективно дополнилась вопросами взаимодействия в рамках реализации программ «Видение» и объединения усилий в сфере обеспечения региональной безопасности. Сегодня все монархии Залива (кроме Бахрейна) имеют с Китаем соглашения о стратегическом партнерстве, развивается стратегический диалог в формате ССАГЗ – Китай, а Саудовская Аравия, ОАЭ и Оман являются крупнейшими торговыми партнерами КНР на Ближнем Востоке[293].

В отличие от Вашингтона, делающего ставку как на военный, так и на гражданский аспект сотрудничества с ССАГЗ и его участниками, в том числе в сфере кибербезопасности, Пекин предпочитает экономические инструменты продвижения китайских интересов в зоне Персидского залива и на Ближнем Востоке в рамках реализации долгосрочной стратегии «мирного возвышения» КНР. Прагматичный подход в ближневосточной политике Китая учитывает высокий конфликтный потенциал региона и его ключевые «болевые точки», предусматривает акцент на взаимодействие с арабскими странами в рамках интеграционных площадок ЛАГ и ССАГЗ, а также саммитов «КНР – Арабские

[293] Мелкумян Е.С. Арабские монархии Залива в XXI веке. С. 272–309.

страны» и «КНР – ССАГЗ». Это позволяет Пекину избегать вовлечения в региональные конфликты и развивать экономическое сотрудничество со всеми региональными акторами (арабскими государствами, Израилем, Ираном и Турцией)[294].

Аналогичной «антиконфронтационной» тактики Китай придерживается и в киберпространстве, предлагая арабском странам сотрудничество в сфере цифровых технологий и киберзащиты под эгидой глобальных инициатив «Один пояс, один путь» и «Цифровой Шелковый путь» сначала через интеграционные площадки ЛАГ и ССАГЗ, а уже затем наращивая взаимодействие в двустороннем формате с конкретными странами с акцентом на государственно-частное партнерство и кооперацию деловых кругов.

Сегодня сотрудничество Китая с монархиями Залива охватывает широкий спектр проектов в области цифровизации и киберзащиты, в том числе реализуемых в рамках строительства объектов критической инфраструктуры и «умных городов» (включая масштабный саудовский проект NEOM), а также проектов по развитию искусственного интеллекта, электронной торговли, криптовалюты, блокчейн-технологии и технологии, обеспечивающих безопасность трансграничных платежей и других элементов финансовой безопасности[295].

Китайских IT-компании довольно успешно конкурируют с американскими корпорациями. Иллюстрацией может служить пример ОАЭ. В секторе обеспечения безопасности данных очевидно явное преобладание крупных американских фирм, а также их большая, по сравнению с китайскими конкурентами, вовлеченность в развитие соответствующей инфраструктуры, в частности системы data-центров[296]. Тем не менее Китай наращивает свое

[294] Liu L. China’s policy and practice regarding the Gulf security // Stepping away from the abyss. San Domenico di Fiesole, 2021. P. 81–83.
[295] 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.
[296] US tech heavyweight Oracle goes live with its second data centre in UAE, this time in Abu Dhabi // Gulf News. 09.11.2021. URL: https://gulfnews.com/business/markets/us-tech-heavyweight-oracle-goes-live-with-its-second-data-centre-in-uae-this-time-in-abu-dhabi (accessed: 29.01.2024).

присутствие в секторе преимущественно за счет усилий компании Alibaba Cloud и углубления научного сотрудничества между профильными университетами двух стран[297].

В секторе разработки ПО для работы с большими массивами данных наблюдается некоторое смещение инициативы в сторону Китая, главным образом за счет продолжающейся экспансии китайских образовательных платформ в странах ССАГЗ. В этой связи следует отметить общий рост авторитета китайской школы компьютерных наук в глазах аравийских специалистов и формирование новых совместных рабочих площадок. Так, например, в 2022 г. при участии Линг Шао (одного из ведущих специалистов в области big data и искусственного интеллекта) в Абу-Даби был создан Начальный институт искусственного интеллекта. Центр стал важной платформой для реализации проектов в области вычислительных наук, способной конкурировать с созданными при участии США исследовательскими структурами (в частности, Американским университетом Шарджи, претендующим на звание ключевого центра подготовки кадров для нужд сферы кибербезопасности в ОАЭ)[298].

В телекоммуникационном секторе по мере внедрения 5G и постепенного перехода к разработке перспективных технологий мобильных коммуникаций (6G) доля китайских компаний (в первую очередь Huawei), специализирующихся на услугах связи в ОАЭ, стремительно растет, в то время как американский телекоммуникационный бизнес, напротив, теряет свои позиции[299].

Вместе с тем США не намерены уступать Китаю в технологической гонке, особенно в зоне Персидского залива. Об этом свидетельствует, например, недавний отказ (предположительно под давлением Вашингтона)

---

[297] UAEU announces six research projects in cooperation with Chinese Academy of Sciences // UAE University. 06.06.2022. URL: https://www.uaeu.ac.ae/en/news/uaeu-announces-six-research-projects (accessed: 30.01.2024).
[298] Terminus Group appoints Chief Scientist for R&D of intelligent IoT // Zawya. 11.05.2022. URL: https://www.zawya.com/en/press-release/terminus-group-appoints-chief-scientist-iot (accessed: 01.02.2024).
[299] Analyzing the entrenchment of Beijing's digital influence in Saudi Arabia and the United Arab Emirates // GSSR. 14.04.2023. URL: https://georgetownsecuritystudiesreview.org/2023/04/14/ (accessed: 03.02.2024).

ведущей эмиратской IT-компанией «G42», которую возглавляет советник по национальной безопасности ОАЭ шейх Тахнун бен Заид ан-Нахайян, работать с китайскими поставщиками оборудования и программного обеспечения, а также ее переориентация на сотрудничество с американскими IT-гигантами Microsoft и OpenAI, а также шведской Ericsson[300].

Если данный инцидент не останется в числе единичных, можно ожидать уже в обозримой перспективе снижения динамики и интенсивности взаимодействия стран ССАГЗ с Китаем ввиду наличия явных признаков нарушения хрупкого баланса интересов США и КНР, который сложился в последнее десятилетие. Об этом, кроме того, свидетельствуют и другие факторы, прежде всего политического характера. Так, в предшествующие годы наметилась определенная схожесть взглядов в вопросах обеспечения региональной безопасности на Ближнем Востоке, в основе которой, по мнению Вашингтона и Пекина (при сохранении разных исходных императивов), должна лежать интеграция региональных акторов, а не ставка на гарантии безопасности со стороны внерегиональных держав[301]. Однако усиление геополитического веса Китая на Ближнем Востоке в связи с посредничеством в деле нормализации отношений между Саудовской Аравией и Ираном в марте 2023 г. способно пошатнуть это равновесие.

С учетом усиления глобальной конкуренции между США и КНР монархии Залива могут оказаться в эпицентре соперничества двух мировых держав за технологическое лидерство. При таком раскладе аравийские монархии, несмотря на стремление развивать отношения и с Вашингтоном, и с Пекином, с высокой долей вероятности будут вынуждены сделать выбор в пользу США как своего давнего стратегического партнера. Немаловажной причиной осмотрительной политики стран ССАГЗ в отношении Китая является также сохраняющееся в отношении Пекина недоверие, которое

[300] UAE’s top AI group vows to phase out Chinese hardware to appease US // Financial Times. 07.12.2023. URL: https://www.ft.com/content/6710c259-0746-4e09-804f-8a48ecf50ba3 (accessed: 01.02.2024).
[301] Mogielnicki R. Smart context-based investments in the Persian Gulf’s economic security. P. 163, 173–174; Liu L. China’s policy and practice regarding the Gulf security. P. 81, 93–94.

обусловлено в том числе в целом недолгой, по сравнению с Вашингтоном, историей взаимодействия, что, однако, вряд ли помешает монархиям Залива использовать китайский фактор в политическом торге с США. В этой связи академик РАН В.В. Наумкин отмечает: «Действительно, у арабских элит накопилась определенная усталость, вызванная диктатом коллективного Запада и использованием им неоколониальных методов. В свете национальных “Видений” на 2030–2040 гг. диверсификации экономик растет заинтересованность арабов в равноправном технологическом и инвестиционном сотрудничестве с Россией, Китаем, Индией… Однако давайте будем реалистами. Зависимость стран субрегиона Персидского залива от США пока очень велика»[302].

Еще одним актором, комплексно наращивающим присутствие в цифровом пространстве ССАГЗ, является *Индия*. Нью-Дели, как и Пекин, придерживается прагматичного подхода к развитию связей с государствами Ближнего Востока и использует киберфактор для продвижения собственных экономических инициатив и проектов. Наиболее предпочтителен для Индии двусторонний формат межгосударственного взаимодействия в рамках отраслевых соглашений и меморандумов о сотрудничестве в киберпространстве. К настоящему моменту соответствующие договоренности достигнуты с четырьмя монархиями Залива – Катаром, Саудовской Аравией, ОАЭ и Оманом.

Ключевым партнером Индии уже много лет остается Оман: контакты Нью-Дели и Маската отличаются наибольшей частотой и демонстрируют тенденцию к расширению, прежде всего в бизнес-сегменте, за счет растущей роли индийской диаспоры в Султанате. Оман стал первой страной ССАГЗ, подписавшей с Индией соглашение о координации усилий по борьбе с террористической угрозой в киберпространстве в 2023 г.[303]. Кроме того,

[302] Наумкин В.В. Новые моменты в ближневосточной политике США // Проблемы национальной стратегии. 2022. № 5. С. 18–19.

[303] India, Oman agree to jointly fight all manifestations of terror // The Economic Times. 18.01.2023. URL: https://economictimes.indiatimes.com/news/defence/india-oman-agree-to-jointly-figh-terror/ (accessed: 06.10.2023).

Маскат и Нью-Дели на регулярной основе проводят координационные мероприятия по защите объектов критической инфраструктуры, реализуют обмен кадрами[304].

Активно развиваются отношения и в частном секторе. Так, за период с 2018 по 2022 гг. уровень присутствия индийского IT-бизнеса на рынках стран ССАГЗ вырос в среднем на 15%, при этом прирост наблюдается как в категории «бизнес для государства» (B2G), так и в категории «бизнес для бизнеса» (B2B)[305]. Это, в свою очередь, позволяет говорить о комплексном подходе к развитию сотрудничества.

В то же время дальнейшее расширение взаимодействия Индии с монархиями Залива в значительной степени осложнено тем, что на приоритеты Нью-Дели в области кибербезопасности применительно к Ближнему Востоку оказывает серьезное влияние фактор его сотрудничества с Израилем[306]. Учитывая общую сложность диалога между аравийскими монархиями и Израилем в свете эскалации ситуации в Секторе Газа, вопрос подключения Индии к реализации проектов, охватывающих все пространство ССАГЗ, в настоящее время не прорабатывается индийским правительством.

По сравнению с США, Китаем и Индией вовлеченность *Европейского союза* (*ЕС*) в создание безопасной цифровой среды в странах ССАГЗ значительно ниже. Евросоюз и ССАГЗ активно сотрудничают с начала 2010-х гг., однако долгое время вопросы киберзащиты оставались за пределами этого диалога. В 2016 г. были предприняты шаги к расширению профильного взаимодействия между Брюсселем и ССАГЗ в области цифровой безопасности, но они не принесли ощутимых результатов, прежде всего из-за разногласий внутри ЕС и ССАГЗ относительно условий долгосрочного

---

[304] Cyber security meet to focus on 'safe economy' in Oman // Zawya. 29.03.2023. URL: https://www.zawya.com/en/legal/crime-and-security/cyber-security-meet-to-focus-on-safe-economy-in-oman-qfwbjvbp (accessed: 14.10.2023).

[305] India Cybersecurity market report. Dublin, 2023. P. 341, 344.

[306] Jindal D., Soliman M. Understanding the growing Indo-Israeli strategic cyber partnership // MEI. 06.07.2023. URL: https://www.mei.edu/publications/understanding-growing-indo-israeli-strategic-cyber-partnership (accessed: 06.10.2023).

сотрудничества. В вопросах развития сектора кибербезопасности стран ССАГЗ Евросоюз делает акцент на помощь в наращивании кадрового потенциала в форматах образовательных семинаров, запущенных в 2017 г. с целью обучения и отработки навыков противодействия киберугрозам; однако они имели нерегулярный характер, а по уровню организации уступали инициативам НАТО[307].

Недостаток политической кооперации между ЕС и ССАГЗ компенсировался сначала посредничеством в тайном взаимодействии монархий Залива и Израиля в области кибербезопасности[308], а затем развитием государственно-частного партнерства и деятельностью арабско-европейского «эпистемического сообщества», которое сформировалось во второй половине 2010-х гг. В рамках данного формата Брюссель и монархии Залива обмениваются знаниями и ресурсами в области технологического развития, а также координируют усилия по развитию сотрудничества в частном секторе[309]. Несмотря на то, что внимание сторон в данном случае сосредоточено в большей степени на экономических аспектах цифровизации (построение цифровой экономики, развитие электронной торговли и сектора высокотехнологичных услуг в целом и пр.), у формата имеется потенциал в перспективе более системно охватить и вопросы безопасности.

Сегодня европейские фирмы, специализирующиеся на противодействии цифровым угрозам, сотрудничают со всеми монархиями Залива и участвуют в реализации ключевых национальных проектов (например, в строительстве «города будущего» NEOM в Саудовской Аравии). В 2022 г. отношения по линии ССАГЗ – ЕС получили значительный импульс к развитию, поскольку вышли на уровень стратегического партнерства, в рамках которого сфера

---

[307] Euro-Gulf regional cybersecurity collaboration // Bussola. 16.09.2021. URL: https://www.bussolainstitute.org/euro-gulf-regional-cybersecurity-collaboration (accessed: 06.10.2023).

[308] 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).

[309] Михайленко В. И., Успенских Т. А. Политика ЕС в отношении Совета сотрудничества арабских государств Персидского залива // Современная Европа. 2019. №. 5 (90). С. 41, 42.

кибербезопасности обозначена в качестве одного из перспективных направлений сотрудничества[310].

Ряд государств – членов ЕС ведут самостоятельный диалог со странами ССАГЗ. Одним из примеров тому является *Франция*. Париж стремится не только к полноценному участию в строительстве региональной системы кибербезопасности на Ближнем Востоке, но и развитию многостороннего диалога с целью укрепления международной безопасности и повышения уровня доверия в цифровом пространстве в целом, что отвечает приоритетам, закрепленным в ключевых стратегических документах Франции – «Национальной стратегии цифровой безопасности» (*«National Digital Security Strategy»*, 2015 г.) и «Международной цифровой стратегии» (*«International Digital Strategy»*, 2017 г.)[311]. В свою очередь, развитие профильного диалога с аравийскими монархиями, играющими значимую роль в системе региональной кибербезопасности, (как в двустороннем формате, так и на уровне ЛАГ и ССАГЗ) укладывается в обозначенные ориентиры.

Следует отметить, что Франция на данном этапе демонстрирует заметные успехи в укреплении сотрудничества по линии кибербезопасности со странами Северной Африки (Египет, Марокко, Алжир), в то время как взаимодействие с аравийскими монархиями пока носит эпизодический характер. Это отчасти объясняется тем, что в силу слабой (по сравнению с США и КНР) вовлеченности Франции в развитие цифрового ландшафта государств ССАГЗ в период правления Франсуа Олланда (2012–2017 гг.), когда формировались основы нынешних систем киберзащиты аравийских монархий, текущие инициативы Парижа сильно проигрывают на фоне американских и китайских предложений схожего характера. Кроме того, взаимодействие с членами ССАГЗ отчасти замедляется в силу наличия неурегулированных разногласий по другим чувствительным вопросам

[310] A strategic partnership with the Gulf. Brussel: European Commission, 2022. 18 p.
[311] Cyber factor in France Middle Eastern policy // TRENDS. 29.01.2024. URL: https://trendsresearch.org/research.php?id=1076 (accessed: 30.01.2024).

безопасности; в частности, это является характерной чертой стратегического диалога Франции и Кувейта[312].

В то же время Париж активно перенимает позитивный опыт других акторов (США, Китай, Индия, Россия) по выстраиванию диалога с монархиями Залива и прорабатывает новые форматы взаимодействия по линии региональных организаций. Так, одним из перспективных шагов Франции может стать углубление сотрудничества с Советом министров по кибербезопасности, о создании которого ЛАГ объявила во второй половине 2023 г.[313]. Активизация диалога с региональными организациями может обеспечить Парижу дополнительное пространство для взаимодействия с аравийскими монархиями и поиска новых точек соприкосновения.

Схожие шаги предпринимает *ФРГ*. Берлин рассматривает монархии Залива в качестве перспективных партнеров в области безопасности, включая ее цифровой аспект, и стремится углубить профильное сотрудничество без формальной привязки к институтам и инициативам ЕС. В целом, стратегические приоритеты Германии применительно к киберпространству ССАГЗ во многом совпадают с интересами Франции, однако, в отличие от Парижа, Берлину удалось достичь устойчивых договоренностей с некоторыми монархиями. Так, например, в 2022 г. Германия и Катар подписали двустороннее соглашение о развитии сотрудничества в энергетическом секторе, подразумевающее, среди прочего, совместную защиту энергоинфраструктуры от внешнего деструктивного воздействия, включая кибератаки[314]. Впоследствии аналогичное по содержанию соглашение было подписано с ОАЭ[315].

---

[312] Kuwait: defense relations with France in trouble // Tactical Report. 02.08.2023. URL: https://www.tacticalreport.com/daily/62072 (accessed: 22.01.2024).
[313] Arab League announces establishment of Council of Ministers for Cybersecurity // Arab News. 11.09.2023. URL: https://www.arabnews.com/node/2371501/ (accessed: 22.01.2024).
[314] Germany, Qatar sign energy partnership agreement // Reuters. 20.05.2022. URL: https://www.reuters.com/business/energy/germany-qatar-sign-energy-partnership-agreement (accessed: 30.01.2024).
[315] UAE signs energy agreement with Germany's Scholz // Reuters. 25.09.2022. URL: https://www.reuters.com/business/energy/uae-signs-energy-agreement-with-germanys-scholz (accessed: 30.01.2024).

Основным проводником интересов Германии в странах ССАГЗ остается средний и крупный технологический бизнес. Национальные IT-компании (Secucloud, RBS Netkom и др.) реализуют контракты в области государственно-частного партнерства во всех монархиях Залива, а в некоторых (ОАЭ, Бахрейн, Катар) также участвуют в подготовке кадров для нужд цифровой отрасли и развитии программ профессиональной переподготовки государственных служащих.

Вместе с тем углубление диалога между ФРГ и странами ССАГЗ осложнено взаимным недоверием. Негативное влияние, в частности, оказывает фактор гибели оппозиционного журналиста Джамаля Хашогги в 2018 г.: Берлин продолжает настаивать на причастности саудовских спецслужб к инциденту и требовать открытого расследования и наказания виновных в незаконной цифровой слежке. Несмотря на то, что фактически данное требование обращено только к Саудовской Аравии (основному участнику инцидента), оно негативно воспринимается и остальными аравийскими монархиями, поскольку власти ФРГ, начиная с правительства Ангелы Меркель, используют пример Хашогги для иллюстрации системных нарушений прав человека в странах ССАГЗ, в том числе права на неприкосновенность частной жизни[316], что ожидаемо вызывает недовольство у национальных элит.

По этой причине диалог между ФРГ и странами ССАГЗ по вопросам кибербезопасности продолжает развиваться скачкообразно и преимущественно в рамках бизнес-сектора, в то время как взаимодействие на межгосударственном уровне пока носит эпизодический и несистемный характер. При этом диалог в формате «государство – региональная организация», подразумевающий взаимодействие ФРГ со всеми структурами ССАГЗ, в настоящий момент не реализуется.

---

[316] How some Gulf citizens hope German polls will usher in more rights // Amwaj. 25.09.2021. URL: https://amwaj.media/article/gulf-citizens-hope-german-polls-will-usher-in-more-rights-in-gcc (accessed: 30.01.2024).

Иного подхода придерживается *Великобритания*. После выхода страны из Евросоюза Лондон существенно нарастил взаимодействие с монархиями Залива, и его влияние, в отличие от других государств Европы, за последние несколько лет возросло. Сотрудничество Великобритании со странами ССАГЗ реализуется преимущественно в двустороннем формате на межгосударственном уровне и в рамках государственно-частного партнерства. Ключевым партнером Лондона в регионе Персидского залива является Эр-Рияд: с 2018 г. стороны консолидировали усилия по борьбе с киберпреступностью и кибертерроризмом[317]. Кроме того, крупные британские киберфирмы (например, Microminder Cyber Security, Darktrace и др.) имеют свои представительства во всех странах Залива, а также осуществляют подготовку профильных специалистов[318].

Следует обратить внимание на *Канаду*. Несмотря на то, что Оттава не входит в ближний круг партнеров монархий Залива, уступая США и европейским странам по степени вовлеченности в региональные проекты в области кибербезопасности, канадские власти стремятся поддерживать взаимодействие со всеми странами ССАГЗ. Между Канадой и Советом сотрудничества с 2013 г. налажен стратегический диалог по широкому кругу вопросов, затрагивающих различные аспекты реагирования на цифровой вызов[319], что позволяет сторонам оперативно реагировать на происходящие в киберпространстве изменения.

Взаимодействие в двустороннем формате на данный момент ограничено, затрагивает только Саудовскую Аравию и ОАЭ, и не подкреплено какими-либо межгосударственными соглашениями[320]. Однако Оттава демонстрирует готовность к расширению профильных контактов: помимо

---

[317] UK-KSA Joint Communiqué // the UK Government. 10.03.2018. URL: https://www.gov.uk/government/news/united-kingdom-saudi-arabia-joint-communique (accessed: 10.12.2023).
[318] The UK Cybersecurity Export Strategy. London, 2018 20 p.
[319] Canada–GCC strategic dialogue // Government of Canada. URL: https://www.international.gc.ca/world-monde/mena-moan/gcc-canada (accessed: 30.01.2024).
[320] Mosly A. Saudi-Canada relations: restoration of ties // GRC. 31.07.2023. URL: https://www.grc.net/single-commentary/103 (accessed: 30.01.2024).

углубления диалога с Эр-Риядом и Абу-Даби, канадские власти проявляют интерес к расширению партнерства с Бахрейном (EdTech) и Оманом (FinTech), а также за счет запуска дополнительных программ академической и профессиональной мобильности[321].

Канадский IT-бизнес представлен на рынке стран ССАГЗ довольно скромно и сконцентрирован преимущественно в секторе цифрового образования (Smart Technologies) и финансов (Sagard Holdings ULC.), однако налицо тренд на его постепенное расширение. Например, в октябре 2023 г. Оттава выразила намерение более активно участвовать в проектах государственно-частного партнерства, затрагивающих сектор связи и телекоммуникаций, цифровых государственных услуг и облачной безопасности[322]. Пока планируется расширить присутствие канадского кибербизнеса только на рынке ОАЭ, однако в дальнейшем этот опыт предполагается распространить и на другие аравийские монархии. Тем не менее, учитывая, что в обозначенных секторах уже осуществляют деятельность американские и китайские компании, ожидать значительного расширения присутствия Канады на рынке IT-услуг и цифровой защиты стран ССАГЗ не приходится.

Япония и *Республика Корея* также сделали ставку на развитие государственно-частного партнерства, нежели на расширение межгосударственных связей в вопросах кибербезопасности. Исключение – Королевство Бахрейн, с которыми у Японии и Южной Кореи подписаны соглашения на уровне национальных министерств образования об учреждении совместных образовательных программ (в том числе под эгидой мегапроекта Королевства «Школы будущего короля Хамада»)[323], а также о сотрудничестве

---

[321] Canada: New Tech Talent Strategy // New Land. 30.06.2023. URL: https://newlandchase.com/canada-new-tech-talent-strategy/ (accessed: 30.01.2024).

[322] Canada seeks to grow tech co-operation with UAE companies // The National Business. 20.10.2023. URL: https://www.thenationalnews.com/business/technology/2023/10/20/canada-seeks-to-grow-tech-co-operation-with-uae-companies/ (accessed: 30.01.2024).

[323] Joint statement on the strengthening of the comprehensive partnership towards stability and prosperity between Japan and the Kingdom of Bahrain // Embassy of Japan in Bahrain. 25.08.2013. URL: https://www.mofa.go.jp/mofaj/files/000012182.pdf (accessed: 20.01.2024).

в вопросах обеспечения комплексной безопасности объектов критической цифровой инфраструктуры[324]. Выделяются также ОАЭ, отношения с которыми у Республики Корея вышли на уровень стратегического партнерства еще в 2010 г. (с 2019 г. – особое стратегическое партнерство), а сектор кибербезопасности стал одним из приоритетных в контексте двустороннего сотрудничества[325]. При этом наибольшую активность частный капитал указанных стран проявил в период дипломатической блокады Катара: например, японские (Caulis Inc., Evixar и др.) и южнокорейские (SecuLetter Co.) компании расширили взаимодействие с катарскими фирмами, частично заняв нишу ушедших с рынка арабских конкурентов, что заметно в том числе по динамике связей между контрагентами на территории Государства.

Вовлеченность *России* в процессы цифровизации и развитие сектора кибербезопасности в странах ССАГЗ к настоящему времени можно охарактеризовать как имеющую потенциал к росту. Российские IT-гиганты в лице «Лаборатории Касперского», Group-IB (также с апреля 2023 г. – F.A.C.C.T.) и ряда других компаний представлены на цифровых рынках арабского мира, однако на профильных рынках монархий Залива доля участия российского IT-бизнеса в целом ниже, чем у компаний США, КНР или ЕС (*см.: Приложение I, Таблица 12*). В значительной степени это обусловлено приоритетами ближневосточной политики РФ, в соответствии с которыми в предшествующие десятилетия российские профильные компании акцентировали внимание на продвижении процессов цифровизации и развитии сектора киберзащиты в тех странах, которые либо являются партнерами России в вопросах обеспечения региональной безопасности (Иран, Сирия[326]), либо принадлежат к так называемой арабской «периферии»,

[324] EDB Signs a MoU with Japan Information Technology Services Industry Association // EDB. 01.10.2014. URL: https://www.bahrainedb.com/latest-news/edb-signs-a-memorandum-of-understanding-with-japan-information-technology-services-industry-association (accessed: 10.02.2024).
[325] Defense chiefs of S. Korea, UAE discuss cooperation in arms industry, cybersecurity // Yonhap. 22.02.2023. URL: https://en.yna.co.kr/view/AEN20230222001451325 (accessed: 20.01.2024).
[326] Kaspersky Security Bulletin 2015. URL: https://securelist.ru/kaspersky-security-bulletin-2015-razvitie-ugroz-v-2015-godu/27466/ (accessed: 06.10.2023).

где в большей степени требуется помощь извне (показательным примером может служить Палестина[327]).

Относительно низкая представленность российского IT-бизнеса на рынках ССАГЗ, кроме того, обусловлена спецификой отношений между Россией и монархиями Залива, которые развивались неравномерно и зависели от текущей ближневосточной и глобальной повестки. Россия не стала стратегическим союзником для стран ССАГЗ, не входила в круг ключевых архитекторов системы региональной безопасности в зоне Персидского залива и крупнейших поставщиков вооружений в арабские страны этого ближневосточного субрегиона. Вместе с тем государства ССАГЗ рассматривают отношения с Россией как перспективные, особенно после принятия курса на расширение внешнеполитических связей в рамках реализации программ «Видения», а также ввиду востребованности согласованных действий в сфере поддержания стабильности на мировых энергетических рынках[328].

В последние годы, особенно после принятия новой концепции внешней политики РФ (2023 г.)[329] и корректировки внешнеполитического курса, в рамках которого проблема безопасности в зоне Персидского залива вошла в число ключевых приоритетов на ближневосточном направлении, Россия заметно нарастила контакты со монархиями Залива, прежде всего с ОАЭ и Саудовской Аравией, по широкому кругу вопросов, несмотря на сдержанную позицию ССАГЗ в отношении Специальной военной операции РФ на Украине (в частности, на саммите организации в Эр-Рияде в декабре 2022 г. страны-участницы выразили готовность выступить в качестве посредника в урегулировании российско-украинского конфликта[330]). Однако несмотря на

---

[327] Валиахметова Г.Н. Информационные технологии и кибербезопасность – новый вектор сотрудничества РФ и Государства Палестина // Известия УрФУ. Сер. 3. 2018. № 1. С. 108–117.
[328] Мелкумян Е.С. Арабские монархии Залива в XXI веке. С. 236–271.
[329] Концепция внешней политики РФ 2023. URL: https://mid.ru/ru/foreign_policy/official_documents/1860586/ (дата обращения: 10.04.2023).
[330] GCC Supreme Council release final communique after 43rd summit // Saudi Gazette. 09.12.2022. URL: https://saudigazette.com.sa/article/627828 (accessed: 12.10.2023).

продвижение политического диалога России и стран ССАГЗ, активное сотрудничество Москвы и Тегерана, в том числе в сфере кибербезопасности[331], по-прежнему ограничивает участие российских профильных компаний в развитии киберсектора монархий Залива, для которых фактор «перманентной иранской угрозы» остается системообразующим в вопросах национальной и коллективной киберазащиты.

Среди ближневосточных партнеров стран ССАГЗ в вопросах создания безопасной цифровой среды особе место отводится *Израилю*, что обусловлено высоким уровнем технологического развития страны, включая кибербезопасность, на которую, по оценкам 2018 г., приходилось порядка 20% мировых инвестиций в сектор цифровой защиты, а стоимость экспорта профильных товаров и услуг составляла около 4 млрд долларов[332]. Ключевым фактором налаживания контактов в отсутствие официальных отношений также стало совпадение интересов монархий Залива и Израиля по линии противостояния Ирану, в том числе в киберпространстве.

Израиль внес колоссальный вклад в развитие национальных систем кибербезопасности стран ССАГЗ. Израиль принимал участие в ликвидации разрушительных последствий организованных предположительно Ираном кибератак на Saudi Aramco и RasGas с использованием вируса Shamoon в 2012 г., в создании интеллектуальной системы общегородского наблюдения «Falcon Eye» в Абу-Даби (ОАЭ) и строительстве «умного города» NEOM (Саудовская Аравия), развитии интернет-банкинга в Омане, разработке софта для мониторинга закрытых каналов в социальных сетях для Саудовской Аравии и Катара и т.д. Помимо поставок технологий кибербезопасности в гражданский сектор, были установлены контакты по линии военных ведомств

---

[331] El-Masry A. The Abraham Accords and their cyber implications. URL: https://www.mei.edu/publications/abraham-accords-and-their-cyber-implications (accessed: 06.10.2023).

[332] Zilber N. Gulf cyber cooperation with Izrael // WINEP. 17.01.2019. URL: https://www.washingtoninstitute.org/policy-analysis/gulf-cyber-cooperation-israel-balancing-threats-and-rights (accessed: 06.10.2023).

и спецслужб (например, поставка в Саудовскую Аравию и ОАЭ шпионского ПО «Pegasus» для слежки за оппозиционерами и диссидентами)[333].

В отсутствие дипломатических отношений стороны использовали формат «дискретного сотрудничества», привлекая в качестве посредников киберфирмы из США, стран Европы, арабского мира и Африки (см.: *Приложение II, Схема 6*). Другим форматом профильной кооперации стали рассмотренные в предыдущем разделе военно-политические альянсы, которые США попытались сформировать после пересмотра своего подхода к обеспечению региональной цифровой безопасности на Ближнем Востоке и в которых Израилю отводилась роль одного из системообразующих элементов (MESA, «Негевская инициатива», проект «Железный киберкупол»).

Подписание «Соглашений Авраама» позволило вывести взаимодействие Израиля с ОАЭ и Бахрейном в открытый формат. Так, например, уже в сентябре 2020 г. руководители служб кибербезопасности ОАЭ и Израиля провели публичную онлайн-встречу, на которой обсуждались проблемы совместного противодействия киберугрозам; в апреле 2021 г. израильские киберфирмы приняли участие в конференции Cybertech Global (Дубай, ОАЭ); кроме того, в публичном пространстве появилась информация об обмене между ОАЭ и Израилем разведданными о деятельности киберподразделений «Хезболлы» (прежде всего в лице группировки «Ливанский кедр»), а также о сотрудничестве национальных групп реагирования на чрезвычайные ситуации (CERT) и планах проведения совместных киберучений[334].

Стремление Израиля развивать сектор кибербезопасности в странах ССАГЗ обусловлено не только целесообразностью объединить усилия в противостоянии Ирану, но и долгосрочными интересами коммерческого и стратегического характера.

---

[333] Ibid.; Khorrami N. Israel's cybersecurity cooperation with the GCC states. P. 5, 8.

[334] Ibid. P. 5–6; El-Masry A. The Abraham Accords. URL: https://www.mei.edu/publications/abraham-accords-and-their-cyber-implications-how-iran-unifying-regions-cyberspace (accessed: 17.10.2023).

Цифровой рынок стран ССАГЗ является чрезвычайно емким и прибыльным с учетом нацеленности программ стратегического развития «Видение» на цифровизацию, а также наличия внушительных финансовых средств и технологической зависимости монархий Залива от внешних поставщиков[335]. Кроме того, израильские поставки шпионского и хакерского ПО и инструментов значительно снижают вероятность того, что аравийские контрагенты начнут развивать собственные возможности[336].

Активное участие в обеспечении киберзащиты монархий Залива не только выдвигает Израиль на роль гаранта цифровой безопасности пространства ССАГЗ, но и значительно снижает риск интеграции на антиизраильской платформе арабского мира в целом, укрепляя тем самым позицию ССАГЗ в ЛАГ по вопросу целесообразности оказания технологической помощи слаборазвитым странам в лице Йемена, Ирака и Сирии, в той или иной степени связанным с Ираном[337].

Вместе с тем динамика сближения с Израилем в области кибербезопасности ограничивалась разногласиями внутри ССАГЗ по вопросу выработки совместной позиции в отношении Израиля и Ирана. Ситуация усугубилась в 2023 г. в свете формальной нормализации отношений между Саудовской Аравией и Ираном, а также с началом военного противостояния Израиля и ХАМАС в Секторе Газа. С началом наземной операции ЦАХАЛ ОАЭ и Бахрейн свернули публичные контакты с Израилем, а Саудовская Аравия, как потенциальный кандидат на нормализацию диалога, вышла из переговорного процесса. Несмотря на то, что отдельные направления взаимодействия, скорее всего, сохранились в кулуарном формате по линии военных ведомств и спецслужб, для полноценного межгосударственного сотрудничества в области кибербезопасности этого явно недостаточно.

---

[335] GCC Cyber Security Market Forecast 2018−2028. URL: https://www.marketresearch.com/Visiongain-v1531/GCC-Cyber-Security-Forecast-11700089/ (accessed: 17.10.2023).
[336] Khorrami N. Israel’s cybersecurity cooperation with the GCC states. P. 18.
[337] Israel is becoming a cybersecurity guarantor in the Middle East // Atlantic Council. 18.11.2021. URL: https://www.atlanticcouncil.org/menasource/israel-is-becoming-a-cybersecurity-guarantor (accessed: 17.10.2023).

Турция уверенно держит курс на региональное лидерство на Ближнем Востоке, что формально выводит ее в разряд геополитических соперников Саудовской Аравии и ОАЭ. Турция является довольно сильным киберигроком: согласно данным МСЭ ООН, страна занимает 11 место в мировом индексе готовности к отражению киберугроз и 3 место в ближневосточном рейтинге, пропуская вперед только Саудовскую Аравию и ОАЭ[338]. В киберпространстве Анкара придерживается тактики проактивной обороны, о чем свидетельствует, например, опыт страны по взаимодействию с хакерским сообществом (*см. Приложение II, Схема 8*) и деятельность координируемой ею «армии киберянычар». Вместе с тем Турция не декларирует своей целью достижение превосходства в киберпространстве и, более того, настаивает на региональной «цифровой разрядке» с переходом к более тесному сотрудничеству с монархиями Залива[339]. Отсутствие прямых угроз, в том числе в цифровом измерении, со стороны Турции не позволяет странам ССАГЗ считать Турцию геополитическим противником, как, например, в случае с Ираном. Более того, Анкара довольно тесно взаимодействует с Дохой в рамках сформировавшегося тактического альянса.

Поэтому сегодня турецкие киберфирмы представлены на цифровых рынках стран ССАГЗ, где имеют возможность развивать свою деятельность на принципах открытой конкуренции, а ведущие турецкие IT-компании (Heraklet, ICterra и др.) принимают участие в реализации ряда проектов на пространстве ССАГЗ, включая проекты, косвенно связанные с развитием военного сегмента кибербезопасности. Так, например, компания ICterra в январе 2023 г. присоединилась к трехлетней программе наставничества Агентства НАТО по связи и информации (NATO Communications and Information Agency, NCIA), ориентированной на подготовку специалистов в области кибербезопасности и

[338] GCI 2020. P. 25, 127.
[339] Kasapoglu C. Turkey's Future Cyber Defense Landscape. Ankara, 2016. P. 11.

организацию стажировок для внеблоковых партнеров Альянса[340], в число которых входят и монархии Залива.

В целом можно резюмировать, что влияние внешних акторов на динамику и масштабы развития систем кибербезопасности монархий Залива за последнее десятилетие существенно возросло. При этом участие внерегиональных акторов в создании безопасной цифровой среды на пространстве ССАГЗ тесно связано с проводимой ими ближневосточной политикой и реализуется как на платформе Совета сотрудничества, так и в двустороннем формате взаимодействия с входящими в его состав странами в рамках межгосударственного взаимодействия и государственно-частного партнерства.

В свою очередь страны ССАГЗ 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 формате, в случае с КНР и Республикой Корея – на уровне партнерств с отдельными членами ССАГЗ. Данный тренд в совокупности с готовностью увеличить число своих стратегических партнеров обусловлен стремлением монархий Залива диверсифицировать свои внешнеполитические связи для расширения доступа к новейшим технологиям.

Вместе с тем высокий уровень конфликтности на Ближнем Востоке и быстро меняющиеся региональные реалии актуализируют проблемы обеспечения безопасности в зоне Персидского залива. В отсутствие единства мнений в ССАГЗ относительно путей решения этой ключевой проблемы апелляция к помощи своих стратегических союзников, прежде всего в лице США, априори сужает поле для открытой конкуренции и ограничивает каждое

[340] ICterra NATO NCIA Collaboration // ICterra. 06.01.2023. URL: https://www.icterra.com/icterra-nato-nci-collaboration/ (accessed: 20.01.2024).

из государств – членов Совета сотрудничества в выборе внешних партнеров для развития сектора кибербезопасности и цифровизации в целом.

3.4. Перспективы и риски развития кооперации по вопросам кибербезопасности в рамках ССАГЗ

Анализ международного сотрудничества монархий Залива в сфере кибербезопасности позволяет говорить о наличии на пространстве ССАГЗ *тенденции к объединению усилий стран-участниц в целях создания безопасной цифровой среды на национальном и региональном уровнях*. Чтобы охарактеризовать эту зарождающуюся в регионе Персидского залива коллективную систему кибербезопасности, целесообразно прибегнуть к методу SWOT-анализа. Данный метод позволяет выявить сильные стороны («strengths») и уязвимые места («weaknesses») ее внутренней среды, а также определить влияние на ее развитие внешних факторов – возможностей («opportunities») и угроз («threats»). Результаты SWOT-анализа представлены в *Приложении I (Таблица 13*).

В числе сильных сторон (*«strengths»*) кооперации монархий Залива по вопросам цифровой защиты прежде всего следует отметить наличие общего пространства цифровых угроз и схожие подходы к их градации. Все рассматриваемые страны в качестве ключевой угрозы для национального и регионального киберпространства рассматривают использование ИКТ-инструментов в военно-политических конфликтах на Ближнем Востоке и в зоне Персидского залива, определяя, тем самым, главным источником угроз государственных акторов и их прокси-силы. Общий ландшафт угроз формируют также киберпреступность и кибертерроризм.

Стимулом к интеграции являются также схожие цели и задачи долгосрочного развития, в которых цифровизация играет ключевую роль, формируя запрос на выработку коллективных мер цифровой защиты. Только путем объединения усилий представляется возможным обеспечить технико-

технологическую и физическую защиту общей для всех стран Персидского залива Интернет-инфраструктуры и коммуникационных сетей, а также совместных проектов развития; преодолеть зависимость от импорта чувствительных технологий и инертность законодательной сферы; обеспечить подготовку высококвалифицированных специалистов и условия для развития собственного кадрового потенциала; снизить роль религиозного фактора при принятии и реализации стратегически значимых инициатив и т.д.

Опорой для реализации совместных инициатив в области кибербезопасности является наличие у каждого актора развитой национальной системы киберзащиты, собственных инструментов и практик обеспечения безопасности в цифровом пространстве. Еще одной сильной стороной является общность взглядов монархий Залива на текущие и долгосрочные приоритеты развития сектора кибербезопасности. Это позволило предпринять ряд важных шагов по координации усилий в рамках ССАГЗ, где действует совместная группа реагирования на чрезвычайные компьютерные инциденты, созданы институты профильного сотрудничества – Комитет CERT, Постоянный комитет по кибербезопасности, Организация по разработке стандартов кибербезопасности и др.

В вопросах развития национальной кибербезопасности все монархии Залива делают ставку на развитие международного сотрудничества. При выборе внешних партнеров приоритет отдается лидерам мировой технологической гонки, которые способны вносить существенный вклад в реализацию стратегических программ «Видение» и с которыми уже наработаны многолетние торгово-экономические связи. Это позволяет выделить группу ведущих государств, с которыми представляется возможным от лица ССАГЗ в относительно короткие сроки выстроить эффективное взаимодействие в области кибербезопасности, в том числе по линии крупного технологического бизнеса. На этом направлении уже сделан ряд важных шагов: Совет сотрудничества установил отношения стратегического партнерства с США и Евросоюзом, стратегический диалог ведется с Китаем (в

формате регулярных саммитов). Аналогичные процессы можно наблюдать и в военном секторе кибербезопасности, где монархии Залива отдают предпочтение развитию сотрудничества с США, которые являются их главным стратегическим союзником, основным поставщиком вооружений и передовых технологий, а также гарантом безопасности в зоне Персидского залива.

Вместе с тем динамика продвижения монархий Залива к системе коллективного реагирования на цифровой вызов ограничивается рядом сдерживающих внутренних факторов (*«weaknesses»*). Прежде всего кооперация сохраняет реактивный и ситуативный характер, ее пока не удается перевести в формат постоянного сотрудничества. Несмотря на декларируемую готовность работать сообща над отражением киберугроз, учреждение на площадке ССАГЗ ряда профильных институтов и некоторые другие позитивные подвижки, страны – участницы Совета сотрудничества пока не обсуждают проект совместной комплексной киберзащиты, а проблемы гармонизации профильных законодательств и разработки общей стратегии кибербезопасности не фигурируют в повестке организации.

В вопросах создания общей безопасной цифровой среды аравийские монархии по-прежнему делают основную ставку на развитие национального сектора кибербезопасности, в то время как профильное взаимодействие на платформе ССАГЗ скорее вторично. Это существенно ограничивает готовность каждого из государств-членов к эффективному реагированию на киберугрозы, поскольку снижает уровень осведомленности, способствует появлению брешей и дополнительных точек уязвимости в системах национальной киберзащиты, увеличивает время реакции на киберинциденты, создает условия для нанесения кратно большего ущерба со стороны деструктивных акторов.

Препятствием к развитию кооперации являются также «изъяны» национальных систем кибербезопасности, присущие всем монархиям Залива: излишняя бюрократизация управления отраслью; дублирование функций

ввиду отсутствия четкого разграничения функционала между различными правительственными учреждениями и ведомствами; соперничество гражданского и военного секторов кибербезопасности; система «нисходящего контроля» со стороны государства, ограничивающая развитие горизонтальных связей между всеми субъектами кибербезопасности и т.д.

Приоритет национальных программ развития киберсектора накладывает определенные ограничения и на сферу международного сотрудничества. Помимо явного преобладания двусторонних форматов взаимодействия (которые к тому же далеко не всегда подкреплены документально), монархии Залива отдают предпочтение сотрудничеству с внерегиональными акторами, в то время как профильные связи между ними развиты относительно слабо. Так, только Саудовская Аравия и ОАЭ заключили двустороннее соглашение о сотрудничестве в области кибербезопасности. Отсутствие устойчивых взаимовыгодных связей между государствами ССАГЗ, в свою очередь, неизбежно порождает конкуренцию и существенно снижает возможности для разработки и реализации совместных инициатив.

Неготовность монархий Залива комплексно и последовательно сотрудничать в сфере кибербезопасности, в том числе на площадке ССАГЗ, обусловлена разногласиями по широкому спектру вопросов, наличием атмосферы взаимного недоверия, нежеланием делиться чувствительными технологиями. Так, например, соперничество за лидирующие позиции в секторе высоких технологий и киберзащиты (сегодня оно наглядно просматривается в «треугольнике» Саудовская Аравия – ОАЭ – Катар) способно углубить противоречия внутри Совета сотрудничества, привести к заморозке совместных проектов и инициатив, перенаправить интеграционный вектор с площадки ССАГЗ в формат взаимодействия в «малых группах». Ограничивает кооперацию и стремление отдельных государств, прежде всего Саудовской Аравии и ОАЭ, обеспечивать за счет ССАГЗ собственные внешнеполитические интересы, ставя их порой выше коллективных.

Серьезные разногласия между аравийскими монархиями также связаны с обеспечением региональной безопасности в зоне Персидского залива и на Ближнем Востоке в целом. В контексте кибербезопасности дискуссионными остаются вопросы об обоснованности и целесообразности использования конструкта «перманентной иранской угрозы» в качестве системообразующего элемента коллективной цифровой защиты, а также о возможностях и допустимых пределах привлечения к ее строительству Израиля. Несмотря на то, что иранский фактор долгое время служил для монархий Залива одним из стимулов к кооперации и позволял обосновать рост военных расходов (в том числе в цифровом сегменте), излишняя акцентуация на теме «иранской угрозы» лоббистами проектов коллективной обороны под эгидой США заметно ослабила его эффективность как инструмента консолидации союзников Вашингтона в зоне Персидского залива. С учетом неоднозначной роли Израиля в ближневосточной системе международных отношений данный тренд породил разногласия не только внутри Совета сотрудничества, но и по линии ССАГЗ – США.

Существенно ослабить интеграционный импульс в ССАГЗ в сфере кибербезопасности способен также комплекс внешних угроз (*«threats»*), обусловленных высоким конфликтным потенциалом Ближнего Востока, его сложным геополитическим ландшафтом, слабой предсказуемостью развития военно-политической обстановки, сильным влиянием фактора случайности на происходящие события, высоким уровнем недоверия и т.д.

Все государства Персидского залива прочно встроены в систему региональных отношений, поэтому в той или иной степени вовлечены в региональные конфликты (палестино-израильский, йеменский, сирийский и др.), а их внешняя политика сильно зависит от характера, динамики и исхода противоборства многочисленных ближневосточных игроков. Наиболее ярким примером тому служит эскалация в Секторе Газа (октябрь 2023 г.), которая обусловила снижение интенсивности публичных контактов в области технологического сотрудничества (включая вопросы кибербезопасности)

подписантов «Соглашений Авраама» из числа аравийских монархий (Бахрейн, ОАЭ) с Израилем, сорвала переговорный процесс на саудовско-израильском треке, в значительной степени обесценила многообещающие результаты длительных переговоров о нормализации отношений между Саудовской Аравией и Ираном. Иными словами, конфликтная региональная среда значительно снижает запас прочности для коллективных инициатив и проектов стран ССАГЗ в области кибербезопасности.

Рост региональной напряженности, кроме того, порождает угрозу возобновления острой фазы противостояния с Ираном в киберпространстве, в которое с высокой долей вероятности вновь будут вовлечены Саудовская Аравия, ОАЭ, Израиль, США, а также большинство монархий Залива. Следует также учитывать, что сегодня участниками кибервойн на Ближнем Востоке являются не только государства, но и их прокси-силы. В этой связи отметим, что с началом эскалации в Секторе Газа иранские хакерские подразделения и лояльные Тегерану кибергруппировки существенно повысили активность в зоне непосредственных интересов монархий Залива. Учитывая, что не все участники ССАГЗ готовы к погружению в асимметричный конфликт с Ираном, их сближение на почве «иранской угрозы» из киберпространства (и, как следствие, формирование общей системы ее отражения) на данном этапе видится сомнительным.

Вместе с тем неблагоприятный региональный фон формирует дополнительные возможности («opportunities») для развития кооперации в сфере цифровой защиты на площадке ССАГЗ, прежде всего в рамках совместных усилий по стабилизации обстановки на Ближнем Востоке. Так, например, обострение палестинского кризиса в октябре 2023 г. вполне ожидаемо привело к всплеску экстремисткой пропаганды и возрастанию рисков проведения кибертеррористических акций. И хотя радикально-исламистские организации в настоящий момент разобщены и не располагают достаточным потенциалом для проведения серьезных кибератак, необходимость противодействия кибертерроризму во всех его формах

способна подтолкнуть аравийские монархии к консолидации усилий как на площадке ССАГЗ, так и в рамках специализированных совместных структур – Глобального центра по борьбе с экстремистской идеологией (GCCEI) и Центра по противодействию финансированию терроризма (TFTC), базирующихся в Саудовской Аравии и действующих в тесном сотрудничестве с США.

Другой фактор позитивного влияния внешней среды лежит в области возможностей развития сотрудничества с другими странами мира в рамках глобальных инициатив и площадок (в первую очередь, ООН и ее специализированных институтов). Монархии Залива в последние годы активнее включаются в глобальный процесс выработки мер регулирования киберпространства (например, на базе Спецкомитета ООН по киберпреступности), более охотно вовлекаются в инициативы МСЭ, стремятся к повышению уровня культуры поведения в цифровом пространстве, проявляют интерес к идеям «цифровой разрядки». Это создает основу для совместной работы над конкретными проектами и по отдельным направлениям.

Так, например, страны ССАГЗ принимают участие в подготовке конвенции ООН по киберпреступности, и по мере продвижения этой работы вполне обоснованно ожидать, что Совет сотрудничества выступит с новыми инициативами по активизации регионального сотрудничества на площадке ЛАГ в борьбе с киберугрозами, прежде всего по доработке Арабской конвенции о борьбе с преступлениями в области информационных технологий 2010 г. Эффективной платформой кооперации может также стать Организация исламского сотрудничества. Использование площадок за рамками ССАГЗ позволит монархиям Залива эффективнее адаптировать передовой опыт в области кибербезопасности и расширить обмен информацией об инцидентах в киберпространстве (по линии CERT и профильных ведомств), а также придаст дополнительный импульс разработке и реализации совместных программ в области развития кадрового потенциала.

Иными словами, факторы внешней среды способны заметно расширить поле для коллективных инициатив монархий Залива в области кибербезопасности, создать возможности для к ним новых участников (подобный формат можно условно назвать «ССАГЗ+»), а также снизить конфликтный потенциал Ближнего Востока (включая «разрядку» в киберпространстве).

С учетом неоднозначного влияния внешних и внутренних факторов на кооперацию монархий Залива в вопросах создания совместной безопасной цифровой среды представляется возможным предложить три сценария дальнейшего развития ситуации на данном направлении.

Согласно первому из них, в свете ухудшающейся региональной обстановки монархии Залива возьмут курс на расширение военного сотрудничества в области кибербезопасности. Очевидно, что подобный проект может быть реализован только при значительном участии США как одного из ключевых архитекторов системы коллективной безопасности на Ближнем Востоке, а по содержанию он будет ориентирован на воссоздание продвигаемых ранее Вашингтоном проектов формата «Арабского НАТО» (MESA) и «Негевской инициативы», но с большим вниманием к специфике выстраивания двусторонних отношений между ключевыми союзниками США в новых геополитических условиях.

Вместе с тем создание подобного военного блока, который с высокой долей вероятности будет иметь выраженный антииранский базис (прежде всего по причине продолжающегося роста напряженности в отношениях между США и Ираном), лишь усилит противостояние между Тегераном и аравийскими монархиями, а также приведет к новому витку борьбы в киберпространстве, что непременно затронет многие страны Ближнего Востока. Также препятствием к продвижению подобного проекта может стать дальнейшая эскалация в Секторе Газа: в силу дистанцирования большинства аравийских монархий от Израиля (в качестве жеста публичной поддержки Палестины) Вашингтону будет гораздо сложнее добиться эффективной

кооперации в рамках создаваемого блока, тем более что гипотетическое выведение Израиля за рамки проекта не отвечает региональным интересам США. В целом, на наш взгляд, вероятность реализации данного сценария – *средняя*.

В рамках второго (алармистского) сценария можно предположить, что дальнейшее погружение монархий Залива в технологическую гонку усилит их соперничество (в первую очередь в «треугольнике» Саудовская Аравия –ОАЭ – Катар), формируя в ССАГЗ центробежные тенденции и укрепляя курс на развитие национальной, а не коллективной кибермощи. При подобном раскладе кооперация по вопросам кибербезопасности приобретет исключительно декларативный характер, а ее уровень будет снижаться не только в Совете сотрудничества, но и на платформах ЛАГ и ОИС. При этом государства сохранят прежнюю вовлеченность в международное сотрудничество, однако акцент будет сделан на развитие контактов с внерегиональными акторами (включая представителей крупного технологического бизнеса), а другие страны арабского мира будут представлять интерес для монархий Залива исключительно как рынки сбыта для своей технологичной продукции.

Однако, на наш взгляд, данный сценарий является *маловероятным.* Переход к индивидуальной модели развития сделает страны ССАГЗ более уязвимыми перед лицом киберугроз со стороны государственных, вне- и антисистемных акторов глобальной и региональной политики, поскольку ограничение оперативного обмена информацией о выявлении и атрибуции кибернарушений неизбежно повлечет за собой неадекватный либо несвоевременный ответ. Кроме того, отсутствие достаточной координации по вопросам цифровой защиты будет снижать геополитический вес монархий Залива и, соответственно, степень их влияния на арабский мир и Ближний Восток. Определенные сложности могут возникнуть и при выстраивании контактов с зарубежными партнерами, поскольку некоторые глобальные технологические лидеры, прежде всего Китай, предпочитают коллективные

форматы взаимодействия, видя в них залог успешного продвижения собственных мегапроектов.

Третий и, на наш взгляд, *наиболее вероятный* сценарий предполагает, что монархии Залива будут придерживаться комплексного подхода к обеспечению кибербезопасности, признаки формирования которого мы можем 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. Такой вектор развития может придать импульс дальнейшей интеграции монархий Залива на площадке ССАГЗ, вокруг которого в долгосрочной перспективе может начать формироваться система коллективной кибербезопасности арабского мира и/или Ближнего Востока.

С учетом быстро меняющейся обстановки на Ближнем Востоке вполне вероятно, что монархии Залива более активно будут прибегать к тактике ситуативных союзов, потому что подобный формат взаимодействия направлен на решение конкретной проблемы, а сотрудничество может быть приостановлено в любой момент. Это позволит государствам не приносить в жертву временному союзнику свои внешнеполитические интересы, получив вместе с тем ряд преимуществ. Кроме того, тактические альянсы создают условия для сотрудничества с различными региональными акторами, причем не только в публичном, но и в кулуарном формате: в этом контексте практика «дискретного сотрудничества», вероятно, получит более широкое распространение, а в случае нормализации обстановки на Ближнем Востоке может затронуть не только Израиль, но и Иран.

Представленные выше сценарии имеют пересекающиеся поля: все они предполагают, что монархии Залива будут и дальше стремиться как можно

скорее адаптироваться к реалиям цифровой эпохи, акцентируя внимание на совершенствовании национальных систем кибербезопасности и сохраняя высокие темпы их развития. Ключевым фактором успешного продвижения к этим целям останется международное сотрудничество, которое будет продолжать наращиваться в том или ином формате, вне прямой зависимости от интенсивности профильного взаимодействия на платформе ССАГЗ.

В целом, анализ взаимодействия монархий Залива по вопросам кибербезопасности на региональных площадки ССАГЗ, ЛАГ и ОИС, в рамках координации действий на военном направлении, а также развития двусторонних и многосторонних связей с внерегиональными и ближневосточными партнерами позволяет 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.

ЗАКЛЮЧЕНИЕ

Монархии Персидского залива находятся в авангарде арабского мира и Ближнего Востока в вопросах обеспечения международной информационной безопасности, в том числе разработки собственных практик и методов киберзащиты. Это является закономерным результатом адекватного реагирования на цифровой вызов, который обусловлен двумя ключевыми факторами – курсом на цифровизацию экономики в рамках стратегических программ «Видение» и, соответственно, востребованностью надежной защиты стремительно развивающейся ИКТ-среды, а также возрастанием угроз со стороны государственных и негосударственных акторов ближневосточной политики, использующих цифровые технологии в качестве инструментов межгосударственного противостояния, в криминальных и террористических целях. В данных условиях аравийские монархии делают ставку на форсированное развитие и гражданского, и военного секторов кибербезопасности, причем в рамках последнего наращивается как оборонительный, так и наступательный киберпотенциал.

Процесс эволюции национальных систем кибербезопасности монархий Залива представляется возможным условно разделить на три периода: 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 отрасти; 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. Сегодня развитие систем кибербезопасности аравийских монархий

характеризуется динамичностью и имеет восходящий вектор. Лидирующие позиции занимают Саудовская Аравия и ОАЭ, которые в течение первых 5 лет после принятия программ «Видение» (2016–2020 гг.) форсированными темпами усилили свои возможности противостоять ИКТ-угрозам и вошли в пятерку мировых лидеров по уровню цифровой защищенности.

В то же время ни одна из аравийских монархий пока не достигла показателя абсолютной готовности к отражению киберугроз, хотя их работа по повышению эффективности национальных систем киберзащиты стала более комплексной и последовательной. Все рассматриваемые государства в той или иной степени испытывают схожие проблемы с наращиванием технического потенциала, 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 на региональных интеграционных площадках ССАГЗ, ЛАГ, ОИС.

В рамках ССАГЗ уже созданы условия для развития сотрудничества в области реагирования на цифровой вызов: 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 на платформе 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.

Внушительный вклад в развитие систем кибербезопасности монархий Залива вносят внерегиональные партнеры: их интерес 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. Монархии Залива, со своей стороны, отдают предпочтение мировым лидерам технологической гонки (главным образом, США и КНР); высокая интенсивность профильных связей также характерна для государств, отношения с которыми вышли на уровень стратегического партнерства (страны Евросоюза, Индия, Республика Корея, Япония и др.). Данный тренд обусловлен стремлением монархий Залива диверсифицировать внешнеполитические связи для обеспечения надежной цифровой защиты и расширения доступа к новейшим технологиям.

Военное направление занимает исключительно важное место в международном сотрудничестве монархий Залива, поскольку ИКТ-угрозы актуализируют проблемы региональной безопасности на Ближнем Востоке с его высоким конфликтным потенциалом. 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 они не вышли на уровень практической реализации, так как заложенная в обозначенных концепциях 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 целом, анализ международного сотрудничества монархий Залива в сфере кибербезопасности позволяет говорить о его многовекторном характере и зарождении на пространстве ССАГЗ тенденции к кооперации стран-участниц в целях создания совместной безопасной цифровой среды. Активизация международного взаимодействия, ставку на которое сделали все аравийские монархии в вопросах кибербезопасности, создает благоприятные условия для развития совместных инициатив и выработки коллективного ответа на цифровой вызов. Вместе с тем комплекс объективных внутренних и внешних факторов не позволяет 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 сближение государств в контексте поиска эффективных инструментов противодействия киберугрозам. В рамках сценарного прогнозирования можно ожидать, что монархии Залива продолжат придерживаться комплексного подхода к обеспечению кибербезопасности, с одной стороны, делая ставку на развитие национальных систем киберзащиты

и наращивание международного сотрудничества в двустороннем формате, а с другой, продвигая совместные профильные проекты, которые позволят повысить уровень цифровой защищенности, ускорить продвижение к технологическому суверенитету и усилить геополитические позиции каждой из стран – участниц ССАГЗ.

Перспективы дальнейшей научной разработки исследуемой темы лежат в плоскости осмысления сотрудничества монархий Залива с ведущими кибердержавами мира (США, КНР, Россией, странами Евросоюза, Индией, Японией, Республикой Корея и т.д.) и выявления специфики диалога по проблемам кибербезопасности с каждой из рассматриваемых стран в рамках case-studies. Дальнейшие исследования также могут быть связаны с определением роли и места проблем международной информационной безопасности в развитии региональных площадок сотрудничества ЛАГ и ОИС, влияния цифрового вызова на интеграционные процессы в арабском мире и в мусульманских сообществах. Значительным исследовательским потенциалом обладает конструктивистский подход, который позволяет сместить фокус исследования в политическую сферу и проанализировать ее влияние на научно-технический прогресс, а также расширить предметное поле анализа за счет негосударственных субъектов многоуровневого сотрудничества в области международной информационной безопасности в лице бизнеса, неправительственных организаций, научных сообществ и образовательных структур.

СПИСОК ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

Источники

I. Официальные документы и материалы

Международные договоры, конвенции, совместные декларации

1. A strategic partnership with the Gulf. Brussel: European Commission, 2022. 18 p.
2. Annex to U.S.-GCC Camp David Joint Statement, May 14, 2015 // The White House. URL: https://obamawhitehouse.archives.gov/the-press-office/2015/05/14/annex-us-gulf-cooperation-council-camp-david-joint-statement (accessed: 14.10.2023).
3. Arab Convention on combating information technology offences. Cairo: Arab League, 2010. 29 p.
4. Arab-Islamic-American summit // Saudi Press Agency. 21.05.2017. URL: https://www.spa.gov.sa/w410192 (accessed: 14.10.2023).
5. Budapest Convention on cybercrime. Budapest: Council of Europe, 2001. 22 p.
6. Doha Declaration of the 44th session of the Supreme Council of the Gulf Cooperation Council (Doha Summit) // Secretariat General of the GCC, 5.12.2023. URL: https://www.gcc-sg.org/en-us/MediaCenter/NewsCooperation/News/Pages/news2023-12-5-1.aspx (accessed: 12.01.2024).
7. Joint statement by United States and Gulf Cooperation Council members on Iran, February 16, 2023 // The U.S. Department of States. URL: https://www.state.gov/joint-statement-by-the-united-states-and-gulf-cooperation-council-members-on-iran (accessed: 21.11.2023).
8. Joint statement on the strengthening of the comprehensive partnership towards stability and prosperity between Japan and the Kingdom of Bahrain // Embassy of Japan in Bahrain. 25.08.2013. URL: https://www.mofa.go.jp/mofaj/files/000012182.pdf (accessed: 20.01.2024).
9. Joint Strategic Vision Declaration for the USA and Kingdom of Saudi Arabia, May 20, 2017 // The White House. URL: https://trumpwhitehouse.archives.gov/briefings-statements/joint-strategic-

vision-declaration-united-states-america-kingdom-saudi-arabia/ (accessed: 14.10.2023).

10. Paris Call for trust and security in the cyberspace security, 12.11.2018. URL: https://pariscall.international/en/call (accessed: 06.10.2023).
11. The Jeddah Communique: A joint statement between the USA and the Kingdom of Saudi Arabia, 15.07.2022 // White House. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2022/07/15/the-jeddah-communique-a-joint-statement-between-the-united-states-of-america-and-the-kingdom-of-saudi-arabia/ (accessed: 20.01.2023).
12. United States – Gulf Cooperation Council second Summit leaders Communique, April 21, 2016 // The White House. URL: https://obamawhitehouse.archives.gov/the-press-office/2016/04/21/united-states-gulf-cooperation-council-second-summit-leaders-communique (accessed: 14.10.2023).

Документы и материалы международных организаций

13. Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Нью-Йорк: ООН, 2013. 8 с.
14. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: Резолюция ГА ООН A/RES/76/19 от 8.12.2021 г.
15. Руководство по разработке национальной стратегии кибербезопасности: – стратегическая деятельность по обеспечению кибербезопасности. Женева: МСЭ, WB, Comsec, CTO, NATO CCD COE, 2018. 76 с.
16. About ARCC // ITU Arab Regional Cybersecurity Centre (ITU-ARCC). URL: https://arcc.om/?GetLang=en (accessed: 10.12.2023).
17. About GCC // Cooperation Council for the Arab States of Gulf. URL: https://www.gcc-sg.org/en-us/AboutGCC/Pages/OrganizationalStructure.aspx (accessed: 10.04.2023).

18. Amnesty International report. L.: Amnesty International, 2021. 408 p.
19. Bahrain: dreams of reform crushed 10 years after uprising // Amnesty International. 11.02.2021. URL: https://www.amnesty.org/en/latest/press-release/2021/02/bahrain-dreams-of-reform-crushed-10-years-after-uprising/ (accessed: 06.10.2023).
20. Cybercrime laws in Arab countries. Washington, DC: Global Laws, 2021. 58 p.
21. Definition of cybersecurity – gaps and overlaps in standardization. Attiki, Greece: ENISA, 2015. 25 p.
22. Development and harmonization of cyber legislation in the Arab region. N. Y.: United Nation, 2013. 21 p.
23. ISO/IES 27032:2023. Cybersecurity: guidelines for Internet security. URL: https://www.iso.org/ru/standard/76070.html (accessed: 21.06.2023).
24. Online jihadist propaganda 2021. Luxembourg: Europol, 2022. 50 p.
25. FIRST members around the world // FIRST. URL: https://www.first.org/members/map (accessed: 10.12.2023).
26. Freedom on the Net. Berlin: Freedom House, 2023. 47 p.
27. Global Cybersecurity Index 2014. Geneva: ITU, 2014. 517 p.
28. Global Cybersecurity Index 2017. Geneva: ITU, 2017. 66 p.
29. Global Cybersecurity Index 2018. Geneva: ITU, 2019. 92 p.
30. Global Cybersecurity Index 2020. Geneva: ITU, 2021. 172 p.
31. Impact of COVID-19 on the Internet ecosystem in the Middle East and North Africa. Reston: Internet Society, 2020. 31 p.
32. Internet infrastructure security guidelines for the Arab states. Washington DC: Internet society, 2020. 26 p.
33. Internet organized crime threat assessment (IOCTA) 2023. Luxembourg: Europol, 2023. 14 p.
34. NCSC-certified cyber incident planning and response // Cyber Management Alliance.15.07.2023. URL: https://www.cm-alliance.com/cyber-incident-response-training-dubai-uae (accessed: 13.10.2023).

35. OIC-CERT launch 5G security working group at GISEC 2021 // Intelligent CIO. 1.06.2021. URL: https://www.intelligentcio.com/oic-cert-launch-5g-security-working-group (accessed: 15.12.2021).
36. OIC will soon establish a Cyber Security Center to combat cyberterrorism // Organization of the Islamic Conference. 07.11.2017. URL: https://www.oic-oci.org/topic/?t_id=16023&t_ref=8082&lan=en (accessed: 10.12.2021).
37. Saudi Arabia // UNIDIR. 10.03.2021. URL: https://unidir.org›cpp›state-pdf-export (accessed: 20.10.2021).
38. TFTC: History // Terrorist Financial Target Center. URL: https://www.tftc-istehdaf.org/history (accessed: 14.10.2023).
39. The new battlefront: cyber security across the GCC. Report. Washington, DC: Gulf International Forum, 2018. 21 p.
40. The OIC-CERT annual report 2022. Kuala Lumpur: OIC, 2022. 116 p.
41. Vision & Mission statement // OIC-CERT. URL: https://www.oic-cert.org/en/missionstatement.html# (accessed: 10.12.2023).
42. World CERTs (aeCERT, CERT.bh, Oman National CERT, Saudi CERT, Qatar's Computer Emergency Response Team) // CERT-In. URL: https://www.cert-in.org.in/s2cMainServlet?pageid=ADWCERTVIEW (accessed: 15.10.2023).
43. بلتقييس المعني العربي العمل لفريق العاشر الاجتماع (X заседание Арабской рабочей группы по стандартизации). Cairo: Arab League, 2016. 16 p.

Нормативно-правовые акты

44. Arab laws Online. Database of laws & legislation // Arab Laws. URL: https://www.arablawsworld.com/ (accessed: 21.11.2023).
45. Laws and regulations // GCC. URL: https://www.gcc-sg.org/en-us/CognitiveSources/Pages/LawsandRegulations.aspx (accessed: 06.10.2023).
46. The Cyber Crime Law (Royal Decree 12/2011). Muscat: MTCIT, 2011. 12 p.

Национальные и отраслевые стратегии и программы развития

47. Доктрина информационной безопасности РФ. М., 2016. 17 с.

48. Концептуальные взгляды на деятельность Вооруженных сил РФ в информационном пространстве. М.: Министерство обороны РФ, 2011. 14 с.
49. Концепция внешней политики РФ, 31 марта 2023 г. // МИД РФ. URL: https://mid.ru/ru/foreign_policy/official_documents/1860586/ (дата обращения: 10.04.2023).
50. Основы государственной политики РФ в области международной информационной безопасности от 12.04.2021. URL: http://www.scrf.gov.ru/security/information/document114/ (дата обращения: 15.06.2022).
51. Abu Dhabi healthcare information and cybersecurity strategy. Abu Dhabi: Dept. of Health, 2020. 16 p.
52. Bahrain Economic Vision 2030. Manama: Bahrain Government, 2008. 26 p.
53. Bahrain National cybersecurity strategy // National Cyber Security Center. 10.01.2022. URL: https://www.ncsc.gov.bh/en/national-strategy.html (accessed: 10.02.2023).
54. Department of Defense: cyber strategy 2023 // U.S. Dept. of Defense. URL: https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF (accessed: 11.12.2023).
55. Developing national information security strategy for the Kingdom of Saudi Arabia. Riyadh: Ministry of Communications and Informational Technology, Riyadh. 2017. 90 p.
56. Dubai cybersecurity strategy. URL: https://u.ae/en/dubai-cyber-security-strategy (accessed: 19.01.2024).
57. Egypt Vision 2030. Cairo: Egypt Government, 2018. 37 p.
58. Kuwait Vision 2035. El Kuwait: CAIT, 2019. 40 p.
59. National Cybersecurity Strategy, March 2023. Washington, DC: White House, 2023. 39 p.
60. Oman Cyber Security Governance guidelines. URL: https://www.ita.gov.om/ITAPortal/Pages/735301 (accessed: 19.01.2024).
61. Oman Vision 2040. Muscat: MoTC, 2021. 39 p.

62. Qatar National cybersecurity strategy. Doha: MoTC, 2014. 35 p.
63. Qatar National Vision 2030. Doha. MoTC, 2008. 40 p.
64. Saudi Vision 2030. Riyadh: NCA, 2016, 85 p.
65. The Abu Dhabi Economic Vision 2030. Abu Dhabi: Council of Economic Development, 2008. 146 p.
66. The UAE Centennial 2071 // the UAE Government. 10.11.2021. URL: https://uaecabinet.ae/en/details/news/mohammed-bin-rashid-launches-five-decade-government-plan-uae-centennial-2071 (accessed: 20.02.2023).
67. The UAE Vision. Abu Dhabi: NCSC, 2023.70 p.
68. The UAE National cybersecurity strategy. Abu Dhabi: NCSC, 2019. 28 p.
69. The UK cybersecurity export strategy. L.: Foreign Office, 2018. 20 p.
70. US National security strategy. October 2022 // The White House. URL: https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf (accessed: 21.11.2023).
71. الكويت لدولة السيبراني للأمن الوطنية الإستراتيجية (Национальная стратегия кибербезопасности Государства Кувейт). El Kuwait: TRA, 2017. 35 p.

Отчеты и пресс-релизы органов государственной власти

72. About OCERT // Oman National CERT. URL: https://cert.gov.om/about.aspx (accessed: 10.12.2023).
73. About the Hackathon 4.0 // Hackathon 4.0. URL: https://hackathon.ae/en/About (accessed: 06.10.2023).
74. Beyon Cyber signs strategic agreement to launch Cyber Security Solutions for Bahrain's SMEs during AICS 2023 // BNA. 06.12.2023. URL: https://www.bna.bh/en/BeyonCybersignsstrategicagreementtolaunchCyberSecuritySolutionsforBahrainsSMEsduringAICS2023.aspx?cms=q8FmFJgiscL2fwIzON1%2BDpsmkryoGUibbCpfxbm%2FFkU%3D (accessed: 12.12.2023).

75. Canada–Gulf Cooperation Council (GCC) strategic dialogue // Government of Canada. URL: https://www.international.gc.ca/world-monde/mena-moan/gcc-canada (accessed: 30.01.2024).
76. Eagle Resolve 23 - field training exercise // CENTCOM. 29.05.2023. URL: https://www.centcom.mil/Press-Release-View/Article/3409929/eagle-resolve-23-exercise-with-saudi-arabia/ (accessed: 10.02.2024).
77. EDB signs a MoU with Japan Information Technology Services Industry Association // EDB. 01.10.2014. URL: https://www.bahrainedb.com/latest-news/edb-signs-a-memorandum-of-understanding-with-japan-information-technology-services-industry-association (accessed: 20.02.2024).
78. FM 3-12: cyberspace and electromagnetic warfare. Washington DC: Headquarters Department of the Army, 2021. 162 p.
79. Intelligence Ministry arrests second man of Tondar terrorist group // Iran Government. 02.02.2022. URL: https://irangov.ir/detail/379412 (accessed: 06.10.2023).
80. Middle East security still critical to U.S. // U.S. Department of Defense, 30.04.2019. URL: https://www.defense.gov/News/News-Stories/Article/Article/1829813/middle-east-security-still-critical-to-us/ (accessed: 21.11.2023).
81. National Electronic Security Authority CyberQuest // NESA. URL: https://www.actionimpact.com/national-electronic-security-authority-cyber-quest-case-study (accessed: 16.10.2023).
82. Red Sands facility brings innovation, collaboration to counter-drone technology // Citadel. 31.08.2023. URL: https://centcomcitadel.com/en_GB/articles/ssc/features/2023/08/31/feature-03 (accessed: 21.11.2023).
83. Saudi Arabia engages in UN cybercrime convention negotiations in New York // KSA.com. 2.02.2024. URL: https://www.ksa.com/saudi-arabia-engages-in-un-cybercrime-convention-negotiations-in-new-york (accessed: 10.02.2024).

84. Saudi National Cybersecurity Authority and U.S. Department of Homeland Security sign MoU to promote cybersecurity cooperation // Saudi Press Agency, 16.07.2022. URL: https://www.spa.gov.sa/2370312 (accessed: 14.10.2023).
85. Treasury announces cybersecurity cooperation MoU with the United Arab Emirates // Dept. of the Treasury. 16.10.2023. URL: https://home.treasury.gov/news/press-releases/jy1808 (accessed: 20.01.2024).
86. U.S. security cooperation with Bahrain // US Department of State. 14.06.2021. URL: https://www.state.gov/u-s-security-cooperation-with-bahrain/ (accessed: 06.10.2023).
87. Update on the International Counter-Ransomware Initiative // US Dept. of State. 15.11.2021. URL: https://www.state.gov/briefings-foreign-press-centers/update-on-the-international-counter-ransomware-initiative (accessed: 06.10.2023).
88. U.S. security cooperation with Saudi Arabia. Fact Sheet // U.S. State Department. January 20, 2021. URL: https://www.state.gov/u-s-security-cooperation-with-saudi-arabia/ (accessed: 10.12.2021).

Отчеты и материалы IT-компаний

89. Неизвестные взломали сеть поставщика шпионского ПО для правительственных спецслужб // SecureLab. 06.07.2015. URL: http://www.securitylab.ru/news/473587.php (дата обращения: 21.12.2023).
90. От Shamoon к StoneDrill. Wiper-подобные программы атакуют компании в Саудовской Аравии и не только // SecureList. 06.03.2018. URL: https://securelist.ru/from-shamoon-to-stonedrill/30350/ (дата обращения: 21.10.2023).
91. Отчет StormWall о DDoS-атаках за 2023 г. М.: StormWall, 2024. 35 с.
92. Стратегии кибербезопасности. Аналитический отчет // InfoWatch. URL: https://www.infowatch.ru/sites/default/files/publication_file/analiticheskiy-otchet-strategii-kiberbezopasnosti.pdf (accessed: 21.06.2023).
93. AI militarization will be ‘force multiplier’ for UAE, Saudi Arabia // C4ISRNET. 24.02.2021. URL: https://www.c4isrnet.com/artificial-

intelligence/2021/02/24/ai-militarization-will-be-force-multiplier-for-uae-saudi-arabia/ (accessed: 30.01.2024).

94. Annual Security Report 2022. Dubai: GBM, 2022. 31 p.

95. Annual Security Report 2023. Dubai: GBM, 2022. 37 p.

96. Canada: new Tech Talent Strategy // New Land. 30.06.2023. URL: https://newlandchase.com/canada-new-tech-talent-strategy/ (accessed: 30.01.2024).

97. CISCO Annual Internet Report. San Jose, 2020.

98. Cost of a data breach report 2023. New York: IBM, 2023. 70 p.

99. Cybersecurity certification training in Kuwait / Mildain. URL: https://mildaintrainings.com/loc/cyber-security-training-in-kuwait/ (accessed: 10.10.2023).

100. Cybersecurity spending for critical infrastructure to surpass US$105 billion in 2021 // ABI Research. 10.02.2021. URL: https://www.abiresearch.com/press/cybersecurity-spending-critical-infrastructure-surpass-us105-billion-2021/ (accessed: 12.11.2023).

101. Cybersecurity threatscape in the Middle East: 2022-2023. Moscow: Kaspersky, 2023. 11 p.

102. Cybersecurity training in the Middle East, Africa & Turkey // SANS Institute. URL: https://www.sans.org/mlp/middle-east-turkey-africa/ (accessed: 23.01.2024).

103. ICterra NATO NCIA collaboration // ICterra. 06.01.2023. URL: https://www.icterra.com/icterra-nato-nci-collaboration/ (accessed: 20.01.2024).

104. Iranian hacktivist proxies escalate activities beyond Israel // CPB. 04.12.2023. URL: https://checkpoint.com/research/shift-in-cyber-warfare-tactics-iranian-hacktivist-proxies-extend-activities-beyond-israel/ (accessed: 20.01.2024).

105. Kaspersky Security Bulletin 2013. URL: https://securelist.ru/kaspersky-security-bulletin-2013-razvitie-ugroz-v-2013-godu/19140/ (accessed: 06.10.2023).

106. Kaspersky Security Bulletin 2015. URL: https://securelist.ru/kaspersky-security-bulletin-2015-razvitie-ugroz-v-2015-godu/27466/ (дата обращения: 15.12.2023).

107. Kingdom of Saudi Arabia cyber readiness at a glance. Arlington, VA: Potomac Institute for Policy Studies, 2017. 34 p.

108. Little Thinking Minds (EdTech platform). URL: https://www.littlethinkingminds.com/en/about-us/ (accessed: 30.01.2024).

109. Microsoft digital defense report 2023. Redmond: Microsoft, 2023. 131 p.

110. PWC: Leveraging public private partnerships in the GCC post COVID-19. L.: PWC, 2021. 28 p.

111. Ready... Or not? Balancing future opportunities with future risks. Moscow: Kaspersky Lab, 2021. 11 p.

112. Stealth Falcon // MITRE. URL: https://attack.mitre.org/groups/G0038/ (accessed: 01.02.2024).

113. What is cyber security // Kaspersky. URL: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security (accessed: 21.06.2023).

114. 2023 State of the Phish. Sacramento: Proofpoint, 2023. 35 p.

115. 2024 State of the Phish. Sacramento: Proofpoint, 2024. 41 p.

II. Статистические отчеты и базы данных

116. GCC cyber security market forecast 2018−2028 // Market Research. URL: https://www.marketresearch.com/Visiongain-v1531/GCC-Cyber-Security-Forecast-11700089/ (accessed: 17.10.2023).

117. India cybersecurity market report 2022-2027. Dublin: Global Markets Reports, 2023. 400 p.

118. Individuals using the Internet (% of population) // The World Bank Statistics. URL: https://data.worldbank.org/indicator/it.NET.user.ZSmost (accessed: 11.12.2023).

119. Internet exchange map. URL: https://www.internetexchangemap.com/#/ (accessed: 21.02.2024).

120. Kaspersky cyberthreat real-time map. URL: https://cybermap.kaspersky.com/ (accessed: 10.01.2024).

121. Middle East cyber security market size & share // Markets and Markets. URL: https://www.marketsandmarkets.com/Market-Reports/middle-east-cyber-security-market-121119697.html (accessed: 20.02.2024).

122. Mobile internet usage in MENA // Statista. URL: https://www.statista.com/topics/8710/mobile-internet-usage-in-MENA/topicOverview (accessed: 20.12.2023).

123. National Cyber Power Index 2022. Cambridge: Belfer Center for Science and International Affairs, 2022. 66 p.

124. Security software booms in the Gulf // Edge. 24.08.2003. URL: https://www.edgemiddleeast.com/news/476981-security-software-booms-in-the-gulf (accessed: 10.02.2024).

125. Submarine cable map. URL: https://www.submarinecablemap.com/ (accessed: 21.02.2024).

126. 2023 military strength ranking // Global Firepower. URL: https://www.globalfirepower.com/countries-listing.php (accessed: 06.11.2023).

III. Официальные заявления и интервью

127. King Abdullah Statement to the 33rd Summit of the GCC Supreme Council in Bahrain // Embassy of the Kingdom of Saudi Arabia. 24.12.2011. URL: https://www.saudiembassy.net/statements/king-abdullah-statement-33rd-summit-gcc-supreme-council-bahrain (accessed: 10.04.2023).

128. Mohammed bin Salman interview on Vision 2030 // Al Arabiya. 28.04.2021. URL: https://www.youtube.com/watch?v=xqXl0L3lL8w (accessed: 15.11.2023).

129. Wahba M. GCC: a force for regional stability // AGSIW. 21.02.2017. URL: https://agsiw.org/gcc-force-regional-stability/ (accessed: 06.10.2023).

130. ‘We are expanding the Abraham Accords to cybersecurity,’ US Homeland Security Official says // Media Line. 31.01.2023. URL: https://themedialine.org/life-lines/we-are-expanding-the-abraham-accords-to-cybersecurity-us-homeland-security-official-says/ (accessed: 20.01.2024).

IV. Новостные публикации СМИ

131. Пентагон начал кибервойну против «Исламского государства» // РБК. 26.02.2016. URL: https://www.rbc.ru/politics/26/02/2016/56d04aca9a794756469e1f94 (дата обращения: 12.07.2022).

132. Россия и Китай начинают партнерство в области кибербезопасности // Газета.ru. 06.05.2015. URL: https://www.gazeta.ru/tech/2015/05/06/6670173/Russia_China_infobezopasnost.shtml (дата обращения: 17.10.2023).

133. Трамп на выезде: почему президент США начал с Саудовской Аравии // РБК. 21.05.2017. URL: https://www.rbc.ru/politics/21/05/2017/5921892d9a79476dcf9d1117 (дата обращения: 12.10.2022).

134. Arab League announces establishment of Council of Ministers for Cybersecurity // Arab News. 11.09.2023. URL: https://www.arabnews.com/node/2371501/ (accessed: 22.01.2024).

135. Artificial intelligence in UAE military // Times Aerospace. 19.02.2023. URL: https://www.timesaerospace.aero/news/defence/artificial-intelligence-in-uae-military (accessed: 10.02.2024).

136. Bahrain uncovers Iran and Qatar cyber terrorism network // Gulf News. 20.05.2019. URL: https://gulfnews.com/world/gulf/bahrain/bahrain-uncovers-iran-and-qatar-cyber-terrorism-network-1.64065789 (accessed: 18.10.2023).

137. Canada seeks to grow tech co-operation with UAE companies // The National Business. 20.10.2023. URL:

https://www.thenationalnews.com/business/technology/2023/10/20/canada-seeks-to-grow-tech-co-operation-with-uae-companies/ (accessed: 30.01.2024).

138. Cyber security meet to focus on 'safe economy' in Oman // Zawya. 29.03.2023. URL: https://www.zawya.com/en/legal/crime-and-security/cyber-security-meet-to-focus-on-safe-economy-in-oman-qfwbjvbp (accessed: 14.10.2023).

139. Deadglyph: new advanced backdoor with distinctive malware tactics // The Hacker News. 23.09.2023. URL: https://thehackernews.com/2023/09/deadglyph-new-advanced-backdoor-with.html (accessed: 30.01.2024).

140. Defense chiefs of S. Korea, UAE discuss cooperation in arms industry, cybersecurity // Yonhap. 22.02.2023. URL: https://en.yna.co.kr/view/AEN20230222001451325 (accessed: 20.01.2024).

141. Experts call for 'Geneva Convention' for cybersecurity at Abu Dhabi strategic debates // India Times. 15.11.2021. URL: https://indiatimes.com/news/experts-call-for-geneva-convention (accessed: 06.10.2023).

142. GCC Supreme Council release final communique after 43rd summit // Saudi Gazette. 09.12.2022. URL: https://saudigazette.com.sa/article/627828 (accessed: 12.10.2023)

143. Germany, Qatar sign energy partnership agreement // Reuters. 20.05.2022. URL: https://www.reuters.com/business/energy/germany-qatar-sign-energy-partnership-agreement (accessed: 30.01.2024).

144. Hacktivism the motivator of cyberattacks in Middle East // Gulf Business. 06.06.2013. URL: https://www.thenationalnews.com/business/hacktivism-the-motivator-of-cyber-attacks-in-middle-east (accessed: 24.01.2024).

145. Hacktivists stoke Israel-Gaza conflict online // Reuters. 11.10.2023. URL: https://www.reuters.com/world/middle-east/hacktivists-stoke-israel-gaza-conflict-online-2023-10-11/ (accessed: 20.01.2024).

146. How Abu Dhabi plans to build up its cybersecurity defences // Arabian Business. 08.01.2022. URL:

https://www.arabianbusiness.com/industries/technology/how-abu-dhabi-plans-to-build-up-its-cybersecurity-defences (accessed: 19.10.2023).

147. How Israeli spyware was sold to Egypt and pitched to Qatar and Saudi Arabia // Haaretz. 05.10.2023. URL: https://www.haaretz.com/israel-news/security-aviation/2023-10-05/how-israeli-spyware-was-sold-to-egypt-and-pitched-to-qatar-and-saudi-arabia/ (accessed: 30.01.2024).

148. How some Gulf citizens hope German polls will usher in more rights // Amwaj. 25.09.2021. URL: https://amwaj.media/article/gulf-citizens-hope-german-polls-will-usher-in-more-rights-in-gcc (accessed: 30.01.2024).

149. India, Oman agree to jointly fight all manifestations of terror // The Economic Times. 18.01.2023. URL: https://economictimes.indiatimes.com/news/defence/india-oman-agree-to-jointly-fight-terror/ (accessed: 06.10.2023).

150. Iran blames foreign country for cyberattack on petrol stations // BBC. 27.10.2021. URL: https://www.bbc.com/news/world-middle-east-59062907 (accessed: 11.10.2023).

151. Iranian cyberthreat hovers over GCC region // The Arab Weekly. 08.03.2020. URL: https://thearabweekly.com/iranian-cyberthreat-hovers-over-gcc-region (accessed: 06.10.2023).

152. Israeli companies aided Saudi spying despite Khashoggi killing // The New York Times. 17.07.2021. URL: https://www.nytimes.com/2021/07/17/world/middleeast/israel-saudi-khashoggi (accessed: 06.10.2023).

153. Israeli spy company attempted hacking phones of Qatar residents, investigation reveals // Doha News. 10.03.2023. URL: https://dohanews.co/israeli-spy-company-attempted-hacking-phones (accessed: 10.01.2024).

154. Jordan's first Cyber Security Summit to kick off next Monday // Ammon News. 23.09.2023. URL: https://en.ammonnews.net/article/68169 (accessed: 30.01.2024).

155. Kuwait, Britain sign deal on cybersecurity coop // Kuna. 30.08.2023. URL: https://www.kuna.net.kw/ArticleDetails.aspx?id=3107460&language=en# (accessed: 12.12.2023).

156. Kuwait: defense relations with France in trouble // Tactical Report. 02.08.2023. URL: https://www.tacticalreport.com/daily/62072 (accessed: 22.01.2024).

157. Mossad targeted in major cyber-attack by Sudanese hackers // Mehr. 25.04.2023. URL: https://en.mehrnews.com/news/199880/Mossad-targeted-in-major-cyber-attack-by-Sudanese-hackers (accessed: 20.01.2024).

158. National Bank of Fujairah: building a robust cybersecurity strategy // Gulf News. 23.02.2022. URL: https://gulfnews.com/gn-focus/national-bank-of-fujairah-building-a-robust-cybersecurity-strategy (accessed: 21.10.2023).

159. New bill aims to boost cybersecurity cooperation between U.S., Abraham Accords nations // Axios. 31.05.2023. URL: https://www.axios.com/2023/05/31/bill-cybersecurity-cooperation-abraham-accords-nations (accessed: 30.07.2023).

160. Oman: MTC signs agreement to promote cybersecurity start-ups // Data Guidelines. 09.01.2020. URL: https://www.dataguidance.com/news/oman-mtc-signs-agreement-promote-cybersecurity-start-ups (accessed: 12.12.2023).

161. Palantir supplying Israel with new tools since Hamas war started // Bloomberg. 10.01.2024. URL: https://www.bloomberg.com/news/articles/2024-01-10/palantir-supplying-israel-with-new-tools-since-hamas-war-started (accessed: 01.02.2024).

162. Pro-Hamas cyber groups target social media with disinfo designed to incite antisemitism // Polygraph. 18.10.2023. URL: https://www.polygraph.info/a/7315940.html (accessed: 27.01.2024).

163. Red Sea cables have been damaged, disrupting internet traffic // CNN. 28.02.2024. URL: https://edition.cnn.com/2024/03/04/business/red-sea-cables-cut-internet/index.html (accessed: 28.02.2024).

164. Sabotage in Iran: een missie in duisternis // Volkskrant. 08.01.2024. URL: https://www.volkskrant.nl/kijkverder/v/2024/sabotage-in-iran-een-missie-in-duisternis/ (accessed: 20.01.2024).

165. SANS Institute to host the GCC region's largest cybersecurity training event // Gulf News. 26.10.2023. URL: https://gulfnews.com/business/corporate-news/sans-institute-to-host-the-gcc-regions-largest-cybersecurity-training-event-1.1698238246182 (accessed: 10.01.2024).

166. Saudi Arabia seeks to tame powerful cyber armies // MENA FN. 08.07.2020. URL: https://menafn.com/1100598791/ (accessed: 20.01.2024).

167. Saudi Arabia, four countries sign cybersecurity MoUs // Asharq Al-Aswat. 03.11.2023. URL: https://english.aawsat.com/business/4645086-saudi-arabia-four-countries-sign-cybersecurity-mous (accessed: 12.12.2023).

168. Saudi Arabia, US ink 18 agreements in energy, space, ICT, healthcare // Gulf Business.16.07.2022. URL: https://gulfbusiness.com/saudi-arabia-us-ink-18-agreements-in-energy-space-ict-healthcare/ (accessed: 11.10.2022).

169. Self-censorship in Arab higher education: an untold problem // Al-Fanar Media. 18.04.2021. URL: https://www.al-fanarmedia.org/2021/04/self-censorship-in-arab-higher-education-an-untold-problem/ (accessed: 14.10.2023).

170. Stealth Falcon group uses custom spyware, fake journalists to target UAE dissidents // CSO. 30.05.2016. URL: https://www.csoonline.com/article/3076178/stealth-falcon-group-uses-custom-spyware.html (accessed: 30.01.2024).

171. Terminus Group appoints Chief Scientist for R&D of intelligent IoT // Zawya. 11.05.2022. URL: https://www.zawya.com/en/press-release/people-in-the-news/terminus-group-appoints-chief-scientist-for-r-and-d-of-intelligent-iot (accessed: 01.02.2024).

172. UAE plans cybersecurity vision for next 50 years // The National News. 20.09.2023. URL:

https://www.thenationalnews.com/business/technology/2023/09/20/uae-plans-cybersecurity-vision-for-next-50-years/ (accessed: 30.01.2024).

173. UAE ransomware attacks decline but payout size grows // AGBI. 19.01.2024. URL: https://www.agbi.com/articles/uae-ransomware-attacks-decline-but-payout-size-grows/ (accessed: 30.01.2024).

174. UAE's top AI group vows to phase out Chinese hardware to appease US // Financial Times. 07.12.2023. URL: https://www.ft.com/content/6710c259-0746-4e09-804f-8a48ecf50ba3 (accessed: 01.02.2024).

175. UAEU announces six research projects in cooperation with Chinese Academy of Sciences // UAE University. 06.06.2022. URL: https://www.uaeu.ac.ae/en/news/uaeu-announces-six-research-projects-in-cooperation-with-chinese-academy-of-sciences.shtml (accessed: 30.01.2024).

176. Undersea internet cables off Egypt disrupted as navy arrests three // The Guardian. 28.05.2013. URL: https://www.theguardian.com/technology/2013/mar/28/egypt-undersea-cable-arrests (accessed: 20.01.2024).

177. US dominates global arms sales, with Saudi Arabia the top customer // Axios. 16.03.2021 URL: https://www.axios.com/2021/03/16/global-arms-exports-us-russia-saudi-arabia-weapons (accessed: 12.11.2023).

178. US tech heavyweight Oracle goes live with its second data centre in UAE, this time in Abu Dhabi // Gulf News. 09.11.2021. URL: https://gulfnews.com/business/markets/us-tech-heavyweight-oracle-goes-live-with-its-second-data-centre-in-uae-this-time-in-abu-dhabi (accessed: 29.01.2024).

179. US, GCC Summit Communique condemns Iran's regional interferences // Al-Arabiya news. 22.05.2017. URL: https://english.alarabiya.net/News/gulf/2017/05/22/US-GCC-Summit-communique-condemns-Iran-s-regional-interferences (accessed: 14.10.2023).

180. Who are the Houthis and how closely linked are they to Iran? // the Washington Post. 16.09.2019. URL:

https://washingtonpost.com/world/2019/09/16/why-iran-is-getting-blame-an-attack-saudi-arabia-claimed-by-yemens-houthis/ (accessed: 30.01.2024)

181. Why Yemen's Houthi rebels welcome conflict with the US // CNN. 01.02.2024. URL: https://edition.cnn.com/2024/02/01/middleeast/houthi-reputation-red-sea-attacks-gaza-mime-intl/index.html (accessed: 03.02.2024).

182. "الإلكتروني الإرهاب".. للعالم؟ الأول التهديد لمصدر يتحول هل («Кибертерроризм»: превратится ли он в первостепенный источник угрозы миру?) // Al Khaleej. 05.04.2016. URL: https://alkhaleej.net/علوم-وتكنولوجيا/الإرهاب-الإلكتروني-هل-يتحول-لمصدر-التهديد-الأول-للعالم؟ (accessed: 06.10.2023).

183. محاربة أخطار الفضاء السيبراني تبدأ ببنية تشريعية قوية. (Борьба с опасностями киберпространства начинается с сильной законодательной структуры) // Al-Arab. 07.03.2021. URL: https://alarab.co.uk/إنشاء-يقترح-والقانون-السيبرانية-كتاب-السيبراني-بالأمن-للتخصص-عالمية-منظمة (accessed: 06.10.2023).

184. اقرار أول قانون عربي استرشادي لحماية الأمن السيبراني بالدول العربية (Принятие первого руководящего арабского закона о защите кибербезопасности в арабских странах) // Addustour. 03.11.2021. URL: http://www.addustour.com/articles/1249438 (accessed: 06.10.2023).

185. قمة الرياض تؤكد وحدة الصف والتكامل الاقتصادي (Саммит в Эр-Рияде подтверждает идею единства и экономической интеграции) // Al Khaleej. 15.12.2021. URL: https://www.alkhaleej.ae/2021-12-15/قمة-الرياض-تؤكد-وحدة-الصف-والتكامل-الاقتصادي/أخبار/الإمارات-من-أخبار-الدار (accessed: 12.10.2023).

186. כיפת ברזל סייבר: פרויקט משותף של "ישראל "ומדינות ערב המדפיסות" («Железный киберкупол»: совместный проект Израиля и арабских стран) // Tasnim. 15.12.2022. URL: https://www.tasnimnews.com/he/news/2022/12/15/2822055/ (accessed: 20.01.2024).

Литература

187. Алпеев А.С. Терминология безопасности: кибербезопасность, информационная безопасность // Вопросы кибербезопасности. 2014. № 5. С. 39–42.

188. Баландин А.Ю. Кибербезопасность и информационная безопасность. Демаркация правовых категорий // Правовая политика и правовая жизнь. 2023. № 3. С. 260–270.

189. Балуев Д.Г. Информационная революция и современные международные отношения. Н. Новгород, 2001. 208 с.

190. 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.

191. Бжезинский З. Великая шахматная доска. М.: Международные отношения, 2009. 280 с.

192. Валиахметова Г.Н. Ближний Восток в цифровую эпоху: глобализация угроз региональной безопасности // Восток. 2017. № 3. С. 6–15.

193. Валиахметова Г.Н. Информационные технологии и кибербезопасность – новый вектор сотрудничества РФ и Государства Палестина // Известия УрФУ: Общественные науки. 2018. № 1. С. 108–117.

194. Веселов Ю.В. Доверие в цифровом обществе // Вестник СПбГУ: Социология. 2020. № 2. С. 129–143.

195. Виртуальный ислам на постсоветском пространстве: киберсреда и религиозные авторитеты / под ред. Хабибулиной З., Муратовой Э. Баку: AVE Print, 2023. 259 с

196. Гафиатулина Н.Х., Брусенцева Д.М. Медийное пространство как источник активности террористической организации // Гуманитарные, социально-экономические и общественные науки. 2017. № 6. С. 37–40.

197. Демидов О.В., Черненко Е.В. Грозный ум на страже кибербезопасности // Индекс безопасности. 2014. № 3. С. 150–161.

198. Забияко А.П. Киберрелигия: наука как фактор религиозных трансформаций. Благовещенск: Амурский госун-т, 2012. 208 с.

199. 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.

200. 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.

201. Зиновьева Е.С. Международное сотрудничество в области обеспечения информационной безопасности // Право и управление: XXI век. 2014. № 4. С. 44–52.

202. Зиновьева Е.С. Мирополитическая концептуализация международного научно-технического сотрудничества // Вестник МГИМО-Университета. 2016. № 6. С. 242–254.

203. Каберник В. Проблемы классификации кибероружия // Вестник МГИМО-Университета. 2013. № 2 (29). С. 72–78.

204. Карасев П.А. Цифровой колониализм vs цифровое неприсоединение // РСМД. 8.11.2021. URL: https://russiancouncil.ru/analytics/tsifrovoy-kolonializm-tsifrovoe-neprisoedinenie/ (дата обращения: 21.01.2022).

205. Карасев П.А. Эволюция национальных подходов к ведению кибервойны // Международная аналитика. 2022. № 2. С. 79–94.

206. 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.

207. Козюлин В.Б. Многостороннее сотрудничество в области регулирования использования технологий искусственного интеллекта. М.: Пир-Центр, 2021. 30 с.

208. Козюлин В.Б. Потенциал российских инициатив в сфере международной информационной безопасности // Вестник ученых-международников. 2022. № 2. С. 34–55.

209. 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.

210. Крутских А.В. Международная информационная безопасность: в поисках консолидированных подходов // Вестник РУДН: Международные отношения. 2022. № 2. С. 342–351.

211. Кузнецов В.А., Наумкин В.В. Глобальные и региональные тренды «столетия+» на Ближнем Востоке: новое прочтение // Вестник Моск. ун-та: Международные отношения и мировая политика. 2023. № 1. С. 70–92.

212. Кузнецов В.А. Арабские общества эпохи неомодерна: поиск новых единств // Восток. 2020. № 2. С. 28–40.

213. 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.

214. Манойло А.В. Информационная война и новая политическая реальность // Вестник МГОУ. 2021. № 2. С. 135–148.

215. Манойло А.В. Модели «мягкой силы» сетевых террористических организаций в системе угроз национальной безопасности // Вестник Российской нации. 2016. № 2. С. 180–194.

216. Международная информационная безопасность: подходы России / А.В. Крутских, Е.С. Зиновьева, В.И. Булва, М.Б. Алборова, Ю.А. Юдина. М.: МГИМО, 2021. 32 с.

217. Мелкумян Е.С. Арабские монархии Залива в XXI веке. Региональные и глобальные аспекты внешней политики. М.: ИВ РАН, 2023. 317 с.

218. Мелкумян Е.С. Власть и ислам в Кувейте: поле взаимодействия // Вестник РГГУ: Политология. 2018. № 2 (12). С. 92–104.

219. Михайленко В.И., Успенских Т.А. Политика ЕС в отношении Совета сотрудничества арабских государств Персидского залива // Современная Европа. 2019. № 5. С. 35–45.

220. Наумкин В.В. Исламский радикализм в зеркале новых концепций и подходов. М.: КомКнига, 2005. 62 с.

221. Наумкин В.В. Новые моменты в ближневосточной политике США // Проблемы национальной стратегии. 2022. № 5. С. 14–25.

222. Ромашкина Н.П. Проблема международной информационной безопасности в ООН // Мировая экономика и международные отношения. 2020. № 12. С. 24–30.

223. 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.

224. Сюкияйнен Л.Р. Глобализация и мусульманский мир: оценка современной исламской правовой мысли. М.: ИД Марджани, 2012. 88 с.

225. Сюкияйнен Л.Р. Исламское право и диалог культур в современном мире. М.: НИУ ВШЭ, 2021. 684 с.

226. Субрегионы Ближнего Востока // Международный дискуссионный клуб “Валдай». URL: https://ru.valdaiclub.com/multimedia/infographics/subregiony-blizhnego-vostoka/ (дата обращения: 15.01.2024).

227. Федоров А.В. Супертерроризм: новый вызов нового века. М.: Права человека, 2022. 198 с.

228. Хлопов О.А. Проблемы кибербезопасности в деятельности ООН // Системный анализ и синтез моделей научного развития общества. 2021. № 3. С. 65–73.

229. Чеснова Е. Н. Цифровизация религии: ислам // Гуманитарные ведомости ТГПУ. 2021. № 4. С. 71–82.

230. 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).

231. Шваб К. Четвертая промышленная революция. М.: ЭКСМО, 2017. 280 с.

232. Шмелева Т. К вопросу о создании Совета арабских и африканских государств, граничащих с Красным морем и Аденским заливом // Институт Ближнего Востока. 08.01.2020. URL: http://www.iimes.ru/?p=65692 (дата обращения: 11.10.2023).

233. Яковлева А.В. Кибербезопасность и ее правовое регулирование (зарубежный и российский опыт) // Социально-политические науки. 2021. № 4. С. 70–81.

234. 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.

235. Analyzing the entrenchment of Beijing's digital influence in Saudi Arabia and the United Arab Emirates // Georgetown Security Studies Review. 14.04.2023. URL: https://georgetownsecuritystudiesreview.org/2023/04/14/ (accessed: 03.02.2024).

236. Arslan A. Neorealist analysis of security dilemma in cyberspace: a quantitative study. Washington DC.: APSA, 2023. 17 p.

237. Baezner M. Iranian cyber-activities in the context of regional rivalries and international tensions. Zurich: CSS Cyberdefense. 2019. 37 p.

238. Bouks B. Israel's strategic threats and challenges: security, influence & cyber // Security Science Journal. 2023. № 1. P. 118–133.

239. Brzezinski Z. Between two ages. America's role in the technetronic era. N.Y., 1970. 352 p.

240. Buzan B., Waever O. Regions and powers: The structure of international security. Cambridge: Cambridge Univ. Press, 2003. 592 p.

241. Carter M., Grover V. Me, myself, and I(T): conceptualizating information technology identity and its implications // MIS Quarterly. 2015. № 4. P. 931–958.

242. Castells M. The Internet galaxy: reflections on the Internet, business, and society. Oxford, 2002. 340 p.

243. Castells M. The rise of the network society. Oxford, 2011. 609 p.

244. Christidis O. Technology and youth drive the future of work in MENA. Washington, DC: Middle East Institute. 2021..

245. Clarke R. A., Knake R. Cyber war. The next threat to national security and what to do about It. N.Y.: Harper Collins; 2010.

246. 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).

247. Crosston M. Cyber colonization: the dangerous fusion of Artificial Intelligence and authoritarian regimes // Cyber, Intelligence, and Security. 2020. № 1. P. 149–171.

248. Cyber Terrorism: assessment of the threat to insurance. Cambridge: Cambridge Centre for Risk Studies, 2017. 48 p.

249. Denning D. Information warfare and security. Washington, DC: Addison Wesley, 1999. 544 p.

250. 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.

251. 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).

252. Euro-Gulf regional cybersecurity collaboration // Bussola. 16.09.2021. URL: https://www.bussolainstitute.org/euro-gulf-regional-cybersecurity-collaboration (accessed: 06.10.2023).

253. Fearon J. Bargaining, enforcement, and international cooperation // International Organization. 1998. № 2. P. 269–305.

254. Gaub F. Stuck in the barracks: the Joint Arab Force. Brussel: EU Institute for Security Studies, 2015. 4 p.

255. Gilpin R. The political economy of international relations. New Jersey, 2016. 302 p.

256. Grieco J. M. Anarchy and the limits of cooperation: A realist critique of the newest liberal institutionalism and the future of realist theory // International Organization. 1988. № 3. P. 485–507.

257. Guzansky Y., Michael K. Revisiting the possibility of a regional military alliance // INSS Insight. 2022. № 1561. 5 p.

258. Haas P. Epistemic communities and international policy coordination // International Organization. 1992. № 1. P. 1–35.

259. 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.

260. Hassib B, Shires J. Cybersecurity in the GCC: from economic development to geopolitical controversy // Middle East Policy. 2022. № 29. P. 90–103.

261. Herrera G.L. Technology and international transformation. N.Y.: State Univ. of N.Y. Press, 2007. 278 p.

262. Is crypto haram or halal? Reasons & opinion of Islamic scholars // Academy for International Modern Studies. URL: https://aims.education/is-bitcoin-halal-or-bitcoin-haram/ (accessed: 12.10.2023).

263. Israel is becoming a cybersecurity guarantor in the Middle East // Atlantic Council. 18.11.2021. URL: https://www.atlanticcouncil.org/menasource/israel-is-becoming-a-cybersecurity-guarantor-the-middle-east (accessed: 17.10.2023).

264. 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.

265. 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).

266. Kasapoglu C. Turkey's future cyber defense landscape. Ankara: Centre for Economics and Foreign Policy Studies, 2016. 20 p.

267. Khorrami N. Israel's cybersecurity cooperation with the GCC states. Singapore: Middle East Institute, 2021. 14 p.

268. 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).

269. Kwet M. Digital colonialism: US empire and the new imperialism in the Global South // Race & Class. 2019. № 4. P. 13–24.

270. Lawrence B. Allah On-line: the practice of global Islam in the information Age. N.Y.: Columbia Univ. Press, 2002. P. 237–253.

271. Libicki M. Cyberdeterrence and cyberwar. Santa Monica, 2009.

272. Liu L. China's policy and practice regarding the Gulf security // Stepping away from the abyss. San Domenico di Fiesole: EU Institute, 2021. P. 81–94.

273. 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.

274. Mearsheimer J. The tragedy of great power politics. N.Y., 2001. 592 p.

275. Migration in the Middle East and North Africa. Tunis: Konrad Adenauer Stiftung, 2021. 7 p.

276. Mihalka M. Cooperative security in the 21st century // Connections: The Quarterly Journal. 2005. № 4. P. 113–122.

277. Mogielnicki R. Smart context-based investments in the Persian Gulf's economic security // Stepping away from the abyss. San Domenico di Fiesole: EU Institute, 2021. P. 163–174.

278. 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).

279. 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).

280. Munawar, S., Afzal, S., Shahid, R. Realism: revisiting the concept of power in the age of information // Global Strategic & Security Studies Review. 2021. № 6. P. 128–137.

281. Nance M., Sampson Ch. Hacking ISIS: how to destroy the cyber jihad. N.Y.: Skyhorse, 2017. 320 p.

282. 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.

283. 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.

284. Onireti A. Cyber-terrorism: an appraisal of the dimensions of the new face of terrorism in a post-9/11 period. L.: Routledge, 2024. 196 p.

285. 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).

286. Schneider N. Governable stacks against digital colonialism // Communication, Capitalism & Critique. 2022. № 1. P 20–31.

287. Sheldon J. Deciphering cyberpower: strategic purpose in peace and war // Strategic Studies Quarterly. 2011. № 2. P. 95–112.

288. Shires J., Hakmeh J. Is the GCC cyber resilient? L.: Chatham House, 2020. 20 p.

289. Skolnikoff E.B. The elusive transformation: science, technology, and the evolution of international politics. Princeton Univ. Press, 1994. 336 p.

290. Siboni G., Cohen D., Rotbart A. The threat of terrorist organizations in cyberspace // Military and Strategic Affairs. 2013. № 3. P. 20–29.

291. Siboni G., Kronenfeld S. Developments in Iranian cyber warfare 2013–2014 // Military and Strategic Affairs. 2014. № 2. P. 83–104.

292. Shanzer J., Miller S. Facebook fatwa: Saudi clerics, Wahhabi Islam, and social media. Washington DC: Foundation for Defense of Democracies, 2012. 103 p.

293. 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.

294. Teasuro L. The role 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).

295. The Negev Summit furthers Arab-Israeli normalization // The U.S. Institute of Peace. 31.03.2022. URL: https://www.usip.org/publications/2022/03/negev-summit-furthers-arab-israeli-normalization (accessed: 14.10.2023).

296. Toffler A. Powershift: knowledge, wealth, and violence in the 21st century. N.Y.: Bantam Books, 1990. 640 p.

297. Walt S. The origins of alliance. New York: Cornell University Press. 1987.

298. Waltz K. Theory of international politics. Reading: Addison-Wesley, 1979.

299. West L. #jihad: Understanding social media as a weapon // Security Challenges. 2016. № 2. P. 9–26.

300. Zhioua S. The Middle East under malware attack dissecting cyber weapons. Philadelphia, PA: IEEE, 2013. 6 p.

301. 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).

302. 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).

ПРИЛОЖЕНИЕ I. ТАБЛИЦЫ

Таблица 1. Количество пользователей мобильной связи в монархиях Залива (по состоянию на декабрь 2023 г.)

№	Название страны	Количество пользователей (млн чел.)	Среднегодовой прирост
1	Саудовская Аравия	48,2	+7%
2	ОАЭ	20,1	+3,8%
3	Кувейт	7,8	+2,5%
4	Оман	6,8	+2%
5	Катар	4,7	+2,3%
6	Бахрейн	2,14	+2,4%

Составлено по: Mobile cellular subscriptions // World Bank. URL: https://data.worldbank.org/indicator/true&locations=SA-AE-KW-OM-BH-QA (accessed: 20.12.2023); Mobile internet usage in MENA // Statista. URL: https://www.statista.com/topics/8710/mobile-internet-usage-in-MENA/topicOverview (accessed: 20.12.2023).

Таблица 2. Динамика изменения позиций монархий Залива в глобальном и региональном (арабский мир) рейтинге кибербезопасности МСЭ ООН

Страна	*КСА*		*ОАЭ*		*Катар*		*Кувейт*		*Бахрейн*		*Оман*	
Уровень / *Год*	*Рег.*	*Глоб.*	*Рег.*	*Глоб.*	*Рег.*	*Глоб.*	*Рег.*	*Глоб.*	*Рег.*	*Глоб.*	*Рег.*	*Глоб.*
2017	5	46	6	47	3	25	17	138	8	65	1	4
2018	1	13	5	33	3	17	6	67	7	68	2	16
2020	1	2	2	5	5	27	9	65	8	60	3	21

Составлено по: Global Cybersecurity Index 2017. Geneva, 2017. P. 1–6; Global Cybersecurity Index 2018. Geneva, 2019. P. 54; Global Cybersecurity Index 2020. Geneva, 2021. P. 25–29.

Таблица 3. Сравнительные характеристики киберподразделений «Объединенный киберхалифат» (ИГИЛ) и «Цифровой батальон ан-Немра» (Аль-Каида)

	«Объединенный киберхалифат»	«Цифровой батальон ан-Немра»
Принадлежность	ИГИЛ	Аль-Каида
Основная специализация	Доксинг, дефейс, DDoS-атаки	Доксинг, DDoS-атаки
Встроенность в структуру группировки	Да	Нет
Количество команд в составе группировки	4	3
Количество лояльных команд	2	9
Контакты с другими радикальными хакерскими группировками	Да	Да
Контакты с хакерами-одиночками	Да	Нет
Пропагандистская деятельность	Да	Да
Вербовочная деятельность	Да	Да
Защита чувствительных данных	Да	Да
Учебная деятельность	Да	Нет
Оборот криптовалюты	Да	Нет

Составлено по: Teasuro L. The Role 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); Nance M., Sampson Ch. Hacking ISIS: How to Destroy the Cyber Jihad. N.Y., 2017. P. 248, 271–273, 277, 290, 301.

Таблица 4. Правовое регулирование в монархиях Залива по отдельным категориям кибербезопасности

Страна Категория	**КСА**	**ОАЭ**	**Катар**	**Бахрейн**	**Оман**	**Кувейт**
Сектор телекоммуникаций	+	+	+	+	+	+
Электронная торговля	+	+	+	+	+	+
Банковский сектор	+	+	+	+	+	Сформировано с лакунами
Противодействие киберпреступности	+	+	+	+	+	+
Защита персональных данных	+	+	+	+	Сформировано с лакунами	+

Составлено по: Arab Laws Online. Database of Laws & Legislation // Arab Laws. URL: https://www.arablawsworld.com/ (accessed: 21.11.2023); Laws and Regulations // GCC. URL: мhttps://www.gcc-sg.org/en-us/CognitiveSources/Pages/LawsandRegulations.aspx (accessed: 06.10.2023).

.

Таблица 5. Степень развития национальных систем кибербезопасности монархий Залива согласно критериям и оценке МСЭ ООН

Страна	Индекс МСЭ*	Параметры оценки МСЭ**				
		Правовые меры	*Технические меры*	*Организационные меры*	*Развитие потенциала*	*Международное сотрудничество*
Бахрейн	77,86	20	12.12	15.11	16.77	13.86
Катар	94,5	20	16.64	18.46	20	19.41
Кувейт	75,05	17.74	14.25	11.13	16.05	15.9
ОАЭ	98,06	20	19.08	18.98	20	20
Оман	96,04	20	16.64	20	20	20
Саудовская Аравия	99,54	20	19,54	20	20	20

* - максимальный показатель -100
** - максимальный показатель - 20
Составлено по: Global Cybersecurity Index 2020. Geneva, 2021. P. 77–82.

Таблица 6. Правовое регулирование сектора торговли криптовалютами в монархиях Залива

Страна Категория	КСА	ОАЭ	Катар	Бахрейн	Оман	Кувейт
Отношение властей к криптовалюте	Компромиссное	Позитивное	Негативное	Компромиссное	Позитивное	Негативное
Наличие регулирующих отрасль нормативно-правовых актов	Да	Да	Да	Да	Да	Нет
Легальность криптобизнеса	Да (с оговорками)	Да	Нет (с оговорками)	Да	Да	Нет
Наличие криптобирж и центров майнинга, их регулирование	Нет	Да	Нет	Да	Да	Нет
Разработка национальных токенов и их регулирование	Да	Да	Нет	Нет	Нет	Нет

Составлено по: Arab Laws Online. Database of Laws & Legislation // Arab Laws. URL: https://www.arablawsworld.com/ (accessed: 21.11.2023).

Таблица 7. Группы реагирования на компьютерные инциденты в монархиях Залива

	Общенациональные группы CERT	**Отраслевые группы CERT**		**Частные мониторинговые группы**	**Профильные аналитические центры (SoC и др.)**
		Статус	**Сектор**		
КСА	+	В процессе создания	Нефтегазовый сектор	+	-
ОАЭ	+	-	-	+	+
Катар	+	+	Нефтегазовый сектор	+	+
Оман	+	+	Финансовый сектор	-	+
Бахрейн	+	В процессе создания	Финансовый сектор	+	-
Кувейт	+	-	-	+	+

Составлено по: The OIC-CERT Annual Report. Kuala Lumpur: IOC, 2022. 116 p.; World CERTs (aeCERT, CERT.bh, Oman National CERT, Saudi CERT, Qatar's Computer Emergency Response Team). // CERT-In. URL: https://www.cert-in.org.in/s2cMainServlet?pageid=ADWCERTVIEW (accessed: 15.10.2023).

Таблица 8. Организационные показатели систем кибербезопасности монархий Залива

Страна / Критерий	КСА	ОАЭ	Катар	Оман	Бахрейн	Кувейт
Первичный орган регулирования киберпространства (год создания)	Комиссия по коммуникациям и информационным технологиям (CITC, 2001)	Регулирующий орган электросвязи (TRA, 2003)	Верховный совет информационных и коммуникационных технологий (SCCIT, 2004)	Управление информационных технологий (ITA, 2006)	Регуляторный орган электросвязи (TRA, 2002)	Центральное агентство информационных технологий (CAIT, 2006)
Специализированный орган регулирования сферы кибербезопасности (год создания)	Национальное управление кибербезопасности (NCA, 2017)	Государственный регулирующий орган в области телекоммуникаций и цифровых технологий (TDRA, 2021)	Министерство транспорта и коммуникаций (MoTC, 2016)	Министерство транспорта, связи и информационных технологий (MTCIT, 2019)	Национальный комитет по кибербезопасности (NCIS, 2017)	Регуляторный орган связи и информационных технологий (CITRA, 2019)
Наличие специализированных департаментов в составе государственных институтов	Да	Да	Да	Да	Да	Да
Наличие вспомогательных агентств в структуре управления кибербезопасностью	Да	Да	Нет	Да	Нет	Нет
Стратегия кибербезопасности	Да (проект)	Да	Да (формально истекла)	Нет (в разработке)	Да	Да (формально истекла)

Составлено автором.

Таблица 9. Соответствие монархий Залива критериям МСЭ ООН в области разработки стратегий кибербезопасности

Страна / Критерий	КСА	ОАЭ	Катар	Оман	Бахрейн	Кувейт
Своевременное обновление документов стратегического характера	Да (с оговорками)	Да	Да	Нет (в процессе)	Да	Нет (в процессе)
Проведение аудитов киберугроз на национальном уровне	Да	Да	Да	Да	Да	Да
Соблюдение принципа приоритезации угроз	Да	Да	Да	Да	Нет	Нет
Соблюдение принципа системности консультационной поддержки	Да	Да	Да	Да	Да	Нет
Ежегодная выработка метрик оценки кибербезопасности	Да	Нет	Да	Да	Нет	Нет

Составлено по: Руководство МСЭ по разработке национальной стратегии кибербезопасности. Женева, 2018; Global Cybersecurity Index 2020. Geneva, 2021. P. 10–13; Bahrain National cybersecurity strategy // National Cyber Security Center. 10.01.2022. URL: https://www.ncsc.gov.bh/en/national-strategy.html (accessed: 10.02.2023); Developing national information security strategy for the Kingdom of Saudi Arabia. Riyadh: Ministry of Communications and Informational Technology, Riyadh. 2017. 90 p.; Oman Cyber Security Governance guidelines. URL: https://www.ita.gov.om/ITAPortal/Pages/735301 (accessed: 19.01.2024); Qatar National cybersecurity strategy. Doha: MoTC, 2014. 35 p.; The UAE National cybersecurity strategy. Abu Dhabi: NCSC, 2019. 28 p.; الكويت لدولة السيبراني للأمن الوطنية الإستراتيجية (Национальная стратегия кибербезопасности Государства Кувейт). El Kuwait: TRA, 2017. 35 p.

Таблица 10. Сотрудничество монархий Залива в двустороннем формате по линии профильных ведомств и государственно-частного партнерства

№	*Страна*	КСА	ОАЭ	Оман	Катар	Бахрейн	Кувейт
1	США	1, 2	1, 2	1, 2	1, 2	1, 2	1, 2
2	Великобритания	1, 2	2	2	2	1, 2	1, 2
3	КНР	1, 2	1, 2	2	2	2	2
4	Россия	2	2	2	2	-	2
5	Франция	2	2	2	2	1, 2	2
6	Германия	2	1, 2	2	1, 2	2	2
7	Италия	2	2	-	2	-	-
8	Канада	2	2	-	2	2	2
9	Австрия	2	2	-	-	-	-
10	Норвегия	2	2	-	2	-	-
11	Япония	2	2	2	2	1, 2	2
12	Южная Корея	2	2	2	2	1, 2	2
13	Израиль	3	1, 2	3	3	1, 2	-
14	Турция	2	-	2	1, 2	-	2
15	Индия	1, 2	1, 2	1, 2	1, 2	2	2
16	Малайзия	-	-	1, 2	-	-	2
17	Австралия	2	-	-	-	2	-
18	Египет	2	2	2	-	2	-
19	Иордания	2	2	2	2	2	2
20	Сомали	3	-	-	-	-	-
21	Йемен	-	3	-	-	-	-
22	Джибути	3	-	-	-	-	-
23	Саудовская Аравия	-	1, 2	2	-	2	2
24	ОАЭ	1, 2	-	2	-	2	2
25	Оман	2	2	-	-	2	-
26	Катар	-	-	-	-	2	-
27	Бахрейн	2	2	2	-	2	2
28	Кувейт	2	2	-	-	2	-

«1» – отраслевые и межведомственные соглашения, меморандумы о взаимопонимании;
«2» – международное государственно-частное партнерство;
«3» – «дискретное» сотрудничество (сотрудничество через посредников).

Составлено автором по открытым источникам.

Таблица 11. Сравнительные характеристики Будапештской конвенции 2001 г. (включая Дополнительный протокол 2003 г.) и Арабской конвенции о борьбе с преступлениями в области информационных технологий 2010 г.

Список положений	Будапештская конвенция 2001 г.	Арабская конвенция 2010 г.
Ключевые понятия		
Компьютер/информация система	+	+
Компьютер/информация сеть	−	+
Устройство/хранилище информации	−	−
Критический инфраструктура	−	−
Компьютерные данные/информация (включая компьютерную программу)	+	+
Электронная запись	−	−
Данные о подписчиках/трафике/контенте	+	+
Электронная связь /почта	−	−
Вредоносное ПО /вредоносное программное обеспечение	−	−
Интернет-провайдер	+	+
Ребенок / несовершеннолетний	+	−
Киберпреступность / преступление в области компьютерных технологий	−	−
Криминализация (противоправные действия)		
Незаконный доступ к компьютерной системе	+	+
Незаконный доступ, перехват или получение компьютерных данных	+	+
Незаконное вмешательство в компьютерные данные	+	+
Незаконное вмешательство в компьютерную систему	+	+

использование компьютерных инструментов	+	+
Нарушение конфиденциальности или меры защиты данных	–	–
Подлог с использованием цифровых средств	+	+
Мошенничество с использованием компьютерных средств	+	+
Правонарушения, связанные с электронными платежными инструментами	–	+
Преступления, связанные с идентификацией в Интернете	–	–
Нарушения в области авторских прав и использования товарных знаков в цифровом пространстве	+	+
Спам	–	–
Кибербуллинг, вымогательство в социальных сетях или иные действия, причиняющие личный вред	–	–
Действия в цифровом пространстве, связанные с расизмом или ксенофобией	+	–
Отрицание или оправдание геноцида или преступлений против человечности с использованием цифрового пространства	+	–
Производство, распространение или хранение детской порнографии	+	+
Цифровой харассмент	–	–
Поддержка террористической деятельности	–	+
Компьютерные преступления, связанные с отмыванием денег	–	+
Компьютерные преступления, связанные с незаконным оборотом товаров и услуг	–	+
Компьютерные преступления против общественного порядка, нравственности или безопасности	–	+

Правонарушения, связанные с расследованием правоохранительных органов	+	+
Отягчающие обстоятельства обычного преступления, совершенного с использованием цифровых технологий	–	+
Подстрекательство в Интернете	+	–
Корпоративная ответственность (ответственность компаний)	+	–
Процедурные полномочия		
Поиск компьютерного оборудования или данных	+	+
Изъятие компьютерного оборудования или данных	+	+
Запрос архивных компьютерных данных	+	+
Запрос информации о подписках	+	+
Запрос информации о трафике (архивные данные)	+	+
Сбор данных о трафике в режиме реального времени	+	+
Сбор данных о контенте в режиме реального времени	+	+
Ускоренное сохранение компьютерных данных	+	+
Использование (удаленных) инструментов судебной экспертизы	–	–
Трансграничный доступ к компьютерным данным	+	+
Оказание содействия в расследовании	+	+
Извлечение частных данных из компьютера	–	–
Электронные доказательства (улики)		
Допустимость использования электронных доказательств / записей	–	–
Допустимость электронной подписи	–	–

Бремя доказывания достоверности	–	–
Правило наилучшего доказательства (приоритет оригинала над копией)	–	–
Использование распечаток (переписок) в качестве серьезного доказательства	–	–
Презумпция честности	–	–
Стандарты хранения электронных вещественных доказательств	–	–
Порядок запроса электронных доказательств из других стран, а также использования иностранных электронных документов	–	–
Юрисдикция		
Территориальный принцип	+	+
Использование компьютерной системы/баз данных, находящихся на территории государства	–	–
Национальный принцип (преступник)	+	+
Национальный принцип (жертва)	–	–
Принцип постоянного места жительства	–	–
Принцип места регистрации юридического лица	–	–
Принцип государственных интересов	–	+
Юрисдикция в случае отказа в экстрадиции	+	+
Корабли и самолеты	+	+
Двойная преступность	+	+
Параллельная юрисдикция	+	+
Установление места правонарушения	–	–
Международное сотрудничество		
Общие принципы международного сотрудничества	+	–
Экстрадиция за преступления, связанные с киберпространством	+	+
Взаимное содействие	+	+

Механизм ускоренной помощи	+	+
Содействие в сохранении и защите компьютерных данных	+	+
Содействие в конфискации / обеспечении доступа/ сборе / раскрытии компьютерных данных	+	+
Трансграничный доступ к компьютерным данным	+	+
Предоставление незапрошенной информации / обмен информацией	+	+
Конфиденциальность запросов	+	+
Двойная преступность (международный аспект)	+	+
Принцип непрерывного мониторинга	+	+
Персональная ответственность и ответственность поставщика услуг		
Обязательства по мониторингу	–	–
Добровольный поставка информации	–	–
Уведомление	–	–
Обеспечение доступа к информации (со стороны провайдеров)	–	–
Кэширование данных	–	–
Хостинг данных со стороны провайдеров	–	–
Ответственность поставщиков поисковых систем	–	–

Составлено по: Budapest Convention on Cybercrime. Budapest: European Commission, 2001. 22 p.; Arab Convention on Combating Information Technology Offences. Cairo: Arab League, 2010. 29 p.; بلتقييس المعني العربي العمل لفريق العاشر الاجتماع (X заседание Арабской рабочей группы по стандартизации). Cairo: Arab League, 2016. 16 p

Таблица 12. Доля иностранных IT-компаний, представленных на рынках аравийских монархий (включая сектор кибербезопасности), %. (по состоянию на начало 2024 г.)

	США	**КНР**	**Россия**	**Страны ЕС**	**Израиль**	**Остальные страны (совокупный показатель)**
КСА	27,4	23	5	8,1	1*	35,5
ОАЭ	26,4	19,6	8	6	17	23
Катар	20,2	20,3	4,5	9,3	5,7*	40
Бахрейн	25	15	4	10	14	32
Оман	24	24	3,9	4,6	4,1*	39,4
Кувейт	35	18	0	4	0	43
Средняя доля по рынкам ССАГЗ	26,4	19,9	4,24	7	6,96	-

* – компании, созданные при участии израильской стороны в рамках «дискретного» сотрудничества.

Составлено и посчитано автором по открытым источникам.

Использованы данные по национальным профилям аравийских монархий, РФ, США, КНР, Европейских стран, Израиля и ряда других стран мира.

Таблица 13. SWOT-анализ. Оценка перспектив и рисков развития кооперации монархий Залива в сфере кибербезопасности на площадке ССАГЗ

	Положительное влияние	**Отрицательное влияние**
Внутренняя среда	***Сильные стороны (strengths)*** – наличие общего пространства цифровых угроз, схожие подходы к их градации – схожие цели и задачи долгосрочного развития, в которых цифровизация играет ключевую роль, формируя запрос на выработку коллективных мер цифровой защиты – наличие у каждого актора развитой системы национальной киберзащиты, общность взглядов на текущие и долгосрочные приоритеты развития сектора кибербезопасности – наличие совместных институтов профильного сотрудничества в рамках ССАГЗ – ставка на развитие международного сотрудничества, схожие подходы к выбору внешних партнеров	***Слабые стороны (weaknesses)*** – реактивный и ситуативный характер кооперации – приоритет развития национальных систем киберзащиты – несовершенство национальных систем кибербезопасности – слабая развитость профильных связей между членами ССАГЗ, приоритет двустороннего взаимодействия с внерегиональными партнерами – разногласия внутри ССАГЗ, в т.ч. по проблемам региональной безопасности, наличие атмосферы недоверия, нежелание делиться чувствительными технологиями
Внешняя среда	***Возможности (opportunities)*** – неблагоприятный региональный фон стимулирует кооперацию в сфере киберзащиты на площадке ССАГЗ – развитие сотрудничества с другими странами мира в рамках участия ССАГЗ в глобальных и региональных инициативах	***Угрозы (threats)*** – высокий конфликтный потенциал Ближнего Востока – вовлеченность монархий Залива в региональные конфликты – рост региональной напряженности

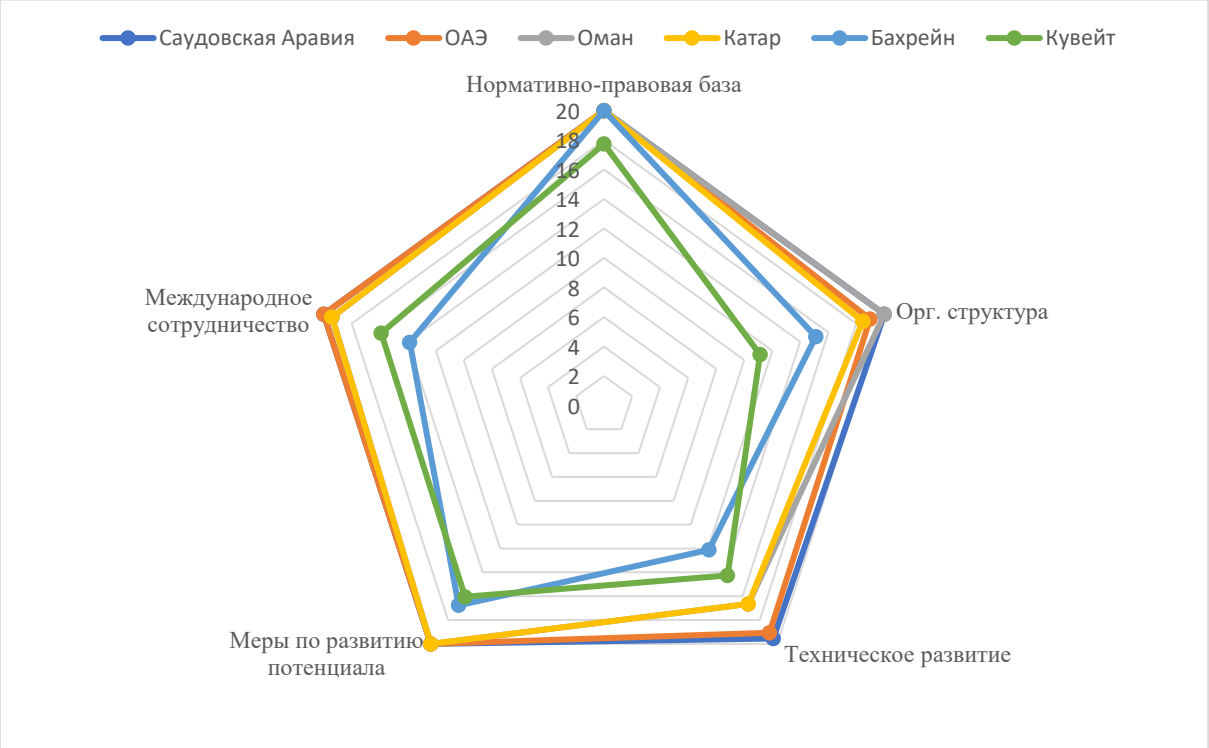
Составлено автором

ПРИЛОЖЕНИЕ II. СХЕМЫ

Схема 1. Структура утечек данных в результате кибератак в монархиях Залива в 2023 г. (в процентах)

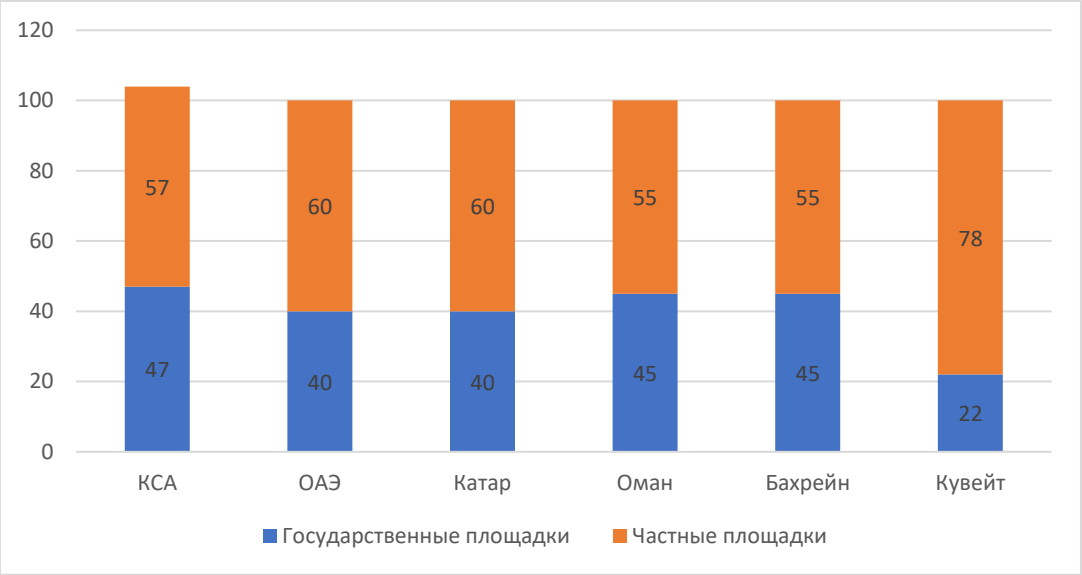
Составлено по: Cost of a Data Breach Report. New York: IBM, 2023. 70 p.

Схема 2. Визуализация текущего состояния систем кибербезопасности монархий Залива (сводная схема)



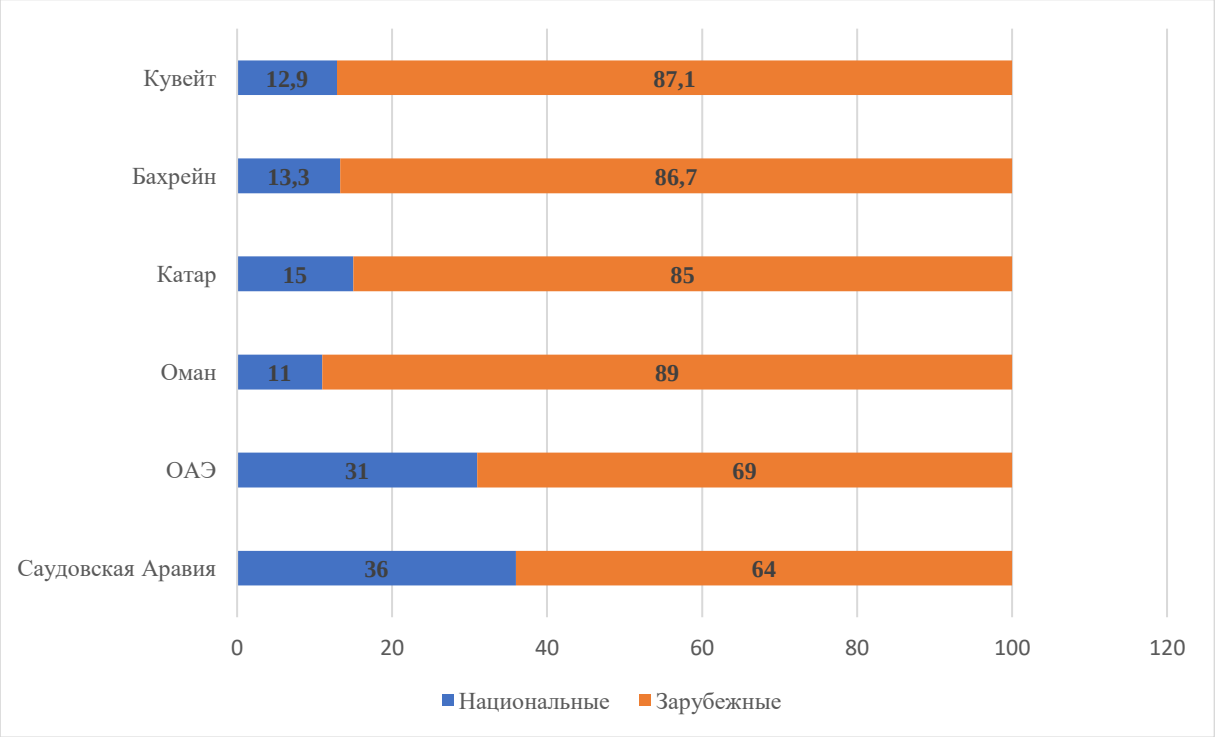
Составлено по: Global Cybersecurity Index 2020. Geneva, 2021. P. 77-82.

Схема 3. Образовательные площадки монархий Залива по профилю «кибербезопасность» (по состоянию на конец 2023 г.)



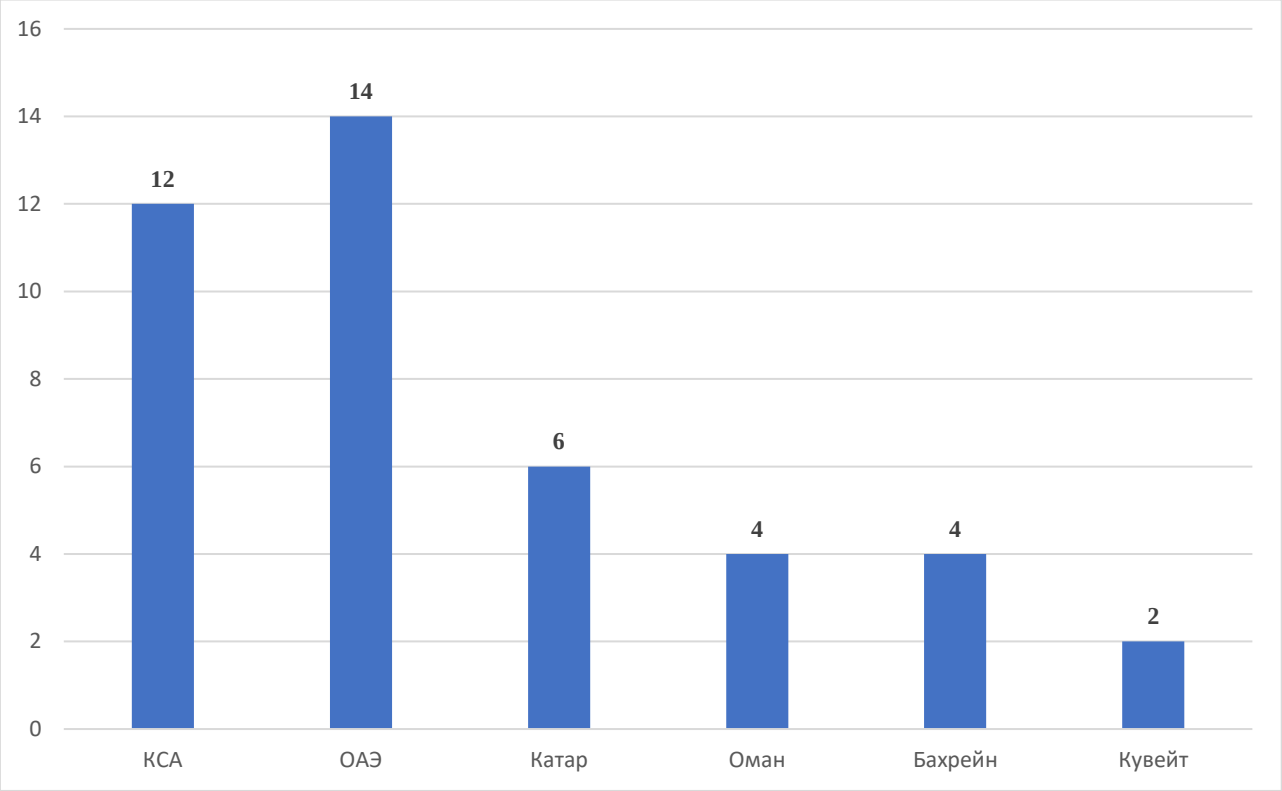
Составлено автором.

Схема 4. Соотношение национальных и зарубежных компаний в секторе кибербезопасности монархий Залива (по состоянию на начало 2024 г., в процентах)



Составлено и посчитано автором по открытым источникам.

Схема 5. Среднегодовое число международных мероприятий по профилю «кибербезопасность», проводимых на территории монархий Залива (среднегодовой показатель за период 2021–2023 гг.)



Составлено автором.

Схема 6. Общая схема организации «дискретного сотрудничества» между Израилем и монархиями Залива (на примере ОАЭ до подписания «Соглашений Авраама» в 2020 г.)

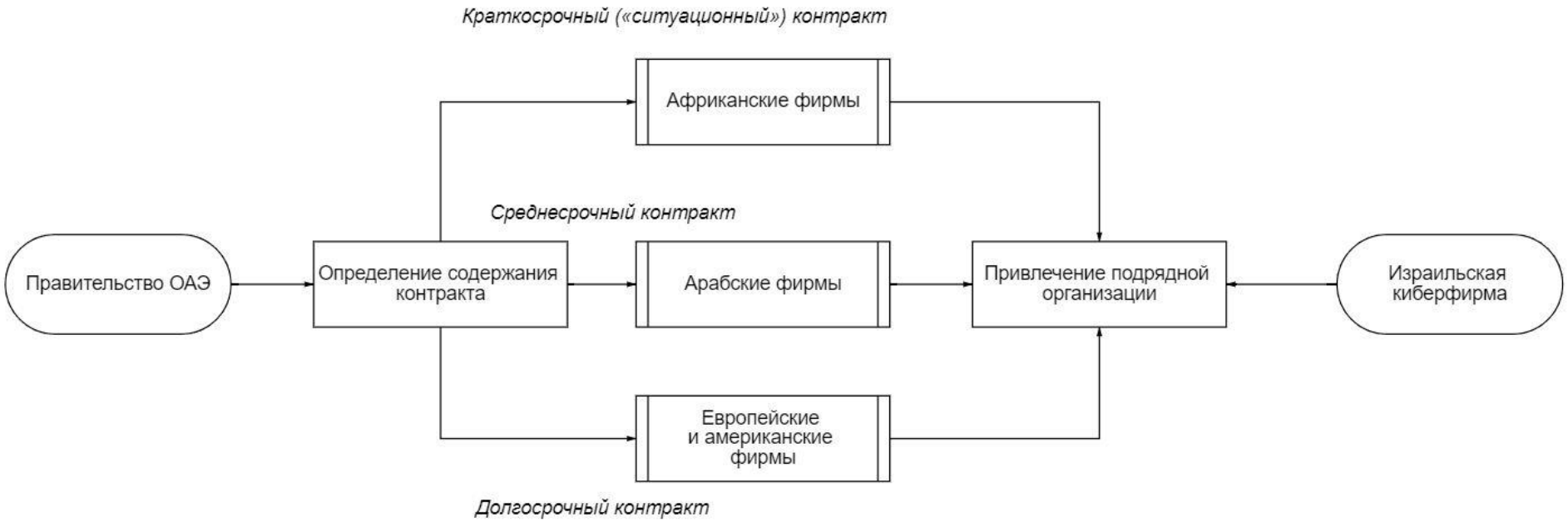
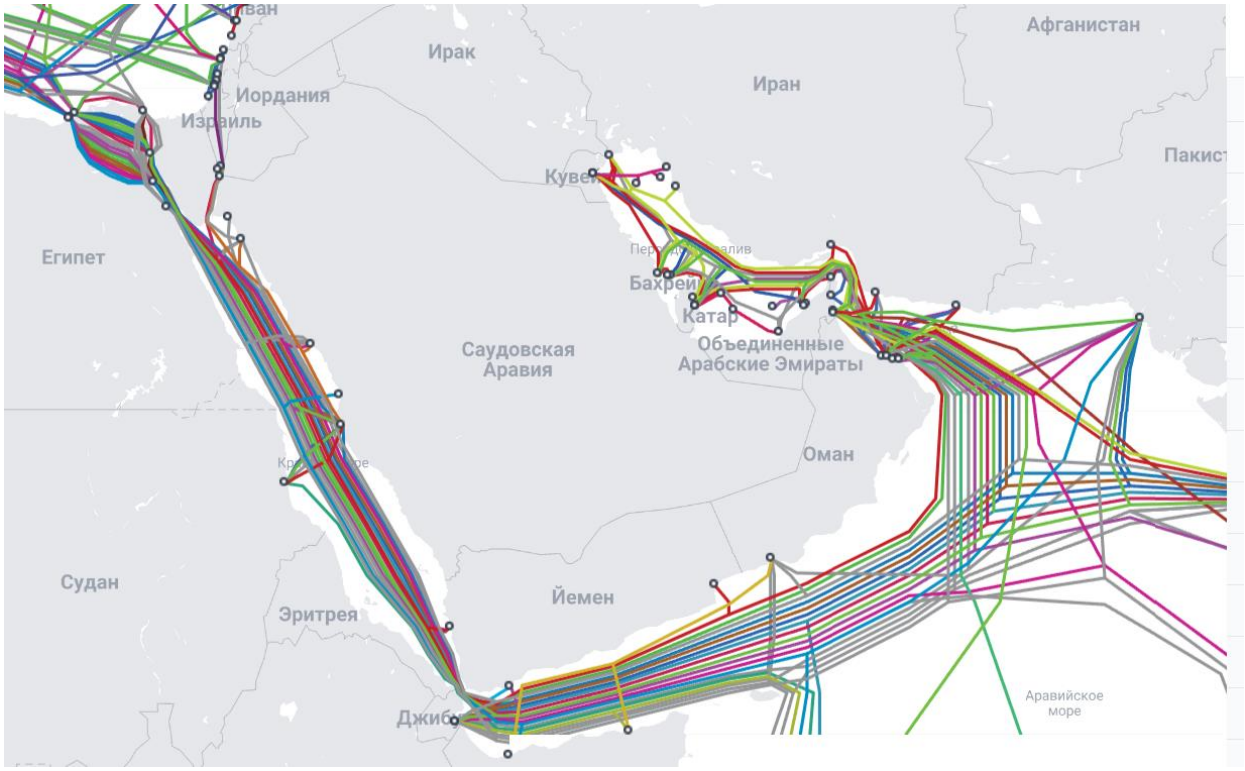
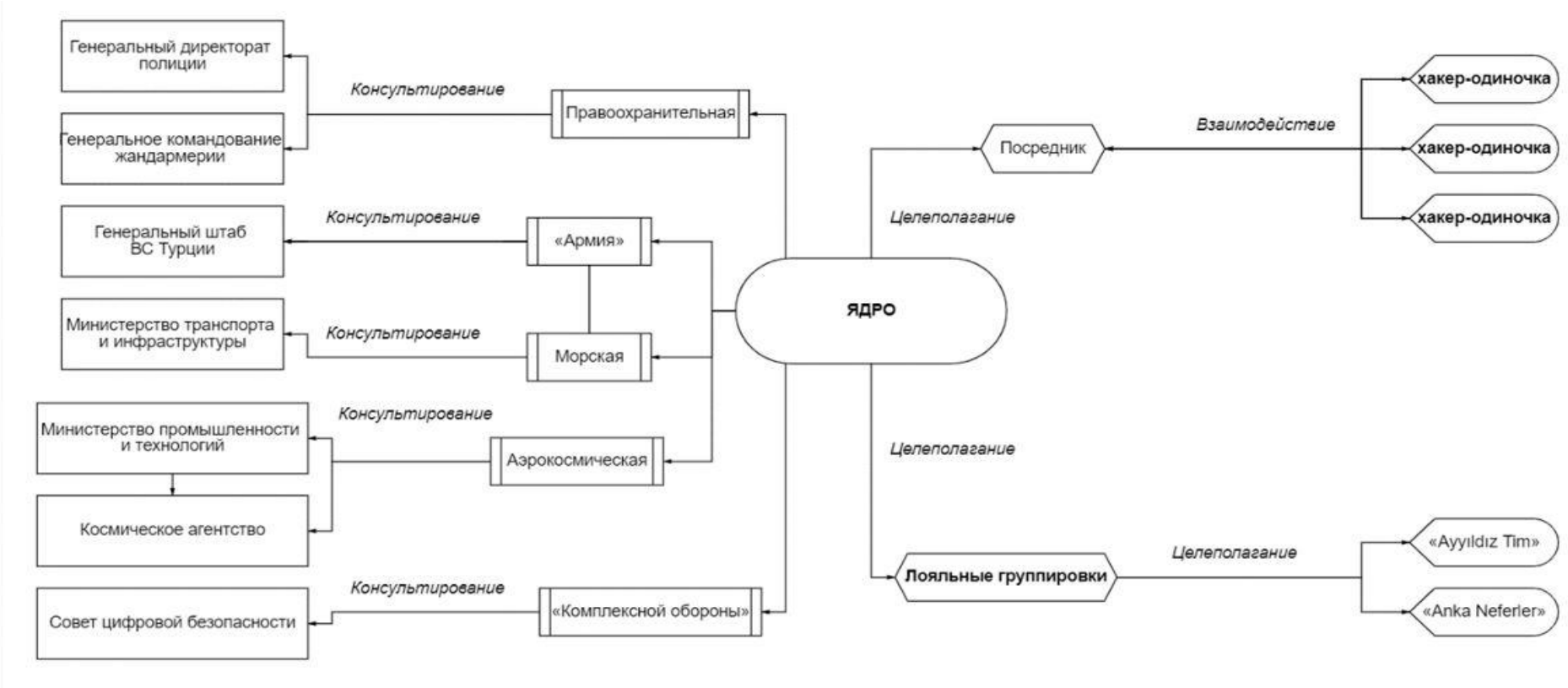


Схема 7. Схема расположения крупнейших подводных оптоволоконных кабелей в регионе Персидского залива (по состоянию на начало 2024 г.)



Источник: Submarine cable map. URL: https://www.submarinecablemap.com/ (accessed: 21.02.2024).

Схема 8. Модель интеграции хакерского сообщества в систему киберзащиты национального государства (на примере Турции)



Составлено автором.

ПРИЛОЖЕНИЕ III. СПИСОК СОКРАЩЕНИЙ

БПЛА – Беспилотный летательный аппарат

ВОЗ – Всемирная организация здравоохранения

ГПЭ – Группа правительственных экспертов

ГЧП – Государственно-частное партнерство

ИКТ – Информационно-коммуникационные технологии

ИКТ – Информационно-коммуникационные технологии

ЛАГ – Лига арабских государств

МИБ – Международная информационная безопасность

МСЭ – Международный союз электросвязи

НКО – Некоммерческая организация

ОАСБР – Объединенные арабские силы быстрого реагирования

ОИС – Организация Исламского сотрудничества

ОМУ – Оружие массового уничтожения

ПО – Программное обеспечение

РГОС – Рабочая группа открытого состава

САС – Смертоносная автономная система (вооружений)

ССАГЗ – Совет сотрудничества арабских государств Залива

ЮПС – Южный переходный совет (Йемен)

AI – Artificial intelligence – Искусственный интеллект

CERT – Computer Emergency Response Team – Компьютерная группа реагирования на чрезвычайные ситуации

CTF – Combined Task Forces – Объединенные оперативные группы

E-Government («E-Gov») – Электронное правительство

ENISA – *The European Union Agency for Network and Information Security* – Европейское агентство по сетевой и информационной безопасности

FIRST – Forum of Incident Response and Security Teams – Форум групп реагирования на инциденты и обеспечения безопасности

GCCEI – Global Center for Combating Extremism Ideology – Глобальный центр по борьбе с экстремистской идеологией (Саудовская Аравия)

GDSI – Global Data Security Initiative – Глобальная инициатива по безопасности данных.

«G2G» – «Government to Government» – Государство для государства (тип услуги)

IBM – International Business Machines – Международные бизнес-механизмы (корпорация; США)

ICI – Istanbul Cooperation Initiative – Стамбульская инициатива по сотрудничеству (НАТО)

IOCTA – Internet Organised Crime Threat Assessment – Оценка угроз организованной преступности в Интернете

ISO – International Organization for Standartization – Международная организация по стандартизации

ITA – Information Technology Authority – Управление информационных технологий (Оман)

ITU–ARCC – The ITU – Arab Regional Cybersecurity Center – Арабский региональный центр кибербезопасности под эгидой МСЭ

IXP – Internet Exchange Point – Точка обмена трафиком

MENA – Middle East and North Africa – Ближний Восток и Северная Африка

MESA – Middle East Strategic Alliance – Ближневосточный стратегический альянс

MoTC / MTC – Ministry of Transport and Communications – Министерство транспорта и коммуникаций (Катар, Оман)

MoU – Memorandum of understanding – Меморандум о взаимопонимании

MTCIT – Ministry of Transport, Communications and Information Technology – Министерство транспорта, связи и информационных технологий (Оман)

NCA – National Cybersecurity Authority – Национальное управление кибербезопасности (Саудовская Аравия)

NCIA – NATO Communications and Information Agency – Агентство НАТО по связи и информации

NCIS – National Committee for Internet Safety – Национальный комитет по безопасности в Интернете (Катар)

NCSC – National Center for Cybersecurity – Национальный центр кибербезопасности (ОАЭ, Кувейт)

NESA – National Electronic Security Authority – Национальное управление электронной безопасности (ОАЭ)

RSIEC – Red Sands Integrated Experimentation Center – Интегрированный испытательный центр «Красные пески»

SCCIT – Supreme Council for Communication and Information Technology – Верховный совет информационных и коммуникационных технологий (Катар)

SoC – Security Operations Center – Центр управления безопасностью

TDRA – Telecommunications and Digital Government Regulatory Authority – Государственный регулирующий орган в области телекоммуникаций и цифровых технологий (ОАЭ)

TFTC – Terrorist Financial Target Center – Центр по противодействию финансированию терроризма (Саудовская Аравия)

TRA – Telecommunications Regulatory Authority – Регулирующий орган электросвязи (ОАЭ, Бахрейн)