OPEN ACCESS

[Научный диалог = Nauchnyi dialog = Nauchnyy dialog, 14(7), 2025]
[ISSN 2225-756X, eISSN 2227-1295]

Check for updates

Информация для цитирования:

Валиахметова Г. Н. Нормативно-правовое обеспечение кибербезопасности в арабских монархиях Залива : этапы и особенности развития / Г. Н. Валиахметова, Л. В. Цуканов // Научный диалог. — 2025. — Т. 14. — № 8. — С. 421—441. — DOI: 10.24224/2227-1295-2025-14-8-421-441.

Valiakhmetova, G. N., Tsukanov, L. V. (2025). Legal and Regulatory Framework for Cybersecurity in Arab Gulf Monarchies: Stages and Features of Development. *Nauchnyi dialog, 14* (8): 421-441. DOI: 10.24224/2227-1295-2025-14-8-421-441. (In Russ.).

Clarivate Web of Science · Scopus · Q1 · DOAJ · ERIHPLUS · eLIBRARY.RU РИНЦ

Перечень рецензируемых изданий ВАК при Минобрнауки РФ

Нормативно-правовое обеспечение кибербезопасности в арабских монархиях Залива: этапы и особенности развития

Валиахметова Гульнара Ниловна [1]
orcid.org/0000-0001-7199-7723
доктор исторических наук,
заведующая кафедрой востоковедения,
корреспондирующий автор
vgulnara@mail.ru

Цуканов Леонид Вячеславович [2]
orcid.org/0000-0001-6882-9841
кандидат политических наук,
научный сотрудник
leon.tsukanov@mail.ru

[1] Уральский федеральный университет
имени первого Президента России
Б. Н. Ельцина
(Екатеринбург, Россия)

[2] ПИР-Центр
(Центр политических исследований)
(Москва, Россия)

Legal and Regulatory Framework for Cybersecurity in Arab Gulf Monarchies: Stages and Features of Development

Gulnara N. Valiakhmetova [1]
orcid.org/0000-0001-7199-7723
Doctor of History, Head
of the Department of Oriental Studies,
corresponding author
vgulnara@mail.ru

Leonid V. Tsukanov [2]
orcid.org/0000-0001-6882-9841
PhD in Political,
Researcher
leon.tsukanov@mail.ru

[1] Ural Federal University
named after the First President of Russia
B. N. Yeltsin
(Yekaterinburg, Russia)

[2] PIR Center
(Center for Political Research)
(Moscow, Russia)

ОРИГИНАЛЬНЫЕ СТАТЬИ

Аннотация:

Рассматривается эволюция нормативно-правовых основ национальных систем кибербезопасности стран — участниц Совета сотрудничества арабских государств Персидского залива. Выявлен и проанализирован комплекс факторов, обусловивших динамику и особенности формирования правового поля монархий Залива в контексте их продвижения к безопасной цифровой среде. Предлагается периодизация истории развития правовой базы сектора кибербезопасности, представлена характеристика ее основных этапов. Особое внимание уделено анализу новых направлений модернизации профильного законодательства, включая области финансовых технологий и искусственного интеллекта. Представлены результаты сопоставительного анализа концепций правового регулирования цифрового пространства и его защиты в аравийских монархиях. Выявлены ключевые проблемы, препятствующие гармонизации правового поля в рамках Совета сотрудничества арабских государств Персидского залива. Авторы приходят к выводу о том, что форсированное развитие нормативно-правовой базы сектора кибербезопасности отвечает национальным интересам стран ССАГЗ и долгосрочным стратегиям развития «Видения». Обосновано, что все рассматриваемые страны наработали собственные уникальные правовые практики в области цифровой защиты, стремятся придерживаться высоких международных стандартов кибербезопасности и проактивного подхода к управлению рисками.

Ключевые слова:
кибербезопасность; правовое регулирование; аравийские монархии; Совет сотрудничества арабских государств Персидского залива.

ORIGINAL ARTICLES

Abstract:

This article examines the evolution of the legal and regulatory foundations of the national cybersecurity systems in the member states of the Gulf Cooperation Council (GCC). The authors identify and analyze a complex set of factors that have shaped the dynamics and distinctive features of the development of the legal framework in the Gulf monarchies within the context of their progress toward a secure digital environment. A periodization of the history of the cybersecurity sector's legal base is proposed, with a characterization of its main stages. Particular attention is paid to the analysis of new directions in the modernization of sector-specific legislation, including the fields of financial technology and artificial intelligence. The paper presents the results of a comparative analysis of the concepts for legal regulation and protection of the digital space in the Arabian monarchies. Key challenges hindering the harmonization of the legal framework within the GCC are identified. The authors conclude that the accelerated development of the cybersecurity legal and regulatory framework aligns with the national interests of the GCC states and their long-term development "Visions" (e.g., Saudi Vision 2030). It is substantiated that all the countries under consideration have developed their own unique legal practices in the realm of digital protection and strive to adhere to high international cybersecurity standards and a proactive approach to risk management.

Key words:
Cybersecurity; Legal Regulation; Arabian Monarchies; Gulf Cooperation Council (GCC); Digital Governance.

OPEN ACCESS
[Научный диалог = Nauchnyi dialog = Nauchnyy dialog, 14(7), 2025]
[ISSN 2225-756X, eISSN 2227-1295]

УДК 94:[34:004.8](532+535+536.2+536.4+536.5+536.8)“1995/2025”
DOI: 10.24224/2227-1295-2025-14-8-421-441

Научная специальность ВАК
5.6.2. Всеобщая история
5.6.7. История международных
отношений и внешней политики

Нормативно-правовое обеспечение кибербезопасности в арабских монархиях Залива: этапы и особенности развития

© Валиахметова Г. Н., Цуканов Л. В., 2025

1. Введение = Introduction

По мере продвижения к цифровому обществу человечество сталкивается с беспрецедентным ростом числа новых угроз. Не стал исключением и Ближний Восток, где динамично меняющийся цифровой ландшафт «наслаивается» на многомерное, внутренне противоречивое цивилизационное полотно региона, усиливая его и без того исключительно высокий конфликтный потенциал. Монархии Персидского залива — Бахрейн, Катар, Королевство Саудовская Аравия (КСА), Кувейт, Объединенные Арабские Эмираты (ОАЭ), Оман, — претендующие на роль мировых и региональных флагманов цифровизации, принимают удар в числе первых. Впечатляющие результаты экономической диверсификации, высокая концентрация предприятий энергетического, финансового и инновационного секторов в совокупности с геополитической спецификой Ближнего Востока делают обозначенную группу стран привлекательной для киберпреступности и государств-оппонентов, использующих информационно-коммуникационные технологии (ИКТ) в качестве инструментов проведения внешней политики и борьбы за региональное влияние. Это подталкивает местные власти к форсированному строительству национальных систем кибербезопасности, включая модернизацию законодательства с опорой на передовой зарубежный опыт и собственные уникальные наработки.

Востребованность научного осмысления правовых практик современных государств в области киберзащиты обусловлена необходимостью гармонизации на международном уровне национальных подходов к реагированию на цифровой вызов для совместного противодействия киберугрозам. Цель данного исследования состоит в выявлении предпосылок, этапов и специфики формирования систем правового регулирования сектора кибербезопасности в аравийских монархиях, а также в определении круга

проблем, препятствующих созданию общего правового поля в границах их интеграционного объединения — Совета сотрудничества арабских государств Залива (ССАГЗ) в конце XX—XXI веков.

2. Материал, методы, обзор = Material, Methods, Review

Методологической матрицей исследования выступают принципы научной объективности и системности, что позволило сформировать целостную картину правового измерения системы обеспечения кибербезопасности в странах ССАГЗ, подчеркнув ее многогранность и противоречивость. Теоретической основой исследования стала концепция «сетевого общества» М. Кастельса [Castells, 2010], в соответствии с которой представляется возможным рассматривать монархии Залива в качестве как самостоятельного цифрового кластера с собственными трендами развития, так и интегральной части глобального информационного общества. Исследование выполнено в рамках исторического подхода с использованием проблемно-хронологического, историко-генетического и сравнительного методов, которые позволяют выявить совокупность факторов, обусловивших особенности и динамику процесса эволюции законодательных основ обеспечения кибербезопасности в группе рассматриваемых стран.

Правовое измерение международной и национальной кибербезопасности имеет многоаспектный характер, в связи с чем исследования по данной проблематике проводятся в рамках различных наук — юридических, политических, исторических, экономических, технических. Внимание политологов-международников, как правило, сосредоточено на проблемах формирования универсального правового режима, способного обеспечить безопасность цифрового пространства на глобальном и региональном уровнях [Полякова и др., 2023]. Общерегиональная специфика, оказывающая непосредственное влияние на выработку правовых подходов монархий Залива к киберзащите, широко представлена в трудах российских востоковедов [Кузнецов и др., 2023; Звягельская, 2020]. Роль сектора кибербезопасности и его высоких нормативно-правовых стандартов в продвижении стран ССАГЗ в авангард цифрового общества раскрывается в работах западных экспертов [Hassib et al., 2022; Lotto, 2022; Strauss, 2025].

Высокая степень дискуссионности в правоведческой научной среде характерна для проблем, связанных с нормативным определением базовых терминов «кибербезопасность», «киберпреступность» и смежных понятий [Баландин, 2023; Старкова, 2021; Яковлева, 2021]. Особенности понятийного аппарата и правовых практик государств ССАГЗ в области противодействия ИКТ-преступлениям стали предметом исследований в публикациях представителей научных сообществ России [Шестак и др., 2023;

Волеводз, 2024] и арабских стран [Abu-Taieh et al., 2018]. Экосистемы цифровых госуслуг и их правовое обеспечение в государствах Персидского залива исследуются в рамках case-study [Al-Khouri, 2012] и компаративистики [Ильин и др., 2024].

С развитием цифровой экономики в странах ССАГЗ исследовательский фокус стал смещаться на проблемы правового регулирования сферы финансовых технологий и цифровых активов [Albanki et al., 2024], в том числе в контексте их соответствия нормам шариата [Ali Sh. et al., 2024; Al-Khalifa, 2022]. Значительный научный интерес привлекает проблематика рисков активного внедрения в аравийских монархиях технологий искусственного интеллекта (ИИ) [Пашенцев, 2024; Choithani et al., 2024].

Несмотря на разнообразие направлений и тематики изучения законодательных основ национальных систем кибербезопасности монархий Залива, особенности эволюции профильного нормативно-правового поля, в немалой степени обусловившие феноменальный успех стран ССАГЗ в области создания безопасной цифровой среды, пока не стали предметом отдельного исследования. Данная статья в определенной мере позволяет восполнить указанный пробел. Дополнительный элемент новизны результатов предлагаемой работы, кроме того, обеспечивает ее источниковая база, которую формируют законы, общенациональные и отраслевые нормативные акты и регламенты, регулирующие деятельность госучреждений, деловых кругов, научно-образовательных и общественных организаций, частных лиц в цифровом пространстве монархий Залива; декларации, принятые по итогам саммитов ССАГЗ; отчеты специализированных структур ООН (Международного союза электросвязи, Конференции по торговле и развитию, Всемирной организации интеллектуальной собственности), межправительственной Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ) и международной профессиональной платформы «Общество Интернета», затрагивающие различные аспекты правового обеспечения цифровой защиты арабских государств; материалы периодической печати.

3. Результаты и обсуждение = Results and Discussion

3.1. Этапы формирования нормативно-правовой базы сектора кибербезопасности

Процесс эволюции правовых систем монархий Залива в сфере кибербезопасности представляется возможным условно разделить на три этапа. Первый охватывает конец 1990-х — 2006 годы, когда закладывались основы правого регулирования цифрового пространства и его защиты путем принятия законов и иных нормативных актов по отдельным секторам эко-

номики (связь, банковское дело, электронная торговля и т. д.). К адаптации национального правового поля под новые цифровые реалии первыми приступили Оман и Саудовская Аравия. В КСА, например, уже в 1999 году был разработан «Порядок деятельности интернет-провайдеров», за которым последовали законы о телекоммуникациях (2001 год), о нормах использования Интернета и спутниковой связи (2002 год), о предоставлении услуг мобильной связи (2006 год) и т. д. [Saudi Arabia Service Regulations]. Законы о телекоммуникациях (приняты в Омане и Бахрейне в 2002 году, ОАЭ в 2003 году, Катаре в 2006 году, Кувейте в 2014 году) регламентировали порядок предоставления услуг связи, устанавливали права и обязанности поставщиков и пользователей, предусматривали меры пресечения за незаконное использование ИКТ-оборудования. Законы об электронных транзакциях (тут «первопроходцем» был Бахрейн в 2002 году [Legislative Decree № 28], за ним последовали ОАЭ в 2006 году, КСА в 2007 году, Оман в 2008 году, Катар в 2010 году, Кувейт в 2015 году) заложили основы безопасности электронных платежей и конфиденциальности ряда групп цифровых данных (электронные записи, документы и подписи, относящиеся к гражданско-правовой, коммерческой и административной деятельности). В рамках реализации новых законов создавались первые профильные государственные институты, на которые в том числе возлагались задачи по развитию нормативной базы секторов ИКТ и цифровой защиты.

Второй этап — с 2007 по 2015 годы — характеризуется акцентом на социально-политические аспекты кибербезопасности и попытками адаптации международных практик к местным реалиям. Импульсом к активизации нормотворческой деятельности послужил комплекс факторов: взрывной рост численности интернет-пользователей, стремительное внедрение ИКТ в различные сферы жизни аравийских обществ, разработка первых стратегических инициатив по диверсификации экономик (Оман 2003 года, Катар и Бахрейн 2008 года, ОАЭ 2010 года) и проектов электронного правительства, а также всплеск правонарушений в ИКТ-пространстве.

Подготовка законов о борьбе с киберпреступностью выявила серьезные разногласия в нормотворческих подходах государств Залива и их концептуальные отличия от зарубежных практик. Прежде всего речь идет о разнообразии понятийного аппарата, выработанного местными законодателями на арабском и английском языках, а также с учетом особенностей исламской правовой мысли [Шестак и др., 2023]. Первый такой закон был принят в ОАЭ в 2006 году, на его основе в 2012 году был разработан базовый федеральный закон «О борьбе с киберпреступностью», в который регулярно вносились изменения (2016 год, 2018 год, 2021 год) в плане расширения спектра преступлений, усиления правовых мер против ИКТ-угроз,

ужесточения наказаний для нарушителей. Обновленный в 2021 году закон (введен в действие в 2022 году) относит к преступным действиям несанкционированный доступ к сайтам, финансовые киберпреступления, нарушение неприкосновенности частной жизни, порочный контент, наносящий вред общественной морали и религиозным символам, а также действия, представляющие угрозу национальной безопасности: терроризм, призывы к протестам, пропаганда ненависти и расизма, подрыв национального единства и репутации государства, его институтов или руководителей [New UAE Cybercrime Law].

Саудовский закон 2007 года определяет пять видов преступлений с использованием ИКТ-средств: шпионаж, несанкционированный доступ, дефейсмент сайтов, вторжение в частную жизнь, клевета и причинение вреда другим лицам [Anti-Cyber Crime Law]. Оманский закон 2011 года был первым на Ближнем Востоке правовым актом, наиболее близким к международным стандартам, поскольку разрабатывался с опорой на европейские практики. Закон определял киберпреступность с точки зрения объекта и средств правонарушений, поэтому вводил в правовой оборот два смежных понятия: «киберпреступление» и «преступление, совершенное с использованием информационных технологий» [Oman Cybercrime Legislation]. В Бахрейне закон 2014 года выделяет три группы правонарушений: против ИКТ-систем, преступления с использованием ИКТ-средств и преступный контент [Law on Combating Cybercrime]. Катарский закон 2014 года криминализирует распространение вредоносного программного обеспечения, несанкционированный доступ, кражу личных данных, мошенничество в Интернете и т. п. [Cybercrime Prevention Law]. Главным стимулом к разработке соответствующего закона в Кувейте стали события Арабской весны: массовые протесты в стране вызвали политический кризис, отставку правительства и роспуск парламента в 2011 году. В связи с этим закон 2015 года преимущественно фокусируется на социально-политических аспектах правонарушений в цифровом пространстве, расширяя уже имеющиеся запреты в отношении СМИ и печатных публикаций практически на любую интернет-информацию, включая онлайн-журналистику, социальные сети и блоги [Law № 63 of 2015].

Несмотря на расхождения в трактовках понятия «киберпреступность», во всех монархиях Залива в него включены любые формы инакомыслия (критика властей, призывы к массовым протестам, координация антиправительственных акций с использованием ИКТ и т. п.), а также кибертерроризм (в том числе вербовочная и пропагандистская деятельность, финансовая и иная поддержка террористических группировок, оправдание терроризма). При этом у каждой страны имеется собственный подход

к пониманию сущности терроризма и кибертерроризма и, соответственно, собственный список запрещенных террористических группировок. Кроме того, хотя процесс совершенствования правовых практик и процедур в области противодействия киберпреступности идет довольно активно [Волеводз и др., 2024], законодательства стран — участниц ССАГЗ еще далеки от гармонизации и требуют доработки на национальном уровне ввиду расширения спектра киберугроз, а также с учетом международных актов, в частности Конвенции по киберпреступности, принятой Генеральной Ассамблеей ООН в декабре 2024 года.

Курс на модернизацию, цифровизацию, развитие несырьевых отраслей и привлечение иностранных инвестиций стимулировали внедрение ИКТ в государственное управление. Первые проекты начали тестироваться в КСА с 2003 года и ОАЭ с 2005 года [Al-Khouri A., 2012], а системная разработка цифровых государственных сервисов и методов их защиты стартовала в регионе в начале 2010-х годов [Ильин и др., 2024, с. 32—33]. Новатором стал Оман: корпус нормативных документов 2010 года [Overview of Oman eGovernance] содержал набор стандартов, передовых методов и процедур, обеспечивающих устойчивость государственных ИКТ-систем, улучшение качества госуслуг и минимизацию рисков в соответствии со стратегией «Цифрового Омана» 2003 года.

Начало третьему этапу — с 2016 года по настоящее время — было положено запуском во всех монархиях Залива стратегических программ «Видение», ускоривших цифровизацию и развитие онлайн-услуг. Важным стимулом к заполнению законодательных лакун стала пандемия covid-19 и переход к удаленным формам деятельности. Во всех странах ССАГЗ были приняты стандарты обеспечения кибербезопасности для государственных органов и бизнес-структур, а также законы и регламенты о защите персональных данных и уведомлении о нарушениях, о новых медиа (Интернет-СМИ, блоги, соцсети и т. п.), об антиобщественном поведении в Интернете и т. д. Появились новые направления нормотворчества — в области цифровых валют, финансовых технологий, искусственного интеллекта. Государства начали активно перенимать передовой зарубежный опыт в области правового регулирования цифровой защиты.

В свете развития государственных информационных сервисов и повышения глобальной конкурентоспособности экономик монархий Залива серьезным нормотворческим прорывом стали законы о защите персональных данных. Первый подобный акт был принят Катаром в 2016 году: он устанавливал строгие правила сбора, обработки и хранения данных, а также подкреплялся стандартами и регламентами применения конкретных средств контроля и уведомлений о нарушениях [National Information Assur-

ance Standard]. Хорошо продуманные и детально структурированные правовые рамки защиты данных на основе профильных законов и регламентов имеются также в Омане (соответствующий закон принят в 2017 году), Бахрейне (2018 год), ОАЭ и КСА (2021 год). В Кувейте обозначенная сфера регулируется отдельными положениями законов об электронной коммерции 2014 года и киберпреступности 2015 года, а также «Регламентом о защите данных и конфиденциальности» 2024 года [Data Protection]. Особенность последнего документа состоит в том, что он не распространяется на физических лиц и органы безопасности, которые собирают и обрабатывают персональные, в том числе семейные данные в целях борьбы с преступностью и предотвращения угроз общественной безопасности.

Монархии Залива, стремясь повысить устойчивость к цифровым угрозам, вводят общенациональные требования безопасности, обязательные к исполнению госучреждениями, частными компаниями, научно-образовательными и общественными структурами. В Омане данный блок нормативных актов сформировался в 2017—2019 годы, в КСА в 2018—2024 годах, в Бахрейне в 2022 году. Признанным лидером региона на этом направлении считаются ОАЭ: регламенты 2014—2025 годов [UAE Information Assurance Regulation] базируются на передовых международных практиках и создают эшелонированную многоступенчатую защиту от физического до прикладного уровней. Активно развивается правовое поле для отдельных отраслей, в первую очередь относящихся к критически значимым. В Катаре разработан закон о защите критической информационной инфраструктуры [Critical Information Infrastructure Law]. Специальные нормативы для правительственных сервисов, ИКТ, финансов, транспорта, здравоохранения, энергетики имеются в Бахрейне [Critical National Infrastructure] и ОАЭ [Critical Information Infrastructure Policy; Abu Dhabi — Healthcare].

В целом, высокая динамика развития сферы правого регулирования кибersектора свидетельствует о том, что для местных властей данное направление стало критически важным приоритетом в реализации национальных стратегических программ развития.

3.2. Новые направления модернизации профильного законодательства

Внедрение цифровых валют и рост рынка финансовых технологий сформировали новое направление модернизации законодательной базы в области цифровизации и киберзащиты, выявив существенные концептуальные расхождения между государствами Залива. Наиболее масштабные подвижки имели место в ОАЭ и Омане, взявших курс на лидерство на криптовалютном рынке Ближнего Востока [Emirates Blockchain Strategy; Cyber Security], а также в Бахрейне, который демонстрирует систем-

ный подход в развитии финтеха и его правовой базы [Albanki et al, 2024, с. 340—342; Bahrain Fintech…, 2022].

В Саудовской Аравии правовые рамки кибербезопасности для финансового сектора внедрены в 2017—2022 годах и продолжают довольно динамично развиваться [Fintech Laws]. Однако в отношении некоторых видов финтеха власти занимают осторожную позицию. К примеру, криптовалюты не признаются законным платежным средством, поэтому криптобиржи и криптовалютные транзакции официально не разрешены (в том числе со ссылкой на их несоответствие нормам исламского банкинга [Al-Khalifa, 2022]), но и не запрещены. При этом с 2022 года страна входит в тройку лидеров арабского мира по объемам цифровых активов [Saudis Come Third among Arab…, 2022]; правительство поддерживает финтех-стартапы, а в развитии профильного сегмента участвуют ведущие игроки мирового рынка, прежде всего в лице «Binance». Схожая ситуация наблюдается в Катаре, где майнинг криптовалют подпадает под закон о противодействии отмыванию денег и финансированию терроризма и классифицируется как преступление [Qatar Cryptocurrency Laws]. Впрочем, как отмечают аналитики ФАТФ, Катар ограничивается преимущественно декларативными мерами: правоохранительные органы не проводят активных мероприятий по выявлению майнеров, а акции по блокировке аккаунтов носят нерегулярный характер [Qatar's Measures…, 2023].

Наиболее жесткую позицию занимает Кувейт. Отсутствие правового регулирования деятельности имевшихся в стране криптобирж сделало Кувейт уязвимым перед лицом угроз со стороны майнеров, работающих в интересах преступных сообществ и недобросовестных предпринимателей. Ввиду стремительного роста «серого» сегмента крипторынка, а также в рамках кампании ФАТФ по борьбе с финансированием терроризма и отмыванием денег в 2023 году правительство наложило «абсолютный запрет на использование виртуальных активов в качестве платежного инструмента / средства» [Ministerial Circular № 1], который, однако, не коснулся цифровых валют, выпускаемых каким-либо правительством.

Очевидно, что среди аравийских монархий отсутствует единство в вопросах легитимности финтеха, направлений и масштабов его развития, ввиду чего профильное законодательство варьируется от страны к стране. Хотя первичная нормативно-правовая база во всех государствах уже сформирована, только три страны — ОАЭ, Бахрейн и Оман — на системной основе разрабатывают регламенты контроля за транзакциями токенов и оборотом криптовалют, порядок лицензирования и функционирования криптобирж и центров майнинга, использования ИИ-инструментов и т. п. [Choithani T. et al, 2024]. При этом оборот и майнинг криптовалют

санкционирован только в ОАЭ, в двух государствах — Кувейте и Катаре — эта деятельность относится к уголовно наказуемым. С 2019 года монархии Залива предпринимают шаги по преодолению имеющихся разногласий в целях развития единого рынка на пространстве ССАГЗ, однако до выработки единой позиции еще довольно далеко [Ali et al., 2024].

Схожий концептуальный разрыв наблюдается и в области технологий искусственного интеллекта и их использования в киберзащите. Системные усилия на данном направлении предпринимают пока только ОАЭ и Саудовская Аравия, которые первыми в мире сформировали специализированные госструктуры (Министерство ИИ ОАЭ в 2017 году, Управление по данным и искусственному интеллекту КСА в 2019 году), а в 2021 году опубликовали стратегии продвижения к глобальному первенству в обозначенной сфере, которые в том числе предусматривают модернизацию профильного законодательства [The National Strategy for Data & AI; UAE National Strategy]. В апреле 2025 года власти ОАЭ анонсировали план внедрения ИИ в поле правового регулирования. Он предусматривает создание единой базы данных федеральных и местных законов, судебных решений, госуслуг и т. п., на основе которой ИИ будет писать новые законы, пересматривать и вносить поправки в действующие нормативные акты [UAE Set to Use AI…, 2025]. Однако эксперты предупреждают о подводных камнях: ИИ становится непостижимым для своих пользователей, данные его обучения могут быть предвзятыми, а интерпретация законов может оказаться непригодной для человеческого общества [Пашенцев и др., 2024]. Сомнения в надежности и этичности технологий ИИ имеются и в других монархиях Залива. Кроме того, нормотворческий процесс в области ИИ, как и в случае с финтехом, сдерживается факторами экономического, технологического, социально-политического и религиозного характера.

3.3. Проблемы гармонизации правового поля в рамках ССАГЗ

Согласно Глобальному индексу кибербезопасности ООН, с 2020 года большинство стран ССАГЗ (Бахрейн, Катар, КСА, ОАЭ) удерживают максимальные показатели по нормативно-правовому критерию [GCI, 2021, с. 77—82; GCI, 2024, с. 70—80]. Незначительно снизил свои позиции в рейтинге 2024 года Оман, который в 2014—2020 годах уверенно лидировал в арабском регионе, а его правовые практики входили в число лучших в мире [GCI, 2017, с. 30—31, 39; Internet Infrastructure, 2020, с. 11]. Одна из причин заключается в том, что в вопросах цифровой трансформации и развития киберсектора Оман, стартовавший значительно раньше своих соседей по Заливу, всегда придерживался размеренного темпа [Lotto, 2024], тогда как другим монархиям (за исключением Кувейта) пришлось перейти на «спринтерский бег», чтобы догнать, а затем и перегнать лидера. В Ку-

вейте полноценный нормотворческий процесс в области киберзащиты был запущен лишь в 2014 году, почти на полтора десятилетия позже региональных партнеров. Тем не менее в последние годы страна активно адаптирует свое законодательство под цифровой вызов, сокращая правовой разрыв с участниками ССАГЗ.

Несмотря на высокие нормативно-правовые стандарты, все монархии Залива сталкиваются с общими проблемами, которые сдерживают темпы продвижения к безопасной цифровой среде как в пределах национальных границ, так и на уровне ССАГЗ. Прежде всего, следует отметить общую инертность законодательной сферы. В условиях стремительной цифровизации и с учетом динамической природы киберугроз правовое поле объективно не успевает своевременно реагировать на новые вызовы, что ведет к появлению законодательных пробелов и усложняет регулирование не только в монархиях Залива, но и в странах, считающихся «абсолютными лидерами» цифрового мира (США, КНР и др.) [Полякова и др., 2023, с. 144]. Однако в странах ССАГЗ ситуация усугубляется «нисходящей» моделью управления, ограничивающей горизонтальные связи и обмен опытом между различными субъектами кибербезопасности, а также высоким уровнем бюрократизации управленческих процессов, замедляющих внедрение инноваций [Internet Infrastructure, 2020, с. 11]. Кроме того, учреждениям зачастую трудно ориентироваться в многочисленных сложных и зачастую противоречивых правилах и нормативах кибербезопасности, а ввод новых регламентов требует значительного времени и ресурсов (финансовых, технических, кадровых), которыми располагают далеко не все государственные и частные структуры [Strauss, 2025].

Концепции стран — членов ССАГЗ в области регулирования ИКТ-пространства и его защиты весьма разнятся, препятствуя гармонизации правового поля. Позиции государств далеко не всегда совпадают даже в вопросах трактовки содержания базовых понятий и терминов (киберпреступность, кибертерроризм и т. д.). Кроме того, до начала 2020-х годов все страны (кроме Омана) придерживались преимущественно реактивного, а не проактивного подхода к развитию киберсектора. Это выражалось в склонности к купированию последствий кибератак и иных нарушений в работе ИКТ-инфраструктуры вместо поэтапной разработки комплексного ответа, предполагающего принятие мер на опережение. Стимулом к активизации нормотворческой деятельности, как правило, выступали крупные кибернападения на объекты критической инфраструктуры, глобальные кризисы (пандемия covid-19) либо инициативы внешних акторов в лице ООН, США и др. И если на национальном уровне эта проблема практически уже решена, но в формате ССАГЗ упреждающий подход пока

не стал доминирующим. Это объясняется чувствительным и конфиденциальным характером киберсферы, а также сохраняющейся атмосферой недоверия, характерной для всего Ближнего Востока с его чрезвычайно высоким конфликтным потенциалом [Кузнецов, 2023; Звягельская, 2020].

Серьезным препятствием к формированию единых законодательных рамок в области кибербезопасности на пространстве ССАГЗ является и то, что все участники этого объединения (кроме Омана) долгое время дистанцировались от мирового нормотворческого процесса, а инициативы ООН и других международных профильных экспертных платформ, с которыми сегодня тесно сотрудничают монархии Залива, далеко не всегда становились руководством к действию. К примеру, рекомендации ООН 2013 года [Development and Harmonization..., 2013] в большинстве своем до начала 2020-х годов оставались без внимания [Internet infrastructure, 2020, с. 16—18]. Кроме того, до недавнего времени страны ССАГЗ увязывали согласование своих политик в вопросах цифровой защиты, включая гармонизацию профильных законодательств, с выработкой общих подходов в рамках всего арабского мира [Hassib et al., 2022; GCC Supreme Council…, 2022], а этот процесс неизменно тормозился ввиду многочисленных доктринальных, нормотворческих и иных разногласий между арабскими государствами. На саммите ССАГЗ в декабре 2024 года [Kuwait Declaration…2024] был взят курс на расширение сотрудничества между участниками объединения путем разработки совместных цифровых стратегий и платформ, а также укрепления кибербезопасности с целью превращения региона в глобальный центр цифровой экономики.

4. Заключение = Conclusions

Нормативно-правовая база в области кибербезопасности, сформированная монархиями Залива в последние десятилетия, отвечает национальным долгосрочным стратегиям развития и способствует созданию безопасной цифровой среды. Хотя каждое государство наработало собственный подход и правовые практики обеспечения киберзащиты, между ними имеются общие черты. Все страны демонстрируют приверженность высоким международным стандартам кибербезопасности, о чем свидетельствуют строгие законы и регламенты (прежде всего в сфере защиты критической ИКТ-инфраструктуры) и жесткий правительственный контроль за их исполнением. Общенациональные и отраслевые законодательства и нормативные акты базируются на триаде кибербезопасности (конфиденциальность, целостность, доступность данных), а также непрерывной атрибуции, оценке и смягчении киберугроз, поскольку кибербезопасность — это постоянный потоковый процесс. Во всех монархиях в той или иной сте-

пени практикуется активное управление рисками и продвигается проактивный подход к организации цифровой защиты, когда речь идет не только о создании оградительных механизмов и надежде на лучшее, но и об активном поиске уязвимых звеньев, понимании меняющегося ландшафта угроз и принятии превентивных продуманных мер.

Вместе с тем 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 и — в первую очередь — преодолеть взаимное недоверие и концептуальные разногласия.

Заявленный вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации.	**Contribution of the authors:** the authors contributed equally to this article.
Авторы заявляют об отсутствии конфликта интересов.	**The authors declare no conflicts of interests.**

Источники и принятые сокращения

1. *Abu Dhabi — Healthcare* Information and Cyber Security Standard [Electronic resource]. — Access mode : https://www.doh.gov.ae›media›Aamen›ADHICS (accessed 7.04.2025).

2. *Anti-Cyber Crime Law* 2007 // WIPO UN [Electronic resource]. — Access mode : https://www.wipo.int/wipolex/en/legislation/details/14570 (accessed 12.03.2025).

3. *Bahrain FinTech* Ecosystem Report 2022 [Electronic resource]. — Access mode : https://theblockchaintest.com/uploads/resources/Bahrain%20FinTech%20bay%20-%20FinTech%20Ecosystem%20Report%20-%202022%20Feb.pdf (accessed 19.04.2025).

4. *Critical Information Infrastructure* Protection Law [Electronic resource]. — Access mode : https://qcert.ncsa.gov.qa/services/critical-information-infrastructure-protection-interdependency-database (accessed 7.04.2025).

5. *Critical Information Infrastructur*e Protection Policy [Electronic resource]. — Access mode : https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security/uae-information-assurance-regulation (accessed 7.04.2025).

6. *Critical National Infrastructure* Cybersecurity Controls [Electronic resource]. — Access mode : https://www.ncsc.gov.bh/en/policies-controls/CNI-cybersecurity-controls.html (accessed 7.04.2025).

7. *Cyber Security* and Resilience Framework // Central Bank of Oman [Electronic resource]. — Access mode : https://cbo.gov.om/sites/assets/FintechCompulsoryDocs/Cyber%20Security%20&%20Resilience%20Framework%20(CS&RF).pdf (accessed 19.04.2025).

8. *Cybercrime Prevention Law* 2014 [Electronic resource]. — Access mode : https://www.cra.gov.qa/en/document/cybercrime-prevention-law-no-14-of-2014 (accessed 12.03.2025).

9. *Data Protection* & Privacy 2025 [Electronic resource]. — Access mode : https://practiceguides.chambers.com/practice-guides/comparison/932/15607/24360-24367-24371-24376-24381 (accessed 7.04.2025).

10. *Development* and Harmonization of Cyber Legislation in the Arab Region. — New York : UNCTAD, 2013. — 21 p.

11. *Emirates Blockchain Strategy* 2021 [Electronic resource]. — Access mode : https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/federal-governments-strategies-and-plans/emirates-blockchain-strategy-2021 (accessed 19.04.2025).

12. *Fintech Laws* and Regulations Saudi Arabia 2024—2025 [Electronic resource]. — Access mode : https://iclg.com/practice-areas/fintech-laws-and-regulations/saudi-arabia (accessed 21.04.2025).

13. *GCC Supreme Council* Release Final Communique after 43rd Summit [Electronic resource] // Saudi Gazette. — 09.12.2022. — Access mode : https://saudigazette.com.sa/article/627828 (accessed 11.04.2025).

14. GCI — *Global* Cybersecurity Index 2017. — Geneva : ITU UN, 2017. — 166 p.

15. GCI — *Global* Cybersecurity Index 2020. — Geneva : ITU UN, 2021. — 156 p.

16. GCI — *Global* Cybersecurity Index 2024. — Geneva : ITU UN, 2024. — 142 p.

17. *Internet Infrastructure* Security Guidelines for the Arab States. — Washington DC : Internet society, 2020. — 26 p.

18. *Kuwait Declaration* Issued at GCC Supreme Council's 45th Session [Electronic resource] // Bahrain News Agency. 1.12.2024. — Access mode : https://www.bna.bh/en/KuwaitDeclarationissuedatGCCSupremeCouncils45thsession.aspx?cms (accessed 11.04.2025).

19. *Law № 63 of 2015* on Combating Information Technology Crimes [Electronic resource]. — Access mode : https://www.moi.gov.kw/main/content/docs/cybercrime/ar/law-establishing-cyber-crime-dept.pdf (accessed 12.03.2025).

20. *Law on Combating Cybercrime* in the Kingdom of Bahrain [Electronic resource]. — Access mode : https://www.asianlaws.org/gcld/cyberlawdb/GCC/Law%20on%20Combating%20Cybercrime%20in%20the%20Kingdom%20of%20Bahrain.pdf (accessed 12.03.2025).

21. *Legislative Decree № 28* (2002) with Respect to Electronic Transactions [Electronic resource]. — Access mode : https://www.bahrain.bh/wps/wcm/connect/1ede6815-4dc0-451c-aa7d-09c3622f0494/CASPMFGX.pdf?MOD=AJPERES (accessed 25.03.2025).

22. *Ministerial Circular* № 1 of the Year 2023 Regarding the Procedures Required Concerning Transactions Related to Virtual Assets [Electronic resource]. — Access mode : https://moci.gov.kw/en/news/194/ (accessed 23.04.2025).

23. *National Information* Assurance Standard [Electronic resource]. — Access mode : https://assurance.ncsa.gov.qa/sites/default/files/publications/policy/2023/NCSA_CSGA_%20 (accessed 15.03.2025).

24. *New UAE Cybercrime Law* : Detailed Insights into Crimes and Penalties [Electronic resource]. — Access mode : https://davidsoncolaw.com/how-to-report-cyber-crime-in-uae/#:~:text=Article (accessed 12.03.2025).

25. *Oman Cybercrime Legislation* [Electronic resource]. — Access mode : https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/id/64859909/pop_up (accessed 12.03.2025).

26. *Overview of Oman eGovernance* Framework [Electronic resource]. — Access mode : https://www.ita.gov.om/ITAPortal/Pages/Page.aspx?NID=559&PID=1848&LID=96 (accessed 15.03.2025).

27. *Qatar Cryptocurrency Laws* [Electronic resource]. — Access mode : https://freemanlaw.com/cryptocurrency/qatar/ (accessed 23.04.2025).

28. *Qatar's Measures* to Combat Money Laundering and Terrorist Financing [Electronic resource] // FATF, 2023. — Access mode : https://www.fatf-gafi.org/en/publications/Mutualevaluations/MER-Qatar-2023.html (accessed 23.04.2025).

29. *Saudi Arabia* Service Regulations [Electronic resource]. — Access mode : https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/ (accessed 25.03.2025).

30. *Saudis Come Third among Arab* Cryptocurrency Owners [Electronic resource] // Saudi Gazette. — 12.01.2022. — Access mode : https://saudigazette.com.sa/article/615778 (accessed 21.04.2025).

31. *The National Strategy for Data & AI* for Saudi Arabia [Electronic resource]. — Access mode : https://sdaia.gov.sa/en/SDAIA/SdaiaStrategies/Pages/NationalStrategyForDataAndAI.aspx (accessed 25.04.2025).

32. *UAE Information Assurance* Regulation [Electronic resource]. — Access mode : https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security/uae-information-assurance-regulation (accessed 7.04.2025).

33. *UAE National Strategy* for Artificial Intelligence 2031 [Electronic resource]. — Access mode : https://ai.gov.ae/strategy/ (accessed 25.04.2025).

34. *UAE Set to Use AI* to Write Laws in World First [Electronic resource] // Financial Times. 21.04.2025. — Access mode : https://www.ft.com/content/9019cd51-2b55-4175-81a6-eafcf28609c3 (accessed 24.04.2025).

Литература

1. *Баландин А. Ю.* Кибербезопасность и информационная безопасность. Демаркация правовых категорий / А. Ю. Баландин // Правовая политика и правовая жизнь. — 2023. — № 3. — С. 260—270. — DOI: https://doi.org/10.52468/2542-1514.2025.9(3).114-123.

2. *Волеводз А. Г.* Цифровые доказательства в уголовном процессе государств — членов ССАГЗ : правовой статус и процедуры признания / А. Г. Волеводз, А. Д. Цыплакова // Вестник экономической безопасности. — 2024. — № 2. — С. 21—29. — DOI: 10.24412/2414-3995-2024-2-21-29.

3. *Ильин А. П.* Развитие государственных информационных систем в РФ, ИРИ и КСА / А. П. Ильин, Ю. И. Ильина // Гуманитарные науки. Вестник Финансового университета. — 2024. — № 14 (4). — С. 32—33. — DOI: 10.26794/2226-7867-2024-14-4-23-38.

4. *Звягельская И. Д.* Ближний Восток в условиях «негативной определенности» / И. Д. Звягельская, И. А. Свистунова, Н. Ю. Сурков // Мировая экономика и международные отношения. — 2020. — № 6. — С. 94—103. — DOI: 10.20542/0131-2227-2020-64-6-94-103.

5. *Кузнецов В. А.* Глобальные и региональные тренды «столетия+» на Ближнем Востоке : новое прочтение / В. А. Кузнецов, В. В. Наумкин // Вестник Московского университета. Серия XXV. Международные отношения и мировая политика. — 2023. — № 1. — С. 70—92. — DOI: 10.48015/2076-7404-2023-15-1-70-92.

6. *Пашенцев Е. Н.* Злонамеренное использование искусственного интеллекта и угрозы информационно-психологической безопасности в ОАЭ / Е. Н. Пашенцев, В. А. Чебыкина // Восток. Афро-азиатские общества: история и современность. — 2024. — № 6. — С. 107—117. — DOI: 10.31696/S086919080032578-2.

7. *Полякова Т. А.* Международная информационная безопасность : универсальное правовое измерение / Т. А. Полякова, Е. С. Зиновьева, А. А. Смирнов // Государство и право. — 2023. — № 12. — С. 139—149.

8. *Старкова Л. М.* Подходы к пониманию и нормативному определению категории «киберпреступность» и смежных понятий в практике региональных международных

организаций / Л. М. Старкова // Московский журнал международного права. — 2021. — № 4. — С. 123—135. DOI: https://doi.org/10.24833/0869-0049-2021-4-123-135.

9. *Шестак В. А.* Понятие и сущность киберпреступлений в государствах-членах ССАГПЗ / В. А. Шестак, А. Д. Цыплакова // Мировой судья. — 2023. — № 4. — С. 2—7. — DOI: 10.18572/2072-4152-2023-4-2-7.

10. *Яковлева А. В.* Кибербезопасность и ее правовое регулирование (зарубежный и российский опыт) / А. В. Яковлева // Социально-политические науки. — 2021. — № 4. — С. 70—81. — DOI: 10.33693/2223-0092-2021-11-4-70-81.

11. *Abu-Taieh E.* Cyber Security Crime and Punishment : Comparative Study of the Laws of Jordan, Kuwait, Qatar, Oman, and Saudi Arabia / E. Abu-Taieh, A. Alfaries, Sh. Al-Otaibi, Gh. Aldehim // International Journal of Cyber Warfare and Terrorism. — 2018. — № 3. — Pp. 46—59. — DOI: 10.4018/IJCWT.2018070104.

12. *Albanki A. A.* Unravelling the Legal Framework for Cryptocurrency : A Comparative Analysis of Regulatory Approaches / A. A. Albanki, N. K. Alshawawreh, M. M. Abdeldayem, S. H. Aldulaim // 2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS). — IEEE Proceeding, 2024. — Pp. 338—343. — DOI: 10.1109/ICETSIS61505.2024.10459412.

13. *Ali Sh.* The Resilience of Shariah-Compliant Investments : Probing the Static and Dynamic Connectedness between Gold-Backed Cryptocurrencies and GCC Equity Markets / Sh. Ali, M. Naveed, H. Hanif, M. Gubareva // International Review of Financial Analysis. — 2024. — Vol. 91. — Pp. 1—19. — DOI: 10.1016/j.irfa.2023.103045.

14. *Al-Khalifa Sh. Z.* CryptoHalal : An Intelligent Decision-System for Identifying Halal and Haram Cryptocurrencies / Sh. Z. Al-Khalifa // Social Science Research Network, November 2022. — Pp. 76—84. — DOI: 10.13140/RG.2.2.26117.22249.

15. *Al-Khouri A.* eGovernment Strategies : The Case of the UAE / A. Al-Khouri // European Journal of ePractice. — 2012. — № 17. — Pp. 126—150.

16. *Castells M.* The Rise of the Network Society / M. Castells. — Oxford : Blackwell Publishing Ltd, 2010. — 625 p. — ISBN 978-1-4051-9686-4.

17. *Choithani T.* A Comprehensive Study of Artificial Intelligence and Cybersecurity on Bitcoin, Crypto Currency and Banking System / T. Choithani, A. Chowdhury, Sh. Patel, P. Patel, D. Patel, M. Shah // Annals of Data Science. — 2024. — № 11 (1). — Pp. 103—135. — DOI: 10.1007/s40745-022-00433-5.

18. *Hassib B.* Cybersecurity in the GCC : From Economic Development to Geopolitical Controversy / B. Hassib, J. Shires // Middle East Policy. — 2022. — № 29 (1). — Pp. 90—103. — DOI: 10.1111/mepo.12616.

19. *Lotto B.* From Zero to One : Oman's Path to Creating a Globally Competitive Cyber Posture [Electronic resource] / B. Lotto // Muscat Daily. — 13.07.2024. — Access mode : https://www.muscatdaily.com/2024/07/13/omans-path-to-creating-a-globally-competitive-cyber-posture/ (accessed 7.04.2025).

20. *Strauss L.* Breaking Down National Cybersecurity Frameworks in the Middle East [Electronic resource] / L. Strauss // 6clicks. — 27.01.2025. — Access mode : https://www.6clicks.com/resources/blog/breaking-down-national-cybersecurity-frameworks-in-the-middle-east (accessed 7.04.2025).

Статья поступила в редакцию 25.05.2025,
одобрена после рецензирования 25.06.2025,
подготовлена к публикации 17.10.2025.

Material resources

Abu Dhabi — *Healthcare Information and Cyber Security Standard.* Available at: https://www.doh.gov.ae›media›Aamen›ADHICS (accessed 7.04.2025).

Anti-Cyber Crime Law 2007. *WIPO UN.* Available at: https://www.wipo.int/wipolex/en/legislation/details/14570 (accessed 12.03.2025).

Bahrain FinTech Ecosystem Report 2022. Available at: https://theblockchaintest.com/uploads/resources/Bahrain%20FinTech%20bay%20-%20FinTech%20Ecosystem%20Report%20-%202022%20Feb.pdf (accessed 19.04.2025).

Critical Information Infrastructure Protection Law. Available at: https://qcert.ncsa.gov.qa/services/critical-information-infrastructure-protection-interdependency-database (accessed 7.04.2025).

Critical Information Infrastructure Protection Policy. Available at: https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security/uae-information-assurance-regulation (accessed 7.04.2025).

Critical National Infrastructure Cybersecurity Controls. Available at: https://www.ncsc.gov.bh/en/policies-controls/CNI-cybersecurity-controls.html (accessed 7.04.2025).

Cyber Security and Resilience Framework. *Central Bank of Oman.* Available at: https://cbo.gov.om/sites/assets/FintechCompulsoryDocs/Cyber%20Security%20&%20Resilience%20Framework%20(CS&RF).pdf (accessed 19.04.2025).

Cybercrime Prevention Law 2014. Available at: https://www.cra.gov.qa/en/document/cybercrime-prevention-law-no-14-of-2014 (accessed 12.03.2025).

Data Protection & Privacy 2025. Available at: https://practiceguides.chambers.com/practice-guides/comparison/932/15607/24360-24367-24371-24376-24381 (accessed 7.04.2025).

Development and Harmonization of Cyber Legislation in the Arab Region. (2013). New York: UNCTAD. 21 p.

Emirates Blockchain Strategy 2021. Available at: https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/federal-governments-strategies-and-plans/emirates-blockchain-strategy-2021 (accessed 19.04.2025).

Fintech Laws and Regulations Saudi Arabia 2024—2025. Available at: https://iclg.com/practice-areas/fintech-laws-and-regulations/saudi-arabia (accessed 21.04.2025).

GCC Supreme Council Release Final Communique after 43rd Summit. (2022). *Saudi Gazette. 09.12.* Available at: https://saudigazette.com.sa/article/627828 (accessed 11.04.2025).

GCI — *Global Cybersecurity Index 2017.* (2017). Geneva: ITU UN. 166 p.

GCI — *Global Cybersecurity Index 2020.* (2021). Geneva: ITU UN. 156 p.

GCI — *Global Cybersecurity Index 2024.* (2024). Geneva: ITU UN. 142 p.

Internet Infrastructure Security Guidelines for the Arab States. (2020). Washington DC: Internet society. 26 p.

Kuwait Declaration Issued at GCC Supreme Council's 45th Session. (2024). *Bahrain News Agency. 1.12.* Available at: https://www.bna.bh/en/KuwaitDeclarationissuedatGCCSupremeCouncils45thsession.aspx?cms (accessed 11.04.2025).

Law № 63 of 2015 on Combating Information Technology Crimes. Available at: https://www.moi.gov.kw/main/content/docs/cybercrime/ar/law-establishing-cyber-crime-dept.pdf (accessed 12.03.2025).

Law on Combating Cybercrime in the Kingdom of Bahrain. Available at: https://www.asianlaws.org/gcld/cyberlawdb/GCC/Law%20on%20Combating%20Cybercrime%20in%20the%20Kingdom%20of%20Bahrain.pdf (accessed 12.03.2025).

Legislative Decree № 28 (2002) with Respect to Electronic Transactions. Available at: https://www.bahrain.bh/wps/wcm/connect/1ede6815-4dc0-451c-aa7d-09c3622f0494/CASPMFGX.pdf?MOD=AJPERES (accessed 25.03.2025).

Ministerial Circular № 1 of the Year 2023 Regarding the Procedures Required Concerning Transactions Related to Virtual Assets. Available at: https://moci.gov.kw/en/news/194/ (accessed 23.04.2025).

National Information Assurance Standard. Available at: https://assurance.ncsa.gov.qa/sites/default/files/publications/policy/2023/NCSA_CSGA_%20 (accessed 15.03.2025).

New UAE Cybercrime Law: Detailed Insights into Crimes and Penalties. Available at: https://davidsoncolaw.com/how-to-report-cyber-crime-in-uae/#:~:text=Article (accessed 12.03.2025).

Oman Cybercrime Legislation. Available at: https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/id/64859909/pop_up (accessed 12.03.2025).

Overview of Oman eGovernance Framework. Available at: https://www.ita.gov.om/ITAPortal/Pages/Page.aspx?NID=559&PID=1848&LID=96 (accessed 15.03.2025).

Qatar Cryptocurrency Laws. Available at: https://freemanlaw.com/cryptocurrency/qatar/ (accessed 23.04.2025).

Qatar's Measures to Combat Money Laundering and Terrorist Financing. (2023). *FATF.* Available at: https://www.fatf-gafi.org/en/publications/Mutualevaluations/MER-Qatar-2023.html (accessed 23.04.2025).

Saudi Arabia Service Regulations. Available at: https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/ (accessed 25.03.2025).

Saudis Come Third among Arab Cryptocurrency Owners. *Saudi Gazette. 12.01.* Available at: https://saudigazette.com.sa/article/615778 (accessed 21.04.2025).

The National Strategy for Data & AI for Saudi Arabia. Available at: https://sdaia.gov.sa/en/SDAIA/SdaiaStrategies/Pages/NationalStrategyForDataAndAI.aspx (accessed 25.04.2025).

UAE Information Assurance Regulation. Available at: https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security/uae-information-assurance-regulation (accessed 7.04.2025).

UAE National Strategy for Artificial Intelligence 2031. Available at: https://ai.gov.ae/strategy/ (accessed 25.04.2025).

UAE Set to Use AI to Write Laws in World First. (2025). *Financial Times. 21.04.* Available at: https://www.ft.com/content/9019cd51-2b55-4175-81a6-eafcf28609c3 (accessed 24.04.2025).

References

Abu-Taieh, E., Alfaries, A., Al-Otaibi, Sh., Aldehim, Gh. (2018). Cyber Security Crime and Punishment: Comparative Study of the Laws of Jordan, Kuwait, Qatar, Oman, and Saudi Arabia. *International Journal of Cyber Warfare and Terrorism, 3:* 46—59. DOI: 10.4018/IJCWT.2018070104.

Albanki, A. A., Alshawawreh, N. K., Abdeldayem, M. M. (2024). Unravelling the Legal Framework for Cryptocurrency: A Comparative Analysis of Regulatory Approaches. *2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS). IEEE Proceeding.* 338—343. DOI: 10.1109/ICETSIS61505.2024.10459412.

Ali, Sh., Naveed, M. (2024). 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, 91:* 1—19. DOI: 10.1016/j.irfa.2023.103045.

Al-Khalifa, Sh. Z. (2022). CryptoHalal: An Intelligent Decision-System for Identifying Halal and Haram Cryptocurrencies. *Social Science Research Network, November.* 76—84. DOI: 10.13140/RG.2.2.26117.22249.

Al-Khouri, A. (2012). eGovernment Strategies: The Case of the UAE. *European Journal of ePractice, 17:* 126—150.

Balandin, A. Y. (2023). Cybersecurity and information security. Demarcation of legal categories. *Legal policy and legal life, 3:* 260—270. DOI: https://doi.org/10.52468/2542-1514.2025.9 (3).114-123. (In Russ.).

Castells, M. (2010). *The Rise of the Network Society.* Oxford: Blackwell Publishing Ltd. 625 p. ISBN 978-1-4051-9686-4.

Choithani, T., Chowdhury, A., Patel, Sh. (2024). A Comprehensive Study of Artificial Intelligence and Cybersecurity on Bitcoin, Crypto Currency and Banking System. *Annals of Data Science, 11 (1):* 103—135. DOI: 10.1007/s40745-022-00433-5.

Hassib, B., Shires, J. (2022). Cybersecurity in the GCC: From Economic Development to Geopolitical Controversy. *Middle East Policy, 29 (1):* 90—103. DOI: 10.1111/mepo.12616.

Ilyin, A. P. (2024). Development of state information systems in the Russian Federation, Iran and KSA. Humanities. *Bulletin of the Financial University, 14 (4):* 32—33. DOI: 10.26794/2226-7867-2024-14-4-23-38. (In Russ.).

Kuznetsov, V. A. (2023). Global and regional trends of the "century+" in the Middle East: a new reading. *Bulletin of the Moscow University. XXV series. International relations and world politics, 1:* 70—92. DOI: 10.48015/2076-7404-2023-15-1-70-92. (In Russ.).

Lotto, B. (2024). From Zero to One: Oman's Path to Creating a Globally Competitive Cyber Posture. *Muscat Daily. 13.07.* Available at: https://www.muscatdaily.com/2024/07/13/omans-path-to-creating-a-globally-competitive-cyber-posture/ (accessed 7.04.2025).

Pashentsev, E. N. (2024). Malicious use of artificial intelligence and threats to information and psychological security in the UAE. *East. Afro-Asian societies: History and modernity, 6:* 107—117. DOI: 10.31696/S086919080032578-2. (In Russ.).

Polyakova, T. A., Zinovieva, E. S., Smirnov, A. A> (2023). International information security: a universal legal dimension. *State and Law, 12:* 139—149. (In Russ.).

Shestak, V. A., Tsyplakova, A. D. (2023). The concept and essence of cybercrime in the GCC member states. *Justice of the Peace, 4:* 2—7. DOI: 10.18572/2072-4152-2023-4-2-7. (In Russ.).

Starkova, L. M. (2021). Approaches to understanding and normative definition of the category "cybercrime" and related concepts in the practice of regional international organizations. *Moscow Journal of International Law, 4:* 123—135. DOI: https://doi.org/10.24833/0869-0049-2021-4-123-135. (In Russ.).

Strauss, L. (2025). Breaking Down National Cybersecurity Frameworks in the Middle East. *6clicks. 27.01.* Available at: https://www.6clicks.com/resources/blog/breaking-down-national-cybersecurity-frameworks-in-the-middle-east (accessed 7.04.2025).

Volevodz, A. G., Tsyplakova, A. D. (2024). Digital evidence in the criminal proceedings of the GCC member states: legal status and recognition procedures. *Bulletin of Economic Security, 2:* 21—29. DOI: 10.24412/2414-3995-2024-2-21-29. (In Russ.).

Yakovleva, A. V. (2021). Cybersecurity and its legal regulation (foreign and Russian experience). *Socio-political Sciences, 4:* 70—81. DOI: 10.33693/2223-0092-2021-11-4-70-81. (In Russ.).

Zvyagelskaya, I. D., Svistunova, I. A., Surkov, N. Y. (2020). The Middle East in conditions of "negative certainty". *World Economy and International Relations, 6:* 94—103. DOI: 10.20542/0131-2227-2020-64-6-94-103. (In Russ.).

The article was submitted 25.05.2025;
approved after reviewing 25.06.2025;
accepted for publication 17.10.2025.