DOI: 10.17803/1729-5920.2020.159.2.133-140

Н. Г. Скачков*

Правовое регулирование отношений по трансграничной морской перевозке опасных грузов в условиях цифровизации

Аннотация. Автор исследует юридические аспекты возникновения рисков сетевых пространств, когда закладываются правовые императивы перевозки и пребывания партии опасных грузов на борту судна. Делается вывод о сложности выбора права, подлежащего применению, в этой связи ориентиром могут послужить те материальные нормы, что составляют пространство операционного риска. Выбор их часто предшествует начислению активов чистой операционной прибыли. В то время как многообразие юридических фактов, с которыми приобретатель имущества по прибытии связывает свое право на подачу владельческого иска, формулируется либо в договоре подключения, либо присоединения. Поэтому выделены отдельные предпосылки возникновения предпринимательских, а также юридических рисков на стадии отказа от потребительского страхования в пользу имущественной его квалификации. Показано, какие обременения сопутствуют проблемам оптимизации расходов страхования от киберрисков, если страховые компании хотя и находят свое предложение выгодным для клиентов, однако основу риска финансовой потери все равно составляет восстановление утраченных данных. Страховщик вынужден распорядиться передовыми аналитическими разработками, такими как, предположим, блокчейн или очень распространенные сегодня смарт-контракты. Страхователи, в свою очередь, пользуются цифровой дистрибуцией, иными моделями виртуального сервиса, чтобы не только сократить до минимума затраты, но и получить конкурентные преимущества. Автор проанализировал нормы конвенционных актов о трансграничной морской перевозке опасных грузов. Исследованы Международные стандарты теле- и радиокоммуникаций ISO/IEC 11801 и ISO/IEC 27001 (ISMS — 2018 г.), делается вывод об отождествлении угрозы технологическим ресурсам и комплексной правовой стратегии владельческой защиты.

Ключевые слова: риски сетевых пространств; морская перевозка опасных грузов; оборотный коносамент; программные продукты; лицензионный договор; интернет-сервис; отчуждаемое страховое покрытие; протокол программирования; владельческая защита.

Для цитирования: *Скачков Н. Г.* Правовое регулирование отношений по трансграничной морской перевозке опасных грузов в условиях цифровизации // Lex russica. — 2020. — Т. 73. — № 2. — С. 133—140. — DOI: 10.17803/1729-5920.2020.159.2.133-140.

© Скачков Н. Г., 2020

* *Скачков Никита Геннадьевич,* кандидат юридических наук, доцент кафедры международного частного права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
Садовая-Кудринская ул., д. 9, г. Москва, Россия, 125993
skanic@mail.ru

Legal Regulation of Cross-Border Shipping of Dangerous Goods in the Conditions of Digitalization

Nikita G. Skachkov, Cand. Sci. (Law), Associate Professor of the Department of International Private Law at Kutafin Moscow State Law University (MSAL)
ul. Sadovaya-Kudrinskaya, d. 9, Moscow, Russia, 125993
skanic@mail.ru

Abstract. The author explores the legal aspects of network space risks, when legal imperatives are laid for the transportation and stay of a consignment of dangerous goods on board a ship. It is concluded that it is difficult to choose the law to be applied. In this regard, the material norms that make up the operational risk space can serve as a guide. Their selection is often a precursor to earning assets net operating profit. At the same time, the variety of legal facts with which the acquirer on arrival of property associates his right to file an ownership claim is formulated either in the contract of connection or accession. Therefore, separate prerequisites for the emergence of business and legal risks at the stage of abandoning consumer insurance in favor of its property qualification are highlighted. The paper shows types of encumbrances that accompany the problems of optimizing the costs of insurance against cyber risks. Even if insurance companies find their offer profitable for customers, the basis of the risk of financial loss is still the recovery of lost data. The insurer is forced to dispose of advanced analytical developments, such as, for example, blockchain or smart contracts that are very common today. Policyholders, in turn, use digital distribution and other virtual service models to not only reduce costs to a minimum, but also gain competitive advantages. The author analyzes the norms of the Convention acts on the transboundary shipping of dangerous goods. The International standards of TV and radio communications ISO/IEC 11801 and ISO/IEC 27001 (ISMS — 2018) are studied, and the conclusion is made that the threat to technological resources is identified with a comprehensive legal strategy for owner protection.

Keywords: risks of network spaces; shipping of dangerous goods; negotiable bill of lading; software products; license agreement; Internet service; alienable insurance coverage; programming Protocol; owner protection.
Cite as: Skachkov NG. Pravovoe regulirovanie otnosheniy po transgranichnoy morskoy perevozke opasnykh gruzov v usloviyakh tsifrovizatsii [Legal regulation of cross-border shipping of dangerous goods in the conditions of digitalization]. *Lex russica*. 2020;73(2):133-140. DOI: 10.17803/1729-5920.2020.159.2.133-140. (In Russ., abstract in Eng.).

Многочисленные технические инновации морской перевозки активно формируются на фоне мировой глобализации. Современное ведение бизнеса характеризуется подчас жестокой конкурентной борьбой за клиента, которую ведут субъекты хозяйствования. Появление каких-либо барьеров интеграционным процессам чреваты для них утратой эффективности в продвижении товаров, а следовательно, потерей миллиардов долларов чистой и операционной прибыли экспортного, импортного проекта. Сто́ит, бесспорно, упомянуть и о нарастании темпов внешнеторговых операций, неотъемлемой частью которых является трансграничная морская перевозка. Наконец, выскажемся в пользу непреложного социально-экономического, правового потенциала обеспечения морской безопасности.

По состоянию на сегодняшний день в мире насчитывается свыше 50 000 судов, не менее половины из общего их числа предназначается для перевозки продуктов переработки нефти, сжиженного природного газа, иных опасных материалов. Вместе с тем правоотношения по перевозке продолжают восприниматься сугубо прагматично: выдача коносаментов или принятие страхового полиса, сертификата рассматриваются в функционально узком методологическом контексте. Транспортная операция рентабельна, если только фрахтовые ставки закладываются как постоянные. В то же время нарушается причинно-следственная связь между прозрачностью положений заключаемого контракта и, казалось бы, вытекающей из этого пригодностью судна. Особо данное обстоятельство заметно в сфере перевозки опасных грузов, где формально довлеющим императивом должно выступать адресованное судовладельцу требование о проявлении осторожности, осмотрительности, контроле за поступлением товарной партии на борт до отплытия либо ее принятием уже напрямую в пути. Соответственно, предпосылки для возникновения, по меткому определению Ю. Базедова, «серых зон правоприменения и правового регулирования в целом» должны быть исключены полностью[1].

На деле выделение в сфере морской транспортировки опасных материалов таких кате-

горий цивилистики, как, скажем, оказание услуг или возмездный характер обязательства, буквально изобилует подобными пробелами правового регулирования. Контрагенту, следуя логике Конвенции ООН от 11 декабря 2008 г. о договорах полностью или частично морской международной перевозки грузов, удается определить разве что издержки, сопряженные с предоставлением оборотного коносамента, который всегда может быть заменен на свою именную классификацию.

Преобладание столь противоречивых норм, очевидно, побуждают того же перевозчика либо судовладельца воздержаться от урегулирования коллизии в пользу материального права, достаточного для признания целесообразным того или иного правопорядка. Выбор права, сто́ит заметить, делается в так называемом пространстве операционного риска и опосредуется его глубиной, когда быстрота идентификации рисков составляет один из юридических приемов защиты от них, наряду с качественной оценкой материальных активов. Здесь сто́ит пояснить, что операционный (управленческий) риск формируется в результате слияния IT и операционных технологий, когда любая из цифровых платформ, где бы она ни была установлена, крайне уязвима перед различными манипуляциями. В этой связи достаточно хорошо известно исследование Paradigm Shifts: Trend Micro Security Predictions for 2018 (Изменения парадигмы: прогнозы по информационной безопасности 2018), выполненное под эгидой японской компании Trend Micro. Продиктовано ли намерение воспользоваться изъянами в механизме защиты правом или одними только отраслевыми стандартами, не принципиально; в данном документе такое явление прямо обозначено внешне далеким от коммерческой практики термином «нападение»[2].

Явно свободное толкование данного понятия приводит к неопределенности формулировок, что, как следствие, выливается в заключение отдельного лицензионного договора. Нормы его ограничены перспективами правообладателя создать локальное сетевое пространство на судне. Однако привязки к статуту так называемой сложной вещи еще менее состоятельны: конструктивно судно продолжает рассматриваться как единообразие видов имущества в рамках родовой и видовой квалификации. Сетевые компоненты включаются в его инженерную инфраструктуру, хотя каждый из подобных узлов еще и самодостаточный объект правоотношений. При таком подходе, пишет М. В. Патрушев, «любая из телекоммуникационных сетей выстраивается de facto, тогда как надо создать для нее правовое поле de jure»[3].

Выбор компетентного правопорядка осуществляется на основании территориальной привязки к законодательству той страны, где контрагенты подписали договор технологического присоединения к цифровой транспортной системе. Альтернативным вариантом признается подлежащее применению право, содержащееся в договоре об оказании услуг, хотя оно и не позволяет определить, в какой последовательности соотносятся между собой процессы присоединения и подключения. Договорное условие, которое наделяло бы, например, инфраструктурную сеть признаками главной вещи, а абонентское оборудование — связанной с ней по назначению принадлежности зачастую просто не сформулировано. Сфера применения сервитута или залога также едва ли определена. В то время как киберриски успевают сформироваться. Надо признать, что современное судоходство все более интегрируется в пресловутый виртуальный мир: те же системы автоматической идентификации (AIS) используются повсеместно на нефтеналивных судах, при перевозке танк-контейнеров, для любого из существующих сегодня комплексов грузообработки[4].

Киберпространство, или цифровая среда, будучи продуктом информационных технологий, позволяет создавать многоаспектные схемы управления ими. В этой новой уникальной, по определению Верховного суда США, среде, ко-

---

1 *Базедов Ю.* Право открытых обществ — частное и государственное регулирование международных отношений : Общий курс международного частного права : пер. с англ. Ю. М. Юмашева. М. : Норма, 2016.

2 См.: *Ференц В.* Все совершенно иначе // Банковское обозрение. 2018. № 1.

3 *Патрушев М. В.* Правовой режим сооружений связи. Современное состояние и перспективы развития российского и международного законодательства : сборник статей Международной научно-практической конференции (13 января 2017 г., г. Казань). Уфа : Аэтерна, 2017. С. 157.

4 Cyber Risks and Insurance In The Marine Industry. 2016 // URL: http://www.cambiasorisso.com/cyber-risks-and-insurance-in-the-marine-industry (дата обращения: 19 апреля 2019 г.).

торая не расположена в привычном нам географическом пространстве, но доступна каждому в любой точке мира посредством ординарного доступа к Интернету, создается глобальная система коммерческого взаимодействия, предоставляющая широкую возможность по-новому использовать все востребованные в этой связи ресурсы[5].

Киберпространство как поле функционирования правовых институтов тесно соотносится с сетевым пространством (по принципу «часть и целое»). Оно, как неизменный атрибут коммуникативных обществ XXI в., обладает тем не менее рядом особенностей, к которым относятся виртуальность, возможность одновременного приобретения публичных и частных признаков, многомерность, с какой обычно конструируются сетевые идентичности. Как следствие, не только открываются новые возможности, но и возникают риски, чаще всего одноименные с понятием кибербезопасности. В современной цифровой экономике они воспринимаются особенно остро.

Такие риски сразу становятся многосоставной правовой категорией, в прикладном отношении от них не застраховано даже оснащенное по последнему слову техники судно. Согласно материалам Allied Market Research, подготовленным американским сообществом регуляторов и рейтинговых агентств Deloitte, морское страхование рассматривается в качестве инструмента возмещения, ввиду чего возникает вопрос о том, насколько отчуждаемое покрытие способно сыграть решающую роль при последующем восстановлении нематериальных активов, а также основных средств. В исследовании WSJ говорится, что по состоянию на 2022 г. глобальный рынок страхования киберрисков достигнет впечатляющих 14 млрд долл., а к 2025 г. он будет составлять уже 20 млрд[6].

При этом упрочнение юридического, а также финансового режимов, как правило, означает переход от страхования непотребительского к имущественному. Потери тем не менее могут оказаться очень специфическими. Первыми в их списке несостоявшиеся услуги по программному обеспечению. В то же время возмещение убытков на фоне особенного имущественного интереса, при котором прибыль обычно распределяется среди держателей полиса по киберрискам для резервирования ресурсов на период расходов, зависит от условий получения доступа по цепочке посредников к облачному сервису, начиная с веб-хостинга, в пределах которого могла быть оформлена лицензия, и завершая почтовыми серверами SAAB.

Между тем разъяснения природы киберрисков существенным образом различаются между собой. Вряд ли в этом случае можно говорить о серьезном нарушении цельности корпуса судна, его механизмов. Вместе с тем та же неограниченная передача коммерческих данных или использование мобильных приложений, где абсолютно подробно сведения о геолокации судна с партией опасных грузов на борту несут в себе угрозу причинения ущерба, поскольку ими может воспользоваться любое третье лицо. В конечном итоге нельзя исключать и пресловутую кибератаку. Так, предположим, что прекращение экспортной транзитной сделки, а следовательно, значительные потери были вызваны длительной остановкой на дистанции движения судна. Причиной тому послужили нарушения в функционировании компонентов оборудования навигации, обусловленные внешними факторами — поступлением вредоносных сведений через удаленный USB-порт с последующей интеграцией его электронных систем в периферийную нейронную сеть, которая в конечном счете и отнесла их к разряду нераспознаваемых объектов. Так же предвидимы дополнительные репутационные риски: сомнения одного из контрагентов в компетентности другого лица.

В этом плане весьма показательны слушания по делу Glencoe International AG v. Mediterranean Shipping Co SA, которые состоялись в Высоком суде Правосудия Англии и Уэльса 8 июня 2017 г[7]. По фабуле искового требования судно ответчика прибыло в порт г. Антверпен, где перевозчик предложил агентам, ожидающим груз, сразу ввести в считывающее устройство предложенные им PIN-коды выпуска контейнеров. Вместе с тем согласно договору рассылка электронных уведомлений,

[5] Reno v. ACLU, 117 S.Ct. 2329 (1997) (casebook at 932—53) // URL: http www.ciec.org/SC_appeal/opinion shtml (дата обращения: 19.апреля 2019).

[6] URL: https://www.vedomosti.ru. (дата обращения: 19 апреля 2019 г).

[7] Glencore International AG v Mediterranean Shipping Co SA (2017) // URL: https://www.i-law.com/ilaw/doc/view.htm?id=382056#LLR:2017020186 (дата обращения: 19 апреля 2019 г.).

в которых и содержались данные средства идентификации товара, а также права на их распоряжение, предусматривалась лишь после предоставления коносамента. Кроме того, PIN-коды по инициативе перевозчика ранее были размещены на сайте открытым списком, хотя это следовало сделать лишь после того, как агенты отправятся за грузом, а не просто проследуют на борт судна. Как уверял истец, здесь налицо нарушение контракта, в то же время разъяснил свою позицию и ответчик: он восстановил подлинные PIN-коды вместо тех, что приведены во всех спецификациях, однако они не соответствовали действительности.

Отсюда следует обобщающее суждение о непреходящей функции резервных копий при нейтрализации киберрисков. Гарантии доступности, но одновременно и конфиденциальности, заключены в авторизированном запросе правомочного лица. Обращение к стандартам телекоммуникационной инфраструктуры ISO/IEC 11801, как сформулировано в Международном кодексе по охране судов и портовых средств (ISPS-Code в редакции от 25 июля 2018 г.), представляется юридически обязательным условием, если иные количественные оценки рисков по каким-либо причинам оказываются затруднены[8].

Вместе с тем в системных положениях другого стандарта функционирования теле- и радиокоммуникаций ISO/IEC 27001 (ISMS — 2018 г.) закрепляется необходимость удостовериться, в чем заключаются утрата или компрометация информации: поскольку она содержится непосредственно в профиле риска, то и едва ли подлежит разглашению. Управление таким риском лишь отчасти корреспондирует корпоративной правовой стратегии, но возлагается на субъекта обязательства, желающего разделить данный риск[9].

Соответственно, сохраняется возможность оказывать влияние на организацию морской перевозки партии опасных грузов, в том числе и не уполномоченным к тому лицом, пользующимся так называемым контекстным меню программного обеспечения и анонимно рассылающим коммерческие сообщения. Отсюда возникает необходимость использования проверенных каналов связи как крайне обособленного сегмента единого сетевого пространства, поскольку в силу именно этого признака они считаются наиболее защищенными.

Вопрос о взаимообусловленности собственно информации и киберриска остается пока открытым, так как еще явно не сформированы устойчивые дефиниции. Тем не менее можно выделить несколько подходов к данной проблеме. Так, согласно Программному руководству по кибербезопасности на борту судна, выпущенному 7 июля 2017 г. под патронатом BIMCO, CLIA, ICS, InterCargo, InterTanko OCIMF и IUMI, первоэлементом идентификации киберрисков должна стать такая внеправовая категория, как угроза, которой придается самостоятельное значение[10]. Подобным образом целеполагающие признаки риска включают в себя удаление, уничтожение данных, безосновательное признание их недоступными, одновременно распространение заведомо искаженных сведений, предназначенных для последующей обработки вне судна.

Напротив, в Циркуляре лучшей практики управления киберрисками Комитета Международной морской организации по безопасности на море MSC-FAL.1 / Circ.3 от 5 июля 2017 г. закрепляется, что квалификация индикаторов данного риска призвана определить источник опасности, когда разглашение тех или иных сведений приводит к неопределенности результатов приобретения риском свойств правореализующего юридического факта[11].

В таком случае нежелательное событие рассматривается только как предполагаемое: нельзя исключать, что оно едва ли осуществится. В то же время согласно Резолюции Комитета ИМО по безопасности на море MSC.428 (98) от

---

8 AS-XI-2%20ISPS%20Code.aspx; ISO/IEC 11801-1:2017 — Information technology — Generic cabling for customer premises // URL: https://www.iso.org/ru/standard/66182.html (дата обращения: 19 апреля 2019 г.).

9 ISO/IEC 27000 Family — Information Security Management Systems.2018 // URL: https://www.iso.org/isoiec-27001-information-security.html (дата обращения: 19 апреля 2019 г.).

10 The Guidelines on Cyber Security Onboard Ships. 2017 // URL: http://www.ics-shipping.org/docs/default-source/resources/safety-security-andoperations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16 (дата обращения: 19 апреля 2019 г.).

11 MSC-FAL.1/Circ.3 5 July 2017 Guidelines on Maritime Cyber // URL: http.www.imo.org/.../MSC-FAL.1-Circ.3%20-%20Guidelines%2 (дата обращения: 19 апреля 2019 г.)

16 июня 2017 г. основу киберриска составляет отождествление угрозы и ущерба за пределами строго определенных правовых рамок для каждого из страховых случаев. Поэтому явление событийности, насколько оно присуще той или иной коммуникации, опосредует ее информационный потенциал[12].

Очевидно, что возникают также риски информационных обменов. По мнению О. Ю. Рыбакова и С. В. Тихонова, одни только предпосылки таковых свидетельствуют о полнейшем провале так называемой трансдисциплинарности, когда недостаточно адекватным было не столько получение, сколько оперирование информацией. Информационные риски, как утверждает исследователь, классифицируются на три группы: «риски ошибки в идентификации субъектов, риски выбора модели взаимодействия, риски снижения качественных характеристик информации»[13].

Дополним данный перечень внесением изменений в протоколы программирования, что также способно привести к появлению рисков цифровой информации. Замещение тех или иных параметров технологического ресурса, структуры данных иными системными характеристиками не менее прогнозируемо. Должным образом учитывается и инсталляция заведомо неэффективных операционных программных продуктов. Пользовательское соглашение заключается строго в интересах правообладателя, а не ординарного потребителя услуг, хотя последнему и предоставляется возможность распорядиться интернет-сервисом.

Сто́ит отметить, что логика ответных действий может даже предшествовать возникновению риска, но чаще сопутствует ему: как сформулировано в последней редакции Международного кодекса по управлению безопасной эксплуатацией судов и предотвращению загрязнения (ISM Code от 1 июля 2018 г.), риск-ориентированное событие не просто предвосхищает либо детализирует их возникновение, оно становится свершившимся фактом, так как риски сетевых пространств практически невозможно опровергнуть юридически[14].

Процедуры управления киберрисками воплощают чуть ли не весь предусматриваемый в этой связи инструментарий сетевых пространств, начиная с эффекта дополненной реальности (AR, «компьютерное зрение») и завершая искусственным интеллектом. Например, система глобального позиционирования наливного танкера, GPS или EGDIS, испытывает на себе некую форму деструктивного воздействия, результатом которого становится появление на электронных картах перечня отмелей или подводных препятствий, досконально известных одному лишь лоцману.

Квалификация киберрисков зачастую сопровождается обоснованием владельческой защиты, поскольку любое из вмешательств или ограничивает пользование имуществом, или, напротив, нивелирует границы хозяйственного господства. Ввиду этого справедливо суждение Р. С. Бевзенко о том, что «каким бы ни было распределение наличных благ, имущественная сфера участников гражданского оборота неизменно предусматривает фактическую связь с определенной вещью»[15].

Конечно, лицо, которое по заблуждению выдает имущество за свое, лишь пользуется им. Проявление воли к владению вполне возможно, но далеко не всегда обязательно. Кроме того, титул владения вряд ли настолько абстрактен. Так, в доктрине, практике и традициях англо-американской правовой семьи владельческая защита предусматривается лишь применительно к конкретной ситуации (estates). Предоставление иска о защите субъективных прав, аналогичного владельческим, вещным искам, получившим широкое признание в национальных правовых системах континентальной семьи, является маловероятным.

Таким образом, уместно предположить, что если допущенная ошибка в процессе об-

---

[12] Resolution MSC.428(98) — Maritime Cyber Risk Management in Safety Management Systems. (2017) // URL: http://www.imo.org/en/OurWork/Security/WestAfrica/Documents/Resolution%20MSC.428%2898%29%20-%20Maritime%20Cyber%20Risk%20Management%20in%20Safety%20Managemet%20Systems.pdf (дата обращения: 19 апреля 2019 г.).

[13] *Рыбаков О. Ю.*, *Тихонова С. В.* Информационные риски и эффективность правовой политики // Журнал российского права. 2016. № 3.

[14] SOLAS XI-2 and the ISPS Code. (2018) // URL: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/SOL (дата обращения: 19 апреля 2019 г.).

[15] *Бевзенко Р. С.* Очерк 14. Проблема владения и держания // Гражданское право : Актуальные проблемы теории и практики / под ред. В. А. Белова. М., 2007. С. 75.

мена информацией обусловила наступление киберриска, то выбор фактического владения в порядке юрисдикции, предположим, англо-американского права создает основания и для владельческого титула до того момента, пока не будет доказано обратное. В то время как выбор в пользу континентального права призван удостоверить фактическое владение per se (как таковое — лат.), так как оно традиционно отделено от права собственности. Юридическая конструкция владения предполагает не столько институциональную среду вещных прав, сколько ограничения, закрепляемые в контрактах по усмотрению непосредственно самих выгодоприобретателей.

К их числу относятся сразу несколько групп хозяйствующих субъектов. Одни из них длительное время находятся на судне, поскольку распоряжаются им на протяжении всего рейса. В то время как другие ограничивают свое пребывание периодом, достаточным для заключения, предположим, чартерного договора. Наконец, нельзя не упомянуть поставщиков, которые благодаря быстрому развитию спутникового Интернета пользуются бизнес-контентом и вовсе посредством удаленного доступа. Вместе с тем в таком случае трудно опровержимо применение принципа наиболее тесной связи между страховым событием и риском. Не является принципиальным, обусловливает ли страховой случай лишь некоторые предпосылки возникновения киберриска, или согласно римской максиме causa proxima non remota spectatur, сформулированной еще в Законе о морском страховании Великобритании 1906 г., опосредованно подводит к нему. Однако даже если страховое событие и явилось прямым следствием сетевого риска (сравнительно нового страхового продукта), то предварительно необходимо определить объемы именно традиционного полисного покрытия, установив, когда они ограничены либо крайне малы.

Страховщики, отчуждая пул киберрисков в интересах страхователей, отчетливо осознают, что оплата абсолютно всех убытков просто нереальна. Онлайн-риски легко переходят в офлайн, что в целом свойственно такому феномену нашего времени, как интернет вещей. При этом границы между институциональной онлайн-средой, где возникновение киберриска еще можно предотвратить, и, соответственно, офлайн-полем, где предвидим разве что страховой случай, постепенно размываются. Тот же страховой полис все чаще включает в себя риски потери учетных данных. Превалируют также нарушения, но далеко не убытки, сопряженные с наступлением сетевого риска. Они обычно начисляются в процентном соотношении от оборота и от лимита того же полиса, когда ставка оборота определяет один лишь только брутто-доход. Кроме того, неизвестно, оплатит ли страховщик далеко непервоочередные расходы, например на восстановление утраченных сведений. Проще отнести киберриски к числу так называемых исключений из страхования, согласно той же оговорке paramount clause, тем более что в комплексном полисе киберстрахования содержатся базисные составляющие тарификации и андеррайтинга. Однако если учитывать, что очень немногие судовладельцы регулярно обновляют свои операционные системы, то кибератака может оказаться катастрофической для всей судоходной отрасли.

БИБЛИОГРАФИЯ

1. *Бевзенко Р. С.* Очерк 14. Проблема владения и держания // Гражданское право : Актуальные проблемы теории и практики / под ред. В. А. Белова. — М., 2007.
2. *Базедов Ю.* Право открытых обществ — частное и государственное регулирование международных отношений : общий курс международного частного права / пер. с англ. Ю. М. Юмашева. — М. : Норма, 2016.
3. *Патрушев М. В.* Правовой режим сооружений связи. Современное состояние и перспективы развития российского и международного законодательства : сборник статей Международной научно-практической конференции (13 января 2017 г., г. Казань). — Уфа : Аэтерна, 2017.
4. *Рыбаков О. Ю., Тихонова С. В.* Информационные риски и эффективность правовой политики // Журнал российского права. — 2016. — № 3.
5. *Ференц В.* Все совершенно иначе // Банковское обозрение. — 2018. — № 1.

Материал поступил в редакцию 25 апреля 2019 г.

REFERENCES

1. Bevzenko RS. Ocherk 14. Problema vladeniya i derzhaniya [Work 14. The problem of ownership and holding]. In: *Grazhdanskoe pravo: aktualnye problemy teorii i praktiki [Civil law: Current problems of theory and practice]*. Belov VA, editor. Moscow; 2007. (In Russ.).
2. Bazedov Yu. *Pravo otkrytykh obshchestv — chastnoe i gosudarstvennoe regulirovanie mezhdunarodnykh otnosheniy: obshchiy kurs mezhdunarodnogo chastnogo prava [The right of open societies — private and public regulation of international relations: General course of private international law].* Transl. from Eng.: Yumashev YuM. Moscow: Norma; 2016. (In Russ.).
3. Patrushev MV. Pravovoy rezhim sooruzheniy svyazi [Legal regime of communication facilities]. In: *Sovremennoe sostoyanie i perspektivy razvitiya rossiyskogo i mezhdunarodnogo zakonodatelstva: Sbornik statey mezhdunarodnoy nauchno-prakticheskoy konferentsii (13 yanvarya 2017 g., g. Kazan) [Current state and prospects of development of Russian and international legislation: Proceedings of the International scientific and practical conference (2017 January 13, Kazan)]*. Ufa: Aeterna; 2017. (In Russ.).
4. Rybakov OYu, Tikhonova SV. Informatsionnye riski i effektivnost pravovoy politiki [Information risks and the efficiency of legal policy]. *Zhurnal Rossiiskogo Prava [Journal of Russian law]*. 2016;3:88-95. (In Russ.).
5. Ferentsc V. Vse sovershenno inache [Everything is completely different]. *Bankovskoe obozrenie*. 2018;1. (In Russ.).