Зарубежный опыт. Международное сотрудничество

ПОЛИТИКА КАТАРА В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Статья рекомендована к публикации членом редакционного совета А. А. Стрельцовым 26.06.2025.

Хайруллин Тимур Радикович

Кандидат политических наук, доцент
Институт Африки РАН, Центр цивилизационных и региональных исследований, старший научный сотрудник
Финансовый университет при Правительстве РФ, старший преподаватель
СПбГУ, старший научный сотрудник
Москва, Российская Федерация
jumglaw16@yandex.ru

Горностаев Яков Николаевич

Российский университет дружбы народов имени Патриса Лумумбы, факультет гуманитарных и социальных наук, студент
Москва, Российская Федерация
yakov.gornostayev@bk.ru

Ильин Егор Вадимович

Российский университет дружбы народов имени Патриса Лумумбы, факультет гуманитарных и социальных наук, студент
Москва, Российская Федерация
Egor-ilin-1111@mail.ru

Аннотация

В работе был проведен анализ законодательной базы Катара, выявивший, что основой регулирования политики кибербезопасности является Национальная стратегия кибербезопасности, а также Закон о борьбе с киберпреступлениями (2014), ставший дополнением к другими нормативными актами, таким как Закон о защите персональных данных (2016) и Закон об электронных транзакциях (2010). Выяснено, что стремление Катара достичь цифрового суверенитета привело к тому, что сегодня государство является одним из самых успешных в области обеспечения информационной безопасности. Этому способствовали наличие устойчивого экономического роста и благоприятный инвестиционный климат, а также продуманная налоговая политика.

Ключевые слова

информационная угроза; государственная политика; законодательная база; критическая информационная инфраструктура; цифровизация; защита данных; киберугроза; кибератака; конфиденциальность, национальная стратегия кибербезопасности

Введение

Район Персидского залива сегодня – один из наиболее динамично развивающихся мировых центров в целом ряде ключевых направлений. Выход на лидерские позиции во многом обеспечивается ведущими странами Залива – Саудовской Аравией, Ираном, ОАЭ и Катаром. Каждое из вышеперечисленных государств стремится к достижению региональной гегемонии, которая обеспечивается опорой на передовые технологии, без которых сегодня невозможен экономический успех. Однако если экономический и военно-политический успех таких региональных гигантов как Саудовская Аравия и

Производство и хостинг журнала «Информационное общество» осуществляется Институтом развития информационного общества.

https://doi.org/10.52605/16059921_2026_03_149

Иран может быть очевиден, то история успеха таких малых монархий Залива как ОАЭ и Катар вызывает интерес [1].

При этом, если успех ОАЭ во многом связан с активностью преимущественно двух эмиратов – коммерческого центра Дубай и военно-административного центра Абу-Даби [2], а также союзническими отношениями с Саудовской Аравией, то история успеха Катара, действующего с относительного недавнего времени вне стратегии монархий ССАГПЗ вызывает особый интерес. Благодаря стратегическому планированию внутреннего развития Катар сумел поднять на мировой уровень такие секторы, как туризм, логистика, *IT*-технологии, робототехника, авиасообщение с созданием крупнейших аэропортов и развитой инфраструктуры. Активное внедрение IT-технологий и элементов искусственного интеллекта (ИИ) требует принятия мер по обеспечению информационной безопасности [3], включающей в себя такие аспекты как политика и стандарты, программы повышения осведомленности и обучения, оценка рисков и анализ пробелов, и т.д. [4]. Основной целью данного исследования является изучение особенностей обеспечения информационной безопасности в Катаре.

1 Отношение Катара к проблеме кибербезопасности

По мере развития инновационных и информационных технологий, необходимость в обеспечении безопасности от киберугроз стала приобретать особую актуальность [5; 6]. В сегодняшних реалиях активного развития технологии искусственного интеллекта обеспечение информационной безопасности выходит на передний план как внутри отдельных государств, так и на межгосударственном уровне [7; 8].

Государство Катар стремительно развивается и трансформируется для достижения целей, поставленных в его национальной стратегии развития на период до 2030 г. Стратегия направлена на преобразование Катара из экономики, зависящей от нефти, в экономику, основанную на знаниях и высоких технологиях. Это достигается за счет развития человеческого, социального, экологического и экономического секторов в Катаре. Для этого Катар последовательно внедряет новые технологии и вкладывает значительные средства в свою инфраструктуру. Государственный и частный секторы Катара быстро переходят к цифровизации своих процессов и услуг [1]. Немаловажным показателем развития IT-технологий, а также развитости коммуникационных технологий является уровень распространение Интернета [9]. Так, на рис. 1 показано изменение доли населения, пользующегося Интернетом, за период с 1990 по 2022 г.

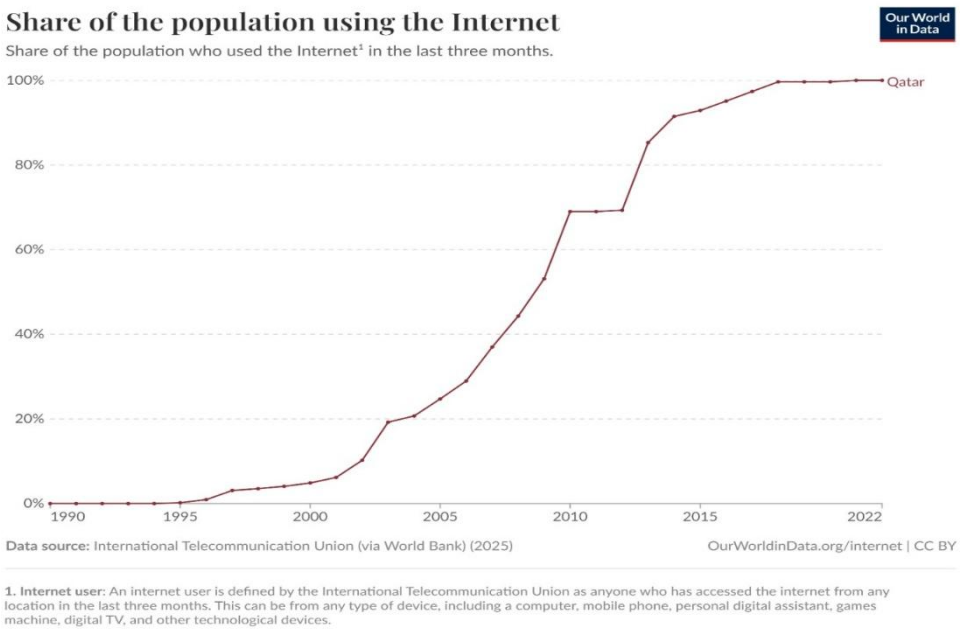

Рис. 1. Охват населения Катара доступом в Интернет.

Источник: International Telecommunication Union (via World Bank) (2025) // Our World in Data. 24.01.2025. URL: https://ourworldindata.org/grapher/share-of-individuals-using-the-internet (accessed: 16.02.2025).

График наглядно показывает стремительный рост доли населения пользующихся интернетом, за исключением, когда произошло торможение роста в 2010-2012 гг. – период революционных потрясений на Ближнем Востоке и в 2018-2020 гг. – нахождение Катара в дипломатической блокаде и, как следствие ухудшение экономической ситуации, а также пандемия COVID-19. Стопроцентный показатель доли населения, пользующихся интернетом достигнутый Дохой к 2021 г. говорит о развитых коммуникационных технологиях, которые необходимо обслуживать, а также обеспечивать информационную безопасность.

Движение в сторону цифровизации привело к тому, что в 2005 г. в Катаре был создан Национальный центр информационной безопасности (Q-CERT) при Министерстве транспорта и коммуникаций (MOTC). Q-CERT нацелен на совершенствование критически важной ИТ-инфраструктуры в Катаре и защиту сетевых линий и киберпространства Катара от любых потенциальных угроз безопасности. Для достижения этой цели Q-CERT разработала Национальную систему обеспечения информационной безопасности (NIAF), которая включает в себя национальное законодательство и политику в области кибербезопасности, которых должны придерживаться все организации в Катаре [10]. Это также оказывает значительное влияние на повышение осведомленности о передовых методах обеспечения кибербезопасности и предоставление отдельным лицам и организациям рекомендаций в этой области [12]. Более того, Q-CERT работает над предоставлением обновленной информации об инцидентах и угрозах кибербезопасности. С этой целью была сформирована группа реагирования на инциденты, которая доступна для широкой общественности, правительства и частного сектора, чтобы сообщать или запрашивать информацию о любых событиях, связанных с безопасностью.

Кроме того, Q-CERT обращает внимание на то, что они предоставляют информационные и обучающие программы, чтобы население в Катаре было осведомлено и находилось в курсе технологических достижений и новых угроз безопасности. В 2014 г. MOTC расширило свои усилия по обеспечению безопасности киберпространства Катара, разработав Национальную стратегию кибербезопасности Катара (NCSS). Стратегия представляет собой сотрудничество между важными структурами Катара, такими как Министерство обороны, Катарский фонд, прокуратура, Министерство внутренних дел и др.

Развитие киберпространства стало одной из главных стратегических задач в эпоху, когда доминируют цифровые технологии. Важнейшим регулятором данной задачи стала обновленная национальная стратегия кибербезопасности на 2024 – 2030 гг. [13]. Эта стратегия, которая была разработана для защиты жизненно важной информационной инфраструктуры страны, определяет основные цели и действия по повышению кибербезопасности во всех отраслях. Тем самым, Катар стремится стать мировым лидером в области кибербезопасности и первопроходцем в области безопасного использования новых технологий.

Успехи в данном направлении, достигнутые Катаром к 2024 г. можно видеть на рис. 2.

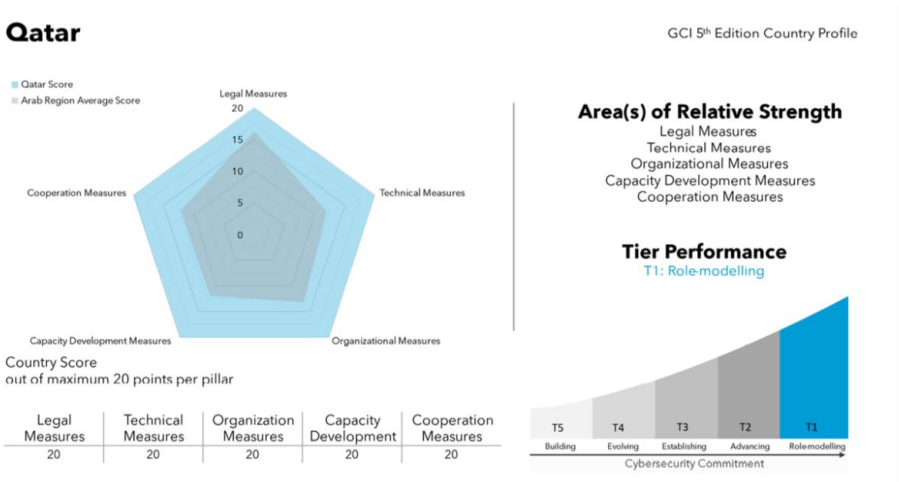

Рис. 2. Позиция Катара в глобальном индексе кибербезопасности.

Источник: Global Cybersecurity Index. 01.03.2025. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (accessed: 02.03.2025).

Согласно отчету Глобального индекса кибербезопасности (Global Cybersecurity Index)[1] Катар получил статус «образцового» за 2024 г., продемонстрировав высокий уровень кибербезопасности на государственном уровне. Успехам эмиратов во многом способствуют наличие устойчивого экономического роста (за исключением кратковременного спада в период пандемии COVID-19) и, как следствие, благоприятный инвестиционный климат, а также продуманная налоговая политика. Немаловажным аспектом здесь является предоставление Катаром иностранным специалистам широких возможностей для раскрытия своего потенциала. Приток высококвалифицированных специалистов во многом обеспечил возможность Дохе осуществить технологический рывок. На государственном уровне поддерживается развитие цифровой экосистемы, что приводит к росту цифровой экономики и большей зависимости от данных. В итоге информационное пространство Эмиратов регулярно подвергается киберугрозам. Согласно отчетам StormWall и Kaspersky Lab по Ближнем Востоку и Северной Африке за 2024 г. геополитическая напряженности в регионе вызвала рост кибератак на 70% по сравнению с прошлым годом. На долю Катара приходилось 7% всех кибератак. Отметим, что годом ранее эта цифра составляла 9%. Основная доля атак пришлась на Саудовскую Аравию – 26%, ОАЭ – 17% и Иран – 12% [15]. К числу наиболее пострадавших относятся финансовый сектор, государственные услуги и розничная торговля. Как мы видим, из числа ведущих государств Персидского залива, Катар подвергся наименьшему количеству кибератак, что говорит о высокой степени защищенности информационного пространства государства.

2 Нормативно-правовая база Государства Катар в области обеспечения информационной безопасности

Серьезность киберпреступлений и их потенциальное воздействие на отдельных лиц и организации вызывают необходимость их предотвращения и нормативно-правого регулирования. В Катаре был принят Закон № 13 от 2016 г. (“Закон о защите конфиденциальности персональных данных”, или PDPL) [16], который вступил в силу в 2017 г. В частности, устанавливаются строгие правила сбора, хранения и обмена персональными данными, а также контролируется порядок их обработки. Катар надеется снизить

[1] Глобальный индекс кибербезопасности (GCI) – измеряет приверженность стран кибербезопасности на глобальном уровне. Поскольку кибербезопасность имеет широкую сферу применения, охватывающую многие отрасли и различные секторы, уровень развития или вовлеченности каждой страны оценивается по 5 основным направлениям – (1) правовые меры, (2) технические меры, (3) организационные меры, (4) развитие потенциала и (5) сотрудничество – а затем суммируется в общую оценку (прим. авт.).

риски, связанные с нежелательным доступом к персональным данным, и защитить право людей на неприкосновенность частной жизни. Тем самым, катарцы стали одними из первых Ближнем Востоке, кто принял специальный закон о защите данных и конфиденциальности. Ключевым регулирующим органом по администрированию и обеспечению соблюдения PDPL является Департамент соблюдения законодательства и защиты данных (CDP) Министерства транспорта и коммуникаций (MOTC). Эта структура выпустила руководящие принципы, касающиеся PDPL ("Руководящие принципы") в 2021 г. с целью обеспечения защиты данных в Катаре [17]. PDPL применяется к персональным данным, которые получены, собраны, извлечены и/или обработаны электронными или традиционными методами. PDPL соответствует универсальным принципам защиты данных, которые были установлены в качестве основы Общих правил защиты данных (GDPR) Европейского союза.

Кроме того, в качестве важного дополнения выступил введенный в действие Закон о защите критической информационной инфраструктуры, целью которого является защита важнейших информационных систем и услуг, в том числе в энергетическом, финансовом и медицинском секторах [18]. Тем самым государство стремится повысить общую устойчивость жизненно важных служб к киберугрозам, устанавливая стандарты безопасности и требования к операторам критически важной инфраструктуры.

Основные положения о защите данных приведены в соответствие с законом о телекоммуникациях, обнародованным декретом-законом Катара № 34 от 2006 г. [19]; Законом об электронных транзакциях и торговле, обнародованным декретом-законом № 16 от 2010 г. [20]; Законом № 2 от 2011 г. об официальной статистике (с поправками, внесенными Законом № 4 от 2015 г.) и Законом о защите персональных данных. Законом № 14 от 2014 г. о борьбе с киберпреступлениями [21]. Отметим, что последний закон является важнейшей правовой основой, регулирующей кибербезопасность в Катаре. Этот закон затрагивает спектр таких киберпреступлений как распространение вредоносного программного обеспечения, незаконный доступ к информационным системам и утечка данных [21]. Режим защиты данных и конфиденциальности в Катаре включает положения, касающиеся наказаний, в других законах, таких как уголовный кодекс (ст. 370—387) [22], Закон о коммерческой тайне, Конституция Катара, Трудовое законодательство и банковские правила Катара, изданные Центральным банком Катара (QCB).

Хотя конкретные статистические данные о киберпреступлениях и результативности применения нормативно-правовой базы для их противодействия в Катаре в открытых источниках присутствуют в ограниченном масштабе, можно утверждать, что государство активно борется с киберпреступностью и улучшает свою систему кибербезопасности. В стране ежегодно проходит национальная информационная кампания по информированию граждан об информационной безопасности, а также запущена горячая линия для сообщений о киберпреступлениях.

Заключение

Таким образом, Катар активно развивает проекты, направленные на повышение цифровой безопасности, защиту критической инфраструктуры и подготовку квалифицированных специалистов. Государство обладает развитой нормативно-правовой базой в области борьбы с киберпреступлениями и системой государственных органов и ведомств, осуществляющих регулирование и обеспечение реализации государственной политики в области борьбы с киберугрозами.

При этом Катар географически находится в нестабильном регионе, где наряду с угрозой религиозного терроризма и экстремизма, растет число хакерских атак. Это вынуждает эмират использовать многосторонний подход для обеспечения информационной безопасности. Для Катара развитие сильного национального цифрового потенциала необходимо для укрепления суверенитета и реализации идей превращения в международный цифровой центр. Поощряя инициативы по подготовке новых специалистов, деятельность бизнес-структур в области информационной безопасности, государство стремится создать основу для обеспечения цифрового суверенитета.

Благодарности

Работа выполнена при поддержке СПбГУ, шифр проекта 116471555.

Литература

1. Elidrisy A. Leveraging Cloud Services & Digital Transformation for Sustainability: Insights from Cases of Qatar // Journal of Innovative Research (JIR). 2024. Vol. 2 (1). P. 21–28.
2. Хайруллин Т.Р., Коротаев А.В. ОАЭ в борьбе за региональное лидерство // Азия и Африка сегодня. 2023. № 9. С. 27–35.
3. Ромашкина Н.П., Стефанович Д.В. Стратегические риски и проблемы кибербезопасности // Вопросы кибербезопасности. 2020. № 5. С. 77-86.
4. Al-Dosari K., Fetais N., Kucukvar M. Artificial Intelligence and Cyber Defense System for Banking Industry: A Qualitative Study of AI Applications and Challenges // Cybernetics and Systems. 2024. Vol.55(2). P. 302–330.
5. Badran A. Regulating Cyberspace for Children: Reflections on the Qatari Case // British Journal of Cyber Criminology. 2024. Vol. 3(1). URL: https://www.pubtexto.com/journals/british-journal-of-cyber-criminology/fulltext/regulating-cyberspace-for-children-reflections-on-the-qatari-case
6. Язов Ю.К. Об определении понятия «кибербезопасность» и связанных с ним терминов // Вопросы кибербезопасности. 2025. № 1 (65). С. 2-6.
7. George W., Al-Ansari T. Road map for National Adoption of Blockchain Technology Towards Securing the Food System of Qatar // Cybernetics and Systems. 2024. Vol. 16(7). P. 29–56.
8. Romashkina N.P. Global'nye voenno-politicheskie problemy mezhdunarodnoj informacionnoj bezopasnosti: tendencii, ugrozy, perspektivy // Voprosy kiberbezopasnosti. 2019. № 1 (29). S. 2-9.
9. Seloom M. Qatar's Security Strategy in the 2022 FIFA World Cup // Journal of Legal & Security Studies. 2024. Vol. 4(4). P. 1–41.
10. Othman S.N., Jawad A.M., Hameed R., Kawad R.T., Khlaponin D. The Impact of Cybersecurity Law in The MiddLe East // ENCUENTROS. 2025. Vol. 23. P. 392–420.
11. International Telecommunication Union (via World Bank) (2025) // Our World in Data.. 24.01.2025. URL: https://ourworldindata.org/grapher/share-of-individuals-using-the-internet (accessed: 16.02.2025).
12. Q-CERT // Q-CERT. URL: https://www.qcert.org/ (accessed: 16.12.2024).
13. National Cyber Security Strategy 2024—2030 State of Qatar // National Cyber Security Agency. URL: https://ncsa.gov.qa/sites/default/files/2024-09/StrategyM9%20-%20Eng%20OL0.pdf (accessed: 18.12.2024).
14. Global Cybersecurity Index. 01.03.2025. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (accessed: 02.03.2025).
15. DDoS Attacks in MENA: 2024 Report by StormWall // StormWall. URL: https://stormwall.network/resources/blog/2024-ddos-attacks-mena?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com (accessed: 20.06.2025).
16. Electronic Commerce and Transactions Law No. 16 of 2010 // Communications Regulatory Authority. URL: https://www.cra.gov.qa/en/document/electronic-commerce-and-transactions-law-no-16--of-2010 (accessed: 16.12.2024).
17. Personal Data Privacy // National Cyber Security Agency of Qatar. URL: https://assurance.ncsa.gov.qa/en/library/privacy?csrt=12343902203125794187 (accessed: 16.12.2024).
18. Law No. 13 of 2016 ("the Personal Data Privacy Protection Law") // National Cyber Governance and Assurance Affairs. URL: https://assurance.ncsa.gov.qa/sites/default/files/library/2020-11/Law%20No.%20%2813%29%20of%202016%20%20on%20Protecting%20Personal%20Data%20Privacy%20-%20English.pdf (accessed: 16.12.2024).
19. Telecommunication Law No. 34 of 2006 Amended Provisions No. of 17 2017 // Communications Regulatory Authority. URL: https://www.cra.gov.qa/en/document/telecommunications-law-no-34-of-2006 (accessed: 16.12.2024).
20. Electronic Commerce and Transactions Law No. 16 of 2010 // Communications Regulatory Authority. URL: https://www.cra.gov.qa/en/document/electronic-commerce-and-transactions-law-no-16--of-2010 (accessed: 16.12.2024).
21. Cybercrime Prevention Law No. 14 of 2014 // Communications Regulatory Authority. URL: https://www.cra.gov.qa/en/document/cybercrime-prevention-law-no-14-of-2014 (accessed: 16.12.2024).
22. Law No. 11 of 2004 Issuing the Penal Code // Qatar Legacy Portal "Al Meezan". URL: https://www.almeezan.qa/LawPage.aspx?id=26&language=en(accessed: 16.12.2024).

QATAR'S INFORMATION SECURITY POLICY

Khayrullin, Timur Radikovich

PhD (Political Science), associate professor
Institute for African Studies of the Russian Academy of Sciences Center for civilizational and regional studies, senior research fellow
Financial University under the Government of the Russian Federation, Department of political sciences, senior lecturer
Moscow, Russian Federation
Saint-Petersburg State University, senior research fellow
Saint-Petersburg, Russian Federation
Jumglaw16@yandex.ru

Gornostaev, Yakov Nikolaevich

Patrice Lumumba Peoples' Friendship University of Russia, Faculty of humanities and social sciences, student
Moscow, Russian Federation
yakov.gornostayev@bk.ru

Ilin, Egor Vadimovich

Patrice Lumumba Peoples' Friendship University of Russia, Faculty of humanities and social sciences, student
Moscow, Russian Federation
Egor-ilin-1111@mail.ru

Abstract

Qatar's National Cybersecurity Strategy is the basis for regulating cybersecurity policy. Qatar's desire to achieve digital sovereignty has led to the fact that today the state is one of the most successful states in the field of information security.

Keywords

information threat; government policy; legislative framework; critical information infrastructure; digitalization; data protection; cyber threat; cyber-attack; privacy, national cybersecurity strategy

References

1. Elidrisy A. Leveraging Cloud Services & Digital Transformation for Sustainability: Insights from Cases of Qatar // Journal of Innovative Research (JIR). 2024. Vol. 2 (1). P. 21–28.
2. Khayrullin T.R., Korotayev A.V. OAE v bor'be za regional'noe liderstvo // Asia and Africa today. 2023. № 9. S. 27–35. DOI: 10.31857/S032150750027592-3.
3. Romashkina N.P., Stefanovich D.V. Strategicheskie riski i problemy kiberbezopasnosti // Voprosy kiberbezopasnosti. 2020. № 5. S. 77-86. DOI 10.21681/2311-3456-2020-05-77-86
4. Al-Dosari K., Fetais N., Kucukvar M. Artificial Intelligence and Cyber Defense System for Banking Industry: A Qualitative Study of AI Applications and Challenges // Cybernetics and Systems. 2024. Vol.55(2). P. 302–330.
5. Badran A. Regulating Cyberspace for Children: Reflections on the Qatari Case // British Journal of Cyber Criminology. 2024. Vol. 3(1). URL: https://www.pubtexto.com/journals/british-journal-of-cyber-criminology/fulltext/regulating-cyberspace-for-children-reflections-on-the-qatari-case
6. Yazov Yu.K. Ob opredelenii ponyatiya «kiberbezopasnost'» i svyazannyx s nim terminov // Voprosy kiberbezopasnosti. 2025. № 1 (65). S. 2-6. DOI: 10.21681/2311-3456-2025-1-2-6.
7. George W., Al-Ansari T. Road map for National Adoption of Blockchain Technology Towards Securing the Food System of Qatar // Cybernetics and Systems. 2024. Vol. 16(7). P. 29–56.
8. Romashkina N.P. Global'nye voenno-politicheskie problemy mezhdunarodnoj informacionnoj bezopasnosti: tendencii, ugrozy, perspektivy // Voprosy kiberbezopasnosti. 2019. № 1 (29). S. 2-9.
9. Seloom M. Qatar's Security Strategy in the 2022 FIFA World Cup // Journal of Legal & Security Studies. 2024. Vol. 4(4). P. 1–41.
10. Othman S.N., Jawad A.M., Hameed R., Kawad R.T., Khlaponin D. The Impact of Cybersecurity Law in The MiddLe East // ENCUENTROS. 2025. Vol. 23. P. 392–420.

11. International Telecommunication Union (via World Bank) (2025) // Our World in Data.. 24.01.2025. URL: https://ourworldindata.org/grapher/share-of-individuals-using-the-internet (accessed: 16.02.2025).
12. Q-CERT // Q-CERT. URL: https://www.qcert.org/ (accessed: 16.12.2024).
13. National Cyber Security Strategy 2024—2030 State of Qatar // National Cyber Security Agency. URL: https://ncsa.gov.qa/sites/default/files/2024-09/StrategyM9%20-%20Eng%20OL0.pdf (accessed: 18.12.2024).
14. Global Cybersecurity Index. 01.03.2025. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (accessed: 02.03.2025).
15. DDoS Attacks in MENA: 2024 Report by StormWall // StormWall. URL: https://stormwall.network/resources/blog/2024-ddos-attacks-mena?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com (accessed: 20.06.2025).
16. Electronic Commerce and Transactions Law No. 16 of 2010 // Communications Regulatory Authority. URL: https://www.cra.gov.qa/en/document/electronic-commerce-and-transactions-law-no-16--of-2010 (accessed: 16.12.2024).
17. Personal Data Privacy // National Cyber Security Agency of Qatar. URL: https://assurance.ncsa.gov.qa/en/library/privacy?csrt=12343902203125794187 (accessed: 16.12.2024).
18. Law No. 13 of 2016 ("the Personal Data Privacy Protection Law") // National Cyber Governance and Assurance Affairs. URL: https://assurance.ncsa.gov.qa/sites/default/files/library/2020-11/Law%20No.%20%2813%29%20of%202016%20%20on%20Protecting%20Personal%20Data%20Privacy%20-%20English.pdf (accessed: 16.12.2024).
19. Telecommunication Law No. 34 of 2006 Amended Provisions No. of 17 2017 // Communications Regulatory Authority. URL: https://www.cra.gov.qa/en/document/telecommunications-law-no-34-of-2006 (accessed: 16.12.2024).
20. Electronic Commerce and Transactions Law No. 16 of 2010 // Communications Regulatory Authority. URL: https://www.cra.gov.qa/en/document/electronic-commerce-and-transactions-law-no-16--of-2010 (accessed: 16.12.2024).
21. Cybercrime Prevention Law No. 14 of 2014 // Communications Regulatory Authority. URL: https://www.cra.gov.qa/en/document/cybercrime-prevention-law-no-14-of-2014 (accessed: 16.12.2024).
22. Law No. 11 of 2004 Issuing the Penal Code // Qatar Legacy Portal "Al Meezan". URL: https://www.almeezan.qa/LawPage.aspx?id=26&language=en (accessed: 16.12.2024).