DOI 10.22394/2073-2929-2022-04-68-81

К 40-летию принятия Конвенции ООН по морскому праву[1]

Роль цифровой трансформации в борьбе с преступностью на море

Кириленко В. П.*, Алексеев Г. В.
Северо-Западный институт управления РАНХиГС, Санкт-Петербург, Российская Федерация
* e-mail: v.vvaas@yandex.ru
ORCID: https://orcid.org/0000-0003-4445-1682

РЕФЕРАТ

Борьба с преступностью на море предполагает создание современной системы безопасности в морских портах, территориальном море и прилежащей зоне на всем протяжении транспортных коридоров в условиях интенсивного судоходства.

Цель. Оценка влияния цифровой трансформации на борьбу с преступностью на море.

Задачи. Во-первых, охарактеризовать воздействие цифровых технологий на характер пиратских нападений и других морских правонарушений, которые являются актуальными угрозами для морской инфраструктуры. Во-вторых, проанализировать влияние современных мер по борьбе с морской преступностью на экономику морских портов, судоходных компаний и других субъектов морского бизнеса. В-третьих, рассмотреть роль администрации морского порта и частных военных компаний в борьбе с правонарушениями на море.

Методология. Исследование проводится формально-правовой и сравнительно-правовой методикой с применением обзорно-аналитического подхода.

Результаты. Анализ данных показывает, что администрации морских портов заинтересованы в оптимизации затрат на безопасность за счет создания удобной цифровой системы управления приморской инфраструктурой. Системы безопасности и логистические решения зависят от эффективности цифровых технологий, внедряемых в интересах обеспечения безопасности мореплавания. Конвенция по охране человеческой жизни на море (СОЛАС-74/88), дополненная Международным кодексом безопасности судов и портовых средств (ISPS) в 2004 г., предусматривает универсальную систему морской безопасности, вместе с тем имплементации этих норм в ряде регионов Мирового океана недостаточно для нейтрализации приморских криминальных угроз.

Выводы. В условиях цифровизации меры по борьбе с преступностью на море приводят к значительным затратам, так как требуют сложной технологической инфраструктуры на судах и в портах. Нормы морского права, нацеленные на борьбу с пиратством и контрабандой, следует имплементировать на национальном уровне с учетом социально-экономических особенностей развития приморской инфраструктуры. Поскольку негативные экономические тренды влекут за собой рост криминальной активности, постольку в борьбе с пиратством и контрабандой не следует приносить в жертву экономические интересы субъектов торгового мореплавания.

Ключевые слова: безопасность, пиратство, контрабанда, терроризм, ЮНКЛОС, СОЛАС, портовый контроль

Для цитирования: Кириленко В. П., Алексеев Г. В. Роль цифровой трансформации в борьбе с преступностью на море. *Евразийская интеграция: экономика, право, политика.* 2022;16(4): 68-81. https://doi.org/10.22394/2073-2929-2022-04-68-81

[1] Конвенция ООН по морскому праву была подписана в ямайском городе Монтего-Бей 10 декабря 1982 г. Вступив в силу 16 ноября 1994 г., Конвенция приобрела универсальный императивный характер, ее текст ратифицирован 168 участниками и приобрел широкую известность в качестве конституции морей. (The UN Convention on the Law of the Sea was signed in the Jamaican city of Montego Bay December 10, 1982. Having entered into force on November 16, 1994, the Convention acquired a universal imperative character, its text was ratified by 168 parties and became widely known as the constitution of the seas.)

The Role of the Digital Transformation in the Fight against Crime at Sea

Viktor P. Kirilenko[*], **Georgy V. Alekseev**
North-West Institute of Management of RANEPA, Saint Petersburg, Russian Federation
[*] e-mail: v.vvaas@yandex.ru
ORCID: https://orcid.org/0000-0003-4445-1682

ABSTRACT
Crime control at the sea involves public activities to create a modern security system in seaports, at the territorial sea and the adjacent zone throughout the sea corridors, as well as in the open sea on sea routes with intensive shipping.
Aim. Impact assessment of digital transformation on maritime crime control.
Tasks. Firstly, to characterize the impact of digital technologies on the nature of pirate attacks and other maritime offenses, which are actual threats to the maritime infrastructure. Secondly, to analyze the impact of modern measures to combat maritime crime on the economy of seaports, shipping companies and other maritime business entities. Thirdly, to demonstrate the role of the seaport administration and private military companies in the fight against offenses at sea.
Methods. The study is carried out by formal legal and comparative legal methodology using a review-analytical approach.
Results. Data analysis shows that the administrations of seaports are interested in optimizing security costs by creating a convenient digital management system for the coastal infrastructure. Security systems and logistics solutions depend on the effectiveness of digital technologies implemented in the interests of ensuring the safety of navigation. The Convention for the Safety of Human Life at Sea (SOLAS-74/88), supplemented by the International Ship and Port Facility Security Code (ISPS) in 2004, provides for a universal maritime security system, however, the implementation of these standards in a number of regions of the World Ocean is not enough to neutralize coastal criminal threats.
Conclusion. In the context of digitalization, measures to combat crime at sea lead to significant costs, as they require complex technological infrastructure on ships and in ports. The norms of the law of the sea aimed at combating piracy and smuggling should be implemented at the national level, taking into account the socio-economic features of the maritime infrastructure development. Since negative economic trends entail an increase in criminal activity, the economic interests of commercial shipping entities should not be sacrificed in the fight against piracy and smuggling.
Keywords: security, piracy, smuggling, terrorism, UNCLOS, SOLAS, port control
For citing: Kirilenko V. P. , Alekseev G. V. The Role of the Digital Transformation in the Fight against Crime at Sea. *Eurasian Integration: Economics, Law, Politics.* 2022;16(4): 68-81. (In Rus.)
https://doi.org/10.22394/2073-2929-2022-04-68-81

Введение

Президент Российской Федерации В. В. Путин принял участие в Дебатах высокого уровня в Совете безопасности ООН по морской безопасности 9 августа 2021 г. и предложил создать специальную структуру в ООН по борьбе с морской преступностью, отметив, что «было бы полезно на регулярной основе осуществлять обмен наработками и наилучшими практиками противодействия пиратству, вооруженному разбою и другой криминальной активности на море»[1]. Такая инициатива во многом определяется тем, что, несмотря на усилия Управления ООН по наркотикам и преступности (УНП ООН) при реализации

[1] Дебаты высокого уровня в Совбезе ООН по морской безопасности. 9 августа 2021 года, Московская область, Ново-Огарево [Электронный ресурс] // Официальный сайт Президента России. URL: http://www.special.kremlin.ru/events/president/transcripts/66352 (дата обращения: 01.11.2022).

Глобальной программы по борьбе с морской преступностью (Global Maritime Crime Programme)[1], отмечается значительный рост преступной активности, направленной против интересов субъектов торгового мореплавания.

Комитет по безопасности на море Международной морской организации (ИМО) принял Резолюцию MSC.428 (98) — Управление киберрисками на море в системах управления безопасностью — 16 июня 2017 г. Это произошло после того, как семнадцать из 76 грузовых терминалов Maersk были заражены компьютерным вирусом NotPetya. Ущерб составил около 300 млн евро. В 2018 г. порты Барселоны и Сан-Диего подверглись кибератакам. В 2020 г. австралийская логистическая группа Toll Group дважды была атакована хакерами[2]. Около 64% морских компаний, опрошенных в 2020 г. журналом Safety at Sea magazine и BIMCO в исследовании Maritime Cybersecurity Survey, заявили, что у их компаний есть план обеспечения непрерывности бизнеса на случай кибер-инцидента[3].

Концепция морской безопасности сильно изменилась после 11 сентября 2001 г. После теракта на XXII сессии Ассамблеи Международной морской организации (ИМО) было единогласно принято решение разработать новые меры по защите судов и портовых сооружений. Международный кодекс безопасности судов и портовых средств (ISPS Code) от 1 июля 2004 г. является поправкой к Конвенции по охране человеческой жизни на море (СОЛАС) 1974/1988 и включает в себя всеобъемлющий перечень мер по повышению безопасности судов и портовых средств. Хотя противодействие террористическим угрозам остается важной частью безопасности на море, очевидно, что в тени террористической угрозы цифровая трансформация вызвала к жизни новые экономические и криминальные вызовы для морской отрасли [33; 40].

Конвенция ООН по морскому праву (UNCLOS) 1982 г. для эффективной борьбы с морской преступностью предусматривает ряд юридических запретов: на перевозку рабов (ст. 99), незаконную торговлю наркотиками или психотропными веществами (ст. 108), несанкционированное вещание из открытого моря (ст. 109), а также устанавливает обязанность сотрудничать в пресечении пиратства (ст. 100), Конвенция дает определение пиратству (ст. 100) и в определенной степени регулирует порядок пресечения угрозы пиратских нападений (ст. 101–107). Очевидно, что за сорок лет, прошедших с момента подписания Конвенции ООН по морскому праву, изменилась не только структура морской преступности, но и актуализировались принципиально новые угрозы, связанные с цифровой трансформацией приморской инфраструктуры и судоходства.

Криминогенные угрозы в условиях цифровой трансформации мореплавания

В условиях цифровизации юридический формализм как рациональная правовая основа обеспечения безопасности судоходства может вступать в противоречие с экономическими интересами морских транснациональных корпораций. Кодекс ISPS 2004 г. предписывает правительствам, судоходным компаниям, судовому персоналу и персоналу портов обязанности «обнаруживать угрозы безопасности и принимать превентивные меры против инцидентов безопасности, затрагивающих суда или портовые сооружения, используемые в международной торговле». В дополнение к новым правилам, включенным в главу XI-2 СОЛАС-74, и частям A и B Кодекса ISPS дипломатическая конференция приняла поправки к существующим правилам СОЛАС-74, способствующие ускорению выполнения требований по оснащению судов системами автоматической идентификации, а также новые правила для включения в главу XI-1 СОЛАС-74, касающуюся идентификационных номеров судов и необходимости ведения журнала непрерывной регистрации истории судна. Все эти меры по-разному сказываются на экономической безопасности субъектов торгового мореплавания.

---

[1] Maritime Crime [Электронный ресурс] // United Nations. URL: https://www.unodc.org/unodc/ru/piracy/index.html (дата обращения: 01.11.2022).

[2] AMMITEC. Empirical Analysis of Cyber Security Maturity in the Maritime Industry. 2021 [Электронный ресурс] // Association of Maritime Managers in Information Technology & Communications. URL: https://smartmaritimenetwork.com/wp-content/uploads/2021/07/AMMITEC-Cyber-Security-Survey-2021.pdf (дата обращения: 01.11.2022).

[3] Maritime Cyber Survey 2018 — the results. Cyber Security Survey Shows More Action is Needed in the Industry. 2018 [Электронный ресурс] // BIMCO. URL: https://www.bimco.org/news/priority-news/20180924-cyber-security-survey (дата обращения: 01.11.2022).

Система безопасности морских портов включает в себя организационные меры и технические средства. Небрежность и попустительство в морской среде, где принято полагаться на цифровые технологии, могут привести к инцидентам, не менее разрушительным, чем пиратские нападения и террористические акты. Взрывы в порту Бейрута (Ливан) 4 августа 2020 г., в результате которых погибло 210 чел., около 300 тыс. жителей остались без крова, были связаны с нарушением правил хранения в районе порта около трех килотонн нитрата аммония, конфискованного с судна Rhosus в 2013 г. Отсутствие эффективной системы государственного контроля за операциями в морском порту привело не только к социально-экономическим потерям и тяжелому политическому кризису в Ливане, но и способствовало росту массового психоза в информационном пространстве. Взрыв в Бейрутском порту и его последствия для жизни граждан оказали негативное влияние на экономику и архитектуру города [34].

Сегодня цифровая среда российских портов стремительно развивается, но этого недостаточно для достижения конкурентных позиций по сравнению с иностранными портами [14; 42]. В начале процесса цифровизации морских портов в 1993 г. беспилотные транспортные средства впервые были использованы для обработки контейнеров в порту Роттердама. Сегодня там автоматизированные беспилотные железнодорожные козловые краны (ARMGs) и беспилотные управляемые транспортные средства (AGV) широко используются для горизонтальной передачи контейнеров с причала [17; 37].

В современной доктрине морской безопасности «порты — это многоуровневые лиминальные (транзитные. — *Примеч. авт.*) пространства. С одной стороны, они являются воротами в город, а с другой — обеспечивают выход к морю» [40, с. 49]. Таким образом, к коммерческим операциям внутри порта должны применяться как нормативные акты прибрежных государств, так и положения международного права. Если «морские порты являются динамичными пространствами, где как законные, так и незаконные операторы и пользователи стремятся извлекать выгоду из социальных, политических, экономических и технологических изменений, чтобы оставаться конкурентоспособными» [40, с. 111], то конкурентные преимущества портовых услуг являются частью системы безопасности только потому, что риски криминализации и банкротства рассматриваются как главная угроза для всех субъектов морского бизнеса.

Цифровизация действительно «выводит морскую отрасль за ее традиционные пределы и предоставляет множество новых возможностей для повышения производительности, эффективности и устойчивости логистики» [27]. С одной стороны, парадигмы «умных портов» и «беспилотного судоходства» могут предоставить новые возможности для бизнеса в морской отрасли, и во многом справедливо, что «концепция „умных портов“ ... направлена на внедрение современных информационных технологий для обеспечения лучшего планирования и управления внутри портов и между ними» [27]. С другой стороны, в некоторых случаях цифровая среда в морском порту и на судах может вызвать значительные проблемы с безопасностью из-за эксплуатационных расходов на компьютерное программное обеспечение, низкого уровня ответственности за решения искусственного интеллекта и возможностей для использования злоумышленниками цифровых технологий при подготовке традиционных правонарушений на море: морского грабежа и пиратских нападений, которые были всесторонне исследованы профессором В. Ф. Сидорченко [9; 10; 11; 12]. Очевидно, что цифровые технологии в морском порту направлены на международное сотрудничество в борьбе с преступностью, так как «терроризм и пиратство на морском транспорте чаще всего являются преступлениями международного характера...» [3].

Ученые из Восточной Европы Адриана Агатич (Adrijana Agatić) и Инес Коланович (Ines Kolanović) последовательно доказывают, что «поскольку качество обслуживания в морских портах не является предписанным и строго определенным, следует учитывать важность цифровизации, которая включает в себя пересмотр факторов качества обслуживания в морских портах» [15], а также потому, что «ведущие морские порты мира, особенно ведущие европейские морские порты, признали возможности цифровых технологий в предоставлении качественных услуг морского порта», их администрации инвестируют во внедрение «цифровых технологий в морскую логистику» [15; 17; 26]. Если цифровые технологии могут повысить безопасность и эффективность операций в морских портах и за их пределами, то «различия в уровне развития конкретной страны влияет на качество внедрения новых технических и технологических достижений, что приводит к разным уровням цифровизации каждого конкретного морского порта» [34].

Нет сомнений в том, что «цифровая трансформация ... требует внедрения новых методов, моделей и инструментов и часто подразумевает новые подходы, бизнес-модели и новые навыки, которые помогут транспортным компаниям и заинтересованным сторонам морских портов оставаться конкурентоспособными в современных условиях, добиваться роста и отражать конкурентные угрозы» [27]. В то время как передовой шведский порт Гетеборг внедряет цифровой инструмент планирования причалов Allberth в работу отдела портового контроля, который теперь принимает все вызовы на объекте, адресованные координаторам по охране на его энергетическом терминале [27], многие другие портовые администрации недооценивают влияние цифровых технологий на современную морскую инфраструктуру [28].

Искусственный интеллект играет все более значительную роль в морских портах. Широко признается, что «морские порты являются наиболее критической точкой в морской логистической цепочке из-за ее мультимодального и сложного характера» [37], где «пространство данных морских портов (Seaport Data Space, SDS), основанное на эталонной архитектурной модели промышленного пространства данных (Industrial Data Space, IDS), обеспечивает безопасное пространство для обмена данными и создает условия для работы умного транспорта на мультимодальном терминале» [Там же, с. 4372]. Сегодня заинтересованные стороны каждого морского порта внедряют «средства IDS для участия в SDS и обмена данными», при этом «архитектура больших данных интегрирована для управления массивными данными, разделяемыми в SDS, и извлечения полезной информации для улучшения процесса принятия решений» [Там же], фактически любая логистическая операция становится частью цифровой среды из морского порта. Такая логика дает администрации порта возможность использовать все системы видеоконтроля как часть инфраструктуры безопасности и предоставлять новые услуги для грузовладельцев.

В ближайшем будущем искусственный интеллект будет управлять логистикой морского порта путем адаптивной оптимизации транспортного пути для оптимального планирования и с целью улучшения выбора маршрута транспорта в акватории порта. Даже на сегодняшний день результаты моделирования показывают, что несколько методов обладают «хорошей адаптивной производительностью и сильной способностью управления оптимизацией маршрутов для оптимального планирования транспортных путей в международных логистических парках прибрежных портов» [41, с. 1125]. Цифровизация и широкий спектр связанных с ней новых технологий «эволюционировали за последнее десятилетие и привели к различным вариантам использования этих технологий с поддержкой данных в различных отраслях, таких как производство, информационные технологии и логистика» [36]. Цифровая среда всегда является результатом государственно-частного партнерства, но использование инфраструктуры общественного контроля в частных целях в некоторых случаях может стать угрозой безопасности.

Приватизация портов может быть представлена как метод повышения их эффективности, однако этот процесс создает и ряд криминогенных факторов. Британский ученый Колин Дэвис (Colin Davis) заметил, что «множество портов и транспортные проблемы во внутренних районах делают приватизацию больше похожей на принятие желаемого за действительное, чем на политику, которая может сработать» [20, с. 154]. С точки зрения безопасности представляется, что тенденция приватизации в морской отрасли может быть опасной для противодействия преступной деятельности и таит в себе некоторые экономические риски. В российских рыночных реалиях низкий уровень государственного участия может быть опасным из-за отсутствия возможности у частной администрации морского порта по противодействию киберпреступности [4]. Морские порты всегда занимают позицию между государственным и частным секторами национальной экономики [43]. В этой ситуации не только искусственному интеллекту, но и администрации порта достаточно трудно решить, каким интересам (частным или общественным) они должны следовать.

Для сохранения статус-кво между государственными и частными интересами при цифровизации морских портов необходимо использовать как негативные, так и позитивные подходы к обеспечению безопасности. Термины «негативная» и «позитивная» безопасность используются норвежским ученым Гунхильд Хогенсен Йорв (Gunhild Hoogensen Gjørv), чтобы внести ясность в ее подход к обеспечению безопасности с участием многих субъектов, который может быть весьма полезен в случае безопасности морских портов. Позитивные перспективы безопасности, которые опираются на ненасильственные ме-

ры, обеспечивают акцент на контексте, ценностях и методах обеспечения безопасности, которые укрепляют доверие, а негативные аспекты безопасности обычно идентифицируются через риски и угрозы защищаемым (часто законом) ценностям [25].

Профессор Ярин Эски (Yarin Eski) из Амстердамского свободного университета (Vrije Universiteit Amsterdam) в своих исследованиях вопросов безопасности на море представляет криминологическое понимание того, как вопросы безопасности и процедуры интегрируются в повседневную жизнь тех, кто защищает промышленные портовые объекты [22; 23]. Его работы на такие темы, как управление безопасностью портов, межведомственная полицейская деятельность, кражи в портах, незаконный оборот наркотиков, контрабанда, работорговля, терроризм и пиратство, стали существенным вкладом в изучение борьбы с транснациональной преступностью на море. Профессор Эски предлагает этнографический подход к безопасности портов и приморских пространств, и поэтому он продвигает сравнительные исследования в области морской безопасности [22].

Противодействие морской преступности и, в частности, пиратству должно осуществляться с привлечением силовых ведомств. Независимо от географического расположения морского порта кадровая политика является центральным вопросом безопасности на приморских пространствах. Безопасность морского транспорта обеспечивается персоналом, охраной складских помещений в зонах перевалки грузов, морских и речных портов, экипажами судов и т.д. При обеспечении безопасности морского транспорта учитывается тот факт, что пираты и морские террористы, скорее всего, являются профессиональными моряками с военной подготовкой [40]. Криминальные структуры на море в основном интересуются экономической уязвимостью инфраструктуры, то есть они ориентированы на кражу груза (а иногда и судна) для их последующей перепродажи или требования выкупа.

Преступность в морских портах развивающихся государств

Морские порты как часть структуры морского транспорта не только играют роль «интерфейсов» между сухопутными перевозчиками и судами, они также обеспечивают безопасность на определенном участке транспортной инфраструктуры [18; 26]. Морские порты становятся местом ведения бизнеса для многих компаний и бизнес-структур. Большинство стивидорных компаний являются акционерными предприятиями, которые обеспечивают все операции по приему и отправке грузов, перевозимых морскими транспортными судами. Ввиду неизбежной цифровизации коммерческой документации внедрение мер защиты информации в цифровую среду морского порта является краеугольным камнем современной безопасности на море.

Наблюдение за управлением портами развивающихся государств показывает участие целого ряда различных коммерческих субъектов в обеспечении безопасности портов и морских границ. Например, тематическое исследование системы управления в порту Момбаса показывает «распределение власти между государственными, частными и криминальными интересами» в Кении [30]. Как государственные, так и негосударственные субъекты здесь получают прибыль от организации контейнерного хранения и участвуют в разработке по сути коррупционных правил грузооборота в морских портах [30]. Безопасность морских портов в Гане сталкивается почти с такими же угрозами [21]. Исследование системы безопасности в порту Белаван «демонстрирует важную, хотя и противоречивую роль, которую частные поставщики услуг безопасности играют в управлении безопасностью в Индонезии» [38]. Существует большое количество государственных и негосударственных субъектов, вовлеченных в обеспечение безопасности. Среди субъектов — охранники, нанятые государственным портовым оператором и частными военными и охранными компаниями (ЧВОК). Участие большого количества различных типов государственных и негосударственных учреждений фактически ослабило безопасность в Белаване [38]. Милитаризация охраны порта несет в себе очевидные угрозы формирования пиратского сообщества из числа бывших сотрудников ЧВОК.

Исследование приватизации портов Нигерии показывает, что финансовые проблемы приводят к снижению уровня безопасности [16]. Негосударственные учреждения вовлечены в портовый бизнес,

чтобы снизить стоимость портовых услуг для заинтересованных сторон, снизить затраты правительства на поддержку портового сектора и привлечь участие частного бизнеса. Хотя конкретные меры по цифровой трансформации мореплавания указывают на последовательный рост технической эффективности, «есть некоторые проблемы, которые влияют на работу портов: высокие портовые сборы, задержки в оформлении грузов, многократное налогообложение и развитие интермодальных перевозок» [16]. Управление тайваньскими торговыми портами приводит к значительно высокому уровню морских потерь, смертельных исходов и травм в результате аварий на паромах во время экономического спада. Усиление безопасности судоходства в порту связано с действиями администрации морского порта, нацеленными на улучшение экономики, так как логистические проблемы в судоходной отрасли стимулируют руководство порта к рискам. На практике приходится, например, «разрешать погрузку и разгрузку небольших судов, которые не соответствуют стандарту причала» [31, с. 201].

Во время любого экономического кризиса отрасль морских портов сталкивается с перебоями в торговой активности и угрозами мобильности. Угрозы конкурентным преимуществам порта вовлекают множество негосударственных субъектов в систему безопасности порта и создают значительные, но не критические угрозы безопасности мореплавания. В случае экономического спада активизируются криминальные структуры, портовая инфраструктура остается на низком уровне безопасности и угрозы криминализации постоянно растут.

Кризис, с которым столкнулся морской бизнес в связи с пандемией коронавирусной инфекции Covid-19, подтверждает взаимосвязь экономической эффективности и безопасности мореплавания. В результате пандемии пострадали многие секторы мировой экономики, и международное судоходство не стало исключением. Поскольку морские суда в ходе своей деятельности заходят в иностранные порты, «цепная реакция» закрытия портов прибрежными государствами вызвала проблемы как для судовладельцев, так и для людей на борту (членов экипажа и пассажиров), а также для работников морских портов. Пассажирские круизные лайнеры, которым власти иностранных портов стали отказывать в заходе и высадке пассажиров, ощутили на себе особенно серьезные последствия карантина в иностранных портах. Хотя практика иностранных и российских портов в условиях пандемии может существенно отличаться даже в пределах одного и того же прибрежного государства [2], в целом пандемия отрицательно сказалась на экономическом аспекте портовой безопасности.

Российская морская отрасль как часть мировой морской экономики переживала стагнацию с начала пандемии, а затем впала в рецессию. При пандемии Covid-19 закрытие портов вызвало беспрецедентный гуманитарный кризис на море. В качестве угрозы безопасности широко рассматриваются несоответствия в объективной и юридической реальности. Так, в частности, «в то время как лицам, находящимся на море, предоставляется значительная защита прав в международном праве, права и обязанности государств часто вступают в противоречие, в результате чего лица, находящиеся на море, могут оказаться в чем-то вроде правового вакуума» [24], данные обстоятельства подтверждаются также и стратегическим отчетом Росморпорта за 2020 г.[1]

Некоторые меры безопасности могут зависеть от профиля морского порта. Риски экологической преступности, связанной с загрязнением Мирового океана, имеют особое значение при транспортировке нефтепродуктов. Результаты статистических данных о пожарах на угольных предприятиях позволяют определить величину потенциального риска в морском порту с комбинированными складами нефти и угля [7]. Такие меры безопасности, как способы безопасной эвакуации людей с судов, пришвартованных у пассажирских причалов, важны в транзитных портах, которые несут высокий уровень террористической угрозы [32]. Высоки риски для пассажирских портов, так как «современные пираты, например сомалийские, как бы вернулись к античному спасанию “по-пиратски”, поскольку они, захватывая людей и имущество, не присваивают их, а обменивают на денежный выкуп…» [12, с. 90].

Безопасность морских портов всегда находилась под угрозой проникновения, манипуляций и использования контрабандистами наркотиков, похитителями грузов, пиратами, преступными организаци-

[1] Strategic Report 2020 [Электронный ресурс] // РОСМОРПОРТ. URL: https://www.rosmorport.ru/about/disclosure/report/presentation/strategicheskiy-otchet/index.html (дата обращения: 01.11.2022).

ями и террористами. Целями этих преступных элементов являются терминалы, суда, грузы, контейнеры, оборудование и персонал [9; 10; 33]. Цифровизация отрасли морских портов вызвала к жизни новые угрозы безопасности, такие как кибератаки и нарушения логистики в результате использования информационных технологий криминальными структурами. Меняющийся технологический уклад всегда требует особых усилий, направленных на поддержание квалификации персонала, доверия клиентов, предотвращения контрабанды и грабежа [39; 40]. Секьюритизация таких усилий является частью портовой инфраструктуры и системы безопасности морских портов в эпоху цифровых технологий.

Цифровые технологии в борьбе с преступностью на море

В морском праве «безопасность портов является краеугольным камнем для внедрения нового международного режима безопасности на морском транспорте в том, что касается защиты пользователей портов и морских коридоров, а также защиты морских судов» [17]. В Европейском союзе Кодекс ISPS имплементирован посредством Регламента 725/2004, который был последовательно распространен на все портовые зоны ЕС Директивой 2005/65/CE. В соответствии с Директивой все морские порты Европейского союза, действующие в соответствии с национальным законодательством, признаются важнейшими интермодальными узлами в сети грузовых и пассажирских перевозок, а также становятся компьютеризированными пунктами пограничного контроля [Там же].

Цифровизация торговли привела к изменению масштаба морского бизнеса, что нарушило баланс сил между компаниями, занимающимися онлайн контейнерными морскими перевозками, и логистической цепочкой, проходящей через европейские морские порты. Крупнейший порт Европы в Роттердаме в настоящее время активно использует цифровые решения, но все еще есть коррумпированные «сотрудники, которые сыграли определенную роль в незаконной торговле наркотиками, будучи вовлеченными в так называемые случаи грабежа» [23, с. 371]. Цифровые технологии позволяют операторам составлять расписание погрузки и отправления судов [19], но они не в состоянии остановить преступную деятельность. Правовые нормы по безопасности на море, в частности Инициатива по безопасности контейнеров (CSI), оказывают влияние на конкуренцию на рынке морских перевозок, однако все инициативы по обеспечению безопасности в морских портах ЕС [44] имеют региональную специфику и практически не действуют вне юрисдикции ЕС.

Для любого морского предприятия криминализация бизнеса, пиратство и нарушение логистики могут стать критическими угрозами. Хотя преступность широко признана угрозой общественной безопасности, а экономика портов, морских перевозчиков и рыболовных предприятий может выглядеть как проблема частного характера, сравнительные исследования показывают, что промышленный спад всегда способствует росту организованной преступности. Таким образом, благополучие морских предприятий — это залог эффективного противодействия критическим криминогенным угрозам на море.

Итальянский профессор криминологии Анна Серджи (Anna Sergi) в своем исследовании системы защиты морских портов от контрабанды наркотиков доказывает, что «роли при импорте и методы обеспечения безопасности меняются постоянно и быстро» [39]. Цифровизация морской отрасли делает актуальным наиболее типичное виртуальное преступление — мошенничество в форме злоупотребления доверием [4] — почти таким же опасным, как и пиратство. Поскольку угрозы безопасности в морском порту не ограничиваются контрабандой и кражами, существует высокий потенциальный риск политической преступной деятельности. Предотвращение проникновения экстремистов в отрасль является эффективной мерой борьбы с морским терроризмом и оказывает благотворное влияние на национальную и международную безопасность [6]. Особое внимание следует уделять психическому здоровью моряков, поскольку хорошо известно, что исполнители терактов — это слабые личности, страдающие синдромом расширенного самоубийства, заинтересованные в общественном внимании к себе [5].

Любые инициативы в области транспортной безопасности встречали большую критику в России из-за высокой стоимости новых мер, направленных на предотвращение морских террористических атак. На практике финансовые ресурсы для цифровизации были перераспределены из области обеспечения

безопасности судоходства и предотвращения производственного травматизма. Криминогенные угрозы для Северного транспортного коридора[1] обусловлены экономическими проблемами морских портов (таких как Диксон и Сабетта) [44] и требуют стратегических решений в области цифровой трансформации морского бизнеса [21].

Если существование морских портов как коммерческих предприятий, работающих с целью получения прибыли, является частью национальной политики, то «разработка и внедрение новых технологий, автоматизация и оптимизация логистики, погрузочно-разгрузочных работ и других видов экономической деятельности, обеспечивающих рост объемов обработки грузов» [34], являются частью национальной экономической безопасности. При принятии любых решений о безопасности морских маршрутов необходимо оценивать все факторы риска. Практика цифрового рынка показывает, что ошибки в логистике, разгильдяйство и некомпетентность персонала могут быть опаснее терактов и пиратских нападений, а финансовые потери морского предприятия могут привести к его криминализации.

Популярность искусственного интеллекта на море приведет к тому, что рано или поздно цифровые технологии будут использованы в пиратских целях. Вспоминая о том, что «когда их никто не нанимал, этолийцы (военные, пираты и корсары) начинали грабить соседей по своему собственному выбору и усмотрению» [11, с. 77], можно прогнозировать, что следующий этап активности пиратов будет связан с нерациональным использованием цифровой инфраструктуры морских портов. Как в первой четверти XXI в. внезапно «сотни инцидентов с судами десятков государств в Аденском и Гвинейском заливах, а также в других регионах открытого моря вновь сделали из пиратства одну из главных угроз международной безопасности» [1, с. 149], так и в будущем нас ждут неприятные сюрпризы, но уже с использованием цифровых технологий. И хотя «в настоящее время Организации Объединенных Наций все же удалось снизить количество пиратских нападений на морские суда» [13, с. 86], нет никаких оснований полагать, что пираты не воспользуются в будущем уязвимостью приморской цифровой инфраструктуры.

Заключение

Цифровизация в интересах обеспечения безопасности морских предприятий требует компонента противодействия преступности, в противном случае цифровая среда будет использоваться не только для контрабанды и кибератак, но и для планирования пиратских нападений и террористических актов, совершаемых организованными преступными группами. Безусловно, что для обслуживания судов искусственный интеллект можно считать ключевой технологией, которая способна наладить связь между диспетчерами и докерами, управлять системой распределенного реестра и переводить документооборот судна в электронный вид. Однако при обслуживании пассажирских терминалов и работе с членами экипажа судна сокращение численности портового персонала в результате его замены цифровыми технологиями создает угрозу активизации организованной преступности, поскольку преступники могут проникать на территорию порта, используя уязвимости компьютерных технологий.

В позитивном плане технологии обеспечения безопасности в морских портах могут варьироваться в зависимости от типа рисков, которые являются общими для определенного вида морского бизнеса или локальными криминогенными угрозами. Криминогенные факторы, связанные с цифровизацией морских портов, с точки зрения позитивной безопасности и целей устойчивого развития нейтрализуются в процессе глобальной трансформации приморской экономики, что во многом связано с позитивным влиянием внедрения цифровых технологий на экономику морских предприятий [27; 28; 41].

В негативном аспекте морской безопасности стивидорным компаниям необходимо получить надзорные конкурентные преимущества, чтобы заставить порт работать на полную мощность. При внедрении цифровых технологий главной угрозой являются кибератаки, фишинг и неправомерный доступ к информации [4], так как не только авторизованные пользователи, но и хакеры могут проникнуть в сеть портов, нарушить ее функционирование и спланировать нападения на суда, пассажиров и грузы. Для

[1] Strategic Report 2020 [Электронный ресурс] // РОСМОРПОРТ. URL: https://www.rosmorport.ru/about/disclosure/report/presentation/strategicheskiy-otchet/index.html (дата обращения: 01.11.2022).

предотвращения правонарушений на море системы управления морским страхованием, судоходными компаниями и портами и должны выстраиваться квалифицированным персоналом с использованием цифровых технологий, которые рассчитаны на угрозы морского терроризма, контрабанды и пиратства.

Литература

1. *Варфоломеев А. А.* Современное морское пиратство и действующее международное право // Международная жизнь. 2015. № 4. С. 149–162.
2. *Гуцуляк В. Н.* Правовое регулирование захода торговых судов в иностранные порты в условиях пандемии Covid-19 // Государство и право. 2020. № 7. С. 100–110. DOI: 10.31857/S102694520010654-0
3. *Гуцуляк В. Н.* Правовые средства борьбы с пиратством и терроризмом на морском транспорте // Транспортное право и безопасность. 2018. № 4 (28). С. 41–44.
4. *Кириленко В. П., Алексеев Г. В.* Гармонизация российского уголовного законодательства о противодействии киберпреступности с правовыми стандартами Совета Европы // Всероссийский криминологический журнал. 2020. Т. 14. № 6. С. 898–913. DOI: 10.17150/2500-4255.2020.14(6).898-913
5. *Кириленко В. П., Алексеев Г. В.* Экстремисты: преступники и жертвы радикального насилия // Всероссийский криминологический журнал. 2019. Т. 13. № 4. С. 612–628. DOI: 10.17150/2500-4255.2019.13(4).612-628
6. *Кириленко В. П., Алексеев Г. В.* Киберпреступность и цифровая трансформация // Теоретическая и прикладная юриспруденция. 2021. № 1. С. 39–53. DOI: 10.22394/2686-7834-2021-1-39-53
7. *Кириленко В. П., Алексеев Г. В.* Противодействие идеологии современного терроризма // Управленческое консультирование. 2018. № 5 (113). С. 8–18. DOI: 10.22394/1726-1139-2018-5-8-18
8. *Кожевин Д. Ф., Поляков А. С., Таранцев А. А.* [и др.]. Пожарная безопасность транспортно-перегрузочных комплексов угля, сжиженных углеводородных газов и нефтепродуктов в морском порту // Морские интеллектуальные технологии. 2020. № 4–1 (50). С. 193–200. DOI: 10.37220/MIT.2020.50.4.027
9. *Сидорченко В. Ф.* Морские пираты: от средневековья к современности. СПб., 2016.
10. *Сидорченко В. Ф.* Морское пиратство. СПб., 2004.
11. *Сидорченко В. Ф.* Первый на Земле «профсоюз» пиратов // Вестник Санкт-Петербургского университета. Право. 2013. № 2. С. 75–78.
12. *Сидорченко В. Ф.* Спасание человеческих жизней и имущества на море «по-пиратски» // Вестник Санкт-Петербургского университета. Право. 2010. № 2. С. 84–92.
13. *Хижняк В. С.* Современные проблемы международно-правового сотрудничества по борьбе с пиратством // Вестник Санкт-Петербургского университета МВД России. 2017. № 1 (73). С. 82–86.
14. *Abliakimova E., Jianjun W.* Legal Regime of Russian Seaports: Security Policy Updates // Lex Portus. 2020, 7 (5). DOI: 10.26886/2524-101X.6.2020.1
15. *Agatić A., Kolanović I.* Improving the Seaport Service Quality by Implementing Digital Technologies // Pomorstvo. 2020, 34, 93–101. DOI: 10.31217/p.34.1.11
16. *Akinyemi Y. C.* Port Reform in Nigeria: Efficiency Gains and Challenges // GeoJournal. 2016, 81 (5), 681–97. DOI: 10.1007/s10708-015-9657-z
17. *Andritsos F., Mosconi M.* Port Security in EU: A Systemic Approach. 2010 International Waterside Security Conference, WSS 2010. DOI: 10.1109/WSSC.2010.5730222
18. *Andritsos F.* Port Security & Access Control: A Systemic Approach. IISA 2013 — 4th International Conference on Information, Intelligence, Systems and Applications. 2013. DOI: 10.1109/IISA.2013.6623728
19. *Corruble P.* EU Competition Law Applicable to Liner Shipping and Seaports: New Challenges of the Regulation. Bruxelles : Bruylant. 2021. 144 p
20. *Davis C.* The Politics of Ports: Privatization and the World's Ports // International Labor and Working-Class History. 2007, 71 (1), 154-161. DOI: 10.1017/S0147547907000385
21. *Effah J., Amankwah-Sarfo F., Boateng R.* Affordances and Constraints Processes of Smart Service Systems: Insights from the Case of Seaport Security in Ghana // International Journal of Information Management. 2021, 58. DOI: 10.1016/j.ijinfomgt.2020.102204

22. *Eski Y.* Policing, Port Security and Crime Control. An Ethnography of the Port Securityscape. Routledge. 2018. 256 p.
23. *Eski Y., Buijt R.* Dockers in Drugs: Policing the Illegal Drug Trade and Port Employee Corruption in the Port of Rotterdam // Policing: A Journal of Policy and Practice. 2017, 11 (4), 371–386. DOI: 10.1093/police/paw044
24. *Galani S.* Port Closures and Persons at Sea in International Law // International and Comparative Law Quarterly. 2021, 70 (3), 605-633. DOI: 10.1017/S0020589321000233
25. *Gjørv G. H.* Security by Any Other Name: Negative Security, Positive Security, and a Multi-Actor Security Approach // Review of International Studies. 2012, 38 (4), 835–859. DOI: 10.1017/S0260210511000751
26. *Gunes B., Kayisoglu G., Bolat P.* Cyber Security Risk Assessment for Seaports: A Case Study of a Container Port // Computers and Security. 2021, 103. DOI: 10.1016/j.cose.2021.102196
27. *Heilig L., Lalla-Ruiz E., Voß S.* Digital Transformation in Maritime Ports: Analysis and a Game Theoretic Framework // NETNOMICS: Economic Research and Electronic Networking. 2017, 18. DOI: 10.1007/s11066-017-9122-x
28. *Jović M.* Digital Transformation of Croatian Seaports. 32nd Bled eConference Humanizing Technology for a Sustainable Society, BLED 2019 — Conference Proceedings. 2020, 1147–1164. DOI: 10.18690/978-961-286-280-0.63
29. *Konvisarova E. V., Levchenko T. A., Pustovarov A. A.* Theoretical and Methodological Approaches to the Supply Chain Strategies Role and Analysis of Seaport Competitiveness in the Far East of Russia // International Journal of Supply Chain Management. 2019, 8 (6), 493–498.
30. *Lamarque H.* Profitable Inefficiency: The Politics of Port Infrastructure in Mombasa, Kenya // The Journal of Modern African Studies. 2019, 57 (1), 85–109. DOI: 10.1017/S0022278X18000630
31. *Liu C. P., Liang G. S., Su Y.* [et all.] Navigation Safety Analysis in Taiwanese Ports // Journal of Navigation. 2006, 59 (2), 201–211. DOI: 10.1017/S0373463306003687
32. *Łozowicka D., Kaup M.* Koncepcja bezpiecznej ewakuacji ze statków cumujących w rzeczno-morskim porcie Szczecin w przypadku zagrożenia terrorystycznego podczas trwania imprez masowych // Bezpieczenstwo i Technika Pozarnicza. 2016, 43, 161–172. (На польском яз.) DOI: 10.12845/bitp.43.3.2016.14
33. *McNicholas M. A.* A Strategic Blueprint for World-Class Seaport Security. Maritime Security. Butterworth-Heinemann. 2016. DOI: 10.1016/b978-0-12-803672-3.00010-8
34. *Nassar C. K., Nastacă C. C.* The Beirut Port Explosion: Social, Urban and Economic Impact // Theoretical and Empirical Researches in Urban Management. 2021, 16 (3), 42–52.
35. *Pavlić Skender H., Ribarić E., Jović M.* An Overview of Modern Technologies in Leading Global Seaports // Journal of Maritime & Transportation Science. 2020, 59, 35–49. DOI: 10.18048/2020.59.02
36. *Philipp R., Gerlitz L., Moldabekova A.* Small and Medium-Sized Seaports on the Digital Track: Tracing Digitalisation Across the South Baltic Region by Innovative Auditing Procedures. Lecture Notes in Networks and Systems. 2020. DOI: 10.1007/978-3-030-44610-9_35
37. *Sarabia-Jacome D., Palau C. E., Esteve M.* [et all.] Seaport Data Space for Improving Logistic Maritime Operations // IEEE Access. 2020, 8, 4372–4382. DOI: 10.1109/ACCESS.2019.2963283
38. *Sciascia A.* Monitoring the Border: Indonesian Port Security and the Role of Private Actors // Contemporary Southeast Asia. 2013, 35 (2), 163–187. DOI: 10.1355/cs35-2b
39. *Sergi A.* Playing Pac-Man in Portville: Policing the Dilution and Fragmentation of Drug Importations through Major Seaports // European Journal of Criminology. 2020. DOI: 10.1177/1477370820913465
40. *Sergi A., Reid A., Storti L.* [et all.] Ports, Crime and Security: Governing and Policing Seaports in a Changing World. Bristol University Press. 2021. DOI: 10.2307/j.ctv1rnpjf6
41. *Tang X.* Optimal Scheduling Method of Transport Path in Coastal Port International Logistics Park // Journal of Coastal Research. 2019, 93, 1125–1131. DOI: 10.2112/SI93-163.1
42. *Turluchev A., Filobok A., Volkova T.* [et all.] A. Sea Ports in the Sustainable Development of the Azov-Black Sea Coast. 14th MEDCOAST Congress on Coastal and Marine Sciences, Engineering, Management and Conservation, MEDCOAST. 2019.

43. *Turnbull P., Weston S.* Employment Regulation, State Intervention and the Economic Performance of European Ports // Cambridge Journal of Economics. 1992, 16 (4), 385–404. DOI: 10.1093/oxfordjournals.cje.a035210
44. *Vukovic N., Mekhrentsev A., Vukovic D.* Transnational Transport Corridor of the Northern Sea Route Based on Sabetta Seaport: Challenges of Regional Development for Russia // Journal of the Geographical Institute Jovan Cvijic, SASA. 2018, 68 (3), 405–414. DOI: 10.2298/ijgi180613005v
45. *Zhang X., Roe M.* Models of Container Port Security. Maritime Container Port Security 2019. DOI: 10.1007/978-3-030-03825-0_4

Об авторах:

Кириленко Виктор Петрович, заведующий кафедрой международного и гуманитарного права Северо-Западного института управления РАНХиГС (Санкт-Петербург, Российская Федерация), доктор юридических наук, профессор, заслуженный юрист Российской Федерации;
e-mail: v.vvaas@yandex.ru; ORCID: https://orcid.org/0000-0003-4445-1682

Алексеев Георгий Валерьевич, доцент кафедры правоведения Северо-Западного института управления РАНХиГС (Санкт-Петербург, Российская Федерация), кандидат юридических наук, доцент;
e-mail: Deltafox1@yandex.ru; ORCID: https://orcid.org/0000-0003-3720-0105

References

1. Varfolomeev A. A. Modern Maritime Piracy and Current International Law. *International life* [Mezhdunarodnaya zhizn']. 2015; (4): 149–162. (In Rus.)
2. Gutsulyak V. N. Legal Regulation of Merchant Ships Entering Foreign Ports in the Conditions of the Covid-19 Pandemic. *State and Law* [Gosudarstvo i pravo]. 2020; (7): 100–110. (In Rus.) DOI: 10.31857/S102694520010654-0
3. Gutsulyak V. N. Legal Means of Combating Piracy and Terrorism in Maritime Transport. *Transport Law and Security* [Transportnoe pravo i bezopasnost']. 2018; 28 (4): 41–44. (In Rus.)
4. Kirilenko V. P., Alekseev G. V. Harmonization of Russian Criminal Legislation on Countering Cybercrime with the Legal Standards of the Council of Europe. *All-Russian Journal of Criminology* [Vserossiiskii kriminologicheskii zhurnal]. 2020; 14 (6): 898–913. (In Rus.) DOI: 10.17150/2500-4255.2020.14(6).898-913
5. Kirilenko V. P., Alekseev G. V. Extremists: Criminals and Victims of Radical Violence. *All-Russian Criminological Journal* [Vserossiiskii kriminologicheskii zhurnal]. 2019; 13 (4): 612–628. (In Rus.) DOI: 10.17150/2500-4255.2019.13(4).612-628
6. Kirilenko V. P., Alekseev G. V. Cybercrime and Digital Transformation. *Theoretical and Applied Jurisprudence* [Teoreticheskaya i prikladnaya yurisprudentsiya]. 2021; (1): 39–53. (In Rus.) DOI: 10.22394/2686-7834-2021-1-39-53
7. Kirilenko V. P., Alekseev G. V. Countering the Ideology of Modern Terrorism. *Administrative Consulting* [Upravlencheskoe konsul'tirovanie]. 2018; 113 (5): 8–18. (In Rus.) DOI: 10.22394/1726-1139-2018-5-8-18
8. Kozhevin D. F., Polyakov A. S., Tarantsev A. A. [et al.]. Fire Safety of Transport and Transshipment Complexes of Coal, Liquefied Petroleum Gases and Petroleum Products in the Seaport. *Marine Intelligent Technologies* [Morskie intellektual'nye tekhnologii]. 2020; 50 (4–1): 193–200. (In Rus.) DOI: 10.37220/MIT.2020.50.4.027
9. Sidorchenko V. F. Sea Pirates: From the Middle Ages to the Present. St. Petersburg, 2016. (In Rus.)
10. Sidorchenko V. F. Maritime Piracy. St. Petersburg, 2004. (In Rus.)
11. Sidorchenko V. F. The First "Trade Union" of Pirates on Earth. *Bulletin of St. Petersburg University. Right* [Vestnik Sankt-Peterburgskogo universiteta. Pravo]. 2013; (2): 75–78. (In Rus.)

12. Sidorchenko V. F. Saving Human Lives and Property at Sea “in a Piratical Way”. *Bulletin of St. Petersburg University. Right* [Vestnik Sankt-Peterburgskogo universiteta. Pravo]. 2010; (2): 84–92. (In Rus.)
13. Khizhnyak V. S. Modern Problems of International Legal Cooperation in Combating Piracy. *Bulletin of the St. Petersburg University of the Ministry of Internal Affairs of Russia* [Vestnik Sankt-Peterburgskogo universiteta MVD Rossii]. 2017; 73 (1): 82–86. (In Rus.)
14. Abliakimova E., Jianjun W. Legal Regime of Russian Seaports: Security Policy Updates. *Lex Portus*. 2020; 7 (5). DOI: 10.26886/2524-101X.6.2020.1
15. Agatić A., Kolanović I. Improving the Seaport Service Quality by Implementing Digital Technologies. *Pomorstvo*. 2020; (34): 93–101. DOI: 10.31217/p.34.1.11
16. Akinyemi Y. C. Port Reform in Nigeria: Efficiency Gains and Challenges. *GeoJournal*. 2016; 81 (5): 681–97. DOI: 10.1007/s10708-015-9657-z
17. Andritsos F., Mosconi M. Port Security in EU: A Systemic Approach. 2010 International Waterside Security Conference, WSS 2010. DOI: 10.1109/WSSC.2010.5730222
18. Andritsos F. Port Security & Access Control: A Systemic Approach. IISA 2013 — 4th International Conference on Information, Intelligence, Systems and Applications. 2013. DOI: 10.1109/IISA.2013.6623728
19. Corruble P. EU Competition Law Applicable to Liner Shipping and Seaports: New Challenges of the Regulation. Bruxelles : Bruylant. 2021. 144 p
20. Davis C. The Politics of Ports: Privatization and the World’s Ports. *International Labor and Working-Class History*. 2007; 71 (1): 154–161. DOI: 10.1017/S0147547907000385
21. Effah J., Amankwah-Sarfo F., Boateng R. Affordances and Constraints Processes of Smart Service Systems: Insights from the Case of Seaport Security in Ghana. *International Journal of Information Management*. 2021; (58). DOI: 10.1016/j.ijinfomgt.2020.102204
22. Eski Y. Policing, Port Security and Crime Control. An Ethnography of the Port Securityscape. Routledge. 2018. 256 p.
23. Eski Y., Buijt R. Dockers in Drugs: Policing the Illegal Drug Trade and Port Employee Corruption in the Port of Rotterdam. *Policing: A Journal of Policy and Practice*. 2017; 11 (4): 371–386. DOI: 10.1093/police/paw044
24. Galani S. Port Closures and Persons at Sea in International Law. *International and Comparative Law Quarterly*. 2021; 70 (3): 605–633. DOI: 10.1017/S0020589321000233
25. Gjørv G. H. Security by Any Other Name: Negative Security, Positive Security, and a Multi-Actor Security Approach. *Review of International Studies*. 2012; 38 (4): 835–859. DOI: 10.1017/S0260210511000751
26. Gunes B., Kayisoglu G., Bolat P. Cyber Security Risk Assessment for Seaports: A Case Study of a Container Port. *Computers and Security*. 2021; (103). DOI: 10.1016/j.cose.2021.102196
27. Heilig L., Lalla-Ruiz E., Voß S. Digital Transformation in Maritime Ports: Analysis and a Game Theoretic Framework. *NETNOMICS: Economic Research and Electronic Networking*. 2017; (18). DOI: 10.1007/s11066-017-9122-x
28. Jović M. Digital Transformation of Croatian Seaports. 32nd Bled eConference Humanizing Technology for a Sustainable Society, BLED 2019 — Conference Proceedings. 2020; 1147–1164. DOI: 10.18690/978-961-286-280-0.63
29. Konvisarova E. V., Levchenko T. A., Pustovarov A. A. Theoretical and Methodological Approaches to the Supply Chain Strategies Role and Analysis of Seaport Competitiveness in the Far East of Russia. *International Journal of Supply Chain Management*. 2019; 8 (6): 493–498.
30. Lamarque H. Profitable Inefficiency: The Politics of Port Infrastructure in Mombasa, Kenya. *The Journal of Modern African Studies*. 2019; 57 (1): 85–109. DOI: 10.1017/S0022278X18000630
31. Liu C. P., Liang G. S., Su Y. [et all.] Navigation Safety Analysis in Taiwanese Ports. *Journal of Navigation*. 2006; 59 (2): 201–211. DOI: 10.1017/S0373463306003687
32. Łozowicka D., Kaup M. The Concept of Safe Evacuation from Sea Faring Vessels at the Port of Szczecin in Circumstances Occasioned by Terrorist Threats during Mass Events = Koncepcja bezpiecznej ewakuacji ze statków cumujących w rzeczno-morskim porcie Szczecin w przypadku zagrożenia terrorystycznego

podczas trwania imprez masowych. *Bezpieczenstwo i Technika Pozarnicza*. 2016; 43: 161–172. (In Polish) DOI: 10.12845/bitp.43.3.2016.14
33. McNicholas M. A. A Strategic Blueprint for World-Class Seaport Security. Maritime Security. Butterworth-Heinemann. 2016. DOI: 10.1016/b978-0-12-803672-3.00010-8
34. Nassar C. K., Nastacă C. C. The Beirut Port Explosion: Social, Urban and Economic Impact. *Theoretical and Empirical Researches in Urban Management.* 2021; 16 (3): 42–52.
35. Pavlić Skender H., Ribarić E., Jović M. An Overview of Modern Technologies in Leading Global Seaports. *Journal of Maritime & Transportation Science*. 2020; (59): 35–49. DOI: 10.18048/2020.59.02
36. Philipp R., Gerlitz L., Moldabekova A. Small and Medium-Sized Seaports on the Digital Track: Tracing Digitalisation Across the South Baltic Region by Innovative Auditing Procedures. Lecture Notes in Networks and Systems. 2020. DOI: 10.1007/978-3-030-44610-9_35
37. Sarabia-Jacome D., Palau C. E., Esteve M. [et all.] Seaport Data Space for Improving Logistic Maritime Operations. *IEEE Access*. 2020; (8): 4372–4382. DOI: 10.1109/ACCESS.2019.2963283
38. Sciascia A. Monitoring the Border: Indonesian Port Security and the Role of Private Actors. *Contemporary Southeast Asia*. 2013; 35 (2): 163–187. DOI: 10.1355/cs35-2b
39. Sergi A. Playing Pac-Man in Portville: Policing the Dilution and Fragmentation of Drug Importations through Major Seaports. *European Journal of Criminology*. 2020. DOI: 10.1177/1477370820913465
40. Sergi A., Reid A., Storti L. [et all.] Ports, Crime and Security: Governing and Policing Seaports in a Changing World. Bristol University Press. 2021. DOI: 10.2307/j.ctv1rnpjf6
41. Tang X. Optimal Scheduling Method of Transport Path in Coastal Port International Logistics Park. *Journal of Coastal Research.* 2019; (93): 1125–1131. DOI: 10.2112/SI93-163.1
42. Turluchev A., Filobok A., Volkova T. [et all.] A. Sea Ports in the Sustainable Development of the Azov-Black Sea Coast. 14th MEDCOAST Congress on Coastal and Marine Sciences, Engineering, Management and Conservation, MEDCOAST. 2019.
43. Turnbull P., Weston S. Employment Regulation, State Intervention and the Economic Performance of European Ports. *Cambridge Journal of Economics.* 1992; 16 (4): 385–404. DOI: 10.1093/oxfordjournals.cje.a035210
44. Vukovic N., Mekhrentsev A., Vukovic D. Transnational Transport Corridor of the Northern Sea Route Based on Sabetta Seaport: Challenges of Regional Development for Russia. *Journal of the Geographical Institute Jovan Cvijic, SASA.* 2018; 68 (3): 405–414. DOI: 10.2298/ijgi180613005v
45. Zhang X., Roe M. Models of Container Port Security. Maritime Container Port Security 2019. DOI: 10.1007/978-3-030-03825-0_4

About the authors:

Viktor P. Kirilenko, Head of the Chair of International and Humanitarian Law of North-West Institute of Management of RANEPA (Saint Petersburg, Russian Federation), Doctor of Science (Jurisprudence), Professor, Honored Lawyer of Russian Federation;
e-mail: v.vvaas@yandex.ru; ORCID: https://orcid.org/0000-0003-4445-1682

Georgy V. Alekseev, Associate Professor of the Chair of Law of North-West Institute of Management of RANEPA (Saint Petersburg, Russian Federation), PhD in Jurisprudence, Associate Professor;
e-mail: Deltafox1@yandex.ru; ORCID: https://orcid.org/0000-0003-3720-0105