DOI: https://doi.org/10.24833/0869-0049-2025-2-86-98

Исследовательская статья
УДК: 341
Поступила в редакцию: 18.02.2025
Принята к публикации: 22.04.2025

Татьяна Владимировна ГОВЕРДОВСКАЯ
Астраханский государственный университет им. В.Н. Татищева
Татищева ул., 20а, Астрахань, 414056, Российская Федерация
tara_goya@bk.ru
ORCID: 0000-0001-6340-4764

Ляйсян Маратовна СТАРКОВА
Астраханский государственный университет им. В.Н. Татищева
Татищева ул., 20а, Астрахань, 414056, Российская Федерация
5leska5@mail.ru
ORCID: 0000-0002-4411-6510

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ПРОТИВОДЕЙСТВИЯ КИБЕРРИСКАМ В МОРСКОМ ПРОСТРАНСТВЕ КАСПИЙСКОГО РЕГИОНА В РАМКАХ ОБЕСПЕЧЕНИЯ РЕГИОНАЛЬНОЙ БЕЗОПАСНОСТИ

ВВЕДЕНИЕ. *На сегодняшний день международное сообщество признает многоаспектность и комплексность понятия «международная безопасность» и призывает к сотрудничеству государств в данной сфере. Представляется, что разработку и реализацию подобных механизмов следует начать с малых региональных групп, и далее на основе выявления наиболее эффективных моделей осуществить их внедрение на универсальном уровне. В качестве примера подобных региональных усилий, направленных на укрепление безопасности, может служить Каспийский регион. Авторы работы фокусируют свое внимание на исследовании одного из направлений в сфере региональной безопасности, а именно системы управления киберрисками в морском пространстве Каспийского региона в контексте обеспечения безопасности морского судоходства и мореплавания. Цель работы авторам представляется в подтверждении гипотезы о необходимости правового регулирования противодействия киберрискам в морском пространстве как неотъемлемого элемента современной системы обеспечения региональной безопасности.*

МАТЕРИАЛЫ И МЕТОДЫ. *Для достижения заявленной цели коллектив авторов решил ряд научных задач, среди которых краткий анализ правовых актов Организации Объединенных Наций (ООН), обосновывающих факт комплексности международной безопасности и взаимозависимости региональной и международной безопасности; обзор договорной базы Прикаспийских государств по вопросам обеспечения безопасности региона и мирного сотрудничества в различных областях. Немаловажным для достижения цели явился обзор актов Международной морской организации (ИМО) по*

вопросам кибербезопасности морского судоходства и мореплавания. Помимо традиционных общенаучных методов исследования, авторы в основном использовали метод доктринального толкования правовых актов, который позволил обосновать возможность правовой регламентации и заключения отдельного Протокола.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ. *В результате проведенного исследования были выработаны рекомендации относительно структуры и содержания Протокола по борьбе с киберрисками в морском пространстве Каспийского региона.*

ОБСУЖДЕНИЕ И ВЫВОДЫ. *В ходе тщательного анализа региональных нормативных источников, действующих в обозначенной сфере в рамках Каспийского региона, авторы приходят к выводу о необходимости принятия Протокола о сотрудничестве в области обеспечения безопасности мореплавания в качестве унифицированного правового источника в сфере противодействия и управления морскими рисками в морском пространстве Каспийского региона.*

КЛЮЧЕВЫЕ СЛОВА: *региональная безопасность, киберриски морской отрасли, безопасность мореплавания, Каспийский регион, киберинциденты на море, Руководство по управлению киберрисками на море, международная безопасность*

ДЛЯ ЦИТИРОВАНИЯ: Говердовская Т.В., Старкова Л.М. 2025. Правовое регулирование противодействия киберрискам в морском пространстве Каспийского региона в рамках обеспечения региональной безопасности. – *Московский журнал международного права.* № 2. С. 86–98. DOI: https://doi.org/10.24833/0869-0049-2025-2-86-98

Авторы заявляют об отсутствии конфликта интересов.

DOI: https://doi.org/10.24833/0869-0049-2025-2-86-98

Research article
UDC: 341
Received 18 February 2025
Approved 22 April 2025

Tatyana V. GOVERDOVSKAYA
Astrakhan State University
20a, Tatishcheva st., Astrakhan, Russian Federation, 414056
tara_goya@bk.ru
ORCID: 0000-0001-6340-4764

Lyasyan M. STARKOVA
Astrakhan State University
20a, Tatishcheva st., Astrakhan, Russian Federation, 414056
5leska5@mail.ru
ORCID: 0000-0002-4411-6510

LEGAL REGULATION OF COUNTERACTING CYBER RISKS IN THE MARINE SPACE OF THE CASPIAN REGION WITHIN THE FRAMEWORK OF ENSURING REGIONAL SECURITY

INTRODUCTION. *Today, the international community recognizes the multidimensional and complex nature of the concept of «international security» and calls for the cooperation of states in this field. It seems that the development and implementation of such mechanisms should start with small regional groups, and then, by identifying the most effective models, they can be implemented universally. The Caspian region is an example of such regional efforts to strengthen security. The authors research the main aspects of regional security. It is the cyber security aspect. The authors propose the idea of creating a cyber incident management center in the maritime space of the Caspian region. The aim of the paper is to confirm the hypothesis of the need to develop a legal framework for the implementation of a cyber risk prevention and management system in the Caspian region as a mandatory part of the system of regional security.*

MATERIAL AND METHODS. *To achieve the stated goal, the authors' team solved a number of scientific tasks, among which is a brief analysis of UN legal acts justifying the fact of international security complexity and regional and international security interdependence. Then, review of the Caspian States' treaty framework for regional security and peaceful cooperation in various fields. The review of IMO acts on maritime and marine cybersecurity was an important step towards achieving this goal. Apart from the traditional general-science methods of research, the authors mainly used the method of doctrinal interpretation of legal acts, which allowed to justify the possibility of legal regulation and conclusion of a separate protocol.*

RESEAECH RESULTS. *The study resulted in recommendations on the structure and content of the Protocol for the Management of Cyber Risks in the Caspian Sea.*

DISCUSSION AND CONCLUSIONS. *In the course of a thorough analysis of regional normative sources operating in the designated area within the Caspian region. The authors conclude that it is necessary to adopt an additional protocol on cooperation in the field of maritime safety.*

KEYWORDS: *regional security, cyber risks of the marine industry, maritime safety, Caspian region, cyber incidents at sea, Guide for management of cyber risks at sea, international security*

FOR CITATION: Goverdovskaya T.V., Starkova L.M. Legal Regulation of Counteracting Cyber Risks in the Marine Space of the Caspian Region within the Framework of Ensuring Regional Security. – *Moscow Journal of International Law.* 2025. No. 2. P. 86–98. DOI: https://doi.org/10.24833/0869-0049-2025-2-86-98

The authors declare the absence of conflict of interest.

1. Введение

Безопасность – многоаспектное комплексное явление, которое включает в себя множество категорий. Среди них «военная безопасность», «политическая стабильность», «мирное сотрудничество», «народонаселение и демография», «экологические и экономические аспекты», «права человека» и «вопросы культуры» и т. д. При этом категория «безопасность» наряду с категориями «национальная безопасность», «публичный интерес» и «национальные интересы» в правовой науке не имеет четкого определения, оставляет простор для субъективных оценок и политической воли.

Вопросам комплексности международной безопасности, а также взаимосвязи международной и региональной безопасности посвящено множество работ российских и зарубежных ученых. Так, С.А. Бокерия подчеркивает, что региональное взаимодействие государств со всей очевидностью оказывает влияние на глобальные международные отношения [Бокерия 2019:21]. Многие авторы отмечают все возрастающий интерес околокаспийских стран к региону, анализируя возможные сценарии развития международных отношений, утверждаются в мысли о взаимосвязанности и взаимозависимости международной и региональной безопасности в Прикаспии [Жуковский, Никитенко 2018:43], [Кулагина, Дунаева 2007:125].

Между тем исследования нормативно-правовой базы в сфере обеспечения кибербезопасности Каспийского региона в российской доктрине находятся на зачаточном уровне. Среди работ российских ученых следует отметить исследования С.А. Семенова, Т.Я. Хабриевой, Р.А. Курбанова, М.В. Жуковского, В.И. Никитенко, А.О. Мурсалиева и др.

Устав ООН в ст. 1 дает наиболее обобщенную интерпретацию термина «международная

безопасность», которая была представлена отцами-основателями исходя из исторических событий, предшествовавших учреждению организации. Ключевая задача ООН заключается в поддержании международного мира и безопасности[1]. В 1970 г. Генеральная Ассамблея ООН в Декларации об укреплении международной безопасности утверждала, что существует значительная взаимосвязь между международной безопасностью, процессом разоружения и экономическим развитием стран[2]. Это подчеркивает, что достижение прогресса в одной из этих областей неизбежно будет способствовать улучшению других. Таким образом, продвижение к одной из поставленных задач означает и прогресс в других направлениях, что демонстрирует важность комплексного подхода к вопросам безопасности и развития[3]. Это свидетельствует о том, что с 1970-х гг. о категории безопасность мировое сообщество начинает говорить без привязки исключительно к военно-политическим аспектам и разоружению, но расширяет данную категорию, включая экономическое развитие, а позднее права человека и вопросы экологии.

Региональная безопасность – безусловная и неотделимая часть безопасности международной, которая определяет состояние межгосударственных отношений в конкретном регионе как мирное, т.е. не содержащее военных угроз, опасностей экономического характера и др., а также вмешательств и вторжений со стороны иных государств или других участников международных отношений, которые могут нанести ущерб или каким бы то ни было образом посягнуть на суверенитет и независимость государств, находящихся в регионе [Курылев, Казанчев 2013:11].

Устав ООН в главе 8 «Региональные соглашения» опосредованно выделяет категорию региональная безопасность, оперируя формулировками «местные споры», «региональные действия», «региональные соглашения, относящиеся к поддержанию международного мира и безопасности». Более того, ч. 3 ст. 52 Устава ООН содержит положение о том, что Совет Безопасности ООН должен поощрять развитие применения мирного разрешения местных споров при помощи региональных соглашений или региональных органов[4]. Таким образом, международное сообщество признает многоаспектность и комплексность термина «безопасность».

2. Нормативно-правовые основы сотрудничества государств в области обеспечения безопасности в Каспийском регионе

Сотрудничество в рамках региональной группы, без сомнения, является более эффективным, особенно в сфере региональной безопасности. Уникальное географическое положение Каспийского моря в сочетании с особой экосистемой, а также специфическими политическими, экономическими и культурными связями между Прикаспийскими государствами придают особое стратегическое значение вопросам комплексной безопасности данного региона [Батырь 2019:51]. Эти факторы обуславливают необходимость совместной работы стран региона и способствуют более глубокому и продуктивному взаимодействию в решении вопросов, касающихся безопасности. Таким образом, региональная группа может эффективно справляться с вызовами и угрозами, находясь в более близком сотрудничестве, учитывая при этом многообразие интересов и особенностей каждого из государств[5]. Вопросы комплексной коллективной безопасности Каспийского региона были обозначены в одном из первых правовых документов, разработанных и принятых к исполнению государствами в рамках рассмотрения Каспийского вопроса, – Декларации о безопасности Прикаспийских государств. В преамбуле данного документа договаривающиеся стороны выражают свою убежденность в том,

[1] ООН: Устав ООН. 26 июня 1945 г. Сан-Франциско. URL: https://www.un.org/ru/about-us/un-charter/full-text?ysclid=mbfjzmq6hx237608809 (дата обращения: : 10.02.2025).

[2] ООН: Декларация об укреплении международной безопасности. Принята резолюцией Генеральной Ассамблеи ООН 2734 (XXV) от 16 декабря 1970 г. – *Действующее международное право: сборник*. Т. 2; Справочно-правовая система «Гарант». URL: https://base.garant.ru/2541111/ (дата обращения: 29.01.2025).

[3] Там же.

[4] ООН: Устав ООН. 26 июня 1945 г. Сан-Франциско.

[5] Мурсалиев А.О. *Охрана окружающей среды Каспийского моря: международно-правовые аспекты:* дис. ... канд. юрид. наук. М. 2021. URL: https://mgimo.ru/upload/diss/2021/mursaliev-diss.pdf?utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru (дата обращения: 29.01.2025).

что сотрудничество пятерки Прикаспийских государств, основанное на дружбе и добрососедстве, отвечает коренным интересам их народов, являясь при этом ключевым фактором укрепления региональной безопасности[6] [Старкова 2022:686].

Названная Декларация содержит ряд ключевых положений по вопросам безопасности, в частности закрепляет тезис о возможности использования Каспийского моря исключительно в мирных целях, решении возможных вопросов и ситуаций мирными средствами, что будет способствовать укреплению взаимного доверия, обеспечению безопасности и стабильности региона. Кроме того, стороны обязуются воздерживаться от применения военной силы во взаимных отношениях. Декларация устанавливает запрет на использование национальных вооруженных сил для нападения на любую из сторон, а также предоставление территории другим государствам для совершения актов агрессии и других военных действий против любой из стран Прикаспийского региона[7]. Между тем стоит отметить, что данный документ имеет декларативный характер, поскольку государства-участники лишь заявляют о своей политической воле, а не берут на себя политические обязательства[8].

Далее следует отметить такой документ, как Соглашение о сотрудничестве государств в сфере безопасности на Каспийском море 2010 г. (Соглашение 2010 г.)[9]. Ключевое положение данного документа закреплено в ст. 1 и звучит как: «Обеспечение безопасности на Каспийском море является прерогативой прикаспийских государств». В Соглашении 2010 г. обозначены конкретные области сотрудничества государств в сфере обеспечения безопасности. Среди них стоит выделить: борьбу с терроризмом; организованной преступностью; незаконным оборотом оружия любых видов и боеприпасов, взрывчатых и отравляющих веществ, военной техники; незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров; отмыванием доходов, в том числе денежных средств, полученных преступным путем; контрабандой; пиратством; торговлей людьми и незаконной миграцией; незаконной добычей биологических ресурсов (браконьерством); обеспечение безопасности морского судоходства и мореплавания. Впрочем, перечень не является исчерпывающим, поскольку п. 2 ст. 2 содержит указание на возможность осуществления сотрудничества в других областях, соответствующих предмету Соглашения 2010 г. и представляющих взаимный интерес, за исключением военных аспектов безопасности[10]. Интересен тот факт, что Соглашение 2010 г. в ст. 4 закрепляет возможность конкретизации нормативно-правовой базы по вопросам комплексной региональной безопасности посредством принятия дополнительных Протоколов о сотрудничестве в названных областях[11]. К примеру, государства Каспийской пятерки разработали детализированный механизм сотрудничества и взаимодействия в сфере пресечения преступлений в рамках принятия Протокола о сотрудничестве в области борьбы с терроризмом на Каспийском море 2018 г.[12] и Протокола о сотрудничестве в области борьбы с организованной преступностью на Каспийском море 2018 г.[13] Стоит отметить возможный

---

[6] Декларация о безопасности Прикаспийских государств Азербайджанской Республики, Исламской Республики Иран, Республики Казахстан, Российской Федерации и Туркменистана. 2007. Принята в г. Тегеране 16 октября 2007 г. – *Справочно-правовая система «КонсультантПлюс»*. URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=INT&n=41172#Ka5XVcUEtErCez9M1 (дата обращения: 11.02.2025).

[7] Там же.

[8] Рожков И.С. *Механизмы многостороннего взаимодействия прикаспийских государств на современном этапе:* дис. ... канд. полит. наук. М. 2021. 605 с. URL: https://search.rsl.ru/ru/record/01011151028 (дата обращения: 23.02.2025).

[9] Соглашение о сотрудничестве государств в сфере безопасности на Каспийском море. Баку, 18 ноября 2010 г. – *Официальный интернет-портал правовой информации*. URL: https://base.garant.ru/70104428/ (дата обращения: 11.02.2025).

[10] Там же.

[11] Там же.

[12] Протокол о сотрудничестве в области борьбы с терроризмом на Каспийском море к Соглашению о сотрудничестве в сфере безопасности на Каспийском море. Актау. 12 августа 2018 г. URL: https://www.mid.ru/problematika-bassejna-kaspijskogo-mora/-/asset_publisher/FX0KRdXqTkSJ/content/id/3319395 (дата обращения: 03.02.2025).

[13] Протокол о сотрудничестве в области борьбы с организованной преступностью на Каспийском море к Соглашению о сотрудничестве в сфере безопасности на Каспийском море. Актау, 12 августа 2018 г. URL: https://www.mid.ru/problematika-bassejna-kaspijskogo-mora/-/asset_publisher/FX0KRdXqTkSJ/content/id/3319409 (дата обращения: 03.02.2025).

потенциал Соглашения 2010 г. в части правового регулирования управления киберрисками как неотъемлемого элемента современной системы обеспечения региональной безопасности Каспия. Несмотря на отсутствие специализированных норм, регулирующих киберриски, в Соглашении 2010 г. заслуживают внимания положения, закладывающие общие принципы сотрудничества государств – участников в обозначенной сфере, механизмы обмена информацией и проведения совместных операций. Практика применения соответствующих норм Соглашения 2010 г. имеет ценность для разработки руководств и процедур совместного реагирования на кибератаки и иные информационные угрозы [Кущенко 2021:118].

В 2018 г. был принят основополагающий документ, к которому стороны шли на протяжении 20 лет – Конвенция о правовом статусе Каспийского моря (Конвенция)[14]. Выступая нормативной основой определения правового статуса Каспийского моря, Конвенция не выделяет вопросы региональной безопасности, так как имеет совершенно иную цель. Между тем ст. 3 содержит принципы, на основе которых будет осуществляться деятельность государств на Каспийском море, среди которых особый интерес представляют:

– использование Каспийского моря в мирных целях, превращение его в зону мира, добрососедства, дружбы и сотрудничества, решения всех вопросов, связанных с Каспийским морем, мирными средствами;

– обеспечение безопасности и стабильности в Каспийском регионе;

– обеспечение стабильного баланса вооружений;

– соблюдение согласованных мер доверия в сфере военной деятельности[15].

Стоит отметить, что ряд положений Конвенции развивают логику Соглашения 2010 г. Так, одним из принципов является «неприсутствие на Каспийском море вооруженных сил, не принадлежащих Сторонам». В ст. 17 Конвенции государства вновь обязуются взаимодействовать в областях, обозначенных в Соглашении 2010 г.[16]

Таким образом, проведенный авторами анализ нормативно-правовых источников, принятых в рамках сотрудничества Прикаспийских государств и определения правового статуса Каспийского моря, позволил выделить такие аспекты безопасности, как экологический, энергетический, военный, а также противодействие преступности и безопасность морского судоходства и мореплавания. При этом названные документы не содержат указание на информационную безопасность как одну из важнейших составляющих комплексной региональной безопасности на современном этапе. Не вызывает сомнения тот факт, что структурные трансформации современного общества обуславливают необходимость выделения так называемого цифрового аспекта безопасности, в частности коллективной безопасности Каспийского региона.

3. Цифровой аспект безопасности Каспийского региона в сфере обеспечения безопасности морского судоходства

Учитывая стремительные темпы и масштабы цифровизации, киберриски могут проявляться практически в любой сфере общественного функционирования и устройства. Охватить рамками данного исследования возможные сферы, виды киберрисков и правовые средства борьбы с ними не представляется возможным. Поэтому мы сузили рамки исследования, сосредоточив свои усилия на анализе системы управления киберрисками в морском пространстве Каспийского региона в контексте обеспечения безопасности морского судоходства и мореплавания. Авторы исследования понимают термины «киберриски» и «киберугрозы» как равнозначные, исходя из анализа нормативных источников, принятых в рамках ИМО. В настоящее время ИМО служит универсальной платформой для обсуждения различных вопросов, касающихся функционирования и развития морской отрасли. Она осуществляет последовательные действия, направленные на адаптацию существующих и создание новых международно-правовых инструментов, направленных на обеспечение

[14] Конвенция о правовом статусе Каспийского моря. Актау, 12 августа 2018 г. – *Справочно-правовая система «Гарант»*. URL: https://base.garant.ru/72347414/ (дата обращения: 29.01.2025).

[15] Там же.

[16] Махдиян М.Х. *История межгосударственных отношений Ирана и России: XIX – начало XXI века:* дис. ... канд. истор. наук. М. 2012. 273 с.

безопасности морских перевозок в условиях современной цифровизации и возникающих киберугроз и уязвимостей. По данному вопросу ИМО разработала и приняла ряд документов:

– Руководство по управлению киберрисками в морской отрасли от 5 июля 2017 г. (Guidelines on Maritime Cyber Risk Management, MSC-FAL.1/Circ.3 2017; Руководство)[17];

– Резолюцию MSC.428(98) Комитета по безопасности на море ИМО «Управление кибернетическими рисками в системах управления безопасностью» MSC 98/23/Add.1 от 30 июля 2017[18]. [Каспий … 2018:422]

Руководство содержит определение понятия «морские киберугрозы», под которыми понимаются «угрозы технологическому ресурсу со стороны потенциальных обстоятельств или событий, которые могут повлечь за собой сбои в перевозке грузов и пассажиров, безопасности мореплавания или безопасности судна, в связи с повреждением, утратой или компрометацией информации или систем» (п. 1.1). Руководство классифицирует потенциальные киберугрозы по различным основаниям, в частности, выделяет преднамеренные (взлом или внедрение вредоносного программного обеспечения (ПО)) и непреднамеренные (ошибки в обслуживании ПО) действия. Руководство возлагает большую ответственность на руководящий кадровый состав как ключевой фактор создания эффективной системы управления киберрисками. В свою очередь, руководящий состав должен реализовывать меры, направленные на повышение уровня подготовки персонала посредством разработки тренинговых программ, что позволит создать целостную систему управления киберрисками на море (п. 3.1). Интересен тот факт, что Руководство представляет подход к управлению киберрисками, в основе которого заложены действующие стандарты безопасности посредством их компиляции и расширительного толкования в условиях вновь формирующихся вызовов и угроз цифровой среды (п. 2.1.8). Руководство называет пять функциональных элементов эффективного управления киберрисками в морской отрасли, в частности, такие как определение, защита, обнаружение, реагирование и восстановление (п. 3.5). Названные элементы должны быть положены в основу деятельности судоходных компаний [Karaś 2023:921].

Большой интерес представляет Резолюция MSC.428(98) об управлении киберрисками в рамках систем управления безопасностью Комитета ИМО по безопасности, поскольку данный документ содержит обязательное к исполнению требование к администрациям судовой отрасли по обеспечению учета киберрисков в действующих системах управления безопасностью судна и устанавливает конкретный срок для реализации этого учета – не позднее 1 января 2021 г. Непредставление указанных данных может расцениваться как нарушение судовой документации по управлению безопасностью. Вследствие этого операторы судов подвергаются риску получения административных штрафов вплоть до применения крайней меры – задержания судна в порту с запретом на дальнейшую эксплуатацию. Тем не менее практическая реализация данного требования судоходными компаниями и до сегодняшнего дня значительно осложнена отсутствием стандартизированных подходов к пониманию и оценке киберугроз, а также отсутствием перечня конкретных процедур в случае выявления потенциальной киберугрозы. Это приводит к тому, что вся ответственность за разработку и внедрение технических и методологических мер по защите от киберугроз возложена непосредственно на судовые компании, которые вынуждены самостоятельно определять, выявлять потенциальные киберриски и уязвимости, производить оценку их масштабов и разрабатывать конкретные методы предупреждения и борьбы с ними [Düzenli 2024:1].

Стоит отметить, что судоходная отрасль реализует различные программы, направленные на включение конкретных правил и практических руководств по борьбе с киберрисками в действующую правовую базу в сфере безопасности

[17] ИМО: Руководство по управлению киберрисками в морской отрасли. 5 июля 2017 г. URL: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3(Secretariat).pdf (дата обращения: 12.02.2025).

[18] ИМО: Управление кибернетическими рисками в системах управления безопасностью. 30 июля 2017 г. URL: https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.428(98).pdf (дата обращения: 12.02.2025).

морского судоходства. Так, Ассоциация Балтийский и международный морской совет (BIMCO), объединив усилия различных судоходных компаний с 2016 г. разрабатывает и публикует ежегодные отчеты – Руководство по кибербезопасности на борту судов (The Guidelines on Cyber Security Onboard Ships)[19]. Эксперты компаний проанализировали потенциальные кибериски в морской сфере и их прогнозируемые последствия. Руководство привнесло большой вклад в процесс систематизации и анализа актуальной информации о киберугрозах информационной безопасности в сфере морского судоходства. Оно содержит практические рекомендации по противодействию киберрискам морской отрасли, а также информацию по страховому покрытию после кибератак. Руководство содержит рекомендации для судовладельцев и операторов по вопросам оценки уязвимостей бортовых информационных систем и разработки мер, направленных на повышение устойчивости киберрискам. В 2019 г. BIMCO и Международная палата судоходства (ICS) опубликовали «Учебник по кибербезопасности для использования на борту судов» (Cyber Security Workbook for On Board Ship Use). Издание охватывает вопросы защиты, выявления, реагирования и восстановления в случае кибернетических атак. Разработчики утверждают, что данное пособие предлагает понятные и легко применимые на практике указания. В 2021 г. опубликована пересмотренная четвертая версия Руководства[20] [Говердовская, Бесчастнова, Крайнюкова 2020:171].

Кроме разработки нормативных источников, проблема кибербезопасности в сфере морского судоходства исследуется на доктринальном уровне, преимущественно западными учеными. При этом помимо обоснования и исследования существа уникальной природы морских киберугроз с учетом отраслевых особенностей, авторы формулируют различные подходы и практические рекомендации относительно возможных направлений политики в области морских киберпространств. Ряд исследователей обосновывают необходимость принятия дополнений и корректировок действующих правовых документов в сфере безопасности морской отрасли, другие разрабатывают проекты новых специализированных нормативных источников.

Так, К. Тэм и К. Джонс в своем исследовании, посвященном анализу киберрисков морской среды, отмечают необходимость принятия дополнений и расширительных положений в кодексы безопасности морского судоходства (Международный кодекс безопасности судов и портовых средств (ISPS) и Международный кодекс управления безопасностью (ISM)). По мнению авторов, названные правовые источники являются эффективными и успешно реализуемыми в практической деятельности судоходных компаний, при возможна конкретизация и дополнения в контексте внесения кибернетического элемента [Tam, Jones 2018:1-18].

Р. Хопкрафт и К.М. Мартин предлагают рассмотреть возможность принятия специализированного Кодекса морской кибербезопасности по аналогии с Полярным кодексом. Авторы приводят оценку возможных этапов разработки и принятия данного международного документа под эгидой ИМО. При этом отмечают, что именно посредством принятия единого специализированного документа можно обеспечить учет и оценку как долгосрочных, так и конкретных киберрисков, которые являются специфическими. Кодекс должен включать обширный и структурированный свод нормативных положений в области безопасности, разработанный на основе уже существующих стандартов и правил с учетом специфики киберрисков [Hopcraft, Martin 2018:1-13].

В числе отечественных исследователей стоит отметить работы С.А. Семенова, посвященные анализу потенциальных сценариев киберинцидентов на судовых и портовых системах. В числе рекомендаций по возможным направлениям развития политики управления киберрисками и обеспечения информационной безопасности морского сектора, автор отстаивает идею естественного и постепенного расширения существующих методов управления безопасностью

[19] Балтийский и международный морской совет: Руководство по кибербезопасности на борту судов. 2017 г. URL: https://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16 (дата обращения: 10.01.2025).

[20] Балтийский и международный морской совет: Руководство по кибербезопасности на борту судов. 2021 г. URL: https://maritimecyprus.com/wp-content/uploads/2020/11/Cyber_Security_IMO2021_Requirements.pdf (дата обращения: 17.02.2025).

мореплавания и безопасностью судна. При этом автор отмечает наличие некой фрагментации в правовом регулировании вопросов кибербезопасности морской отрасли. Поскольку, с одной стороны, под эгидой ИМО на международном уровне принимается ряд обязательных для исполнения стандартов и регламентов, посвященных вопросам кибербезопасности морских систем управления на борту судов и в терминалах. С другой стороны, в рамках национальной правоприменительной практики государств, управление в сфере морской кибербезопасности осуществляется на основе отдельных нормативно-правовых актов при отсутствии единого структурированного документа, что, в свою очередь, препятствует реализация комплексного подхода к обеспечению безопасности [Семенов 2018:43].

С учетом изложенного стоит отметить, что к проблеме кибербезопасности морской отрасли, в частности анализу и разработке правовой основы для создания и эффективной реализации системы управления киберрисками, есть определенный интерес в среде западных и отечественных ученых. При этом независимо от обоснования того или иного подхода, ученые сходятся во мнении о необходимости совершенствования и реформирования стандартов безопасности морской отрасли с целью их адаптации к новым формам угроз. Посредством анализа подходов, предлагаемых в рамках других исследований, и их последующей компиляции с результатами, полученными авторами данной работы, была произведена критическая оценка и апробация результатов. В числе важных положений, получивших свое обоснование и закрепление в ряде работ, можно отметить понимание необходимости разработки и принятия глобальных обновленных стандартов кибербезопасности морской отрасли с учетом технологических аспектов. Учитывая трансграничный характер киберугроз, обусловленный спецификой цифровой инфраструктуры, а также отраслевые особенности и международный масштаб морских систем, разработка правовых основ и создание системы управления киберрисками в морской отрасли должны быть реализованы на международном уровне посредством универсального глобального подхода. В частности, данная идея и конкретные предложения по разработке Международного Кодекса кибербезопасности морской отрасли были представлены авторами в более ранних исследованиях [Говердовская, Бесчастнова, Крайнюкова 2020:171].

4. Практические рекомендации и предложения

В настоящем исследовании авторами предпринята попытка концептуального применения разработанных ранее предложений и подходов к потребностям конкретного региона. Отмечая при этом, что региональные инициативы также должны быть учтены в рамках комплексного и многоаспектного процесса создания системы управления киберрисками в морской отрасли. Авторы отмечают незначительное количество доктринальных исследований и отсутствие нормативных положений по проблеме обеспечения информационной безопасности Каспийского региона, в частности кибербезопасности морских систем Каспия. В связи с чем в ходе проведенного анализа нормативных источников были найдены положения, закрепляющие конкретный механизм принятия дополнительных соглашений, посвященных различным направлениям в сфере обеспечения безопасности.

Запрос правоприменительной практики обозначил необходимость разработки и принятия унифицированного правового источника регионального характера в сфере противодействия киберрискам на Каспийском море. С этой целью может быть использован правовой механизм, закрепленный в ст. 3 и 4 Соглашения 2010 г.

В качестве рекомендаций относительно структуры и содержания Протокола можно предложить следующие положения.

1. Протокол должен включать нормативные определения соответствующих правовых категорий, используемых в сфере противодействия киберрискам в морской отрасли, что позволит избежать их свободного неаутентичного толкования, некой фрагментации и несогласованности в подходах.

2. Протокол должен определять критерии для определения сущностных признаков деяний, которые могут быть отнесены к группе так называемых киберинцидентов в морской отрасли. Закрепить исчерпывающий перечень деяний, входящих в состав данной группы, не представляется возможным вследствие стремительных темпов информационной революции и повсеместных процессах цифровизации.

3. Протокол должен закрепить базовые принципы, на которых будет выстраиваться вся система взаимодействия и сотрудничества государств в сфере противодействия киберрискам

в морском пространстве. Принципы должны не просто содержать общие рекомендации, но и отражать сущностные особенности и специфический характер взаимодействия, с учетом наличия технического аспекта, исходя из определения особого правового статуса объектов нефизического мира, таких как информация, данные, компьютерная система, автоматизированная система управления, цифровой суверенитет, электронные доказательства и др.

Среди возможных принципов может быть предложен принцип **сотрудничества** посредством создания системы координации и обмена информацией (в рамках круглосуточных контактных центров в формате 24/7, включая государственно-частное партнерство).

4. Представляется, что Протокол должен содержать особый сущностный подход к управлению киберрисками, в основу которого должна быть заложена организованная, многоуровневая и многосторонняя система, включающая как технический, так и экономический и социальный аспект, основанная на уважении прав и свобод человека, конечной целью которой является защита людей от угроз цифровой безопасности. Такая система должна охватывать правительства, государственные и частные организации, а также отдельных пользователей и быть реализована на уровне национальных, региональных и международных стратегий.

Считаем, что все вышеобозначенные пункты заложат теоретико-правовую основу взаимодействия и реализации механизма сотрудничества. Но для его успешной практической реализации (другими словами, для воплощения в жизнь) необходима детальная проработка конкретного механизма взаимодействия и осуществления совместной политики по таким значимым направлениям, как оценка факторов риска и уязвимости морской отрасли; трансграничный обмен информацией и данными, содержащимися в цифровой форме; создание единой унифицированной базы электронных доказательств, с учетом особых требований к их обработке, хранению, фиксации и приданию им юридической силы; своевременный (мгновенный) обмен данными о киберинцидентах и мерах борьбы с ними; оценка и анализ факторов риска и киберуязвимостей систем в сфере морского судоходства на Каспии; проработка совместных сценариев потенциальных кибератак с целью обучения персонала и повышения уровня осведомленности и др. По мнению авторов исследования, для эффективной реализации подобного механизма сотрудничества необходимо создание специализированной структуры, в полномочия которой будет входить круглосуточный мониторинг киберинцидентов в морском пространстве Каспийского региона и незамедлительный обмен информацией и данными по типу круглосуточных контактных центров в формате 24/7. Данная структура будет представлять роль координирующего органа, где будет осуществляться сбор всей информации, электронных доказательств, цифровых данных, что позволит осуществлять сотрудничество уполномоченных органов государств.

5. Заключение

В заключение следует отметить, что сектор международных морских перевозок успешно развивается. Согласно статистике, приведенной в обзоре Конференции ООН по торговле и развитию (ЮНКТАД) за 2022 г., сокращение морских перевозок произошло на 0,4 %. При этом в 2023 г. рост объема морских перевозок составил 2,4 %. Отрасль проявляет свою устойчивость, и, согласно прогнозам ЮНКТАД на среднесрочную перспективу (2024–2028 гг.) рост объема морских перевозок будет непрерывным[21]. Для повышения конкурентоспособности морская отрасль постоянно стремится к расширению масштабов и повышению эффективности. Различные экономические, политические, технологические факторы оказывают влияние на показатели работы морского сектора. Одной из таких тенденций является, в частности, распространение цифровых технологий.

Между тем внедрение информационных технологий и автоматизация процесса управления в морских системах делают их потенциально уязвимыми для преступных элементов, использующих достижения информационно-коммуникационных технологий в злонамеренных целях. Обеспечение должного уровня безопасности и

[21] ООН: Общий обзор морского транспорта 2023 г. Издание ООН, выпущенное Конференцией ООН по торговле и развитию. Женева, Швейцария. 2023. URL: https://unctad.org/system/files/official-document/rmt2023overview_ru.pdf (дата обращения: 10.02.2025).

защищенности морских систем в этих условиях требует комплексных мер, включающих не только технико-технологический аспект, но и разработку соответствующей правовой базы как на национальном, так и на международном уровне. Что, в свою очередь, обуславливает необходимость укрепления механизмов сотрудничества между заинтересованными сторонами на уровне правительств государств, представителей морской индустрии, международных организаций, разработчиков технологий, частных компаний и инвесторов. Одним из основополагающих факторов развития Каспийского региона является наличие Каспийского моря, располагающего обширными природными ресурсами и имеющего статус связующей логистической артерии между прикаспийскими территориями и странами Персидского залива. В связи с этим предложенные авторами исследования рекомендации по расширению и конкретизации нормативно-правовой базы в сфере противодействия киберрискам в морском пространстве Каспийского региона в рамках создания системы региональной безопасности представляют особую практическую значимость.

Список литературы

1. Батырь В.А. 2019. Сбалансированный современный особый международно-правовой статус Каспийского моря. – *Lex Russica.* № 9 (154). URL: https://cyberleninka.ru/article/n/sbalansirovannyi-sovremennyi-osobyi-mezhdunarodno-pravovoi-status-kaspii-skogo-morya (дата обращения: 24.02.2025).
2. Бокерия С.А. 2019. Взаимосвязь глобальной и региональной систем безопасности (на примере ООН, ОДКБ и ШОС). – *Вестник международных организаций: образование, наука, новая экономика.* № 14 (1). С. 21-38. DOI: 10.17323/1996-7845-2019-01-02.
3. Говердовская Т.В., Бесчастнова О.В., Крайнюкова Л.М. 2020. Международные стандарты обеспечения кибербезопасности морской отрасли. – *Материалы конференции «Управление в морских системах» (УМС 2020).* С. 171-173. URL: https://www.elibrary.ru/item.asp?id=44719972 (дата обращения: 10.01.2025).
4. Жуковский М.В., Никитенко В.И. 2018. Обеспечение безопасности Каспийского региона: основные проблемы и пути их решения. – *Международное сотрудничество евразийских государств: политика, экономика, право.* № 4 (17). С. 43-54.
5. Каспий: международно-правовые документы. 2018. Под ред. С.С. Жильцова. Москва: Международные отношения. 568 с. URL: https://ibooks.ru/bookshelf/371567/reading (дата обращения: 21.02.2025).
6. Кулагина Л.М., Дунаева Е.В. *Россия и Иран: история формирования границ.* 2-е изд., доп. Москва: Гуманитарий, 2007. 184 с. URL: https://book.ivran.ru/f/kulagina-dunayeva---russia-and-iran-m-2007.pdf (дата обращения: 20.02.2025).
7. Курылев К.П., Казанчев Д.В. 2013. Стратегическая концепция НАТО 2010 года в контексте обеспечения безопасности в Европе. – *Вестник Российского университета дружбы народов. Серия: Международные отношения.* № 1. С. 11-23.
8. Кущенко А.А. Реализация решений V саммита Прикаспийских государств: проблемные аспекты. – *Сборник материалов Международной научной конференции.* 10 декабря 2020 г. г. Астрах. Москва: Русайнс, 2021. 118 с. URL: https://book.ru/book/940609 (дата обращения: 21.02.2025).
9. Семенов С.А. 2018. Кибербезопасность морского и речного транспорта. – *Транспорт Российской Федерации. Журнал о науке, практике, экономике.* № 1 (74). С. 43-46.
10. Старкова Л.М. 2022. Правовые основы обеспечения информационной безопасности Каспийского региона. – *Каспий и глобальные вызовы. Материалы Международной научно-практической конференции.* Астрахань: Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Астраханский государственный университет». С. 686-690.
11. Karaś A. 2023. Maritime Industry Cybersecurity: A Review of Contemporary Threats. – European Research Studies Journal XXVI. Issue 4. P. 921-930. URL: https://www.researchgate.net/publication/376701918_Maritime_Industry_Cybersecurity_A_Review_of_Contemporary_Threats (accessed date: 19.02.2025).
12. Düzenli E. 2024. Conducting An Analysis of Maritime Cybersecurity Incidents. – *Turkish Journal of Maritime and Marine.* Sciences 10. (Özel Sayı: 1). URL: https://www.researchgate.net/publication/384263903_Conducting_An_Analysis_of_Maritime_Cybersecurity_Incidents (accessed date: 20.02.2025).
13. Hopcraft R., Martin K. 2018. Effective maritime cybersecurity regulation – the case for a cyber code. – *Journal of the Indian Ocean Region.* № 14 (3). P. 1-13. DOI: 10.1080/19480881.2018.1519056.
14. Tam K., Jones K. 2018. Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping. – *Journal of Cyber Policy.* № 3 (2). P. 1-18. DOI: 10.1080/23738871.2018.1513053.

References

1. Batyr' V.A. Sbalansirovannyĭ sovremennyĭ osobyĭ mezhdunarodno-pravovoĭ status kaspiĭskogo morja [Balanced modern special international legal status of the Caspian Sea]. – *Lex Russica.* 2019. № 9 (154). URL: https://cyberleninka.ru/article/n/sbalansirovannyi-sovremennyi-osobyi-mezhdunarodno-pravovoi-status-kaspii-skogo-morya (data obrashhenija: 24.02.2025). (In Russ.)

2. Bokerija S.A. Vzaimosvjaz' global'noj i regional'noj sistem bezopasnosti (na primere OON, ODKB i ShOS) [Interrelationship of global and regional security systems (UN, CSTO and SCO)]. – Vestnik mezhdunarodnyh organizacij: obrazovanie, nauka, novaja jekonomika [The Messenger of international organizations: education, science, new economy]. 2019. № 14 (1). P. 21-38. DOI: 10.17323/1996-7845-2019-01-02. (In Russ.)
3. Düzenli E. Conducting An Analysis of Maritime Cybersecurity Incidents. – *Turkish Journal of Maritime and Marine.* Sciences 10. (Özel Sayı: 1). 2024. URL: https://www.researchgate.net/publication/384263903_Conducting_An_Analysis_of_Maritime_Cybersecurity_Incidents (accessed date: 20.02.2025).
4. Goverdovskaja T.V., Beschastnova O.V., Krajnjukova L.M. Mezhdunarodnye standarty obespechenija kiberbezopasnosti morskoj otrasli [International Standards for Cybersecurity in the Marine Industry]. – *Materialy konferencii «Upravlenie v morskih sistemah» (UMS 2020) [Conference Materials Management in Marine Systems (PMS 2020)].* 2020. P. 171-173. URL: https://www.elibrary.ru/item.asp?id=44719972 (data obrashhenija: 10.01.2025). (In Russ.)
5. Hopcraft R., Martin K. Effective maritime cybersecurity regulation – the case for a cyber code. – *Journal of the Indian Ocean Region.* 2018. № 14 (3). P. 1-13. DOI: 10.1080/19480881.2018.1519056.
6. Karaś A. Maritime Industry Cybersecurity: A Review of Contemporary Threats. – *European Research Studies Journal XXVI.* 2023. Issue 4. P. 921-930. URL: https://www.researchgate.net/publication/376701918_Maritime_Industry_Cybersecurity_A_Review_of_Contemporary_Threats (accessed date: 19.02.2025).
7. *Kaspij: mezhdunarodno-pravovye dokumenty [The Caspian Sea: international legal documents].* Pod red. S.S. Zhil'cov. Moscow: Mezhdunarodnye otnoshenija. 2018. 568 p. URL: https://ibooks.ru/bookshelf/371567/reading (data obrashhenija: 21.02.2025). (In Russ.)
8. Kulagina L.M., Dunaeva E.V. *Rossija i Iran: istorija formirovanija granic [Russia and Iran: the history of the formation of borders].* 2-e izd., dop. Moscow: Gumanitarij. 2007. URL: https://book.ivran.ru/f/kulagina-dunaeva---russia-and-iran-m-2007.pdf (data obrashhenija: 20.02.2025). (In Russ.)
9. Kurylev K.P., Kazanchev D.V. Strategicheskaja koncepcija NATO 2010 goda v kontekste obespechenija bezopasnosti v Evrope [NATO Strategic Concept 2010 in the context of ensuring security in Europe]. – *Vestnik Rossijskogo universiteta druzhby narodov. Serija: Mezhdunarodnye otnoshenija [The Bulletin of the Russian University of Friendship of Nations. Series: International relations].* 2013. № 1. P. 11-23. (In Russ.)
10. Kushhenko A.A. Realizacija reshenij V sammita Prikaspijskih gosudarstv: problemnye aspekty [Implementation of the decisions of the V Summit of the Caspian Littoral States: problematic aspects]. – *Sbornik materialov Mezhdunarodnoj nauchnoj konferencii. 10 dekabrja 2020 g. [Collection of materials of the International Scientific Conference. December 10, 2020].* Astrakh: collection of articles. Moscow: Rusains, 2021. 118 p. URL: https://book.ru/book/940609 (дата обращения: 21.02.2025). (In Russ.)
11. Semenov S.A. Kiberbezopasnost' morskogo i rechnogo transporta [Maritime and river transport cybersecurity]. – *Transport Rossijskoj Federacii. Zhurnal o nauke, praktike, jekonomike [Transport of the Russian Federation. Journal on science, practice, economy].* 2018. № 1 (74). P. 43-46. (In Russ.)
12. Starkova L.M. Pravovye osnovy obespechenija informacionnoj bezopasnosti Kaspijskogo regiona [The legal framework for ensuring the information security of the Caspian region]. – *Kaspij i global'nye vyzovy. Materialy Mezhdunarodnoj nauchno-prakticheskoj konferencii [The Caspian Sea and Global Challenges. Proceedings of the International Scientific and Practical Conference]* Astrahan': Federal'noe gosudarstvennoe bjudzhetnoe obrazovatel'noe uchrezhdenie vysshego professional'nogo obrazovanija «Astrahanskij gosudarstvennyj universitet». 2022. P. 686-690. (In Russ.)
13. Tam K., Jones K. Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping. – *Journal of Cyber Policy.* 2018. № 3 (2). P. 1-18. DOI: 10.1080/23738871.2018.1513053.
14. Zhukovskij M. V., Nikitenko V. I. Obespechenie bezopasnosti Kaspijskogo regiona: osnovnye problemy i puti ih reshenija [Security in the Caspian region: main problems and ways to solve them]. – *Mezhdunarodnoe sotrudnichestvo evrazijskih gosudarstv: politika, jekonomika, pravo [International cooperation of the Eurasian states: politics, economy, law].* 2018. № 4 (17). P. 43-54. (In Russ.)

Информация об авторах

Татьяна Владимировна ГОВЕРДОВСКАЯ
кандидат юридических наук, доцент, заведующая кафедрой государственно-правовых дисциплин и международного права Астраханский государственный университет им. В.Н. Татищева

Татищева ул., 20а, Астрахань, 414056, Российская Федерация

tara_goya@bk.ru
ORCID: 0000-0001-6340-4764

About the Authors

Tatyana V. GOVERDOVSKAYA
Candidate of Law Sciences, Associate Professor, Head of the Department of State and Legal Disciplines and International Law Astrakhan State University

20a, Tatishcheva st., Astrakhan, Russian Federation, 414056

tara_goya@bk.ru
ORCID: 0000-0001-6340-4764

Ляйсян Маратовна СТАРКОВА
старший преподаватель кафедры государственно-правовых дисциплин и международного права Астраханский государственный университет им. В.Н. Татищева

Татищева ул., 20а, Астрахань, 414056, Российская Федерация

5leska5@mail.ru
ORCID: 0000-0002-4411-6510

Lyasyan M. STARKOVA,
Senior Lecturer of the Department of State and Legal Disciplines and International Law Astrakhan State University

20a, Tatishcheva st., Astrakhan, Russian Federation, 414056

5leska5@mail.ru
ORCID: 0000-0002-4411-6510