МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА (РУТ (МИИТ))

Ю Р И Д И Ч Е С К И Й И Н С Т И Т У Т

ЦИФРОВОЙ СУВЕРЕНИТЕТ И КИБЕРБЕЗОПАСНОСТЬ

Материалы Четвертого международного транспортно-правового форума

DIGITAL SOVEREIGNTY AND CYBERSECURITY

Materials of the Fourth International Transport and Legal Forum

МОСКВА—2022

УДК 336
ББК 16.8
Ц75
ISBN 978-5-7876-0311-8

Ответственные редакторы:

Чеботарева Анна Александровна — доктор юридических наук, доцент, заведующая кафедрой «Правовое обеспечение государственного управления и экономики» Юридического института Российского университета транспорта (МИИТ);

Чеботарев Владимир Евгеньевич — кандидат экономических наук, доцент, заведующий кафедрой «Морское право и международное право» Юридического института Российского университета транспорта (МИИТ).

Цифровой суверенитет и кибербезопасность // Материалы Четвертого международного транспортно-правового форума / под редакцией А. А. Чеботаревой, В. Е. Чеботарева. — Москва : Изд-во Юридического института РУТ (МИИТ), 2022. — 335 с.

На базе Юридического института Российского университета транспорта (МИИТ) 9—10 февраля 2022 г. состоялся Четвертый международный транспортно-правовой форум «Цифровой суверенитет и кибербезопасность». В работе форума участвовали представители разных стран — России, Марокко, Египта, Алжира, Туниса, Судана, Иордании и Беларуси.

В сборнике представлены тезисы докладов и выступлений участников международного форума.

Конференция проводилась при поддержке справочной правовой системы КонсультантПлюс и издательской группы «Юрист».

Изд. заказ 13	Подписано в печать 30.09.2022	Тираж 100 экз.
Усл.-печ. л. 20,9	Уч.-изд. л. 17,6	Формат 60×901/16

Типография Юридического института МИИТ
127994, Москва, ул. Образцова, д. 9, стр. 9.

Содержание

Чеботарева Анна Александровна,
доктор юридических наук, доцент, заведующая кафедрой «Правовое обеспечение государственного управления и экономики»
Юридического института Российского университета транспорта

Чеботарев Владимир Евгеньевич,
кандидат экономических наук, доцент, заведующий кафедрой «Морское право и международное право» Юридического института Российского университета транспорта

Цифровой суверенитет и кибербезопасность на транспорте в санкционных условиях

Аннотация. В статье анализируются задачи, связанные с решением проблемы цифрового суверенитета и кибербезопасности на транспорте. Актуализируется вопрос государственного суверенитета в целом, территориальной целостности России, подчеркивается значение решения проблемы импортозамещения применительно к транспортной инфраструктуре.

Ключевые слова: цифровой суверенитет; государственный суверенитет; безопасность; цифровая трансформация; кибербезопасность на транспорте; проблема импортозамещения.

Anna A. Chebotareva,
doctor of law, Russian University of Transport, Law Institute, Head of the Department «Legal support of public administration and economy» of Russian University of Transport

Vladimir Ev. Chebotarev,
candidate of Economical Sciences, docent, Head of the Department «Maritime law and international law» of Russian University of Transport

Digital sovereignty and cybersecurity in transport under sanctions

Abstract. The article analyzes the tasks associated with solving the problem of digital sovereignty and cybersecurity in transport. The issue of state sovereignty in general, the territorial integrity of Russia is being updated, the importance of solv-

ing the problem of import substitution in relation to transport infrastructure is emphasized.

Keywords: digital sovereignty; state sovereignty; security; digital transformation; cybersecurity in transport; the problem of import substitution.

Наш мир все больше погружается в «цифру» и опирается на коммуникации — отсюда стратегии обеспечения безопасности привлекают все больше внимания. При этом, по мнению Д. Пескова, спецпредставителя президента по вопросам технологического развития, «сегодня в мире нет ни одной страны, у которой был бы достигнут уровень технологического суверенитета. Можно спросить: а зачем тогда он нужен, если его ни у кого нет? Жизнь меняется, условием выживания в прямом смысле этого слова любой крупной страны в ближайшие десятилетия будет достижение этой страной технологического суверенитета»[1].

В качестве примера. С точки зрения кибербезопасности современный город представляет собой место, где в большом объеме и с высокой плотностью концентрируются различные информационно-телекоммуникационные сети и системы управления технологическими процессами. Они составляют основу промышленности, транспорта, инфраструктуры телекоммуникаций и электросвязи. С точки зрения кибербезопасности город — это большая проблема. Отключи «Яндекс.Пробки» — город остановится…

Развитие беспилотного транспорта, использование дронов… Растет цена взлома, возрастают угрозы кибербезопасности в случае перехвата доступа к обеспечивающим их работу системам.

В феврале 2022 г. кафедрой «Административное право, экологическое право, информационное право» Юридического института Российского университета транспорта организовывался и был успешно проведен четвертый Международный транспортно-правовой форум на данную тематику — цифровой суверенитет и кибербезопасность на транспорте. Как показывает время и санкционная ситуация — тема получает свое мощнейшее развитие и актуальность. Характерно и то, что наши зарубежные коллеги-ученые также активно включаются в исследования данной проблематики.

[1] https://www.rbc.ru/opinions/economics/09/06/2022/62a0e95b9a79472d8b713207 (дата обращения: 09.06.2022).

Таким образом, мы наблюдаем — формируется четкое понимание того, что способность обеспечить свой цифровой суверенитет становится ключевым признаком независимости государства в целом. И по мере появления и распространения глобальных сетей правительства всех стран все больше и больше осознают свою уязвимость в вопросах контроля над инфраструктурой. Что более чем актуально для транспортной инфраструктуры.

Вообще же, рассуждая о вопросах правового обеспечения суверенитета и информационной безопасности государства и общества (так называемого цифрового суверенитета), можно согласиться с мнением о том, что «о проблемах с территориальным действием законов юристы пишут уже давно, особенно при рассмотрении вопроса о праве, применимом к отношениям в киберпространстве. Среди слов, которые использовались и используются для описания этой проблемы, главных два — сложность и неопределенность. Это символически замыкает круг развития суверенитета как правовой категории. Созданный в XVII в. для увеличения правовой определенности и упрощения решения вопроса о применимом праве, в XXI в. суверенитет лишь порождает сложность и неопределенность в том, какими правовыми нормами руководствоваться субъектам»[1].

В утвержденной 27 ноября 2021 г. распоряжением Правительства РФ № 3363-р Транспортной стратегии до 2030 года с прогнозом до 2035 года впервые выделен важнейший блок — по цифровой трансформации — в качестве важнейшего инструмента достижения целей. По уточнениям представителей Минтранса России, прозвучавшим на различных площадках, именно цифровизация позволит отрасли достичь снижения издержек и роста производительности труда минимум в два раза. При этом все эти процессы невозможны без обеспечения кибербезопасности и цифрового суверенитета.

Согласно Доктрине информационной безопасности Российской Федерации (утверждена Указом Президента РФ от 05.12.2016 № 646) «интересы государства в информационной сфере заключаются в создании условий для обеспечения суверенитета и территориальной целостности России», т.е. собственно, традиционного государственного суверенитета. Понятия «цифровой» или «информационный су-

[1] Дмитрик Н. А. Государства в своем праве // Закон. 2021. № 11. С. 66.

верenитет», «суверенитет в информационном пространстве» — новые. Примечательно, что до 2016 г. они фактически отсутствовали в российских нормативных документах. То есть в науке до сих пор не сложилось четких дефиниций, что требует отдельных исследований.

Сегодня предлагаются различные меры по самоопределению государств в цифровом пространстве и контролю с их стороны за цифровой инфраструктурой. При этом однозначен факт, что вопрос о цифровом суверенитете не сводится только к политико-правовой стороне вопроса, чрезвычайно важна экономическая сторона.

Недооценка обеспечения цифрового суверенитета для транспортного комплекса в целом чревата серьезными потерями. Однозначно «транспортная инфраструктура жизненно важна для каждого человека; устойчивая транспортная система помогает строить лучшее будущее и сокращать бедность, одновременно защищая окружающую среду и обеспечивая экономический рост»[1]. Одним из основных направлений деятельности по достижению цифровой трансформации в транспортной отрасли выступает решение проблемы импортозамещения, перехода на отечественные цифровые решения. В конечно итоге, от эффективности решения данной проблемы зависит результативность и других мероприятий, в числе которых — противодействие терроризму на транспорте.

Провозглашение цели добиться большей независимости от иностранных ИТ-технологий и развитие отечественной индустрии сегодня выступает одной из ключевых тем, обсуждаемых в рамках вопросов цифрового суверенитета. Мы наблюдаем широкие меры государственной поддержки разработчиков отечественного программного обеспечения. Прежде всего, требуется масштабная поддержка со стороны государства отечественных ИТ-производителей на глобальном рынке. А решение всего комплекса проблем обеспечения цифрового суверенитета и кибербезопасности более чем актуально для всего транспортного комплекса.

[1] Chebotareva A. A., Chebotarev V. E., Danilina E. I. Mechanism of the administrative and legal regulation of public transportation system // International Journal of Civil Engineering and Technology, 2018. Volume 9(13), p. 144. https://www.scopus.com/record/display.uri?eid=2-s2.0-85059772216&origin=resultslist

Архангельская Екатерина Владиславовна,
кандидат физико-математических наук, доцент кафедры информационного права и цифровых технологий, Саратовская государственная юридическая академия

Анализ эффективности рекламы на транспорте математическими методами

Аннотация. В статье анализируются задачи, связанные с увеличением эффективности рекламы на транспорте, выявляются математические модели, соответствующие постановке каждой задачи. В зависимости от математической модели используются различные методы математического программирования для решения задач оптимизации эффекта рекламной деятельности на транспорте. В статье приводятся задачи и методы их решения.

Ключевые слова: оптимизация затрат и прибыли от рекламы на транспорте; линейное программирование; динамическое программирование.

Arkhangelskaya V. Ekaterina,
candidate of physical-mathematical Sciences, Associate professor of the Department of Information Law and Digital Technologies, Saratov State Law Academy

Analysis of the effectiveness of advertising in transport by mathematical methods

Abstract. The article analyzes the problems associated with increasing the effectiveness of advertising on transport, identifies mathematical models corresponding to the formulation of each problem. Depending on the mathematical model, various methods of mathematical programming are used to solve problems of optimizing the effect of advertising activities on transport. The article presents the tasks and methods of their solution.

Keywords: optimization of costs and profits from advertising in transport; linear programming; dynamic programming.

Внешняя реклама активно используется для продвижения товаров и услуг. В условиях рыночной экономики реклама является неотъемлемой частью деятельности предпринимателей, частных фирм и

крупных компаний. Наряду с традиционными видами рекламных услуг, таких как реклама в печатных изданиях, на радио и телевидении, активно осуществляется размещение рекламы на транспортных средствах и внутри них, если речь идет об общественном транспорте. Реклама на общественном транспорте гораздо дешевле рекламы на телевидении и радио, привлекает внимание как пассажиров, так и пешеходов и других участников дорожного движения. Пассажиры изучают рекламные объявления, размещенные внутри салонов трамваев, троллейбусов, автобусов и маршрутных такси, чтобы скоротать время в поездке.

Взаимодействие двух сторон, заключающих договор о рекламе на транспорте, регламентируется ст. 20 «Реклама на транспортных средствах и с их использованием» Федерального закона «О рекламе», в которой сказано, что «размещение рекламы на транспортном средстве осуществляется на основании договора, заключаемого рекламодателем с собственником транспортного средства или уполномоченным им лицом либо с лицом, обладающим иным вещным правом на транспортное средство». В тексте договора прописываются права и обязанности сторон, например, данный договор может иметь следующие пункты: «Предприятие обязуется предоставить Пользователю право размещения информации на рекламных носителях Предприятия, а Пользователь за использование предоставленного права обязуется уплатить Предприятию денежные средства в размере и порядке, предусмотренном настоящим договором».

Под рекламными носителями понимаются транспортные средства — трамваи и троллейбусы, автобусы или маршрутные такси, принадлежащие предприятию и осуществляющие перевозку пассажиров по маршруту. Пользователь в рамках договора приобретает право размещения информации, например, на боковых, задних и передних наружных поверхностях транспортных средства, а также внутри салонов.

Как и в других сферах деятельности, для оценки эффективности рекламы необходим прогноз и точный расчет оптимальных параметров на основе анализа статистических данных [1].

Сформулируем несколько задач, решение которых приводит к увеличению эффективности рекламы на транспорте. Допустим предприятие может предоставить достаточное количество транспортных

средств различного типа (трамваем и троллейбусов, или автобусов и маршрутных такси), и ставит условие, что в рекламе должно быть задействовано не менее указанного числа машин. Рекламодателю необходимо определить затраты на каждый вид рекламы — стикеров, листовок внутри салона, плакатов на наружной поверхности, и минимизировать суммарные затраты, учитывая требования предприятия по количеству задействованных машин. В данном случае постановка задачи сводится к классической модели задачи линейного программирования, при решении которой необходимо минимизировать линейную функцию затрат $Z(x) = c_1x_1 + c_2x_2 + c_3x_3$, где в качестве переменных выступают виды рекламной продукции, очевидно, что все переменные неотрицательны. Ограничения на транспортные средства задаются линейными неравенствами $a_{i1}x_1 + a_{i2}x_2 + a_{i\,3}x_3 \geq b_i$, в которых коэффициенты a_{ij} выражают число рекламных стикеров, листовок и плакатов, которое можно разместить на одном транспортном средстве каждого типа, b_i — минимальное число используемых машин каждого типа.

Существуют классические методы решения задач линейного программирования — графический и симплекс метод, также решение данных задач можно быстро найти с помощью компьютерных программ — математических пакетов и широко распространенного табличного процессора Microsoft Excel [2].

Для максимизации прибыли от размещения рекламы необходимо формулировать следующую задачу. Допустим, рекламодателю нужно определить, сколько и какого вида транспортных средств запрашивать у предприятия, если известна прибыль от размещения рекламы на каждом виде транспортных средств, например, на автобусах, микроавтобусах и маршрутных такси. При этом следует учитывать, что большее вынимание привлекают к себе новые машины. У рекламодателя существуют ограничения на затраты, в том числе на материалы — пленку, бумагу, дизайнерские и полиграфические услуги, а также ограничения на используемую поверхность. Последние требования могут быть прописаны в заключаемом договоре между рекламодателем и транспортным предприятием, например, на наружных стеклах допускается использование только перфорированной пленки; на боковых стеклах бортов допускается наружное размещение стикеров, размером 100×20, в количестве не более трех штук на одном транс-

портном средстве; внутри салонов на стеклах бортов допускается размещение стикеров, изготовленных на прозрачной пленке, размером 60×40, в количестве не более одного в каждом салоне транспортного средства; размещение информации на баннерных перетяжках допускается в салоне каждого транспортного средства в количестве не более двух перетяжек и т.п. При составлении задачи линейного программирования в представленной ситуации в качестве переменных нужно взять число машин каждого типа, т.е. число автобусов, микроавтобусов и маршрутных такси, и осуществить максимизацию функции прибыли $W(x) = c_1x_1 + c_2x_2 + c_3x_3$, при линейных ограничениях-неравенствах на затраты материальных и трудовых ресурсов.

Для увеличения эффекта от рекламы необходимо учитывать различные части населенного пункта, города, по которым осуществляются рейсы общественного транспорта. В центре города наблюдается большее скопление людей, значит эффект от рекламы будет более ощутимым при размещении на рейсах, проходящих по центру города. В другом случае наиболее эффективной будет реклама, если маршрут проходит в непосредственной близости от компании, рекламирующей услуги или товары. Допустим, рекламодатель намерен запросить некоторое число транспортных средств одного типа, например, автобусов, для проведения рекламной акции в различных частях города. Из предыдущего опыта известно, какую прибыль приносит реклама в зависимости от числа машин в каждой части города. Эти данные обычно представляются в виде таблицы. Математическая постановка задачи в данном случае заключается в следующем: нужно максимизировать целевую функцию прибыли $Z = \sum_{k=1}^{n} \phi_k(x_k) \rightarrow \max$, где n — число частей города, в которых планируется проводить рекламную акцию, переменные x_k — число транспортных средств, задействованных в каждой части города, функции ϕ_k определяют прибыль от числа транспортных средств с рекламой, курсирующих в k-той части города. Переменные x_k должны удовлетворять условиям $x_1 + x_2 + ... + x_n = A, x_k \geq 0$, ($k$ = 1, 2, …, n), где A — общее число транспортных средств, предоставленных рекламодателю. Данная задача является классической задачей динамического программирования о распределении средств. Решение задачи состоит двух этапов — условной и безусловной оптимизации. Этап условной оптими-

зации осуществляется по шагам, число шагов в данном случае определяется числом частей города. Для автоматизации расчетов при решении задачи можно также использовать табличный процессор *Microsoft Excel* или специально разработанные программные средства [3].

Реклама на транспортных средствах является популярной на сегодняшний день из-за того, что имеет большой охват целевой аудитории и сравнительно низкую затратность. Тем не менее для повышения ее эффективности нужно использовать данные статистики применения рекламы и проводить расчеты, используя различные математические модели и методы. Примеры, рассмотренные в статье, наглядно показывают, что для оптимизации рекламной акции можно использовать в том числе методы линейного и динамического программирования. При большом числе переменных в задаче и большом числе ограничений решение задачи можно осуществлять с использованием информационных технологий [4].

Литература

1. Архангельская, Е. В. Методы обработки статистических данных в правовых исследованиях // Вестник Саратовской государственной юридической академии. 2013. № 1 (90). С. 198—204.
2. Архангельская, Е. В. Курс информатики для юристов : учебно-методическое пособие. Саратов, 2008.
3. Архангельская, Е. В. Об одной реализации метода динамического программирования для решения задачи о замене оборудования с помощью прикладной программы // Системы и средства информатики. 2018. Т. 28. № 2. С. 178—188.
4. Проблемы и вызовы цифрового общества: тенденции развития правового регулирования цифровых трансформаций : монография в 2 томах. Том 2 / Е. Н. Абанина [и др.]. Саратов, 2020.

Боярчук Анна Владимировна,
кандидат исторических наук, преподаватель кафедры военно-политической работы в войсках (силах), Московское высшее общевойсковое командное училище

Тенденции и противоречия в строительстве Вооруженных Сил Российской Федерации на современном этапе развития общества

Аннотация. В настоящей статье автором рассмотрены основные закономерности построения и развития Вооруженных Сил РФ в соответствии с актуальными направлениями государственной военной политики на современном этапе. Анализируя факторы построения закономерностей развития Вооруженных Сил, автор приходит к выводу о существовании некоторых противоречий в построении военной организации государства, причина которых видится в отсутствии системных мер, направленных на установление взаимосвязи между регулированием вопросов обороны и иными государственно значимыми сферами жизни.

Ключевые слова: Вооруженные Силы Российской Федерации; военная доктрина; военное строительство; государственное управление; государственная политика.

Boiarchuk V. Anna,
candidate of Historical Sciences Lecturer at the Department of Military and Political Work in the in Troops (forces), the Moscow Higher Combined Arms Command School

Tendency and contradictions in construction of the military forces of the Russian Federation at the present stage of developmet

Abstract. In this article, the author considers the main patterns of the construction and development of the Military Forces of the Russian Federation in accordance with the current directions of state military policy at the present stage. Analyzing the factors of constructing patterns of development of the Military Forces, the author comes to the conclusion that there are some contradictions in the construc-

tion of the military organization of the state, the cause of which is seen in the absence of systemic measures aimed at establishing the relationship between the regulation of defense issues and other state-significant spheres of life.

Keywords: Military Forces of the Russian Federation; military doctrine; military construction; public administration; public policy.

Строительство Вооруженных Сил РФ как система взаимосвязанных мероприятий, реализуемых органами государственной власти в сфере военного управления, направлена на создание, подготовку и развитие вооруженных сил с учетом актуальных задач мирного и военного времени.

В связи с этим меры воздействия военно-политического руководства на сферу обороны обусловлены действующими угрозами территориальной целостности Российской Федерации, соображениями национальной и международной безопасности.

Основные принципы и задачи военного строительства заложены в Военной доктрине Российской Федерации (далее — Военная доктрина), утверждаемой Верховным Главнокомандующим — Президентом РФ. В настоящий момент действует Военная доктрина, утвержденная Президентом РФ 25.12.2014 № Пр-2976.

Согласно п. 37 Военной доктрины, основной задачей строительства и развития Вооруженных Сил выступает приведение их структуры, состава, численности и оснащенности современными (перспективными) образцами вооружения, военной и специальной техники в соответствие с прогнозируемыми военными угрозами, содержанием и характером военных конфликтов, задачами в мирное время, в период непосредственной угрозы агрессии и в военное время, а также с политическими, социально-экономическими, демографическими и военно-техническими условиями и возможностями Российской Федерации.

В п. 39 Военной доктрины указаны способы обеспечения реализации основных задач строительства и развития Вооруженных Сил, среди которых: эффективное военно-экономическое обеспечение и достаточное финансирование войск; повышение эффективности функционирования оборонно-промышленного комплекса; поддержание способности экономики страны обеспечить потребности Вооруженных Сил; эффективное обеспечение информационной безопасности Вооруженных Сил, других войск и органов; совершенствование

системы военного образования в специализированных образовательных учреждениях; повышение уровня реализации социальных гарантий прав военнослужащих и гражданского персонала; противодействие коррупции в органах управления Вооруженными Силами; совершенствование системы военно-патриотического воспитания граждан; обеспечения государственного и общественного контроля деятельности государственных органов в области обороны.

Приведенные положения Военной доктрины подчеркивают сущностные черты и закономерности развития Вооруженных Сил: будучи не только военной организацией, но и особым социальным институтом, его функционирование зависит от совокупности иных социальных факторов, носящих политический, экономический и культурный характер. Учет данных факторов позволяет судить о возможности стабильного и планомерного развития Вооруженных Сил в целом.

Исходя из этого, основные закономерности развития Вооруженных Сил можно сформулировать в следующем виде: сущность вооруженных сил, боеспособность войск, входящих в их состав, прямо зависят от экономической стабильности и безопасности государства, от культурно-идеологического уровня развития общества и от политической повестки государства.

В США одним из основных критериев оценки боеспособности армии выступает способность федерального бюджета удовлетворить потребности военной организации в своевременном и полномерном финансировании. В 2000-х гг. была разработана система «Планирование, программирование, разработка и исполнение бюджета», направленная на создание единой нормативно-взаимосвязанной схемы планирования реализации военных проектов и их финансового обеспечения с учетом возможностей войск противостоять внешним угрозам при реализации одного из сценариев развития сценариев развития военно-политической и стратегической обстановки в мире и его отдельных регионах[1].

Система планирования возможностей Вооруженных Сил РФ отражена в Военной доктрине: «реализация задач оснащения Вооруженных Сил, других войск и органов вооружением, военной и специальной техникой предусматривается в государственной программе во-

[1] Мединн А. О. Проблемы внедрения новой системы планирования строительства вооруженных сил США // Военная мысль. 2019. № 4. С. 63—64.

оружения и других государственных программах (планах)». Материальное обеспечение войск также осуществляется в соответствии с планированием возможных угроз и сценариев развития событий в военно-политической сфере.

Материально-техническое обеспечение Вооруженных Сил, в зависимости от степени возникновения военной угрозы, следует подразделить на три вида: обеспечение в период мирного времени (накопление и поддержание в боеготовности частей и соединений, вооружения и военной техники, предприятий оборонно-промышленного комплекса с учетом возможности их ускоренного перевода на режим военного времени), в период непосредственной угрозы (дообеспечение войск (сил) материальными средствами по штатам и нормам военного времени) и в период военного времени (передача запасов и ускоренное восполнение потерь вооружения и материальных средств).

В настоящий момент государство придерживается принципа максимизации капиталовложений в оборону и безопасность государства. Так, на плановый период 2022—2024 гг. расходы на национальную оборону в 2022 г. составят 3 510 419,6 млн руб., в 2023 г. — 3 557 223,3 млн руб. и в 2024 г. — 3 811 777,5 млн руб.[1] По замечанию председателя Комитета Государственной Думы по обороне А. В. Картаполова, «бюджетные расходы должны основываться не на несбыточных желаниях, а на исключительно прагматичных расчетах достижения поставленных программных целей и возможности контроля принимаемых решений»[2].

Материальное обеспечение собственно военнослужащих, удовлетворенность бытовыми условиями влияет на боеспособность войск, выступает залогом сосредоточенности служащих на выполнении служебных задач, вследствие чего указанный фактор связывает воедино экономический и идеологический компоненты боеспособности Вооруженных Сил.

Культурно-идеологическая составляющая в настоящее время концентрирует внимание военно-политического руководства государства и нацеливает на возрождение единой и масштабной системы поддержания боевого духа армии. В частности, задачей военно-

[1]Андрей Картаполов: «оборонный бюджет» на 2022—2024 сбалансирован и эффективен // URL: http://duma.gov.ru/news/52593/ (дата обращения: 10.01.2022).
[2] Там же.

политической работы является «обеспечение высокого уровня морально-политического и психологического состояния личного состава, правопорядка и воинской дисциплины, формирование у военнослужащих морально-политических и психологических качеств, сплоченных воинских коллективов, обеспечивающих выполнение задач по предназначению в любых условиях»[1]. Будучи одним из социальных институтов, как было отмечено ранее, статус Вооруженных Сил, их оценка обществом в целом непосредственно влияет на развитие армии и, с другой стороны, отражает реальное положение дел в самих Вооруженных Силах. В настоящий момент, по словам министра обороны РФ, генерала армии С. К. Шойгу, «по социологии 10—12-летней давности доверие к вооруженным силам в нашей стране было 27—29%. Была уверенность, что наша армия в состоянии защитить страну, что на нее можно надеяться. Сегодня это от 79% до 86% — это самый доверяемый институт в нашей стране»[2].

Рост доверия к армии, которая ассоциируется с мощью государства, обусловлен общим укреплением позиций нашей страны на международной арене, утверждением новой концепции внешней политики России, сочетающей принципы миролюбия, уважения суверенитета других государств, построения системы коллективной международной безопасности, неконфронтации с государствами и народами. Так, в Концепции внешней политики Российской Федерации, утвержденной Указом Президента РФ от 30.11.2016 № 640, подчеркивается нацеленность на обеспечение безопасности нашего государства, упрочении позиций Российской Федерации как одного из влиятельных центров современного мира при одновременном продвижении курса на укрепление международного мира, соблюдение общепринятых норм и принципов международного права, формирование отношений добрососедства с сопредельными государствами и предотвращение очагов вооруженных конфликтов.

В то же время, несмотря на стремление государства обеспечить закономерное развитие Вооруженных Сил, мы можем наблюдать противоречивые тенденции, обусловленные пробельным характером воздействия управленческой силы государственного механизма на сферу обороны. Наиболее болезненным элементом в строительстве Воору-

[1] Приказ Министра обороны РФ от 22.07.2019 № 404 «Об организации военно-политической работы в Вооруженных Силах Российской Федерации».
[2] URL: https://tass.ru/armiya-i-opk/12099069 (дата обращения: 10.01.2022).

женных Сил, как и во многих других сферах общественной жизни с участием государства, является коррупция.

Стоит отметить, однако, что в последнее время наблюдается нацеленность на ликвидацию правового пробела в регулировании противодействия коррупции в армии. В Плане противодействия коррупции в Вооруженных Силах Российской Федерации на 2021—2024 годы (утвержден приказом Министра обороны РФ от 17.09.2021 № 555) сформулированы основные направления антикоррупционной борьбы: повышение эффективности механизмов урегулирования конфликта интересов, организация оценки коррупционных рисков и внедрения антикоррупционной экспертизы нормативных документов, принимаемых органами управления Вооруженных Сил.

Другим значимым элементом противоречия в развитии Вооруженных Сил выступает система контроля. Несмотря на нацеленность государства внедрить внешний, гражданский контроль в рамках данного института, степень общественного участия представляется смутным образом ввиду сущностных особенностей военной организации. Вооруженные Силы — закрытая организация, многие стороны жизни которой по соображениям национальной безопасности охраняются режимом государственной тайны, в частности, некоторые расходные статьи федерального бюджета. Промежуточным звеном, по мнению Ф. С. Бородина, может стать установление специализированного контроля со стороны прокуратуры, в частности посредством создания специализированного подразделения возможно осуществление и внешнего независимого бюджетного контроля[1].

Таким образом, преодоление противоречий и пробелов в закономерном и поступательном развитии Вооруженных Сил РФ видится нами в систематизации регулирования основ военного строительства, построения взаимосвязи между компонентами системы построения и развития Вооруженных Сил и внешними институтами: гражданским обществом, институтами антикоррупционного воздействия, научным и образовательным сообществом, дипломатической сферой. В таком случае стратегические инициативы, заложенные в программных документах в сфере обороны, найдут свое качественное воплощение.

[1] Бородин Ф. С. Исполнение бюджетного законодательства в Вооруженных силах РФ: Актуальные вопросы контроля и прокурорского надзора // Вестник ННГУ. 2016. № 6. С. 107.

Вологдина Екатерина Сергеевна,
старший преподаватель кафедры административного права и таможенного дела Юридического факультета Забайкальского государственного университета

О некоторых аспектах правового регулирования кибербезопасности в Китайской Народной Республике

Аннотация. Автором анализируются особенности правового регулирования кибербезопасности на примере Китайской Народной Республики, акцентируется внимание на отдельных проблемных аспектах и практических вопросах предметного регулирования, которые направлены на противодействие киберугрозам и совершенствование исследуемого феномена.

Ключевые слова: информационная безопасность; кибербезопасность; киберпространство; киберугрозы; Закон «О кибербезопасности КНР».

Ekaterina S. Vologdina,
Senior Lecturer, Department of Administrative Law and Customs Affairs Transbaikal State University

On some aspects of legal regulation of cybersecurity in the People's Republic of China

Abstract. The author analyzes the features of the legal regulation of cybersecurity on the example of the People's Republic of China, focuses on certain problematic aspects and practical issues of subject regulation, which are aimed at countering cyberthreats and improving the phenomenon under study.

Keywords: information security, cybersecurity, cyberspace, cyber threats, Law «On Cybersecurity of the People's Republic of China».

В современном мире проблемы обеспечения кибербезопасности становятся имманентным условием для развития информационного общества. В данный момент особое внимание уделено вопросам обеспечения безопасности и стабильности в киберпространстве, что оказывает влияние на суверенитет, национальные интересы всех стран мира. Одна из основных проблем — это отсутствие междуна-

родной правовой системы, юридически устанавливающей нормы и правила поведения в этой сфере, о которой дискутируют многие ученые, в том числе исследователи [2; 3]. Назревшая правовая и организационная проблематика обеспечения мировой кибербезопасности на современном этапе усиливает уровень реагирования на новейшие риски и актуализируют требования к уровню информационной защиты данных субъектов различных правоотношений.

Центральной идеей исследуемой категории является утверждение о том, что кибербезопасность как неотъемлемая часть в системе национальной безопасности многих государств, вопросы ускоренного развития новых прорывных технологий в последние несколько лет являются острой проблемой развития многих стран [1; 4], в том числе и Китая. Возникновение новых вызовов и угроз (как реальных, так и мнимых), террористические и экстремистские атаки, кибератаки и киберугрозы, дестабилизация политической, экономической обстановки за счет распространения дезинформации через информационно-коммуникационные технологии и социальные сети, безусловно, актуализировали вопросы обеспечения кибербезопасности на пространстве всех мировых держав, в том числе и Китая. Кроме того, необходимо отметить, что в Китае за период 2019—2020 гг. наблюдались кибератаки на общемировые гиганты техноиндустрии, в частности Huawei, Alibaba, ZTE, технологии 5G, облачные хранилища и др. В связи с этим констатируем, что развитие структуры современных информационно-коммуникационных технологий неразрывно связано с важностью и необходимостью обеспечения глобальной конкурентоспособности и безопасности.

Не решенными на сегодняшний день являются вопросы определения границ внутри такого пространства в связи с развитием Интернета в количественном (например, увеличение интернет-пользователей) и качественном отношении (например, развитие интернет-услуг), поскольку на международном уровне нередко происходят взаимные обвинения стран в распространении ложной и фальсифицированной информации, вредоносных вирусов, логических бомб, троянов. Интерес Китая к киберпространству и возможностям его использования чрезвычайно велик, что обусловлено применением комплексного подхода трансформации системы: от законодательных инициатив до стратегий международного сотрудничества в киберпространстве.

Для исследования сущностных характеристик данного феномена и аспектов его правового регулирования, необходимо проанализировать законодательную базу управления киберпространством в Китайской Народной Республике и рассмотреть организационную структуру органов, участвующих в обеспечении кибербезопасности.

Правовая практика по обеспечению кибербезопасности в КНР начинает формироваться с 2000 г., когда Всекитайским собранием народных представителей были предприняты организационно-правовые меры по защите интернет-пространства, что позволило определить систему возможных правонарушений в информационной сфере. Затем, в 2003 г. Канцелярией Центрального Комитета Коммунистической партии Китая было принято Постановление государственной информатизированной руководящей группы по работе в области укрепления информационной безопасности [5], которое регламентировало обязанности ответственных субъектов информационных правоотношений в сфере защиты стратегической инфраструктуры и предусмотрело процедуру проведения мониторинга интернет-пространства на наличие возможных или реальных уязвимостей в виде киберугроз и атак.

В дальнейшем информационное пространство КНР формируется как «новая область», которая охвачена повышенным вниманием развития информационных технологий и стратегических направлений процессов информатизации в стране. Подтверждением вышесказанного явилось принятие Государственной стратегии по развитию информатизации КНР на период с 2006 по 2020 годы. В Стратегии КНР усматриваются предпосылки формирования единого информационного пространства. Также в положениях исследуемого документа урегулированы наиболее уязвимые сферы жизнедеятельности человека и государства: политическая, экономическая, социальная и культурная. Кроме этого, активно начинают внедряться новые информационные идеи и концепции. Всеобщее распространение получили концепция «активной обороны и симметричного ответа на возникающие угрозы» и идея «здорового информационного общества, развития интернет-культуры в Китае». Следовательно, одним из ключевых направлений Стратегии признано создание национальной системы защиты информационной безопасности и укрепление цифрового суверенитета, которая направлена не только на обеспечение кибербезопасности страны, но и на защиту данных граждан в сети Интернет.

В положениях стратегического документа впервые появилось единое законодательное закрепление понятия «киберпространство», которje не упоминалось в ранее принятых правовых актах. Киберпространство рассматривается как «виртуальное пространство общественной деятельности, созданное людьми на основе информационных технологий и являющееся новой областью, вошедшей в повседневную жизнь людей» [6]. Правовой анализ Стратегии объективно подтверждает, что процессы трансформации и модернизации традиционных отраслей промышленности и торговли Китая, изменения направлений экономического потенциала и развития страны формируются под воздействием сети Интернет, которая давно стала движущей силой инновационного развития, и в то же время создала новые вызовы и угрозы. Итак, в Стратегии впервые изложено понимание необходимости обеспечения кибербезопасности, что возможно достичь путем успешного управления киберпространством.

В 2016 г. в Китае был принят специальный Закон «О борьбе с терроризмом», в положениях которого усматривается противодействие киберугрозам, выразившееся в балканизации трансграничного распространения информации террористического, экстремистского содержания в глобальной сети Интернет. Примечательно и то, что на территории Китая закон ввел цензуру для новостной деятельности, наделив специальными полномочиями соответствующие органы государственной власти.

Следующий важный вектор формирования кибербезопасности ознаменовал Закон «О кибербезопасности КНР» (известный под названием как Закон «об интернет-безопасности»)[1]. Цель принятия Закона вполне очевидна и состоит в обеспечении национальной и сетевой безопасности, защите национального «киберсуверенитета» Китая, прав и интересов государства, граждан, юридических лиц и других субъектов публичных правоотношений. Проведенный анализ закона позволил выявить отдельные аспекты предметного регулирования, которые направлены на противодействие киберугрозам. В частности, Закон установил обязательства к субъектам — сетевым операторам, операторам критически важной информационной инфраструк-

[1] Закон «О кибербезопасности КНР» был принят на 24-м заседании Всекитайского собрания народных представителей 7 ноября 2016 г. и вступил в силу 1 июня 2017 г.

туры (к таковым относятся предприятия в сфере общественных коммуникаций, обороны, транспорта, энергетики, водоснабжения, финансов, электронного правительства, институт государственной службы), поставщикам сетевых продуктов и услуг (ст. 21, 24, 25, 26, 28, 42 и 47) [7].

В этом отношении показательны следующие положения. Во-первых, поставщики серверов и услуг обязаны своевременно обеспечить информирование пользователей и соответствующие компетентные органы о любых ставших известными уязвимостях и угрозах в области безопасности и принять необходимые меры по их устранению. При этом порядок такого информирования закон не раскрывает. Во-вторых, в случае, если серверы собирают и используют личные данные пользователей, то поставщики обязаны их уведомлять об этом. В-третьих, сбор и хранение личных данных пользователей должны осуществляться только в целях, официально обозначенных поставщиком интернет-услуг. И в-четвертых, за счет введения всеобщего требования об обязательной верификации для доступа к сети исключается анонимность пользователей.

Рассматривая аспекты правового регулирования исследуемого феномена, необходимо назвать несколько фундаментальных положений, которые представляют интерес для китайской правовой науки с позиции установления релевантности развития законодательства о кибербезопасности для других стран. Так, в Законе «О кибербезопасности КНР» регламентированы организационные меры, направленные на повышение уровня грамотности населения в области кибербезопасности и ориентированности населения в киберпространстве (безусловно, при участии органов государственного управления всех уровней и средств массовой информации); тотальное ужесточение требований к профессиональной подготовке сотрудников сферы информационной безопасности через введение полного запрета на хранение данных за пределами Китая; закупка сетевых серверов и услуг должна осуществляться под контролем уполномоченных государственных органов, а предприятия в критически важных отраслях обязаны проводить ежегодную оценку рисков и угроз безопасности и отражать полученные результаты в отчетах. Кроме этого, в случае выявления нарушений предусмотрены санкции в виде штрафов в зависимости от тяжести киберпреступления.

Необходимо акцентировать внимание, что в нормах рассматриваемого Закона предусмотрена попытка выделения информационного суверенитета государства, что подтверждается разработкой новых механизмов контроля информационного пространства, следствием чего является установление запретов и ограничений. Общеизвестно, что на территории КНДР с 2000 г. функционирует сеть Кванмен, представляющая собой пример Интранета (внутреннюю сеть организации, использующую стандарты, протоколы и технологии сети Интернет).

Итак, Закон о кибербезопасности КНР определил безусловную передовую модель и главные направления обеспечения киберпространства. Позволил обобщить стратегические принципы, определяющие действия страны в области кибербезопасности.

Обращаясь к рассмотрению организационной структуры государственного аппарата Китая, констатируем, что она включает широкий перечень органов, наделенных полномочиями в исследуемой сфере и состоит из партийного аппарата КНР и военных структур по обеспечению кибербезопасности. Координирующую роль играет Центральная комиссия по киберпространству. Военные структуры Народно-освободительной армии Китая (НОАК) наделены разведывательными полномочиями, связанными с поиском атак и угроз в информационных системах. В структуре государственного аппарата созданы специализированные подразделения (министерства, комитеты, институты, бюро), функции которых направлены на формирование национальной стратегии страны и на решение вопросов обеспечения кибербезопасности. Назовем некоторые из них: Министерство государственной безопасности, Центральный комитет по кибербезопасности и информатизации, Научно-исследовательский институт безопасности, Бюро общественной информации и надзора за сетевой безопасностью.

Таким образом, в Китае продолжает формироваться система правового регулирования данных, информации, вопросов обеспечения безопасности личности в информационном пространстве. Что, безусловно, подтверждается принятыми ранее актами (например, Законы «О безопасности данных», «О сетевой безопасности») и вступившими в силу 1 сентября и 1 ноября 2021 г. Законами «О безопасности данных», «О защите персональных данных».

Изучение аспектов правового регулирования и практического опыта Китайской Народной Республики в вопросах кибербезопасности объективно доказывает, что одним из достоинств является наличие специализированных, уполномоченных государственных органов, отвечающих за обеспечение кибербезопасности.

Литература

1. Лобач Д. В., Смирнова Е. А. Политико-правовые меры обеспечения кибербезопасности в Китайской народной республике на современном этапе // Азиатско-Тихоокеанский регион: экономика, политика, право. 2020. № 1. С. 118—130.
2. Chebotarev V.E., Rozanov A.S. Communication society and security: Current threats and legal maintenance // Digital Communication Management. — InTech Open Science Croatia, Spain, 2018. P. 135—182. DOI: https://dx.doi.org/10.15405/epsbs.2018.09.02.72.
3. Chebotareva Anna A., Kazantseva Natalia G., Vologdina Ekaterina S., Grigorian T.V., Sukhanova I.S. Digital transformation and artificial intelligence in the activities of customs services in Russia and foreign countries // RUDN Conference on Legal Theory, Methodology and Regulatory Practice (RUDN LTMRP Conference 2021): сборник РУДН Международной научно-практической конференции, 2021 P. 1—6. DOI: https://doi.org/10.1051/shsconf/202111804014.
4. Chebotareva A.A., Kazantseva N.G , Vologdina E.S. Artificial Intelligence and Information Security: Legal regulation, prospects, and risks (real and perceived threats) // Proceedings of the International Scientific and Practical Conference on Computer and Information Security — INFSEC, Russian Federation, Yekaterinburg, 2021. ISBN:978-989-758-531-9. P. 110—115. DOI: 10.5220/0010619400003170.
5. 国家信息化领导小组关于加强信息安全保障工作的意见 (Guójiā xìnxī huà lǐngdǎo xiǎozǔ guānyú jiāqiáng xìnxī ānquán bǎozhàng gōngzuò de yìjiàn; Постановление государственной информатизированной руководящей группы по работе в области укрепления информационной безопасности). 26.08.2003. URL: https://wenku.baidu.com/view/bdfba07271fe910ef02df886.html (дата обращения: 01.02.2022).
6. National informatization Development Strategy 2006—2020 // China Copyright and Media. — URL: https://chinacopyrightandmedia.wordpress.com/2006/03/19/2006-2020-national-informatization-development-strategy/ (дата обращения: 20.01.2022).

7. 国务院关于深化制造业与互联网融合发展的指导意见 [Law of the People's Republic of China on cybersecurity]. — URL: http://www.npc.gov.cn/npc/xinwen/ 201611/07/content_2001605.htm/ (дата обращения 25.01.2022).

Горенская Елена Владимировна,
кандидат юридических наук, доцент, старший научный сотрудник Института законодательства и сравнительного правоведения при Правительстве Российской Федерации

К вопросу о кибербезопасности автомобильного транспорта

Аннотация. В статье рассмотрены понятийно-содержательные аспекты такого важного направления безопасности автомобильного транспорта, как кибербезопасность. Определены пути совершенствования кибербезопасности автомобильного транспорта, в том числе внедрение цифровых технологий и беспилотных транспортных средств, построение Единой цифровой транспортно-логистической среды, а также использование онлайн-тахографов. Обоснован вывод о необходимости повышения уровня кибербезопасности автомобильного транспорта путем проведения мероприятий на государственном уровне.

Ключевые слова: автомобильный транспорт; автомобиль; безопасность; кибербезопасность; киберзащищенность; тахограф.

Elena V. Gorenskaya,
Candidate of Legal Sciences, Associate Professor, Senior Researcher Institute of Legislation and Comparative Law under the Government of the Russian Federation

On the issue of cybersecurity of road transport

Abstract. The article discusses the conceptual and substantive aspects of such an important area of road transport security as cybersecurity. The ways of improving the cybersecurity of road transport, including the introduction of digital technologies and unmanned vehicles, the construction of a unified digital transport and logistics environment, as well as the use of online tachographs, have been identi-

fied. The conclusion about the need to increase the level of cybersecurity of road transport by holding events at the state level is substantiated.

Keywords: automobile transport; automobile; security; cybersecurity; cyber security; tachograph.

Автомобильный транспорт (АТ) — один из самых распространенных видов транспорта, образующих в совокупности транспортную систему Российской Федерации, отличающийся скоростью доставки и маневренностью, позволяющей изменить маршрут в случае возникновения форс-мажора, однако у него небольшая грузоподъемность и высокая себестоимость эксплуатации (с учетом цены на топливо). На сегодняшний день около 56 млн транспортных средств (ТС), в том числе автомобильных транспортных средств (АТС), являются единицами автомобильного транспорта. Около миллиона из них задействовано в пассажирских перевозках (в основном, это автобусы, на которых перевозится 90% пассажиров). И в данной ситуации остро встает вопрос обеспечения безопасности пассажирских перевозок, сохранности грузов и багажа, а также самих транспортных средств [1].

При этом с учетом современного развития концепции цифрового государства и цифровой правовой среды [2] речь идет уже не просто об обеспечении безопасности [3], а кибербезопасности объектов автомобильного транспорта, к которым относятся «объекты автотранспортного бизнеса, включая предприятия отрасли и занимаемые ими земельные участки с коммуникациями, производственные и вспомогательные здания и сооружения, технологическое и вспомогательное оборудование, нематериальные активы (транспортные и производственные технологии, нормативно-техническая документация, изобретения, ноу-хау и т.п.), объекты инфраструктуры предприятий и организаций автомобильного транспорта» (см. п. 2.5 Требований к исполнителю услуг по оценке автотранспортных средств и объектов отрасли автомобильного транспорта. РД-03112194-1039-99. Система «СЕРТОЦАТ»).

Возникает вопрос о содержании термина «кибербезопасность», который в настоящее время законодательно не закреплен. Специалисты предлагают следующее определение: «кибербезопасность — условия защищенности от физических, духовных, финансовых, политических, эмоциональных, профессиональных, психологических, образователь-

ных или других типов воздействий или последствий аварии, повреждения, ошибки, несчастного случая, вреда или любого другого события в киберпространстве, которые могли бы считаться не желательными» [4].

В данном случае, на наш взгляд, происходит увязка одного термина, который не имеет законодательного закрепления, с другим термином — «киберпространство», который упоминается в ряде нормативных правовых актов, однако его дефиниция в данных актах не приводится. Более или менее легально можно использовать понятия, имеющиеся в Международном стандарте ISO/IEC 27032:2012 Information technology, в котором под «киберпространством» понимается сфера деятельности в информационном пространстве, образованная совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства), а под «кибербезопасностью» — совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями. Интересным представляется определение киберпространства как «пространства функционирования продуктов информационно-коммуникационных технологий, позволяющих создавать чрезвычайно сложные системы взаимодействий агентов с целью получения информации, обмена и управления ею, а также осуществления коммуникаций в условиях множества различных сетей» [5].

На наш взгляд, если рассматривать кибербезопасность как направление безопасности автомобильного транспорта, то его можно трактовать двояко:

1) в широком смысле — как совокупность условий, при которых все составляющие киберпространства, связанного с автомобильным транспортом (и в целом с транспортной системой страны [6]), защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями (сайты, системы, серверы, средства управления и контроля и др.);

2) в узком смысле — как защиту определенного объекта автомобильного транспорта или автомобильного транспортного средства от

любых инцидентов, от актов незаконного вмешательства, а также от преступных посягательств (здесь речь идет о степени защиты системы управления объектом АТ или АТС, их оборудованности средствами активной (высокая устойчивость, отличная управляемость, надежные тормозные свойства) и пассивной (специальная конструкция кузова, ремни, подушки безопасности) безопасности, многие из которых сейчас управляются дистанционно, в том числе через Интернет).

Одним из самых перспективных путей совершенствования безопасности автомобильного транспорта, в том числе ее киберсоставляющей, является построение Единой цифровой транспортно-логистической среды (ЕЦТЛС). По мнению А. Семенова — заместителя Мминистра транспорта РФ, «ЕЦТЛС — это не просто множество цифровых платформ. Для быстрого и безопасного обмена актуальными, унифицированными и достоверными данными обо всех этапах перевозки в реальном режиме времени необходима именно единая доверенная среда, которой и является ЕЦТЛС. Сервисы цифровой платформы позволяют реализовать взаимодействие с партнерами — странами ЕАЭС, со всей мировой транспортной системой в режиме «единого окна». Целями проекта являются повышение эффективности управления транспортным комплексом, его интеграция в мировую цифровую транспортную систему. Особое внимание при реализации проекта уделяется безопасности российской транспортной системы»[1].

Второй путь — комплексное применение цифровых систем мониторинга, контроля и поддержания работоспособного состояния водителя, помогающих заблаговременно выявлять и предотвращать опасные состояния, которые могут вызвать потерю внимания и снижение работоспособности в пути, — как наиболее эффективное средство контроля факторов поведения и состояния водителя.

Министр транспорта РФ В. Савельев назвал одним из приоритетов в развитии транспортной отрасли внедрение цифровых технологий и беспилотных транспортных средств[2]. Так, Минтрансом России прорабатывается вопрос повсеместного использования онлайн-

[1] https://mintrans.gov.ru/press-center/interviews/508
[2] https://mintrans.gov.ru/press-center/news/10012

тахографов, которые будут фиксировать нарушение максимальной скорости, установленной правилами дорожного движения для конкретного транспортного средства[1]. В рамках реализации пилотного проекта по сбору, хранению, обработке и передаче информации из тахографов прорабатывается возможность осуществления передачи данных в АИС «Тахографический контроль» со всех устройств через тахограф, что в конечном итоге позволит владельцам транспортных средств использовать одно передающее устройство в составе тахографа и, как следствие, одну sim-карту.

Помимо этого, целесообразно повышать степень киберзащищенности автотранспортных средств, включая дистанционный контроль за системой торможения и рулевого управления движущихся автомобилей (учитывая, что автомобили становятся все более компьютеризованными, возрастает опасность использования данного факта в преступных целях, а взлом или перехват управления автомобилем могут иметь крайне серьезные последствия). Специалисты в России и за рубежом включают в понятие киберзащищенности: устойчивость компьютерных систем автомобиля против кибервзлома (особенно управляемых через беспроводное подключение (*Wi-Fi*- и *bluetooth*-модули), например, подсистем, влияющих на работу тормозов или датчики парковки), установку в автомобилях самописцев, регулярное обновление программного обеспечения и аппаратных устройств, внедрение принципов сегментированности электронных систем автомобиля.

В данном случае необходимо отметить, что автомобили, обладающие высокой степенью компьютеризации, подвержены «IT-угонам» [7]. Соответственно, любой объект АТ, например автопарк, может подвергнуться такой кибератаке. Так, в декабре 2020 г. сотрудниками УУР ГУ МВД России по Свердловской области совместно с ОУР УМВД России по г. Екатеринбургу была пресечена деятельность организованной группы, похищавших корейские и японские легковые машины (возбуждено уголовное дело по ч. 4 ст. 158 УК РФ). Пре-

[1] См.: Приказы Минтранса России от 13.02.2013 № 36 «Об утверждении требований к тахографам, устанавливаемым на транспортные средства, категорий и видов транспортных средств, оснащаемых тахографами, правил использования, обслуживания и контроля работы тахографов, установленных на транспортные средства», и от 21.08.2013 № 273 «Об утверждении Порядка оснащения транспортных средств тахографами».

ступники устанавливали в автомобили перепрограммированные электронные блоки управления двигателем, а машины с сигнализацией открывали с помощью код-грабберов и ретрансляторов сигнала бесконтактных электронных ключей. Примечательно, что 20 лет назад о таких технических достижениях писали фантасты, а автовладельцы ставили противоугонки типа «Саргис» или «Полкан», фиксировали руль, клали на заднее сиденье милицейскую фуражку и т.п. [8]

Таким образом, приветствуя технический прогресс, необходимо повышать уровень кибербезопасности автомобильного транспорта путем совершенствования правового регулирования (в том числе закрепления на законодательном уровне понятий и приоритетных направлений кибербезопасности), моделирования ситуаций, угрожающих кибербезопасности, механизмов реагирования и защиты, в том числе уголовно-правовых и административных [9], а также эффективного выполнения мероприятий, предусмотренных Транспортной стратегией Российской Федерации до 2030 года с прогнозом на период до 2035 года, утвержденной паспоряжением Правительства РФ от 27.11.2021 № 3363-р.

Литература

1. Транспортная безопасность и противодействие терроризму на транспорте: правовые и организационные аспекты: сборник научных трудов по результатам II Международного научного форума / ответственные редакторы В. М. Корякин, Е. А. Нестеров. Москва : Российский университет транспорта, Юридический институт, 2021.
2. Концепция цифрового государства и цифровой правовой среды: монография / Н. Н. Черногор [и др.]. Москва : ИЗиСП при Правительстве РФ: Норма: ИНФРА-М, 2021.
3. Трансформация правовой реальности в цифровую эпоху: сборник научных трудов / под общей редакцией Д. А. Пашенцева, М. В. Залоило. Москва : ИЗиСП при Правительстве РФ: ИНФРА-М, 2019.
4. Алпеев, А. С. Терминология безопасности: кибербезопасность, информационная безопасность // Вопросы кибербезопасности. 2014. № 5(8). С. 39—42.
5. Добринская, Д. Е. Киберпространство: территория современной жизни // Вестник Московского университета. 2018. Т. 24. № 1. С. 52—70.

6. Лещов, Г. Ю. О контроле качества подготовки сил обеспечения транспортной безопасности: сборник материалов круглого стола / под общей редакцией Т. А. Дикановой. Москва, 2019.
7. Горенская, Е. В. Береги железного «коня» // Интерпол в России. 2000. № 4. С. 28—30.
8. Горенская, Е. В. Проблемы борьбы с нелегальным автобизнесом. Москва : Московский институт МВД России, 2001.
9. Нудель, С. Л. Уголовно-правовое воздействие в механизме обеспечения экономической безопасности (проблемы и тенденции законодательной регламентации) // Журнал российского права. 2020. № 6. С. 106—119.

Данилина Елена Ивановна,
доктор экономических наук, профессор, профессор кафедры «Административное право, экологическое право, информационное право», Юридический институт Российского университета транспорта (МИИТ)

Эфендиев Тахир Сейпуевич,
кандидат юридических наук, доцент кафедры «Административное право, экологическое право, информационное право», Юридический институт Российского университета транспорта (МИИТ)

Особенности цифровизации и кибербезопасности российских железных дорог

Аннотация. В статье рассмотрены результаты внедрения цифровизации, проблемы и пути их устранения на железнодорожном транспорте. Особое внимание уделено кибербезопасности российских железных дорог. Представлен отечественный и зарубежный опыт проведения цифровизации на транспорте.

Ключевые слова: цифровизация; железнодорожный транспорт; информационные ресурсы; кибербезопасность; прогнозирование.

Danilina I. Elena,
Doctor of Economic Sciences, Professor, Professor of Department «Administrative Law, Environmental Law, information law», Russian University of Transport

Efendiev S. Tahir,
PhD in Economics, assistant professor Department «Administrative Law, Environmental Law, information law», Russian University of Transport

Features of digitalization and cybersecurity of Russian railways

Abstract. The article discusses the results of the introduction of digitalization, problems and ways to eliminate them in railway transport. Special attention is paid to the cybersecurity of Russian railways. The domestic and foreign experience of digitalization in transport is presented.

Keywords: digitalization; railway transport; information resources; cybersecurity; forecasting.

В настоящее время происходит стремительное развитие цифровизации в том числе на транспорте, что позволяет не только оптимизировать затраты, но и повышать удобство для пассажиров. В ближайшем будущем внедрится искусственный интеллект в объекты инфраструктуры, в частности, имеет место результат применения автоматизированных технологических процессов на железнодорожном транспорте, что показывает наглядно возможности цифровизации перевозочного процесса[1]. В процессе внедрения данных инноваций можно видеть, что основное внимание в цифровизации обращено на автоматизацию технологических процессов, позволяющее обеспечить гарантию безопасности и повышения качества перевозок.

Говоря о значимости искусственного интеллекта, необходимо отметить, что его роль в большей степени сейчас проявляется при работе с персоналом и при принятии решений при нештатных ситуациях. Здесь выявляется проблема необходимости замены устаревших технологий, которую можно устранить на основе использования передового зарубежного опыта. Для этого предусмотрено развитие технологий «автоматического построения графика движения поездов», перехода к киберфизическим системам управления движением поездов, создания автоматических комплексов управления движением поездов на основе цифровой инфраструктуры. В практике развития железно-

[1] Смагин Ю. С., Ефремов А. Ю. Первая цифровая система централизации в Германии // Железные дороги мира. 2018. № 8. С. 63—67.

дорожного транспорта выделены особенности и необходимость внедрения систем автоведения вплоть до полной автоматизации и беспилотного выполнения отдельных операций; внедрение систем автоматического диспетчерского управления движением поездов на основе технологий нейронных сетей и искусственного интеллекта. Данные изменения невозможны без цифровизации базового уровня инфраструктуры, что предусматривает переоснащение соответствующего оборудования.

Как видно из опыта внедрения искусственного интеллекта, на сегодняшний день необходимо использовать роботизированные и киберфизические системы, позволяющие в дальнейшем использовать и объединять «умные» сети и наделяемые «умной» оболочкой обработки получаемых данных. Это говорит о том, что основное значение в развитии цифрового железнодорожного комплекса отводится совершенствованию и интеллектуализации систем технического диагностирования и мониторинга. Как отмечается в зарубежных источниках, сейчас средства технического диагностирования и мониторинга используются в основном как объекты, позволяющие автоматизировать работы по ручному техническому обслуживанию и не включают в себя искусственный интеллект, т.е. они работают по фиксации достижений пороговых границ отказов и предотказных состояний каждого отдельного диагностического параметра[1]. Также мы видим, что указанные системы широко внедрены в практику, например в работе со средствами железнодорожной автоматики и телемеханики, однако реального эффекта не приносят[2].

Разработка, совершенствование данных систем позволят осуществлять оперативное диагностирование и достоверное прогнозирование. Это дает возможности для оптимизации ведения поездов с учетом возникающих дефектов. Как показывают исследования коллектива авторов[3], системы технического диагностирования и мониторинга на железнодорожном транспорте подобную задачу не решали.

---

[1] Heidmann L.Smart Point Machines: Paving the Way for Predictive Maintenance // Sign.+Draht. 2018. Is. 9. P.70—75.

[2] Ефанов Д . В . Функциональный контроль и мониторинг устройств железнодорожной автоматики и телемеханики. Санкт-Петербург : ФГБОУ ВО ПГУПС, 2016.

[3] Романчиков А. М. и др. Цифровизация железнодорожного транспорта в России // Транспорт Российской Федерации. 2018. № 6 (79). С. 10—13.

Однако без наделения их новыми свойствами невозможно перейти к улучшенной версии железнодорожного комплекса. Авторы показывают, что интеграция и сбалансированное распределение функций управления движением поездов между «умным» цифровым локомотивом и цифровыми системами автоматики, диагностики и диспетчеризации создадут комплекс по управлению перевозочным процессом нового уровня, способный к разрешению конфликтов и оптимизации графика с учетом изменений в реальном времени. Именно такие шаги представляют собой базовые важнейшие технологии в решении задачи построения «умного» железнодорожного комплекса, находящегося на передовых позициях в транспортных системах регионов.

Необходимо отметить, что в данных разработках рекомендуется учитывать и кибербезопасность, особенно при искусственном искажении информации должно быть обеспечено безошибочное управление движением поездов.

Основная цель при решении проблем кибербезопасности в ОАО «РЖД» — сохранение способности различных программно-аппаратных систем автоматического управления обеспечивать безопасное и эффективное выполнение возложенных на них функциональных задач в условиях целенаправленных, умышленных, несанкционированно-деструктивных и, как правило, дистанционно-безуликовых воздействий различной физической природы. В первую очередь защищаются системы, при сбое функционирования которых есть угроза жизни и здоровью пассажиров, угроза утраты или порчи грузов, при этом унифицировать программно-аппаратные решения не получается.

Как показывают исследования, до сих пор объектами кибератак на железнодорожном транспорте могут являться системы диспетчерской и электрической централизации, формирующие безопасные маршруты движения поездов, системы обеспечения безопасного движения локомотивов и проезда железнодорожных переездов, системы защиты и регулирования электроснабжения, системы горочной автоматики, ответственные за сборку и расформирование поездов. Также с использованием летальных и нелетальных психофизических технологий могут проводиться атаки на операторов и обслуживающий персонал — диспетчеров, дежурных и машинистов.

В соответствии с полученными данными на сегодняшний день уже разработана классификация кибератак на железную дорогу, а также

определены меры для противодействия возможным кибератакам, в том числе развитие отечественного производства, осуществление легендирования и централизации закупок, необходимость обязательного обеспечения входного контроля, тестирования комплектующих, что позволит снизить риски негативных последствий цифровизации.

Elhoucine Chougrani,
Associate Professor of International Law,
University Cadi Ayyad-Marrakesh

The Copenhagen School's Securitization Theory and the Cyber Security Concept

Abstract. The Copenhagen school securitization is a reference in the fields of military-political, societal, and environmental securitization theory. Incorporating cyber security into the Copenhagen school theory covers a variety of issues, particularly critical security studies. The importance of the Copenhagen school's constructivist approach to security studies needs no demonstration. Yet, its weakness is in how to integrate cyber security concepts and ensure the complexity analysis for securitization under various geopolitical and economic contexts worldwide especially in the Global South.

Keywords: The Copenhagen School; Constructivist Approach; Securitization Theory; Cyber Security; Critical Security.

Introduction

The term Copenhagen school refers to the University of Copenhagen, which was home to the proponents of the securitization approach*. The importance of the Copenhagen school is that it brings a social perspective to security studies. This school is best known through Barry Buzan, Ole Waever, and Jaap Dewilde. The Copenhagen school elaborately systema-

* Security is the core concept. The foreign military and economic policies of States, the intersection of these policies in areas of change or dispute, and the general structure of relations which they create, are all analyzed in terms of national and international security. Barry Buzan. People, States and Fear. The National Security Problem in International Relations (Wheatsheaf Books, 1983). P. 3.

tized the deepening and broadening of security studies, both with sectors and levels of analysis, and then through securitization theory[1].

Arguably, amalgamate the cyber security concept into the Copenhagen securitization theory academically and scientifically speaking? The aim is to (re) think the boundaries of the security studies as we shall see if we can include cyber securitization to the Copenhagen school analysis as its actor's identity (states, international organization, societal actors, non-state actors, etc.) and different characteristics theaters especially military, economic, environmental, societal, and cultural. Since the Copenhagen school has not constructed theoretical tools to corroborate this possible connection, the current study will focus on the Copenhagen theory of securitization instead. It will also present a critical study of the contemporary security dilemma about the referent objects (states, nations, etc.) to »update« the Copenhagen School theory of Securitization.

In fact, Wæver (Wæver 1980s) and subsequently Barry Buzan and Jaap de Wilde have pioneered the idea of securitization. A more contextual-bound securitization second generation of scholars have elaborated various ways to incorporate the notions of context and power into securitization theory. They aimed at constructing a more comprehensive understanding of securitization underlying processes[2].

Securitization refers to a process of socially constructing a particular issue as an existential threat to a valued referent object in the economic, environmental, and societal sectors[3]. This process can enhance our thinking to include others fields of securitization and new forms of security.

Securitization theory emerged in the 1990s as a new approach to address developing security concerns that fell outside of traditional military tensions that had dominated scholarship throughout the Cold War. During this time, numerous schools of thought emerged, including the Copenhagen School (CS), which sought new ways of understanding security and its processes. One area of focus, for example, is the role of securitizing actors,

[1] Aydindag, D. (2021). "Copenhagen school and securitization of cyberspace in turkey", Propósitos y Representaciones, 9 (SPE1), e850. Doi: http://dx.doi.org/10.20511/pyr2021.v9nSPE1.e850, P. 4.

[2] Holger Stritzel. "Security as translation: threats, discourse, and the politics of localization, Review of International Studies", Vol. 37, No. 5 (December 2011). P.2492.

[3] Barry Buzan, Ole Wæver, and Jaap de Wilde, Security: A New Framework for Analysis (Boulder: Lynne Rienner, 1998). P. 2.

such as politicians, and their use of discourse. They argue that a security concern can only be addressed through the use of extraordinary measures rather than normal political actions[1]. The application of extraordinary measures such as a tool can improve our analyses of securitization fields.

In this connection, new forms of security sectors encompass a broad range of security threats. The first is the military sector, which investigates traditional military threats, as well as conflicts between state militaries. The second is the political sector that explores non-military threats, such as terrorism and other incidents that peril sovereignty. As for the third form, it is related to the societal sector, which seeks to understand how certain actions threaten group identity (-ies). Another fourth form is also connected to the environmental sector that assesses threats to the ecosystem, and finally, there is the economic sector that examines threats to the economy. Both speech and sector analyses have their merits and contribute to a broader understanding of security[2]. It should be stated that the fourth sector can take advantage to seek other areas and passage start.

The interpretation of cyber phenomena involves the analysis of a new body of experiences that existing theories may be unable to elucidate. Moreover, it presupposes a technical understanding of a transforming technology, whose implications require time to master because of its scientific complexity[3].

We can consult the technical expert to integrate some elements of cyber security. Also, it is necessary to confer with the interaction of cyber security with other areas of social sciences, especially International Law.

Security is a category of conflict »Although security in International Relations may generally be better than insecurity (threats against which no adequate countermeasures are available), a secure relationship still contains serious conflicts—albeit ones against which some effective countermeasures have been taken«[4].

[1] Karen Everett. Canada's Northern Borders in the Context of National Border Regimes, UCL Press. (2019), P. 176.
[2] Ibid. P. 176.
[3] Lucas Kello. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft", International Security, Vol. 38, No. 2 (FALL 2013). P. 7.
[4] Barry Buzan, Ole Wæver, and Jaap de Wilde, Security: A New Framework for Analysis, ibid. P. 4.

Materials and Methods

This paper refers to the analytic approach. It focuses on the discussion of the cyber securitization concept. The focal point of this study is how to include, on the one hand, cyber security into securitization theory and, on the other hand, the vision of critical security for this issue. More generally in this investigation, the holistic approach can help us to understand the necessity of incorporating cyber security into the security complex configuration.

Results

1. Level of Analysis and Cyber Security

Buzan defines five security sectors and five levels of analysis in security studies. The sectors are political, societal, environmental, military, and economic. The levels of analysis in question are a systemic, sub-systemic, unit, subunit, and finally individual (Buzan, Wæver, & de Wilde, 1998:7). The approaching sections focus on the theory's strengths and weaknesses regarding particularly the individual level and cyber security's relationship with these main sectors[1].

The Copenhagen School suggests that the study of security should be expanded beyond its traditional focus on military affairs and nation-state actors to wrap a variety of threats posed in various sectors. These can be approached by actors located at separate analytical levels (Buzan et al., 1998, Emmers, 2016)[2]. What means can be used to enlarge the notion of securitization?

By indicating that threats are social constructs centered on speech acts, the concept of securitization provides an alternative constructivist perspective to the age-old debate dispute over whether a threat may be regarded as an objective fact or a reflection of subjective experience. In various strands of social theory, 'speech acts' refers to the idea that verbalization is the basis for 'doing'[3]. The cyber security concept can play a role in this doctrine debate. Perhaps, it is not a speech act refers, but it is a fact of the international scene.

---

[1] Aydindag, D. (2021). Copenhagen school and securitization of cyberspace in turkey. Propósitos y Representaciones, 9 (SPE1), e850. Doi: http://dx.doi.org/10.20511/pyr2021.v9nSPE1.e850. P.4.

[2] What kind of cyber security? Theorizing cyber security and mapping approaches // https://policyreview.info/articles/analysis/what-kind-cyber-security-theorising-cyber-security-and-mapping-approaches.

[3] Steven Ratuva. Exploring the contours of threat: Competing security discourses (ANU Press, 2019). P. 24.

A noteworthy constructivist approach to security is the theory of «securitization,» developed by the Copenhagen school. This is about how, when, and with what consequences political actors define something (anything) as a security issue (Buzan et al., 1998; Wæver, 1995; Williams, 2003)[1]. Conceivably Cyber security is a (new) framework for analysis.

According to the Copenhagen School, security is an intersubjective construct that is created by «speech acts» of relevant actors, such as authorities, parties, ministers, or other influential figures[2]. It should be stated that being able to create a tool is an enormous work to make a new debate about cyber security and State behavior.

The Copenhagen school of security defines a security issue not necessarily because a real existential threat exists, but because the issue is successfully presented by key agents as a threat[3]. Cyberspace identity must be understood as an intersubjective social construction. For Joseph Nye, cyber security involves a blurring of public and private vulnerabilities[4].

2. Theorizing Cyber Security

Generally, the Copenhagen school rejects the idea, which incorporates cyber security into the security analysis. In the paper entitled "Security: A New Framework for Analysis" 1998, the Copenhagen School declares that there is no need to theorize cyber security as a distinct sector akin to the military, political, environmental, societal, economic, and religious ones (Buzan et al. 1998; Laustsen and Wæver 2000)[5].

However, in the digital transformation, it is firm to ignore the significance of cyber security and its effects on actors especially between the global North and global South.

---

[1] Johan Eriksson and Giampiero Giacomello, "The Information Revolution, Security, and International Relations: (IR) Relevant Theory?", International Political Science Review, Vol. 27, No. 3 (Jul., 2006). P. 234.

[2] Beatrice de Graaf and Cornel Zwierlein. "Historicizing Security— Entering the Conspiracy Dispositive", Historical Social Research / Historische Sozialforschung, 2013, Vol. 38, No. 1 (143), Security and Conspiracy in History, 16th to 21st Century (2013). P. 49.

[3] Myriam Dunn Cavelty. Cyber-Security and Threat Politics US Efforts to Secure the Information Age (CSS Studies in Security and International Relations, 2007). P. 25.

[4] Joseph S. Nye, Jr., The End of Cyber-Anarchy, How to Build a New Digital Order, Foreign Affairs Volume 101, Number 1 (January—February 2022). P. 34.

[5] Lene Hansen and Helen Nissenbaum. "Digital Disaster, Cyber Security, and the Copenhagen School", International Studies Quarterly, Vol. 53, No. 4 (Dec., 2009). P. 1156.

Discussion

1. Cyber Securitization and the Reality of Emergency Measures

As a matter of fact, theorizing the cyber security sector requires addressing the following questions: What threats and referent objects characterize cyber security; what distinguishes it from other security sectors; how can concrete instances of cyber securitizations be analyzed; and what can critical security scholars learn from taking cyber discourse seriously?[1]

While advocating a broad understanding of security, the Copenhagen school has made no mention of the information revolution[2].

If it is not possible to insert cyber security into securitization, we can explore the following citation: securitization serves to justify emergency measures to cope with the perceived threat. The securitization approach serves to underline the responsibility of actors as well as of analysts who choose to frame an issue as a security issue (Buzan, Wæver, and DWild, 1998): as a result, cyber security cannot ignore this emergency measure, especially in developed countries. Thus, what about developing countries' vision?

Since cyberspace has no boundaries, developing countries face many similar cyber threats as the developed world. These threats can range from malware to cyber-crime, in the form of attacks on state infrastructure, information technology, vital industry, and individuals[3]. Security is being perceived in increasingly general terms. It includes technologies, information, and more importantly, the idea that security problems are no longer systematically related to any politico-military player[4]. But, Cyber security presents an urgent subject to High Politics in developed countries and developing countries. It is the opportunity to cooperate and to enhance digital sovereignty in the era of digital trans-disciplinary discursive.

2. How (should) Cyber Security be Included in Security Studies?

The Copenhagen School framework sides with the wideners in terms of keeping the security agenda open to many different types of threats. It ar-

---

[1] Ibid. P. 1157.

[2] Johan Eriksson and Giampiero Giacomello, "The Information Revolution, Security, and International Relations: (IR) Relevant Theory?", International Political Science Review, Vol. 27, No. 3 (Jul., 2006). P. 234.

[3] Lilly Pijnenburg Muller. "Cyber Security Capacity Building in Developing Countries", Norwegian Institute for International Affairs (NUPI) (2015). P. 2—3.

[4] Zaki Laidi. "Rethinking Post-Cold War", Economic and Political Weekly, Aug. 6, 1994, Vol. 29, No. 32 (Aug. 6, 1994). P. 2068.

gues that the core of Security Studies is war and force, and other issues are relevant only if they are related to that[1].

The cyber security dilemma is mainly built upon the framework of Hansen and Nissenbaum's article "*digital disaster*". The cyberspace sector, like the environmental and, to a lesser extent, economic sectors, easily crosses national borders. Cavelty argues that "cyber security and national security differ most decisively in scope, in terms of *actors* involved and in their referent objects" (Dunn Cavelty, 2012).

Hansen Aydindag and Nissenbaum[2]emphasize the importance of cyber security in International Relations and securitization theory as follows: cyber securitizations are particularly powerful precisely because they involve a double move out of the political realm: from the politicized to the securitized, from the political to the technical, and it requires an interdisciplinary effort to assess and possibly counter the implications of that double move, . . . cyber security stands at the intersection of several disciplines, and it involves both analysis and academic communication. This work is useful to elaborate a counter-strategy to digital conflict in the trans-disciplinary discursive.

The technical underpinnings of cyber security require, for instance, that International Relations scholars acquire some familiarity with the main technical methods and dilemmas, and vice versa that computer scientists become more cognizant of the politicized field in which they design and how their decisions might impact the (discursively constituted) trade-offs between security, access, trust, and privacy[3]. The intersection between thus scholars and computer scientists is a good job to secure and save our digital sovereignty.

Bearing in mind the emphasis on discursive securitization, Copenhagen scholars have neglected to explain how non-traditional security (NTS) issues are subsequently governed, even though very different governance arrangements have emerged to address ostensibly similar securitized prob-

[1]Barry Buzan. "Rethinking Security after the Cold War", Nordic International Studies Association (Sage Publications, 2008). P. 13.

[2]Aydindag, D. (2021). "Copenhagen school and securitization of cyberspace in turkey". Propósitos y Representaciones, 9 (SPE1), e850. Doi: http://dx.doi.org/10.20511/pyr2021.v9nSPE1.e850. P. 6—7.

[3] Lene Hansen and Helen Nissenbaum. "Digital Disaster, Cyber Security, and the Copenhagen School", International Studies Quarterly, Vol. 53, No. 4 (Dec., 2009). P. 1172.

lems[1]. Cyber governance must take to account the cyber security challenge faced by countries and other actors.

2. Theorizing Cyber Security and Threats to National Security

Cavelty's starting point is the so-called Copenhagen School of securitization (Buzan, Wæver, and de Wilde 1997), which belongs to the social constructivist of IR theory. Threats to national security, according to this school, are not defined by rational calculations but are socially constructed from discourses that arise from and are shaped and promoted by policy communities[2].

Cyber security is moving upwards in the political agenda and expanding sideways as a problem area to a multitude of additional policy domains[3]. The task to defy the digital gap between the North and the South is incredible to work.

Many scholars are tempted to exclude technical threats from security studies because they bear little discursive resemblance to political-military threats. As the debates over the expansion of the concept of security gained ground in the 1990s, this linkage of security to urgency and extreme[4] and radical defense measures was central. The technical task is an essential element to make a good decision.

Conclusion

1. Critical Security Studies and Cyber Security

The critical security studies reflect the efforts of Barry Buzan, Ole Wæver about (societal security), in the works of Heidegger, Michaël Dillon, (philosophic and political analysis), a Neorealism (Mohammed Ayoob) a constructivism *modéré* (Beverly Crawford, Karin Fierke et Thomas Risse— Kappen), postmodernism (Ronnie D. Lipshutz, Michaël Williams, Keith Krauze, Simon Dalby, R. B. J. Walker, Ken Booth[5].

---

[1] Shahar Hameiri and Lee Jones. "The Politics and Governance of Non-Traditional Security", International Studies Quarterly, September 2013, Vol. 57, No. 3 (September 2013). P. 462.

[2] Ronald J. Deibert. "The Virtual Absence of Malice: Cyber Security and Threat Politics", International Studies Review, Jun., 2009, Vol. 11, No. 2 (Jun., 2009). P. 373.

[3]Myriam Dunn Cavelty & Andreas Wenger (2020) "Cyber security meets security politics: Complex technology, fragmented politics, and networked science", Contemporary Security Policy, 41:1, 5-32, DOI: 10.1080/13523260.2019.1678855. P. 7.

[4] Buzan and Hansen. The Evolution of International Security Studies (Cambridge: 2009). P. 12.

[5] Ayse Ceyhan. Analyser la sécurité: Dillon, Waever, Williams et les autres, Cultures et Conflits, Automne-hiver 1998, No. 31-32. P. 42—43.

As Wæver argued, security is a kind of stabilization of conflict or threatening relations, often through emergency mobilization of the state[1].

While the securitization theory was an attempt to broaden the scope of analysis beyond military affairs (Wæver, 2010), it has sparked debates that it is too narrow and lacks universal contextual relevance[2]. The international context to implement the Copenhagen school securitization theory remains the core concern.

2. Copenhagen School: Less Applicable in Non-Western contexts

Although many criticisms of the Copenhagen School by European theorists were based on the need to refine securitization theory to make it more appropriate, criticisms by some non-Western scholars and those from the critical security perspectives were more directly dismissive, arguing that securitization theory was not relevant to non-Western societies (Bilgin, 2011; Sheikh, 2005; Vuori, 2008)[3].

We must take into consideration the different national geopolitical and economic contexts.

There was also a view that even de-securitization was a conservative process that reproduced the existing liberal order (Aradau, 2004). Those who used the peace studies lens argued that securitization had no morally defensible position on such issues as minorities and AIDS (Elbe, 2006; Roe, 2004). The theory's Eurocentric and statist nature tended to be too analytically restrictive to be of much use in unpacking the complex security situation in postcolonial societies whose historical and cultural evolution had been shaped by complex colonial and postcolonial forces[4]. Postcolonial theory developed (…) the notion that ideas of reason, secular tolerance, equality under the Law, and democratic rule, need not be, and indeed historically have not been, mutually exclusive with European practices of violent domination, exclusion, and systematic and instrumental use of terror[5].

---

[1] Barry Buzan. "Rethinking Security after the Cold War", Nordic International Studies Association, Sage Publications, 2008. P. 8; Ole Wæver. Securitization and Desecuritization, On Security, by Ronnie D. Lipschutz (Columbia University Press, 1995).

[2] Steven Ratuva. Exploring the contours of threat: Competing security discourses (ANU Press, 2019). P. 25.

[3] Ibid. P. 27.

[4] Ibid. P. 27.

[5] Rosi Braidotti. The Posthuman-Polity (2013). P. 46.

3. Cyber Security in the Political Realm or Societal Context

We will focus on the problems and trends that have emerged, and the possibility to include cyber securitization. Simply put, we need to reconsider the problems of cyber security in the 'political realm'. We must research cyber security and 'political realms' in various parts of the world. It is also necessary to go beyond the often hyper securitizing images of digital danger and 'otherness' emerging from 'non-western countries'. Such a step is vital for exploring the complexity of cyber security both from the perspective of new 'everyday security strategies' that individuals may confront, but also in terms of the potential for 'digital disasters' that might emerge from specific technological, legal, political, and security contexts[1].

The IR scholars examine the specific contexts, controversies, and challenges in diverse spaces beyond the often simplistic geographies of cyber-threat that often serve to fuel the hyper securitized visions of geopolitical imaginaries[2]. Therefore, the social of non-western countries (the global South) may be an appropriate context for countering cyber security de-securitization.

The essay, by Hansen and Nissenbaum, is a call to investigate the complexities of cyberspace, to think more critically about what constitutes a catastrophe or digital disaster and the various problems that can be absorbed into the discourses of hyper securitized threat. However, what is clearer now is the need to explore the complexity* of cyber security in different geopolitical and economic contexts around the planet, to become more granular in our analyses.[3] This is a challenge for the IR Schools.

---

[1] Mark Lacy and Daniel Prince. Securitization and the Global Politics of Cybersecurity. P. 4 // https://eprints.lancs.ac.uk/id/eprint/89179/2/securitizationcyber21.pdf.

[2] Ibid. P. 5.

[*] A security complex is defined as a group of states whose primary security concerns link together sufficiently closed that their national securities cannot realistically be considered apart from one another. Barry Buzan. People, States and Fear. The National Security Problem in International Relations, op, cit. P. 106.

[3] Mark Lacy and Daniel Prince. Securitization and the Global Politics of Cybersecurity, op, cit. P. 15.

Зайкова Светлана Николаевна,
кандидат юридических наук, доцент, доцент кафедры административного и муниципального права ФГБОУ ВО «Саратовская государственная юридическая академия»

Реформирование контрольно-надзорной деятельности в области транспортной безопасности: новые вызовы

Аннотация. Контрольно-надзорная деятельность в области обеспечения транспортной безопасности после проведенной «регуляторной гильотины» претерпевает существенные изменения. В статье приводятся результаты анализа изменений законодательства, введенных в 2021 г. Автор приходит к выводу о необходимости законодательного установления понятий «тест-задание» и «тест-ситуация», порядка их использования; определения и правового закрепления исчерпывающего перечня индикаторов состояния транспортной безопасности и их пороговых значений для оценки эффективности административно-правового регулирования. Внесены предложения по профилактике нарушений в рассматриваемой области и проведению широкомасштабной разъяснительной работы среди контролируемых лиц.

Ключевые слова: транспортная безопасность; система транспортной безопасности; национальная безопасность.

Zajkova N. Svetlana,
Candidate of Juridical Sciences, Associate Professor, Associate Professor of the Administrative and Municipal Law Department of Saratov State Law Academy

Reforming control and supervision activities in the field of transport security: new challenges

Abstract. Control and supervisory activities in transport security are undergoing significant changes after the ‘regulatory guillotine’. The article contains the results of the changes in legislation analysis of 2021. The author comes to the conclusion that it is necessary to legally establish the concepts of ‘test-task’ and ‘test-situation' and their application procedure; to define and legally consolidate an exhaustive list of the transport security state indicators and their threshold values for assessing the effectiveness of administrative and legal regulation. The author makes pro-

posals for the preventive control in the area under consideration and for extensive awareness-raising work if needed.

Keywords: transportation security; transportation security system; national security.

Реформирование контрольно-надзорной деятельности в области транспортной безопасности (далее — ТБ) в Российской Федерации потребовало принятия новых нормативных правовых актов, отвечающих современным вызовам по развитию транспортного комплекса и обеспечению его защищенности, в том числе в условиях новых вызовов кибербезопасности.

Как ранее отмечалось[1], Федеральный закон от 31.07.2020 № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» закрепил риск-ориентированный подход при проведении контрольных мероприятий, определил новые принципы, в том числе принцип стимулирования добросовестного соблюдения обязательных требований, которым установлены приоритеты в сторону превентивных мероприятий, направленных на профилактику, снижение риска причинения вреда (ущерба). Законом заложены правовые основы для внедрения эффективных механизмов кадровой политики как контролируемых лиц, так и контрольно-надзорных органов.

Новая редакция ст. 11.1 Федерального закона от 09.02.2007 № 16-ФЗ «О транспортной безопасности» коренным образом изменила законодательные положения о контрольно-надзорной деятельности.

Во-первых, ранее Закон предусматривал множественность федеральных органов исполнительной власти, уполномоченных на проведение контрольных мероприятий по ТБ, отсылая к их компетенции. Действующая норма определяет только один орган федерального надзора — Ространснадзор[2]. Порядок организации и осуществления

[1] Зайкова С. Н. Реформирование контрольно-надзорной деятельности в области транспортной безопасности // Актуальные проблемы административного и административно-процессуального права (Сорокинские чтения): сборник статей по материалам международной научно-практической конференции, 26 марта 2021 года / под ред. А. И. Каплунова. М., 2021. С. 789—793.

[2] Постановление Правительства РФ от 30 июля 2004 г. № 398 «Об утверждении Положения о Федеральной службе по надзору в сфере транспорта».

федерального государственного контроля (надзора) (далее — Положение) утвержден постановлением Правительства РФ от 29.06.2021 № 1051.

Следует отметить, что указанная новелла по закреплению федерального надзора за единственным органом не препятствует проведению контрольных (надзорных) мероприятий с участием сотрудников ФСБ России и МВД России в установленных случаях. Например, уполномоченные представители указанных органов участвуют при рейдовых осмотрах (п. 55 Положения), при проведении экспериментов или выездных поверок с применением тест-предметов, с использованием тест-субъектов (п. 56 Положения).

Во-вторых, в прежней редакции Закона контрольно-надзорная деятельность осуществлялась в соответствии с порядком, установленным Правительством РФ. Законом ранее устанавливались основания для проведения плановой (внеплановой) проверки, возможность использования тест-предметов, перечень органов власти, участвующих в указанных проверках. Действующая редакция ст. 11.1 использует отсылочную норму к Федеральному закону от 31.07.2020 № 248-ФЗ и Положению, что будет способствовать единообразному применению нового закона о контроле уполномоченными органами.

В-третьих, впервые законодательно установлены предмет и объект контроля (надзора) в области ТБ. Предметом является соблюдение обязательных требований, установленных российским законодательством в области ТБ, широким кругом контролируемых лиц. К ним относятся: субъекты транспортной инфраструктуры, перевозчики, застройщики объектов транспортной инфраструктуры (далее — объекты ТИ), подразделения ТБ, учебные центры, специализированные организации, органы аттестации, аттестующие организации, граждане.

Также законом установлен перечень объектов контроля (надзора). В зависимости от видов экономической деятельности в транспортной отрасли контролируемых лиц выделены следующие объекты: деятельность субъектов по обеспечению ТБ, результаты такой деятельности, транспортные средства, объекты ТИ и аналогичные строящиеся объекты, зоны безопасности.

В-четвертых, законодательно расширился перечень допустимых тестов при проведении проверок. К ранее используемым тест-

предметам (предметам, имитирующим оружие или другие устройства, предметы, запрещенные для перемещения в зону транспортной безопасности) добавились тест-субъекты, тест-задания и тест-ситуации. Следует отметить, что Положение подробно описывает порядок использования тест-предметов и тест-субъектов, а понятия «тест-задание» и «тест-ситуация» не только не раскрыты в законе, но и не упоминаются в Положении.

В-пятых, новой редакцией ст. 11.1 Закона впервые установлены специальные режимы федерального надзора: обязательный мониторинг и постоянный рейд. В отношении отдельной категории объектов ТИ предусмотрено осуществление обязательного мониторинга в режиме реального времени с использованием специальных технических средств, имеющихся на объектах ТИ. Удаленный доступ к данным технических средств представляется контролируемыми лицами должностным лицам Ространснадзора (территориальных управлений службы).

Постоянный рейд может проводиться в отношении транспортных средств, производственных объектов, деятельности граждан и организаций. Для его проведения устанавливаются пункты контроля на объектах, определенных Положением. К ним относятся объекты дорожного хозяйства (в зависимости от статуса автомобильных дорог: федерального, регионального и межмуниципального значения); аэропорты, автомобильные и железнодорожные вокзалы и станции первой и второй категорий; объекты ТИ, обслуживающие международные перевозки.

Отдельно в законе регламентировано информационное обеспечение в области транспортной безопасности. В п. 1 ст. 11 Закона за Минтрансом России закрепляется обязанность по созданию государственного информационного ресурса — ЕГИС ОТБ. Основное предназначение системы заключается в информационном обеспечении деятельности в сфере транспортного комплекса федеральных органов исполнительной власти. Сроки создания системы законом не определены.

Одним из структурных элементов ЕГИС ОТБ являются автоматизированные централизованные базы персональных данных о пассажирах, а также о персонале (экипаже) транспортных средств. Сохранение персональных данных является первоочередной задачей системы.

Таким образом, рассмотренные правовые новеллы будут способствовать систематизации форм и методов государственного управления в рассматриваемой области, взаимодействию органов и субъектов ТБ, и как следствие, приведут к повышению эффективности государственного управления в области обеспечения транспортной безопасности.

Ивакин Виктор Иванович,
кандидат юридических наук, доцент кафедры «Административное право, экологическое право, информационное право» Юридического института Российского университета транспорта (МИИТ)

Правовое обеспечение экологической безопасности автодорожного комплекса, современные инновационные технологии и образование

Аннотация. В данной работе рассмотрены вопросы юридического обеспечения экологической безопасности, связанные с деятельностью автодорожного комплекса. Проанализирована в связи с этим судебная практика и сделаны соответствующие выводы.

Ключевые слова: охрана окружающей среды; автодорожный комплекс; юридическая ответственность; судебная система; инновации; высшее образование.

Ivakin I. Victor,
Candidate of legal Sciences, Associate Professor, Department of Administrative Law, environmental law, information Law of Law Institute of the Russian University of Transport

Legal support of environmental safety of the road complex, modern innovative technologies and education

Abstract. In this paper, the issues of legal provision of environmental safety related to the activities of the road complex are considered. Judicial practice has been analyzed in this regard and relevant conclusions have been drawn.

Keywords: environmental protection; road complex; legal responsibility; judicial system; innovation; higher education.

Правовое регулирование вопросов безопасности в области охраны окружающей среды, экологической безопасности, вызванной воздействием автодорожного комплекса, — проблема в настоящее время весьма актуальная и сложная. Важную роль в решении этой задачи должны оказать новейшие достижения науки и техники, которые обозначаются в настоящее время как инновационные. К последним относятся, естественно, и цифровые технологии. В век, когда цифра стала лучшим собеседником *homo sapiens*, и теперь все дело за буквой, немалое место в реализации таких технологий отводится и учреждениям высшего образования. Это институты, университеты, академии и особенно транспортные вузы, среди которых особое место занимает Российский университет транспорта. Исходя из обозначенного посыла, рассмотрим применительно к юриспруденции данные моменты. Итак, автодорожный комплекс включает различные составляющие, в систему которого входят не только, например, автомобильные дороги и автомобильные мосты. Это также система автосервиса, дорожного строительства, непосредственно автомобильный транспорт, автомобили. Сюда относится, кроме того, ремонт и содержание автодорог, их проектирование, автомобильные заводы и т.п. В частности, объекты, связанные с обследованием для строительства указанных дорог соответствующих местностей и территорий. Отсюда видно, что данный комплекс огромен. В связи с чем вопросы юридической защиты экологии, связанной с такой деятельностью весьма актуальны, поскольку негативному воздействию от автодорожного комплекса подвергаются различные объекты природной среды. Среди них водные ресурсы, атмосферный воздух, животный мир, почвы, лес. О чем свидетельствует административная, судебная и арбитражная практика. В качестве примера также можно привести научные исследования. Однако по поводу последних необходимо заметить, причем, как это не парадоксально, но практически нет работ юридического характера, в которых раскрывается заданная тема, за некоторым немногочисленным, а порой и единичным исключением. Других трудов, анализирующих проблемы рассматриваемого вопроса, хотя бы отдаленно, посвященной, в частности, юридической ответственности в области

экологии[1], не обнаружено. Однако, конечно бесспорно, с другой стороны, то, что широко продемонстрированы научные труды, написанные представителями инженерных и иных специальностей. Вместе с тем в законодательстве более активно решается вопрос, например, связанный, в частности, с применения экологической ответственности, которую большинство юристов-экологов рассматривают как включающую такие традиционные разновидности юридической ответственности, как уголовную, гражданско-правовую, дисциплинарную и административную ответственность. К примеру, для более широкого анализа, в частности, последней, а именно установленной КоАП РФ, обратимся к примечанию ст. 12.1. В обозначенной норме дано определение транспортных средств. Конечно, к цитируемому понятию относятся и автомобили или точнее средства автомототранспортные с соответствующими данными. Например, скорость последних должна быть более 50 км/ч, объем двигателей, ДВС также должен превышать 50 куб. см и т.д. Но к автомобильному транспорту в нашем понимании не относятся, например, трактора или комбайны. Хотя в широком плане их можно рассматривать в качестве таковых. Однако вопросы непосредственно экологической ответственности за совершение экологических правонарушений, как особой разновидности ответственности, наряду, например, с гражданско-правовой или уголовной ответственностью, в российском законодательстве практически не представлены. В то же время административная ответственность, как видно, демонстрируется в необходимом потенциале. Поскольку борьба с негативным воздействием автодорожного комплекса на экологию с применением указанного института ответственности в нашей стране ведется давно и широко. Так, если обратить внимание непосредственно на заводы, выпускающие автомобили, и находящиеся в России, то например, на АвтоВАЗе весьма эффективно функционирует экологическая координация деятельности, по-другому называемая управлением. На этом предприятии утверждена концепция политики в области охраны природы. В соответствии с обозначенной концепцией, например, допускается предельно открытая информация в данной сфере. Одним из принципов работы завода является также

[1] Ивакин В. И. Библиография юридической ответственности за экологические правонарушения (1880—2020 гг.). М., 2022.

то, что деятельность организации должна соответствовать как отечественным, так и международным стандартам в области охраны окружающей среды, соответствовать действующему законодательству в рассматриваемой области отношений. Аналогичные требования закрепляются и в коллективных договорах общества. Тем не менее по сообщениям СМИ, АвтоВАЗ как юридическое лицо не раз привлекался к административной ответственности, в частности, за нарушения норм в области обращения с производственными отходами, включая обращение с опасными веществами. Санкциям рассматриваемой разновидности ответственности неоднократно подвергались и должностные лица этой организации. Определенные юридические документы по данному вопросу приняты, также, например, и на Камском автозаводе.

С использованием автомобилей, в результате деятельности всего автодорожного комплекса совершаются многие экологические правонарушения, а не только вышеуказанные. Дела данной категории рассматривают различные органы, в том числе судебные. Для примера рассмотрим одно из таких дел. В частности, постановление Арбитражного суда Северо-Западного федерального округа, в который входят, как известно, 11 различных субъектов РФ, в том числе, Санкт-Петербург, а также Псковская и Новгородская области. Так, в постановлении от 13.01.2022 № А44-2117/2021 речь идет о возмещении экологического вреда, причиненного водным биоресурсам при реконструкции автодорожного моста через реку. В судебном заседании приняли также участие в качестве истцов представители Северо-Западного территориального управления Росрыболовства. Тем самым принимали участие в заседании суда, в частности, представители организации, которая наделена правами в области контроля за водными биологическими ресурсами, а также правом надзора за средой, местом обитания указанной фауны. Кроме того, в названном заседании участвовали по доверенности в качестве ответчика представитель администрации одного из муниципальных районов, на территории которого и велась реконструкция автодорожного моста и заказчиком ремонта которого выступала местная муниципальная администрация. А именно представитель администрации Крестецкого района Новгородской области. Дело рассматривалось открыто. Основанием рассмотрения явилась подача жалобы по кассации истцом на постанов-

ление 14-го апелляционного арбитражного суда от 21.09.2021[1]. Суть дела была в следующем. Указанный территориальный орган Росрыболовства 18 июня 2021 г. обратился в арбитражный суд с иском к администрации названного района, указанного муниципального образования, т.е. администрации Крестецкого муниципального округа[2]. Истец просил суд обязать муниципальную администрацию возместить вред, который был причинен при ремонте автодорожного моста водным биоресурсам, обитающим в реке Волма, водосборный бассейн которой принадлежит Балтийскому морю. Данный мост непосредственно проходит через указанный водный объект в районе деревни Вороново обозначенного района. При этом истец просил взыскать с ответчика вред в натуре посредством осуществления в срок до 1 декабря 2021 г. единовременного выпуска в озера указанного субъекта РФ, т.е. Новгородской области, сеголетков судака, далее цитируем из постановления суда «со штучной навеской от 3 до 10 граммов» в количестве около 7000 штук, а также о взыскании в случае неисполнения определенной месячной неустойки в сумме 10 тыс. руб., начиная со срока неисполнения, а именно с 1 декабря 2021 г. 18 июня 2021 г. суд первой инстанции в данном иске отказал. Однако суд апелляционной инстанции удовлетворил исковые требования (постановление от 21.09.2021). В свою очередь, в жалобе администрация просила отменить такое решение, поскольку в материалах данного дела не содержится тех доказательств, которые свидетельствуют о том, что реконструкция моста была проведена в соответствии с проектом. Кроме того, в деле нет доказательств, свидетельствующих, по мнению подателя жалобы, о причинении вреда биоресурсам данного водного объекта. Представитель администрации отмечал, что когда проходила реализация аналогичного проекта годом ранее, и в другом населенном пункте, а водный объект тот же, то никаких подобных мероприятий, связанных с компенсацией проведено не было. В свою очередь, делая отзыв на жалобу, поданную в кассационном порядке, управление Росрыболовства в то же время просило суд обжалуемые акты оставить в силе. А также признать их как обоснованными, так и законными. В ходе заседания администрация в лице представителя

[1] https://sudact.ru/arbitral/doc/IZC5hpqkHzWx/ (дата обращения: 08.05.2022).
[2] https://sudact.ru/arbitral/doc/EsWwWugWW7xL/ (дата обращения; 09.05.2022).

свои доводы поддержала, а Управление по рыболовству просило отказать в удовлетворении жалобы. В кассационном порядке акт суда, который обжаловался, был проверен. И установлено следующее. В 2016 г., когда происходила реконструкции (ремонт) автодорожного моста, был причинен вред указанным речным биоресурсам. Данный проект реконструкции готовил научно-исследовательский институт, который занимался вопросами как океанографии, так и рыбного хозяйства. Обозначенный НИИ имеет статус Всероссийского. Управление, в свою очередь, ссылалось на то, что ремонт моста выполнялся администрацией по проекту, согласованному в 2014 г. Каких-либо дополнительных обращений для получения заключения не проводилось. В то же время управление обратилось к администрации округа с определенным требованием. Последнее заключалось в том, чтобы администрация муниципального образования выполнила мероприятия связанные с устранением последствий негативного характера, а именно осуществила выпуск в озера данного субъекта РФ сеголетков судака. Но администрация указанных требований не выполнила. Это и послужило основанием для обращения в арбитражный суд. При этом суд по первой инстанции все требования, которые заявляло управление, признал необоснованными. Однако суд апелляции удовлетворил исковые требования территориального управления Росрыболовства. В то же время кассационная инстанция на нашла соответствующих оснований для того, чтобы жалобу администрации муниципального образования удовлетворить. Из постановления об отказе удовлетворения жалобы видно, что суд по первой инстанции руководствовался тем, что проектные материалы, связанные с ремонтом указанного моста, были согласованы со всеми заинтересованными субъектами, в том числе с истцом. Об этом указывалось в заключении управления от 25.02.2014 № 07-06/671 и выдан на материалы проекта реконструкции моста, которые подготовило ООО АПМ «Атриум». Истец, а именно управление Росрыболовства, на основании запроса указанного общества согласовал все вопросы и условия, связанные с осуществлением соответствующей деятельности по реконструкции моста. Одним из условий как раз было то, что муниципальное образование, с целью компенсации, осуществит выпуск в озера указанного субъекта РФ, т.е. в озера Новгородской области сеголетков судака. Причем было определено количество этой рыбы — 6170 штук. Одна-

ко, как посчитал суд по первой инстанции, в деле отсутствовали доказательства того, что администрацией был реализован именно такой проект реконструкции автодорожного моста на территории Крестецкого района в одном из его населенных пунктов, а именно в деревне Вороново. Это не подтверждает и муниципальный контракт, связанный с реконструкцией указанного автодорожного объекта. Суд в первой инстанции при этом посчитал также, что проект ремонта моста не реализовался в связи с тем, что была очень высокая его стоимость. После чего 14 ноября 2016 г. был заключен по результатам аукциона, проводившегося в электронном порядке, муниципальный контракт с ООО «Мостопоезд № 816». Данное общество обязывалось выполнить все мероприятия по ремонту обозначенного моста, располагающегося на трассе «Вороново-Курово», до конца 2016 г. Исходя из указанных обстоятельств, суд по первой инстанции пришел к выводу, что в соответствии с техзаданием, связанным с ремонтом моста, такой ремонт осуществлялся на основании соответствующей сметы, о чем свидетельствовали документы. Такая сметная документация включала в себя как подготовительные работы, так и разборку старых конструкций моста, сооружение таких элементов, как пролетные строения, мостовое полотно и т.д. А это сооружение устоев и сопряжение промежуточной опоры, рекультивацию строительной площадки и др. Среди них в частности, сооружение различных подходов к мосту. Одновременно разработка проектных документов, связанных с ремонтом моста, в контракте не предусматривалась.

Указанный автодорожный мост ремонтировался не более двух месяцев — при такой продолжительности разработка проектной соответствующей документации не требуется, как и получения необходимого заключения от Управления Росрыболовства. Поэтому суд по первой инстанции не усмотрел вины в причинении вреда окружающей среде местной администрации, на основании чего в иске было отказано. Однако суд апелляции с такими доводами суда по первой инстанции не согласился и отменил решение указанного суда. Соответствующие доводы были приведены в решении апелляционного суда, и обязанность возместить заявленный экологический вред была возложена на администрацию соответствующего муниципального образования.

Отсюда на основании изложенного примера можно сказать, что автодорожным комплексом, его объектами, в том числе деятельностью, связанной с реконструкцией мостов через реки, причиняется значительный вред окружающей среде, в том числе соответствующим водным биоресурсам. Хотя, заметим, что в данном случае ответчиком выступало все-таки соответствующее муниципальное образование, но как заказчик по реконструкции автодорожного моста. Для борьбы с такими экологическими правонарушениями и необходимы современные инновационные технологии, в том числе связанные с образованием. Так, изложенное свидетельствует, что возможно в системе дополнительного профессионального образования ведение курса по правовому обеспечению экологической безопасности на автодорожном комплексе. Причем, как для работников местных муниципальных администраций, так и сотрудников, например, Росавтодора, работников проектных НИИ и других структур, занимающихся подготовкой проектной документации, в частности, связанной с ремонтом мостов через водные объекты. Среди таких структур необходимость в повышении квалификации распространяется и на представителей Росрыболовства. Естественно, в настоящее время весьма необходимы научные наработки по данной проблематике, поскольку юридические вопросы обеспечения экологической безопасности при строительстве и реконструкции автодорожных мостов, как выше отмечалось, не находят соответствующего отражения в научной литературе по экологическому праву или иным отраслям юриспруденции. Актуально в целом правовое регулирование экологической безопасности на всем автодорожном комплексе. Хотя представляется, о чем указывалось выше, есть определенные работы, например, других специалистов, затрагивающих с иных позиций эти вопросы. Отсюда необходимы монографические, диссертационные исследования по этой проблеме, а также написание статей и учебных пособий по данному вопросу именно в юридическом институте, действующем в транспортной отрасли. Естественно, в ряде случаев возможно проведение научных исследований совместно с представителями других институтов РУТ и вообще иных вузов с привлечением практических работников соответствующих структур. Существует необходимость проведения научно-практических конференций, различных иных аналогичных форумов по данному направлению. Так, 2 июня 2022 г. планируется вы-

ступление заместителя Министра транспорта РФ Д. С. Зверева по вопросам, связанным с проблемами применения законодательства в сфере транспорта. Выступление планируется с докладом, затрагивающем новеллы транспортных норм на конференции «*Global Legal Skills*». Можно также говорить о введении спецкурса «Правовое обеспечение экологической безопасности на транспорте», в процессе изучения которого рассматривать данные вопросы применительно к воздушному, железнодорожному, автомобильному и иным видам транспорта, поскольку вообще транспорт вносит существенный вклад в загрязнение природной среды.

Лескина Элеонора Игоревна
кандидат юридических наук, доцент кафедры информационного права и цифровых технологий ФГБОУ ВО «Саратовская государственная юридическая академия»

Реализация принципов правового регулирования инновационного развития отраслей экономики в информационном обществе

Аннотация. Цифровизация производственных и управленческих процессов, переход в эпоху Индустрии 4.0. приводит к необходимости развития инновационных форм машиностроения и построения в связи с этим особой государственной политики во всем мире. Все это обусловливает необходимость оперативного и адекватного реагирования. Создавая и совершенствуя собственное правовое регулирование в области инновационного развития различных отраслей экономики, необходимо особое внимание обратить на принципы правового регулирования в эпоху цифровизации.

Ключевые слова: цифровые технологии; информационное общество; государственная политика; цифровизация; инновационное развитие.

Leskina I. Eleonora,
PhD in Law, Associate Professor of the Department of Information Law and Digital Technologies, Saratov State Academy of Law

Implementation of the principles of legal regulation of innovative development of economic sectors in the information society

Abstract. Digitalization of production and management processes, transition to the era of Industry 4.0. leads to the need to develop innovative forms of mechanical engineering and, in this regard, to build a special state policy around the world. All this necessitates a prompt and adequate response. Creating and improving our own legal regulation in the field of innovative development of various sectors of the economy, it is necessary to pay special attention to the principles of legal regulation in the era of digitalization.

Key words: digital technologies, information society, public policy, digitalization, innovative development.

Современное состояние развития экономических, социальных, технологических и иных аспектов обусловлено, с одной стороны, беспрецедентной скоростью внедрения инновационных разработок, а с другой стороны, затянувшимся выходом из кризисных ситуаций, связанных как с кризисом 2009 г., так и с кризисом, вызванным пандемией коронавирусной инфекции. Все это обусловливает необходимость оперативного и адекватного реагирования, в том числе посредством правового инструментария, на новые вызовы для развития экономического роста, поддержания наиболее значимых отраслей экономики, стимулирования их перевода на новую модель с учетом инновационного развития и конкурентоспособности.

Основные принципы нормативно-правового регулирования инновационного развития экономики должны учитывать как методологические основания, так и основные цели соответствующего правого обеспечения. Среди первых необходимо назвать:

1) системность, в соответствии с которой как сами правовые нормы, правовые институты, так и принципы должны соответствовать, не противоречить друг другу, иметь единые цели и учитывать условия и перспективы развития отрасли;

2) научную обоснованность в использовании подходов, методологии, качества информации для выработки правовой политики в рассматриваемой сфере.

В качестве целей правового регулирования инновационного развития различных отраслей экономики можно назвать такие, как страте-

гичность, координация, информационная открытость, адресность поддержки, ответственность, осуществление контроля и надзора, мониторинга и оценки, стимулирования инноваций, конкурентоспособности, интеграции науки и предпринимательства, оценка вклада в экономическое и социальное развитие России, влияние развития промышленности на доходы населения или доходы работников.

На основе анализа зарубежного законодательства в области регулирования инновационного развития предприятий можно выявить и сформулировать следующие основные принципы нормативного правового регулирования инновационного развития отраслей экономики:

1) принцип свободы осуществления инновационной деятельности;

2) принцип признания многообразия форм инновационной деятельности;

3) единство и системность государственной поддержки инновационной деятельности предприятий. Следует отметить, что все меры как финансовой, так и нематериальной помощи от государства должны носить системный характер, обеспечивать функционирование целостной, характеризующейся внутренним единством системой инновационной деятельности;

4) содействие конкурентоспособности в сфере инновационной деятельности. При этом защита конкуренции должна обеспечиваться одновременно и грамотной реализацией правовой политики в сфере охраны интеллектуальной собственности, поскольку и право интеллектуальной собственности, и антимонопольное регулирование преследуют цели инновационного развития. Сотрудничество между конкурентами также не должно рассматриваться в качестве нарушения антимонопольного законодательства, необходимо оценивать результат такого сотрудничества, его влияние на инновационное развитие предприятий;

5) неотвратимость ответственности при совершении противоправных деяний, посягающих на инновационное развитие, права и законные интересы субъектов в сфере инноваций. Должны быть сформулированы четкие правовые модели ответственности субъектов правоотношений, складывающихся в процессе осуществления инновационной детальности, механизмы реализации такой ответственности;

6) развитие межрегионального, трансграничного, международного сотрудничества в инновационной сфере;

7) системность, структурированность и многоуровневость развития законодательства в сфере правого регулирования развития инновационной деятельности предприятий машиностроения. Такое законодательство должно комплексно воздействовать на инновационную активность, максимально поощрять данную активность, обеспечивать ее непрерывный качественный рост и совершенствование[1];

8) стимулирование частного сектора на инвестирование инновационной деятельности, в том числе иностранных инвестиций;

9) поддержка экспортной ориентации инновационной деятельности, в связи с чем в частности должны быть предусмотрены механизмы гармонизации стандартизации Российской Федерации;

10) формирование эффективного с учетом эпохи *Big Data* правового режима данных. От данного принципа зависит развитие таких технологий, как искусственный интеллект, интеллектуальный анализ, машинное обучения и другие.

Важнейшая роль в инновационном развитии отраслей экономики в ведущих в данной отрасли государствах отводится кадровому вопросу, в частности подготовке специалистов высшей квалификации. За последние годы число ученых и инженеров возрастает с каждым годом, что напрямую зависит от политики государства в этой сфере.

Кадровая политика в аспекте инновационного развития является одним из приоритетных направлений. Она должна включать такие цели, как организацию социальных, экономических и профессиональных условий работы ученых на современном уровне, использование платформенных решений для аккумуляции, обмена и генерации навыков, знаний, опыта в сфере инновационной деятельности; создание кадрового потенциала в машиностроении, учитывая технологии шестого уклада, обеспечение сотрудничества бизнес-сообщества, хозяйствующих субъектов, академических и вузовских секторов в сфере разработки и внедрения инновационных технологий.

Государственная поддержка машиностроения может включать и государственные заказы, где приоритет отдается именно отечественному производителю. Закупки товаров и услуг могут осуществляться

[1] Степаненко Д. М. Инновационная функция Российского государства как ключевой фактор его развития в XXI веке // Российская юстиция. 2020. № 4. С. 5—8.

здесь с ограничением по проведению торгов для отдельной продукции машиностроения.

Обращая внимание на опыт Китая в проведении политики и построении государственно-частного партнерства[1], отметим, что некоторые из этих мер могут казаться весьма жесткими и нелиберальными, однако при их временном введении, учитывая санкционную политику зарубежных государств, следует обратить внимание на возможную реализацию указанного принципа следующим путем. Учитывая риски в связи с наличием в производственной базе предприятий машиностроения зарубежного оборудования и разработок, необходимо обязать банки разработать систему формирования процентных ставок при выдаче кредитов для развития бизнеса в области инноваций, в высокотехнологичных отраслях.

В заключении отметим, что правовое регулирование инновационного развития предприятий машиностроения в современных условиях является важнейшим фактором совершенствования экономики страны в целом, инновационного развития всего государства. В Российской Федерации должна быть сформирована грамотная и эффективная в условиях развития информационного общества правовая среда, которая обеспечивала бы благоприятный правовой режим для инновационного развития, разработки и ускоренного внедрения новых технологий на предприятиях машиностроения. Учет и критический анализ лучшего зарубежного опыта в этой сфере будет способствовать решению указанных задач.

[1] Белых В. С., Алексеенко А. П. Правовое обеспечение модернизации экономики: опыт России и КНР // Юрист. 2018. № 1. С. 44—51.

Малахова Вероника Юрьевна,
кандидат юридических наук, доцент, доцент Департамента международного и публичного права ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации»

Современные и актуальные проблемы расследования киберпреступлений

Аннотация. Рассматривается проблематика расследования преступлений, совершаемых с использованием компьютерных и телекоммуникационных технологий. Уделено внимание вопросам использования новых технологий в совершении ряда преступлений в экономической сфере. На основе статистических данных, несмотря на все предпринимаемые меры, в последние годы рост дистанционных хищений стремительно увеличивается и по прогнозам специалистов будет только расти. Также в статье рассмотрен комплекс мер, направленный на борьбу с преступлениями данного вида.

Ключевые слова: киберпреступность; информационные технологии; хищение; преступление; расследование; киберпространство.

Malakhova Y. Veronika,
PhD in Law, Associate Professor, Associate Professor of the Department of International and Public Law of the Financial University under the Government of the Russian Federation

Modern and actual problems of cybercrime investigation

Abstract. The problem of investigating crimes committed with the use of computer and telecommunication technologies is considered. Attention is paid to the use of new technologies in the commission of a number of crimes in the economic sphere. Based on statistical data, despite all the measures taken, in recent years, the growth of remote theft has been rapidly increasing and, according to experts' forecasts, it will only grow. The article also considers a set of measures aimed at combating crimes of this type.

Keywords: cybercrime; information technology; theft; crime; investigation; cyberspace.

По данным Генеральной прокуратуры РФ, а точнее по данным Главного управления правовой статистики и информационных технологий криминогенная ситуация в стране по итогам 2020 г. осталась стабильной.

Наиболее распространены мошенничества в сфере информационно-телекоммуникационных технологий или компьютерной информации, на них приходится около 70% всех хищений, совершаемых путем обмана или злоупотребления доверием (+73,4%, 237,1 тыс.). Многие столкнулись с таким новым явлением, как «социальная инженерия», при совершении 25,8 тыс. (+42,4%) мошенничеств использовались электронные средства платежа. Заметное увеличение таких деяний зафиксировано в большинстве регионов.

В целом на деяния, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, по-прежнему приходится одно из четырех зарегистрированных преступлений (+73,4% 51,4 тыс.). Если рассмотреть статистику за более длительный период, то за последние пять лет число таких преступлений увеличилось более чем в 11 раз, а удельный вес в структуре преступности возрос с 1,8% до 25%.

Заметно увеличилось число краж, совершенных с банковского счета или в отношении электронных денежных средств. За 2020 г. зарегистрировано более 169,5 тыс. таких преступных посягательств, в 2019 г. таких преступлений было зафиксировано 93,7 тыс. [1]

В общем и целом по статистике видно, что преступления против собственности переходят в «киберпространство». Массовое распространение преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, сегодня стало возможным благодаря тому, что по ряду направлений предоставление услуг сотовой связи и интернета наметилась четкая тенденция к внедрению сервисов, обеспечивающих их защищенность и анонимность. И тенденция по упрощению оформления абонентских договоров тоже играет немаловажную роль. К тому же в последнее время, особенно в период вводимых карантинных мер в связи с распространением вируса COVID-19, роль информации и информационного пространства стала более значимой и для отдельного гражданина, и для государства в целом.

Хищения, совершаемые в цифровой среде, имеют сложный характер, поскольку:

— предметом хищения может выступать любой вид ресурсов, который имеет товарную стоимость, а также имущественных прав, конфиденциальной информации и персональных данных, которые при-

сваиваются злоумышленником (или группой злоумышленников) в целях обогащения, тем самым причиняя ущерб пострадавшему физическому или юридическому лицу (группе физ. или (и) юр. лиц);

— существуют сложности с идентификацией субъектов правонарушения и установления механизма преступления, в том числе по причине стремительного развития информационно-телекоммуникационных технологий, усложнения механизмов совершения правонарушений, недостаточной квалификации экспертов, а также отстающей динамикой роста компьютерной грамотности граждан [2].

К ключевым проблемам в области расследования преступлений с использованием современных технологий можно отнести следующее:

— трансграничный характер преступлений данной категории;

— местом совершения преступления является киберпространство, что не позволяет определить обстановку и условия совершения правонарушений, а также позволяет сохранять максимальную скрытность для злоумышленников;

— отсутствие нормативной правовой базы, регламентирующей сферу цифровых отношений в России;

— отсутствие единой следственной и судебной практики по уголовным делам в отношении преступлений, совершаемых с использованием новых технологий (современных возможностей);

— плохая применимость или же неприменимость иностранных методик расследования преступлений данной категории.

Раскрытие данного вида преступлений, как правило, заключается в получении и отработке всей технической информации об интернет-соединениях абонента, телефонии и движении денежных средств, установлении причастных лиц и документировании преступной деятельности установленных лиц [4].

В качестве предложений по улучшению ситуации по расследованию преступлений в киберпространстве можно выделить следующее:

— необходима интеграция сферы информационных технологий в область криминалистики для достижения синергии ресурсов и возможностей в целях поиска максимально эффективных решений в предметной области;

— обозначить категории объектов правонарушения в киберсреде, так как киберпреступники продолжают вводить новации и штамповать новые эксплойты для атак на бизнес и обычных граждан. Под эксплойтами

подразумеваются компьютерные программы, фрагмент программного кода, или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему. Целью атаки может быть, как захват контроля над системой, так и нарушение ее функционирования (*DoS*-атаки).

Подводя итоги, можно сделать вывод, что в связи с актуальностью вопроса об обеспечении правоохранительных органов специалистами, обладающими углубленными знаниями как в юридической, так и в технической областях, с начала ноября 2020 г. на платформах многих интернет-газет появилась информация о том, что МВД России создаст подразделения по борьбе с преступлениями в сфере высоких технологий, в том числе через интернет [3].

А наиболее значимым является то, что такие подразделения должны появиться не только в центральном аппарате МВД России, но и в его территориальных органах.

В настоящее время в России предпринимаются системные действия по созданию нормативно-правовой базы, регламентирующей сферу преступлений с использованием ИКТТ. Так, главой профильного комитета Госдумы по бюджету и налогам А. Макаровым озвучены предложения по внесению положения о кибербезопасности личности, общества и государства в Конституцию РФ [5].

Литература

1. Статистика состояния преступности в России за январь-июнь 2020 года, опубликованная на официальном сайте МВД России // https://genproc.gov.ru/upload/iblock/4fb/sbornik_6_2020.pdf
2. Бирюкова, Ю. В. Хищения, совершаемые с использованием компьютерных и телекоммуникационных технологий, способы их совершения и пути их расследования // Юридические науки, 2020.
3. https://www.rbc.ru/rbcfreenews/5dbc325 89a7947dcb50ecbc9
4. Костенко, Н. С. Основные проблемы раскрытия и расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, на современном этапе» / Н. С. Костенко, Г. М. Семененко, А. А. Пшеничкин // Вестник Воронежского института МВД России. 2020. № 4.
5. Путин поддержал идею закрепить в Конституции положение о кибербезопасности // Аргументы и факты. 2020. 26 февр. // URL: https://aif.ru/ politics/russia/putin_podderzhal_ideyu_zakrepit_v_ konstitucii_polozhenie_o_kiberbezopasnosti

Habib Hasan Al-Badawi
Ph.D-Professor, Lebanese University, Beirut

Tallinn Manual as a Legal Approach towards Cyber Warfare

Abstract. The Tallinn Manual examines the international law governing cyber warfare. As a general matter, it encompasses both the jus ad bellum, the international law governing the resort to force by States as an instrument of their national policy, and the jus in bello, the international law regulating the conduct of armed conflict (also labelled the law of war, the law of armed conflict, or international humanitarian law). Related bodies of international law, such as the law of State responsibility and the law of the sea, are dealt with in the context of these topics. The Tallinn Manual[1] on the International Law Applicable to Cyber Warfare was published by the International Group of Experts at the invitation of the North Atlantic Treaty Organization NATO. It is an academic, non-binding study on how international law applies to cyber conflicts and cyber warfare. The manual was revised in 2017 and published by Cambridge University Press as a book titled Tallinn Manual 2.0[2].

Keywords: National Security; State Sovereignty; Cyberespionage; International Law; Tallinn Manual.

Cyberespionage under International Law

Cyberespionage is a form of cyberattack that aims to steal confidential, sensitive, or intellectual property data to gain an advantage over a rival government company or entity, espionage is «using spies to obtain important information about plans and activities of a foreign government or a rival company[3]».

[1] Tallinn manual on the international law applicable to cyber warfare. (n.d.). Центр стратегических оценок и прогнозов // https://csef.ru/media/articles/3990/3990.pdf (accessed: 10.12.2021).

[2] Schmitt M., Vihul L. Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge : Cambridge University Press, 2018.

[3] "Espionage, according to Merriam-Webster, is "the practice of spying or using spies to obtain information about the plans and activities especially of a foreign government or a competing company." What is Cyber Espionage | VMware Glossary [online] // VMware. 2021 // URL: https://www.vmware.com/topics/glossary/content/cyber-espionage (accessed: 10.12.2021).

In the world of the Internet, spies are armies of infiltrators from all over the world who use war and electronic means for economic, political, or military gain. These high-value cybercriminals have the knowledge and technical capacity to penetrate government infrastructure, financial and real estate systems, or utility resources such as airports, ports, etc., and have been able to influence the outcome of political elections in several countries (accusing the United States of Russia of interfering in the election results that led to Trump's victory), creating international chaos, and helping companies succeed or fail[1]. Many of these attackers use Advanced Persistent Threats[2] as modus to sneak into corporate and state networks or systems and stay undetected for years.

Article 29[3] of the Hague Convention of 1907[4] stipulates that an individual can only be considered a spy for a particular State if he or she obtains information in the enemy's area of operations by acting secretly and intending to inform the hostile party, and therefore undetected soldiers who enter the area of operations of an army hostile to obtain military or intelligence information are not considered spies, nor are spies of soldiers or civilians of a particular State who carry out their duties in public or are Mandated to deliver letters addressed either to their army or to the enemy army.

Article 46 (2) of the First Additional Protocol of 1977 of the Geneva Convention stipulates that it is not engaged in espionage by members of the armed forces of a party to a particular conflict and is mandated by that

[1] Justice, J. W., & Bricker, B. J. (2019). Hacked: Defining the 2016 Presidential Election in the Liberal Media. Rhetoric and Public Affairs, 22(3), 389—420 // https://doi.org/10.14321/rhetpublaffa.22.3.0389 (accessed: 12.12.2021).

[2] What is APT (Advanced Persistent Threat) | APT Security | Imperva [online] // Learning Center. 2021 // URL: https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/ (accessed: 12.12.2021).

[3] Treaties, States parties, and Commentaries — Hague Convention (IV) on War on Land and its Annexed Regulations, 1907 — Regulations: Art. 29 — [online] // Ihl-databases.icrc.org. 2021 // URL: https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=090BE405E194CECBC12563CD005167C8 (accessed: 12.12.2021).

[4] Treaties, States parties, and Commentaries — Hague Convention (IV) on War on Land and its Annexed Regulations, 1907 [online] // Ihl-databases.icrc.org. 2021 // URL: https://ihl-databases.icrc.org/ihl/INTRO/195 (accessed: 12.12.2021).

party and in an[1] adversary-controlled territory to collect information or attempt to collect it in the uniform of its country's armed forces[2].

Tallinn Manual[3]

A group of legal and military experts published a guide known as the Tallinn Guide, a non-binding document for States, to which the International Committee of the Red Cross ICRC[4] contributed as an observer. This document indicates that international humanitarian law applies to cyber warfare as with conventional wars and determines the role that the rules of international humanitarian law will play in this area[5], despite many negative observations[6].

For legal advisers, policymakers, and military leaders interested in international law as it relates to electronic weapons, the Tallinn Guide is an important starting point for analyzing how international humanitarian law applies to cyber operations and weapons. Tallinn's 2017 guide addresses the issue of cyber weapons review, as well as many other vital issues related to this area in nearly 600 pages of rules and instructions related to public international law.

In 2009, the NATO Cooperative Cyber Defence Centre of Excellence[7], a renowned online defense research and training institution in Tallinn, Estonia, invited a group of independent cyber experts to prepare a guide on international law that should govern electronic activities during wars like

---

[1] Treaties, States parties, and Commentaries — Additional Protocol (I) to the Geneva Conventions, 1977 — 46 — Spies [online] // Ihl-databases.icrc.org. 2021. URL: https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/ART/470-750056?OpenDocument (accessed: 12.12.2021).

[2] Customary IHL — Practice Relating to Rule 107. Spies [online] // Ihl-databases.icrc.org. 2021 // URL: https://ihl-databases.icrc.org/customary-ihl/rus/docindex/v2_rul_rule107 (accessed: 12.12 2021).

[3] The Tallinn Manual [online] // Ccdcoe.org. 2021 // URL: https://ccdcoe.org/research/tallinn-manual/ (accessed: 18.14 2021).

[4] Mandate and mission [online] // International Committee of the Red Cross. 2021 // URL: https://www.icrc.org/en/who-we-are/mandate (accessed: 14.12.2021).

[5] Jensen E. The Tallinn Manual 2.0: Highlights and Insights [online] // Ssrn.com. 2021 // URL: https://ssrn.com/abstract=2932110 (accessed: 14.12.2021).

[6] A Warning About Tallinn 2.0 … Whatever It Says [online] // Lawfare. 2021 // URL: https://www.lawfareblog.com/warning-about-tallinn-20-%E2%80%A6-whatever-it-says (accessed: 18.12.2021).

[7] CCDCOE — The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary hub of cyber defence expertise. About us [online] // Ccdcoe.org. 2021 // URL: https://ccdcoe.org/about-us/ (accessed: 14.12.2021).

traditional activities. The legality associated with electronic warfare and its clarification. In 2013, the first version of the Tallinn Guide to International Law was published and became the only reference in this area and because of the success of the first guide, CCD COE began a follow-up project to expand coverage with an updated and developed guide to international law governing electronic activities during peacetime[1].

In February 2017, the second group of more diverse cyber experts participated, and their work led to the creation and dissemination of the second updated version of the Tallinn Guide. The extensive guide included material from the Tallinn I manual and another to cover the legal frameworks of forces involved in cyber activities and incidents in peacetime. It contained 154 rules, the most important of which was Rule 110 on the arms review process under international humanitarian law. The detailed commentary of each rule provides some important ideas regarding the legal basis and justification of the rules and their context, as well as justifying the effects of the application of the rules in the cyber context in terms of the field results and legal consequences of the weapon. This level of access to detail is particularly useful for legal advisers and academics. In addition to that, there is an explanation of experts' justifications for explaining legal rules and their positions on them when reaching an agreement. Also, they are unable to reach a consensus on a particular issue, as well as highlighting the reasons for incompatibility to understand the legal context of consensus or not[2].

The Tallinn analysis states that pre-cyber era international law applies to cyber operations, both conducted by, and directed against, states. This means that cyber events do not occur in a legal vacuum and thus states have both rights and bear obligations under international law[3].

Rule 110 of Tallinn Manual

---

[1] "Defend Forward" and Sovereignty. (n.d.). Hoover Institution // URL: https://www.hoover.org/sites/default/files/research/docs/goldsmith-loomis_webreadypdf.pdf (accessed: 18.12.2021).

[2] Allinn manual 2.0 on the international law applicable to cyber operations. (n.d.) // Assets.cambridge.org. 2021 // URL:https://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf (accessed: 18. 12. 2021), p. 467.

[3] Cyber operations and international humanitarian law: five key points — Humanitarian Law & Policy Blog [online] // Humanitarian Law & Policy Blog. 2021 // URL: https://blogs.icrc.org/law-and-policy/2019/11/28/cyber-operations-ihl-five-key-points/ (accessed: 18.12.2021).

All States are required to ensure that the electronic warfare methods they obtain, or use comply with binding rules of armed conflict law.

States parties to Protocol I are required to examine the means and methods of electronic warfare to determine whether their use, in some or all circumstances, is prohibited under that Protocol or any other rule of international law.

There are at least six points to be illuminated concerning Rule 110:

1. Rule 110 of the Tallinn Guide must be read from the perspective of the Advisory Opinion of the International Court of Justice on Nuclear-Weapons[1], which confirmed the idea that international humanitarian law applies to new weapons as old as they are. Although cyber weapons were invented after the emergence of most of the principles and rules of international humanitarian law, it would be wrong to conclude that international humanitarian law did not apply to them, and as noted by the International Court of Justice, it would be incompatible with the fundamental humanitarian nature of the legal principles of international humanitarian law to believe that this law does not apply to new weapons. As a result, international humanitarian law applies to all forms of electronic or conventional warfare and to all types of weapons that exist past and present and can be invented in the future.

2. To reinforce the point above, the classification of any equipment used in war or peace as an electronic weapon also means that such a weapon must at any time comply with international humanitarian law.

Subparagraph (a) reflects customary international law and stems from a general duty to comply with international humanitarian law. Subparagraph (b) is derived from Article 36, the obligations outlined in this paragraph are not limited to international humanitarian law but extend to the entire international law, they are much broader and more comprehensive than those in subparagraph (a).

Subparagraph (b) does not specify or require a specific methodology for conducting a review of cyber weapons, so States are not obliged to make their weapons reviews public, and this is particularly relevant in the context of cyberweapons because of the highly secretive nature of such weapons. As in all arms under international humanitarian law, the legality

[1] Legality of the threat or use of nuclear weapons | International Court of Justice. (n.d.). Cour internationale de Justice — International Court of Justice | International Court of Justice // https://www.icj-cij.org/en/case/95 (accessed: 18.12.2021).

of a cyber weapon must be determined by reference to its natural and expected use at the time of assessment.

5. If one State receives an electronic weapon from another for use in its future cyber operations, the fact that the arms supplier has conducted a review does not exempt the possessing State from its obligations about that cyber weapon. The acquired State may consider the review conducted by the supplier State and must fulfill its obligations under international humanitarian law.

6. Regarding what needs to be reviewed, for States parties to Protocol I, to answer the question of what specifically constitutes weapons, means, or electronic methods, it can be said that all States, regardless of whether they have ratified The First Additional Protocol, are required to systematically assess the legitimacy of their new weapons, means, and methods. This obligation logically stems from the common public duty to comply with international humanitarian law and the fact that States are prohibited from using illegal weapons, means, or methods of war and are contrary to the Bill of Human Rights.

Мальцев Виталий Анатольевич,
кандидат юридических наук, доцент, заведующий кафедрой административного, финансового и международного права образовательного учреждения профсоюзов высшего образования «Академия труда и социальных отношений»

Правовые механизмы обеспечения кибербезопасности финансово-кредитной сферы в Российской Федерации

Аннотация. В статье рассматривается содержание международного принципа обеспечения безопасности информационно-коммуникационной среды, в соответствии с которым на государство возлагается обязанность по разработке государственной политики по защите от противоправных деяний в информационном пространстве. Раскрываются основные положения законодательных и иных нормативных правовых актов, принятых в Российской Федерации по обеспечению кибербезопасности финансово-кредитной сферы. Освещены цели и направления деятельности специальных правовых механизмов обеспечивающих ее кибербезопасность. Особое внимание уделено

вопросам защиты информационно-коммуникационной среды банковской системы, как наиболее уязвимой сферы деятельности.

Ключевые слова: информационно-коммуникационной среда; финансово-кредитная сфера; банковская система; кибербезопасность; киберустойчивость; мониторинг.

Maltsev A. Vitaliy
Candidate of Law, Associate Professor, Head of the Department of Administrative, Financial and International Law of the educational Institution of Trade Unions of Higher Education «Academy of Labor and Social Relations»

Legal mechanisms for ensuring cybersecurity of the financial and credit sphere in the Russian Federation.

Abstract. The article examines the content of the international principle of ensuring the security of the information and communication environment, according to which the state is obliged to develop a state policy to protect against illegal acts in the information space. The main provisions of legislative and other regulatory legal acts adopted in the Russian Federation to ensure the cybersecurity of the financial and credit sphere are disclosed. The goals and activities of special legal mechanisms ensuring its cybersecurity are highlighted. Special attention is paid to the protection of the information and communication environment of the banking system as the most vulnerable area of activity.

Keywords: information and communication environment, financial and credit sphere, banking system, cybersecurity, cyber stability, monitoring.

Один из основных международно-правовых принципов обеспечения безопасности информационно-коммуникационной среды содержит обязательство государства способствовать социальному и экономическому развитию и осуществляться таким образом, чтобы быть совместимой с задачами поддержания международного мира и безопасности, соответствовать общепризнанным принципам и нормам международного права. Это целиком и полностью относится к финансовой сфере, которая охватывает все направления экономической деятельности как государства, так и частных субъектов. В связи с этим вопросы обеспечения безопасности в указанной области стали

предметом особого внимания законодательных органов, органов исполнительной власти и иных органов.

Известно, что финансово-кредитная сфера деятельности является особым объектом защиты в современном международном и национальном праве. Обеспечение ее кибербезопасности включается в основные положения всех действующих и принимаемых договоров и нормативных правовых актов, регламентирующих отношения, возникающие в указанной сфере. Так, в принятой в 2011 г. Конвенции ООН об обеспечении международной информационной безопасности прямо говорится о необходимости реализации государствами политики, нацеленной на защиту граждан от противоправных деяний в информационном пространстве, в том числе путем принятия соответствующих законодательных актов и укрепления международного сотрудничества.

В Российской Федерации за последние годы приняты целый комплекс законодательных и иных нормативных правовых актов, регулирующих обеспечения кибербезопасности финансово-кредитной сферы. К данным актам следует отнести не только общие законы, например, Гражданский кодекс Российской Федерации, но и специальные Федеральные законы, такие как «О национальной платежной системе», «О банках и банковской деятельности», «О безопасности критической информационной инфраструктуры Российской Федерации» и др. В частности, в Федеральном законе от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» к субъектам критической информационной инфраструктуры отнесены государственные органы, государственные учреждения и российские юридические лица, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в банковской сфере и иных сферах финансового рынка.

Также отдельные вопросы обеспечения безопасности информационно-коммуникационной среды финансово-кредитной сферы регулируются нормативные актами Президента РФ, Правительства РФ. В отдельных областях финансовой деятельности применяются нормативные акты федеральных органов исполнительной власти (ФНС России, ФТС России), которые регламентируют обеспечение информационной безопасности в соответствующей сфере.

Особое место в системе обеспечения безопасности информационно-коммуникационной среды финансово-кредитной сферы занимает Центральный банк РФ. Банковская сфера является одним из основных направлений киберпреступлений, которые становятся не только внутринациональной, но и глобальной международной проблемой.

В целях защиты банковской системы в структуре Банка России был образован Департамент информационной безопасности. Он участвует в разработке и межведомственном согласовании федеральных законов, нормативных актов Банка России, а также рекомендательных писем и других документов по вопросам обеспечения информационной безопасности, киберустойчивости и применения информационных технологий в отношении финансовых организаций, кроме вопросов обеспечения безопасности сведений, составляющих государственную тайну.

В сфере нормативного регулирования основной задачей Департамента является переход к комплексной организации обеспечения информационной безопасности и киберустойчивости организаций кредитно-финансовой сферы. В рамках этой задачи спланировано и уже осуществляется реализация информационной безопасности финансовых организаций на трех технологических уровнях: уровне инфраструктуры, уровне прикладного программного обеспечения (или уровне приложений) и уровне технологий обработки данных.

Другой важной задачей Департамента является регулирование и контроль (надзор) за обеспечением информационной безопасности, киберустойчивости и применением информационных технологий в отношении финансовых организаций. Для этого Банк России планирует перейти к рискориентированному подходу в надзорной деятельности в области информационной безопасности и получать объективные данные, характеризующие уровень и качество управления киберриском в каждой организации кредитно-финансовой сферы. Это позволит делать выводы об их киберустойчивости и операционной надежности, а также степени влияния киберриска на уровень финансовой стабильности финансового рынка России в целом.

В 2015 г. в структуре Департамента был образован специальный Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере. Основными задачами Центра мониторинга являются формирование единой системы противодействия угрозам с

участием заинтересованных федеральных органов исполнительной власти, финансовых организаций и структурных подразделений Банка России, а также участие в разработке методологии его контрольно-надзорной деятельности. В его функции входят организация и координация обмена информацией между поднадзорными кредитными организациями и правоохранительными органами, ведение мониторинга открытых ресурсов сети «Интернет» для обнаружения и предупреждения информационных атак, взаимодействие с иностранными группами реагирования на компьютерные атаки, проведение компьютерных исследований [1].

Особую роль в обеспечении кибербезопасности занимает созданная и функционирующая в Центре мониторинга система информационного обмена между участниками финансового рынка, правоохранительными органами, провайдерами и операторами связи, системными интеграторами, разработчиками антивирусного программного обеспечения и другими компаниями, работающими в сфере информационной безопасности. В информационном обмене на сегодняшний день участвует более 800 различных организаций, в том числе все российские банки. Участники информационного обмена сообщают о выявленных ими угрозах и совершенных на них кибератаках, а Центр мониторинга дает рекомендации по противодействию этим рискам. Это помогает оперативно реагировать на возникающие угрозы, не допускать их распространения, а также минимизировать потери финансовых организаций и их клиентов.

В Федеральном законе от 27.06.2018 № 167-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств» были расширены полномочия Банка России по регулированию информационной безопасности не только в кредитных организациях, поднадзорных субъектах национальной платежной системы, но и во всех некредитных финансовых организациях, вплоть до микрофинансовых организаций, сельскохозяйственных кредитных потребительских кооперативов, ломбардов, страховых, инвестиционных компаний, брокеров и негосударственных пенсионных фондов.

Практически одновременно с вышеназванным Федеральным законом Банк России издает указание от 07.05.2018 № 4793-У «О внесении изменений в Положение Банка России от 9 июня 2012 года №

382-П “О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств”» (в настоящее время утратило силу. Действует Положение Банка России от 04.06.2020 № 719-П), в соответствии с которым для операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств устанавливается обязательность информирования о выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств на всех технологических участках, участвующих в осуществлении переводов денежных средств, не только на участке платежной системы Банка России.

Однако несмотря на принимаемые законодательные, нормативные и технико-правовые меры обеспечить эффективную кибербезопасность банковской сферы нашей страны не всегда удается. Так, по итогам 2019 г. ущерб российских банков от кибератак составил более 510 млн руб. В начале 2021 г. Банк России сообщил о существенном росте потерь от всех видов киберпреступлений с использованием вредоносных программ, направленных как напрямую на банки, так и на их клиентов. Общий ущерб от этого составил почти 9,77 млрд руб. [2]

В то же время Банк России значительно усилил надзор в области обеспечения информационной безопасности в организациях кредитно-финансовой сферы. В числе мероприятий дистанционного надзора включаются обработка отчетности кредитных организаций, мониторинг средств массовой информации, обращения граждан через интернет-приемную Банка России, информация по инцидентам. В рамках контактного надзора осуществляются инспекционные проверки по вопросам обеспечения информационной безопасности и применения информационных технологий в организациях кредитно-финансовой сферы.

В связи с этим следует сделать вывод о необходимости продолжать деятельность на всех уровнях финансово-кредитной системы по внедрению наиболее эффективных правовых механизмов, которые способствовали бы укреплению и повышению устойчивости в обеспечении кибербезопасности. Здесь необходимо обратить внимание на

создание и внедрение в кредитных организациях и иных участников финансового рынка специальных структурных подразделений, в обязанность которых входит защита от кибератак как проводимых операций, так и персональных данных клиентов. Так, в ВТБ в прошлом году было зарегистрировано 750 тыс. событий, связанных с подготовкой и проведением кибератак, но благодаря внедрению современных технико-правовых механизмов внутри банка только с начала 2021 г. удалось «спасти» почти 2 млрд руб. клиентов [3].

На сегодняшний день во многих организациях финансово-кредитной сферы уже функционируют структурные подразделения и приняты специальные нормативные акты, регламентирующие вопросы обеспечения кибербезопасности [4], однако в полной мере обеспечить надежность защиты еще не удается. Поэтому необходимо и дальше разрабатывать и внедрять комплекс мер, включающий как формирование правовых механизмов, так и совершенствование технических средств для повышения эффективности кибербезопасности.

Литература

1. Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере — специальное структурное подразделение Банка России // https://cbr.ru — официальный сайт Банка России.
2. Group-IB: ущерб от кибератак на российские банки и их клиентов // https://vc.ru (дата обращения: 23.01.2022).
3. Костин, А. Актуальные инициативы в области кибербезопасности // ПЛАС. 2021. 28 мая.
4. Правила личной кибербезопасности Сбербанка России // https://www.sberbank.ru — официальный сайт Сбербанка России.

Dr. Nashaat Edward Nashed

Economic consequences of implementing smart contracts in the transport sector

Abstract. The transport sector is considered one of the most important vital service sectors, which is closely and directly linked to all other sectors in the country, and transport networks are the main nerve on which the economic and social de-

velopment programs are based. The transport sector promotes economic activity and is fundamental to human well-being, but this sector has significant impacts on the environment and human health. Transportation activity is increasing worldwide as economies grow, which means that gas emissions from the sector are also increasing. This is largely because 95 percent of the world's transportation energy still comes from fossil fuels.
Keywords: economy; smart contracts; transportation.

Chapter 1: smart contract in transport sector

1. The transport sector is considered one of the most important vital service sectors, which is closely and directly linked to all other sectors in the country, and transport networks are the main nerve on which the economic and social development programs are based. And the river.

A smart contract is a self-executing contract with the terms of the agreement between the buyer and seller written directly into lines of code. The code controls the execution, and the transactions are traceable and irreversible. Smart contracts allow trusted transactions and agreements between disparate and anonymous parties to be executed without the need for a central authority, legal system, or external enforcement monitoring mechanism (1).

In the context of smart flood insurance where the customer installs a tamper-resistant flood sensor, a GPS system and a camera capable of determining the water level and sending information about the water level to the Ledger System

This information will enable an appropriate premium to be determined based on risk information, details and the client's particular circumstances.

2. The customer will choose the document or smart contract based on the indications they have set in advance. With the document in place, Pinsent Masons envision the possibility of using the smart contract to collect the monthly installment from the customer and to pay compensation to the customer when a flood occurs

Overall, there seems to be a huge opportunity for automatic payments in the market. The smart contract can be used to automatically pay com-

[1] Helen Eenmaa-Dimitrieva and Maria José Schmidt-Kessen : Smart Contracts: Reducing Risks in Economic Exchange with No-Party Trust?, European Journal of Risk Regulation, 2019. P. 4.

pensation to customers when the risk occurs, as soon as the customer pays the insurance premium.

Securing cargo Regarding cargo, IBM and Maersk have recently developed an electronic container tracking and tracing system between ports that enables all parties involved to track the container and results in a simplified and efficient shipping process, as containers are equipped with sensors.

The suggestion is that these physical sensors could provide information in shipping documents as they act just like the sensors on roofs that were used to coat local buildings to initiate moisture claims.

Data generated from sensors in underwriting can be used to calculate premiums more accurately, reduce the possibility of data inaccuracies, mitigate losses and damages, and automatically pay resulting claims when risk occurs.

This technology can be used to settle a claim without any additional human intervention.

For example: a shipment exposed to heat in connection with loss mitigation If the sensors detect a temperature increase the sensors will be sent to the customer to take the necessary measures to prevent the loss of the shipment.

If a shipment loss occurs and is detected by the trusted Oracle system hardware, the compensation will be paid to the customer automatically.

Case of Aviation

With regard to aviation, current technology offers several ways in which smart contracts can be applied in this field.

The digital asset records will enable customers to enter all the information about their fleet and then this information is sent across the systems where the appropriate fair premium is calculated for them.

Just like systems already used in auto insurance, Telematics technology can be used to collect and analyze data on aircraft use and care to increase the accuracy of the underwriting process. Two chances:

To track the customer's responsibility to pay an additional premium if the aircraft enters a restricted area outside the scope of insurance coverage.

Provide the necessary warning and instructions if the aircraft is approaching unusually bad weather to mitigate losses.

Helfand also specified that the software be used in estimating the repair cost or compensation amount by comparing photos of the condition of the insured property before the loss with photos after the loss.

Claims assessment and settlement

Self-executing smart contracts have the potential to achieve greater efficiency in distribution channels such as when renewing, updating data when any changes occur and also on making claims that can be used in a variety of areas, from healthcare to supply chains to financial services in cases of cooperation with the transportation sector.

Financial Services

Smart contracts are helping to transform traditional financial services in multiple ways. In the case of insurance claims, they check for errors and route payments and remit them to the user if they find everything suitable.

Smart contracts include important tools for bookkeeping and eliminating the possibility of intrusion into accounting records. It also enables shareholders to participate in decision-making in a transparent manner. These smart contracts also aid in trade clearing, whereby funds are transferred once trade settlement amounts are calculated.

For example, transaction costs may be much lower when viewing and settling claims as they are automated and programmed and there is no potential for human error.

The claims stage is an important moment in the insurance relationship. This is the moment when the insurer is required to perform its contractual obligation, as traditionally understood (Maritime Insurance Act, 1906) but which incurs significant costs to insurers in evaluating the claim, negotiating and paying the customer.

Currently, the compensation settlement process is a lengthy process even in cases where there is no dispute or doubt about the underwriter's liability for the claim, as lengthy procedures are taken to verify the validity of the claims.

The automatic payment of compensation in these cases may mean that the customer will receive the compensation value more quickly and thus the smart contract may respond more effectively when the loss occurs, which will end many disputes between the customer and the insurance companies, which will not require them to go to the courts again and save the costs of cases and will increase the confidence of the customer and company each other.

Chapter 2: Economic benefits of smart contracts

The importance of the economic return from transport projects and the attraction of more foreign investments in this sector, which is one of the

most attractive elements of investment, as the volume of investment reached one trillion and 600 million pounds," according to what the Ministry of Transport announced, a large number that reflects the importance of this vital sector. And for the record, starting from 1/4/2019, payment will be made electronically, in implementation of the decision of the Egyptian Prime Minister, in the event that the value reaches a certain segment.

1-Autonomy and saving

Smart contracts do not need intermediaries or other intermediaries to confirm the agreement; Thus, it eliminates the risk of manipulation by third parties.In addition, the lack of an intermediary in smart contracts leads to cost savings.

2-Backup

All documents stored on the blockchain are duplicated multiple times, thus, the originals can be restored if any data is lost.

3-Safety(1)

Smart contracts are encrypted, and encryption keeps all documents safe from intrusion.

4-Speed

Smart contracts automate tasks using computer protocols, saving hours of different business processes.

Precision

Using smart contracts eliminates errors that occur due to manual filling of many forms.

The smart card, which was launched by the Egyptian Ministry of Transport and carries all the data of its holder for use in various means of transportation in the subway, railways and other means of transportation, will facilitate the Egyptian citizen and save a lot of time, and even end the stage of the paper ticket once and for all, especially with the direction of the Egyptian state to transform digital at the moment.

Declared models of protocols in the transport sector:

Between Egypt and the Arab countries

Between Egypt and foreign countries

t and African countries

Protocols of port cooperation between Egypt and Arab countries

[1] Leena S. Alotaibi and Sultan S. Alshamrani: Smart Contract: Security and Privacy, Computer Systems Science & Engineering, 2021. P. 97.

Cooperation protocols between free zones

Port cooperation protocols with foreign countries

Protocols of port cooperation between Egypt and African ports

Between Egypt and the countries of the world to recognize the certificates of seafarers

The essential texts of the Egyptian maritime conventions

•The competent maritime authority of the two contracting parties, a ship of a contracting party, a crew member, a shipping company ... etc.

The spatial scope of the application of the agreement as it applies in the territory of each of the contracting parties

Encouraging shipping companies in the two countries to operate a regular navigation service between their ports

•Participation of the ships of the two contracting parties in the transfer of mutual foreign trade between the two contracting parties on equal bases(1)

•Identification documents for seafarers (naval passport or passport for Egypt)

•Treating the ships of the two contracting parties in their respective ports on the basis of reciprocity with regard to the entry and exit of ships and the use of the facilities for loading and unloading goods and the boarding and disembarking of passengers

•Mutual recognition of documents on board

•Allow crew members to disembark to the port city and allow them to pass in transit to their ship or to any other vessel

Providing assistance to the ship, its crew, its cargo and its passengers in the event of its sinking, delinquency, or any other accident in the port or territorial waters of the other party.

The revenue generated from the maritime transport activity of shipping companies in the ports of the other contracting party is subject to income tax in the territory of the party whose flag the ship is flying only()

•Forming a joint navigation committee between the specialists in the two countries to follow up the implementation of the agreement and resolve any disputes arising from the implementation.

Entry into force of the agreement

A data bank(1) in the Egyptian maritime transport sector:

[1] Lyle Daly:What Are Smart Contracts, the motley fool. 2022. P. 1.

The first specialized data bank in the Middle East, Africa and the Arab world to provide distinguished, high-level information services based on information accuracy, speed of performance, periodic update, unlimited informational benefit for a limited fee. The official source of information approved by the state for maritime transport data.

The vision is to provide all information to decision makers, those interested in the maritime transport industry and researchers, through a central database connected to the Egyptian port authorities.

The message includes contributing to an effective role in raising the performance of Egyptian maritime transport by providing accurate and documented information, with diverse printed and visual visions; With high quality, for all those dealing with the Egyptian shipping industry using the latest information technology technologies.

One of the Bank's objectives is to provide accurate data and information on the sector's activities to serve planners, decision makers and those interested in the maritime transport industry.

The bank's operating systems consist of several main groups that cover most of the Egyptian maritime transport activities through a central database that is updated periodically from all external data bank sites:

•Egyptian port movement systems, including the movement of ships, goods, containers and passengers.

•The systems of the Egyptian Authority for the Safety of Maritime Navigation, including the data of Egyptian ships and marine units, marine passports, contracts, accidents and pollution.

•Bibliographical systems including maritime legislation.

Data Bank Services(2)

•Providing information and interactive services through the Bank's official website: www.mts.gov.eg

•Issuing all kinds of pre-processed reports.

•Designing and preparing various detailed and statistical reports.

•Direct search of databases.

•Issuing periodicals (in both Arabic and English), which include:

— Statistical Yearbook: An economic and statistical analysis of Egyptian port traffic data.

[1] www.mot,gov.eg

[2] Nick Szabo : Smart Contracts: Building Blocks for Digital Markets, 2018. P. 12.

— Sea Ports Directory: Basic data for the main and specialized Egyptian ports and the economic zone of the Suez Canal.

— Entities and Companies Directory: Basic data for companies and entities working in the field of maritime transport.

— Maritime legislation: a set of volumes that include laws and decisions regulating maritime transport activities within the Arab Republic of Egypt.

The transport sector promotes economic activity and is fundamental to human well-being, but this sector has significant impacts on the environment and human health. Transportation activity is increasing worldwide as economies grow, which means that gas emissions from the sector are also increasing. This is largely because 95 percent of the world's transportation energy still comes from fossil fuels.(1)

Transportation activity is increasing worldwide as economies grow, which means that the sector's emissions are also rising. This is largely because 95 percent of the world's transportation energy still comes from fossil fuels. At UN Environment, work is being done to sever the link between increased mobility and increased emissions. We believe low-carbon mobility can reduce pollution while creating jobs, making streets safer, strengthening infrastructure and stimulating local economies. The United Nations is a partner in many leading global transport programs in areas such as fuel economy, small particle pollution, and infrastructure development, some of which are implemented through public-private partnerships. This is done through contracts between organizations.

Technological applications are the key factor to stay competitive

The current period is witnessing strong competition between smart or participatory transport companies, and the success of each of them is linked to the quality of service, and keeping pace with technological applications aimed at providing a good service for the passenger.

The transport sector in Egypt is one of the promising fields, especially since there are a number of elements for Hajj, including the number of passengers increasing on a daily basis, and the current road network, in addition to the government seeking to involve the private sector in basic services.

[1] StefaniaFiorentino , Silvia Bartolucci : Block chain-based smart contracts as new governance tools for the sharing economy, Elsevier, 2021. P. 1.

Reference

1. Helen Eenmaa-Dimitrieva and Maria José Schmidt-Kessen: Smart Contracts: Reducing Risks in Economic Exchange with No-Party Trust? European Journal of Risk Regulation, 2019.
2. Leena S. Alotaibi and Sultan S. Alshamrani: Smart Contract: Security and Privacy, Computer Systems Science & Engineering, 2021.
3. Lyle Daly:What Are Smart Contracts, the motley fool, 2022.
4. Nick Szabo: Smart Contracts: Building Blocks for Digital Markets, 2018.
5. StefaniaFiorentino, SilviaBartolucci: Block chain-based smart contracts as new governance tools for the sharing economy, Elsevier, 2021.
6. www.mot,gov.eg

Маликова Яна Ивановна,
кандидат экономических наук, доцент, доцент кафедры менеджмента,
Образовательная автономная некоммерческая организация высшего профессионального образования «Институт образовательных технологий и гуманитарных наук»

Горелов Дмитрий Владимирович
кандидат экономических наук, доцент, доцент кафедры менеджмента,
Образовательная автономная некоммерческая организация высшего профессионального образования «Институт образовательных технологий и гуманитарных наук»

Эфендиев Тахир Сейпуевич,
кандидат юридических наук, доцент кафедры «Административное право, экологическое право, информационное право», Юридический институт Российского университета транспорта (МИИТ)

Информационная безопасность на транспорте проблемы и пути решения

Аннотация. В статье рассмотрены особенности информационной безопасности на транспорте, указаны проблемы и пути решения. Основное внимание уделено железнодорожному транспорту. Отражена проблема формирования в России системного подхода к обеспечению транспортной безопас-

ности. Обоснована необходимость совершенствования нормативной базы регулирования транспортной безопасности.

Ключевые слова: цифровизация; информационная безопасность; информационные ресурсы; транспортная безопасность.

Malikova I. Iana,
PhD in Economics, assistant professor Department of management
Educational Autonomous Non-commercial Organization of higher education «Institute of Educational Technologies and Humanities»

Gorelov V. Dmitry,
PhD in Economics, assistant professor Department of management
Educational Autonomous Non-commercial Organization of higher education «Institute of Educational Technologies and Humanities»

Efendiev S. Tahir,
PhD in Economics, assistant professor Department «Administrative Law, Environmental Law, information law»

Information security in transport problems and solutions

Abstract. The article discusses the features of information security in transport, identifies problems and solutions. The main attention is paid to railway transport. The problem of the formation of a systematic approach to ensuring transport security in Russia is reflected. The necessity of improving the regulatory framework for regulating transport security is substantiated.

Keywords: digitalization; information security; information resources; transport security.

На сегодняшний день, когда видны результаты цифровизации во многих отраслях производства, в том числе в сфере транспортной безопасности, можно сформулировать не только выявленные проблемы, но и пути их решения. Бесспорным утверждением можно считать, создание необходимых технических условий для обеспечения цифровой трансформации процессов транспортной безопасности.

Как отмечается в оценке экспертов Организации экономического сотрудничества и развития, к 2030 г. инвестиционные потребности

мировой транспортной инфраструктуры, включающей аэро- и морские порты, железные дороги, а также трубопроводы, составят 11,3 трлн долл. Предполагается, что более 44% этого объема должны составить инвестиции в железнодорожную инфраструктуру (порядка 5 трлн долл.), что связано в первую очередь с развитием информационных технологий.

Целесообразно отметить, что в соответствии с положениями Доктрины информационной безопасности Российской Федерации (утверждена Указом Президента РФ от 05.12.2016 № 646) одним из национальных интересов в информационной сфере является обеспечение устойчивого и бесперебойного функционирования критической информационной инфраструктуры (КИИ) Российской Федерации. Важным направлением деятельности в области устойчивого и бесперебойного функционирования КИИ является обеспечение ее информационной безопасности. Информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере транспорта, Федеральным законом РФ от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры» отнесены к субъектам КИИ.

На сегодняшний день созданы надежные средства защиты информации и обеспечения информационной безопасности сложных систем, которые предусматривают решение проблем в управлении их информационной безопасностью; разработана концепция обеспечения информационной безопасности в автоматизированных, информационных и телекоммуникационных системах, методология и задачи защиты информации в них; определены принципы управления информационной безопасностью; обоснована необходимость создания подсистемы управления безопасностью информации; разработаны отдельные модели, методы и методики управления защитой информации в программно-аппаратных комплексах; разработана методология динамической защиты компьютерных систем; исследованы различные аспекты выявления, обнаружения и ликвидации уязвимостей и компьютерных атак, а также проблемы устойчивого функционирования компьютерных систем в условиях информационно-технических воздействий; предложена архитектура и подходы к построению системы интеллектуальных сервисов защиты информации в критически важных инфраструктурах.

Данные достижения позволили в целом обеспечить приемлемый уровень информационной безопасности в сфере применения информационных технологий, но динамика развития самих информационных технологий, динамика их внедрения в практику автоматизации деятельности транспортной системы, динамика быстрого морального «старения» средств защиты информации свидетельствует, что эффективность управления обеспечением должного уровня защищенности критической информационной инфраструктуры не будет отвечать критерию приемлемого риска получения недопустимого ущерба (делового, коммерческого, функционального), не позволяет обеспечить высокий уровень готовности автоматизированных систем критического применения к решению своих функциональных задач в условиях деструктивных информационно-технических воздействий.

Одна из проблем, которая вносит существенные ограничения, — это обеспечение информационной безопасности и защиты персональных данных в сфере транспорта. Необходима разработка рекомендаций для внесения в нормативно-правовые акты, регламентирующие обеспечение транспортной безопасности в части использования и защиты персональных данных пассажиров.

Также отдельные виды транспорта отличаются низкой мобилизационной готовностью, что влечет опасности при вовлечении нашей страны в систему международного транзита. Существенная проблема — отсутствие четкой и единой системы разделения сфер ответственности между государственным и частным сектором в сфере транспортной безопасности при осуществлении перевозок.

Военная угроза в настоящее время требует масштабного использования транспортной сферы, так как может возникнуть необходимость экстренно и массово произвести эвакуацию населения из крупных городов, для чего должна быть задействована вся система транспорта, посредством которого возможно вывести значительное число людей[1].

Сегодня как никогда большое значение имеет государственная политика в сфере транспортной безопасности, которая направлена на обеспечение национальной безопасности в целом, на предотвращение

[1] Коморин А. Н. Проблемы в сфере обеспечения транспортной безопасности и пути их решения // Развитие личности и общества: экономические, политико-правовые и культурные аспекты : сборник научных трудов по материалам Международной научно-практической конференции 28 декабря 2021 г. Белгород : ООО Агентство перспективных научных исследований (АПНИ), 2021. С. 56—58 // URL: https://apni.ru/article/3437-problemi-v-sfere-obespecheniya-transportnoj

материального ущерба, причинения вреда здоровью людям, на предотвращение иных негативных последствий, что может быть достигнуто на основе совершенствования правовой базы.

Сейчас регулирование транспортной безопасности осуществляется посредством отдельного федерального закона, существуют и специальные программы развития транспорта, определяющие в том числе и содержание государственной политики в области обеспечения транспортной безопасности[1]. То есть идет работа в сфере совершенствования законодательной базы, регламентирующей вопросы транспортной безопасности, но их явно недостаточно.

Таким образом, на современном этапе следует рассматривать совершенствование законодательства в анализируемой сфере в качестве приоритетной задачи. Сейчас выделяют следующие проблемы, влекущие к снижению защищенности транспортной сферы:

— отсутствие осознания государством необходимости использовать на всех видах транспорта наиболее эффективные и современные технологии безопасности, руководствуясь при этом зарубежным опытом, и, как следствие, недостаточность финансирования данного направления;

— отсутствие эффективного анализа соотношения затрат и выгод от тех или иных процедур, реализуемых в целях обеспечения транспортной безопасности.

Подводя итог, можно утверждать, что в настоящее время требуется совершенствовать нормативную базу регулирования транспортной безопасности, распределять зоны ответственности в данной сфере и формировать комплекс специальных мер, позволяющих минимизировать угрозы. И выработку системного подхода к повышению эффективности обеспечения транспортной безопасности нельзя откладывать на долгий срок, необходимо как можно быстрее начать работу в данном направлении, поскольку значение транспортной безопасности во всех сферах жизнедеятельности огромно, ее качество оказывает существенное влияние и на социально-экономическое развитие государства, и на защиту государственного суверенитета и национальной безопасности.

[1] Чередниченко А. Е. Транспортная безопасность как важнейшая составляющая национальной безопасности // Актуальные вопросы науки и практики. Сборник научных трудов по материалам XIII Международной научно-практической конференции. М., 2019. С. 108

Овечкин Александр Петрович,
доктор философских наук, профессор, профессор кафедры «Административное право, экологическое право, информационное право» Юридического института Российского университета транспорта (МИИТ)

К вопросу о понятии кибербезопасность

Аннотация. Повсеместная цифровизация обнаружила одну из важнейших глобальных проблем — проблему кибербезопасности. Понятие кибербезопасности начинает шире и активнее использоваться как в международном праве, так и правовых системах многих государств. Однако в российском законодательстве оно не получило своего должного освещения.

Ключевые слова: кибербезопасность; информационная безопасность; защита информации.

Alexander P. Ovechkin,
Doctor of Philosophy, Professor, Professor of the Department of Administrative Law, Environmental Law, Information Law of the Law Institute of the Russian University of Transport

On the question of the concept of cybersecurity

Abstract. Ubiquitous digitalization has turned into one of the most important global problems — the problem of cybersecurity. The concept of cybersecurity is becoming more widely and actively used both in international law and in the legal systems of many States. However, it has not received its proper coverage in Russian legislation.

Keywords: cybersecurity; information security; information protection.

Информатизация и цифровизация представляют обществу и человеку все больше и больше разнообразных благ. Но одновременно с приходом информационных технологий резко активизировалась деятельность преступных группировок, а в обиход прочно вошло новое слово «хакер». Причем преступления в информационной сфере оказались куда более разрушительными и общественно опасными. С помощью кибертехнологий осуществляются теракты, незаконно изымаются огромные денежные суммы, парализуется деятельность круп-

ных компаний, крадутся сведения о миллионах людей. По расчетам некоторых экспертов убытки, причиненные действиям хакеров мировой экономики, достигают триллионов долларов, а количество случаев хакерских атак в 2019 г. возросло в два раза по сравнению с предыдущим годом [3]. При этом все эти преступления совершаются в глобальном киберпространстве, что серьезным образом затрудняет поиск киберпреступников.

Победу в борьбе с киберзлом можно одержать только принятием глобальных многоуровневых системных мер. Одной из наиболее эффективных и действенных мер является обеспечение правового регулирования отношений в киберпространстве как на международном, так и национальном уровне. Однако правовая регламентация этих отношений далека от совершенства. Среди множества имеющихся в этой сфере проблем особо выделяется проблема отсутствия правовой терминологической ясности и несогласованности. В данной статье обратимся к исходному и ключевому понятию кибербезопасность — термин, получивший прописку в международном и зарубежном законодательстве, но не нашедший никакого отражения в отечественных нормативных актах. Предпринятая в 2014 г. попытка принятия Концепции стратегии кибербезопасности Российской Федерации, в которой был разработан современный терминологический аппарат, оказалась нереализованной.

В правовых нормативных актах нашей страны закреплены термины: информационная безопасность и защита информации. Из ст. 1 и 8 Федерального закона от 28.12.2010 № 390-ФЗ «О безопасности» вытекает, что эти термины включены в иные виды безопасности. В гл. 16 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» речь идет не об информационной безопасности, а о защите информации, а за правонарушения в этой сфере ст. 13.12 Кодекса РФ об административных правонарушениях предусмотрена административная ответственность.

В Стратегии и Доктрине национальной безопасности Российской Федерации говорится уже не о защите информации, а об информационной безопасности, которая рассматривается как вид национальной безопасности, целью которого является укрепление суверенитета государства в информационном пространстве. В Основах государствен-

ной политики Российской Федерации в области международной информационной безопасности (см. Указ Президента РФ от 12.04.2021 № 213) и Концепции внешней политики Российской Федерации (см. Указ Президента РФ от 30.11.2016 № 640) появляется еще один термин — международная информационная безопасность. Но не ясно как он соотносится с термином «национальная безопасность», то ли он является его разновидностью, то ли самостоятельным направлением деятельности по обеспечению информационной безопасности/

Таким образом, законодатель, прежде всего, опирается на термин «информационная безопасность». Однако было бы неверным сбрасывать со счетов кибертерминологию, тем более что она все активнее входит в правовой оборот международного права и национальные правовые системы многих государств. В научной литературе по этому вопросу существуют различные точки зрения. В некоторых источниках оба эти понятия рассматриваются как тождественные [4]. Вряд ли такая точка зрения отражает современные реалии. Нормативное определение информационной безопасности сводится лишь к социальным аспектам, а именно защищенности личности, общества и государства. Но эта защищенность обеспечивается многими факторами: организационными, техническими, нравственными и др., которые не нашли своего отражения в данном определении. Правда, некоторые из них названы в системе обеспечения информационной безопасности.

Ряд правоведов предлагают свести кибербезопасность к совокупности методов, которые призваны защищать информацию, посредством защиты телекоммуникационных каналов как хранителей и распространителей информации [2]. Трудно согласиться с тем, что кибербезопасность ограничивается исключительно совокупностью приемов, средств и способов информационной защиты. Она требует целого комплекса мер, включая специализированное программное обеспечение, наличие подготовленных кадров, определенной информационной культуры пользователей и т.д.

Распространенным является взгляд на кибербезопасность лишь как на техническую часть информационой безопасности [1]. В этом случае она сводится только к информационным технологиями по защите сетей, портов, программного обеспечения, технических устройств от хакерских атак. Но при таком подходе нивилируется роль субъективного фактора.

Существует и противоположенная точка зрения, согласно которой кибербезопасность кроме информационной безопасности включает в себя безопасность приложений, сетевую и операционную безопасность, обучение пользователей и т.д. [5] На наш взгляд, такая позиция допустима. Но при условии, что главным разграничителем понятий «информационная безопасность» и «кибербезопасность» является способ распространения и хранения информации.

В соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» под информацией понимаются сведения (сообщения, данные) независимо от формы их представления. Исходя из п. 1 ст. 16 защите подлежит любая указанная в ней информация, независимо от формы ее представления (бумажная, устная, электоронная и т.д.). Из содержания Доктрины также вытекает, что информационная безопасность предполагает защиту информацию в любых формах ее представления. Поэтому, когда говорят об информационной безопасности, подразумевается защита информации, представленной и распространяемой в любой форме и любыми способами. Кибербезопасность обеспечивает защиту информации, хранящуюся на специальных технических устройствах и распространяемую через телекоммуникационные системы.

Таким образом, кибербезопасность — это организационная, правовая, нравственная, техническая и технологическая защита информации граждан, юридических лиц, публичных образований, хранящейся на технических устройствах и распространяемая с помощью телекоммуникационных систем от несанкционированного доступа к ней. Кибербезопасность включает в себя непосредственную защиту самой информации (например, путем ее кодирования, запрета на копирование, скрытия папок и файлов и др.), а также опосредованную защиту информации. Она осуществляется посредством ограничения или запрета доступа к техническому устройству, на котором хранить-ся информация (компьютер, мобильный телефон, планшет), к серверам, сетям, софтам, программному обеспечению и т.д. Кибербезопасность решает задачи по сохранности информации, нейтрализации или снижению рисков от киберататк, недопущению сбоев и отказов в работе техники, защите от различного рода террористических и мошеннических действий.

Литература

1. Демидов, О. В. Обеспечение международной информационной безопасности и российские национальные интересы // Индекс Безопасности. 2013. № 1.
2. Елизарова, Е. О. Правовое регулирование цифровой безопасности в России и странах АТР и ее соотношение с кибербезопасностью / Е. О. Елизарова, В. М. Настич, С. С. Чекулаев // Юридическая наука. 2020. № 6. С. 42—46.
3. Мухин, В. Н. Современные тенденции развития цифровой экономики и ее влияние на предпринимательскую деятельность. -// Молодой ученый. 2020. № 48 (338).
4. https://megatrends.su%D)%B1%D0%BB%D0%BE%D0%B3/cybersecurity.
5. https://elcomienzo.ru/kiberbezopasnost.

Arbia Hlali
Department of economics, University of Sfax, Tunisia

The challenge of data protection in the maritime transport: case of shipping industry

Abstract. The arrival of new technologies or more generally the digital transformation of the maritime sector is driving a critical shift in the volume and importance of the data processed for and by the ship. In Due to the exponential growth of digital data, the need of management and security of these becomes the first challenge of the maritime activities. In addition, the sector is increasingly using objects connected or insufficiently protected embedded systems. Management of data in the broad sense is therefore at the center of maritime activities and naval defense. This requires the establishment of a real policy of data security, integrating the detection of intrusion attempts, malicious code, data leaks and suspicious behavior. In this context, this paper studies the challenges of data protection in the maritime sector with focus on the shipping case in particular. The organization of the paper is as follows: the first section represent a view on the data protection in maritime sector. The section two studies the different challenges that maritime industries survey. In third section study the case of shipping industry.

Keywords: maritime transport, digital transformation, data protection in maritime sector.

Introduction

Digitization and digitization of transport are latent, especially in transport of goods. The fragmentation of this sector once again poses problems: the investment needed to digitize and facilitate transactions and the supply chain in general is difficult to advance for small structures than for large ones groups.

In addition, the shipping industry systems are linked to separate integrated transport systems (Jović et al. 2019). For example, maritime operations involve complex procedures that require the interaction of many actors (Jović et al. 2019). Additionally, numerous rules and regulations govern the industry, making transactions rigid, complex, and costly both in time and money (Jain 2018). In addition, the maritime sector operates using an information network that has different parties (Jabbar and Bjørn 2018). Also, in the maritime industry there is a large amount of data that is generated from different sources and in different formats. This includes traffic data, freight data, etc., (Zaman, I. et al. (2017).

1. Data protection in the maritime transport

Digitization affects the maritime sector, like many others sector, into the world of hyper-connection: list of precious cargoes, tracing and intelligent routing, connected objects, predictive refueling, assisted positioning of loads, port optimisations, etc.

The ecosystem, ship, cargoes and port infrastructures, become targets for cybercriminals

Operational technologies, automated data processing tools industrial environments are still in the early stages apprehension of cybersecurity issues but move forward quickly in this area in order to cope with the digital convergence.

The ships or Port infrastructure is no exception to this observation. The flaws in the industrial system are linked to the following observations:

• The absence of partitioning between the general information systems and unsecured industrial systems;

• the low level of access protection with controls sometimes nonexistent or very simple, the widespread use of administrator accounts and the lack of protection on access terminals;

• The very low level of updating and the use of protocols not reliable and unencrypted;

• The lack of vision and integration of security into the often internal developments;

• Lack of monitoring of anomalies;

• The ever-increasing integration of non-hardened systems available easily and not mastered or not known to the teams in charge;

• the lack of control of stakeholders on the systems such as subcontractors or maintainers.

In the same context, the cybersecurity is at the heart of many security topics and the manipulation of data is becoming more and more frequent. Today, where information is a resource, the data manipulation can give a competitive advantage by providing many information. Maritime transport is increasingly exposed to cyber-attacks due to increasing technological developments and crews destined to be restricted. Hacking the data of shipowners, container ships, carriers and port officials could be used for cargo. This risk highlights the need for cybersecurity related to the availability, integrity, confidentiality of information.

However, this is not the only type of attack. For example, the recent context has demonstrated large-scale destabilization of data integrity. Malicious software which, once entered into the computer network, is able to encrypt all the data present on an information system and generate a general paralysis of the activity of a targeted company. If this same type of attack appeared in a port area, paralysis, even of short duration, would disorder completely the supply chains of several companies, and this, simultaneously.

There are a multitude of plausible attacks due to the digitization and exploitation of old information systems, such as ransomware, identity theft, tampering with data, disclosure of information, denial of service, or elevation of privilege to within an information system, in order to become omnipotent as an attacker. Organizations have, until today, reacted to the drastic changes in the supply chains in different ways. Some put pressure on suppliers in order to integrate common systems to obtain a better visibility of the goods.

For contractors, some still use old systems to integrate and communicate information like the EDI system. This decision may be related to a lack of strategy by these actors, or even a fear of digitizing all the information because the transition is not mastered, or there is no expertise to do so. Although this transition is costly, other players have directly opted for a digital solution, with a specialized and secure network to manage information in a precise manner. Thanks to data analysis and sometimes artifi-

cial intelligence, some organizations have become incredibly sophisticated in their ability to understand their surroundings and know where their goods are. However, this secure network construction is incredibly expensive and the acceptance of the partners as to the security compliance standards imposed by this type of digital system is difficult.

Today, the new challenges of data protection target flow transformation information to ports and terminals. This is the type of challenge that TradeLens wants to take up, an emerging IBM venture that works in conjunction with the transportation juggernaut Maersk. The solution provided by TradeLens is that of advanced visibility from a platform promoting several aspects of the supply chain, including optimization ports and terminals. Basically, the information will be structured once received by the port in real time. This will allow the entity to continue to receive updates from dynamically on the status of the reservation, arrival times, estimates as well as modifications to the transportation plan. Due to the number of different entities involved in the transportation of goods for go to the other side of the world, there is an inherent cost complexity, imposed by the new technologies. Current systems for communicating and maintaining the visibility of the freight are not sufficient to ensure the complex supply chains that we need today. Take as an example the geolocation of container ships between two ports that assist navigation, provide an estimate of the arrival time, and prevent collisions between ships.

Navigation data systems are provided by satellites via the GPS system. These can also be subject to cyberattacks or serve as espionage. Economical by the data transiting via the satellite used. The anticipation of a journey, identity theft, degradation or blocking of positioning services, are palpable risks in this sector. This is partly why each major player has developed its own satellites with geolocation systems, for example.

New solutions, particularly involving geolocation, provide a sharing of secure data, in a structured way and allow complete visibility of the journey of end-to-end container across all stakeholders involved. The need increasing number of tracking devices such as those used for traceability or GPS applied to transport and logistics, highlights a real need for data protection.

2. The challenge of data protection in the maritime transport

In order to cover the risks and ensure a significant cyber-resilience of the vessels, it should be determined whether these environments include

specificities and which ones. The potential cyber risks for a ship are of several orders due to the different subsets that make up its information system:

• a ship foremost a set of on-board industrial systems, an operational network that moves with all the risks and specific constraints;

• a ship is a large flow of data processed by a conventional computer system of greater or lesser size depending on the context, on cruise ships, real floating cities, they are extremely large, complex and include public networks;

• a ship is a set of specific operational systems used for identification, navigation, positioning (AIS,RADAR, GNSS,…). data mining in the shipping industry have a positive impact on the safety and quality of service for customers

The arrival of the digital transformation driving a critical change in the volume and importance of the data processed for and by the ship cause of the exponential growth of digital data, the need of management and security of these becomes the first challenge of the maritime activities.

This is a strategic issue, including with regard to concerns commercial ships transporting goods or passengers.

Management of data in the broad sense is therefore at the center of maritime activities and naval defence. This requires the establishment of a real policy of data security, integrating the detection of intrusion attempts, malicious code, data leaks and suspicious behavior.

2.1. Blockchain as a response to data protection problem

The need of data security is a priority in the strategic development of companies. In order to guard against the risk of data corruption, some companies in the transport sector have turned towards a recent technological alternative as the blochain. The technology of the blochain was a great solution in the supply chain for helping shippers, carriers, brokers, financial agents, banks, customs offices, and other stakeholders (Zhou, 2021).

The blockchain can be defined as a storage and transmission of information, transparent, secure, and operating without a central body of control. In other words, it is a database made up of blocks, each having access to part of the information. These nodes are interconnected, thus forming chain. This chain makes it possible to guarantee the security of the system and therefore the confidentiality and data immutability; it is a network of trust.

Still recent, this technology is little known to small players who are not familiar with data protection issues, but it is increasingly becoming a major asset for large companies.

2.2. A secure and efficient system

In maritime transport, the supplier will transmit the information concerning his origins to the carrier link in the chain (the carrier). Assuming that the message was transmitted using a ten-node blockchain, the latter will receive ten messages. If one of the users has attempted to modify the information, the carrier will receive nine correct messages and one incorrect message. It will be easy to know which one is wrong, because each message transmitted contains the history of changes made to the initial information.

In addition, the data transmitted in the blockchain is encrypted and users must use, in order to be able to transmit the data, decryption keys which are specific to them. It is not therefore not possible to usurp the identity of a block, without having the decryption keys.

In addition to the better data security it offers, the blockchain allows the company a significant productivity gain. By removing the intermediaries, normally present in the process of transmitting information, the latter circulates more freely and more quickly.

In addition, it is possible to automate the management of nodes. Thus, on criteria objectives, an algorithm can automatically verify the veracity of the information transmitted.

Human intervention is then completely eliminated, erasing the risk of alteration of the given by man. This automation reduces the processing time of the information of several days in the event that an intermediary verifies the information a few time.

The use of a blockchain system has many advantages and its variation in the transmission of data improves the productivity of the company and better protect the transmitted information. This technology could therefore be used in the sector transport in order to reduce processing times between actors and improve trust in a sector in which intermediaries are very numerous.

3. The case of shipping industry

3.1. The role of shipbuilding in maritime cybersecurity

Those who build and equip ships have the heavy responsibility for integrating the cyber spatial dimension into the design, construction and maintenance throughout their life cycle.

The cybersecurity of maritime spaces is nourished by what is played out «at land», at sea and on board. If the consideration of one of the three dimensions is insufficient, the result obtained will be below expectations and the permeability to likely attacks.

For example, on board ships, it necessary take into account the digitalization to develop first a digital approach to meet the challenges of embedded cybersecurity.

3.2. Shipbuilding at the center of the challenges cybersecurity

The shipping industry will be in front of several challenges such as data processing, reliability, and data security. Also, Various regulations rely on ship data Zaman et al., 2017.

The shipbuilding industry sees its action evolve gradually, as the mentality and the perception of an acceleration of cyber threats. The ship is no longer isolated and ransomware on board can infect the entire chain logistics of a shipping company, and its customers.

The answers are multiple and appropriate with the challenges.

The cost of an attack becomes prohibitive and the naval industry has resolutely focused on sector strategies that allow the State and the private sector to federate their initiatives.

Cybersecurity is one of the sector projects for the security industry.

At the same time, the marine industry sector wishes to develop its strategy around the digitization of the shipyard, its development in a 4.0 perspective and the design of «smart» solutions for new generation vessels.

Conclusion

The standardization of maritime transport is a key factor in the competitiveness of ports. It is now based on the capacity of their systems information to automate and process voluminous flows of information related goods, passengers and ships. The shipping Companies need to ensure the cybersecurity measures to protect the data in their own systems and make sure that the data is sent and received in a secure way. The objective of cybersecurity is to limit risks and protect the park attackers with malicious intent. Security information technology, which consists of maintaining the confidentiality, integrity and data availability, is a subset of cybersecurity

References

1. Ibna Zaman, Kayvan Pazouki, Rose Norman, Shervin Younessi, Shirley Coleman, Challenges and Opportunities of Big Data Analytics for Upcoming Regulations and Future Transformation of the Shipping Industry, Procedia Engineering, Volume 194, 2017, Pages 537-544, ISSN 1877-7058, https://doi.org/10.1016/j.proeng.2017.08.182.

2. Li, L., Zhou, H. A survey of blockchain with applications in maritime and shipping industry. Inf Syst E-Bus Manage 19, 789—807 (2021). https://doi.org/10.1007/s10257-020-00480-6.
3. Jabbar K, Bjørn P (2018) Infrastructural grind: introducing blockchain technology in the shipping domain. In: Proceedings of the 2018 ACM conference on supporting groupwork. P. 297—308.
4. Jain P (2018) Improving the process of container shipping using blockchain. Master's thesis. Massachusetts Institute of Technology.
5. Jović M, Filipović M, Tijan E, Jardas M (2019) A review of blockchain technology implementation in shipping industry. Pomorstvo 33:140—148.

Правкин Сергей Алексеевич,
кандидат юридических наук, доцент, доцент кафедры «Административное право, экологическое право, информационное право» Юридического института Российского университета транспорта (МИИТ)

Регулирование цифровых прав на финансовом рынке

Аннотация. Вследствие развития технологий на финансовом рынке происходит цифровая его трансформация, внедряются механизмы искусственного интеллекта, машинного обучения, аналитики больших данных и распределенного реестра. Появляются цифровые финансы и цифровые финансовые активы, которые имеют способность к устойчивому спросу. Цель статьи состоит в выявлении правовых средств регулирования финансового рынка в новых условиях осуществления и защиты цифровых прав.

Ключевые слова: финансовый рынок; цифровые права; финтех; блокчейн; цифровые финансовые активы

Pravkin A. Sergey
Candidate of Law, Associate Professor, Associate Professor of Administrative Law, ecological right, information right» Russian University of Transport

Regulation of digital rights in the financial market

Abstract. Due to the development of technologies in the financial market, its digital transformation is taking place, mechanisms of artificial intelligence, machine

learning, big data analytics and distributed registry are being introduced. Digital finance and digital financial assets are emerging that have the ability to sustain demand. The purpose of the article is to identify legal means of regulating the financial market in new conditions, the implementation and protection of digital rights.

Keywords: financial market; digital rights; fintech; blockchain; digital financial assets.

Спецификой российского финансового рынка является стремление населения обслуживаться не только в кредитных организациях, но и в организациях небанковского профиля. Кредитные организации в Российской Федерации предоставляют помимо банковского обслуживания услуги на фондовом рынке. Большую роль имеет у населения востребованность банковских вкладов, хотя уровень накоплений населения в целом оказывает сдерживающее влияние на развитие финансового рынка. У населения меньшим уровнем спроса обладают некредитные продукты. На финансовом рынке активно используются стартапы и краудфандинговые платформы, в которых все более принимает участие население.

В последнее время развиваются инструменты финтеха, который включает в себя такие направления, как развитие финансовых платформ, появление и стремительное развитие криптовалют, платежных систем, интернет-банкинга.

Федеральный закон от 02.08.2019 № 259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» устанавливает оборот утилитарных цифровых прав.

Базовым актом при осуществлении деятельности с использованием инвестиционных платформ выступает договор об оказании услуг. Возможность использования инвестиционной платформы возникает у оператора, когда он открывает доступ инвестору. Способами привлечения инвестиций выступают: предоставление займов, приобретение эмиссионных ценных бумаг, утилитарных цифровых прав и цифровых финансовых активов. «Развитие цифровых технологий приводит также к постоянному размыванию границ финансовой отрасли в институциональном выражении. Банки и другие финансовые организации начинают кооперироваться с финтех-компаниями, все больше

финансовых сервисов предоставляют отнюдь не финансовые организации» [3, стр.75].

Для того чтобы инвестировать с использованием инвестиционной платформы, не надо признания физического лица индивидуальным предпринимателем.

Утилитарные цифровые права означают: право требовать передачи вещей, выполнения работ, оказания услуг, исключительных прав. Права признаваться утилитарными должны возникнуть на инвестиционной платформе. Всякая передача утилитарного права осуществляется по правилам инвестиционной платформы. Допускается просто ознакомление с содержанием права без заключения договора. Сделки возможны, если эти права возникли в инвестиционной платформе. Всякий переход, возникновение и прекращение права в ней отражается. Государственная регистрация прав не требуется.

Депозитарий может учитывать эти права и цифровые финансовые активы в соответствии с Федеральным законом от 22.04.1996 № 39-ФЗ «О рынке ценных бумаг». Цифровые права могут одновременно содержать утилитарные цифровые права и цифровые финансовые активы.

Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» учитывает их вместе с утилитарными цифровыми правами. Владельца цифрового финансового актива удостоверяет цифровое свидетельство как неэмиссионная бездокументарная ценная бумага с уникальным номером.

Переход прав на утилитарные права осуществляется в соответствии с Федеральным законом «О рынке ценных бумаг».

Инвестиционная платформа сделки совершает в автоматическом режиме по принципу «оферта—акцепт». Права инвестора удостоверяются выпиской из реестра.

Статья 141.1 ГК РФ отнесла цифровые права к объектам гражданских прав. Права являются цифровыми, если они созданы по правилам информационной системы, и осуществление этих прав осуществляется по правила информационной системы без обращения к третьему лицу. Обладателем права является лицо, приобретшее его по правилам информационной системы (например, блокчейн). При этом ес-

ли цифровое право переходит по сделке, не требуется согласия лица, обязанного по цифровому праву.

Важным направлением цифровизации является обеспечение правовых условий внедрения и использования инновационных технологий на финансовом рынке. Остаются проблемы информационной безопасности в отношении криптовалюты. Что касается цифровой валюты, ее регулирование нашло отражение в Федеральном законе от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», вступившем в силу с 1 января 2021 г. Впервые в истории России были закреплены понятия «цифровые финансовые активы» и «цифровая валюта». Оператор информационной системы регулирует их оборот. Цифровая валюта обладает средством накопления и осуществления инвестиций.

Банк России является эмитентом цифровой валюты — цифрового рубля, который будет зачисляться на виртуальные кошельки владельцев. Теперь рубль существует в трех формах: наличная, безналичная, цифровая. Цифровые рубли наделяются качеством наличных денежных знаков, имея свой собственный цифровой код, и являются настоящим средством платежа. Но для полноценного использования цифрового рубля должна быть создана совершенная правовая база. Возможно, потребуется детальный нормативный акт, регулирующий применение национальной цифровой валюты. Необходимо разработать меры налоговой, административной и уголовной ответственности в отношении нарушений использования цифровой валюты. Должна быть обеспечена защита прав участников отношений, связанных с применением цифрового рубля.

Большую роль имеют финансовые организации в сфере обращения финансовых инструментов. На определение сущности финансовой организации влияет характер финансового рынка в стране. Финансовые организации являются посредниками на финансовых рынках.

Важным направлением деятельности финансовой организации являются действия с финансовыми инструментами. В условиях трансформации финансового рынка классические элементы финансирования уступают место новым инструментам, связанным с цифровыми платформами, с размещением производных финансовых инструментов. Постепенно уменьшается количество посредников на финансовом рынке.

В своем сформировавшемся виде финансовый рынок представлен институциональными организациями. На финансовом рынке преобладают кредитные организации и соответственно активы кредитных организаций преобладают над иными активами

Развитие цифровизации финансового рынка связано с его детальным организационно-правовым регулированием. Цифровизация приводит к выпуску новых активов, которая стала причиной трансформации многих отраслей экономики. Банки вышли на новые технологии взаимодействия с потребителями, которые диктуют спрос на новые финансовые продукты. Новой сферой взаимодействия на рынке стал финтех. Важной инновацией финтеха стало появление криптовалют.

Модели взаимодействия финтех-компаний с банками отличаются многообразием, включая взаимодействие внутри банковских холдингов.

Новые платформенные решения и сервисы оказывают влияние на банковский сектор России. Финансовые сервисы становятся доступнее традиционных банковских продуктов на основе применения блокчейн, мобильных платежей, больших данных, машинного обучения. Финтех-компании, кооперируясь с банками, создают эффект банковских холдингов. В структуре банковского холдинга находится более одной кредитной организации. Большое место в современной банковской деятельности имеет процесс управления личными данными. Появляется новый вид активов — криптоактивы и финансовые инструменты — криптоваютные деривативы. Но в целом Банк России не допускает к обращению криптовалют из за высоких рисков.

Требуется развитие специального законодательства, регулирующего развитие рынка производных финансовых инструментов. Необходима защита прав инвесторов, в том числе при заключении и исполнении сделок с криптовалютными деривативами.

Большое место по-прежнему на рынке играют банковские холдинги, совокупная доля кредитных организаций в них должна быть не менее 40%. При этом финтех-компании взаимодействуют друг с другом, банками. «В результате на рынке появляются финансово-промышленные холдинги, осуществляющие банковскую, инвестиционную, страховую, лизинговую деятельность, деятельность профессиональных участников рынка ценных бумаг, а также иную, в том

числе нефинансовую (торговую, промышленную), деятельность» [2, стр. 90]

Финансовые системы континентального и англо-американского типа за счет использования цифровых финансовых активов постепенно сближаются. Современная финансовая система становится децентрализованной, основанной «на технологиях распределенных реестров и блокчейна … развитие финансового рынка неразрывно связано с централизованными технологиями искусственного интеллекта и применения программных интерфейсов, аналитикой больших данных и машинного обучения». [1, стр. 1315]

Таким образом, применение цифровых финансов очень важно в современных условиях для устойчивого развития финансового рынка. А его правовое регулирование требует дальнейшей детализации.

Правовое регулирование цифровых прав требует дальнейшего развития. Преимуществом цифровых прав является возможность их реализации в информационной платформе в любом количестве. Преимущество, которое создают банки, заключается в созданной клиентской базе, что создает основы цифровизации финансовых услуг, связанных с аналитикой больших данных. Это создает условия для институциональных организаций финансового рынка к сохранению своих лидирующих позиций, по реализации цифровых прав, цифровых активов и валюты. Но для полноценного использования цифровой валюты должна быть создана совершенная правовая база.

Литература

1. Андрюшин, С. А. Финансовые рынки, технологические инновации и финансовая стабильность: риски и проблемы регулирования / С. А. Андрюшин, В. В. // Кузнецова Актуальные проблемы экономики и права. 2019. Т. 13. № 3.
2. Иванова, С. П. Актуальные вопросы деятельности интегрированных банковских структур / С. П. Иванова, К. В. Садыкова // Вестник РЭУ им. Г. В. Плеханова. 2018. № 1 (97).
3. Марамыгин, М. С. Цифровая трансформация российского рынка финансовых услуг: тенденции и особенности / М. С. Марамыгин, Г. В. Чернова, Л. Г. Решетникова // Управленец. 2019. Т. 10. № 3.

Dr Nadjat Wassila Belghanami

Information network Security between Risk and reality: the case of Algeria, the justice sector

Abstract. In this research paper we address the problematic of information security and its importance as the system in various fields by referring to the most famous definitions of it as a concept and as the process in light of the development of information networks and cybersecurity, which leads to the favorites strategies and plans that enable to ensure the availability of information to the people referred to them as a preventive application without any threats and in preparation for all emergencies in an easy, safe and at the same time from all information crimes, which we summarized in this research in its first part. In the second aspect of our research, we presented the case of Algeria with reference to the justice system and the confrontations it presented in order to ensure cyber security while praising the effective role of the security authorities. Accordingly, we presented a number of statistics, the most important of which are 8000 cyber crimes during the year 2020, where the General Directorate of National Security recorded a number Record high from 500 crimes in 2015 to 5200 cases. related to cybercrime in 2020, while the National Gendarmerie Command recorded 1,362 cybercrime involving 1,028 people during 2020.

Keywords: Information ; Network ;Security ; System. National security.

Introduction

Information Security is not a new invention, but man has always been keen to benefit from the information he has and does not disclose it except to those who trust him or can benefit from this information, but with the development of information technology and the huge and steady increase in the quantities of information and data available in the world and the emergence of information networks And the databases in which information is stored, it has become necessary to organize access to this information by specifying who is authorized to access this information and how and the level of access to it.Where the information security strategy aims to achieve and implement the specific duties of users and administrators by

restricting their access and ensuring emergency preparedness to make information available to its authorized persons in an easy and secure manner at the same time.

First: Defining the Security of the Information Network and its Importance : We can define it:

- It is a set of procedures through which it is possible to provide maximum protection for information and data in networks from all risks that threaten them, by providing the necessary tools and means to protect information from internal or external risks.
- A set of standards that prevent information stored in networks from reaching people who are not authorized to obtain it.

Why Information Network Security?

It is obvious that the importance of information has a degree of protection that varies in importance with the importance of the information stored in these networks.

- The first case It was recorded in 2003 when an employee of a Russian company hacked the company's information network, and he modified his monthly salary and a group of his colleagues increased salaries by a certain percentage, which led to financial losses for the company for Several months because this hack was not discovered.
- The second case .the hacking of the information network of the US Department of Defense, which has happened many times in recent years, and we can see the extent of the losses represented by such security breaches of information networks, whether these losses are financial, as in the case of companies, or information and intelligence losses that are inestimable and can affect independence of large countries such as America.

From here it becomes clear the paramount importance of sum security information networks, and we up some of the reasons that led to the recent interest in the topic of "information network security" in the following points:

1. Technological Progress Just as the tremendous developments in the field of information and communication technology led to a major boom in the means of communication and information network technology and storage, at the same time it led to the presence of minds working on finding security holes in these networks and exploiting them badly in the so-called "ugly face of technology".
2. Childishness and Impulsivity where some personalities have childish and impulsive motives to obtain information in ways just to feel the

euphoria of victory and break the barriers of confidentiality and security imposed on information networks.

3. The Spread of Information Crimes In the recent period, the obsession with cybercrime has prevailed from people, organizations, and competing companies, and ends with countries, in what is known as "information war".

Do all information networks need to be secured?

Certainly, this depends on the information and data that these networks contain and the nature of the users in them, as well as the desire of the party responsible for these networks to protect the resources and properties of these networks or not, but in general there must be some kind of protection, even if at least simple protection for these networks, for example On the other hand, there are types of information networks that must have a security and protection system, and they cannot be left without security, due to the great importance they represent, both in terms of the level of data and information they carry or on The level of users of these networks, and examples of these networks are the following.

- Intranetslan. Such as Small business networks schools or hospitals.
- Wide networks WAN. Like international networks that connect parts of countries.
- Private networksintranet.

It came to the point that the US government launched in February 2003 a special initiative concerned with protecting the information field, which it called (Cyber Space, and many of the submitted countries have begun to move in the same direction in order to find solutions that work to reduce the phenomenon of cybercrime.

Second: Defining Information Crimes and Their Classifications :

It can be said that it is "a comprehensive expression that refers to a crime related to the use of an information and communication technology means for the purpose of deceiving or misleading others, or in order to achieve a specific goal or profit.».

Crimes that are committed through the use of information technology are classified into several sections, and each section specializes in a specific type of crime that can be committed, as follows:

a. Crimes aiming to publish information:

In this type ,confidential information obtained illegally through penetration into information networks is published and this information is pub-

lished publicly, for example, publishing Debit or Credit Card information, Bank Account Numbers, and also publishing intelligence information related to countries or People like what happened in the CIA hack CIA.

b. Crimes aimed at spreading rumors

Here , false and incorrect information related to people, beliefs, or countries are published ,as well as spreading rumors about some things and causing confusion in societies.

c. Electronic counterfeiting crimes

Here the means of technology are used in forgery operations with the aim of achieving a specific goal ,such as forging credit cards, passports and other official papers, and fake bank transfers from one account to another by penetrating bank networks fall under It.

d. Information technology crimes

The most important example is the piracy operations that occur on the original computer programs, copies of which are made to be sold in the market instead of the original copies ,such as expensive drivers or application programs, which are imitated by professional hackers in this field

Third: The components of information network security and the motives for attacking it:

When we talk about the topic of «information security» and information networks, the first thing that comes to mind is how to maintain the confidentiality of information, and when we mention information crimes, we mean that this information has been leaked, which means that A violation of this confidentiality has occurred, so what are the components of this system we call information security or information network security.Where specialists see that information security is a process that is not simple, but rather a complex process consisting of three components

- First : Confidentiality of Information Data Confidentiality
- This aspect includes the procedures and measures necessary to prevent unauthorized access to information, whether confidential or sensitive .Of course, the degree of this confidentiality and the type of information varies from place to place according to the policy followed in the same place .Examples of this information that must be kept confidential are .personal information of individuals, the financial budget of companies before Announcement, military information and data of the armies and military sites in the country.
- Second : Information Safety) Data Integrity

- In this aspect, the greatest concern is not to preserve the confidentiality of information, but rather to preserve the integrity of this information from forgery and alteration after it has been publicly announced . Insured against alteration and forgery in it by deleting names and putting other names , which causes legal problems for institutions, and also for financial information by changing a sum of money from 100 to 1000000 which results in huge losses in money.

• Third :Ensuring Access To Information Availability

The objective of the information industry is to deliver information and data to the right people at the right time , and therefore maintain the confidentiality of information ,ensuring its safety and not changing it does not mean anything if authorized or authorized persons cannot access it , and Here comes the importance of the third aspect of Aspects or components of information security, which is to ensure that information reaches the persons authorized to access it by providing safe and fast channels and means to obtain that information . Devices for storing and destroying, or at least sabotaging, information

Why do Vandals or Hackers do Operations like Hacking Information Networks?

• First : The Existence of a Motive

This motive may be obtaining funds, intentional sabotage, or even just proving the capabilities of the hacker and proving his ability to penetrate a particular site as a kind of technical challenge.In some cases, the situation has political motives or some of the intellectual, ideological and political affiliations of individuals and countries.

• Second : The Existence of the Plan

And we mean that the attacker will not be able to implement his goals without having a solid plan that allows him to launch his attacks on the site and hack it and do what he wants.

• Third, There Are Loopholes

Any weaknesses in the information system as a whole or in the information network or the devices that operate within the network or even the software that is made available on the information network, and these gaps can be in the design of the information network or in the configuration of the network or the software or databases contained in the network.

Fourth: Sources of Danger to Information Networks

After all of the above-mentioned dangers facing information networks and their protection systems, we would like here to list the sources through which a threat or penetration into information networks can be formed..

First, the Internal Danger

And they are the attackers from within the scope of the information network, and they are individuals or workers who belong to the same target party, and perhaps this type of danger is more deadly and dangerous than the danger of external enemies ,and this represents the Greater threat to institutions and is difficult to detect in many cases, especially if the person The attacker has access to the information network system, so he does not face any difficulty in the security and confidentiality operations on the network, and he can even blur the features of the attack and erase the traces of his entry easily, and the most important aspects of internal dangers can be summarized as follows

A — Penetration of the internal networks of the enterprises.

B — Hacking information systems by stealing, switching, changing or deleting.

C — Finding and creating loopholes in the network security system.

D — Changing the configuration of the information network system.

A report issued in the United States of America in 2003 showed that 36% of the entities consider that internal users are more dangerous to the information systems available within these institutions than the external threat.

Among the most important motives for attacking the party he works for are

1-Cases of Dissatisfaction*:*

Material or career, revenge against a manager, or other personal reasons.

2-Self-Proof

Just to satisfy his ego that he is capable of challenge, or fame to promote the spread of jailbreaking software

3-Material Benefit

In cases of paid competitors, the hack may be for the purpose of harm or loss by bribery of some people for the purpose of leaking information in exchange for sums of money.

• Second, the External Danger

They are the people who make hacking attempts from outside the institutions by some Internet hackers such as banks and other institutions that have information networks with a high degree of confidentiality and security.

- Third: The Risk of Interference
- This means the factors that affect the sending and receiving of data and information through information networks through some equipment or programs that work on it .that affects transmitting and receiving towers, especially in networks that depend on optical fibers and wireless communication systems, and in other times, "jamming" is the result of a deliberate and intentional action by certain parties, by monitoring information by signals similar to the same frequency bands used in transmissions through the network .Mother.
- Fourth: The Risk of Poor Design
- Technical errors in the design of networks or the systems on which these networks operate, and these unintended errors are the weak point in the information network, through which the security and integrity of information can be threatened.
- Fifth: The Risk of Misuse
- Whenever the human element is trained and qualified in a scientific manner and sufficiently, that is one of the reasons for protecting information networks ,.so that it can be a window to create ports in the firewall.
- Sixth: Intruders Hackers

The hacker is the person who creates and modifies software and computer hardware .They try to break into it, and they do not necessarily have the intention of committing a crime or even A misdemeanor , but their success in penetration is considered a success of their abilities and skill . However, the law considered them intruders who managed to enter a hypothetical place where they should not be.

- Seventh: Viruses
- It is an external program that is deliberately manufactured with the purpose of changing the properties of the files that it infects in order to carry out some commands either by removing, modifying or sabotaging and similar operations: stealing important data, and it is written in a certain way..A virus is one of the malicious or intrusive programs, and other intrusive programs are called worms, trojans, adware or spyware .Malicious programs can only be a nuisance by affecting and slowing down computer usage, causing interruptions and malfunctions at regular times and affecting various programs and documents that may be desired. The user can access it, and the more dangerous malicious programs can become a secu-

rity problem by Obtaining information such as personal from your emails and other data stored in your device through the information network.

Reading in the Case of Algeria at the Level of the Justice Sector:

The specialized pole in cybercrime was established in the justice sector, along with the criminal pole specialized in combating financial and economic crimes, to enhance the treatment of cybercrime currently before justice . Where this specialized national pole contributions to combating cybercrime, which has become more dangerous than traditional crimes, as it has evolved from threats, defamation and extortion of people to compromising the security of the Algerian state, and therefore, it has become imperative for all concerned interests to define mechanisms, tasks and powers for each party.

In the context, the security services warned of the rise in cybercrime in Algeria, as they confirmed that the crime actually moved from the real world to the virtual cross-border due to the speed of its implementation, as the gender and police services registered according to the numbers.

Nearly 8,000 cyber crimes during the year 2020, where the General Directorate of National Security recorded a record high, ie from 500 crimes in 2015 to 5,200 cases related to cybercrime in 2020, while the National Gendarmerie Command recorded 1,362 cyber crimes involving 1,028 people during 2020.

The process of analyzing the data for the recorded crimes showed that defamation and insult through the virtual space took the lead with a rate of more than 55% , followed by crimes against public security, then acts affecting private life and disclosure of secrets, and finally blackmail, fraud, fraud, sexual exploitation and acts contrary to public morals and similar issues.

Specialists in the fight against cybercrime confirmed that, according to the latest report of the "Datareportal" website " ,DATAREPORTAL "A specialist in statistics related to the fixed and mobile internet in the world, the number of internet users in Algeria increased by 3.6 millions in a year, moving to 26.35 millions users.

The report highlighted that Algeria counted as of January 31, 26.35 millions users, which represents an estimated increase of 3.6 millions users since January 2020. The same report also included statistics related to social media and e-commerce, in addition to trends and information regarding the situation of digitization in the world .Users of social networking sites "Facebook, Twitter, YouTube, Instagram" increased in Algeria until

January 31, 2021, where about 3 millions new users of social networking sites were registered, an increase of 13.6% percent within one year, which made the total number of users of these applications jump to 25 millions, or 56.5% of the total population, where the majority of users of social networking sites use smartphones and electronic panels to connect to these networks.

For its part, the "Kaspersky" company, which specializes in fighting cybercrime, thwarted 95,000 electronic attacks against Algeria during the year 2020, as the year 2018 ranked first in the Arab world and the 14th globally in terms of countries most vulnerable to electronic attacks.

And the top five places in the countries with the highest levels of crime in the Middle East were for Libya, which ranked first with a score of 57.81 to be ranked 22 globally after Tanzania and before Mongolia, which ranked 23.

Libya was followed by the Republic of Algeria, which ranked second with a score of 57.58, and Egypt in third place with a score of 56.53, Somalia in fourth place with a score of 55.72, then Syria in fifth place with a score of 54.73, noting that not all Arab countries were mentioned in the index .Like what is indicated below.

Levels of crime in the Middle East& Arab countries	Countries	evaluation in the Crime Index	Ranking internationally
1	Libya	57.81	22
2	Algeria	57.58	24
3	Egypt	56.53	28
4	Somalia	55.72	29
5	Syria	54.73	31
6	Iran	52.37	36
7	Iraq	51.51	37
8	Lebanon	50.56	39
9	Morocco	50.28	40
10	Jordan	46.89	52
11	Turkey	39.43	71

Conclusion

Cybercrime over the Internet has become a global phenomenon, and most of its victims, whether they are individuals or productive sectors,

even intangible human values have not been spared .The perpetrators of these crimes are distinguished by high culture and brilliant intelligence, and they are called white-collar;Because of their experience in dealing with computers, they also possess the characteristic of patience and passion to reach their goals.Finally, information and communication networks can be considered a blessing and a curse, a double-edged sword, as they are security systems

Information networks require the protection of the assets and resources of information systems in legitimate ways, as well as the regulation of relationships and communications within information networks without affecting the efficiency of the system or the ability of users to perform.Therefore, it is better to rely on rules (data, information, knowledge ...) and other safe means as legal and backup copies.

Reference

1. Kamal Mahmoud Jabra,(2015), Insurance and Risk Management, Publishing House: Al-Manhal.
2. Abdelali Derby,(2012), Cybercrime, Publishing House: Al-Manhal.
3. Marwa Zine El Abidine Saleh, (2016),the international legal protection of personal data online between international international law and national law Publishing house: Al-Manhal.
4. Muhammad Ali Skiker,(2010),Information crime and how to address it, publishing house .ktab INC.
5. Muhammad Sultan Al Ulama,(2003) , Internet crimes and counting them, The Arab Journal for Security Studies and Training, Vol18n number 26October.
6. Yassin Sheikh,(2010), Information Systems Security and Control (Control), Publishing House .Informatics Engineering, University of Damascus.
7. Abdul Karim Al-Radaydah,(2013),New crimes and the strategy to confront them, Publishing House: Al-Manhal.
8. Kamal Mahmoud Jabra,(2015), Insurance and Risk Management, Publishing House: Al-Manhal.

Смирнова Вера Владимировна,
кандидат юридических наук, доцент, доцент кафедры «Административное право, экологическое право, информационное право» Юридического института Российского университета транспорта

Правовое регулирование мультимодальной перевозки груза в условиях цифровизации

Аннотация. Статья посвящена правовому регулированию мультимодальной перевозке груза в России с использованием цифровых технологий. Указывается на необходимость применения унифицированного электронного документооборота, которое требует нормативного закрепления. Рассмотрено применение цифровых технологий при мультимодальной перевозке, которые затрагивают информационное сопровождение относительно тарифов, маршрутов, статуса и срока доставки груза, технического сопровождения, обслуживания транспорта, оказании онлайн-услуг по оформлению страховки и таможенных платежей. При этом встает проблема недостаточного регулирования данных правоотношений, которая может привести к негативным последствиям.

Ключевые слова: мультимодальная перевозка; груз; транспорт; цифровизация; информационные технологии; электронный документооборот.

Vera V. Smirnova,
PhD in Law, Associate Professor, Associate Professor of the Chair “Administrative Law, Environmental Law, Information Law” of the Law Institute of Russian University of Transport

Legal regulation of multimodal transportation of goods in the context of digitalization

Abstract. The article is devoted to the legal regulation of multimodal transportation of goods in Russia using digital technologies. It is indicated the need to use a unified electronic document management, which requires regulatory consolidation. The use of digital technologies in multimodal transportation is considered, which affect information support regarding tariffs, routes, status and delivery time of cargo, technical support, transport services, the provision of online services for obtaining insurance and customs payments. At the same time, the problem of insufficient

regulation of these legal relations arises, which can lead to negative consequences.

Keywords: multimodal transportation; cargo; transport; digitalization; information technology; electronic document management.

В современном мире мультимодальные перевозки стали наиболее востребованы, особенно из-за действия ограничительных мер по предупреждению распространения новой коронавирусной инфекции во всем мире. Концепция перевозок от двери до двери позволяет минимизировать контакты, а также оптимизировать собственную логистику внутри компаний. Мультимодальные перевозки являются эффективным сочетанием железнодорожного, морского, воздушного и автомобильного транспорта, позволяющие оперативно доставлять грузы как внутри страны, так и по всему миру. Такие перевозки позволяет оперативно и экономично доставлять грузы по всему миру.

При мультимодальных перевозках учитывается специфика перевозимого груза и разрабатывается их оптимальная доставка с использованием преимущества того или иного вида транспорта. При мультимодальных перевозках сокращаютсякак время доставки груза, так и финансовые затраты. Данная перевозка наиболее экономически выгодна.

Многие страны, в том числе и Российская Федерация движутся по пути развития законодательства в области мультимодальных перевозок грузов. Однако на сегодняшний день существует множество проблем, связанных с мультимодальными перевозками грузов как технических, так и правовых.

Понятие мультимодальной перевозки было сформулировано в Словаре терминов, используемых в комбинированной перевозке или имеющих отношение к этим перевозкам, изданном Европейской экономической комиссией ООН (*United Nations Economic Commission for Europe* (*UNECE*). Под мультимодальной перевозкой понималась перевозка двумя и более видами транспорта» [7].

Правовое регулирование мультимодальных перевозок начинается с принятием Токийских правил Международным морским комитетом в 1969 г. А в 1973 г. на основе Токийских правил Международной торговой палатой были разработаны правила, регламентирующие документальное оформление такой перевозки. Понятие мультимодаль-

ной перевозки было предложено в Конвенции ООН о международных смешанных перевозках грузов 1980 г., в ней отмечалось, что: «международная смешанная перевозка означает перевозку грузов по меньшей мере двумя разными видами транспорта на основании договора смешанной перевозки из места в одной стране, где грузы поступают в ведение оператора смешанной перевозки, до обусловленного места доставки в другой стране». Кроме того, было дано пояснение операции по вывозу и доставке грузов, осуществляемые во исполнение договора перевозки только одним видом транспорта — такая операция не считается международной смешанной перевозкой. Однако данная Конвенция в силу не вступила.

Правила ЮНКТАД определяют договор смешанной перевозки как договор перевозки грузов по меньшей мере двумя различными видами транспорта. Лицо, заключившее такой договор и взявшее на себя ответственность за его осуществление в качестве перевозчика, называется оператором смешанной перевозки.

Затем в 2008 г. принята Конвенция о договорах полностью или частично морской международной перевозки грузов. «В ней затрагиваются не только морские перевозки, но и смешанные перевозки наземным и морским транспортом. Данная конвенция может выступать альтернативой для участников мультимодальной перевозки» [5, стр. 143].

Что касается самого термина «мультимодальная перевозка», то его закрепление отсутствует в российском законодательстве. Законодатель отождествляет «мультимодальные перевозки» с «перевозками в прямом смешанном сообщении» и «комбинированными перевозками». В ст. 788 Гражданского кодекса РФ закреплено, что прямое смешанное сообщение — это возможность перемещения грузов, пассажиров и багажа при помощи различных транспортных организаций, принадлежащих к разным видам транспорта по одному перевозочному документу. Соответствующие нормы и понятие содержатся в отдельных нормативных актах транспортного законодательства. Например, гл. 5 Устава железнодорожного транспорта РФ и гл. 14 Кодекса внутреннего водного транспорта РФ посвящена перевозке грузов в прямом смешанном сообщении. Но специальный закон отсутствует.

В 2004 г. был принят ГОСТ Р 52297-2004, в котором под мультимодальной перевозкой закреплялась перевозка, при которой один

экспедитор организует и осуществляет доставку и перевозку груза от места отправления до места назначения транспортом различных видов, при этом он принимает ответственность за все расстояние перевозки и оформляет единый транспортный документ на перевозку груза.

В научной российской литературе даются следующие определения данной перевозки. С. В. Милославская и К. И. Плужников определяют мультимодальную перевозку как перевозку, «в которой доставка груза от отправителя к получателю осуществляется как минимум двумя различными видами транспорта (автомобильным, железнодорожным, морским, воздушным) под ответственностью одного перевозчика, по единому транспортному документу, подтверждающему заключение договора перевозки», и оплачиваемую «по единой сквозной тарифной ставке» [4, стр. 13]. М. А. Кузьмина, С. Л. Надирян, Е. О. Чернобривец представляют мультимодальную перевозку, осуществляемую как минимум двумя видами транспорта [3, стр. 68]. По мнению И. А. Кругловой, А. Н. Кириллова, мультимодальная перевозка представляет собой перевозку груза, выполняемую по одному договору и предполагающую применение разных видов транспорта: автомобильного, морского, железнодорожного и воздушного, охватывая перегрузки на различных терминалах [2, стр. 124].

В принятой Транспортной стратегии Российской Федерации на период до 2030 года с прогнозом на период до 2035 года поставлены ряд задач при осуществлении перевозок в мультимодальным сообщении. Так, для повышения уровня взаимодействия всех видов транспорта необходимо создание органов по координации работы всех видов транспорта и обеспечению их рационального взаимодействия в крупных транспортных узлах и принять Федеральный закон «О смешанных (комбинированных) перевозках грузов» [6], в котором необходимо закрепить понятие мультимодальной перевозки.

При доставке груза большое значение имеет информационное и документационное сопровождение. Пакет транспортных документов дает возможность старта осуществления загрузки транспортного средства, по прибытию — выгрузки груза заказчику. Говоря о мультимодальных перевозках, следует особое внимание обратить на сложный документооборот и более сложный учет грузопотока. Идет учет грузов, идущих по различным транспортным коридорам в раз-

ные пункты доставки. При такой грузоперевозке используют документы, относящиеся к соответствующей перевозке. При железнодорожной перевозке — железнодорожная накладная (*railway bill или RWB*), при авиаперевозке — авианакладная (*airwaybill* или *AWB*), коносамент (*Bill of lading — B/L,* «цифровой» аналог — *waybill*) — при морской перевозке; накладная *CMR* (*Convention relative au contrat de transport international de Marchandise par Route*) — при перевозке автомобильном транспортом.

Требуется создание виртуальных систем документооборота (в том числе с использованием электронных накладных и иных транспортных документов). С 2023 г. в России будут введены электронные накладные, которые станут началом перехода на новые технологии. Создание систем электронного документооборота, интерфейсов взаимодействия оператора мультимодальных перевозок и клиента, оператора и перевозчиков, а также иного программного обеспечения и мобильных приложений позволит снизить риски мультимодальных перевозок грузов, а также повысить эффективность управления. Необходимо принять соответствующий нормативный правовой акт для регулирования электронного документооборота при осуществлении грузоперевозок на всех типах транспорта, а также в прямых смешанных перевозках (мультимодальных перевозках).

Осуществление мультимодальных перевозок неразрывно связано с типом перевозимого груза, срочностью доставки, местоположением пункта отправления и пункта назначения, а также с преимуществами и недостатками отдельных видов транспорта (логистических, управленческих, экономических и правовых). В целях оптимального построения маршрута из точки отправления в точку назначения выбираются именно те виды транспорта, при которых возможна минимизация различных рисков, связанных с порчей, недостачей и утратой груза. Для мультимодальных перевозок цифровизация дает автоматизацию в логистике, роботизацию при обслуживании транспорта, техническое сопровождение, которое очень важно при смене видов транспорта, быстрое получение информации о тарифах и маршрутах, статусе и сроке доставки своего груза, онлайн-услуге по оформлению страховки и таможенных платежей. Долгосрочная стратегия развития транспортной отрасли России, принятая распоряжением Правительства РФ от 27.11.2021 № 3363-р «О Транспортной стратегии Россий-

ской Федерации до 2030 года с прогнозом на период до 2035 года», предполагает активное внедрение цифровых сервисов.

В Стратегии говорится, что цифровизация создает условия для увеличения скорости мультимодальной перевозки в четыре раза, в том числе в части транзитных и внутрироссийских грузовых и пассажирских перевозок, за счет цифровизации планирования и управления грузовыми и пассажирскими потоками и связанного документооборота; сокращение сроков ожидания и прохождения таможенных процедур в 10 раз за счет цифровизации трансграничного информационного обмена.

Актуальными на сегодняшний день направлениями в развитии мультимодальных перевозок являются: создание крупнейших мультимодальных транспортных центров, обеспечивающих внешнеторговые операции и транзит; создание программного обеспечения и виртуальных сред, обеспечивающих коммуникацию всех участников мультимодальной перевозки; создание современных электронных систем мониторинга контейнеров, вагонов и грузов; создание сервисов и технологических платформ взаимодействия с клиентом; создание мобильных приложений, направленных на оперативное получение информации о грузе, на отслеживание перемещения груза, оперативное взаимодействие с клиентом с целью получения дополнительной информации о перевозке, о грузе, о получателе груза и др. Вышеперечисленные меры могут позволить наиболее эффективно управлять как отдельными этапами перевозки, так и всей перевозкой в целом: от взаимодействия с клиентом до распределения маршрутов.

Показателен пример Казахстана, где после обновления законодательства блокчейна различные перевозчики и операторы внутри страны стали рассматривать технологии блокчейна и системы смарт-контрактов в рамках документооборота, автоматизации процессов выставления счетов и оплаты и устранения посредников при осуществлении мультимодальной перевозки [1].

Из этого следует, что по сей день остается потребность в принятии нормативного правового акта, который бы мог регулировать данные общественные отношения.

В заключение следует отметить, что рассмотренные выше проблемы следует разрешить путем принятия закона о прямых смешанных перевозках. Также необходимо внести в закон существующее в пра-

вовой доктрине понятие мультимодальнй перевозки, разработать и внести в закон специальные нормы контроля на терминалах мультимодальных перевозчиков, правовые нормы, обеспечивающие повышение защищенности транспортной инфраструктуры и транспортных средств при организации мультимодальных перевозок. Законодательное регулирование мультимодальной перевозки в современных условиях с использованием цифровых технологий отстает и на международном, и на национальном уровне. Встает вопрос о дополнении нашего законодательства новыми нормами. Неурегулированность правоотношений, связанных с мультимодальными перевозками грузов может привести к снижению безопасности и качества оказания перевозки, а в целом привести к негативным последствиям для развитие всей экономики страны.

Литература

1. Бадябина, К. Ю. Внедрение информационной системы при помощи технологии Блокчейн для модернизации мультимодальных перевозок в Казахстане// Логистика — евразийский мост: Материалы XVI Международной научно-практической конференции, Красноярск-Енисейск, 28 апреля 2021 г. Красноярск : Красноярский государственный аграрный университет, 2021.
2. Круглова, И. А. Развитие системы мультимодальных перевозок в новых технологических условиях / И. А., Круглова А. Н. Кириллов // Ученые записки Международного банковского института. 2019. № 2(28). С. 122—135.
3. Кузьмина, М. А. Основные концепции развития технологий мультимодальных перевозок / М. А. Кузьмина, С. Л. Надирян, Е. О. Чернобривец // Научные труды КубГТУ. 2015. № 6. С. 68—72.
4. Милославская, С. В. Мультимодальные и интермодальные перевозки : учебное пособие / С. В. Милославская, К. И. Плужников. Москва : Росконсультант, 2001.
5. Смирнова, В. В. Особенности правового регулирования мультимодальной перевозки грузов / В. В. Смирнова, А. В. Романов // Инновационные процессы в условиях глобализации мировой экономики: проблемы, тенденции, перспективы (IPEG-2021): сборник научных трудов / под редакцией П. А. Неверова, Б. А. Аманжоловой. Прага : Vědecko vydavatelské centrum «Sociosféra-CZ», 2021.
6. Смирнова, В. В. Правовое регулирование мультимодальных грузоперевозок в России: история и современность / В. В. Смирнова, А.

В. Романов // Вестник Юридического института МИИТ. 2021. № 2 (34). С. 81-88.
7. TRANS/WP.24/2000/1. Терминология комбинированных перевозок// https://unece.org/DAM/trans/wp24/documents/wp24-00-1r.pdf.

Dr. Djama Malika,
University Professor, University Center Of Alih KafiTindouf

Confronting information crime in Algerian legislation at the national and international levels

Abstract. The cybercrime, as one of the contemporary transnational information crimes, raises in its entirety a lot of problems in various respects, such as the difficulty of discovering it as well as proving it due to the absence of physical evidence that condemns its perpetrator, in view of the foregoing, and aware of the seriousness of cybercrime and the significant damage it causes to individuals and state institutions, the Algerian legislator proceeded to develop legal texts to address this crime on the one hand, and on the other hand, amended many laws, especially the Penal Code, to make them respond to criminal developments in The field of information and communication technology.

Through this intervention, we will try to shed light on the efforts made by the Algerian legislator to combat cybercrime in two axes. In the first axis, we address the efforts made at the national level, and in the second axis we review the efforts made at the international level.

Keywords: information crime, Algerian legislation, the national and international levels.

Introduction

The development in information and communication technology and the emergence of the Internet, with all its progress and services, did not pass over the world peacefully, because the more it had positive effects and changed the lifestyle of societies and contributed to the development and advancement in all fields, especially electronic transactions, the more it had a negative impact on The lives of people and the interests of states,

manifested in adapting the Internet and electronic means to become a world of crime[1].

Thus, the information revolution witnessed by human societies in the past decades left a great echo that led to the destabilization of a number of traditional concepts that had prevailed for a long period of time, as criminals tried to adapt to the new situation, and invented modern methods and means that were able to transcend the traditional methods that were They are used to committing crimes[2], which led to the emergence of electronic, information or technical crime, which is a criminal activity in which computer technology or smart phones connected to the Internet are used directly or indirectly to carry out the criminal act[3].

And cybercrime, as one of the contemporary transnational information crimes, raises in its entirety a lot of problems in various respects, such as the difficulty of discovering it as well as proving it due to the absence of physical evidence that condemns its perpetrator, especially that the information criminal is characterized by resourcefulness and cunning and uses highly efficient information technologies, which leads to network penetration. and computers connected to the Internet, where the network security system is breached and the device is accessed to reveal or destroy its contents and manipulate the information stored in it[4].

In view of the foregoing, and aware of the seriousness of cybercrime and the significant damage it causes to individuals and state institutions, the Algerian legislator proceeded to develop legal texts to address this crime on the one hand, and on the other hand, amended many laws, especially the Penal Code, to make them respond to criminal developments in The field of information and communication technology.

Through this intervention, we will try to shed light on the efforts made by the Algerian legislator to combat cybercrime in two axes. In the first

[1] Hafoda elamir Abdelkader, Ghardaine Hossam, Cybercrime and the Mechanisms to Counter it, the National Forum on Mechanisms for Combating Cybercrime in Algerian Legislation, Algeria, March 29, 2017. P. 83.

[2] Zoaiti Amina, Bernaoui Radhia, Combating Cybercrime in the Light of the Algerian Penal Code, A Comparative Study, Journal of Human Rights and Public Freedoms, Mostaganem University, Volume 04, Issue 07, June 2019. P. 222.

[3] Hafoda elamir Abdelkader, Ghardaine Hossam, Previous reference. P. 84.

[4] Linda Sharabshah, International and Regional Policy in the Field of Combating Cybercrime (International Trends in Combating Cybercrime), Journal of Studies and Research, Volume 01, Issue 01, Zayan Ashour University, Djelfa, 09/15/2009. P. 241.

axis, we address the efforts made at the national level, and in the second axis we review the efforts made at the international level.

The first axis:The efforts of the Algerian legislator in the field of combating cybercrime at the national level

We will talk about the efforts of the Algerian legislator in the penal code, then Law 09-04 related to information and communication technologies.

I. Combating cybercrime under the Penal Code

In order to fill the legislative void in the field of cybercrime, the Algerian legislator amended the Penal Code by virtue of Law No. 04-15 of November 10, 2004, whereby he created a seventh bis section in which he dealt, Breaches of automated data processing systems in Articles 394 bis to 394 bis 7 of the Penal Code. It included a set of substantive rules according to which it determined the actions affecting the automated data processing systems and the corresponding penalty.

The data processing system means «every system or group of systems, whether connected, separate from each other, or linked, and one or more of them automatically processes data in implementation of a specific program»[1].

The act of assault is carried out by the offender performing one of the acts specified in the aforementioned articles, and they can be traced back to:

— Entering or staying by cheating in all or part of an automated data processing system or attempting to do so. Such as theft and forgery of information, information espionage, assault on the sanctity of private life, and other crimes.

— The fraudulent entry of data into the automated processing system, or the fraudulent removal or modification of the data contained therein.

— Designing, researching, compiling, providing, publishing or trading in data stored, processed, or transmitted through an information system in which the crimes stipulated in this section may be committed.

Possessing, disclosing, publishing or using for any purpose the data obtained from one of the crimes stipulated in this section.

II. Combating cybercrime in accordance with Law 09-04

[1] Article 02/b of Law No. 09-04 of August 05, 2009 containing special rules for preventing and combating crimes related to information and communication technologies, Official Gazette No. 47.

The Algerian legislator issued Law No. 09-04 of August 5, 2009, which includes rules for preventing and combating crimes related to information and communications technology, whereby he expanded the concept of cybercrime to include in addition to crimes against the automated data processing system specified in the Penal Code. Crimes that are committed or facilitated through an information system or an electronic communication system.

This law included preventive measures and procedural rules.

1. Preventive measures

These measures are represented in the monitoring of electronic communications, as stipulated in Article 04 of Law 09-04, and specifying four cases in which the security authorities may monitor electronic communications after obtaining written permission from the judicial authority. These are four cases:

— Prevention of acts described as crimes of terrorism, sabotage and crimes against state security.

— In the event that information is available about the possibility of an attack on an information system in a way that threatens the system, national defense, state institutions, or the national economy.

— For the requirements of judicial investigations, if it is difficult to reach a conclusion that benefits the ongoing research without resorting to electronic monitoring.

— In the context of the implementation of requests for international judicial assistance.

2. Rules of Procedure

In addition to the preventive measures, the Algerian legislator added new measures that support the procedures stipulated in the Code of Criminal Procedure in the field of combating cybercrime. These measures are:

A. Inspection of information systems: Article 05 of Law 09-04 allowed judicial authorities as well as judicial police officers within the framework of the Code of Criminal Procedure to enter for the purpose of inspecting the information system. Inspection cases were limited to the cases stipulated in Article 04 of the same law, which are the same cases related to monitoring Electronic communications.

B. Information data reservation: When the stored data is useful for detecting cybercrime.

It is worth noting that Law 09-04 stipulates in its fifth chapter the establishment of the National Authority for the Prevention and Control of

Crimes Related to Information and Communication Technologies, to activate and coordinate operations to prevent and combat crimes related to information and communication technologies, and to assist the judicial authorities and the judicial police in their investigations regarding these crimes.

It also undertakes the exchange of information with its counterparts abroad, in order to collect all the data useful in identifying the perpetrators of cybercrime and determining their whereabouts.

The composition of this body was determined by Presidential Decree No. 19-172 of 06/06/2019, which includes determining the composition of the National Authority for the Prevention of Crimes Related to Information and Communication Technologies combating it, regulating it and how works[1]. It is a public institution of an administrative nature that enjoys legal personality and financial independence and is placed under the authority of the Ministry of National Defense.

In its last chapter, this law also emphasized the principle of international judicial cooperation and assistance within the framework of the principle of reciprocity.

This law also dealt with the issue of jurisdiction through the requirements of Article 15, where this article states that "in addition to the rules of jurisdiction stipulated in the Code of Criminal Procedure, Algerian courts have jurisdiction over crimes related to information and communication technologies committed outside the national territory when the perpetrator is a foreigner and targets state institutions The algerian, national defense, or the strategic interests of the national economy".

In addition to these procedural mechanisms included in Law 09-04, the Algerian Code of Criminal Procedure included a set of mechanisms for investigations and investigations into crimes related to information and communication technologies, such as the mechanism related to the interception of correspondence (Articles 65 bis 5 to Article 65 bis 10 of the Code of Criminal Procedure).

According to Article 16 of the Algerian Code of Procedure, it is allowed to extend the jurisdiction of judicial police officers to the entire national territory if it comes to researching and examining crimes related to

[1] Presidential Decree No. 19-172 of 06/06/2019 defining the composition of the National Authority for the Prevention, Control, Regulation, and Operation of Crimes Related to Information and Communication Technologies, Official Gazette No. 37.

automated data processing systems, in addition to what Article 37 stipulates that the local jurisdiction of the Public Prosecution may be extended if it comes to crimes related to systems Automated data processing.

The second axis: the efforts of the Algerian legislator in the field of combating cybercrime at the international level

Eager to provide protection in the field of technology and technology, Algeria ratified the Arab Convention against Information Technology Crimes liberated in Cairo on 12/21/2010, pursuant to Presidential Decree No. 14-252 of 08/09/2014[1]. The most important thing that the agreement emphasized in its preamble is that it is convinced of the need to adopt a common criminal policy aimed at protecting the Arab community against information technology crimes, and it also takes into account the lofty religious and moral principles, especially the provisions of Islamic law, as well as the human heritage of the Arab nation that rejects all forms of crimes and with due regard for the system It also aims to enhance and strengthen cooperation between Arab countries in the field of combating information technology to ward off the dangers of these crimes in order to preserve the security and interests of Arab countries and the safety of their societies and individuals[2].

The agreement criminalizes the attack on the sanctity of private life by means of information technologies[3], and Article 02/1 of the agreement defines information technology as "any material or moral means or group of interconnected or unconnected means used to store, arrange, organize, retrieve, process, develop and exchange information in accordance with orders and instructions." This includes all the inputs and outputs associated with it, wired or wirelessly, in a system or network.

The convention also obligates each state party to tighten penalties for traditional crimes if they are committed by means of information technology[4].

Conclusion

The Algerian legislator has worked hard to address cybercrime by amending the provisions of the Penal Code and the Code of Criminal Pro-

[1] Presidential Decree No. 14-252 of 08/09/2014 includes the ratification of the Arab Convention against Information Technology Crimes, liberated in Cairo on December 21, 2010, Official Gazette No. 57.

[2] Article 01 of the Arab Convention against Information Technology Crimes.

[3] Article 14 of the Arab Convention against Information Technology Crimes.

[4] Article 21 of the Arab Convention against Information Technology Crimes.

cedure, and introducing several legal texts such as Law No. 09-04 and Law No. 18-07 of June 10, 2018 relating to the protection of natural persons in the field of data processing of a nature Personal and Law 18-05 of May 10, 2018, related to electronic commerce, and other laws that confirm the legislator's desire to confront cybercrime and everything related to it.

Through this intervention, we were able to reach some recommendations, which we summarize as follows:

1) We recommend the Algerian legislator to issue a special and independent law related to cybercrime and ways to combat it, and to include in it all the substantive and procedural rules related to this type of crime.

2) Holding training courses for judicial police officers, the Public Prosecution Office and judges, in order to rehabilitate them and make them aware of all services related to information and communication technologies.

3) Organizing awareness campaigns for users of electronic media (computers, the Internet, smart phones...), and informing them of the magnitude of the danger that awaits them if the necessary preventive precautions are not taken.

Протас Елена Васильевна,
доктор педагогических наук, профессор кафедры «Гражданское право, международное частное право, гражданский процесс» Юридического института Российского университета транспорта (МИИТ)

Тарасенко Юрий Александрович,
кандидат юридических наук, доцент кафедры «Гражданское право, международное частное право, гражданский процесс» Юридического института Российского университета транспорта (МИИТ)

О некоторых проблемах смарт-контрактов в трансграничных отношениях

Аннотация. Процессы цифровизации затронули и сферу международного частного права. Появление смарт-контрактов породило дискуссию о возможности использования последних в трансграничных отношениях. Помимо основного вопроса (о природе смарт-контракта) ответа требуют проблема вы-

бора права (в тех случаях, когда стороны при заключении договора упустили этот момент), возможность определения места заключения самого договора, а также проблема внесения изменений в условия смарт-контракта. Краткий анализ названной проблематики показывает, что в настоящее время не существует ни на законодательном, ни на доктринальном уровне приемлемого ответа на поставленные вопросы. Сфера трансграничных отношений характеризуется сложным правовым регулированием с активным использованием правовых конструкций из различных правопорядков. Указанный момент порождает в определенной степени состояние правовой неизвестности, поскольку контрагенты не всегда точно знают, на какой правопорядок укажет коллизионная норма. Смарт-контракты получили распространение в областях, не требующих наличие многоэтапного правового регулирования. Условие для реализации смарт-контракта — максимально простое, соответствующее схеме «если — то».

Ключевые слова: смарт-контракт; внешнеторговая сделка; трансграничные отношения; выбор права; место заключения контракта; исполнение смарт-контракта.

Elena V. Protas,
Doctor of Pedagogical Sciences, Professor of the Department "Civil Law, International Private Law, Civil Procedure" of the Law Institute of the Russian University of Transport (MIIT)

Yuri Al. Tarasenko,
Candidate of Law, Associate Professor of the Department of "Civil Law, Private International Law, Civil Procedure" of the Law Institute of the Russian University of Transport

About some problems of smart contracts in cross-border relations

Abstract. Digitalization processes have also affected the sphere of private international law. The emergence of smart contracts has given rise to a discussion about the possibility of using the latter in cross-border relations. In addition to the main question (about the nature of the smart contract), the problem of choosing the law requires an answer (in cases when the parties missed this moment when concluding the contract), the possibility of determining the place of conclusion of the

contract itself, as well as the problem of making changes to the terms of the smart contract. A brief analysis of these issues shows that there is currently no acceptable answer to the questions posed either at the legislative or doctrinal level. The sphere of cross-border relations is characterized by complex legal regulation with the active use of legal structures from various legal systems. This moment generates to a certain extent a state of legal uncertainty, since counterparties do not always know exactly what kind of law and order the conflict of laws rule will indicate. Smart contracts have become widespread in areas that do not require multistage legal regulation. The condition for the implementation of a smart contract is the simplest possible condition corresponding to the "if — then" scheme.

Keywords: smart contract; foreign trade transaction; cross-border relations; choice of law; place of conclusion of the contract; execution of the smart contract.

1. Одним из традиционных способов заключения договора в международном частном праве является способ обмена взаимосогласованными сообщениями (оферта—акцепт). Для участников международного коммерческого оборота при заключении контракта важным моментом представляется определение места заключения договора, поскольку в зависимости от того, где (в каком месте) возник договор, будет определяться применимое к правоотношениям право страны[1]. Это соответствует коллизионному принципу *lex loci contractus* (место заключения контракта).

Одним из способов, основанных на электронной технологии, является технология смарт-контракта. Ее суть в том, что информация о условиях контракта зашифрована определенным протоколом и хранится на разных компьютерах, объединенных в единую сеть и связанную с единым сервером. При заключении договора посредством средств электронной связи проблема определения места заключения контракта раскрывается наиболее остро, поскольку не всегда очевидно место нахождения оферента или акцептанта.

В ряде случаев стороны не делают оговорку о применимом праве вполне сознательно, оставляя этот вопрос на волю случая, поскольку заранее не известно, какое условие может быть нарушено и кем. Нередко коллизия возникает не в связи с согласованными условиями, а в

[1] Речь идет о тех случаях, когда стороны специально не сделали в самом соглашении оговорку о применимом праве.

отношениях, сторонами не урегулированными, но вытекающими из договора. В зависимости от этого в дальнейшем решать вопрос о применимом праве будет коллизионная норма, которая может указать на любой правопорядок. Решить эту проблему смарт-конракт не способен в силу наличия уже заранее четко прописанного алгоритма действия, которое не предполагает появления ситуации с неизвестным содержанием.

2. Помимо трудности определения места заключения смарт-контракта существует проблема изменения уже заключенного соглашения, основанного на технологии блок-чейн. В процессе исполнения договоров нередко возникают ситуации, требующие корректировки ранее согласованных позиций. Обычно стороны решают такие вопросы посредством переговоров и изменения того или иного условия. Применительно к смарт-контрактам этот путь недоступен.

Проблему внесения изменений в смарт-контракт можно упрощенно описать следующим образом: существуют уже заранее заданные параметры, которые соответствовали условиям заключаемого контракта. Сами параметры хранятся на самых разных компьютерах, объединенных в единую взаимосвязанную цепь, что делает невозможным какой-либо стороне контракта или третьему лицу что-либо изменить. Если какой-либо из указанных параметров не будет совпадать (а именно это и произойдет, если стороны захотят какое-либо условие изменить), то надлежаще исполнить смарт-контракт не удастся.

Такая ситуация применительно к трансграничным отношениям не допустима, поскольку лишает стороны многих традиционных способов корректировки своих взаимоотношений на стадии исполнения обязательств.

3. Смарт-контракты в настоящий момент ориентированы на предельно упрощенные условия, которые можно описать следующей формулой: «если — то»: например, если за товар поступает оплата в таком-то размере, то право собственности на товар переходит к покупателю. Таким образом, электронный протокол сориентирован на простые и четко определяемые параметры. За пределами смарт-контрактов остаются более сложные условия, ориентированные на такие оценочные категории, как «разумный срок», «добросовестность», «заблаговременно» и т.п.

По сути дела, смарт-контракт не есть полноценный договор, имеющий содержание. Это некие действия, переведенные на язык алгоритмов, которые направлены на то, чтобы последовательно исполняться при наступлении заранее заданных параметров. В эти действия (команды) невозможно уложить юридические условия, из которых составляется содержание любого договора, поскольку условия выражают права и обязанности сторон. Действие, облеченное в команду в смарт-контракте может отразить только лишь небольшой аспект какого-либо традиционного условия договора, но не полностью описать и заменить его.

Трансграничные торговые контракты характеризуются довольно сложным уровнем правового регулирования. В результате, именно указанная сложность выводит договоры, осложненные иностранным элементом на уровень, где невозможно оперировать простым (элементарным) инструментарием по формуле «если — то».

В качестве иллюстрации приведем типовое условие трансграничного контракта купли-продажи, относительно цены: «Цена по договору включает любые расходы, которые возлагаются на продавца в соответствии с согласованным базисом поставки. Однако если продавец принимает на себя расходы, которые в соответствии с согласованным базисом поставки или иными условиями конкретного договора купли-продажи относятся на покупателя, такие суммы не включаются в цену товара и подлежат возмещению покупателем. Если продавец принимает на себя расходы, в отношении которых, по согласованному базису поставки обязательств нет ни у одной из сторон, такие расходы подлежат возмещению покупателем, только если это согласовано сторонами».

Данное (типовое для внешнеторговой купли-продажи условие) содержит весьма гибкое описание возможных вариантов того, что может включать цена при исполнении такого контракта. Вполне понятно, что описать настолько точно указанное условие на языке алгоритма невозможно. Попытка упростить подобное условие, представив его в виде нескольких условий по простой схеме «если — то», приведет к деградации смысла статьи.

4. В настоящее время смарт-контракты получили распространение в сфере электронной коммерции. В частности, речь идет о сделках на бирже, заключаемых по принципу «покупаю — продаю». Подобные биржевые сделки имеют такую особенность — совершаются продав-

цом или покупателем пакетами (т.е. за один раз стороной посредством электронных торгов могут заключаться десятки, а то и сотни сделок). Специфика подобных операций в том, что тут покупателями и продавцами не обсуждаются никакие иные условия, характерные для обычного договора, кроме как условия о цене. Смысл таких торговых действий не в том, чтобы купив, стать собственником и получить соответствующие товары, а в том, чтобы «сыграть» на курсовой разнице — приобрел за меньшие деньги, продал за большие, когда конъюнктура рынка изменится. Иной подход на биржах и невозможен, в силах означенной специфики. Но распространять его на обычные (в том числе и внешнеторговые) сделки в настоящее время нет никакой необходимости.

Сторонники внедрения технологии смарт-контрактов подчеркивают преимущества, которыми обладает новая технология. В частности, отмечается:

— скорость. Обработка документов вручную занимает много времени и задерживает выполнение задач. Смарт-контракты предполагают автоматизированный процесс и в большинстве случаев не требуют личного участия, что экономит драгоценное время;

— независимость. Смарт-контракты исключают возможность вмешательства третьих сторон. Гарантия на транзакцию — сама программа, которая, в отличие от посредников, не даст основания сомневаться в ее целостности;

— надежность. Данные, записанные в *blockchain*, не могут быть изменены или уничтожены. Если одна сторона сделки не выполняет свои обязательства, другая сторона будет защищена условиями интеллектуального договора;

— нет ошибок — автоматическая система для выполнения транзакций и удаления человеческого фактора обеспечивает высокую точность при выполнении контрактов;

— сбережения. Смарт-контракты могут обеспечить значительную экономию за счет устранения расходов для посредников и сокращения операционных расходов, а также возможность для сторон работать вместе на более выгодных условиях[1].

[1] Что такое смарт-контракты? // URL: https://habr.com/ru/post/448056/ (дата обращения: 10.01.2022).

На поверку все названные преимущества таковыми не являются, поскольку в равной мере присущи и обычным контрактам. Так, скорость в трансграничной купле-продаже достигается посредством использования типовых форм, содержащих все необходимые условия, к которым другой стороне можно присоединиться. Независимость от вмешательства третьих лиц — не совсем понятное обоснование, поскольку на практике (до сих пор) не встречались случаи, когда третье лицо могло каким-то образом вмешаться во взаимоотношения контрагентов. Надежность, понимаемая как невозможность уничтожения данных, — характерна и для обычных контрактов, поскольку все необходимые документы существуют в нескольких экземплярах и видах (бумажном, электронном). Отсутствие ошибок — вероятно, речь идет об ошибках в условиях, а не орфографических. В частном праве эти ситуации называются просчетом одной из сторон, когда контрагент навязывает явно не выгодные условия. Но от подобного не свободен и смарт-контракт, поскольку алгоритмы последнего составляются человеком. Наличие сбереженных средств — также не абсолютный аргумент, поскольку подавляющее большинство традиционных договоров заключается без всяких посредников.

В заключении отметить следующее.

Специального правового регулирования данного явления в России нет. Не существует и какого-либо международного акта, на который можно было бы опереться при осмыслении возникшего и реально существующего процесса, основанного на блок-чейн технологии. Фактически, на сегодняшний день, сфера смарт-контрактов в России развивается вне всякой связи с ее правовым регулированием. Принимая во внимание суть технологии блок-чейн, пока можно утверждать, что традиционные институты договорного права не подходят для полноценной регламентации нового явления. Необходимо отдельное регулирование. На современном же этапе важно оценить, насколько новая регламентация может быть вписана (соответствовать) основным институтам и материи гражданского права. Есть опасность того, что новый институт может быть описан терминами техническими и иметь больше экономическое содержание[1], что повлечет общую нестыковку с основной структурой ГК РФ.

[1] В качестве примера подобного подхода можно привести практически любой закон, выходящий из недр Минэкономразвития России. Например, Федеральный закон от 25.02.1999 № 39-ФЗ «Об инвестиционной деятельности в Российской Федерации, осуществляемой в форме капитальных вложений».

Helen Nashaat Edward Nashed

Digital loyalty to transport customers and its security implications

Abstract. Security is a necessary requirement that everyone seeks to achieve, and that the nation's gains are at the top of these priorities. Security is synonymous with tranquility. From this point of view, loyalty and belonging are among the pillars of life that cannot be straightened without it, noting that this means confidence and calmness of the soul as a result of a sense of not being afraid of any danger or harm. The state's ability to secure the continuity of the basis of its internal and external strength in all economic activities in various sectors, especially transport, in order to face the dangers that threaten it from inside and outside is of the importance of paying attention to transport clients. Digital marketing is growing very fast compared to traditional marketing methods. This requires a lot of research into exposure to electronic security and threats to customers.

Keywords: digitization; loyalty; security; customer.

The first chapter
Loyalty and belonging to transport customers

You can't ignore its length when you know: Inbound marketing costs 62% less leads than traditional outbound marketing. Blogger companies get 55% more web traffic 57% of all companies gain clients through blogging. 78% of online users search for product information online before making a purchase. The number of marketers who believe Facebook is essential to their success has increased 83% in two years. It's also important to understand that people have more options than ever when browsing the web. If they aren't motivated by the site, and if they don't get what they want within seconds of showing up, they will hold back and never come back.

First, social loyalty sharing on social media is one of the best ways to get people involved in your business. When you offer clients a small reward for posting about your work on social media. You can customize this, so that it suits your own needs of course. For example, if you want to make sure a broad base of people knows about one of your new seasonal offers, you can motivate your customers to spread the word about that offer. Or if you want people to publish a certain post, you can offer a reward for it([1]).

[1] Nina Semeryanova , Alexander Mordvinov: Information security in the field of transport services, E3S Web of Conferences 135, 04072 (2019) ITESE-2019. P. 5.

Second, emotional loyalty everyone loves to feel known and understood. A customer is happy when the owner asks to be greeted by name is a great thing to hear — it makes him feel at home. When customers feel that you know them, they automatically feel loyal to your business. You can give your customers that sense of belonging by sending them special offers on their birthday or anniversary celebrations. You may want to send them a message a few days before their birthday to remind them that a special offer is coming up, just to build anticipation and engagement.

Third: Behavioral loyalty Behavioral loyalty is one of the best ways to build a strong relationship with customers. Behavioral loyalty means working to get customers to do the kinds of things that build success for your business. If you're on a points system, you can offer your customers extra points — maybe double or triple points — for certain types of purchases([1]). For example, you may want to offer bonus points to customers who make purchases in the off-season or during any time that is usually slow for you. You can also offer bonus points to customers who make a number of purchases at once.

Fourth: Loyalty to the Call Loyalty Endorsement means offering a reward to your customers every time they recommend your business to new customers. In simple form, loyalty to an invitation is like word of mouth. It's a great way to get new customers excited about your business and products. In general, people are more willing to try a business if they hear about it from a trusted friend — which is why word of mouth is so valuable. If you use a points system to award rewards to customers, it may be a good idea to offer double points — or even three points — every time a customer successfully refers a friend to your business. Of course, if their friends turn out to be loyal customers, they may eventually recommend other friends. The idea behind customer loyalty plans is that they will generate greater rewards for your business([2]). There are some marketing programs that are used to optimize resources including: The points-based program is the most widely used loyalty program. In this program, the customer gets points for every purchase, and these points give him the advantage of converting them to a certain amount of money that he uses in

[1] Pratiwi, M № and others : Analysis of satisfaction and loyalty level of online taxi bike customer, Journal of Physics, 2020. P. 7.

[2] Vidila Rosa and otherd: Mobile Customer Relationship Management, ICCOMSET 2018. P. 8.

the same organization that is covered by the transport sector, or you give him a gift in exchange for the points he collects.

— Layers program and this is somewhat similar to the previous program, but the difference is that the more purchases are transferred from one layer to another, and each layer has more material and moral advantages. It moves from category to category. Blue, silver, gold. Each unit gives you better advantages in terms of the method of calculating the miles and additional services during the entire journey.

— A program that increases value, and here the transport sector is concerned with the social and humanitarian motives of customers and offers something to serve the community or donates a certain amount in exchange for the operations that customers conduct with them. The campaign with the slogan "One for One" Example: A program that takes a monthly amount in exchange for the delivery service in the fastest possible way and for free, as well as additional services that include exclusive rights to watch exclusive movies and TV programs with the medium used.

— Loyalty program through games. In this program, the organization engages customers in games for the purpose of entertainment And try to increase purchases, including getting a coupon (scrape and win) for every amount equal to the value of a ticket, or getting a picture or a game after each purchase, and you get a valuable gift if you collect all the group.

— Alliance program in this program, the organization([1]) is in relationship with other organizations under the name of a well-known alliance program, and the customer gets points for every purchase, but he can convert them to a sum of money to be used by any organization affiliated with the same alliance. Example: The loyalty program of Saudi Airlines gives you points However, these points can be used on any other lines under another alliance to which Saudi Airlines belongs.

— The mixed program and in this program companies use more than one loyalty program from the previous systems. Few companies resort to more than one type, and the greater the size of the company and the size of its assets, the greater the chance that it will follow more than one program at once.

Fifth: Forms of affiliation: One of its forms is loyalty to the homeland and maintaining the cleanliness of transportation, public places and facili-

[1] Yueqiu Li, Chunming You: Brand Loyalty Measurement Model Based on Machine Learning Clustering Algorithm, IOP, u 2021. P. 6

ties. Participation in voluntary and charitable works that serve the community, adhering to the laws and rules of conduct. Discipline at work. Choosing a conscious dialogue method in solving problems and conflicts that occur between individuals and groups. Respect the customs, traditions and customs of the community. Commitment to national symbols, such as the national anthem, the flag, and everything that falls under these symbols. Pride in the homeland, its name, and its symbols, at home and abroad. Loyalty and affiliation reflects the participation of the transport sector in the joys and sorrows of the people of the country., Forms of non-belonging to the homeland, such as rebellion against the system and society. Resorting to electronic violence to solve problems. Rebellion against the laws of the country. Igniting the fuse of strife, whether sectarian, partisan or other. Stealing real estate and movable property owned by the transport sector, and seizing the property of others. Cover up the traitors, the corrupt. Cooperation with the enemy is against the interest of the country.

Sixth: The concept of the customer: It is a person or company that receives, consumes, or buys a product or service and can choose between different goods and suppliers, as the main objective of all businesses or establishments is to attract customers or consumers, and make them buy what they have for sale. The passenger, as a customer in the transport sector with others who deal with this sector, is the person who uses a vehicle or a public or private means of transportation to move from one place to another.

Seventh: The importance of belonging and loyalty to transport customers: It is represented in the fear for his interest and its transcendence above all interests, and the consequent respect for the laws, adherence to the constitution and public morals, and the preservation of his property, so society rises and the nation rises economically to be at the forefront of nations. Customer loyalty is crucial to the success of the transport company's brand success because loyal customers can grow the business faster than sales and marketing, as customer loyalty is the result of their satisfaction, positive customer experiences and the overall value of the goods or services the customer receives from the business. Benefits of Customer Loyalty Importance: Customer loyalty has many benefits, the most prominent of which is increased business, as you are more likely to repeat your business with loyal customers when the service becomes appropriate for their needs, plus because they develop a stronger connection to your business, they are

more likely to make larger and more expensive purchases. However, customer loyalty is also the most effective way to protect your business from competition. Loyal customers are committed to your company; This means that you don't have to worry too much about losing your customers, especially for one-time deals or new competitors, since when you can establish a connection with a customer, you don't necessarily have to be the biggest company or get the best rates, as often it's possible for smaller businesses. It competes with big companies mostly by taking advantage of customer loyalty. Also, when errors or quality problems arise, loyal customers will give you the benefit of the doubt and stick with your business, of course if you abuse their loyalty and continue to provide poor service, they will eventually leave, however by increasing customer loyalty, you can avoid the repercussions of a one-time disaster one.

1. Bring in new business People love to spread the word about great products. Happy customers tend to tell their friends about the great mode of transport they used, for example. It's possible that the friends you told about the mode of transport have gone online and peeked at the mode of transport you used to take your errands. Some of them may decide to use the same method. This is how word-of-mouth advertising works — and loyal customers lead to a lot of this kind of free marketing to work. It is hard to overstate the importance of customer loyalty. For an online business, customer loyalty can mean the difference between success and failure — between making it big and falling back. Online retailers know that building strong relationships with customers is the key to taking their business to the next level. In today's global market, companies are constantly competing against each other for customers. This means that having a loyal customer — someone who already knows and trusts your products — is invaluable. A loyal customer will constantly return to your brand or store over a long period of time. . In the internet world, we see this in affiliate marketing. Many companies have successfully used software to create a commission system — which allows them to market their products and services to a wider and newer audience with the help of affiliates acting as brand ambassadors.

2. Bumper Shopping: Once people find a business they like, they tend to return to that business Much. They may even start shopping more than they used to. This is because they are excited about the great new products they find in their favorite businesses. Customers at a local farmer's market,

for example. Maybe they started going to the market because they heard it had fresh greens. Once they realized how good the greens are.

3. Helping improve the product the loyal customers already trust the transportation services provided by you. This means that in return, you can turn to them for information on how to improve your transportation products or services. One way to look at this is to treat loyal customers almost like a focused group. They can tell which means they would like to see changes in the transportation services offered and what they think needs improvement. The more you turn to loyal customers for feedback, the stronger the relationship the organization builds with them. Customers will be motivated by different things, depending on their needs, money and desires. To inspire customer loyalty, you must consider the unique set of circumstances for transportation customers and the kinds of things that might motivate them as a result.

4. Loyalty Transactions Transactional loyalty is the primary form of customer loyalty The great thing about this type of customer loyalty program is that it is straightforward and easy to deal with. After all, everyone wants free rewards, so it makes sense for customers to keep coming back until they earn their free item. However, the downside to this system is that you don't build an especially strong connection with customers. Simply offering a free item after a certain number of visits is not enough to make your customers feel engaged and engaged. It doesn't build the kind of lasting relationship you're looking for either. So while transactional loyalty is a good starting point, it is not enough on its own. It is hard to overstate the importance of customer loyalty. For an online business, customer loyalty can mean the difference between success and failure — between making it big and falling back. Online retailers know that building strong relationships with customers is the key to taking their business to the next level. However, it can be difficult to know exactly what «customer loyalty» means. It can be more difficult to figure out how to foster that loyalty. In today's global market, companies are constantly competing against each other for customers. This means that having a loyal customer — someone who already knows and trusts your products — is invaluable. A loyal customer will constantly return to your brand or services in the transportation sector over a long period of time. 5— Shopping a lot: Once people find a business they like, they tend to return to that business often. They may even start shopping more than they used to. This is because they are excited about the great new products they find in their favorite businesses.

The second chapter

Security required in the transport sector

First: The definition of security is a set of measures and laws that a person follows to achieve protection for himself, his money and property, or any valuable thing he fears.

Second: Diversity of security in the transport sector:

1. National security: it is the state's ability to secure the continuity of the basis of its internal and external strength, in all economic activities in various sectors, especially transportation, in order to face the dangers that threaten it from within and without.

2. Corporate security: It is a legal protection for its capital, which it deals with in providing its services and products under contracts that have now changed their shape and become smart contracts, and their profits are collected through smart or virtual money in some countries.

3. Food security: for meals provided through companies to passengers of the various means of transportation or logistics that serve this sector.

4. Economic security: It is the state's ability to maintain the well-being of individuals and their standard of living by providing them with the main resources. The transport sector is a clear example of economic activity in countries. As for the threat factors of an economic nature, there are several indicators to measure economic threats, the most important of which are: Imposing an economic blockade on The state or its boycott, and economic blocs that conflict with the interests of the state in the form of competition or dumping of light transport means, in addition to stopping the economic aid provided by the transport sector to customers.

5. Social security: It is the state's ability to preserve its heritage, language and culture, or it can be defined as the state's ability to protect its society from corruption and social crimes that harm society's stability, and protect them from external dangers that may cause them harm. The transport sector seeks to provide security Social for all customers with this sector. As for the threat factors of a social nature, they are represented in the export of ideologies that are incompatible with the values and principles of society, and the use of psychological warfare through counter broadcasts.

6. Environmental security: It is about protecting environmental resources from pollution and depletion, and using them in sound ways that serve the state and its society.

7. Cyber security: is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It is also known as information technology security, or electronic information security. Network security is the main system in the transportation sector from In order to practice securing a computer network from intrusive and opportunistic elements, whether targeted attackers, or malware.

Third: Electronic Security: Electronic security has become very necessary for users of the Internet, without it, the user loses his privacy and security on the Internet. different. This requires Exposure to: Application Security Application security: This term refers to security that focuses on keeping hardware and electronic programs away from any external threat or penetration that may cause access to data, as the hacked application can provide access to data designed for protection, and the successful application of the concept of security It begins in the initial design phase before the software or hardware is deployed([1]).

Information Security • Protects the integrity and privacy of data, whether in the stage of storage or transmission from one system to another via networks, protecting data and maintaining its integrity and establishing its privacy when it is stored within the systems Network security: It is one of the most important types of electronic security, due to its necessary function in protecting the network on which systems and programs are built, and provides internal tribal protection that protects against any external threats. different. Operational Security It includes the processes and decisions that handle and protect data assets. The permissions users have when accessing the network, and the procedures that determine how and where data can be stored or shared, all fall under this umbrella.

Fourth: Its importance. Electronic security in the transportation sector: is the increase in the use of the Internet and smart phones by individuals all over the world. Hardly a home is devoid of the Internet and a mobile phone, and most of the daily tasks are carried out via the Internet, so it has become necessary to pay attention to this area and take Considering its presence in all systems to increase the confidence of transport customers and protect data from any external influence. Also, technological security

[1] Jiyang Chen and others : Research on the Impacts of Multisensory Marketing on Customer Loyalty Based on Data Analysis, IOP Publishing. P. 10.

is an electronic term that refers to the protection of devices, servers, systems, data and networks from any external attack that may harm them or lead to damage or theft, and this concept is related to a group of other electronic concepts that branch from it and perform the same or similar function. Disaster recovery is the method that defines how to respond to various security incidents and determines how companies and organizations can recover processes, data and information that have been lost to restore operational capacity within the organization. Educating the end user, which is the security method that protects systems and companies from internal errors resulting from the wrong practices of individuals working in institutions and organizations.

Fifth: Elements of electronic security Electronic security has a set of important elements that must be present in order to be fully functional, namely:

- Safety of information.
- Useful information.
- Availability of information.
- Certification of access to information.
- Reliability and objectivity of information.
- Acknowledgment of responsibility for the information.

Sixth: Types of electronic threats Electronic security threats often have many forms according to their general classifications, and they are as follows:

- Electronic terrorism: It is the process that aims to weaken and dismantle the electronic system and sow fear and panic in the hearts of its users through social engineering with the aim of harming the transportation system.
- Electronic attacks: These are often purely politically motivated attacks carried out by major organizations, and the damages resulting from them are very severe and affect greatly on states and governments.
- Electronic crime: It is crimes that are carried out in an electronic manner by an individual or group of individuals and target the systems and institutions associated with the transport sector in order to obtain funds or cause system failures or for the purpose of electronic extortion of transport customers and other purposes. Achieving electronic security is a goal that everyone desires, and it can be implemented at high rates through a set of easy and simple practices, and among the most prominent ways that help in achieving electronic security:

• Use very strong passwords and make sure that they are not easy for people to guess.

• Do not use unsecured Wi-Fi networks, especially those in public places. • Avoid opening any links in e-mail messages from unknown persons.

• Do not open e-mail attachments from unknown persons.

• Updating the operating systems first hand.

• Using anti-virus programs of all kinds.

Хотько Ольга Александровна,
кандидат юридических наук, доцент, доцент кафедры экологического и аграрного права, Белорусский государственный университет

Роль государств — членов Евразийского экономического союза в реализации направлений формирования цифрового пространства в контексте проведения транспортной и экологической политики: правовые стратегии

Аннотация. В статье рассматриваются вопросы возможных способов развития направления формирования цифрового пространства Евразийского экономического союза при проведении скоординированной транспортной политики. При этом поскольку транспорт оказывает воздействие на окружающую среду и изменение климата, автор обращает внимание на взаимосвязь с экологической безопасностью. Раскрыта специфика решения проблем государствами — членами данного Союза с правовой позиции. Автор приходит к выводу о целесообразности развития согласованных мер, направленных на гармонизацию экологического и транспортного законодательства стран — участниц ЕАЭС для защищенности окружающей среды в свете цифровой трансформации и достижения принципов «зеленой» экономики.

Ключевые слова: цифровое пространство; экологическая безопасность; транспортная политика; Евразийский экономический союз; «зеленая» экономика.

Olga Al. Khotko,
candidat of law, docent, associate Professor at the department of environmental and agricultural law, PhD (law), Belarusian State University

The role of the Eurasian Economic Union member states in the implementation of the directions of formation of digital space in the context of transport and environmental policies: legal strategies

Abstract. The article discusses the issues of possible ways to develop the direction of the formation of the digital space of the Eurasian Economic Union when conducting a coordinated transport policy. At the same time, since transport has an impact on the environment and climate change, the author draws attention to the relationship with environmental safety. The specifics of solving problems with the Member States of this Union from the Legal Position are disclosed. The author comes to the conclusion about the feasibility of the development of agreed measures aimed at harmonizing the environmental and transport legislation of the EAEEC countries to protect the environment in the light of digital transformation and achieve the principles of the Green Economy.

Keywords: digital space; environmental safety; transport policy; Eurasian Economic Union; green economics.

В рамках функционирования интеграционных образований каждое государство, участвующее в нем, становится сильнее и могущественнее с различных позиций, поскольку постоянно поддерживается взаимный интерес и взаимопомощь, в том числе в сферах развития права и научных достижений. При этом, как верно пишет профессор Л. А. Савенок, рассматривая перспективы эксплуатации беспилотного транспорта, «инновационное развитие должно осуществляться без угроз для национальной безопасности, сохраняя жизнь и здоровье граждан» [1, стр. 63]. В литературе уделяется особое внимание свободе движения информации, укреплению кибербезопасности внутри интеграционного объединения, защите данных, инновационному регулированию вопросов управления информацией [2, стр. 43]. Целью данной работы является анализ взаимосвязи направлений транспортной политики и формирующейся в юридической науке экологической политики в условиях цифровизации на евразийском пространстве.

В свете исследования ключевых особенностей права ЕАЭС М. В. Шугуров отмечает о том, что большое значение имеет совершенствование договорной базы, в свете тенденций отставания уровня право-

вого регулирования научно-технического сотрудничества и расширения сферы науки, технологий и инноваций [3]. Так, цифровая повестка ЕАЭС включает ряд направлений формирования цифрового пространства, позволяющих снизить риски и обеспечить возможности развития стран Союза в перспективе до 2030 г., включающие следующие: реализация цифровой модернизации интеграционных процессов и переход всех институтов на новый уклад; создание условий для формирования цифровых рынков и обеспечение более высокого уровня защиты прав потребителей; системная организация построения цифровых инфраструктур, цифровых платформ и др. При реализации цифровой повестки ЕАЭС предполагается, что могут быть разработаны предложения по формированию цифрового пространства исходя из принципа баланса между глобальными тенденциями цифровизации и интеграционными возможностями Союза, что позволит отметить отличительную оригинальность проектов ЕАЭС, отразить позитивные изменения в перспективе при наращивании интеграционных связей с учетом проведения многовекторной политики.

Государства — члены ЕАЭС увеличивают инфраструктурное развитие в сфере транспорта, выстраивая цифровое пространство, расширяют объем грузооборота и пассажирооборота, разрабатывают совместные проекты по созданию и развитию евразийских транспортных коридоров в рамках сопряжения процесса развития ЕАЭС с международными инициативами. Так, Республика Беларусь в числе первых государств поддержала международную инициативу «Один пояс — один путь», предполагающую сопряжение двух концепций — построения Экономического пояса Шелкового пути и дальнейшего развития ЕАЭС. По мнению исследователей, «одним из ключевых узлов возрождаемого Шелкового пути станет новый высокоскоростной мультимодальный маршрут «Евразийский транспортный коридор», который будет основан на реализации принципа «5с» — скорость, сервис, стоимость, сохранность, стабильность» [4]. Согласно Договору о Евразийском экономическом союзе от 29 мая 2014 г. (далее — Договор о ЕАЭС) скоординированная (согласованная) транспортная политика направлена на обеспечение экономической интеграции, последовательное и поэтапное формирование единого транспортного пространства и предполагает осуществление сотрудничества государств — членов ЕАЭС на основе общих подходов, одобренных в рамках Союза и

гармонизацию правового регулирования для достижения совместных целей [5]. Вместе с тем осуществление такой политики при расширении евразийских транспортных коридоров невозможно в современных условиях цифровой трансформации интеграционных процессов без учета воздействия транспорта на окружающую среду.

Среди мер достижения социально-экономический эффекта реализации Программы поэтапной либерализации выполнения перевозчиками, зарегистрированными на территории одного из государств — членов Евразийского экономического союза автомобильных перевозок грузов между пунктами, расположенными на территории другого государства — члена Евразийского экономического союза, на период с 2016 по 2025 годы, названо снижение вредного воздействия на окружающую среду за счет расширения на внутреннем рынке современных грузовых автомобилей [6]. В качестве одной из задач политики по созданию общего рынка транспортных услуг предусматривается интеграция транспортных систем государств — членов в мировую транспортную систему [7], в рамках которой государства — члены должны направлять усилия на снижение вредного воздействия транспорта на окружающую среду и здоровье человека, внедрение альтернативных видов топлива и возобновляемых источников энергии.

Более четкое развитие экологической политики начинает прослеживаться в последнее время при разработке мер и механизмов «зеленой» экономики и вместе с тем установления концептуальных подходов развития «зеленого» транспорта в ЕАЭС [8]. Так, впервые обращается внимание на необходимость формирования климатической политики в ЕАЭС и закреплении ее в Договоре о ЕАЭС. В действительности, развитие инновационной деятельности не может не затрагивать иные сферы, соответственно, в особом подходе нуждается охрана климата на современном этапе. В рамках процессов формирования цифрового пространства и расширения транспортных коридоров такие аспекты должны быть учтены каждым государством — членом ЕАЭС и в рамках общего права Союза, что поспособствует обеспечению как национальной безопасности, так и формированию эколого-безопасного пространства в ЕАЭС.

Прежде всего на национальном уровне должен быть выработать механизм экологической безопасности либо на основании общей согласованной политики Союза следует развивать направления «зеле-

ной» экономики с учетом устойчивого роста транспорта и развития цифровых транспортных коридоров. Особое значение представляет согласованность действий государств — членов ЕАЭС, чему обязывает цифровая повестка ЕАЭС и реализаций направлений формирования цифрового пространства, среди которых также должно быть эколого-безопасное развитие государств.

Изложенное в настоящем исследовании позволяет говорить уже не о необходимости развития в ЕАЭС согласованных экологической и транспортной политик в рамках инновационного развития и цифровой трансформации, а о потребности разработки мер гармонизации законодательства в рассматриваемой сфере, в том числе технического регулирования. Так, хотя государства — члены ЕАЭС и придерживаются курса на обеспечение экологической безопасности, в отношении деятельности отдельных видов транспорта необходимо устранение пробелов и недостатков в праве ЕАЭС, а также согласование норм экологического и транспортного законодательства. С нашей позиции, целесообразно утверждение документа по обеспечению экологической безопасности на евразийском пространстве. Данный подход позволит выявить совместный механизм снижения воздействия транспорта на окружающую среду, определить способы защищенности климата и тем самым скоординировать действия органов государственного управления государств — членов ЕАЭС при цифровой трансформации и обеспечении устойчивого развития.

Литература

1. Савенок, А. Л. Проблемы правового регулирования научно-технического прогресса // Государство и право в XXI веке : материалы междунар. научно-практ. конф., посвящ. 95-летию юридического факультета Белорус. гос. университета, 26—27 ноября 2020 г., г. Минск / БГУ, Юридический фак. ; [редкол.: Т. Н. Михалева (гл. ред.) и др.]. Минск : БГУ, 2021.
2. Михалева, Т. Н. Цифровая повестка ЕАЭС: правовые стандарты и перспективы // Государство и право в XXI веке : материалы междунар. научно-практ. конф., посвящ. 95-летию юридического факультета Белорус. гос. университета, 26—27 ноября 2020 г., г. Минск. Минск : БГУ, 2021.
3. Шугуров, М. В. Право ЕАЭС в сфере науки, технологий и инноваций: системный подход // Моск. журнал межд. права. 2020. № 3. С. 44—63.

4. Шелест, К. Д. Геополитические вызовы и геоэкономические возможности формирования Евразийского транспортного коридора / К. Д. Шелест, А. Ю. Терешенкова, А. В. Шепелева // Евраз. юрид. журн. 2018. № 3 С. 53—57.
5. Договор о Евразийском экономическом союзе: подписан в г. Астане, 29.05.2014.
6. Программа поэтапной либерализации выполнения перевозчиками, зарегистрированными на территории одного из государств-членов Евразийского экономического союза автомобильных перевозок грузов между пунктами, расположенными на территории другого государства-члена Евразийского экономического союза, на период с 2016 по 2025 годы: утв. Решением Высшего Евразийского экономического совета от 8 мая 2015 г., № 13 // КонсультантПлюс, 2022.
7. Об основных направлениях и этапах реализации скоординированной (согласованной) транспортной политики государств-членов Евразийского экономического союза : решение Высш. Евраз. экон. совета, 26 дек. 2016 г., № 19 // Консультант Плюс, 2022
8. О международном опыте разработки и внедрения принципов, мер и механизмов «зеленой» экономики и концептуальных подходах в Евразийском экономическом союзе // https://eec.eaeunion.org/upload/medialibrary/939/Doklad_Zelenaya_ekonomika_PDF_sayt.pdf (дата обращения: 06.01.2022).

Шатская Ирина Ивановна,
кандидат экономических наук, доцент, доцент кафедры «Административное право, экологическое право, информационное право» Юридического института Российского университета транспорта (МИИТ)

Правовое регулирование цифрового формата взаимодействия государства и налогоплательщиков

Аннотация. В настоящей статье оцениваются масштабы применения цифрового формата взаимодействия государства и налогоплательщиков в правовом поле, анализируются влияние цифровых технологий на изменения налоговых правоотношений с учетом интересов государства и налогоплательщиков, современные направления и тенденции цифровизации в сфере налогообложения с применением рационального налогового законодательства.

Ключевые слова: законодательство; нормативно-правовая база; государство; цифровой формат; налоговая служба; налогоплательщики.

Irina I. Shatskaya,
Candidate of Economic Sciences, Associate Professor, Associate Professor of the Department «Administrative law, environmental law, information law «Institute of Law Russian University of Transport

Legal regulation of the digital format of interaction between the state and taxpayers

Abstract. This article assesses the scope of application of the digital format of interaction between the state and taxpayers in the legal field, analyzes the impact of digital technologies on changes in tax legal relations, taking into account the interests of the state and taxpayers, analyzes modern trends and trends in digitalization in the field of taxation using rational tax legislation.

Keywords: legislation; regulatory framework; state; digital format; tax service; taxpayers.

В современном обществе налоги являются основной формой доходов государства и наиболее действенным инструментом регулирования новых экономических отношений, которые на современном этапе невозможно представить без применения цифровых технологий. В налогообложении в цифровой формат переведены различные виды документов, способы их подписания, аутентификации, способы передачи, хранения документов, налоговые процедуры и разнообразные услуги: счета-фактуры; накладные на товары; платежи; цифровая подпись; регистрация бизнеса и получение в налоговой инспекции сведений об индивидуальном номере налогоплательщика; базы данных о налогоплательщиках, о сделках налогоплательщиков; базы данных об объектах налогообложения; подача налоговой отчетности; уплата налогов и пошлин; налоговые калькуляторы, налоговый учет; получение форм налогового контроля. Цифровые технологии в налогообложении успешно реализуются на разнообразных информационно-цифровых платформах: линейки личных кабинетов; платформы для анализа рисков бизнеса и сведений из различных реестров; контрольно-кассовой системы онлайн; налогового контроля; технологии

налогового мониторинга без выездных проверок; контроля налога на добавленную стоимость; механизма прослеживаемости товаров; системы налогового администрирования для самозанятых граждан.

Современный этап развития государства с широким охватом цифровизацией всех сфер хозяйственной деятельности субъектов налоговых правоотношений предъявляет новые требования как к формированию информационно-технологической среды для них, так и к созданию условий упрощения действий налогоплательщиков и повышения эффективности функционирования налоговых служб.

В рамках реализации Указов Президента РФ от 07.05.2018 № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года», от 21.07.2020 № 474 «О национальных целях развития Российской Федерации на период до 2030 года», Правительством РФ была сформирована национальная программа «Цифровая экономика Российской Федерации», утвержденная протоколом заседания президиума Совета при Президенте РФ по стратегическому развитию и национальным проектам от 04.06.2019 № 7, которая непосредственно затронула сферу налогообложения и послужила руководством для совершенствования процессов цифровизации в этой сфере. Результатом реализации программы стал ряд мероприятий: визуализация электронной подписи в электронном документе, уточнение правового статуса аккредитованной сертификации, определение порядка хранения электронных документов и др.

Даниил Егоров, руководитель ФНС России на заседании Общественного совета при ФНС России заявил: «Речь идет не только об электронных сервисах, но и выстраивании новой стратегии взаимодействия с налогоплательщиками. Новая концепция заключается в сокращении непроизводственных издержек компаний, которыми является администрирование налогов. Мы пытаемся их забрать на свой борт, чтобы люди занимались своим делом, а мы на основании первичных данных занимались своим и давали такие модели налогообложения, которые позволят бизнесу только подтверждать наши расчеты».

В ближайшей перспективе процессы цифровизации в налоговом администрировании могут быть реализованы в части полного охвата сдачи всех деклараций, обязательных сведений и расчетов в элек-

тронном виде инспекциями ФНС России, Пенсионным фондом РФ, Фондом социального страхования РФ, Росстатом. С 2021 г. налоговые службы самостоятельно рассчитают земельный и транспортный налог компаниям, владеющим транспортом, земельными участками, направляя сообщения об исчисленных суммах [Федеральный закон от 15.04.2019 № 63-ФЗ].

С середины 2022 г. вводится новый налоговый режим автоматической упрощенной системы налогообложения [Федеральный закон от 25.02.2022 № 17-ФЗ]. Похожий порядок налогообложения реализован для самозанятых лиц, когда используется мобильное приложение, при помощи которого возможно решение налоговых вопросов без непосредственного обращения в налоговую инспекцию. Основная особенность автоматической упрощенной системы налогообложения в том, что единый налог, который заменит налоговую отчетность и отчетность, предоставляемую во внебюджетные фонды, будет рассчитываться автоматически, с минимальным участием налогоплательщика. Для этих целей налоговая служба создает для юридических лиц личный кабинет налогоплательщика, где в режиме реального времени можно будет отслеживать все платежи. Данные для расчета будут взяты из отчетов кассовых аппаратов и безналичных расчетов компании. Отчеты по работникам, в части перечисления заработной платы, начисления и отчисления НДФЛ в этом случае возложены на банк.

Автоматическая упрощенная система налогообложения — это еще один шаг налоговых служб в снижении издержек администрирования и увеличения поступлений в бюджет. Однако отмены налоговой отчетности новый порядок не предусматривает, так что у налогоплательщика остается возможность подмены и подлога в отчетных и других документах. При этом новая система будет удобна налогоплательщикам в применении, а также позволит показывать весь фонд заработной платы, так как отменяется обязанность уплачивать страховые взносы, что, безусловно, положительно отразится на зарплатах сотрудников.

В отношении отчетности организаций из года в год наблюдаются изменения в порядке ее предоставления в ФНС России. В настоящий период времени остаются отчеты, которые можно представлять в налоговый орган на бумажном носителе, однако представление таких отчетов ограничено численностью работников. При этом некоторые

формы отчетности необходимо сдавать только в электронной форме с применением информационно-коммуникационной сети, и такая тенденция становится закономерностью, не только по решению налоговых органов, так как способствует прозрачности, но и по желанию самих налогоплательщиков, так как облегчает и ускоряет процесс сдачи отчетности.

Сдача годовой бухгалтерской отчетности для всех организаций, субъектов малого предпринимательства производится только электронно, по телекоммуникационным каналам связи через оператора электронного документооборота. Организации, индивидуальные предприниматели, среднесписочная численность за отчетный год у которых превысила 100 человек, предоставляют отчетность также только в электронной форме через интернет. Расчет сумм налога на доходы физических лиц, исчисленных и удержанных налоговым агентом в электронной форме по телекоммуникационным каналам (форма 6-НДФЛ) могут сдавать все налоговые агенты. Представить форму 6-НДФЛ на бумажном носителе могут те налоговые агенты, у которых численность физических лиц, получивших доход в отчетном периоде, менее 10 человек. Такой же порядок предусмотрен по расчетам страховых взносов (РСВ). Отчетность через информационно-коммуникационную сеть отправляют все организации. Возможность использовать бумажный носитель сохраняется у работодателя в том случае, если среднесписочная численность за отчетный период не превышает 10 человек. Все плательщики НДС и налоговые агенты в обязательном порядке отчитываются в электронной форме. Тенденция увеличения отчетности в электронном виде продолжается и в ближайшей перспективе отчетность на бумажных носителях будет сведена к нулю.

Для более понятного взаимодействия налогоплательщиков и налоговых служб приказом ФНС России от 16.07.2020 № ЕД-7-2/448@ утвержден порядок направления и получения в электронной форме документов, используемых налоговыми органами для реализации своих полномочий, а также представления документов по требованию налогового органа по телекоммуникационным каналам связи, в котором описаны этапы прохождения электронного документа от отправителя до получателя, определены правила отправки, получения и хранения документов, а также установлен перечень технологических

электронных документов, которыми оформляется процедура обмена документами: подтверждение даты отправки электронного документа; квитанция о приеме электронного документа; уведомление об отказе в приеме электронного документа. С 2022 г. введен обновленный порядок обмена электронными документами с ФНС России, приказ от 07.09.2021 № Д-7-8/795@ скорректировал порядок направления и получения налоговых документов и представления их в электронной форме по телекоммуникационным каналам связи. Введение обновленного порядка обмена электронными документами с ФНС России закрепило правила отправки и получения электронных документов, порядок предоставления документов по требованию налоговых служб. Новый документ объединил актуальные требования и правила и позволил налогоплательщикам не разбираться во множестве нормативных актов, заменив одним.

Кроме того в сфере цифровизации налогообложения разрабатываются и внедряются онлайн-сервисы для автоматической проверки правильности данных, отражаемых в налоговых декларациях налогоплательщиков, позволяющие контролировать деятельность налогоплательщиков таким образом, что использование серых схем, сокрытие или уход от уплаты налогов становятся невыгодными.

В отношении НДС, когда подача электронных деклараций стала обязательной, применяются автоматизированные системы контроля (АСК НДС-2), (АСК НДС-3) для автоматической проверки правильности данных с возможностью электронной корректировки деклараций и способствующие оперативности уточнения данных декларации. Кроме того автоматизированная система контроля АСК НДС-3 позволяет налоговым службам полностью автоматизировать процесс контроля за движением средств между счетами юридических и физических лиц, производить контроль движения товара, установить факты уплаты НДС и размеры выплаченных сумм. Выстраивание последовательных цепочек позволяет выявить недобросовестных плательщиков, использующих схемы уклонения от налогов. «Контроль НДС» дает возможность проверяющим не только отслеживать показатели налоговой отчетности, но и обмениваться информацией с другими подразделениями налоговой службы. При этом данные банков автоматически попадают в базу данных по НДС, анализируются программой, позволяющей выявить налоговые недоборы. В перспективе

намечено включение в систему контроля информации от ФТС России, данные об уплате страховых взносов и налогов на доходы физических лиц (НДФЛ).

Введение автоматизированной системы контроля применения контрольно-кассовой техники (АСК ККТ) способствовало в дистанционном формате отслеживать все розничные продажи [Федеральный закон от 03.07.2018 № 192-ФЗ], а также уменьшить случаи сокрытия налогов, упростить налоговые проверки, за счет оперативного получения информации и автоматизированного анализа, не требующего дополнительных проверок.

Введение государством Единой системы маркировки и прослеживаемости товаров способствовало целям, на которые эта система направлена: обеспечение получения оперативной и достоверной информации о движении товаров в рамках хозяйственной деятельности организаций, создание необходимых условий для сокращения объемов незаконного оборота продукции, повышение собираемости налогов, таможенных пошлин, улучшение налоговой дисциплины, а также мониторинг и контроль конкурентной среды на товарных рынках, в рамках перечней, утвержденных распоряжениями Правительства РФ от 28.04.2018 № 792-р, 28.02.2019 № 224 и др. К 2024 г. маркировке будут подлежать все товарные группы. Система «Честный знак», введенная в России, подразумевает идентификацию каждой единицы товара путем присвоения уникальных цифровых кодов, защищенных криптографией, что позволяет государству, бизнесу и потребителю контролировать путь любого товара от производителя до конечного покупателя, противодействуя незаконному обороту и способствуя повышению налоговых выплат.

Автоматизированная информационная система «Налог-3» постоянно совершенствуется, планируется полностью автоматизировать камеральные и выездные проверки налогоплательщиков. В систему включены данные банков, таможенной службы и правоохранительных органов. Вскоре система начнет отслеживать движение импорта на территории ЕАЭС, в автоматическом режиме система определит недобросовестных налогоплательщиков.

Концепция развития и функционирования в России системы налогового мониторинга [распоряжение Правительства РФ от 21.02.2020 № 381-р], целью которой стало определение путей и способов цифровизации налогового контроля на основе применения риск-

ориентированного подхода, позволила налоговым службам на основании доступа к информационным системам налогоплательщика обрабатывать и передавать необходимые документы в налоговые органы и самостоятельно направлять уведомление налогоплательщику. Такой процесс позволяет обеспечить добровольное, своевременное исчисление и уплату налогов, сборов в бюджет, способствует повышению эффективности налогового контроля и снижению административной нагрузки для плательщиков. Что в свою очередь потребовало внесения значимых изменений в область регулирования применения электронной подписи ко всем документам. Особенностями применения усиленной квалифицированной электронной подписи юридических лиц с 2022 г. стало то, что электронная подпись выдается удостоверяющими центрами ФНС России, Казначейства России и Банка России. Особенностями применения усиленной квалифицированной электронной подписи физических лиц являются расширение сферы применения квалифицированного сертификата УКЭП и выдача подписи аккредитованным УЦ. При этом одна и та же УКЭП будет использоваться как для личных целей, так и при выполнении должностных обязанностей на работе в интересах работодателя.

Процессы глобальной цифровой трансформации ставят перед ФНС России задачу дальнейшего развития информационной системы. Налоговая служба разработала концепцию автоматизированной информационной системы (АИС) четвертого поколения «Налог-4» с учетом применения технологий импортозамещения. Разработка концепции АИС «Налог-4» в значительной степени ориентирована на внешнеэкономические сделки.

Системы АСК НДС, АСК ККТ, Единая система маркировки и прослеживаемости товаров, АИС Налог-3, АИС Налог-4 дают возможность государству отслеживать товарные, финансовые потоки хозяйствующих субъектов, снижают административные и организационные издержки всех участников налоговых правоотношений, делают бизнес честным и прозрачным, выравнивают конкурентные условия функционирования бизнеса. Кроме того они позволяют сократить число налоговых проверок, упростить работу налоговых служб, увеличить доходность бюджетов.

В ближайшем будущем автоматизированных систем в сфере налогообложения станет намного больше, разрабатываются и внедряются

АСК Прибыль, АСК ДОМ, АСК ДФЛ. Заканчивается разработка единой платформы «Цифровое государство» в целях автоматизации управления на федеральном и региональном уровнях, а это способ повышения эффективности и решения того количества задач для налогоплательщиков и государства, которые возникают в эпоху цифровых технологий. Переход на новую централизованную технологию налогового администрирования обеспечивает повышение «открытости» налоговых органов для налогоплательщика за счет качества предоставления электронных услуг и расширения их спектра, позволяет увеличить эффективность налогового администрирования, дает снижение общего уровня налоговых нарушений и существенно снижает нагрузку на налоговые органы.

Однако необходимо обратить внимание на проблемы, которые возникают в процессе использования цифровых технологий в налогообложении — это сбои на сайтах, в программах, ведущие к нарушениям сроков в предоставлении налогоплательщиком необходимых отчетных документов, в свою очередь ведущие к сбоям в работе налоговых служб. Кроме того остаются проблемы с созданием, отправлением, доставкой налогоплательщику электронных форм индивидуальных правовых актов, с систематизацией документов, занесением документов в базу данных в электронном виде, с использованием цифрового дублирования электронных подписей налогоплательщиков, а следовательно, с фальсификацией документов. Также остаются проблемы взаимодействия налоговых служб с другими органами государственной власти и пробелы в работе специалистов налоговых служб, требующих высокой квалификации в использовании новых программ. Возможность решения данных проблем в научно-теоретической и практической плоскости обусловливает необходимость адаптации передовой практики цифровых технологий в части внедрения новых стандартов, способов мониторинга операций налогоплательщиков за счет внедрения более эффективных каналов взаимодействия с налогоплательщиками.

Темпы развития цифровых технологий и искусственного интеллекта в налогообложении подтверждают перевод налогообложения полностью в электронный формат, когда все налоговые процессы: регистрация налогоплательщика, учет налоговых обязательств и проверка их исполнения будут протекать в электронном формате, что в

свою очередь позволит в значительной степени облегчить работу как государственных органов, так и налогоплательщиков. Кроме того опыт внедрения цифровых технологий в налоговые правоотношения позволит ускорить процесс выработки перспективных направлений цифровизации налогообложения, которые должны быть закреплены рациональным налоговым законодательством и способствовать созданию рациональной системы налогообложения и достижению такого уровня налоговой дисциплины среди налогоплательщиков и налоговых агентов, при которых минимизируются нарушения законодательства о налогах и сборах.

Липунов Валерий Иванович,
кандидат юридических наук, доцент, доцент кафедры «Транспортное право» Юридического института Российского университета транспорта (МИИТ)

Кочетков Александр Сергеевич,
магистрант Юридического института Российского университета транспорта (МИИТ)

Современные проблемы правового регулирования транспортных отношений в Российской Федерации

Аннотация. В статье на основе применения методик формально-правового анализа рассматриваются актуальные вопросы правового регулирования общественных отношений, образующихся на транспорте и носящих комплексный характер. В работе рассматривается проблема развития работы транспортных организаций, от которых зависит эффективное функционирование всех остальных отраслей экономики и жизнедеятельность государства и общества в целом. Значительное внимание уделяется проблемам обеспечивания транспортных перевозок и транспортной безопасности, представлены некоторые аспекты относительно необходимости привести к созданию единой системы правовых терминологий и механизмов в образовании специалистов на транспорте.

Ключевые слова: транспортное право; транспортная стратегия; транспортный комплекс; отрасль права; система права.

Valery I. Lipunov,
Candidate of Law, Associate Professor, Associate Professor of the Department of "Transport Law" of the Law Institute of the Russian University of Transport

Alexander S. Kochetkov,
Graduate student of the Law Institute of the Russian University of Transport

Modern problems of legal regulation of transport relations in the Russian Federation

Abstract. The article considers topical issues of legal regulation of public relations formed in transport and having a complex character on the basis of the application of methods of formal legal analysis. The paper considers the problem of the development of the work of transport organizations, on which the effective functioning of all other sectors of the economy and the vital activity of the state and society as a whole depend. Considerable attention is paid to the problems of ensuring transport transportation and transport security, some aspects are presented regarding the need to lead to the creation of a unified system of legal terminology and mechanisms in the education of specialists in transport.

Keywords: transport law; transport strategy; transport complex; branch of law; system of law.

В настоящее время транспорт является одним из важнейших компонентов производственной и социальной структуры Российской Федерации. Стратегическая цель развития транспортного комплекса России состоит в удовлетворении спроса экономики и общества на конкурентоспособные и качественные транспортные услуги. Миссия государства в сфере обеспечения функционирования и развития транспортной системы заключается в создании условий для повышения качества жизни и здоровья граждан, экономического роста и повышения конкурентоспособности национальной экономики, укрепления безопасности и обороноспособности страны, реализации ее транспортного потенциала через опережающее развитие транспортной инфраструктуры и расширение доступа к безопасным и качественным транспортным услугам с минимальным воздействием на окружающую среду и климат, использование географических осо-

бенностей Российской Федерации в качестве ее конкурентного преимущества[1].

Выстраивание гармоничной системы правового регулирования транспортных отношений в стране является одной из задач государственного строительства любого современного государства. В связи с их значимостью общественные отношения на транспорте подлежат правовому регулированию, что предопределяет потребность оформления транспортного законодательства и транспортного права как относительно самостоятельных комплексных образований соответственно российского законодательства и права. При этом активно используются средства как публично-правового, так и частноправового регулирования. Принципы, регулирующие транспортное право, содержатся в Конституции РФ, в международных договорах РФ, в федеральных законах, в указах Президента РФ, в постановлениях Правительства РФ и в нормативных правовых актах федеральных органов власти РФ и субъектов РФ.

Среди проблем развития транспортного комплекса Российской Федерации можно назвать недостаточное финансирование, дефицит и климатическая уязвимость транспортной инфраструктуры. В Российской Федерации все еще сохраняется исторически сложившееся отставание в уровне обеспеченности транспортной сетью от развитых стран. При этом развитые страны имели возможность вкладывать в свою транспортную инфраструктуру относительно больше ресурсов, из-за чего при улучшении абсолютной обеспеченности в Российской Федерации нарастает относительное отставание.

Увеличивающаяся с каждым годом интенсивность транспорта приводит к снижению качества транспортного обслуживания населения, которое проявляется в росте затрат времени на перемещение, несоблюдении расписания и интервала движения на маршрутах, снижении уровня культуры вождения и обслуживания пассажиров, безопасности и комфортности перевозок, экологичности услуг, неполном обустройстве остановок транспорта [1, стр. 44].

Одним из важных направлений развития транспортных отношений является обеспечение транспортной безопасности, в том числе и профилактика террористических актов на объектах транспортной инфра-

[1] Транспортная стратегия Российской Федерации до 2030 года с прогнозом на период до 2035 года, утвержденная распоряжением Правительства РФ от 27.11.2021 № 3363-р.

структуры. Из-за высокой уязвимости, в сравнении со многими другими потенциальными целями, объекты транспорта особенно привлекательны для террористов, так как обычно приводят к большому количеству жертв, могут парализовать ключевые секторы экономики и вызвать серьезные общественные потрясения.

Таким образом, изложенное привлекает законодателя к вопросам обеспечения повышения транспортной безопасности, а также комфортности и безопасности транспорта. Одним из основных значение имеет Федеральный закон от 10.12.1995 № 196-ФЗ «О безопасности дорожного движения». Данный Закон включает в свое содержание государственный аппарат, цели, задачи и принципы обеспечения транспортного права, а также обеспечение транспортной безопасности. Закон определяет, что основная задача транспортного права заключается в охране жизни, здоровья и имущества граждан, защиты их прав и законных интересов, а также защиты интересов общества и государства путем предупреждения дорожно-транспортных происшествий, снижения тяжести их последствий. Также закон содержит отсылку к перечню актов, содержащих обязательные требования для соблюдения в сфере транспорта федерального государственного контроля.

В то же время стоит отметить постановление Правительства РФ от 07.10.2020 № 1616 «О лицензировании деятельности по перевозкам пассажиров и иных лиц автобусами». Данный правовой акт определяет порядок лицензирования деятельности по перевозкам пассажиров и иных лиц автобусами. Под лицензируемой деятельностью понимается перевозка пассажиров автобусами лицензиата на основании договора перевозки пассажиров или договора фрахтования транспортного средства (коммерческие перевозки) и (или) перевозки автобусами иных лиц лицензиата для его собственных нужд.

Обратим внимание на то, что данный Закон ведет к наиболее сбалансированной и эффективно функционирующей транспортной системе сообщения, которая стимулирует мобильность населения [2, стр. 54, 33], что влечет за собой выравнивание темпа экономического роста и инновационной привлекательности различных муниципальных образований, которые связываются между собой. Стоит отметить, что вместе с развитием транспортной отрасли повышается культурно-просветительский уровень населения, поскольку именно транспорт обеспечивает доставку населения к основным объектам культурного

наследия страны. Также без транспорта становится практически невозможным создание большого количества общественно-полезных и значимых благ. От состояния, надежности и качества объектов транспортной инфраструктуры и транспортного комплекса в целом зависит экономика города. Кроме того, от комфортности и затраченного времени в пути при проезде на общественном транспорте напрямую зависят умственные и физические силы в месте приложения труда.

В заключении можно сделать вывод, что современные проблемы правового регулирования транспортных отношений разнообразны, требуют комплексного подхода и системных решений. Путь решения этих проблем лежит через дальнейшее совершенствование и развитие транспортного права.

Литература

1. Транспортное право : учебник / Н. А. Духно [и др.]. 3-е изд., пер. и доп. Москва, 2022.
2. Землин, А. И. Организационно-правовые проблемы предупреждения завоза и распространения массовых инфекционных заболеваний на транспорте (на примере пандемии коронавирусной инфекции COVID-19) : монография / А. И. Землин, М. В. Кленов, И. В. Холиков. Москва : РУСАЙНС, 2020.

Матвеева Мария Андреевна,
кандидат юридических наук, доцент кафедры «Транспортное право» Юридического института Российского университета транспорта (МИИТ)

Семенец Виктория Сергеевна,
магистрант Юридического института Российского университета транспорта (МИИТ)

Деятельность открытого акционерного общества «Российские железные дороги» по цифровизации перевозок

Аннотация. На содержание общественного сознания всегда влияли бытие людей, культура их жизненных миров, идеологии и мифы. Ныне одним из

значимых факторов радикальных трансформаций в общественном сознании является цифровизация, которая по существу осуществляет интервенции в индивидуальное сознание, резко меняя «старое» и формируя новое знание об обществе, технике и природе. В представляемом материале приведен анализ деятельности ОАО «РЖД» по вопросам цифровизации перевозок, в том числе касающимся взаимодействия компании с перевозчиками многих других стран. Целью исследования выступает изучение характеристик указанного процесса. Задачи исследования предопределены его целью и сформулированы таким образом, что позволяют рассмотреть некоторые электронные площадки холдинга, документы, разработанные ОАО «РЖД» в данной сфере, изучить процесс создания уникального проекта, с помощью которого могут осуществляться даже интермодальные перевозки. Методология исследования составляют общенаучные (системно-структурный анализ, индукция и дедукция, анализ, синтез, аналогия, сравнение и др.) и частнонаучные методы (метод толкования права, формально-юридический метод). По результатам исследования были сделаны выводы о постоянном повышении эффективности деятельности российских железных дорог в данном вопросе и ускорении развития транспортного комплекса страны.

Ключевые слова: цифровизация; перевозки; безопасность; российские железные дороги; грузовые перевозки; информационное пространство.

Maria A. Matveeva,
Candidate of Law, Associate Professor of the Department of "Transport Law" of the Law Institute of the Russian University of Transport (MIIT)

Victoria S. Semenets,
Master's student of the Law Institute of the Russian University of Transport (MIIT)

Activities of the Open Joint Stock Company "Russian Railways" on digitalization of transportation

Abstract. The content of public consciousness has always been influenced by the existence of people, the culture of their life worlds, ideologies and myths. Nowadays, one of the significant factors of radical transformations in the public consciousness is digitalization, which, in essence, intervenes in individual consciousness, dramatically changing the "old" and forming new knowledge about society, technology and nature. The presented material provides an analysis of the activi-

ties of JSC "Russian Railways" on the issues of digitalization of transportation, including those related to the Company's interaction with carriers of many other countries. The purpose of the study is to study the characteristics of the process. The objectives of the study are predetermined by its purpose and formulated in such a way that they allow us to consider some electronic platforms of the Holding, documents developed by JSC "Russian Railways" in this area, to study the process of creating a unique project with which even intermodal transportation can be carried out. The research methodology consists of general scientific (system-structural analysis, induction and deduction, analysis, synthesis, analogy, comparison, etc.) and private scientific methods (method of interpretation of law, formal legal method). According to the results of the study, conclusions were drawn about the constant increase in the efficiency of the Russian railways in this matter and the acceleration of the development of the country's transport complex.

Keywords: digitalization; transportation; security; Russian railways; freight transportation; information space.

Современный этап развития общественных отношений характеризуется повсеместным внедрением новых принципов и методов управления, базирующихся на возможностях оптимизации деятельности на основе цифровых технологий. В последнее время грузовладельцы предъявляют все более высокие требования к перевозчикам по улучшению качества перевозочного процесса. Как свидетельствует зарубежный опыт, качественного «скачка» в транспортной сфере можно достигнуть лишь за счет использования новых технологий обеспечения процессов перевозок, отвечающих современным требованиям и высоким международным стандартам.

ОАО «РЖД» активно реализует проекты по информационному и цифровому обеспечению международных железнодорожных перевозок. Перевозка начинается с обращения клиента. Для цифровизации этого этапа компания запустила проект по созданию Электронной торговой площадки «Грузовые перевозки» (далее — ЭТП ГП). На ней грузоотправители, грузополучатели, собственники подвижного состава, владельцы терминально-складской инфраструктуры, в том числе морских портов, и другие заинтересованные участники рынка заключают договоры, связанные с осуществлением железнодорожных перевозок. Это значит, что на веб-сайте размещены общие условия ЭТП ГП, являющиеся предложением — офертой, адресованной неограни-

ченному кругу лиц заключить договор на указанных условиях. Когда клиент или поставщик услуг регистрируется в системе, он автоматически акцептует общие условия ЭТП ГП. Тем самым подтверждается заключение договора.

Но избавиться от бумажных документов необходимо не только на этапе заключения договора, но и на стадии собственно перевозки. ЭТП ГП обеспечивает простой доступ к услугам ОАО «РЖД», не обременяя излишними формальностями. За удобным интерфейсом стоит гражданско-правовая конструкция: оцифрованная публичная оферта.

Для решения данного вопроса требуется решить ряд организационных задач. Одна из них — унификация стандартов электронных сообщений. По инициативе ОАО «РЖД» и при его активном участии в рамках Постоянной рабочей группы по кодированию и информатике организации сотрудничества железных дорог (ПРГ КИ) разработаны памятки ОСЖД Р-942 «Технология информационного сопровождения грузовых перевозок по СМГС при электронном обмене данными в стандарте UN/EDIFACT», Р-943 «Библиотека стандартных электронных сообщений для грузовых перевозок в международном сообщении на условиях СМГС в стандарте UN/EDIFACT» и Р-944 «Перечень классификаторов и кодов элементов данных. Библиотека перечней кодов для грузового сообщения на условиях СМГС». Эти документы задают принципы построения единого информационного пространства. Предложенные в них решения помимо ОАО «РЖД» уже применяют перевозчики Финляндии (ВР Карго), Эстонии (ЭВР), Литвы (ЛГ), Латвии (ЛДЗ), Польши (ПКП КАРГО, ДБ КАРГО ПЛ), Германии (ДБ АГ), Белоруссии (БЧ), Украины (УЗ), Азербайджана (ЗАО «АЖД»), Казахстана (АО «НК «КТЖ»), Монголии (АО «УБЖД») и Китая (КЖД). Это в очередной раз доказывает, что важнейшим глобальным вызовом является всеобщая цифровизация [1, стр. 40].

Выработка стандартных решений ведется не только на площадке ОСЖД, но и в Евразийской экономической комиссии (ЕЭК), Международном союзе железных дорог (МСЖД), Международном комитете железнодорожного транспорта (ЦИТ). Компания наладила сотрудничество и с российскими государственными органами.

Другая актуальная задача — организовать в электронном формате совместную работу железнодорожных перевозчиков с таможней.

Компания реализует такой пилотный проект с ФТС России, государственным таможенным комитетом и железной дорогой Беларуси. Его цель — обеспечить применение электронной транзитной декларации. Для этого 6 декабря 2018 г. решением № 29/23 Объединенной Коллегии таможенных служб государств — членов Таможенного союза был принят «Порядок совершения таможенными органами таможенных операций при помещении товаров под таможенную процедуру таможенного транзита и завершении действия такой процедуры на принципах электронного документооборота при перевозке товаров железнодорожным транспортом по маршруту Наушки—Брест».

С марта 2019 г. на этом пилотном маршруте сведения электронной транзитной декларации предоставляются в автоматизированную систему железной дороги Беларуси с применением веб-сервисов. Данный порядок позволяет без применения бумажных документов завершить на территории одного государства — члена ЕАЭС таможенный транзит, открытый в другом государстве-члене. В безбумажном формате возможно осуществлять не только исключительно железнодорожные, но и интермодальные перевозки. Впервые в истории это позволил сделать проект ИНТЕРТРАН. А. В. Колик отмечает, что данный вид перевозок создает выгоду как для грузовладельцев, так и для внутреннего транспорта, где прямая автомобильная перевозка все чаще замещается комбинированной железнодорожно-автомобильной [2, стр. 6].

В рамках проекта ИНТЕРТРАН взаимодействуют оператор морской линии, железнодорожные перевозчики, таможенные органы, грузоотправители и грузополучатели. Алгоритм работы проекта описан в утвержденной ОАО «РЖД» 23 августа 2019 г. информационной технологии «Электронное взаимодействие — дорога» при осуществлении мультимодальной перевозки грузов через порты Дальнего Востока с применением электронных документов и сведений. Она охватывает операции в информационных системах, производимые как автоматически, так и с участием должностных лиц.

Документ затрагивает такие сферы, как оформление транспортных и товаросопроводительных документов в иностранном порту, передача электронных данных в автоматизированную систему Владивостокского морского торгового порта, таможенное декларирование и предоставление электронных транзитных деклараций в автоматизи-

рованные системы ОАО «РЖД», оформление заявок и железнодорожных накладных на перевозку грузов во взаимодействии с АС ЭТРАН и/или ЭТП ГП, электронный документооборот при подаче/уборке вагонов на путях необщего пользования в порту с применением АСУ МР, АСУ Станции и АС ЭТРАН, завершение в электронном виде таможенной процедуры таможенного транзита на станции назначения Российской Федерации с применением АСУ Станции и АС ЭТРАН.

Кстати говоря, первоначально по проекту ИНТЕРТРАН осуществлялись безбумажные интермодальные перевозки грузов из Владивостока на железнодорожные станции Российской Федерации (Силикатная, Кольцово, Ховрино, Новосибирск-Восточный, Базаиха).

18 марта 2020 г. ОАО «РЖД» и железная дорога Беларуси утвердили План совместных мероприятий в рамках проекта ИНТЕРТРАН по маршруту перевозки из портов Китая/Южной Кореи/Японии в порт Владивосток (ВМТП) и далее железнодорожным транспортом по территории РФ назначением в Республику Беларусь.

Чтобы сообщения, передаваемые по электронным каналам, были не просто набором сведений о перевозке, а документами, специалисты ведут работы по внедрению защищенного юридически значимого электронного документооборота. Правовой основой для него являются двухсторонние соглашения о сотрудничестве между центрами сертификации (в случае применения усиленной электронной подписи), о взаимном признании электронных подписей и об осуществлении безбумажных перевозок. К слову, ОАО «РЖД» применяет электронные накладные СМГС в международном сообщении с 2012 г. В течение 2020—2021 гг. ОАО «РЖД» осуществляло защищенный юридически значимый трансграничный электронный документооборот с использованием электронной подписи (ЭП) и технологии «доверенной третьей стороны» (ДТС) в рамках грузоперевозок по безбумажной технологии с железной дорогой Беларуси, АО «НК «КТЖ», ЛДЗ, ЛТГ, АО «УБЖД» и ЭВР.

Компания старается привлечь новых участников к обеспечению юридической значимости электронных накладных путем взаимного признания электронной подписи. Это позволило бы организовать электронный документооборот по всему маршруту Китай — Европа — Китай. Одним из основных препятствий для этого является то, что

в Европейском Союзе не завершена пятая фаза внедрения Новой электронной автоматизированной транспортной системы (NCTS), в рамках которой в Союзе будет поддерживаться полностью безбумажная среда.

Полнофункциональное внедрение системы запланировано к концу 2023 г. Для цифровизации транзита в рамках Совместной рабочей группы по перевозкам контейнерными поездами в сообщении Китай — Европа создана Подгруппа экспертов по информационному взаимодействию (далее — Подгруппа ИВ). В ней по инициативе ОАО «РЖД» принято решение автоматизировать взаимодействие участников перевозки контейнерных грузов в направлении Китай — Европа — Китай с применением технологии «блокчейн», гарантирующей целостность и достоверность передаваемой информации и равноправный доступ на основании согласованных и прописанных правил (политик) между участниками. Стоит согласиться с тем, что цифровизация транспортной деятельности привела к резкому ускорению развития транспортного комплекса страны. Цифровизация оказывает влияние на общество и человека, и все последствия предвидеть весьма и весьма трудно.

Сейчас обсуждается форма документа, который будет определять взаимодействие сторон. В результате каждый из участников транспортного коридора сможет не только повысить эффективность процессов взаимодействия за счет отслеживания проследования отправок в составе международных контейнерных поездов, но и предоставлять сервис по мониторингу исполнения перевозки своим клиентам.

Также стоит упомянуть и о том, что немаловажную роль в процессе цифровизации сыграл Президент РФ. В 2019 г. В. В. Путин в Послании Федеральному Собранию обозначил научно-технологическое развитие страны в качестве приоритета, поручил парламенту принять генеральную схему развития инфраструктуры цифровой экономики, включая сети телекоммуникаций, мощности по хранению и обработке данных. После этого Государственная Дума начала настраивать все законодательство на новую технологическую реальность: оперативно приняла законы, приоритетные для создания правовой среды новой, цифровой экономики, которые позволили заключать гражданские сделки и привлекать финансирование с использованием цифровых технологий, развивать электронную торговлю и сервисы [3, стр. 9].

Литература

1. Попов. Е. В. Умные города : монография / Е. В. Попов, К. А. Семячков. Москва : Издательство Юрайт, 2022.
2. Колик. А. В. Грузовые перевозки: комбинированные технологии : учебник для вузов. — Москва : Издательство Юрайт, 2022.
3. Баукин, А. О. Обеспечение законности в сфере цифровой экономики : учебное пособие для вузов / А. О. Баукин [и др.] ; под редакцией Н. Д. Бут, Ю. А. Тихомирова. Москва : Издательство Юрайт, 2022.

Расулов Алекпер Вагифович,
кандидат юридических наук, доцент, доцент кафедры «Транспортное право» Юридического института Российского университета транспорта (МИИТ)

Фурцева Виктория Алексеевна,
магистрант Юридического института Российского университета транспорта (МИИТ)

Правовые основы защиты интересов открытого акционерного общества «Российские железные дороги» в арбитражных судах

Аннотация. В статье рассматриваются правовые основы защиты интересов в арбитражных судах. Защита прав в арбитражном суде — это юридическая процедура, направленная на защиту прав и интересов предпринимателей или других участников экономической сферы. Существующие проблемы защиты интересов в арбитражных судах вызваны отсутствием в российском законодательстве концептуальных основ механизма защиты правовых интересов в сфере экономической деятельности. Данное обстоятельство не может благоприятным образом сказаться на эффективности судебной защиты и, как следствие, доступности правосудия, укреплении законности и предупреждении правонарушений, являющимися задачами судопроизводства в арбитражных судах. В условиях рыночной экономики отношения, возникающие в процессе функционирования транспортной системы, приобретают особое значение. Поскольку одной из форм социальной активности является транспортная деятельность, а транспорт — одна из важнейших отраслей эко-

номики. Для Российской Федерации этот постулат имеет особое значение: уникальная географическая протяженность Российской Федерации обусловливает повышенную роль транспортной системы.

Ключевые слова: защита интересов; ответчик; арбитражное судопроизводство; форма защиты; судебная защита.

Alekper V. Rasulov,
Candidate of Law, Associate Professor, Associate Professor of the Department of "Transport Law" of the Law Institute of the Russian University of Transport

Victoria Al. Furtseva,
Master's student of the Law Institute of the Russian University of Transport

Legal basis for the protection of the interests of the Open Joint Stock Company "Russian Railways" in arbitration courts

Abstract. The article discusses the legal basis for the protection of interests in arbitration courts. Protection of rights in the arbitration court is a legal procedure aimed at protecting the rights and interests of entrepreneurs or other participants in the economic sphere. The existing problems of protection of interests in arbitration courts are caused by the absence in Russian legislation of the conceptual foundations of the mechanism of protection of legal interests in the field of economic activity. This circumstance cannot favorably affect the effectiveness of judicial protection and, as a result, the availability of justice, the strengthening of the rule of law and the prevention of offenses, which are the tasks of judicial proceedings in arbitration courts. In the conditions of a market economy, the relations arising in the course of the functioning of the transport system acquire special importance. Since one of the forms of social activity is transport activity, and transport is one of the most important sectors of the economy. For the Russian Federation, this postulate is of particular importance: the unique geographical extent of the Russian Federation determines the increased role of the transport system.

Keywords: protection of interests; defendant; arbitration proceedings; form of protection; judicial protection.

На сегодняшний момент процессуально-правовой механизм судебной защиты правовых интересов остается одним из важных правовых институтов, регламентация которого вызывает много нарека-

ний в научном и судейском сообществе. Это определено тем, что законодательная база в данной области характеризуется не только динамикой, но и несогласованностью нормативных правовых источников, сложностью формирования единой судебной практики и противоречием позиций судебных органов при разрешении споров, затрагивающих правовые интересы.

Защита прав в арбитражном суде — это юридическая процедура, направленная на защиту прав и интересов предпринимателей или других участников экономической сферы. Согласно ст. 59 АПК РФ физические и юридические лица могут вести дело как лично, так и через адвоката.

Под формой защиты прав принято понимать юридическую деятельность по защите субъективных прав, комплекс согласованных организационных мероприятий, протекающих в рамках одного правового режима.

Во многом аналогичные проблемы вызваны отсутствием в российском законодательстве концептуальных основ механизма защиты правовых интересов в сфере экономической деятельности. Данное обстоятельство не может благоприятным образом сказаться на эффективности судебной защиты и, как следствие, доступности правосудия, укреплении законности и предупреждении правонарушений, являющихся задачами судопроизводства в арбитражных судах.

Также недопустимы пробелы законодательного регулирования, нормативных правовых актов и многочисленные юридические коллизии.

В условиях рыночной экономики отношения, возникающие в процессе функционирования транспортной системы, приобретают особое значение. Поскольку продукция транспорта как отрасли материального производства — это деятельность по территориальному перемещению грузов или людей, постольку транспорт является связующим звеном экономики страны, охватывающим все виды общественного производства, распределения и обмена. Транспортные отношения находятся в тесной связи с другими социально-экономическими отношениями, что во многом определяет их природу.

Транспортная деятельность — одна из форм социальной активности. По содержанию транспортная деятельность представляет собой физическое перемещение каких-либо объектов.

Транспорт — одна из важнейших отраслей экономики. Процесс товарного обмена в современном обществе немыслим без транспорта. Для России этот постулат имеет особое значение: уникальная географическая протяженность России обусловливает повышенную роль транспортной системы.

Наличие одной из самых протяженных железных дорог в мире вызывает необходимость тесного сотрудничества с соседними странами на двусторонней основе и на уровне международных организаций, таких как Организация сотрудничества железных дорог (ОСЖД) и Евразийского экономического союза (ЕАЭС).

Следует особо выделить тесное сотрудничество России с Китайской Народной Республики на двусторонней основе и в рамках стран БРИКС, например российско-китайское сотрудничество в области науки регулируется Меморандумом о сотрудничестве в области науки, технологий и инноваций между Правительством Федеративной Республики Бразилия, Правительством Российской Федерации, Правительством Республики Индия, Правительством Китайской Народной Республики и Правительством Южно-Африканской Республики (Меморандум БРИКС) 2015 г.

Наглядным примером всему этому является также толкование процессуальных норм, регламентирующих участие ОАО «РЖД» в арбитражном судопроизводстве.

ОАО «РЖД» — это современный транспортно-логистический комплекс, имеющий стратегическое значение для Российской Федерации, а также одна из самых крупных компаний в мировом транспортном секторе, осуществляющая напрямую деятельность в сфере железнодорожных перевозок. Компания обеспечивает активную хозяйственную деятельность промышленных предприятий, обеспечивает доступный транспорт для миллионов граждан и представляет собой связующее звено в единой экономической системе России.

ОАО «РЖД» оказывает полный спектр услуг в таких сферах, как грузовые перевозки, предоставление услуг локомотивной тяги и инфраструктуры; ремонт подвижного состава; пассажирские перевозки в дальнем и пригородном сообщении; контейнерные перевозки, логистические, инжиниринговые услуги; научно-исследовательские и опытно-конструкторские работы; а также прочие виды деятельности.

Компании ОАО «РЖД» зачастую приходится выступать в арбитражном суде в качестве ответчика. Существует основное отличие

права на судебную защиту от точно такого же права истца — это «специфичные» средства защиты «ответчика». Эта специфичность заключается в том, что средствами защиты правовых интересов ответчика являются возражения, встречный иск или же самое простое — отрицание иска. Данные средства могут привести к прекращению судопроизводства по иску или участию лица в качестве ответчика в таком производстве, к полному или частичному отказу истцу в иске или освобождению от его удовлетворения, к созданию удобных для ответчика условий удовлетворения исковых требований. Защита ответчика осуществляется в условиях искового производства, в основе которого лежит правовой конфликт сторон, при этом складывающиеся отношения обладают двумя существенными особенностями — они возникают в сфере правовых отношений и разрешаются по специальным правилам гражданского и арбитражного судопроизводства. Данные особенности определяют специфику защиты ответчика: объем доступных средств защиты, использование их в условиях стадийной, строго регламентированной законодательством процедуры разрешения конфликта судом [1, стр. 234].

Групповые иски также могут быть «полезны» ответчикам во избежание их участия во многих однотипных делах, предъявленных к ним, а сосредоточиться на подготовке к одному процессу.

Несомненным плюсом группового производства также является и снижение нагрузки с судов, экономии временных ресурсов и посвящении одному групповому производству вместо тех же многочисленных однотипных индивидуальных споров, таким образом перейдя с количества в качество.

Актуальность исследования правовых особенностей защиты интересов ОАО «РЖД» в арбитражном суде обусловлена обстоятельствами, среди которых можно выделить следующее:

— вопрос обеспечения ответчику гарантий его прав является одним из наиболее деликатных, требующих соблюдения баланса интересов сторон спора;

— важность самого объекта исследования: эффективность судебной защиты является показателем демократичности государства, позволяет дисциплинировать договорные отношения, разрешать споры, содействовать укреплению законности и предупреждению правонарушений в сфере экономической деятельности;

— постоянное совершенствование и развитие законодательства, направленное на обеспечение доступности правосудия и эффективности защиты прав и интересов.

Влияние на деятельность ОАО «РЖД» также оказала пандемия короновируса QOVID-19, как показывает опыт борьбы с эпидемиями, при должной организации работы объекты транспортной инфраструктуры могут быть эффективно использованы для осуществления профилактики инфекции, организации карантинных мероприятий и первичной помощи зараженным. Использование средств общественного транспорта в указанных целях также представляется весьма перспективным. В частности, для оказания помощи в проведении профилактических мероприятий, оказания медицинской помощи жителям отдаленных районов и т.п. представляется вполне применимым опыт использования для борьбы с чумой, холерой, иными инфекционными заболеваниями, санитарных поездов, судов, мобильных санитарных летучек, размещаемых на автомобильном транспорте, укомплектованных специалистами различного профиля, необходимым оборудованием и инвентарем.

Изложенные положения подтверждают актуальность, практическую значимость исследования и предопределяют необходимость всестороннего изучения судебной защиты правовых основ и интересов ОАО «РЖД».

До настоящего момента не сформировалось единой позиции относительно цели защиты ответчика против иска, а также круга и правовой природы способов и форм защиты, которые могут быть использованы для достижения цели.

Недостаточно изучены различные тактики защиты ответчика против иска. Не в должной мере реализован потенциал сравнительно-правового метода при изучении участия ответчика в процессе осуществления правосудия.

Стоит обратить внимание, что изначально групповые иски в российском праве были введены в АПК РФ и охватывали только те споры, которые имели экономический характер, а также подразумевали более «сильных» участников процесса, в то время как в тех же европейских странах, имеющих более длительную историю групповых исков, данный институт был внедрен как раз с целью защиты прав более незащищенной категории населения против могучих корпора-

ций, что может говорить о том, что изначально в Российской Федерации по аналогии стоило бы вводить групповые иски изначально в гражданское производство, которое распространяется на такие максимально вбирающие по количеству участников споры, как трудовые, о защите прав потребителей и др., что позволило бы на данном этапе уже сформировать обширную практику и усовершенствовать процессуальное законодательство.

Таким образом, изложенное определяет необходимость проведения дополнительных теоретических изысканий, анализа состояния правового регулирования и судебной практики в данной сфере, а также обусловливает актуальность данной темы исследования.

Литература

1. Максимов, В. А. К вопросу о соотношении понятий «законный интерес», «охраняемый законом интерес», «правовой интерес», «юридический интерес» // Правда и закон. 2017. № 2. С. 25—28.

Аль Али Насер Абдель Рахим,
кандидат юридических наук, доцент кафедры «Морское право» Юридического института Российского университета транспорта (МИИТ)

Международно-правовое регулирование применения технологии блокчейн и смарт-контракт на морском транспорте

Аннотация. В статье анализируется потенциальное влияние технологии блокчейн и смарт-контрактов на судоходную отрасль. Поскольку судоходная отрасль представляет собой сложную систему различных действий, которые необходимо контролировать и регистрировать, технология блокчейн может служить инструментом, позволяющим оптимизировать многочисленные процессы в этой области, в то же время исключение человеческого фактора из множества элементов является проблемой. Поэтому автор сначала показывает, как работает технология блокчейна и раскрывает сущность смарт-контрактов, чтобы дать представление об их применимости в секторе судоходства. После общего обзора технологических и правовых характеристик технологии блокчейн и смарт-контрактов автор демонстрирует примеры их

применения в судоходной отрасли. Помимо преимуществ блокчейн-технологий автор также указывает на существующие недостатки, которые до сих пор затрудняют применение технологии блокчейн в правоотношениях в судоходной отрасли. Основываясь на этих выводах, автор освещает текущие разработки в этой области и представляет существующие и ожидаемые реформы регулирования блокчейн-решений и смарт-контрактов в морском транспорте.

Ключевые слова: блокчейн; смарт-контракты; судоходная отрасль; контракты на отгрузку; чартерная партия.

Al Ali Naser Abdel Raheem,
PhD in Law, Associate Professor of the Department of Maritime Law of the Law Institute of the Russian University of Transport

International legal regulation application of blockchain technology and smart contract in maritime transport

Abstract. The article analyzes the potential impact of blockchain technology and smart contracts on the shipping industry. Since the shipping industry is a complex system of various activities that need to be controlled and recorded, blockchain technology can serve as a tool to optimize numerous processes, while at the same time, eliminating the human factor from many elements is a challenge. Therefore, the author first introduces how blockchain technology works and reveals the essence of smart contracts to give an idea of their applicability in the shipping sector. After a general overview of the technological and legal characteristics of blockchain technology and smart contracts, the author presents examples of their application in the shipping industry. In addition to the advantages of blockchain technologies, the author also points out the existing shortcomings that still hinder the use of blockchain technology in legal relations in the shipping industry. Based on these findings, the author highlights current developments in this area and presents existing and expected regulatory reforms for blockchain solutions and smart contracts in maritime transport.

Keywords: blockchain; smart contracts; shipping industry; shipment contracts; charter party.

Введение. В современных условиях участники морского транспорта все чаще стали пользоваться и внедрять технологии блокчейна

и смарт-контракты в судоходной отрасли. Правовое регулирование применения технологии блокчейна и смарт-контрактов на морском транспорте стало предметом широко распространенных правовых споров по определению смарт-контрактов, их содержанию и т.д.

Вопросу технологии блокчейна и смарт-контрактов посвящены различные научные работы в виде статьей, монографий, диссертаций как зарубежных и российских ученых-теоретиков, так и практикующих специалистов в этой сфере. Несмотря на это, единообразного подхода к данной проблеме нет, и к сожалению, во многих странах отсутствует четкое правовое регулирование применения технологии блокчейн и смарт-контрактов в различных сферах, в том числе и на морском транспорте.

Цель данного исследования — выяснить сущность технологии блокчейн, определить правовую природу смарт-контрактов и их содержание, условия их применения в судоходной отрасли, а также выяснить, способны ли действующие нормативные акты регулировать правовые отношения, вытекающие из их использования в судоходной отрасли.

Методологическая основа исследования — методы анализа, обобщения, научной абстракции, сравнительно-правовой, технико-юридический и метод толкования.

Сущность технологии блокчейн и ее применение на морском транспорте. Когда кто-то упоминает блокчейн или смарт-контракты, большинство людей сразу же думает о виртуальных валютах, таких как биткойн, лайткойн или эфир. Это связано с тем, что технология блокчейн и смарт-контракты, какими мы их знаем сегодня, произошли от виртуальных валют. Однако технология блокчейн и смарт-контракты постепенно начинают использоваться в других областях, таких как страхование, строительство, фондовые рынки, банковское дело и, конечно же, судоходная отрасль. Судоходная отрасль из-за своей сложности и существенной ценности для мирового рынка находится в самом центре адаптации блокчейн и смарт-контрактов к их способу функционирования.

Наша задача как исследователей в области юриспруденции — проанализировать внутреннюю работу блокчейн и смарт-контрактов, где они могут использоваться (или уже используются) в судоходной отрасли между юридическими лицами, которые находятся на террито-

рии разных государств и определить существующие правила или правовые нормы, которые могут применяться к блокчейн и смарт-контрактам в судоходной отрасли. Затем на основе проведенного анализа разработать и принять специальные правовые акты на национальном и международном уровнях для правового регулировании блокчейн и смарт-контрактов в судоходной отрасли, что могло бы помочь в их общем применении с целью снижения затрат, экономии времени и в целом повышения эффективности и обеспечения безопасности судоходной отрасли.

Прежде чем сформулировать понятие блокчейн, мы должны подчеркнуть, что общепринятого определения не существует. Но в доктрине уже сформировался довольно широкий спектр определений, в которых автор рассматривает блокчейн с разных сторон.

Атоши Накамото (создатель биткойна) определяет биткойн как «цепочку цифровых подписей, записанных распределенным сервером меток времени в криптографически защищенном регистре, называемом цепочкой блоков» [7, стр. 1174].

Marko Perkušića и соавторы определяют блокчейн как «распределенную базу данных, которая совместно используется и согласовывается с одноранговой сетью. Он состоит из связанной последовательности блоков, содержащих транзакции с отметками времени, которые защищены криптографией и проверены сетевым сообществом. Как только элемент добавлен к цепочке блоков, его нельзя изменить, превращая цепочку блоков в неизменяемую запись прошлой активности» [5, стр. 366].

В. Прохоров дает следующее определение: «блокчейн — это технология, в которой происходит передача информации посредством цепочек блоков, где каждый из них содержит информацию о предыдущем блоке» [1].

Из этих определений мы можем отметить, что основными характеристиками блокчейна являются следующие:

• это распределенная база данных (данные не хранятся в одном месте, а рассредоточены по сети взаимосвязанных компьютеров);

• блокчейн совместно используется и согласовывается между одноранговыми сетями (одноранговые узлы образуют одноранговую сеть и являются равноправными участниками, которые позволяют сети функционировать для всех участников без необходимости цен-

тралізованной координации, и они это делают, позволяя своим компьютерам выполнять задачи, требуемые сетью);

• блокчейн состоит из связанной последовательности блоков (записи в цепочке блоков хранятся в блоках, которые содержат данные и связаны друг с другом посредством криптографической аутентификации, называемой хэшированием, которое затем формирует цепочку блоков);

• блокчейн использует метки времени (точки данных, которые показывают, когда каждый блок был подключен в хронологическом порядке и он защищен от несанкционированного доступа);

• блокчейн защищен криптографией (система, которая связывает блоки вместе и обеспечивает безопасную передачу и обмен цифровыми данными децентрализованным способом);

• проверяется сетевым сообществом (централизованного органа не существует, но вся проверка выполняется одноранговыми узлами);

• блокчейн нельзя изменить (чтобы изменить существующие данные в цепочке блоков, нужно было бы сделать это задним числом и изменить все последующие блоки. Чтобы сделать это, нужно было бы иметь консенсус большинства сети).

Смарт контракт. Идея смарт-контракта была создана Ником Сабо (ученый в области информатики, криптографии, а также в области права, известный в связи с исследованиями в области умных контрактов и криптовалюты). В 1994 г. он определил смарт-контракт как «компьютеризированный протокол транзакций, который выполняет условия контракта» [8]. Тем не менее первая система смарт-контрактов была создана в 2014 г. на платформе *Ethereum* с использованием криптовалюты *Ehter* и функций с технологией публичного блокчейна.

На данный момент с юридической точки зрения нет единого определения смарт-контракта.

Несмотря на то что это называется смарт-контрактом, с юридической точки зрения мы считаем, что смарт-контракты в первую очередь не являются контрактами или формами контракта, а обычно являются способом реализации или исполнения контракта. Подтверждение этому служит определение смарт-контракта Хорватского ученого, согласно которому смарт-контракты можно определить как «способ выполнения условий, на которые соглашаются две или более

сторон, чтобы они могли выполнять, используют компьютерный код, расположенный в сети блокчейна» [5, стр. 367].

В качестве ключевых преимуществ смарт-контрактов указывается, что они:

1) снижают риски, поскольку сохраняются в неизменной цепочке блоков;

2) сокращают расходы на администрирование и обслуживание, поскольку автоматизация заменяет необходимость в посреднике или центральном брокере;

3) повышают эффективность бизнес-процессов, исключив из них посредников.

Возможности применения блокчейна и смарт-контрактов в морском транспорте. Современная судоходная отрасль представляет собой сложное объединение различных видов деятельности, субъектов бизнеса. В качестве примера можно использовать рынок танкерных перевозок и контракты, связанные с этой сферой. В типичном перемещении наливных грузов (жидкие грузы) из одного порта в другой участвуют несколько лиц, а именно:

• грузоотправитель (поставщик) — занимается экспортом товара, который он произвел или приобрел у производителя;

• грузополучатель (получатель) — импортер товара;

• портовые терминалы — облегчают погрузку и разгрузку, операции на борту корабля;

• портовые власти — управляют судами в своих водах и несут ответственность за их безопасное плавание;

• трейдеры — торговцы, действующие по собственной инициативе и стремящиеся извлечь прибыль непосредственно из процесса торговли. Находят разрывы между спросом и предложением и торгуют этим товаром, чтобы получить прибыль;

• фрахтователи — физическое или юридическое лицо, получившее по договору фрахтования право за установленную плату перевезти морем определенный груз на зафрахтованном судне или его части. Занимаются логистикой перемещения товаров для трейдеров и часто являются частью той же организации, что и трейдеры;

• судовладелец — юридическое или физическое лицо, эксплуатирующее судно от своего имени. Судовладелец не обязательно является владельцем судна, им может быть лицо, эксплуатирующее судно на основании договора с собственником;

• брокеры — посредники между фрахтователями и судовладельцами;

• портовые агенты — это комплекс услуг, которые компания-агент оказывает собственнику или арендатору судна или груза, получателю, страхователю, фрахтователю груза в определенном порту. Это местные представители фрахтователей и судовладельцев, которые помогают с логистикой и связью в каждом порту.

Понятно, что между всеми этими лицами возникают различные договоры, но в качестве наиболее важного договора можно выделить чартер-партию, которая представляет собой договор между судовладельцем и фрахтователем на перевозку товара морем.

Весь процесс начинается с того, что трейдер заключает сделку с грузоотправителем (поставщиком) и грузополучателем (получателем), а затем дает задание фрахтователю организовать отгрузку этого товара. Фрахтователь связывается со своими брокерами и сообщает им данные о грузе, который необходимо перевезти. Затем брокеры ищут доступное судно, которое может перевозить этот груз. Найдя подходящее судно, брокеры соединяют стороны, которые затем начинают договариваться об условиях перевозки. Если они могут договориться об условиях контракта, они подписывают контракт физически или по электронной почте. После заключения договора судно перевозит груз в согласованный порт и выполняет свои обязательства по договору. Если все условия контракта соблюдены судовладельцем, фрахтовщик осуществляет перечисление денежных средств, и таким образом контракт выполняется с обеих сторон.

Как мы видим из примера, процесс перемещения груза из точки А в точку Б требует большого количества посредников, бумажной волокиты, времени и денег. В качестве основных проблем можно выделить следующие:

• пустая трата времени, пока все эти юридические лица найдут друг друга;

• медленные переговоры об условиях контракта;

• высокая стоимость посредников;

• обширная документация, поддерживающая связь между несколькими договаривающимися сторонами, которые общаются по нескольким каналам;

• плохое управление документами (некоторые документы, такие как коносамент, по-прежнему должны быть доставлены получателям

груза в оригинале, что в прошлом часто приводило к задержкам в случаях, когда оригинал коносамента не был получен вовремя);

• постоянная необходимость быть в сети, чтобы находить клиентов и отслеживать тенденции рынка;

• медленные международные денежные переводы, которые доставляются в течение нескольких дней.

Поэтому многие заинтересованные стороны (компании, страны, порты, государственные органы) пытаются найти решения этих проблем за счет применения блокчейн и смарт-контракта в судоходной отрасли.

Большой прорыв в области блокчейн-решений в судоходной отрасли произошел в 2017 г., когда судоходный гигант *Maersk* и его партнеры (*IBM, Schneider Electronic* и др.) объявили, что у них есть блокчейн-решение для оцифровки глобальной торговли. Описав преимущества блокчейн, *Maersk Group* считает, что блокчейн может сократить расходы на администрирование и обработку физических документов, остановить мошенничество, особенно на неразвитых рынках, а также кибератаки. После *Maersk Group* другие важные участники судоходной отрасли (например, *Hyundai Merchant Marine, Samsung SDM, Mitsui OSK Lines* и др.) начали искать собственные блокчейн-решения [1].

В результате такого большого интереса появляются решения, основанные на блокчейн и смарт-контрактах, — это:

• более эффективная система обмена информацией между фирмами;

• упрощение бумажного процесса и бумажного документооборота;

• противодействие грузовому мошенничеству;

• улучшение эффективности использования контейнеров;

• экономия средств и времени на перевозку груза.

Большинство из вышеперечисленных решений в основном основаны на блокчейн, но есть аспекты судоходной отрасли, где и смарт-контракты могут играть очень важную роль.

Например, смарт-контракты на основе блокчейн можно использовать для того, чтобы:

• отслеживать коносамент и автоматизировать денежные переводы;

• заключать договоры чартера;

• инициировать перевод средств между судовладельцем и фрахтователем;

• рассчитывать аренду и демередж (простои) на основе заранее определенной формулы.

Еще один интересный подход к внедрению блокчейн-решений в судоходной отрасли предлагает гонконгский стартап 300Cubits. 300Cubits пытается запустить собственную криптовалюту (на основе блокчейн) для судоходной отрасли, которая будет использоваться в качестве депозита. В процессе бронирования, т.е. если грузоотправитель не явится с грузом, он потеряет свой залог, а контейнерная линия или компания — грузоперевозчик потеряет свой залог, если она не загрузит груз в соответствии с соглашением.

Сложности применения блокчейн и смарт-контрактов в судоходной отрасли. Использование упомянутых решений порождают многие сложности. В качестве основных факторов, по которым существующие решения не получили широкого распространения, можно выделить следующие:

• блокчейн-приложения все еще не настолько просты в использовании и недостаточно дешевы, чтобы вносить изменения в существующую систему;

• для надлежащего функционирования решений на основе блокчейн требуется более широкое использование, что, в свою очередь, означает, что различные заинтересованные стороны должны будут присоединиться к широкому консорциуму, однако решения на основе блокчейн еще не достигли того уровня экономической эффективности, чтобы форсировать создание такого консорциума;

• по-прежнему существует множество экономических, технологических и правовых барьеров, которые необходимо полностью устранить, прежде чем решения на основе блокчейн станут общепринятыми в судоходной отрасли.

Роль Международной морской организации (ИМО) в разработке и принятия международных правовых норм, стандартов и правил по применению блокчейн и смарт-контрактов в судоходной области. ИМО является специализированным учреждением Организации Объединенных Наций и отвечает за безопасность судоходства, за предотвращение загрязнения морской и атмосферной среды международного судоходства, которое перевозит более 80% мировых

грузов. Основной целью ИМО является создание эффективной нормативно-правовой базы (через конвенции) для судоходной отрасли, которая может быть принята и внедрена повсеместно. Конвенции, за которые отвечает ИМО, можно разделить на четыре категории:

• безопасность на море;

• предотвращение загрязнения моря;

• ответственность и компенсация (особенно в отношении ущерба, причиненного загрязнением);

• другие соглашения, касающиеся, например, измерения тоннажа, незаконных действий против судоходства и спасения и т.д. [6]

Из вышеизложенного можно сделать вывод, что меры ИМО охватывают множество аспектов международного судоходства, но процесс заключения договоров между юридическими лицами, а также применение новых технологий в судоходной отрасли во многом регулируются правилами и законами рынка, а ИМО конвенциями не углубляется в эту область. Но необходимо расширить полномочия ИМО как учреждения, которое возьмет на себя ведущую роль в регулировании блокчейн и смарт-контрактов в судоходной отрасли.

Регулирование блокчейна и смарт-контрактов в Европейском Союзе (ЕС). Европейский Союз осознал важность морской торговли, Европа является одним из ведущих морских центров мира (на ее побережье расположено 329 ключевых морских портов). Поэтому неудивительно, что ЕС создал обширную законодательную базу для обеспечения безопасности, защиты окружающей среды и качественного судоходства.

Европейский парламент и Совет ЕС приняли Директиву 2010/65/ЕС о формальностях отчетности для судов, прибывающих в порты государств-членов и/или отбывающих из них. Данная Директива создала среду, позволяющую централизованно предоставлять информацию в цифровом виде путем создания морского «единого окна», также она включает в себя довольно большое количество органов, включая транспорт, таможню, пограничный контроль, безопасность, здравоохранение и окружающую среду [4].

В 2017 г. министры транспорта ЕС приняли декларацию по морскому праву, так называемую Валлеттскую декларацию европейских министров, ответственных за комплексную морскую политику, о голубом росте. Данная декларация выступает в качестве важной основы

для подготовки стратегии развития судоходной отрасли ЕС в течение следующего десятилетия.

Учитывая огромный потенциал для оптимизации технических и эксплуатационных аспектов морского сектора, включая административное упрощение, в п. 19 данной декларации подчеркивается важность цифровизации. Декларация также призывает к необходимости более эффективного использования имеющихся данных и информации путем содействия обмену информацией и обращает внимание на его преимущества, такие как предотвращение дублирования усилий и снижение административной нагрузки, а также использование существующих инструментов для сбора и обмена данными между государствами — членами ЕС [2].

Подчеркивая необходимость полностью согласованного интерфейса и стандартизированного максимального набора данных, включая информацию, необходимую для управления портом и портовыми терминалами, все представленные меры показывают, что ЕС уделяет большое внимание модернизации и цифровизации судоходной отрасли в целом.

Однако помимо общего регулирования процесса цифровизации в судоходной отрасли, ЕС также предпринял значительные шаги в регулировании виртуальных валют. В 2018 г. ЕС принял Директиву о предотвращении отмывания денег и финансирования терроризма В ней дано определение «виртуальная валюта» — это средство обмена, принимаемое физическими или юридическими лицами, которое может передаваться, храниться и продаваться в электронном виде и которое не выпускается и не гарантируется центральным банком или государственным органом [3].

Такая виртуальная валюта имеет значение в контексте регулирования судоходства в тех случаях, когда контракты на доставку структурированы на основе решений блокчейна или смарт-контрактов, которые используют виртуальную валюту в качестве средства обмена или страхования.

Однако упомянутая директива не регулирует сам блокчейн или смарт-контракты не потому что ЕС не знает о потенциале технологии блокчейн, а скорее из-за того, что она еще на ранней стадии и не определено направление, в котором эта технология может развиваться в будущем.

Европейская комиссия считает блокчейн новой технологией, которая позволяет большим группам людей или организациям, независимо от уровня доверия между ними, коллективно согласовывать и постоянно записывать информацию без необходимости использования стороннего органа. Комиссия осознает потенциальную ценность этой технологии и подошла к технологическим разработкам, касающимся блокчейн и смарт-контрактов, путем создания широкой стратегии блокчейн ЕС, предусматривающей создание европейского блокчейн-партнерства, а также продвижение правовой определенности и установление стандартов функциональной совместимости.

Среди прочего Европейская комиссия и другие европейские органы создали многочисленные экспертные группы и подразделения, такие как подразделение цифровых инноваций и блокчейн, которое управляет инициативой *Startup Europe* и *Innovation Radar*. В сочетании с уже упомянутыми усилиями по модернизации судоходной отрасли и созданию общеевропейской структуры в этой области можно ожидать, что ЕС будет в авангарде регулирования и реализации интеграции блокчейн в секторе судоходства.

Заключение. Из приведенных выше соображений можно сделать вывод, что на данный момент еще нет определенности в правовом регулировании блокчейн и смарт-контрактов в судоходной отрасли. Это связано с тем, что в настоящее время не ясно, как будет спроектирована новая система, прежде чем она сможет полностью заменить существующую организацию судоходной отрасли, а также отсутствует ясность в отношении блокчейн из-за общего отсутствия судебной практики в понимании его поведения, какие субъекты будут вовлечены в систему, каковы будут их права и обязанности и как будет разработана система проверки. Хотя у нас есть некоторые индикаторы, показывающие, что заинтересованные стороны будут основными движущими силами технологий, этого недостаточно, чтобы представить всю правовую базу. Кроме того, роли всех участников будут сильно зависеть от технической осуществимости определенных решений и конкретных договоренностей между вовлеченными сторонами. Поэтому еще рано выявлять необходимые факты для создания качественной нормативно-правовой базы, при этом лучше дождаться развития системы, чем действовать преждевременно, зарегулировав эту сферу, тем самым препятствуя ее развитию.

Поведение блокчейн требует, чтобы законодатели сосредоточили внимание не только на технологии или приложениях, но и на тех, кто взаимодействует с ними или полагается на них (разработчики, дизайнеры, пользователи, потребители, поставщики данных, менеджеры данных и т.д.).

В настоящее время смарт-контракты и реестры на основе блокчейн не могут действовать автономно. Наоборот, необходим высокий уровень гибридизации, чтобы преодолеть разрыв, прежде всего, между технологическими устремлениями и правовыми (имущественными, договорными и т.д.) нормами и культурами. Это означает, что смарт-контракты работают в тандеме с онлайн-и офлайн-, а также внутри- и в нечейн-транзакционными модальностями. Кроме того, это означает, что реестры на основе блокчейн действуют как традиционные базы данных или аналогичные электронные архивы, а не заменяют их. Как следствие, важные новые законы и правила, адаптированные к смарт-контрактам и реестрам на основе блокчейн, еще не появились. Однако от законодателей и ученых требуется разработать правила и принципы, лежащие в основе создания качественной нормативно-правовой базы для регулирования блокчейн и смарт-контрактов на морском транспорте.

Литература

1. Владимир Прохоров. Применение технологии Блокчейн и Смарт-контракт в морских перевозках // http://www.logistika-prim.ru/articles/primenenie-tehnologiy-blokcheyn-i-smart-kontrakt-v morskih-perevozkah (дата обращения: 20.05.2022).
2. Declaration of the European Ministers responsible for the Integrated Maritime Policy on Blue Growth // https://data.consilium.europa.eu/doc/document/ST-8037-2017-INIT/en/pdf (дата обращения: 20.05.2022).
3. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance) PE/72/2017/REV/1, OJ L 156, 19.6.2018.
4. European Commission Directorate-General for mobility and transport Directorate D — Logistics, maritime & land transport and passenger rights D.1 — Maritime transport & logistics National Single Window

Guidelines, from April 17th 2015, available under https://ec.europa.eu/transport/sites/transport/files/modes/maritime/doc/2015-06-11-nswguidelines-final.pdf (дата обращения: 20.05.2022).
5. Marko Perkušić, Šime Jozipović, Damir Piplica.(2020): The Need for Legal Regulation of Blockchain and Smart Contracts in the Shipping Industry, Transactions on Maritime Science, Vol. 09 No. 02.
6. Международная морской организация. http://www.imo.org/en/About/Pages/Default.aspx (дата обращения: 22.05.2022).
7. Pflaum, I., Hateley, E. (2014): A bit of a problem: National and extra-territorial regulation of virtual currency in the age of financial disintermediation, Georgetown Journal of International Law, vol. 45.
8. The fine print in smart contracts, NBER Working Paper Series, Working Paper 25443, available at: http:// www.nber.org/papers/w25443 (дата обращения: 24.05.2022).

Романов Александр Владимирович,
магистрант Юридического института Российского университета транспорта (МИИТ)

Правовое регулирование мультимодальной перевозки грузов в России и за рубежом

Научный руководитель — кандидат юридических наук, доцент В. В. Смирнова.

Аннотация. В представленной статье автор акцентирует внимание на проблемах, связанных с мультимодальными перевозками. Рассматривается правовое регулирование мультимодальной перевозки в России, США, Германии и в Сингапуре. Выделяются перспективные решения и недостатки правового регулирования, которые рекомендуется учитывать при подготовке проекта нормативного акта, посвященного мультимодальным перевозкам.

Ключевые слова: транспорт; мультимодальные грузоперевозки; международный опыт; нормативный акт.

Alexander V. Romanov,
Master's student of Law Institute of Russian University of Transport

Scientific adviser — Ph.D. Sc., Associate Professor Vera V. Smirnova

Legal regulation of multimodal transportation of goods in Russia and abroad

Abstract. In the presented article, the author focuses on the problems associated with multimodal transportation. It examines the legal regulation of multimodal transportation in Russia, the USA, Germany and Singapore. Promising solutions and shortcomings of legal regulation are highlighted, which are recommended to be taken into account when preparing a draft regulatory act on multimodal transportation.

Keywords: transport; multimodal cargo transportation; international experience; normative act.

В условиях постоянно развивающейся экономики как в мире, так и в отдельно взятых странах, технического прогресса и усиливающейся глобализации транспорт играет ключевую роль. Именно перевозки являются связующим звеном между различными аспектами экономики той или иной страны, создавая возможность беспрепятственного товарообмена. Сегодня в условиях роста необходимости в быстрых, универсальных решениях на рынке перевозок явным фаворитом являются мультимодальные и комбинированные перевозки. Первые позволяют наиболее эффективно обеспечить доставку груза «от двери до двери», а вторые позволяют значительно сократить время доставки за счет перевозки груза в одной транспортной единице (контейнере, вагоне и др.). Несмотря на растущую популярность таких перевозок, на сегодня нет единого понимания мультимодальных перевозок грузов в рамках правового поля. Предлагается рассмотреть различные подходы правового регулирования мультимодальных перевозок на примере России, США, Германии и Сингапура.

В российском праве определение мультимодальных перевозок впервые было зафиксировано в ГОСТ Р 52297-2004. Под мультимодальными перевозками понимались такие перевозки, которые сопровождались одним экспедитором на всем пути следования груза (от пункта отправления до места назначения) транспортом различных видов. Ответственность за повреждение, недостачу и утрату груза в таких перевозках несет экспедитор. На весь путь следования груза оформляется единый транспортный документ (договор). На момент принятия ГОСТ термин «мультимодальная перевозка» нигде закреп-

лен не был. В ст. 788 Гражданского кодекса Российской Федерации (далее — ГК РФ) содержится определение перевозок в смешанном сообщении, что отождествляется с комбинированными перевозками. Данный термин, следуя содержанию нормы, должен в себя включать как мультимодальные перевозки, так и иные перевозки, осуществляемые несколькими видами транспорта по единому транспортному документу и (или) осуществляемые единым транспортным перевозчиком (единым оператором). ГК РФ предоставляет нам общее понятие договора перевозки, без распределения на отдельные виды транспорта, не создавая одно универсальное понятие, подходящее для всех видов транспорта. Для того чтобы конкретизировать понимание различных видов перевозок, законодатель в данной статье ссылается на закон о прямых смешанных (комбинированных) перевозках. Несмотря на наличие отсылочной нормы в ГК РФ, на сегодняшний день закон о прямых смешанных (комбинированных) перевозках не был принят. Последняя попытка предложить рассмотреть законопроект «О прямых смешанных (комбинированных) перевозках» была предпринята весной 2020 г. Несмотря на существенную необходимость в принятии данного закона, ни один законопроект так и не дошел до слушаний.

В России на сегодняшний день мультимодальные перевозки регулируются Таможенным кодексом Евразийского экономического союза, ст. 788, 801 ГК РФ, транспортными кодексами (Уставом железнодорожного транспорта, Уставом автомобильного транспорта, Кодексом торгового мореплавания Российской Федерации и лр.), Федеральным законом от 30.06.2003 № 87-ФЗ «О транспортно-экспедиционной деятельности», международными договорами и соглашениями (соглашение о международном железнодорожном грузовом сообщении (СМГС) и др.). Также в Российской Федерации нет единого транспортного документа.

Помимо всего прочего коносамент также не является обязательным транспортным документом: в соответствии со ст. 142 Кодекса торгового мореплавания РФ коносамент не является обязательным документом и выдается по требованию отправителя. В России мультимодальные перевозки осуществляются на основании заключения нескольких договоров (договора перевозки груза, договора экспедирования груза и т.д.).

Особенностью мультимодальных перевозок в США является сочетание национального и международного права. В отношении транспортных документов применяется Международная конвенция об унификации некоторых правил о коносаменте 1924 г., а также Протокол 1968 г. (Гаагско-Висбийские правила). Тем не менее в случае, если пункт отправления находится на территории США, а также если какой-либо этап мультимодальной перевозки проходит по территории США или же через иные территории, на которые распространяется юрисдикция этой страны, наравне с международным правом применяются положения Закона «О морских перевозках грузов Соединенных Штатов Америки» 1936 г. Данные положения применяются ко всей перевозке груза, если хотя бы частично она удовлетворяет вышеназванным критериям. Пределом ответственности оператора мультимодальной перевозки грузов в этом случае является заявленная в транспортном документе стоимость груза, если стоимость фрахта была заранее согласована и оплачена перевозчику. В случае, если стоимость груза не указана, то размер возмещения за повреждение, утрату или недостачу груза не может превышать 500 долл. за единицу груза.

Единым транспортным документом по данной перевозке в США может являться мультимодальный коносамент, который включает в себя все необходимые данные о перевозчике, отправителе, получателе, о свойствах груза, о транспортной единице и т.д. Данный документ следует вместе с грузом на всем пути следования, и иные транспортные документы при осуществлении перевозок с мультимодальным коносаментом не требуются.

В праве США по мультимодальным перевозкам может применяться право отдельных штатов, но только на ту часть перевозки, которая подпадает под юрисдикцию данного штата. Также существует множество оговорок. Например, такой оговоркой можно считать «Гималайскую оговорку» 1954 г., в соответствии с которой ни один служащий, агент или подрядчик перевозчика ни при каких обстоятельствах не несет какой-либо ответственности перед грузоотправителем, грузополучателем или владельцем груза, или перед любым держателем коносамента за любые убытки, ущерб или задержку любого рода, прямо или косвенно возникающих в результате какого-либо действия, небрежности или невыполнения обязательств с его (перевозчика) стороны при выполнении им своих обязательств. По решению Вер-

ховного суда США оговорка не распространяется на операторов мультимодальной перевозки, так как оператор такой перевозки должен предвидеть необходимость привлечения иных перевозчиков, если такая необходимость возникнет в пути следования груза. Можно прийти к выводу, что в праве США оператор мультимодальной перевозки также ответственен на всем пути следования груза за свои действия перед грузоотправителями, грузополучателями или иными лицами до договору или транспортному документу, а также за действия привлеченных им перевозчиков.

В Германии основными нормативными правовыми актами, содержащими положения о мультимодальной перевозки, являются: Вводный закон 1896 г. Германии к Гражданскому кодексу (EGBGB) и § 452—452d Коммерческого кодекса Германии (HBR). В HBR мультимодальная перевозка определяется как «перевозка грузов, осуществляемая различными видами транспорта на основании единого договора перевозки, о которой можно сказать, что если бы между сторонами были заключены отдельные договоры на отдельные части перевозки, включающие один вид транспорта, то не менее двух таких договоров подпадали бы под действие различных правовых норм». Данные положения применяются к договору, если иное не предусмотрено специальными положениями, применимыми в соответствии с международными конвенциями. Данные положения применяются, когда хотя бы часть перевозки осуществляется морем.

В немецком законодательстве предусмотрена и ответственность оператора мультимодальной перевозки, которая соответствует такому же размеру ответственности перевозчика, который бы осуществлял перевозку на отдельном этапе такой перевозки. Если повреждение, утрата или задержка в перевозке относятся к определенному этапу, то перевозчик (оператор такой перевозки) несет ответственность в соответствии с правилами, которые применялись бы, если бы грузоотправитель заключал договор с мультимодальным перевозчиком (оператором) только на этот этап. Оператор мультимодальной перевозки также приравнивается к перевозчику в случае бремени доказывания. Лицо, заключившее договор мультимодальной перевозки с оператором, несет бремя доказывания факта повреждения, утраты или задержки груза в пути.

Параграф 452a HGB упоминает договор, который является договором, заключенным между грузоотправителем и перевозчиком, если бы перевозка охватывала только один этап, на котором произошло повреждение или утрата груза. Существенной разницы между таким договором и фактическим мультимодальным договором нет.

Нельзя не упомянуть практику Сингапура, где 5 января 2021 г. был принят к рассмотрению законопроект «О мультимодальных перевозках», который в свою очередь был разработан в соответствии с рамочным соглашением АСЕАН «О мультимодальных перевозках» 2005 г. В законопроекте описываются следующие основные аспекты мультимодальных перевозок:

1) регистрация операторов мультимодальных перевозок грузов в специальном регистрирующем органе;

2) составление и выдача мультимодальных транспортных документов (в том числе мультимодального договора);

3) обязательства оператора мультимодальной перевозки;

4) обязанности и ответственность грузоотправителей и др.

Из содержания данного законопроекта можно выделить понятие мультимодального транспортного документа, а также и его назначение: помимо универсальности на всем пути следования, он также сможет подтвердить существование договора мультимодальной перевозки, факт приемки груза от отправителя, существование обязательства оператора мультимодальной перевозки перед отправителем по доставке грузов получателю.

При рассмотрении транспортного документы нельзя не упомянуть концепцию единого Договора на осуществление мультимодальных перевозок (мультимодального договора). Рассмотрев пример Сингапура, стоит обратить внимание на то, что в рамках вышеупомянутого документа может существовать договор мультимодальных перевозок.

Правовое регулирование мультимодальных перевозок в различных странах неоднородно. Отсутствие единства в понимании мультимодальных перевозок порождает множество трудностей при их осуществлении. При этом, рассматривая опыт различных стран, можно выделить как перспективные решения, так и недостатки в различных подходах правового регулирования. Стоит учитывать опыт различных стран при подготовке проекта закона «О прямых смешанных перевозках».

Воронцов Максим Владимирович,
аспирант Юридического института Российского университета транспорта (МИИТ)

Цифровизация логистической отрасли: основные направления и правовое регулирование

Аннотация. Современные информационные технологии и технические средства совместно с развитием научно-технического прогресса упраздняют границы между технологиями и наукой и способствуют проникновению инноваций во все сферы и отрасли экономики и социума. Формирование цифровой экономики является задачей стратегического развития Российской Федерации. Различные сферы и отрасли экономики России проходят через цифровую трансформацию на основе цифровых технологий. Транспорт и логистика, относящиеся к транспортно-логистической отрасли, не являются исключением. В статье рассмотрены актуальные правовые и нормативные аспекты, регулирующие транспортно-логистическую отрасль России на примере транспортной логистики и регламентацию ее цифровизации. Данные законодательные документы создают возможность осуществлять цифровое государственное регулирование и управление с целью достижения поставленных целей и максимального эффекта.

Ключевые слова: цифровизация; цифровая трансформация; логистика; правовые аспекты; правовое регулирование.

Maxim V. Vorontsov,
post graduate of the Law Institute of the Russian University of Transport

Digitalization of the logistics industry: main directions and legal regulation

Abstract. Modern information technologies and technical means together with the development of scientific and technological progress abolish the boundaries between technology and science and facilitate the penetration of innovations into all spheres and sectors of the economy and society. The formation of a digital economy is a task of strategic development in the Russian Federation. Various spheres and sectors of the Russian economy are undergoing a digital transformation based on digital technology. Transport and logistics related to the transport

and logistics industry are no exception. The article deals with the current legal and regulatory aspects regulating the transport and logistics industry in Russia on the example of railway transport logistics and the regulation of its digitalization. These legislative documents create an opportunity to implement digital state regulation and management in order to achieve the goals and maximum effect.

Keywords: digitalization; digital transformation; logistics; legal aspects; legal regulation.

Сегодня наблюдается активная цифровая трансформация транспортной отрасли — создается цифровая транспортная инфраструктура (например, интеллектуальные транспортные системы, цифровые решения для пассажирских и грузовых терминалов и др.), происходит цифровизация транспортных средств (тестирование беспилотных транспортных средств, развитие мониторинга и предиктивных обслуживания и ремонта транспортных средств и др.), разрабатываются цифровые сервисы (например, решения «мобильность как сервис» ($MaaS$)) и т.д.

Необходимость цифровизации транспортно-логистической отрасли — это вопрос конкурентоспособности компаний, оперирующих на рынке, которые заинтересованы в увеличении объемов движения товаров, развитии несырьевого экспорта и росте доходов товаропроизводителей.

Одним из ключевых направлений деятельности Российской Федерации на среднесрочную перспективу является развитие цифровой экономики.

Тема цифровизации экономики и развития блокчейн-систем является крайне актуальной и вызывает большой интерес у современного общества. Рынок заинтересован в увеличении объемов движения товаров, развитии несырьевого экспорта и росте доходов отечественных товаропроизводителей, в том числе за счет процесса цифровизации экономики и логистики.

Цифровизация логистической отрасли — вопрос конкурентоспособности компаний, оперирующих на данном рынке, поэтому поддержка развития технологий со стороны всех стейкхолдеров данного рынка принесет выгоду всем участвующим на рынке компаниям.

Правовое обеспечение логистики — комплекс и/или процесс осуществления организационных мероприятий, определяемых действующими нормами международного и национального права, выполне-

ние которых в определенной совокупности и последовательности позволяет законным образом содействовать достижению поставленных логистических целей и решению требуемых логистических задач в установленный срок с минимальными издержками для исполнителя логистических действий, а также вовлеченных вольно или невольно в это действие физических и юридических лиц при минимуме отрицательного воздействия на окружающую среду и безусловное соблюдении гарантированных Конституцией РФ прав и свобод физических лиц, вовлеченных в логистический процесс.

Правовое обеспечение логистики включает деятельность как внутри страны, так и за рубежом, по разработке новой законодательной базы и заключению международных соглашений, направленную на совершенствование логистической деятельности в стране и за ее пределами при сохранении приоритета интересов Российской Федерации, ее граждан и союзников.

Внедрение цифровых технологий в логистические процессы предприятия необходимо рассматривать как неотъемлемую часть развития логистической системы и предприятия в целом в современных условиях. Формирование комплексной цифровой инфраструктуры способствует оптимизации логистических процессов предприятия с минимальным участием человеческого фактора.

Сейчас цель — сформировать в России единое цифровое транспортное пространство, сделать пассажирские и грузовые перевозки более безопасными, удобными, доступными для людей и бизнеса, снизить издержки, расширить экспортные и транзитные возможности. Для решения этих задач предусмотрен ведомственный проект «Цифровой транспорт и логистика», который разрабатывается в рамках государственных программы по цифровизации экономики, логистики и развитию на этой основе транспорта [https://www.mintrans.ru].

Цифровая логистика — это управление людскими, материальными, информационными и финансовыми потоками на основе их оптимизации для решения задачи минимизации затрат с применением современных информационных технологий.

В целом, цели цифровой трансформации логистики состоят в следующем: 1) повышение транспортно-транзитного потенциала и внешнеторгового оборота России; 2) внедрение и развитие смешанных (мультимодальных) перевозок; 3) обеспечение доступности и

качества транспортно-логистических услуг грузовых перевозок; 4) обеспечение доступности и качества транспортных услуг для населения в соответствии с социальными стандартами; 5) повышение эффективности управления транспортной инфраструктурой; 6) создание платформы тарифного регулирования перевозок и оплаты проезда.

Нормативное регулирование логистической деятельности представляет собой единую структуру или процесс реализации мероприятий организации в соответствии с действующими нормами международного и отечественного законодательства, следование которым в некоторой системе и хронологии дает возможность легитимным способом способствовать результативности выполнения целей в области логистики и решению необходимых логистических задач.

Принятый на текущий период план работы по выработке законодательных инициатив в области цифровой экономики, цифровой логистики и правового регулирования, а также предложение о создании Координационного совета по обсуждению законодательных инициатив при Минтрансе России, будет способствовать росту конкурентоспособности и укреплению позиции транспортных и логистических компаний России на внутреннем и международном рынках перевозок, повысит эффективности взаимодействия различных видов транспорта в логистических системах и товаропроизводящих сетях, поможет снизить физические и нефизические барьеры в движении грузов, будет способствовать развитию транзитного потенциала нашей страны. Все это в конечном итоге будет способствовать снижению доли транспортной составляющей в стоимости товаров и оптимизации транспортных затрат.

Таким образом, формирование современной технологической среды на основе передовых информационных технологий, которые активно стремиться использовать транспортная логистика, создают определенную совершенно новую плоскость гражданско-правового регулирования.

Подводя итог, можно сказать, что в настоящее время видны как эволюционные, так и революционные пути развития отрасли, к которым и относятся цифровые технологии. Формирование современной технологической среды на основе передовых информационных технологий, которые активно стремиться использовать транспортная логистика, создают определенную совершенно новую плоскость гражданско-правового регулирования.

Зиновьева Вера Викторовна,
аспирант Юридического института Российского университета транспорта (МИИТ)

Анализ судебной практики по административным правонарушениям в сфере информационной безопасности

Аннотация. В статье проводится исследование судебных дел о нарушениях, связанных с защитой информации по статьям Кодекса Российской Федерации об административных правонарушениях, выделяются характерные особенности изученных судебных дел и делаются выводы о проблемах привлечения к административной ответственности в рассматриваемой сфере.

Ключевые слова: информация; информационная безопасность; административная ответственность; персональные данные; защита информации.

V. Vera Zinovieva,
post graduate of the Law Institute of the Russian University of Transport

Analysis of judicial practice on administrative offenses in the field of information security

Abstract. The article studies some court cases on violations related to the protection of information under the articles of the Code of the Russian Federation on Administrative Offenses, highlights the characteristic features of the studied court cases and draws conclusions about the problems of bringing to administrative responsibility in this area.

Keywords: information; information security; administrative responsibility; personal data; information protection.

Перевод большинства информационных архивов, денежных средств и коммуникаций в электронную форму создал самостоятельный тип актива — информацию. Как любая ценность, она подвергается различным преступным и несанкционированным посягательствам. Возникают существенные риски и в области обеспечения государственной безопасности в сфере информации, основные угрозы названы в Доктрине информационной безопасности Российской Фе-

дерации (утверждена Указом Президента РФ от 05.12.2016 № 646). Игнорирование возникающих проблем приводит к потере конкурентоспособности как на государственном, так и на корпоративном уровне. Страдают от преступлений, совершаемых в информационной сфере, и граждане.

В последние годы вопросы обеспечения информационной безопасности приобретают очень важное значение, а с учетом объявленного перехода к цифровой кономике, актуальность этой проблемы усиливается многократно. Увеличение угроз целостности и конфиденциальности информации требует внимательного отношения к задаче ее защиты.

В связи с этим представляется актуальным провести исследование судебных дел о нарушениях, связанных с защитой информации по статьям Кодекса Российской Федерации об административных правонарушениях (далее — КоАП РФ).

Для исследования были выбраны статьи, которые относятся к обработке и обеспечению безопасности персональных данных, нарушению правил и незаконной деятельности в области защиты информации и разглашению информации ограниченного доступа.

Основной акцент исследования был сделан на вопросы обеспечения защиты информации в автоматизированных системах, в том числе при обработке персональных данных.

Для подготовки настоящего исследования рассмотрено более 2 тыс. записей, содержащихся в ГАС «Правосудие» и относящихся к правоприменительной практике по ст. 13.11—13.14 КоАП РФ (13.11 — 72% и 13.14 — 25,8% дел) за период с 1 января 2019 г. по 31 декабря 2020 г.

Инициаторами возбуждения дел являлись не только сами пострадавшие от распространения их персональных данных, но и государственные органы: Роскомнадзор или прокуратура РФ (38% дел) при проведении проверок.

Важно отметить, что срок давности для административного правонарушения составлял в 2019—2020 гг. три месяца. Таким образом, заявителям в 18% дел отказали в рассмотрении судебного дела в связи с истечением срока давности.

КоАП РФ содержит следующие статьи по исследуемой теме: 13.11 — «Нарушение законодательства Российской Федерации в области

персональных», 7.31.1 — «Нарушение порядка и (или) сроков возврата денежных средств, внесенных в качестве обеспечения заявок на участие в определении поставщика (подрядчика, исполнителя), порядка и (или) сроков блокирования операций по счету участника закупки, порядка ведения реестра участников электронного аукциона, получивших аккредитацию на электронной площадке, правил документооборота при проведении электронного аукциона, разглашение оператором электронной площадки, должностным лицом оператора электронной площадки информации об участнике закупки до подведения результатов электронного аукциона», 13.12 — «Нарушение правил защиты информации», 13.13 — «Незаконная деятельность в области защиты информации», 13.14 — «Разглашение информации с ограниченным доступом», 15.21 — «Неправомерное использование инсайдерской информации», 17.13 — «Разглашение сведений о мерах безопасности», 20.24 — «Незаконное использование специальных технических средств, предназначенных для негласного получения информации, в частной детективной или охранной деятельности».

С 27 марта 2021 г. вступили в силу положения Федерального закона от 24.02.2021 № 19-ФЗ, согласно которым были увеличены штрафы за нарушение законодательства РФ в области персональных данных, предусмотрены штрафы за повторные нарушения и исключена мера административного наказания в виде предупреждения по некоторым пунктам.

Вместе со штрафами увеличен срок давности привлечения к административной ответственности за нарушения в области персональных данных с трех месяцев до года (ч. 1 ст. 4.5 КоАП РФ). В случае признания административного правонарушения длящимся, срок исчисляется со дня обнаружения данного правонарушения (ч. 2 ст. 4.5), т.е. со дня, когда должностное лицо, уполномоченное составлять протокол об административном правонарушении, выявило факт его совершения.

11 июня 2021 г. был опубликован федеральный закон об увеличении штрафов за разглашение персональных данных. Согласно документу увеличились штрафы за разглашение информации с ограниченным доступом (ст. 13.14): для граждан (ранее составляли от 500 руб. до 1 тыс. руб.) от 5 до 10 тыс. руб., для должностных лиц (ранее составляли от 4 тыс. до 5 тыс. руб.) — до 50 тыс. руб. Уточняется, что

под данное определение попадают различная конфиденциальная информация, включая коммерческую и банковскую тайны, тайну связи. Для юридических лиц штрафы не изменились и составляют от 100 тыс. до 200 тыс. руб.

Условно статьи по нарушениям в сфере информационной безопасности можно разделить на три типа. Первый тип таких статей относится к утечкам персональных данных, второй — к нарушениям в сфере защиты информации, третий — к нарушениям, связанным с отказом в доступе к информации, неразмещением информации в открытом доступе, со свободой слова, пропагандой, клеветой, нарушением авторских прав, размещением вакансий, содержащих информацию дискриминационного характера и т.п.

Важно отметить, что настоящее исследование было ограничено статьями и теми их частями, по которым за исследуемый период имеется информация в ГАС «Правосудие» и релевантными тематике утечек информации ограниченного доступа, которые относятся к нарушениям в области защиты информации, в том числе персональных данных, а именно: ст. 13.11 (ч. 1, 7 и 8), 13.12 (ч. 1), 13.13 и 13.14 КоАП РФ.

Для примера рассмотрим самые громкие дела в исследуемой области. Так, с 1 сентября 2015 г. компании обязаны обрабатывать и хранить персональные данные россиян с использованием баз данных, размещенных на территории РФ. Однако ответственность была установлена только со 2 декабря 2019 г. За нарушение закона в части локализации (требования ч. 8 ст. 13.11 КоАП РФ) предусмотрено наказание в виде штрафа для юридических лиц в размере до 6 млн руб.

На сегодня хранение персональных данных российских пользователей локализовали порядка 600 представительств зарубежных компаний в России, среди которых *Apple, Microsoft, LG, Samsung, PayPal, Booking* и др. Тем не менее ряд крупнейших иностранных компаний проигнорировали требования закона по обеспечению информационной безопасности данных граждан России.

Роскомнадзор в 2019 г. инициировал в отношении *Twitter* и *Facebook* административное производство. 13 февраля 2020 г. мировым судьей Таганского районного суда г. Москвы компании данные компании за отказ локализовать персональные данные россиян на территории РФ были признаны виновными в правонарушениях,

предусмотренных ч. 8 ст. 13.11 КоАП РФ. Каждой корпорации было назначено наказание в виде административного штрафа в размере 4 млн руб. Компания *Facebook* штраф оплатила, в то время как *Twitter* отказался выполнять требование и подал апелляционную жалобу 28 февраля 2020 г. Суд жалобу отклонил.

В сентябре 2021 г. судебные приставы пришли в российский офис американской корпорации *Google*, чтобы взыскать неоплаченные штрафы, выписанные компании. Адвокат компании сообщил приставам, что они пришли в офис ООО *Google*, а претензии суда касаются компании *Google LLC*, которая находится в США.

И чтобы избежать подобных ситуаций в будущем в 2021 г. Государственная Дума одобрила законопроект, обязывающий крупные зарубежные ИТ-компании с ежедневной аудиторией в России от 500 тыс. человек открывать свои представительства в России. Такие организации должны будут с 1 января 2022 г. создать филиалы, открыть представительства или учредить российские юридические лица, которые в полном объеме будут представлять интересы головных компаний во взаимодействии с Роскомнадзором.

Следует отметить, что явной корреляции между тяжестью нарушения и величиной наказания не прослеживается. Так, злоумышленнику, который скопировал из ГАС «Выборы» на съемный носитель данные избирателей одного из участков в Республике Татарстан, назначили штраф в размере 1500 руб. (кстати, даже такой штраф нарушитель пытался оспорить, причем четырежды, но безрезультатно). А за звонки в рекламных целях суды назначали административные штрафы от 5 до 30 тыс. руб.

Также по итогам исследованию можно сделать вывод, что более трети правонарушений были совершены с помощью сети «Интернет», компьютеров, телефонов и других систем, что говорит о недостаточно высоком уровне информационной безопасности организаций. В остальных случаях утечки конфиденциальной информации произошли через неавтоматизированные каналы обработки данных.

Интересной особенностью изученных судебных дел является то факт, что во всех делах доступ к раскрытым персональным данным и другой конфиденциальной информации был правомерным, т.е. персональные данные были раскрыты сотрудниками организаций. Ответчиками в судебных делах выступали сотрудники и должностные

лица, а не злоумышленники, получившие доступ к данным нелегально извне. Очевидно, что дела, касающиеся несанкционированного доступа к конфиденциальной информации со стороны хакеров или других нарушителей, суды рассматривают по статьям УК РФ.

Таким образом, учитывая изложенное, можно сделать следующие выводы.

1. Несмотря на наличие федеральных законов и статей КоАП РФ, относящихся к защите информации, в том числе персональных данных, на текущий момент судебная практика в этой сфере неразвита. Причиной этому может служить отсутствие государственных требований и практики информирования пострадавших и государственных органов об утечках конфиденциальной информации, в связи с чем необходимо установление административной и уголовной ответственности в отношении должностных лиц за неинформирование о подобных инцидентах.

2. Ввиду редкости обращений в суд лицами, пострадавшими от утечек персональных данных, и низкими штрафами за большинство нарушений правил безопасной обработки персональных данных, ситуация в этой сфере пока плохо контролируема.

В 2022 г. при поступлении новых данных за 2021 г. планируется изучить, как изменилась ситуация и повлияло ли на нее повышение штрафов за нарушения, связанные с обработкой персональных данных.

Козаченко Надежда Евгеньевна,
аспирант Юридического института Российского университета транспорта (МИИТ)

Правовое регулирование и критерии производственной системы

Аннотация. Объектом исследования настоящей работы является правовое регулирование производственного процесса, где выступает система стандартизации и производства. В качестве предмета исследования выступает правовая система, правовые нормы охраны окружающей среды, хозяйственная деятельность, транспортная и промышленная безопасность, с использованием которых осуществляется правовое регулирование и производ-

ственная система. По результатам исследования с использованием методики формально-юридического анализа автором сделаны выводы о возможности охарактеризовать производственное регулирование как наиболее эффективное в случае, если прогнозируемый результат воздействия достижим при наборе определенных параметров. Обозначены проблемные аспекты правового регулирования и критерии производственной системы. В то же время для такого регулирования производственной сферы нужно обозначить следующие, требующие более фундаментального изучения проблемные аспекты. В статье рассмотренные теоретические идеи и методологические принципы подхода к организации управления производственной деятельности промышленных предприятий. Развитие системы в дальнейшем способно обеспечить ощутимое продвижение в направлениях организационной системы управления и диагностика состояния предприятия.

Ключевые слова: правовое регулирование; производство; стандартизация; транспортная безопасность; регулирование; продукция; экономика.

Nadezhda E. Kozachenko,
post graduate of the Law Institute of the Russian University of Transport

Legal regulation and criteria of the production system

Abstract. The object of research of this work is the legal regulation of the production process, where the system of standardization and production acts. The subject of the study is the legal system, legal norms of environmental protection, economic activity, transport and industrial safety, with the use of which legal regulation and the production system are carried out. Based on the results of the study using the methodology of formal legal analysis, the author concludes that it is possible to characterize production regulation as the most effective if the predicted impact result is achievable with a set of certain parameters. Problematic aspects of legal regulation and criteria of the production system are identified. At the same time, for such regulation of the production sphere, it is necessary to identify the following problematic aspects that require more fundamental study. The article discusses the theoretical ideas and methodological principles of the approach to the organization of management of production activities of industrial enterprises. The development of the system in the future is able to provide tangible progress in the directions of the organizational management system and diagnostics of the state of the enterprise.

Keywords: legal regulation; production; standardization; transport security; regulation; products; economy.

Правовая система определяется как «реальность, охватывающая собой всю совокупность внутренне согласованных, взаимосвязанных социально-однородных юридических средств, с помощью которых государственная власть оказывает регулятивно-организующее и стабилизирующее воздействие на общественные отношения. Это комплексная регулирующая категория, отражающая всю правовую организацию общества, целостную правовую действительность» [6]. Правовая система, и правовое регулирование фактически объединяют в себе юридические средства.

Административное право, как отрасли права выступают в сфере государственного управления, в пределах которой субъекты исполнительной власти повседневно руководят хозяйственными, социально-культурными и административно-политическими процессами [1]. Закрепляя правила поведения в области государственного управления, административное право придает управленческим отношениям статус правоотношений, ряд экономико-правовых регуляторов производства.

В пользу производственного регулирования выступают такие факторы, как значительное увеличение общего объема регуляторов (эффективность новых нормативных правовых актов в ряде случаев очень низкая, а некоторые сферы отношений практически не охвачены). Нередко это влечет за собой прямо противоположный первоначальным целям результат, провоцируя тем самым стагнационные процессы в обществе. Ю. А. Тихомировым совершенно верно было отмечено, что «хаотичный порядок регуляции создает иллюзию правового регулирования и его эффективности» [3].

При обозначении актуализации системных исследований указывалось на «потребность внедрения системного подхода и метода не только в науку, но и в организацию и управление производством», где «возникает объективная потребность не только в систематизации знания и деятельности, но и в их интеграции, синтезе, в восстановлении общей картины общественного бытия, общественной практики в целом» [4].

В работах российских ученых структура правовой системы характеризуется тремя группами правовых явлений. Во-первых, юридические

нормы, принципы и институты (нормативная сторона); во-вторых, совокупность правовых учреждений (организационная сторона); в-третьих, совокупность правовых взглядов, представлений, идей, свойственных данному обществу, правовая культура (социокультурная сторона) [5]. Представленная структура правовой системы в целом соответствует структуре правового регулирования. Нормы права, излагаемые в нормативных правовых актах, устанавливают общие, юридически обязательные правила поведения участников производственных отношений, находящихся в сфере правового регулирования.

Несмотря на постоянно увеличивающееся в правовой системе количество законодательных актов, неэффективность законодательства и правовая незащищенность людей обостряются, значительно снижая тем самым эффективность правового регулирования в целом. Несовершенство современного российского законодательства обусловлено его необоснованной многочисленностью, зачастую приводящей к противоречивости и понятийной неопределенности.

Таким образом, на примере анализа функционирования законодательства становится ясно, что качественное правовое регулирование осуществляется лишь при наличии качественного состояния его элементов — правовых средств, направленных на гарантированное обеспечение реализации общественно полезных целей и интересов субъектов. Эти же самые правовые средства в своей совокупности образуют совершенную либо несовершенную правовую систему.

Право выражается в категории правовой системы, в правовом регулировании, показывающим поэтапное движение от одного элемента к другому в их взаимодействии, начиная с правотворчества, реализуясь в правоотношениях и заканчивая достижением цели правового регулирования — обеспечением законности и правопорядка на основе развитой правовой культуры личности и общества.

В ходе практической деятельности производящие материальные блага люди сталкиваются не только с определенным уровнем развития техники и технологии, но и со сложившимися по этому поводу отношениями, которые принято называть технологическими.

Для выполнения своей программы развития предприятия создают научно-конструкторские и технологические подразделения, заказывают и приобретают технологическое оборудование, покупают лицензии и т.д.

В интересах достижения успеха в реализации продукции предприятия осуществляют активный маркетинг: создают собственные каналы сбыта, рекламируют свою продукцию, вступают в хозяйственные связи с транспортными, складскими и торговыми организациями.

Точные и объективные измерения являются обязательным условием обеспечения эффективности производства, проведения научных исследований по созданию новых видов продукции и новых технологий, разработки и выпуска высококачественной продукции [2].

В рыночной экономике каждое предприятие находится в условиях жесткой конкурентной борьбы, неблагополучный исход которой может привести к финансовому кризису и/или банкротству. Это предопределяет потребность в формировании и использовании эффективных инструментов оперативного управления производственной системы, составной частью которых являются методы и правовое регулирование [7].

Специализация нормативных правовых актов России происходила в зависимости от объективных факторов развития промышленного сектора экономики: для опасных производств разрабатывались многочисленные инструкции, детализировался порядок хранения взрывчатых веществ. Появлялись нормы, выполнение которых способствовало снижению рисков (экологических, противопожарных); устанавливались правила организации, устройства и функционирования промышленных заведений; был введен правовой режим для отдельных производств, технологических и сопутствующих операций.

Сложность формирования области регулирующего воздействия (определение сферы). Общемировые тенденции экономического развития и необходимость защиты национальных интересов России ориентируют на отказ от искусственного формирования той или иной сферы регулирования и бесплодных попыток ввести в нее объективно существующие и зарождающиеся общественные отношения. Отсутствие четкой (строго очерченной) предметной области упорядочивания приводит к самым неблагоприятным последствиям. Так, сфера действия Федерального закона от 27.12.2002 № 184-ФЗ «О техническом регулировании» неоправданно расширена (охватывает практически все области хозяйственной деятельности людей). Следует также подчеркнуть, что разграничение технико-юридического и технического регулирования обоснованно: конкретизирующая функ-

ция первого не должна отождествляться со сферой действия Федерального закона «О техническом регулировании». При этом ряд областей общественных отношений по не совсем понятным причинам исключены из сферы действия данного нормативного правового акта, что обозначает наиболее общую фундаментальную проблему.

Следует предположить, что ощутимый результат в достижении цели регулирования может дать лишь более точное формирование модели для регулирующего воздействия, в чем-то схожей с понятием системы отсчета в физике, в рамках некой сферы отношений. В то же время объективный взгляд на обозначенные проблемные аспекты говорит о сложности решения поставленных задач в ближайшей перспективе без опоры на фундаментальные теоретические исследования. Обозначенное выше только в определенной мере способно корректировать регуляцию в наиболее чувствительной ее части — производственном (производящем) секторе экономики, неизбежность регламентации которой очевидна. В связи с этим правовое регулирование и критерии производственной системы могут стать предметом дальнейших комплексных исследований.

Литература

1. Административное право России : учебник и практикум для бакалавриата и специалитета / под редакцией А. И. Стахова, П. И. Кононова. Москва: Издательство Юрайт, 2019.
2. Анфилатов, В. С. Системный анализ в управлении / В. С. Анфилатов, А. А. Емельянов, А. А. Кукушкин ; под редакцией А. А. Емельянова. Москва : Финансы и статистика, 2002
3. Керимов, Д. А. Методология права (предмет, функции, проблемы философии права). 2-е изд. Москва : Аванта, 2001.
4. Ковалева, Н. В. Техническое регулирование в законодательстве Российской империи (XIX — начала XX веков) : монография. Кострома : Изд-во Костром. гос. технол. ун-та, 2012.
5. Кожевников, В. В. Теория государства и права / В. В. Кожевников, И. Н. Сенин. Омск, 2008.
6. Матузов, Н. И. Право и правовая система // Теория государства и права. Москва, 1997.
7. Правкин, С. А. Актуальные проблемы права : учебное пособие. Москва : Юридический институт МИИТ, 2019.

Кузнецов Андрей Евгеньевич
аспирант Юридического института Российского университета транспорта (МИИТ)

Правовое обеспечение кибербезопасности на транспорте

Аннотация. В статье рассматривается правовое обеспечение кибербезопасности на транспорте. Рассмотрены проблемы обеспечения информационной безопасности. Изучена защита персональных данных в сфере транспорта. Проанализированы нормативные правовые акты, регламентирующие обеспечение транспортной безопасности в части использования и защиты персональных данных пассажиров.

Ключевые слова: кибербезопасность; транспорт; транспортная безопасность; информационная безопасность; правовое обеспечение.

Andrey Ev. Kuznetsov
post graduate of the Law Institute of the Russian University of Transport

Legal support for cybersecurity in transport

Abstract. This article examines the legal framework for cyber security in transport. The problems of ensuring information security has considered. The protection of personal data in transport has studied. Regulatory legal acts regulating the provision of transport security in terms of the use and protection of passenger's personal data has analysed.

Keywords: cybersecurity; transport; transport security; information security; legal support.

При широком внедрении цифровизации на транспорте возникает проблема в информационной защите, которая входит в число первоначальных приоритетов в обеспечении безопасности в транспортной отрасли. Задача любого государства — это защита информационных систем на транспорте.

Кибербезопасность транспорта — безопасность личных данных, которыми пользователь делится с транспортным устройством или агрегатором транспортных данных. Сегодня «умные» системы окружают нас повсюду: они контролируют трассы и железные дороги с

помощью платформ для мониторинга, отслеживают и предотвращают пробки как навигаторы, отвечают за безопасность пассажиров и водителя внутри автомобилей.

Все эти системы используют контроллеры и датчики, которые позволяют держать связь с внешними источниками данных. На практике оказывается, что чем больше у транспортного средства связи с внешним миром, тем уязвимее для кибератак извне он становится и тем больше ему нужна особая система защиты.

Мы ежедневно передаем свои персональные данные, пользуясь каршерингом, прокатом самокатов или велосипедов, такси и даже метро — при этом, давая на это личное согласие (и часто пренебрегая чтением пользовательских соглашений или прочтением всей информации про *cookies*). Мы делимся с сервисами данными карты, в качестве адреса для выставления счета указываем личную почту, а в некоторых случаях — и адрес проживания, и редко задумываемся о том, что может произойти с этими данными дальше.

При использование транспорта автоматически возникает вопрос об информационной безопасности, такой как защита персональных данных. Этот вопрос становится обсуждением в международном сообществе.

Минтранс России разработал концепцию безопасности на транспорте, которая нашла отражение в Федеральном законе «О транспортной безопасности», где информационное обеспечение является одним из факторов транспортной безопасности.

В Федеральном законе от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» информация имеет достаточно большое значение. Нововведение в информационной безопасности в транспортной отрасли - это использование беспилотного транспорта.

Ключевая роль в обеспечении кибербезопасности на транспорте отводится информационной безопасности в деятельности русских компаний, в которых информационной безопасности уделяют достаточное внимание.

Очевидно, что проблема обеспечения информационной безопасности, а также цифровизации Российской Федерации будет оставаться актуальной. Становится очевидным приоритет информационной безопасности критически важных объектов инфраструктуры, прежде всего, транспорта.

Сербиненко Екатерина Юрьевна
аспирант Юридического института Российского университета транспорта (МИИТ)

Правовое регулирование цифровой валюты: сравнительно-правовой анализ

Аннотация. В данной статье к рассмотрены типы цифровой валюты. Для более подробного анализа была выбрана криптовалюта и ее использование в различных странах мира. В сравнительно-правовой анализ вошли такие страны, как Объединенные Арабские Эмираты, Германия, Румыния, Республика Беларусь и Российская Федерация.
Ключевые слова: валюта; цифровая валюта; криптовалюта; правовое регулирование; биткоин; цифровая экономика.

Ekaterina Yu. Serbinenko
post graduate of the Law Institute of the Russian University of Transport

Legal regulation of digital currency: comparative legal analysis

Abstract. This article proposes the types of digital currency. For a more detailed analysis, cryptocurrency was chosen and its use in various countries of the world. The comparative legal analysis includes countries such as the United Arab Emirates, Germany, Romania, the Republic of Belarus and the Russian Federation.
Keywords: currency; digital currency; cryptocurrency; legal regulation; bitcoin; digital economy.

Цифровая валюта (цифровые деньги, электронные деньги или электронная валюта) — это любая валюта, деньги или денежный актив, который в основном управляется, хранится или обменивается в цифровых компьютерных системах, особенно через Интернет. Типы цифровых валют включают криптовалюту, виртуальную валюту и цифровую валюту центрального банка.

Виртуальная валюта или игровая валюта — частные электронные деньги, которые используются для приобретения и продажи виртуальных товаров в различных сетевых сообществах: социальных сетях, виртуальных мирах и онлайн-играх. В каждой среде виртуальная ва-

люта используются для специфических целей: покупка авотаров; покупка различных игровых артефактов: например, оружия, земли, статуса; покупка расширенных возможностей пользования форумом.

Цифровая валюта центрального банка — цифровая валюта центрального банка. Это электронное обязательство монетарного регулятора, номинированное в национальной счетной единице и служащее средством платежа, меры и сохранения стоимости. В Российской Федерации цифровой валютой выступает цифровой рубль. Цифровой рубль — это цифровая форма российской национальной валюты, которую Банк России планирует выпускать в дополнение к существующим формам денег.

Более подробно остановимся на рассмотрении криптовалюты и ее использовании в различных странах мира.

Криптовалюта — цифровые деньги: максимально защищенный от взлома программный код. Чаще всего основаны на технологии блокчейн. Криптовалюта — это цифровая валюта, создание и контроль которой основаны на криптографии, т.е. защищены от взлома.

Криптовалюта получила свое название, поскольку использует шифрование для проверки транзакций. Это означает, что расширенное кодирование участвует в хранении и передаче данных криптовалюты между кошельками и в публичные книги. Целью шифрования является обеспечение безопасности.

Первой криптовалютой стал биткоин, который был основан в 2009 г. и остается наиболее известной на сегодняшний день. Большая часть интереса к криптовалютам заключается в том, чтобы торговать с прибылью, а спекулянты временами подгоняют цены.

Правовой статус криптовалют существенно варьируется от одной юрисдикции к другой и по-прежнему не определен или не изменяется во многих из них [1]. В то время как в большинстве стран использование криптовалюты само по себе не является незаконным, его статус и удобство использования в качестве платежного средства (или товара) различаются, с различными нормативными последствиями [2].

Объединенные Арабские Эмираты становятся прогрессивной крипто- и блокчейн-страной, внедряющей новое возрастное законодательство и правовую структуру, чтобы усилить крипто-стартапы для переезда в ОАЭ. ОАЭ принимает криптоплатежи, в том числе биткоин, с государственной лицензионной фирмой *KIKLABB*, а также разрабатывает собственную цифровую валюту.

19 августа 2013 г. Минфин **Германии** объявил, что биткойн по сути является «счетной единицей» и может использоваться для целей налогообложения и торговли в стране, что означает, что покупки, сделанные с его помощью, должны платить НДС, как и при сделках в евро. Он не классифицируется как иностранная валюта или электронные деньги, а означает «частные деньги», которые можно использовать в «многосторонних клиринговых кругах», считают в министерстве. Бундесбанк говорит, что биткойн не является виртуальной валютой или цифровыми деньгами. Рекомендуется использовать термин «криптотокен» [3]. В ноябре 2019 г. принятый парламентом Германии закон разрешает банкам продавать и хранить криптовалюты с 1 января 2020 г.

Румыния. В марте 2015 г. в официальном заявлении Румынского национального банка говорилось, что «использование цифровых валют в качестве платежа имеет определенные риски для финансовой системы» [4].

В октябре 2017 г. Национальное агентство фискальной администрации (АНАФ) заявило, что вокруг биткойна отсутствует законодательная база, в связи, с чем оно не в состоянии также создать для него рамки налогового регулирования (подразумевающие отсутствие налогообложения) [5].

В январе 2019 г. Закон № 30/2019 уточняет, что начиная с 2019 г. доходы от торговли «виртуальной валютой» классифицируются по «доходам от других источников». Кроме того, существует новый подпункт, ст. 116. (2) в), уточняя, что налог на прибыль в размере 10% применяется только к «положительной разнице между ценой продажи и ценой приобретения» (а не ко всей полученной сумме от продажи). Кроме того, прибыль в размере менее 200 леев за транзакцию, общая сумма которой в течение финансового года составляет менее 600 леев, освобождается от уплаты налога [6].

Республика Беларусь. Положения Указа Президента Республики Беларусь «О развитии цифровой экономики» создают правовую основу для обращения цифровых валют и токенов на основе технологии блокчейн, чтобы компании-резиденты парка высоких технологий могли предоставлять услуги фондовых рынков и обменных пунктов криптовалютами и привлекать финансирование через *ICO* (первичное предложение валюты). Для юридических лиц Указом предоставляются пра-

ва на создание и размещение собственных токенов, осуществление операций через фондовые рынки и биржевых операторов; физическим лицам Указ дает право заниматься добычей полезных ископаемых, владеть токенами, приобретать и менять их за белорусские рубли, иностранную валюту и электронные деньги. В 2023 г. Указ исключает доходы и прибыль от операций с токенами из налогооблагаемой базы. В отношении физических лиц приобретение и продажа токенов не считается предпринимательской деятельностью, а сами токены и доходы от сделок с ними декларированию не подлежат. Особенность введенного регулирования в том, что все операции придется проводить через компании-резиденты парка высоких технологий.

Продление срока действия специального правового режима парка высоких технологий до 1 января 2049 г., расширение перечня деятельности компаний-резидентов. По новым правилам резидентами могут стать разработчики блокчейн-решений, разработчики систем машинного обучения на базе искусственных нейронных сетей, компании из медицинской и биотехнологической отраслей, разработчики беспилотных автомобилей, а также разработчики программного обеспечения и издатели. Список перспективных направлений неограничен и может быть расширен решением наблюдательного совета парка высоких технологий.

Российская Федерация. В 2021 г. Президент РФ заявил, что Россия принимает роль криптовалют, и что криптовалюты могут использоваться для оплаты.

С точки зрения действующего российского законодательства криптовалюта является денежным заменителем. Согласно ст. 27 Федерального закона «О Центральном банке Российской Федерации (Банке России)» выпуск денежных суррогатов в Российской Федерации запрещен.

Банк России и Росфинмониторинг в своих информационных обращениях неоднократно предупреждали граждан России, что все операции с криптовалютой носят спекулятивный характер и несут высокий риск потери стоимости. Банк России заявляет: «большинство операций с криптовалютами совершается вне правового регулирования как Российской Федерации, так и большинства других государств. Криптовалюты не гарантируются и не предоставляются Банком России».

Законопроект о цифровых финансовых активах был внесен в Госдуму 20 марта 2018 г. Он определяет майнинг криптовалют как «деятельность, направленную на создание криптовалюты с целью получения компенсации в виде криптовалюты» и рассматривает его как «предпринимательскую деятельность, подлежащую налогообложению, если майнер три месяца подряд превышает установленные правительством лимиты энергопотребления».

В законопроекте биткоины классифицируются как имущество и не считаются законным платежным средством. Обмен криптовалюты на рубли и иностранную валюту разрешен, но только через лицензированных операторов. Законопроект также предусматривает определение смарт-контракта.

В январе 2022 г. Банк России предложил запретить «вся эмиссия криптовалют и операции, запрет банкам инвестировать в криптовалюты, блокирование обмена крипто на традиционную валюту и введение юридической ответственности за использование крипто в покупках», ссылаясь на системный финансовый риск [7]. По данным *Bloomberg News* и *Meduza*, ФСБ России убедила Банк России запретить криптовалюты в России, так как они используются для финансирования оппозиции и независимых СМИ. В феврале 2022 г. Правительство РФ в итоге заявило, что будет поддерживать, легализовывать и регулировать криптовалюты, а не запрещать их [8].

Проведя сравнительно-правовой анализ, можно сделать вывод, что важным аспектом является выработка согласованной позиции в отношении регулирования криптовалют.

Литература

1. Assessing the Differences in Bitcoin & Other Cryptocurrency Legality Across National Jurisdictions Information Systems & Economics eJournal. Social Science Research Network (SSRN). Accessed 25 September 2017.
2. Regulation of Cryptocurrency Around the World. Library of Congress. The Law Library of Congress, Global Legal Research Center. June 2018. Retrieved 14 August 2018.
3. Gesetz zur Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie. Bundesrat (in German). 15 November 2019.
4. Evenimentul Zilei: Tranzacțiile cu monedele BITCOIN nu sunt impozitate de FINANȚE. Un hacker inculpat de DIICOT a învins Statul la acest capitol. evz.ro. Retrieved 6 December 2017.

5. Legea nr. 227/2015 privind Codul fiscal — ART. 116 — Declararea, stabilirea și plata impozitului pentru unele venituri din alte surse. Retrieved 19 February 2019.
6. On the use of private «virtual currencies» (cryptocurrencies). Press Service of The Central Bank of Russia. 27 January 2014.
7. Press review: What Macron told Zelensky and Russia moves to regulate cryptocurrency. TASS. Retrieved 9 February 2022.
8. Bank of Russia Seeks to Outlaw Mining and Trading of Crypto. Retrieved 20 January 2022.

Сустина Татьяна Ильинична,
аспирант Юридического института Российского университета транспорта (МИИТ)

Развитие законодательства в сфере защиты информационных прав несовершеннолетних

Аннотация. В статье автор определяет защиту информационных прав детей как одно из приоритетных направлений государственной политики России, основные принципы развития законодательства в этой области. Автор выделяет типы информации для детей по степени их полезности, делая вывод, что основным направлением при обеспечении информационной безопасности детей должно быть обеспечение доступа детей к «полезной» информации.

Ключевые слова: дети; безопасность; информационная безопасность; «полезная» информация.

Tatiana I. Sustina,
post graduate of the Law Institute of the Russian University of Transport

Development of legislation in the field of protection of information rights of minors

Abstract. In the article, the author defines the protection of children's information rights as one of the priorities of the state policy of Russia. Defines the basic principles for the development of legislation in this area. The author singles out the

types of information for children according to the degree of usefulness. He concludes that this happened as a result of addressing the information security of children, should be the provision of children with «useful» information.
Keywords: children; security; information security; «useful» information.

Указом Президента РФ от 29.05.2017 № 240 в целях совершенствования государственной политики в сфере защиты детства, учитывая результаты, достигнутые в ходе реализации Национальной стратегии действий в интересах детей в 2012—2017 годах 2018—2027 гг. в Российской Федерации объявлены десятилетием детства. Данным Указом на высшем уровне установлен приоритет прав детей и защита их интересов в рамках государственной политики.

В современных условиях жизни дети стали активными пользователями сети Интернет, однако в силу своего возраста, психологической и физической незрелости именно дети являются более уязвимыми к воздействию на них ИКТ-среды, а соответственно требуют большего внимания государства в целях защиты своих прав.

Ввиду активного поведения детей в киберпространстве направления развития законодательства в сфере информационной безопасности детей должны исходить из следующих принципов:

1) государство, общество и законные представителей несовершеннолетних обеспечивают защиту информационных прав несовершеннолетних, как субъектов информационного права, которые состоят из совокупности правовых норм, закрепляющих их права на создание, обладание, использование и распространение информации, а также состояние их защищенности, определяемое обеспечением информационной безопасности несовершеннолетних, а также права на безопасную цифровую среду и приоритетного обеспечения доступа к «полезной» информации;

2) государству, обществу и законным представителям несовершеннолетних необходимо создавать условия для нахождения несовершеннолетних в состоянии защищенности при использовании ИКТ-среды. Под состоянием защищенности необходимо понимать ограждение несовершеннолетнего субъекта от угроз деструктивного информационного воздействия в цифровой среде посредством обеспечения доступа к полезному контенту, с одной стороны, и формирование «информационного скафандра» несовершеннолетнего с целью

его защиты и формирования самостоятельных навыков фильтрации информации и самозащиты от цифровых угроз как элемента «цифровой зрелости», с другой стороны.

Для определения термина полезности контента необходимо проанализировать законодательство.

Согласно ст. 2 Федерального закона от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» информация, причиняющая вред здоровью и (или) развитию детей», — информация (в том числе содержащаяся в информационной продукции для детей), распространение которой среди детей запрещено или ограничено в соответствии с Законом.

Статья 5 устанавливает виды информации, причиняющей вред здоровью и (или) развитию детей, к которой относится информация:

1) побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству, либо жизни и (или) здоровью иных лиц, либо направленная на склонение или иное вовлечение детей в совершение таких действий;

2) способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, никотинсодержащую продукцию, алкогольную и спиртосодержащую продукцию, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;

3) обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных Законом;

4) отрицающая семейные ценности, пропагандирующая нетрадиционные сексуальные отношения и формирующая неуважение к родителям и (или) другим членам семьи;

5) оправдывающая противоправное поведение;

6) содержащая нецензурную брань;

7) содержащая информацию порнографического характера;

8) о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), включая фамилии, имена, отчества, фото- и видеоизображения такого несовершеннолетнего, его родителей и иных законных представителей, дату рождения такого несо-

вершеннолетнего, аудиозапись его голоса, место его жительства или место временного пребывания, место его учебы или работы, иную информацию, позволяющую прямо или косвенно установить личность такого несовершеннолетнего.

К информации, распространение которой среди детей определенных возрастных категорий ограничено, относится информация:

1) представляемая в виде изображения или описания жестокости, физического и (или) психического насилия (за исключением сексуального насилия), преступления или иного антиобщественного действия;

2) вызывающая у детей страх, ужас или панику, в том числе представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий;

3) представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;

4) содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

Согласно ст. 4 Федерального закона от 24.07.1998 №124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации» целью государственной политики в интересах детей является содействие физическому, интеллектуальному, психическому, духовному и нравственному развитию детей, воспитанию в них патриотизма и гражданственности, а также реализации личности ребенка в интересах общества и в соответствии с не противоречащими Конституции РФ и федеральному законодательству традициями народов Российской Федерации, достижениями российской и мировой культуры.

Согласно толковому словарю Ушакова «полезный» означает приносящий пользу и является противоположным по значению слову «вредный».

Представляется, что полезность информации для несовершеннолетних могут определять ее качественные характеристики. Однако ограничивать такие характеристики условиями, установленными ст. 2, 5 Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию», не достаточно. Ограничивая качественные характеристики полезности информации указанными

нормами права, информационный продукт соответствует информации не вредной. Исключая из характеристик информации всю вредную информацию в информационном пространстве, можно говорить, что остальная информация классифицируется на информацию:

— нейтральную, например, рекламу, соответствующую указанным нормам закона;

— полезную для развития и образования детей. К полезной информации может быть отнесена информация, которая способствует физическому, интеллектуальному, психическому, духовному и нравственному развитию детей, воспитанию в них патриотизма и гражданственности, а также реализации личности ребенка в интересах общества и в соответствии с не противоречащими Конституции РФ и федеральному законодательству традициями народов Российской Федерации, достижениями российской и мировой культуры.

Таким образом можно систематизировать информацию для детей на вредную, нейтральную (т.е. не наносящую вреда и не приносящую пользу) и полезную информацию.

Важной задачей государства должно стать оказание всесторонней и помощи детям, родителям и учителям в формировании так называемой «цифровой зрелости», в противодействии цифровому насилию, в получении качественного интернет-образования.

Решение этой проблемы видится в разработке эффективных государственных программ в области образования, семейной и молодежной политики, центральным звеном которых было бы обеспечение информационной безопасности детей.

Тарасова Марина Сергеевна,
аспирант Юридического института Российского университета транспорта (МИИТ)

Смарт-контракты: правовые аспекты реализации

Аннотация. В статье рассматривается правовая природа смарт-контракта, его специфическая особенность, а также отличие от электронного контракта. Определены положительные и отрицательные стороны влияния

на сферу человеческой деятельности. Особый упор сделан на перспективы развития правового регулирования смарт-контрактов в законодательстве РФ.
Ключевые слова: смарт-контракт; умный контракт; цифровой контракт; электронный контракт; цифровая платформа.

Marina S. Tarasova,
post graduate of the Law Institute of the Russian University of Transport

Smart contracts: legal aspects of implementation

Abstract. This paper deals with the legal nature of a smart contract, its specific feature, as well as the difference from an electronic contract. The positive and negative sides of the influence on the sphere of human activity are determined. Particular emphasis is put on the prospects for the development of legal regulation of smart contracts in the legislation of the Russian Federation.
Keywords: smart contract; digital contract; electronic contract; digital platform.

Банк России определяет «умный контракт» (смарт-контракт) как цифровой контракт, предусматривающий автоматизацию исполнения, контроля и учета юридически значимых действий и событий в рамках ИТ-систем[1]. В законодательстве РФ понятия «смарт-контракт» или «цифровой контракт» не закреплены, однако с внесением изменений в ст. 309 Гражданского кодекса Российской Федерации урегулирована сама возможность их заключения, установлено, что условиями сделки может быть предусмотрено исполнение ее сторонами возникающих из нее обязательств при наступлении определенных обстоятельств без направленного на исполнение обязательства отдельно выраженного дополнительного волеизъявления его сторон путем применения информационных технологий, определенных условиями сделки.

Смарт-контракт следует отличать от электронного договора, последний является электронной версией традиционного договора на бумажном носителе, тогда как смарт-контракт — это договор, существующий в форме программного кода.

[1] Основные направления развития финансового рынка Российской Федерации на 2022 год и период 2023 и 2024 годов (разработаны Банком России) // http://www.cbr.ru/about_br/publ/onfinmarket/ (дата обращения: 31.01.2022).

По мнению Антона Вашкевича, «смарт-контракт — разновидность письменной формы сделки. По своей сути фиксация условий сделки в виде программного кода является разновидностью письменной формы»[1]. Однако возможен и иной подход, заключающийся в том, что цифровая форма является самостоятельной формой сделки, не закрепленной в настоящий момент законодательством РФ.

Специфической особенностью смарт-контракта является среда, необходимая для его заключения. Как правило, ею выступает «цифровая платформа», т.е. информационная система, работающая через сеть Интернет, которая обеспечивает взаимодействие участников платформы друг с другом, позволяя им создавать и обмениваться ценностями. Вместе с тем периметр ИТ-систем не может исключать и системы без доступа к сети Интернет, в этом случае взаимодействие участников контракта в любом случае должно обеспечивается при посредничестве автоматического устройства, действующего по заранее заложенной программе.

Традиционно смарт-контракты классифицируют в зависимости от сферы их применения — имущественные отношения, банковская сфера, страхование, электронное правительство, краудфандинг и т.д. Перечень является открытым и не перестает расширяться.

Безусловными преимуществами смарт-контракта являются:

— сокращение сроков на его заключение и исполнение, это происходит благодаря автоматизации процессов;

— автоматическое создание протокола исполнения контракта, что позволяет снимать споры и разногласия сторон, касающиеся просрочки.

Вместе с тем нельзя не упомянуть и о недостатках смарт-контрактов:

— автоматизация процессов практически исключает какую-либо вариативность в случае нестандартной ситуации, которая не была предусмотрена на этапе написания программного кода для смарт-контракта;

— ошибки в цифровом коде смарт-контракта, которые могут быть заложены на этапе работы юриста и/или программиста, либо вызваны внешними факторами (компьютерный вирус, перепады электрического напряжения и прочее);

[1] Вашкевич А. Смарт-контракты: что, зачем и как. М. : Симплоер, 2018 С. 73.

— недостаточно развитое правовое регулирование сферы цифрового права;

— неготовность отдельных субъектов выступить стороной смарт-контракта (низкий уровень компьютерной грамотности, сложности с оформлением электронной подписи, например, для иностранцев в России и прочее).

Не смотря на то что изменение в ст. 309 ГК РФ внесено в 2019 г., правоприменительная практика этой новой нормы отсутствует. Это связано в первую очередь с тем, что смарт-контракты пока не получили широкое распространение в хозяйственном обороте нашей страны.

Для развития института смарт-контрактов необходимо не только внедрение большего числа цифровых платформ, но также разработка и принятие нормативных правовых актов, регулирующих данную сферу правоотношений.

По мнению А. И. Савельева, для функционирования смарт-контрактов, строго говоря, не требуется правовая система, они способны существовать в правовом вакууме[1]. Однако в этом случае очень велик риск нарушения одного из ключевых принципов гражданского законодательства РФ о признании равенства участников регулируемых им отношений и защите от злоупотребления доминирующим положением на рынке. В рамках смарт-контракта такой доминирующей стороной всегда будет разработчик кода, т.е. составитель смарт-контракта.

В целях регулирования правоотношений в сфере смарт-контрактов первоочередным действием видится закрепление понятийного аппарата — определение терминов «смарт-контракт» и «цифровая платформа» на уровне закона. Далее должны быть определены условия, исходя из которых, смарт-контракт можно квалифицировать как заключенный или незаключенный договор, а именно, установить соблюдена ли его форма. Необходимо выработать механизмы защиты стороны «присоединяющейся» к смарт-контракту. Следует установить правила определения подсудности и подведомственности споров, основанных на смарт-контрактах.

[1] Савельев А. И. Договорное право 2.0: «умные» контракты как начало конца классического договорного права // Вестник гражданского права. 2016. № 3. С. 32—60.

Троицкий Александр Олегович,
аспирант Юридического института Российского университета транспорта (МИИТ)

Состояние и тенденции незаконного оборота оружия в киберпространстве

Аннотация. Статья посвящена проблеме предупреждения преступлений, связанных с нелегальным оборотом оружия в киберпространстве. Приводятся статистические данные, характеризующие незаконный оборот оружия в Российской Федерации и за рубежом. Раскрываются способы реализации и приобретения оружия в сети Интернет. Сформулирован вывод о необходимости установления ответственности за распространение информации о способах преобразования предметов конструктивно схожих с оружием в боевое.

Ключевые слова: кибербезопасность; нелегальный оборот оружия; безопасность в сети Интернет; профилактика преступлений; предупреждение преступлений.

Alexander O. Troitsky,
post graduate of the Law Institute of the Russian University of Transport

The state and trends of illegal arms trafficking in cyberspace

Abstract. The article is devoted to the problem of preventing crimes related to illegal arms trafficking in cyberspace. Statistical data characterizing illegal arms trafficking in the Russian Federation and abroad are presented. The methods of selling and purchasing weapons on the Internet are revealed. The conclusion is formulated about the need to establish responsibility for the dissemination of information about ways to transform objects structurally similar to weapons into combat.

Keywords: cyber-security; illegal arms trafficking; security on the Internet; crime preventative; crime prevention.

Стремительное развитие информационных технологий интенсивно влияет на появление новых угроз для личности, общества и государства. Одной из таких угроз является незаконный оборот оружия, осуществляемый в киберпространстве. Криминальный оборот оружия

затрагивает как внутригосударственный, так и транснациональный рынок сбыта и выступает опаснейшим явлением в связи с тем, что множество посягательств, таких как: убийства, разбои, вымогательства, террористические акты и др., совершаются именно с применением оружия[1].

Данные Управления ООН по наркотикам и преступности говорят о ежегодном росте преступлений в сфере незаконного оборота оружия. Каждый год странами участницами насчитывается примерно 550 тыс. единиц оружия, изъятого из нелегального оборота[2]. Данные цифры исследователями считаются чрезвычайно заниженными в связи с тем, что преступления в сфере оборота оружия имеют высокий уровень латентности, чему в большей степени способствует информационно-коммуникационная среда.

Показатели преступности, связанной с незаконным оборотом оружия на территории РФ, составляли: в 2017 г. — 28 916 преступлений, в 2018 г. — 27 452 преступления, в 2019 г. — 26 557 преступлений, в 2020 г. — 24 792 преступления, в 2021 г. — 23 507 преступлений[3]. Несмотря на снижение общей динамики рассматриваемых преступлений, наблюдается стабильная доля нераскрытых преступлений: в 2019 г. — 7365, что составляет 27,53% от общего числа зарегистрированных преступлений, в 2020 г. — 6715, что составляет 27,15% от общего числа зарегистрированных преступлений, в период с января по декабрь 2021 г. — 28,11% от числа зарегистрированных преступлений[4].

Одним из факторов, обусловливающих сложности выявления, расследования и раскрытия преступлений, связанных с незаконным оборотом оружия, является использование преступниками быстроразвивающихся современных технологий. Неподконтрольные государству интернет-ресурсы становятся основными площадками, на которых реализуется криминальное оружие. К их числу относятся ресурсы обеспечения анонимности, зачастую использующие системы многоуровневой маршрутизации и ключей-шифрования, такие как

[1] Задоян А. А. Незаконный оборот оружия: международно-правовой аспект // Юрист. 2011. № 14. С. 42.

[2] United Nations office on drugs and crime «Global Study on Firearms Trafficking». UN, New York 2020 г. P. 3—6.

[3] URL: http://crimestat.ru (дата обращения: 06.02.2022).

[4] Там же.

Dedicated-серверы, *VPN*-сервисы, *Tor*, I2P, а также *SSH*-туннели[1]. В совокупности данные сервисы образовывают информационно-коммуникационные поля: «*DarkNet*», «*DeepWeb*», «*DarkWeb*».

Необходимо отметить, что и в общей среде сети Интернет существуют площадки по продаже оружия. Проводимый нами анализ информационных ресурсов выявил ряд магазинов, привлекающих клиентов в мессенджере «*Telegram*». Так, группа-магазин осуществляла деятельность по поиску клиентов для продажи им травматического оружия без лицензии на условиях полной анонимности. Механизм работы магазина предусматривал рекламирование данного сообщества под разными названиями. При переходе в данную группу лицо, заинтересованное в покупке оружия, обнаруживало ссылку для перехода на внешний сетевой ресурс «теневого интернета», где в последствии совершается незаконная сделка купли-продажи.

Реализация незаконного оружия в «теневых» ресурсах сети Интернет происходит при помощи браузера «Tor» с использованием асимметричного шифрования. Лицо, имеющее преступный умысел (далее продавец), создает публичный ключ, при помощи которого лицо, имеющее умысел на покупку оружия (далее покупатель), отправляет ему зашифрованное сообщение, которое может просмотреть только продавец. Далее механизм совершения сделки проводится при помощи цифровой валюты (биткойн) с использованием системы защиты покупателя «Гарант». Покупатель производит оплату товара через специализированную площадку, которая перейдет продавцу только после получения товара. Продавец помещает оружие в специальный тайник на определенной местности и после подтверждения оплаты отправляет координаты данного тайника покупателю[2].

Таким образом, задача по выявлению и пресечению такого рода преступлений правоохранительными органами усложняется. В связи с этим необходимо тесное сотрудничество со специалистами в обла-

[1] Сергеев С. М. Некоторые проблемы противодействия использованию в преступной деятельности средств обеспечения анонимизации пользователя в сети Интернет // Вестник Санкт-Петербургского университета МВД России. 2017. № 1(73). С. 137—140.

[2] Каримов В. Х. Влияние современных информационно-телекоммуникационных технологий на криминальный оборот огнестрельного оружия и боеприпасов // Право и политика. 2019. С. 2—4.

сти программирования и информационной безопасности, для моделирования данных ситуации, с последующим выявлением точек интереса (маркеров), наличие которых могло бы послужить указателем для правоохранительных органов о готовящихся и совершенных преступлениях. Также необходимо обратить внимание на усиленное установление контроля за использованием сети Интернет в целях нелегального оборота оружия, заключающиеся в постоянном мониторинге и выявлении нелегальных площадок[1].

Теневая продажа и приобретение оружия в сети Интернет является не единственной угрозой безопасности в данном направлении. Опасным явлением также представляется размещение схем, инструкций, обучающих видео, по переделке предметов конструктивно схожих с оружием в предметы, которые соответствуют всем критериям боевого оружия. Опасность нахождения данной информации в ресурсах сети Интернет заключается в возможности воспроизведения при помощи полученных из нее данных технического процесса и тем самым создания огнестрельного оружия.

Так, одним из примеров негативного влияния данной информации приводится в приговоре Ступинского городского суда Московской области от 09.07.2020 № 1-151/2020 по делу № 1-151/2020, согласно которому гражданин Б. Д. В. у себя дома просматривал видеоролики по изготовлению и переделке огнестрельного оружия и боеприпасов к нему. В один из дней у данного лица возник приступный умысел на переделку охолощенного оружия в нарезное огнестрельное, а также на изготовление боеприпасов к нему. Для проверки своих возможностей и теоретических навыков, приобретенных путем просмотра видеороликов, Б. Д. В. через интернет-магазины приобрел все необходимое в свободной продаже, а именно:

— охолощенное оружие пистолет модели «*Baikal CX* 442»;

— изготовленный заводским способом макет массово-габаритного ствола пистолета Макарова (ПМ) (нарезной ствол без патронника);

— развертки патронника 9×18 мм от ПМ;

— пресс ручной для снаряжения патронов «*LEE*», к нему матрицы для патронов калибром 9×18 мм «ПМ» и возвратную пружину;

[1] Мазур А. А. Актуальные проблемы предупреждения преступности в социальной сети Даркнет // Вестник Российского университета кооперации. 2018. № 3 (33).

— пустые гильзы и пули в количестве 250 штук для последующего снаряжения их порохом и изготовления боеприпасов.

Б. Д. В., продолжая реализовывать свой преступный умысел, направленный на незаконную переделку оружия и изготовление боеприпасов к нему, используя дрель, высверлил штифт, который удерживал оригинальный деактивированный ствол в данном оружии, после чего используя молоток, выбил данный ствол. Продолжая реализовывать совой преступный умысел, Б. Д. В. в ранее приобретенном им макете ствола сформировал патронник под стандартный патрон 9×18 мм и с помощью тисков запрессовал ствол в рамку пистолета, затем используя напильник и наждачную бумагу, сформировал горку подачи патрона. Таким образом Б. Д. В. произвел замену ствола охолощенного пистолета, тем самым по заключению проведенной баллистической экспертизы получил во владение пистолет, пригодный для стрельбы патронами калибра 9×18 мм с метаемым снаряжением и относящимся к категории короткоствольного нарезного огнестрельного оружия.

Помимо инструктажей, зачастую лица, их публикующие, предлагают приобрести у них «заготовки» для переделки охолощенного, сигнального или пневматического оружия в боевое. Данные предметы продажи могут свободно пересылаться почтой или продаваться через любые торговые площадки, так как по законодательству не являются основными частями оружия. Чаще всего данными «заготовками» выступают: макеты стволов, части ударно-спускового механизма и т.д.

Резюмируя все вышесказанное, необходимо отметить, что незаконный оборот оружия является фактором, обусловливающим совершение множества преступлений, обладающих определенной спецификой, которую необходимо учитывать при разработке мер предупреждения такого вида преступной деятельности. Особое внимание необходимо обращать на преступления, совершаемые с использованием информационно-коммуникационных технологий, так как они являются одними из наиболее опасных ввиду высокой латентности.

Для предупреждения деятельности по распространению информации по переделке оружия нами предлагается установить уголовную (административную) ответственность за публикацию подобных материалов, в том числе в сети «Интернет», исключив из круга субъектов

лиц, осуществляющих лицензированную образовательную, научную, конструкторскую деятельность, а также деятельность, напрямую связанную с необходимостью ограниченного распространения данной информации.

Шашкин Александр Андреевич,
аспирант Юридического института Российского университета транспорта (МИИТ)

Основные направления обеспечения кибербезопасности на транспорте

Аннотация. Актуальность данного исследования обусловливается тем, что в последние годы киберпреступность проникла практически во все сферы общественной деятельности. Не исключением стал и транспорт (автомобили, железнодорожные пути, самолеты и т.д.). Таким образом объектом данного исследования выступают ключевые направления обеспечения кибербезопасности на транспорте.

Ключевые слова: транспорт; направления деятельности; кибербезопасность; киберпреступность; деятельность правоохранительных органов.

Alexander An. Shashkin,
post graduate of the Law Institute of the Russian University of Transport

Main directions for ensuring cyber security in transport

Abstract. The relevance of this study is due to the fact that in recent years cybercrime has penetrated almost all spheres of public activity. Transport (cars, railroad tracks, airplanes, and so on) was no exception. Thus, the object of this study is the key areas for ensuring cybersecurity in transport.

Keywords: transport; activities; cybersecurity; cybercrime; law enforcement activities.

XXI век — это век инновационных технологий, которые стали одним из ключевых направлений государственной политики. В связи с этим встал вопрос о защите данных технологий от преступных пося-

гательств. Таким образом, появилось такое понятие, как кибербезопасность — это относительно новый термин, означающий исключение постороннего вмешательства в информационную собственность, как целой страны, так и отдельно взятого человека.

Современный мир уже невозможно представить без цифровых гаджетов, умных технологических устройств, 3D-моделирования и прочее. Цифровым технологиям свойственно динамичное, постоянно прогрессирующее состояние. Люди уже привыкли доверять все свои личные данные: банковские счета, паспортные данные, документы на автомобиль и прочее информационным хранилищам. В связи с этим у некоторых людей возникает соблазн воспользоваться чужими данными из корыстных целей. Так и появилась киберпреступность — это преступления в сфере информационных технологий, которые направлены на получение частной информации с целью извлечения собственной выгоды. Достигается все это путем взлома паролей, внедрения вредоносных программ, хищения денежных средств с банковских карт или же паролем самих банковских карт, распространением заведомо ложной информации о других лицах.

Федеральные законы от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» регулируют безопасность информационной инфраструктуры. По сути это единственные законы в Российской Федерации, которые регламентируют порядок обеспечения информационной безопасности.

Киберпреступность за последние несколько лет стала носить глобальный характер и представлять собой серьезную проблему не только для отдельно взятых граждан, которые пострадали от преступлений такого рода, но и для государственностей политики. В России доля раскрытия киберпреступности приходиться на оперативно-розыскные органы, которые сталкиваются со следующими преступлениями:

— мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ);

— сбыт наркотических средств, психотропных веществ или их аналогов, совершенные с использованием информационно-телекоммуникационных сетей, включая сеть Интернет (п. «б» ч. 2 ст. 228.1 УК РФ);

— распространение через сеть Интернет призывов к экстремистской деятельности (или ее пропаганда, ст. 282.1 и 282.2 УК РФ).

Выше перечисленные примеры далеко не являются исчерпывающими, а лишь показывают самые распространенные преступные деяния в сфере киберпреступности.

Однако из всех видов преступлений самым распространенным является киберпреступность на транспорте. За последние несколько лет все чаще в новостях можно увидеть, как произошла утечка личных данных пользователей системой каршеринга, незаконная продажа транспортных карт с бесконечным балансом на счету, взлом электросамокатов и многое другое, что нарушает транспортную безопасность.

Таким образом возникла киберпреступность на транспорте. А кибербезопасность на транспорте[1] — это система безопасности, которая защищает личные данные пользователей, предоставивших свои данные той или иной организации, связанной с транспортной сферой; также это защита транспортных информационных систем на таких объектах, как железнодорожные пути, воздушный транспорт, водный транспорт.

За кибербезопасностью на транспорте следят соответствующие правоохранительные органы. Однако такого подразделения или органа, как киберполиция, нет, но существуют структуры, которые претендуют на данное наименование, так как борются с киберпреступностью. К ним относятся органы, осуществляющие оперативно-розыскную деятельность (МВД, ФСБ России и прочее), управление «К» — подразделение МВД России, а также подразделение «БСТМ» (бюро специальных технических мероприятий).

Данные органы работают по следующим основным направлениям по обеспечению кибербезопасности на транспорте[2]:

1) проведение оперативных исследований, а также экспертиз (назначение следователем компьютерно-технических экспертиз). Данные исследования и заключения позволят понять точный меха-

[1] Айсанов Р. М. Компьютерная информация как предмет преступления, предусмотренного ст. 272 УК РФ // «Черные дыры» в российском законодательстве. 2017. № 1. С. 279—280.

[2] Лапонина, О. Р. Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия. М., 2018.

низм совершения преступления, последовательность проведения преступных действий. С помощью анализа таких заключений можно составить примерный план расследования, какие технические средства понадобятся. Самую ключевую роль здесь играет специалист или эксперт, который обладает специальными навыками и познаниями в данной области. Данный специальный субъект может расшифровать компьютерный (программный язык), ответить на интересующие нас вопросы, дать экспертную оценку механизма совершенного преступления, которая в дальнейшем послужит доказательством в судебном порядке;

2) проведение профилактических (виктимологических) работ с населением. 90% всех мошеннических операций происходит по вине самих потерпевших, которые предоставляют данные банковских карт неизвестным лицам, переводят собственные денежные средства, не читают условия договора (например, с каршеринговой компанией). Можно сделать вывод, что люди сами же помогают мошенникам совершить в отношении себя преступление. Таким образом стоит проводить профилактическую работу с населением путем бесед, расклеивания листовок. Однако как быть с транспортными организациями, которые не предоставляют никому свои данные? В данном случае нужно проводить проверки по наличию соответствующих систем безопасности на транспортных объектах, всех лицензионных документов, которые требуются для установки соответствующего уровня защиты;

3) внедрение постоянного мониторинга за технической оснащенностью организаций, которые связанны с транспортной сферой. Каждая организация должна понимать, что любая кибератака может привести не только к потере каких-либо денежных средств, но и к человеческим жертвам, так как речь идет о транспортной сфере. Например, кибератака привела к сбою алгоритма работы железнодорожных путей, после чего два поезда стали направляться друг в друга по одной железнодорожной полосе;

4) непрерывное улучшение программного обеспечения. Данный фактор достигается привлечением компетентных специалистов, использованием профессионального и лицензионного оборудования для настройки безопасности на транспорте. Все это и многое другое

должно реализовываться самими организациями, а также контролироваться правоохранительными органами;

5) совершенствование законодательной базы, в которую бы входили правила, методики, условия работы, связанные с кибербезопасностью на транспорте;

6) противодействие потенциальным преступным лицам, которые собираются совершить кибератаку. Безусловно, в современных реалиях практически невозможно понять, кто собирается совершить преступление данного рода. Однако правоохранительным органам следует регулярно проверять лиц, которые недавно отбыли свое наказание за киберпреступления;

7) совершенствование материально-технической базы правоохранительных органов для более качественного раскрытия и предотвращения киберпреступлений на транспорте.

Таким образом были рассмотрены основные направления, по которым стоит работать не только контролирующим органам, но и самим организациям и обществу в целом для того, чтобы обеспечить кибербезопасность на транспорте.

Кибербезопасность на транспорте в современных условиях — одна из первостепенных задач государственной политики, на которую стоит обратить особое внимание, а именно: создать единый центр по подготовке высококвалифицированных специалистов в сфере IT-технологий; составить новые законопроекты, регламентирующие порядок, методики и техники расследования киберпреступлений; обеспечить современной материально-технической базой все подразделения, которые тем или иным образом связанны с борьбой с информационной преступностью; проводить более тщательную профилактику населения в сфере информационной грамотности.

Логинова Людмила Николаевна,
кандидат технических наук, доцент, доцент кафедры «Управление и защита информации» Российского университета транспорта (МИИТ)

Шиян Владислав Иванович,
студент Российского университета транспорта (МИИТ)

Аспекты правового регулирования технологии блокчейн

Аннотация. Освящены проблемы совершенствования налогового законодательства РФ на этапе активного внедрения блокчейн-технологии, которая характеризуется противоречивостью тенденций правового регулирования цифровых технологий. Актуальность исследования вопросов применения блокчейн в налоговых отношениях обусловливается необходимостью оценки налоговых последствий сделок, совершаемых с использованием цифровых финансовых активов, основанных на технологии блокчейн, а также появлением новых направлений совершенствования налогового контроля с применением блокчейн-технологии. Проведенное исследование показывает опосредованность анализа технологии блокчейн для целей правового регулирования, осуществляемого путем выработки концепций использования данного технологического решения в качестве инструмента при осуществлении криптовалютных операций.

Ключевые слова: блокчейн-технология; цифровые транзакции; криптовалюта; правовое регулирование; международное регулирование; зарубежные исследования.

Ludmila N. Loginova,
ScD, Associate Professor, Department of Control and Information Security Russian University of Transport

Shiyan I. Vladislav,
student of Russian University of Transport

Aspects of legal regulation of blockchain technology

Abstract. The problems of improving the tax legislation of Russia at the stage of active implementation of blockchain technology, which is characterized by the in-

consistency of trends in the legal regulation of digital technologies, are consecrated. The relevance of studying the issues of using blockchain in tax relations is determined by the need to assess the tax consequences of transactions made using digital financial assets based on blockchain technology, as well as the emergence of new areas for improving tax control using blockchain technology. The conducted research shows the indirectness of the blockchain analysis for the purposes of legal regulation, carried out by developing concepts for using such a technological solution as a tool in the implementation of cryptocurrency transactions.

Keywords: blockchain technology; digital transactions; cryptocurrency; legal regulation; traceability; international regulation; foreign research.

Современная экономическая наука находится под сильным влиянием процесса информатизации. Информационная экономика приносит новые экономические явления, но в силу своей новизны они до конца не изучены. К явлению современной сетевой экономики относятся электронные деньги.

При рассмотрении феномена «электронные деньги» с точки зрения информационных технологий можно прийти к выводу, что криптовалюта — это цифровая валюта, выпуск и подсчет которой основан на шифровании[1]. Особым сторонником использования криптовалюты в качестве платежного средства является Япония, в которой с 1 апреля 2017 г. криптовалюты приравнены к иностранным валютам и рассматриваются как законное средство платежа. При этом нормативным правовым актом, детально регулирующим обращение виртуальных валют, является Закон Японии от 24.06.2009 № 54 «О платежных услугах».

Государственное регулирование в Японии затронуло три направления:

1) легальное понятие биткоина и виртуальной валюты. Несмотря на признание на территории Японии криптовалют блокчейн и эфириум, последние не являются легализированной валютой, а лишь официальным платежным средством, «выполняющим функции валюты»;

2) регулирование рынка криптовалют. Согласно правилам от бирж криптовалют требуется принять стандарты *KYC/AML*, используемые в

[1] URL: https://dic.academic.ru/dic.nsf/ruwiki/840224 (дата обращения 25.01.2022).

других странах, получить лицензии на торговлю виртуальной валютой и зарегистрироваться в Японском агентстве финансовых услуг (*FSA*), которое регулирует выпуск национальной валюты;

3) налогообложение: с 1 июля 2017 г. виртуальная валюта освобождена от уплаты 8% налога на потребление (*JCT*), аналога российского НДС. Доход от виртуальной валюты относится к числу прочих поступлений и является доходом от ведения бизнеса, который облагается налогом на прибыль и прирост капитала[1].

Китай включил разработку технологии блокчейн в план национального развития на 2016—2020 гг., став одним из первых государств, включившим технологию в официальную политику[2].

В настоящее время цифровизацию валют проводят и в Европе, в частности, в Швейцарии в деревне Церматт местным жителям разрешено платить налоги в биткойнах. 9 марта 2020 г. конгрессмен Пол Госар представил законопроект о криптовалюте, направленный на определение и регулирование индустрии цифровых активов в США. Авторы вышеупомянутого проекта полагают, что законопроект призван обеспечить не только ясность, но и легитимность криптоактивов в США[3].

Интерес также представляет российское законодательство в отношении регулирования сферы блокчейн. Отсутствие законодательных актов, регулирующих сферу деятельности криптовалюты в Российской Федерации, порождает споры среди экспертов в этой области. В отчете Федерального совета о виртуальных валютах были названы следующие потенциальные области применения блокчейн: логистика, микротранзакции и маркетинг (в виде бонусных баллов)[4].

---

[1] URL: https://forknews.io/legal/000304-pravovoj-status-kriptoval.html (дата обращение 25.01.2022).

[2] URL: http://www.gov.cn/zhengce/content/2016-12/27/content_5153411.htm (дата обращения 25.01.2022).

[3] URL: https://coinspot.io/law/us_and_canada/v-kongresse-ssha-predstavili-obnovlennuyu-versiyu-zakona-o-kriptovalyute-2020-goda/ (дата обращения 26.01.2022).

[4] URL: https://www.news.admin.ch/NSBSubscriber/message/attachments/35355.pdf (дата обращения 26.01.2022).

Большое число возможностей для применения блокчейн можно найти в первую очередь в финансовой сфере, поскольку организации, которые перейдут на блокчейн-технологии, смогут сделать более эффективными ранее дорогостоящие и ненадежные операции, а также установить новые модели сотрудничества. Как верно отметил А. А. Ситник, «вышеперечисленные направления деятельности в области применения цифровых технологий свидетельствуют о том, что в настоящее время формируется цифровое пространство»[1], в рамках которого необходимо определить сферу правового регулирования цифровых активов и порядок реализации и взаимодействия субъектов этих прав[2].

Цифровые права являются воплощением универсальных прав человека (через законы), гарантированных международным правом и национальными конституциями, и связаны с потребностями отдельных лиц и граждан в информационном обществе[3].

Задача выработки как общеправовых, так и отраслевых (и прежде всего в сфере налогового права) подходов к вопросу легализации в целом, а также к нормативному регулированию границ, форм и способов применения технологии блокчейн признается одной из первостепенных задач государственного уровня. Для налогового права она актуализируется прецедентами использования блокчейн-технологии налоговыми органами для сокращения издержек, связанных с бумажным документооборотом. Например, в 2020 г. на основе применения блокчейн-технологии создана цифровая платформа ФНС России (постановления Правительства РФ от 02.04.2020 № 422 «Об утверждении Правил предоставления субсидий из федерального бюджета российским кредитным организациям на возмещение недополученных ими доходов по кредитам, выданным в 2020 году субъектам малого и среднего предпринимательства на неотложные нужды для поддержки и сохранения занятости», от 16.05.2020 № 696 «Об утверждении Правил предоставления субсидий из федерального бюджета российским

[1] URL:https://cyberleninka.ru/article/n/ponyatie-i-pravovoe-regulirovanie - kriptovalyuty-v-zarubezhnyh-stranah (дата обращения: 25.01.2022).

[2] Актуальные проблемы блокчейн-технологий в финансовом праве / под ред. Е. Ю. Грачевой, Л. Л. Арзумановой. М. : Норма, 2021.

[3] Там же.

кредитным организациям на возмещение недополученных ими доходов по кредитам, выданным в 2020 году юридическим лицам и индивидуальным предпринимателям на возобновление деятельности»), которая обеспечивает информационный обмен сведениями между налогоплательщиками, банками (первыми получили возможность подключения ВТБ и Сбербанк, а позднее к проекту присоединились и другие банки), внебюджетными фондами и налоговыми органами для обеспечения льготного кредитования малого и среднего бизнеса в условиях распространения новой коронавирусной инфекции COVID-19. Помимо этого дальнейшее внедрение блокчейн-технологий в налоговые отношения планируется осуществить с целью полного отказа от налоговой отчетности.

Однако такие международные решения встречаются очень редко. Несмотря на большой объем торгов криптовалютами, глобальных законов и правил не существует. Обсуждения темы среди отечественных специалистов начались одновременно с появлением нынешних криптовалют в 2009 г. Первой реакцией российских властей, когда-то ознакомившихся с технологией, было рассмотрение новых запретов. Однако с апреля 2018 г. все изменилось. Премьер-министр поручил изучить перспективу использования блокчейна для решения административных задач на федеральном уровне. Через месяц был сформирован Архивный комитет. Его основная задача — создание стандартов технологии блокчейн, а также систем, основанных на распределенных методах хранения и обработки информации. Проект берет на себя разрешение предприятия и организатора, определение достаточных условий и механизма выкупа токена[1].

Итак, говоря про особенности правового регулирования технологии блокчейн, можно сделать вывод, что правовое регулирование, несомненно, придет, и оно постепенно внедряется в различных странах, поскольку в настоящее время мы наблюдаем сопротивление технологии блокчейн внешнему противодействию.

При внедрении блокчейн-технологии в правовое регулирование Российской Федерацией отношений, связанных с прослеживаемостью товаров, на основании такого зарубежного опыта необходимо руко-

[1] URL: https://ex4.ru/blokchejn/pravovoe-regulirovanie-blokchejna-v-rossii-i-v-mire/ (дата обращения 25.01.2022).

водствоваться следующими принципами: безопасность, защищенность личных данных, децентрализация, прозрачность, доступность, консенсус (доверие).

В настоящее же время большинство исследователей все еще придерживаются точки зрения об отсутствии необходимости правового регулирования понятия технологии блокчейн.

Землина Ольга Михайловна,
кандидат юридических наук, доцент, доцент кафедры «Транспортное право» Юридического института Российского университета транспорта (МИИТ)

Артебякина Ксения Андреевна,
магистрант Юридического института Российского университета транспорта (МИИТ)

Проблемы квалификации финансирования терроризма

Аннотация. Терроризм во всех его формах и проявлениях и по своим масштабам и интенсивности, по своей бесчеловечности и жестокости превратился ныне в одну из самых острых и злободневных проблем глобальной значимости. Проявление терроризма влекут за собой массовые человеческие жертвы, разрушаются духовные, материальные, культурные ценности, которые невозможно воссоздать веками. Он порождает ненависть и недоверие между социальными и национальными группами. В статье рассматриваются проблемы применения уголовного законодательства в области противодействия финансирования терроризма, необходимости международного сотрудничества в сфере перекрытия финансовых потоков, которые направленны на поддержание террористов и их деятельности. Выявлены значимые вопросы, возникающие при обмене информацией между зарубежными странами, касающиеся деятельности террористических организаций и групп, а также вопрос квалификации данной категории преступлений. По результатам сравнительно-правового и формально-догматического анализа международных нормативных правовых актов, законодательства РФ, а также осмысления судебно-следственной практики в статье предложены представляющиеся рациональными способы решения исследуемых вопросов.

Ключевые слова: финансирование терроризма; противодействие терроризму; террористическое сообщество; террористическая организация; международное сотрудничество.

Olga M. Zemlina,
Candidate of Law, Associate Professor, Associate Professor of the Department of "Transport Law" of the Law Institute of the Russian University of Transport

Ksenia An. Artebyakina,
Master's student of the Law Institute of the Russian University of Transport

Problems of terrorist financing qualification

Abstract. Terrorism in all its forms and manifestations, both in its scale and intensity, in its inhumanity and cruelty, has now become one of the most acute and topical problems of global significance. The manifestation of terrorism entails massive human casualties, spiritual, material, and cultural values that cannot be recreated for centuries are being destroyed. It breeds hatred and distrust between social and national groups. The article discusses the problems of the application of criminal legislation in the field of countering the financing of terrorism, the need for international cooperation in the field of blocking financial flows that are aimed at supporting terrorists and their activities. Significant issues arising during the exchange of information between foreign countries concerning the activities of terrorist organizations and groups, as well as the question of the qualification of this category of crimes, have been identified. Based on the results of a comparative legal and formal dogmatic analysis of international normative legal acts, the legislation of the Russian Federation, as well as an understanding of judicial and investigative practice, the article suggests rational ways to solve the issues under study.

Keywords: financing of terrorism; countering terrorism; terrorist community; terrorist organization; international cooperation.

«Российский и зарубежный опыт антитеррористической деятельности показал, что борьба с терроризмом не может быть эффективной, если лишь реагировать на совершенные преступления. Надо активно формировать условия, при которых к минимуму должны быть сведены как сама возможность совершения террористического акта, так и его последствия»[1].

[1] https://rg.ru/2006/03/21/patrushev.html

Особую опасность представляет собой терроризм на транспорте, что предопределено, в первую очередь, сущностными характеристиками транспортной инфраструктуры и объектов транспорта, как источников повышенной опасности [1, стр. 108], имеющих высокую степень уязвимости [2, стр. 17; 3. стр. 37], что делает их особенно привлекательными целями террористических атак [5, стр. 1, 21]. Как основательно отмечается, в совокупности эти проблемы детерминируют необходимость научного и образовательного обеспечения [4, стр. 18; 6].

Одной из самых популярных на сегодняшний день способов содействия террористической деятельности — финансирование терроризма, который нуждается не только в его пресечении, но и предупреждении. Федеральный закон от 06.03.2006 № 35-ФЗ «О противодействии терроризму», пришедший на смену Федеральному закону от 25.07.1998 № 130-ФЗ «О борьбе с терроризмом», направлен не только на противодействие терроризму, но и непосредственно на его предупреждение во всех формах и проявлениях, что повышает эффективность раскрытия данных категорий преступления.

Исследуемая проблема продолжает оставаться особенно актуальной в сфере транспорта [2, стр. 246], учитывая угрозу, представляемую террористическими организациями.

Основательно отмечается, что «террористические и диверсионные акции (угон или захват транспортных средств — воздушных, морских и речных судов, автотранспорта, железнодорожного подвижного состава; взрывы в аэропортах, на железнодорожных вокзалах, портах, на транспортных средствах, на гидротехнических сооружениях и др.) по частоте проявлений и тяжким последствиям находятся на втором месте после чрезвычайных происшествий, вызванных техническим состоянием транспортных систем, но на первом по общественному реагированию» [2, стр. 11].

Особенностью террористических атак на транспорте является то, что «из-за высокой уязвимости, в сравнении со многими другими потенциальными целями, объекты транспорта особенно привлекательны для террористов, так как обычно приводят к большому количеству жертв, могут парализовать ключевые секторы экономики и вызвать серьезные общественные потрясения» [2, стр. 13].

Следует учитывать и то обстоятельство, что «высокая степень уязвимости объектов транспортной инфраструктуры, обусловленная из-

начально их предназначением и, соответственно, открытостью к доступу неограниченному числу лиц, делает указанные объекты особенно привлекательными для террористов» [3, стр. 101]. Эта специфика транспортной инфраструктуры подчеркивается и иными авторами [4, стр. 14, 16; 5, стр. 400], что ставит особые задачи перед правовым образованием специалистов на транспорте [5, стр. 402, 400; 6, стр. 37; 8, стр. 23].

Угроза также исходит от небольших террористических группировок и отдельных террористов, которые могут совершить террористический акт и нанести большие увечья обществу, что также делает своевременное предупреждение террористических атак на транспорте весьма затруднительным, требует особых усилий для подготовки квалифицированных специалистов в области обеспечения транспортной безопасности [1, стр. 128; 4. стр. 14, 16]. Хотя количество и виды террористических ячеек, а также представляемые ими угрозы претерпели изменения со временем, основные потребности террористов в сборе, перемещении и использовании денежных средств остались прежними.

Анализ правоприменительной практики свидетельствует о наличии коллизий в вопросах квалификации финансирования терроризма, что требует глубокой теоретико-прикладной аргументации.

Международные террористические группы не стремятся к финансовой выгоде как к конечной цели, однако им необходимы денежные средства, так как значительные средства тратятся на привлечение новых сторонников, организацию вербовки, боевую подготовку отрядов и наемников, создание современной материально-технической базы. Именно поэтому задача борьбы с терроризмом не сводятся к выявлению и пресечению отдельных террористических преступлений, она гораздо шире и заключается в пресечении самой террористической деятельности, важную роль в существовании которой играет ее финансовая база, которая дает терроризму, его людским и материальным ресурсам наращиваться.

Сбор средств террористическими организациями чаще всего ведется под благотворительными предлогами и через третьих лиц, из этого следует, что проблема состоит в выявлении истинных целей спонсируемой и спонсирующей стороны. Одними из главных источников финансирования терроризма является: пожертвования через социальные и религиозные организации, получение финансовых

средств через законно действующие коммерческие организации, принадлежащие как участникам террористической организации, так и другим людям из сфер строительства, банковского дела, торговли товарами, ресторанного бизнеса. Именно поэтому отслеживание финансовых потоков террористических организаций затруднительно, так как методика финансового контроля направлена на технику отмывания денег, получения их преступным путем.

Создание правовой базы и развитие новых форм правового сотрудничества государств, направленных не только на противодействие терроризма, но и непосредственно на его предупреждение во всех формах и проявлениях, не решает всей проблемы, поскольку для пресечения финансовых операций в пользу террористов необходима своевременная и полная разведывательная информация об истинных ее целях и адресатах. Задача по получению всей необходимой информации относится к компетенции разведывательных органов государства. Однако учитывая глобальный аспект финансирования терроризма, данные органы не обладают всей полнотой необходимых разведывательных данных, что препятствует выявлению и ликвидации международных каналов финансирования. Решение данной проблемы видится в повышении многостороннего уровня сотрудничества между государствами, в том числе в сотрудничестве разведывательных служб, взаимодействие которых должно происходить на основе кодекса поведения в области экономической разведки.

Большое значение имеет установление конечного адресата (террористических организаций или групп) при выявлении и пресечении финансовых операций, осуществляемых в поддержку террористической деятельности. Однако большинство стран в борьбе с финансированием терроризма руководствуются своими списками таких запрещенных на их территории организаций, не признавая решений других стран. Целесообразным видеться выработать согласованную позицию относительно критериев отнесения организаций к террористическим и механизма объявления ее таковой.

Анализируя вышеизложенные проблемы, очевидна необходимость в налаживании постоянного обмена с зарубежными странами информацией, касающейся деятельности террористических организаций и групп. Формы обмена должны устанавливаться с учетом мнения всех заинтересованных сторон.

Еще одним из сложных вопросов квалификации является правовая оценка действий лиц, финансируемых терроризм под воздействием угрожающих факторов. Действия лица, получающего предметы финансирования терроризма, используя при этом угрозы применения насилия или иные способы принуждения, образуют идеальную совокупность, устанавливаемую в ст. 205.1 «Содействие террористической деятельности» и ст. 163 «Вымогательство» УК РФ. Однако встает вопрос о квалификации действий лиц, предоставивших предметы финансирования терроризма под воздействием угрозы применения насилия и иных способов принуждения.

Данный вопрос стоит решать в плоскости определения наличия реальной возможности или невозможности отказаться от предоставления средств финансирования терроризма.

Если у лица есть возможность уклониться от предоставления указанных средств, т.е. выдвигаемые в его адрес угрозы и иные способы принуждения не воспринимаются как реальные, то его действия следует квалифицировать в соответствии со ст. 205.1 «Содействие террористической деятельности» УК РФ. Однако если лицо не имело возможности отказаться от предоставления средств финансирования, в силу реального оказания на него давления и принуждения, то его действия стоит рассматривать как крайняя необходимость либо физическое или психологическое принуждение. Данное разъяснение подтверждается авторами, утверждающими, что если лицо не имело возможности отказаться от предоставления средств, то его действия стоит рассматривать через призму обстоятельств, исключающих преступность деяния [7, стр. 56].

В данном вопросе решение видится в необходимости совершенствования постановления Пленума Верховного Суда РФ «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» путем внесения разъясняющих положений о квалификации действий лиц, предоставивших предметы финансирования терроризма под воздействием угрозы применения насилия и иных способов принуждения.

Подводя итог, стоит сказать, что проблема выявления и пресечения финансирования терроризм, несомненно, заключается в исключительном разнообразии используемых преступниками методов получения необходимых средств, так как они могут включать в себя как легальные, так и нелегальные источники.

Совершенствование российского законодательства в борьбе с финансированием терроризма, безусловно, имеет важное значение. Однако создание правовой базы не решает всех вопросов. Налаживание системы международного сотрудничества посредством обмена информацией стала бы звеном в создании механизмов своевременного и эффективного пресечения финансирования терроризма. Сотрудничество в данной области видится во взаимодействии в пограничном контроле ввоза и вывоза валют, координации совместной финансовой разведывательной деятельности, выработке согласованной позиции относительно критериев и механизмов отнесения организации к террористической. Поскольку терроризм является международной проблемой, постольку и контртеррористическая деятельность является международным вопросом, что еще раз подтверждает необходимость в тесном международном сотрудничестве государств в борьбе с ним.

Литература

1. Гадицкий, М. М. Правовая характеристика антитеррористической защищенности объектов железнодорожного транспорта / О. М. Землина, М. М Гадицкий // Транспортное право и безопасность. 2020. № 2 (34).
2. Землин, А. И. Противодействие терроризму. Организационно-правовое обеспечение на транспорте : учебное пособие / А. И. Землин, В. В. Козлов. Москва : Юрайт, 2019.
3. Землин, А. И. Безопасность жизнедеятельности для транспортных специальностей: противодействие терроризму на транспорте : учебное пособие / А. И., Землин, В. В. Козлов. Москва : Юрайт, 2020.
4. Землин, А. И. Правовые и организационные аспекты обеспечения противодействия терроризму на транспорте : учебник для вузов / А. И. Землин [и др.]. Москва : Юрайт, 2020.
5. Землин, А. И. Актуальные организационно-правовые вопросы непрерывного профессионального образования сил обеспечения транспортной безопасности // Образование и право. 2020. С. 399—408.
6. Лещов, Г. Ю. Современная система транспортного образования в контексте управления безопасностью на транспорте: проблемы и перспективы развития // Транспортное право и безопасность. 2021. № 4(40). С. 36—43.
7. Меркурьев, В. В. Вымогательство, сопряженное с финансированием терроризма: квалификация / В. В. Меркурьев, П. В. Агапов // Уголовный процесс. 2012. С. 55—57.
8. Нестеров, Е. А. Перспективы развития Юридического института Российского университета транспорта // Транспортное право и безопасность. 2021. № 3(39). С. 22—34.

Землин Александр Игоревич,
доктор юридических наук, профессор, заведующий кафедрой «Транспортное право» Юридического института Российского университета транспорта (МИИТ)

Батусова Виктория Алексеевна,
магистрант Юридического института Российского университета транспорта (МИИТ)

Правовые основы, порядок и регулирование развития транспортной системы России на основе проектного и программно-целевого подходов

Аннотация. В статье исследованы теоретические и организационно-правовые основы применения программно-целевого и проектного подходов развития транспортной системы России, раскрыты некоторые проблемные вопросы соотношения программно-целевого и проектного подходов, рассмотрены положения и процедуры принятия и реализации государственных программ Российской Федерации, федеральных и межгосударственных целевых программ, национальных проектов, цели и задачи государственной программы «Развитие транспортной системы», а также международные стандарты, ресурсное обеспечение федереальных целевых программ. В статье рассмотрена методология программно-целевого и проектного подходов для развития транспортной системы, а также критически оценены конечные результаты целевой программы «Развитие транспаортной системы». В процессе исследования выявлена необходимость повышения роли программного планирования для решения системных задач развития Российской Федерации, сформулированы отдельные предложения по совершенствованию правовых основ применения проектного и программно-целевого подходов в интересах эффективного развития транспортной системы России.

Ключевые слова: программно-целевой подход; проектный подход; развитие транспортной системы; правовое регулирование; государственная программа; государственное регулирование; целевые программы; международные стандарты.

Alexander I. Zemlin,
Doctor of Law, Professor, Head of the Department of "Transport Law"
of the Law Institute of the Russian University of Transport

Victoria Al. Batusova,
Graduate Student of the Law Institute of the Russian University of Transport

Legal basis, procedure and regulation of the development of the transport system of Russia on the basis of project and program-target approaches

Abstract. The article examines the theoretical and organizational and legal foundations of the application of program-target and project approaches to the development of the transport system of Russia, reveals some problematic issues of the correlation of program-target and project approaches, considers the provisions and procedures for the adoption and implementation of state programs of the Russian Federation, federal and interstate target programs, national projects, goals and objectives of the state program "Development of the transport system", as well as international standards, resource provision of federal target programs. The article considers the methodology of program-target and project approaches for the development of the transport system, as well as critically assesses the final results of the target program "Development of the transport system". In the course of the research, the necessity of increasing the role of program planning for solving systemic problems of the development of the Russian Federation was identified, separate proposals were formulated to improve the legal foundations for the application of project and program-target approaches in the interests of the effective development of the transport system of Russia.

Keywords: program-target approach; project approach; development of the transport system; legal regulation; state program; state regulation; target programs; international standards.

Миссия транспорта — удовлетворение потребностей экономики и общества в конкурентоспособных качественных транспортных услугах.

Четкое и однозначное понимание места и роли транспортного права в российской правовой системе имеет для будущих специалистов в области транспорта особое значение, поскольку от этого прямо зависит возможность адекватного его использования ими в процессе будущей деятельности, степень законности принимаемых ими управленческих решений [1, стр. 12]. В связи с этим обоснованно ставится задача совершенствования содержания преподаваемых студентам-

транспортникам правовых дисциплин, исходя из современных потребностей отрасли [7, стр. 36; 8, стр. 24].

Проектная деятельность — это уникальная деятельность, направленная на достижение заранее определенного результата, создание определенного уникального продукта или услуги. Как правило, используется следующее определение: «проект (от лат. брошенный вперед) — это деятельность, имеющая начало и конец во времени, направленная на достижение заранее определенного результата/цели, создание определенного, уникального продукта или услуги, при заданных ограничениях по ресурсам и срокам, а также требованиям к качеству и допустимому уровню риска» [3, стр. 129; 4, стр. 57—58].

Основными признаками, которые отличают проект от других видов деятельности, являются:

– направленность на достижение конкретных целей с определенным началом и концом;

– ограниченная протяженность по срокам, стоимости и ресурсам;

– неповторимость и уникальность (в определенной степени);

– комплексность — наличие большого числа факторов, прямо или косвенно влияющих на прогресс и результаты проекта;

– правовое и организационное обеспечение — создание специфической организационной структуры на время реализации проекта.

Проектная деятельность всегда имеет ряд ограничений:

– продолжительность проекта;

– наличие бюджета проекта;

– наличие ресурсов для проекта;

– уровень приемлемого риска в проекте;

– потенциальные социальные или экологические последствия проекта;

– законы, нормы и другие законодательные требования, необходимые для реализации проекта.

Порядок разработки, реализации и оценки эффективности государственных программ Российской Федерации утвержден постановлением Правительства РФ от 02.08.2021 № 588. Данный порядок не распространяется на государственную программу вооружения (федеральную программу разработки, создания и производства вооружения и военной техники на десятилетия вперед), предусмотренную Федеральным законом «О государственном оборонном заказе».

Порядок разработки и реализации федеральных целевых программ и межгосударственных целевых программ утвержден постановлением Правительства РФ от 26.06.1995 № 594 «О реализации Федерального закона “О поставках продукции для федеральных государственных нужд”».

Принятие и реализация приоритетных (национальных, федеральных, региональных и ведомственных) проектов регулируются Положением об организации проектной деятельности в Правительстве Российской Федерации, утвержденным постановлением Правительства РФ от 31.10.2018 № 1288.

В связи с их значимостью общественные отношения на транспорте подлежат правовому регулированию, что предопределяет потребность оформления транспортного законодательства и транспортного права как относительно самостоятельных комплексных образований соответственно российского законодательства и права. При этом активно используются средства как публично-правового, так и частноправового регулирования [2, стр. 14; 5, стр. 28], существенно различающиеся между собой [6, стр. 19], что создает дополнительные затруднения для участников правоотношений.

Таким образом, соотношение предусмотренных порядками и положениями процедур принятия и реализации государственных программ Российской Федерации, подпрограмм, федеральных и межгосударственных целевых программ, национальных проектов, а также приоритетных (национальных, федеральных, региональных и ведомственных) проектов, не говоря уже о федеральных адресных инвестиционных программах, установлено недостаточно четко.

Основными принципами проектной деятельности являются:

– принцип прогностичности, который обусловлен самой природой проектирования, ориентированного на будущее состояние объекта;

– принцип пошаговости, который предполагает постепенный переход от проектного замысла к формированию образа цели и образа действий. Причем каждое последующее действие основывается на результатах предыдущего;

– принцип нормирования является обязательным прохождения всех этапов создания проекта в рамках регламентированных процедур, в первую очередь связанных с различными формами организации мыслительной деятельности;

– принцип обратной связи, обусловлен необходимостью после осуществления каждой проектной процедуры получать информацию о ее результативности и соответствующим образом корректировать действия;

– принцип продуктивности подчеркивает прагматичность проектной деятельности, обязательность ее ориентации на получение результата, имеющего прикладную значимость;

– принцип культурной аналогии указывает на адекватность результатов проектирования определенным культурным образцам. Опасность получения проектного результата, лежащего вне культурного поля, снимается, если у участников проектной деятельности есть понимание того, что индивидуальное творчество лиц не является самодостаточным;

– принцип саморазвития касается как субъекта проектирования на уровне ветвящейся активности участвующих лиц, так и порождения новых проектов в результате реализации поставленной цели. Решение одних задач и проблем приводит к постановке новых задач и проблем, стимулирующих развитие новых форм проектирования;

– для того чтобы более точно понять суть проектирования, необходимо рассмотреть понятия близкими по смыслу и значению, такими как прогнозирование, планирование, конструирование;

– прогнозирование — форма предвидения, благодаря которой возможно предположить оценку будущего состояния объекта или определение условий достижения поставленных целей для достижения результатов;

– планирование — это научное и практическое обоснование определения целей, выявление задач, сроков, темпов, пропорций развития того или иного явления, его реализация;

– конструирование — это интеллектуальная деятельность, состоящая в целенаправленном построении в идеальной форме какого-либо объекта.

В целях нормативного обеспечения проектной деятельности в Российской Федерации издано постановление Правительства РФ от 31.10.2018 № 1288 «Об организации проектной деятельности в Правительстве Российской Федерации», которым устанавливаются порядок и функциональная структура организации проектной деятельности, а также определены:

— единые подходы к проектной деятельности в Правительстве РФ;

— органы управления проектной деятельностью;

— последовательность действий;

—функции;

— полномочия и ответственность участников проектной деятельности в ходе инициирования, подготовки, реализации, мониторинга и завершения проектов.

К основным целям и задачам государственной программы «Развитие транспортной системы» относятся:

1) цели:

— ускорение товародвижения и снижение транспортных издержек в экономике;

— повышение доступности транспортных услуг;

— повышение конкурентоспособности транспортной системы России на мировом рынке транспортных услуг;

— повышение комплексной безопасности и устойчивости транспортной системы;

2) задачи:

— развитие федеральных автомобильных дорог;

— развитие железнодорожных линий;

— повышение качественных характеристик внутренних водных путей;

— развитие аэропортовой сети;

— развитие высокоскоростного железнодорожного движения;

— развитие региональных и местных автомобильных дорог;

— государственная поддержка перевозок;

— развитие и обустройство международных транспортных коридоров;

— комплексное развитие крупных транспортных узлов;

— увеличение пропускной способности российских морских портов;

— обновление парков транспортных средств, транспортного флота;

— обеспечение безопасности транспортных процессов;

— повышение антитеррористической защищенности;

— совершенствование системы контроля безопасности.

Эффективное функционирование и поступательное развитие транспортной системы России в качестве первоочередной задачи является обязательным условием социально-экономического развития России, обеспечения национальной безопасности и суверенитета государства.

Выбор направлений развития транспортной системы базируется на проекте Концепции долгосрочного социально-экономического развития Российской Федерации, бюджетном послании Президента РФ Федеральному Собранию, а также на широком спектре документов, определяющих перспективные направления развития общества и экономики России, ее регионов, отраслей экономики, транспортной системы страны в целом.

Паспорт проекта транспортной стратегии Российской Федерации до 2030 года содержит обязательные разделы, такие как: общие положения, цели и целевые показатели проекта, задачи и результаты ведомственного проекта, финансовое обеспечение реализации ведомственного проекта, а также участники ведомственного проекта и дополнительная информация. Результатом проекта является достижение поставленных целей по целевым индикаторам в сравнении с их значениями за отчетных период. Основными целями, стоящими перед транспортным комплексом страны, являются:

- образование и расширение единого транспортного пространства;
- создание доступных и качественных транспортно-логистических услуг в сфере грузовых перевозок и транспортных услуг для населения страны;
- интеграция и расширение на мировом транспортном уровне;
- повышение показателей уровней безопасности;
- снижение отрицательного воздействия транспортного комплекса на окружающую среду.

В документах стратегического планирования, программно-целевого и проектного развития, к числу которых следует отнести Государственную программу Российской Федерации «Развитие транспортной системы», входящие в ее состав подпрограммы, а также Национальный проект и приоритетные проекты в качестве задач, а в последующем и индикаторов их реализации обозначены в числе первоочередных такие, как нормативное правовое регулирование и подготовка кадров. Обосновано отмечается необходимость развития си-

стемы непрерывного профессионального образования специалистов на транспорте, включающая правовую составляющую [5, стр. 37], обеспечивающую в том числе навыки проектной деятельности на основе знания и понимания норм российского законодательства [4, стр. 60].

Инвестиционные мероприятия государственной программы «Развитие транспортной системы» включают:

— строительство автомагистралей и скоростных дорог;

— развитие железнодорожных линий;

— улучшение состояния внутренних водных путей;

— модернизацию авиатранспортной инфраструктуры и инфраструктуры морских и речных портов;

— комплексное развитие транспортных узлов;

— развитие региональных автомобильных дорог;

— совершенствование технических характеристик международных транспортных коридоров и транспортно-технологической инфраструктуры;

— обновление парка транспортных средств;

— повышение надежности объектов инфраструктуры и безопасности судоходства на внутренних водных путях;

— техническое переоснащение аварийно-спасательных служб на воздушном и водном видах транспорта;

— развитие Единой системы управления воздушным движением спутниковых систем навигации.

При этом следует понимать, что программно-целевой метод бюджетного планирования основан на системном планировании выделения бюджетных средств на реализацию утвержденных законом или нормативным актом целевых программ с использованием таких инструментов, как федеральные (долгосрочные) целевые программы; ведомственные целевые программы; программы [2; 4, стр. 59].

Для установления целей программы (подпрограмм), которые должны быть одновременно и амбициозны, и достижимы, имеют определяющее значение приоритеты и цели государственной политики Российской Федерации в сфере транспорта. [3, стр. 151; 4, стр. 59].

Все изложенное свидетельствует о повышении роли программного планирования для решения системных задач развития России, в более

широком использовании методологии и технологии проектного подхода не только в бюджетной сфере, но и применительно к прогнозированию результатов развития экономики. Указанное предполагает дальнейшее совершенствование системы правового обеспечения проектной деятельности на транспорте, что невозможно без участия подготовленных в правовом отношении специалистов.

Литература

1. Артамонова, С. Н. Правовое обеспечение профессиональной деятельности (для студентов транспортных вузов : учебник / С. Н. Артамонова [и др.]. Москва : Издательство Юрайт, 2020.
2. Артамонова, С. Н. Актуальные проблемы правового обеспечения профессиональной деятельности : учебник для вузов / С. Н. Артамонова [и др.] ; ответственный редактор А. И. Землин. М. : Издательство Юрайт, 2020.
3. Землина, О. М. Правовые аспекты финансового обеспечения развития транспортной системы в условиях программно-целевого и проектного финансирования // В сборнике: Актуальные проблемы транспортного права и транспортной безопасности в контексте современных вызовов и угроз. сборник научных трудов Международной научно-практической конференции. Москва : Издательство Юридического института МИИТ, 2020.
4. Землина, О. М. Актуальные организационно-правовые вопросы применения программно-целевого метода финансового обеспечения развития железнодорожного транспорта в России / А. И. Землин, О. М. Землина, Ю. В. Денисова // Транспортное право и безопасность. 2017. № 12 (24). С. 57—71.
5. Землин, А. И. Транспортное право : учебник / / А. И. Землин [и др.] ; ответственный редактор А. И. Землин. Москва, 2019.
6. Колонтаевская, И. Ф. Актуальные проблемы частного и публичного права: монография / И. Ф. Колонтаевская [и др.]. Москва : Московский университет им. С. Ю. Витте, 2016.
7. Лещов, Г. Ю. Современная система транспортного образования в контексте управления безопасностью на транспорте: проблемы и перспективы развития // Транспортное право и безопасность. 2021. № 4(40). С. 36—43.
8. Нестеров, Е. А. Перспективы развития Юридического института Российского университета транспорта // Транспортное право и безопасность. 2021. № 3(39). С. 22—34.

Бебурия Давид Бесикович,
специалист учебного отдела Юридического института Российского университета транспорта (МИИТ)

Основные направления правового регулирования цифровизации в логистической и транспортной отрасли

Аннотация. Цифровизация развивается в быстром темпе, и ни одной отрасли не удается остаться от нее в стороне. В сфере транспортной логистики правильное понимание трендов и их значение позволит как повысить эффективность субъектов транспортного рынка, так и получить конкурентные преимущества в краткосрочной перспективе. Формирование цифровой экономики является задачей стратегического развития Российской Федерации. Многие сферы и отрасли экономики России проходят через цифровую трансформацию на основе цифровых технологий. В статье рассмотрены основные направления правового регулирования цифровизации, регулирующие транспортно-логистическую отрасль России.

Ключевые слова: цифровизация; цифровая трансформация; логистика; правовое регулирование; транспорт.

David B. Beburia,
specialist of the Educational Department of the Law Institute of the Russian University of Transport

The main directions of legal regulation of digitalization in the logistics and transport industry

Abstract. Digitalization is developing at a rapid pace, and no industry can remain unaffected by it. In the field of transport logistics, a proper understanding of the trends and their significance will allow both increasing the efficiency of transport market entities and gaining a competitive advantage in the short term. The formation of a digital economy is a task of strategic development of the Russian Federation. Many areas and sectors of the Russian economy are undergoing digital transformation based on digital technology. The article discusses the main directions of legal regulation of digitalization, regulating the transport and logistics industry in Russia.

Keywords: digitalization; digital transformation; logistics; legal regulation, transport.

Сфера транспорта одной из первых ощутила на себе внедрение цифровых технологий: объективная необходимость в автоматизации управления, повышения надежности транспортной системы подтолкнули транспортные компании раньше других провести компьютеризацию управленческих процессов, а после — и цифровизацию всей сферы.

Несмотря на существенные отраслевые особенности и неравномерность внедрения цифровых технологий, практически все исследователи и эксперты сходятся в самых высоких оценках значимости цифровизации для социально-экономического развития. Многие авторы отмечают фактически безальтернативность этого процесса даже в самых технологически инертных отраслях. Более того, в последнее время получил распространение «сильный» термин «цифровая трансформация», что отражает растущие ожидания радикальных сдвигов и эффектов от внедрения нового поколения цифровых технологий.

Распоряжение Правительства РФ от 21.12.2021 № 3744-р «Об утверждении стратегического направления в области цифровой трансформации транспортной отрасли Российской Федерации до 2030 года» предполагает активное внедрение цифровых сервисов. По итогам реализации заявленных планов технологии интеллектуальных транспортных систем должны будут охватить крупнейшие агломерации.

В настоящий момент перед транспортной отраслью Российской Федерации стоит ряд вызовов:

— высокая аварийность ввиду человеческого фактора;

— неэффективность перевозочного процесса традиционными видами транспорта;

— низкая мобильность населения;

— высокая доля «серых» перевозок при оплате проезда наличными;

— низкий уровень использования транзитного потенциала Российской Федерации;

— низкая привлекательность транспортных коридоров Российской Федерации ввиду высокой транзакционной нагрузки (бумажные документы, контрольные процедуры, посредники);

— отсутствие возможности оперативного управления транспортным комплексом из единого центра в зависимости от ситуации;

— низкая информированность и скоординированность действий федеральных, региональных и местных органов власти, субъектов транспортной деятельности по вопросам обеспечения безопасности на транспорте (включая транспортную безопасность, кибербезопасность);

— отсутствие возможности мониторинга состояния объектов транспортной инфраструктуры на всех этапах жизненного цикла.

Исходя из текущего состояния, в стратегии определены следующие направления развития транспортного комплекса в части развития технологий, включая цифровые:

— повышение уровня технологического развития транспортного комплекса, в том числе уровня цифровизации пассажирских и грузовых перевозок, в целях снижения издержек, повышения надежности, безопасности инфраструктуры и транспортных средств, а также экологичности транспортного комплекса;

— развитие цифровых решений для взаимодействия с клиентами и их информационного обеспечения;

— повышение уровня проникновения цифровых технологий по всему жизненному циклу транспортной инфраструктуры и транспортных средств для всех видов транспорта;

— повышение уровня цифровизации при организации управления транспортным комплексом.

Российская Федерация обеспечивает решение задач путем эффективного регулирования и контроля, а также путем участия в развитии цифровизации в логистической и транспортной отрасли.

Правовое регулирование в логистической и транспортной отрасли находится в ведении Российской Федерации.

Постановление Правительства РФ от 20.12.2017 № 1596 «Об утверждении государственной программы Российской Федерации “Развитие транспортной системы”» в рамках государственной программы, реализация которой намечена до 2024 г., планирует достижение следующих основных целей:

— ускорение товародвижения;

— повышение доступности качественных транспортных услуг;

— повышение конкурентоспособности транспортной системы России на мировом рынке транспортных услуг;

— рост экспорта услуг транспортного комплекса;

— повышение комплексной безопасности и устойчивости транспортной системы.

Приоритетными направлениями достижения стратегических целей настоящей программы являются:

— формирование единой опорной транспортной сети и ликвидация инфраструктурных ограничений;

— развитие мультимодальных и транспортно-логистических технологий;

— обновление транспортных средств всех видов транспорта.

Таким образом, формирование современной среды цифровой трансформации на основе передовых технологий, которое активно стремиться использовать логистическая и транспортная отрасли, открывает совершенно новую сторону гражданско-правового регулирования.

Едигарева Юлия Геннадьевна,
кандидат социологических наук, доцент кафедры «Транспортное право» Юридического института Российского университета транспорта (МИИТ)

Голосницкая Олеся Вячеславовна,
магистрант Юридического института Российского университета транспорта (МИИТ)

Правовое обеспечение безопасности на железнодорожном транспорте

Аннотация. В данной статье рассматривается нормативно-правовая база, регулирующая российскую транспортную систему, а также отражены основные вопросы, стоящие перед транспортной системой в области обеспечения безопасности движения и эксплуатации железнодорожного транспорта. Помимо этого проанализированы основные источники правового регулирования безопасности на железнодорожном транспорте в Российской Федерации.

Ключевые слова: транспортное право; транспортная безопасность; железнодорожный транспорт; законодательные правовые акты; подзаконные правовые акты; транспортная система.

Yulia G. Edigareva,
Candidate of Sociological Sciences, Associate Professor of the Department of Transport Law at the Law Institute of the Russian University of Transport

Olesya V. Golosnitskaya,
Master's student of the Law Institute of the Russian University of Transport

Legal provision of safety in railway transport

Abstract. This article examines the regulatory framework governing the Russian transport system, and also reflects the main issues facing the transport system in the field of traffic safety and operation of railway transport. In addition, the main sources of legal regulation of safety in railway transport in the Russian Federation are analyzed.

Keywords: transport law; transport security; railway transport; legislative legal acts; subordinate legal acts; transport system.

Как отмечается отечественными правоведами, изучающими транспортное право, а в частности вопросы безопасности в сфере транспорта, транспортная безопасность является структурным элементом национальной безопасности. Безопасность на железнодорожном транспорте — это комплекс организационно-технических мер, направленных на снижение вероятности возникновения фактов угрозы жизни и здоровью пассажиров, сохранности перевозимых грузов, сохранности объектов инфраструктуры и подвижного состава железнодорожного транспорта, экологической безопасности окружающей среды.

Стоит согласиться с мнением ученых, что указание на возможные угрозы благополучию населения на транспорте связаны не только и исключительно с возможными актами незаконного вмешательства, но и чрезвычайными ситуациями природного и техногенного характера на транспорте, которые более полно отражают сущность и содержание как возможных угроз, так и соответствующих им мер обеспечения безопасности населения на транспорте. Внушительная часть нарушений безопасности движения происходит из-за несоблюдения Правил технической эксплуатации железных дорог Российской Феде-

рации (утверждены приказом Минтранса России от 21.12.2010 № 286), которые обязаны соблюдать все без исключения железнодорожники. К тому же нередко недочеты в эксплуатационной работе происходят из-за халатности, недисциплинированности, небрежного отношения отдельных железнодорожников к выполнению своих должностных обязанностей. Отрицательно на безопасности движения тягового и подвижного составов сказывается и низкая надежность технических устройств, несоответствие технологических процессов и технических средств требованиям ремонта и восстановления работоспособности подвижного состава, устройств железнодорожного пути, автоматики, телемеханики, связи, систем энергообеспечения и других устройств.

Нельзя не отметить тот факт, что высокая степень уязвимости объектов транспортной инфраструктуры, обусловленная изначально их предназначением и, соответственно, открытостью к доступу неограниченному числу лиц, также делают указанные объекты особенно привлекательными для террористов.

Еще одним видом нарушения правил безопасности на железнодорожном транспорте выступает поведение отдельных граждан, к которым относится зацеперство, проезд на подножках, крышах вагонов и в других не приспособленных для этого местах, а также обозначена самовольная без надобности остановка поезда и самовольный проезд в грузовом поезде.

Правовое регулирование безопасности движения, нормативных критериев системы эксплуатации железнодорожного транспорта, разработка и реализация государственной политики в области безопасности движения и эксплуатации железнодорожного транспорта, транспортных и иных связанных с перевозочным процессом технических средств возложено на Минтранс России. Именно этот федеральный орган исполнительной власти в области железнодорожного транспорта уполномочен утверждать правила технической эксплуатации железных дорог Российской Федерации, правила перевозок грузов и пассажиров и т.д.

В Российской Федерации основополагающим законодательным актом по вопросам обеспечения безопасности является Конституция РФ. В соответствии со ст. 71 Конституции РФ вопросы обеспечения безопасности находятся в ведении государства. В случае создания

угрозы жизни и здоровью людей, окружающей среде, обороноспособности государства, возникновению чрезвычайных ситуаций из-за нарушения безопасности на железнодорожном транспорте могут вводиться режимы закрытия и ограничения свободного движения. В этом случае ч. 2 ст. 74 Конституции РФ устанавливает жесткое требование — такие закрытия и ограничения могут вводиться только на основании соответствующего федерального закона.

Основным федеральным законом, который регулирует вопросы обеспечения безопасности на железнодорожном транспорте, является Федеральный закон от 10.01.2003 № 17-ФЗ «О железнодорожном транспорте в Российской Федерации». В соответствии со ст. 2 указанного Закона безопасность движения и эксплуатации железнодорожного транспорта определяется как «состояние защищенности процесса движения железнодорожного подвижного состава и самого железнодорожного подвижного состава, при котором отсутствует недопустимый риск возникновения транспортных происшествий и их последствий».

В соответствии с п. 2 ст. 6 Федерального закона от 27.02.2003 № 29-ФЗ «Об особенностях управления и распоряжения имуществом железнодорожного транспорта» одним из основных принципов осуществления деятельности на железнодорожном транспорте является обеспечение стабильной работы, безопасности движения и эксплуатации железнодорожного транспорта, включая железнодорожные перевозки в условиях военного и чрезвычайного положений.

Надежная и слаженная работа всех звеньев железнодорожного транспорта во многом базируется на соблюдении обязательных требований к техническим устройствам, оборудованию, сооружениям, иным железнодорожным объектам, процессам их производства, эксплуатации, грузо- и пассажироперевозкам. Основным нормативным правовым актом здесь является Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании». Согласно определению, приведенному в ст. 2 Закона, «технический регламент — это документ, утверждающий обязательные для применения требования к объектам технического регулирования». Этот же Закон установил правовые положения о сертификации и стандартизации. Так, сертификация осуществляется с целью удостоверения соответствия технических устройств, оборудования, сооружений, процессов производ-

ства железнодорожных объектов, эксплуатации, перевозки требованиям технических регламентов, стандартам, условиям действующих договоров, а стандартизация совершается с целью повышения уровня безопасности объектов с учетом риска возникновения чрезвычайных ситуаций природного или техногенного характера. Более того, Федеральным законом «О железнодорожном транспорте в Российской Федерации» установлена обязательная сертификация подвижного состава, контейнеров, специализированного оборудования, элементов инфраструктуры, специальных программных средств, используемых для организации процесса железнодорожных перевозок, услуг, оказываемых при перевозках грузов и пассажиров, а также организация стандартизации и обеспечения единства измерений на железнодорожном транспорте. В качестве объектов добровольной сертификации могут выступать технические средства железнодорожного транспорта, специализированные программные средства, системы управления, персонал железнодорожного транспорта, процессы предоставления услуг на железнодорожном транспорте при грузо- и пассажироперевозках.

Федеральным законом от 10.03.2003 № 18-ФЗ «Устав железнодорожного транспорта Российской Федерации» предусматривается обязательное соблюдение установленных требований технических и технологических стандартов (государственных стандартов, санитарных норм и правил, строительных норм и правил, сертификационных требований, норм безопасности) всеми лицами, которые причастны к перевозочному процессу на железнодорожном транспорте. К тому же в Законе предусмотрена ответственность участников процесса перевозок:

- за неисполнение или ненадлежащее исполнение отдельных требований в сфере эксплуатации железнодорожного транспорта;
- за искажение в транспортной железнодорожной накладной наименований грузов, особых отметок, сведений о грузах, об их свойствах, в результате чего снижается стоимость перевозок или возможно возникновение обстоятельств, негативно отражающихся на безопасности движения и эксплуатации железнодорожного транспорта;
- за отправление багажом или грузобагажом предметов, перевозка которых данным видом отправок не предусматривается; за превышение грузоподъемности вагона;
- за вред, причиненный жизни или здоровью пассажира железнодорожного транспорта.

Примером подзаконных нормативных актов, входящих в систему транспортного права и регулирующих вопросы безопасности на железнодорожном транспорте, являются, в частности, Указы Президента РФ от 31.03.2010 № 403 «О создании комплексной системы обеспечения безопасности населения на транспорте» и от 16.03.2010 № 321 «О мерах по организации движения высокоскоростного железнодорожного транспорта в Российской Федерации». Отсюда следует, что законодательное обеспечение безопасности было и остается краеугольным камнем в государственном управлении. Отсюда же вытекает обязанность государства создать законодательную базу, способную четко сориентировать человека на определенное законопослушное поведение, а также обеспечить эффективное функционирование механизма предупреждения правонарушений. Отдельные вопросы обеспечения безопасности на железнодорожном транспорте разрабатываются Правительством РФ и реализуются в подзаконных нормативных правовых актах. Среди них приказы Минтранса России:

- от 11.02.2010 № 34 «Об утверждении Порядка разработки планов обеспечения транспортной безопасности объектов транспортной инфраструктуры и транспортных средств». Реализация данного приказа подразумевает целый ряд мероприятий организационного и технического характера, предпринимаемых с целью защиты объектов железнодорожной инфраструктуры от потенциальных и непосредственных угроз совершений актов незаконного вмешательства, а также при подготовке и проведении контртеррористических операций;
- от 06.09.2010 № 194 «О Порядке получения субъектами транспортной инфраструктуры и перевозчиками информации по вопросам обеспечения транспортной безопасности». Данный приказ устанавливает процедуру получения субъектами транспортной инфраструктуры от уполномоченных федеральных органов исполнительной власти информации по вопросам обеспечения транспортной безопасности, в частности, по вопросам обеспечения безопасности на железнодорожном транспорте;
- от 29.12.2010 № 307 «О создании Совета по реализации Комплексной программы обеспечения безопасности населения на транспорте», утверждающий положение о Совете по реализации Комплексной программы обеспечения безопасности населения на транспорте, в том числе железнодорожном, его основные задачи, состав,

структуру и организацию деятельности и др. Уголовным кодексом Российской Федерации (ст. 263, 266), Кодексом Российской Федерации об административных правонарушениях, Положением о дисциплине работников железнодорожного транспорта (утверждено постановлением Правительства РФ от 25.08.1992 № 621) предусмотрена ответственность за нарушение требований транспортной безопасности на железнодорожном транспорте.

Таким образом, правовое регулирование вопросов контроля соблюдения и обеспечения безопасности перевозочного процесса в железнодорожной отрасли является довольно сложной системой, в которой прослеживается взаимная связь между нормативными правовыми актами законодательного и подзаконного уровней.

На современном этапе Минтранс России находит одной из главных задач принятие ведомственных нормативных правовых актов, необходимых для реализации федеральных законов в области обеспечения государственной транспортной безопасности. В транспортном законодательстве накоплена достаточная отраслеобразующая «критическая масса» нормативного материала. С помощью разработки новых и пересмотра действующих законодательных и нормативных правовых актов РФ планируется усовершенствовать нормативно-правовую базу контроля соблюдения и обеспечения безопасности функционирования железнодорожного транспорта. Помимо этого, проведенный анализ современной системы управления безопасностью на транспорте позволяет говорить о том, что вопросы подготовки специалистов, как управляющих транспортными средствами, так и отвечающих за обеспечение безопасности движения, становятся приоритетными для дальнейшего прогрессивного развития транспорта. Указанные меры должны способствовать значительному повышению безопасности движения, обеспечению эффективной работы аварийно-спасательных служб, достижению безопасного уровня функционирования инфраструктурных объектов и транспортных средств железнодорожного транспорта.

Жариков Михаил Вячеславович,
доктор экономических наук, доцент, профессор департамента мировых финансов Финансового университета при Правительстве РФ

Особенности регулирования имущественных отношений в рамках неконвертируемых токенов

Аннотация. Журнал *The Economist* провел аукцион неконвертируемого токена, который показал возможности децентрализованных финансов, а также большие проблемы. Помимо всего прочего, этот аукцион имел привлекательный характер. Он стартовал в понедельник 25 октября 2021 г., когда журнал и его представители выдвинули предложение — выставить на продажу неконвертируемый токен графического изображения обложки одного из октябрьских выпусков, посвященного децентрализованным финансам. Неконвертируемые токены представляют собой цифровую собственность, некую купчую на объект цифровой собственности, которая имеет обращение в блокчейн и цифровых финансовых платформах с помощью и при посредстве цифровых валют.

Ключевые слова: децентрализованные финансы; цифровизация; цифровая собственность; цифровое пространство; цифровая биржа; цифровой аукцион; капитализация цифровых активов.

Mikhail V. Zharikov,
World Finance Department, Financial University under the Government of the Russian Federation

Specifics of regulating property rights involved in non-fungible tokens

Abstract. The Economist magazine held an auction of a non-convertible token, which showed the possibilities of decentralized finance, as well as big problems. Among other things, this auction had an attractive character. It started on Monday, October 25, 2021, when the magazine and its representatives put forward a proposal — to put up for sale a non-convertible token of a graphic image of the cover of one of the October issues dedicated to decentralized finance. Non-convertible tokens are digital property, a kind of bill of sale for an object of digital property,

which has circulation in the blockchain and digital financial platforms with and through digital currencies.

Keywords: decentralized finance; digitization; digital property; digital space; digital exchange; digital auction; digital assets' capitalization.

С одной стороны, группа будущих партнеров, которые будут предъявлять спрос на эти финансовые продукты, создала децентрализованную автономную организацию под названием *Rabbit Hole Dow,* для того чтобы с применением краудсорсинга накопить достаточное количество средств или фондов, которые позволят приобрести токен журнала. В результате сбора ставок победителем оказался человек с аватаром X, предложивший за токен 99,9 *Ether*, или около 420 тыс. долл. Доход, чистая сумма за вычетом комиссионного сбора, налога и трансакционных издержек перечислены редакцией журнала в виде пожертвования в образовательный фонд *The Economist*, независимую благотворительную организацию, входящую в эту медиа-группу.

Множество других игроков тоже участвуют в подобных мероприятиях. Неконвертируемые токены, или покемоны, создаются на основе деятельности четверти миллиона пользователей одной видеоигры *ActiInfinity*. Многочисленные любители искусства торгуют объектами цифровой собственности коллекционного назначения. Неконвертируемые токены, работающие на блокчейн *Ethereum*, в настоящее время имеют капитализацию в 14 млрд долл. В 2020 г. эта сумма составляла всего 340 млн долл. Инвестиционный банк *Jeffries* полагает, что совокупный объем токенов к 2025 г. достигнет 80 млрд долл. [1]

Тут, наверное, можно было бы посомневаться, что на самом деле создается в сфере неконвертируемых токенов. Лучший способ получить для себя ответ на этот вопрос заключается в том, что неконвертируемые токены являются одним из способов раскрытия прав собственности, т.е. чтобы воспользоваться своими правами собственности. Если существуют желающие получить юридический (имеющий юридическую силу) титул на нетрадиционный, нестандартный актив, то они имеют стандартный набор вариантов выбора для выгодоприобретателя. В случае жилого дома, автомобиля, акций корпораций юридический титул носит в себе доказательство собственности, прав на исключительное использование, способность взимать за его использование плату с других лиц — пользователей, и право получать доходы от продажи [2].

В сфере финансов распространены дорогостоящие услуги адвокатов за получение этих прав, их дробление, например на основе деривативного контракта. Такого рода гибкость, однако, сложно получить. Потребуются немалые средства. Такие услуги недосягаемы для многих физических лиц по причине дороговизны. Неконвертируемые токены обладают потенциалом — изменить ситуацию. В рамках описанного аукциона журнал определил права собственности согласно модели по умолчанию, принятой на цифровой платформе, на которой проводился сам аукцион. Новый собственник неконвертируемого токена имеет права, аналогичные по своим свойствам лицензионному соглашению. Такое соглашение отражает спецификацию отображения цифрового актива, однако не дает полномочий на коммерциализацию, например в результате продажи футболок с изображением токена. Благотворительная организация, о которой шла речь, может получить от будущей продажи токена скидку в 10% [3].

Теоретически продажа неконвертируемого токена может нести в себе сочетание прав собственности, предъявленные продавцом. Имеются и иные преимущества. Публичный, безотзывный акт совершения сделки существует в блокчейн и работает на других цифровых платформах. Все же несмотря на перспективы концептуального развития в будущем, неконвертируемые токены содержат в себе тонкости практических недостатков, как показал эксперимент журнала. Несмотря на удобство интерфейса цифровой платформы для торговли неконвертируемыми токенами, весь процесс представляет собой некий кошмарный сон. Этот процесс предполагает создание цифрового кошелька, его финансирование через оплату любых комиссионных сборов, связанных с созданием неконвертируемых токенов, создание самого токена, выбор способа коммерциализации доходов в виде обычных денег на банковский счет [4].

Для большинства юрист-консулов по вопросам налогов и сборов все это — территория неизвестности, дремучий лес. Сам процесс очень дорогой. Журнал заплатил неким газом, товаром в оплату комиссионного сбора и других налогов. Чтобы вся система вышла на платформу мейнстрима в системе децентрализованных финансов, она должна работать, как программное обеспечение на *iPhone*, она гораздо дешевле по стоимости обслуживания в отличие от сделок с участием обычного посредника. Вторая проблема носит энергетический

характер. Скромный эксперимент журнала привел к выбросам такого же количества CO2, как количество выбросов в расчете на одно место в реактивном самолете. Большинство цифровых платформ ищут пути сокращения затрат на электроэнергию [5].

Если неконвертируемые токены будут представлять собой новую, навороченную вещицу, то они должны путем инноваций работать на той платформе, которая не будет вредить окружающей среде в виде выбросов углекислого или парникового газа и в конечном счете должна будет свести выбросы на нет. Третья проблема заключается в исполнении условий контракта. Журнал надеется на то, что в случае с его токеном такая проблема на возникнет, потому что сам актив как уникальный цифровой отпечаток картинки на обложке уже находится в тираже журнала, только теперь она будет обращаться в сфере децентрализованных финансов [6].

При этом не существует стимулов с чьей бы то ни было стороны к любого рода злоупотреблениям. Тем не менее, в случае с неконвертируемыми токенами эта ситуация распространяется на активы, находящиеся за пределами мира децентрализованных финансов, существующих сами в себе, включая патенты или активы в виде зданий и сооружений, т.е. права собственности, распространяющиеся на использование неконвертируемых токенов, могут вступать в конфликт с другими контрактами, так что суды по разрешению коммерческих споров не будут признавать цифровой договор. Конечно, ситуация может измениться. Например, одна квартира в одном доме в Киеве в 2021 г. поменяла хозяина, после того как неконвертируемый токен, представлявший эту квартиру, был продан согласно сделке купли-продажи, признанной украинским законодательством.

Все равно децентрализованные финансы должны будут пройти очень долгий путь, прежде чем они интегрируются в законную систему. Количество этапов для этого весьма большое. Но если эти проблемы решить, то некоторые неконвертируемые токены еще могут стать чем-то большим, чем сам токен [7].

Неконвертируемые токены обладают и другими потенциально полезными характеристиками. Поскольку они существуют в рамках открытой системы блокчейн, история сделок с их участием позволяет рассматривать их сообществом людей. Поэтому можно кодировать определенные черты, преобразовывать их в контракты, регулирую-

щих покупку и продажу этих токенов. Художники-цифровики (цифровисты) стремятся сохранить определенную долю своих прав на произведение искусства, что обеспечивает для них некоторую долю дохода в случае, если цифровой оригинал поступает в продажу. Это есть то, чего многие художники пытаются добиться с использованием традиционных средств. Теоретически неконвертируемый токен можно привязать к тексту, например, правового договора, контракта, предполагающего наличие установленного набора прав и обязанностей в отношении того или иного имущества [8].

На практике, однако, в него ничего не включается. Права собственности на произведение искусства, представленного токеном, как правило, устанавливаются на основе особой платформы, на которой они имеют хождение. Некоторые специалисты поясняют, что эмитенты неконвертируемых токенов должны сохранять за собой копирайт на произведение искусства, носителем которого они и являются. Условия благотворительного фонда и цифровой платформы для обращения токена журнала *The Economist* указывают на то, что покупатель неконвертируемого токена имеет право, аналогичное лицензии, позволяющей использовать какой-нибудь предмет, его образное представление в установленных рамках, например, обе организации могут публично демонстрировать его, копировать токен в личных целях и исходя из личных побуждений, но они не могут использовать его в коммерческих целях. Купля-продажа неконвертируемых токенов на специальных платформах, предназначенных для торговли произведениями искусства, включая *Melinda & Bill Gates Foundation*, привлекла 205 млн долл. В марте 2021 г. после продажи образа, созданного Биплом, вся эта лихорадка достигла некоторой кульминации. С тех пор инвесторы несколько охладели к такому виду искусства. Однако весь рынок неконвертируемых токенов продолжает непрерывно развиваться. Идея создания оригинального цифрового токена, который содержит информацию, доказывающую наличие признаков собственности, прав собственности, включает непосредственно сами права собственности, получила распространение и в других сферах деятельности для использования.

Литература

1. Афанасьев, Д. Как искусственный интеллект меняет отношение бизнеса к покупателю // БИТ. Бизнес & Информационные технологии. 2019. № 5 (88).

2. Алексеев, Р. А. Искусственный интеллект на службе государства: аргументы «за» и «против» // Журнал политических исследований. 2020. Т. 4. № 2.
3. Бутенко, Е. Д. Искусственный интеллект в банках сегодня: опыт и перспективы // Дайджест-финансы. 2020. Т. 25. № 2 (254).
4. Жуков, Д. С. Искусственный интеллект для общественно-государственного организма: будущее уже стартовало в Китае // Журнал политических исследований. 2020. Т. 4. № 2.
5. Колин, К. К. Цифровая революция и искусственный интеллект: новые горизонты и опасности // Партнерство цивилизаций. 2020. № 1-2.
6. Паршина, Л. Н. Технологии будущего: блокчейн и искусственный интеллект / Л. Н. Паршина, Д. С. Кузьминич // Журнал естественнонаучных исследований. 2020. Т. 5. № 2.
7. Пороховский, А. А. Цифровизация и искусственный интеллект: перспективы и вызовы // Экономика. Налоги. Право. 2020. Т. 13. № 2.
8. Устинова, О. Е. Искусственный интеллект в менеджменте компаний // Креативная экономика. 2020. Т. 14. № 5.

Ромашкина Наталья Юрьевна,
аспирант Института законодательства и сравнительного правоведения при Правительстве Российской Федерации

Отдельные аспекты организации системы киберзащиты в финансово-кредитном секторе экономики

Аннотация. Финансово-кредитные отношения в Российской Федерации несколько лет назад вошли в процесс цифровизации, и сегодня множество участников финансового рынка продолжают эту тенденцию. Внедрение множества новейших функций в деятельность банковских организаций способствует уменьшению издержек и упрощает получение клиентом необходимых услуг. Достаточно большое количество исследований подтверждает, что процессы цифровизации имеют множество преимуществ, однако на фоне положительных моментов существуют и проблемы. Становится понятно, что помимо вложений в технологические улучшения, банкам следует уделить большое внимание созданию и поддержанию стабильно функционирующей системы безопасности, поскольку параллельно банкам развиваются и злоумышленники, подстраиваясь под новые технологии и услуги.

Ключевые слова: кибербезопасность; финансово-кредитная система; банк; киберзащита; информационные технологии.

Romashkina Y. Natalia,
post graduate of the Law Institute of the Russian University of Transport

Some aspects of the organization of the cyber defense system in the financial and credit sector of the economy

Abstract. Financial and credit relations in the Russian Federation entered the process of digitalization several years ago, and today many financial market participants continue this trend. The introduction of many new functions in the activities of banking organizations helps to reduce costs and simplifies the client's receipt of the necessary services. A fairly large number of studies confirm that digitalization processes have many advantages, but there are also problems against the background of positive aspects. It becomes clear that in addition to investing in technological improvements, banks should pay great attention to the creation and maintenance of a stably functioning security system, since in parallel with banks, attackers are also developing, adapting to new technologies and services.

Keywords: cybersecurity; financial and credit system; bank; cyber defense; information technology.

Использование информационных технологий и основанных на них бизнес-решений является одним из основных инструментов снижения издержек различными организациями и предприятиями в целях снижения расходов, расширения клиентской базы, т.е. для повышения их конкурентоспособности. Ускоренными темпами развивается внедрение различных информационных технологий и в кредитно-финансовой сфере. Они, в частности, обеспечивают быстрый и бесперебойный доступ пользователям финансовых услуг к продуктам финансово-кредитных организаций, с одновременной гарантией конфиденциальности, безопасности и оперативности.

Необходимость и обоснованность введения в деятельность кредитных организаций новейших технологий обосновывается многими исследованиями. Так, по подсчетам одной из крупнейших международных компаний в области оказания финансовых услуг Citi Group, внедрение в банковскую деятельность информационных технологий помогает уменьшить на

50% повседневные затраты банка на ведение своей деятельности, и оказания услуг[1]. Компания Accenture, являющаяся одним из лидеров мирового рынка профессиональных услуг и цифровых технологий, также опубликовала исследование, проводимое в 2019 г., которое показывает, что наиболее продвинутые в плане цифровизации банки увеличивают рентабельность капитала в среднем на 0,9%, то есть внедрение технологий позволяет увеличивать прибыль, занижая при этом издержки. Это же исследование показало, что банки, не использующие автоматизацию бизнес-процессов, снизили этот же показатель в среднем на 1,1%, т.е. были вынуждены затрачивать больше ресурсов для поддержания конкурентоспособности на рынке финансовых услуг[2].

На необходимости внедрения технологий сказалась и внезапно возникшая пандемия COVID-19. По отчету *Deloitte*, международной сети компаний, оказывающих услуги в области консалтинга и аудита, входящих в «большую четверку» аудиторских компаний, опубликованному по итогам 2019 г., около 60% банков по всему миру либо полностью перешли на удаленный формат оказания услуг, либо максимально сократили рабочее время в офисах, что спровоцировало необходимость в оказании многих услуг в онлайн-формате, включая сложные: открытие счета, дистанционную верификацию клиента, решение нетиповых вопросов[3].

Летом 2021 г. исследователи ведущего экспертного центра по автоматизации государства и бизнеса в России *TAdviser* провели беседы с топ-менеджерами российских банков, чтобы узнать о результатах и тенденциях в цифровизации банковской отрасли, и получили примерно одинаковые ответы.

Цифровизация во многих банках уже который год остается одним из приоритетных направлений. Банки продолжают развитие инфраструктуры, увеличивают штат сотрудников IT-отделов, внедряют и совершенствуют цифровизацию бизнес-процессов.

Однако при этом процесс внедрения новых технологий помимо положительных моментов влечет и негативные — появление угроз,

[1] URL: https://online.citi.com/US/JRS/pands/detail.do?ID=market-insights&section= global-perspective-and-solutions (дата обращения 20.12.2021).
[2] URL: https://www.accenture.com/_acnmedia/PDF-102/Accenture-Banking-Does-Digital-Leadership-Matter.pdf (дата обращения 20.12.2021).
[3] URL: https://disk.yandex.ru/d/sa2JNgq4h6mudg (дата обращения 20.12.2021).

именуемых киберрисками. В качестве мирового тренда отмечается увеличение финансовых потерь от кибератак, нарушение целостности и непрерывности функционирования в том числе финансового рынка (17% всего объема кибератак приходится на финансовый сектор). Изощренность методов, способов и средств совершения кибератак требует от регуляторов гибкости, оперативности, использования инновационных цифровых технологий и методов работы[1].

В России за одиннадцать месяцев 2021 г. было зарегистрировано почти 32 тыс. преступлений, связанных с финансово-кредитной системой (а почти все из них совершаются путем кибератаки), тогда как в 2018 г. (т.е. до пандемии), эта цифра достигала 29 тыс.[2] Это связано с пробелами в системах киберзащиты банков, выражающихся в различных аспектах. Некоторые из них выявили аналитики *Varonis*, американской компании, разработавшей программную платформу по кибербезопасности (на сегодняшний день, по оценке различных аналитиков, *Varonis* занимает более 70% мирового рынка в этой области). Они проанализировали 4 миллиарда файлов в 56 финансовых организациях по всему миру (банки, страхование, инвестиции) на базе случайной выборки результатов аудита киберрисков (*Data Risk Assessment*). По данным отчета *Varonis* «2021 *Financial Data Risk Report*», «в среднем сотрудник финансовых служб имеет доступ к почти 11 млн файлов в день. Для крупных организаций количество увеличивается вдвое: 20 млн файлов открыты для всех сотрудников». При этом, учетные записи этих сотрудников также не отвечают всем требованиям защиты, и по тем же данным, в более чем 60% финансовых организаций эксперты *Varonis* обнаружили минимум 500 паролей без истечения срока действия, т.е. один и тот же пароль может использоваться десятилетиями. В небольших банках уровень киберзащиты еще ниже[3].

Недостаточно эффективные системы киберзащиты банков приводят к тому, что ущерб получают не только сами банки, но и их клиенты. В отчете ФинЦЕРТа Банка России (Центра мониторинга и реагирования

[1] URL: https://cbr.ru/Content/Document/File/83253/onrib_2021.pdf (дата обращения 13.01.2022).
[2] URL: https://www.izh.kp.ru/online/news/4275712/ (дата обращения 19.12.2021).
[3] URL: https://www.varonis.com/blog/2021-financial-data-risk-report/ (дата обращения 26.12.2021).

на компьютерные атаки в кредитно-финансовой сфере, специальное структурное подразделение Банка России) указаны следующие данные: в 2020 г. мошенниками похищено с карт жителей России примерно 9,8 млрд руб., что в сравнении с 2018 г. в семь раз больше[1].

Пробелы в системах киберзащиты организаций финансово-кредитной системы пытаются урегулировать на нормативном уровне.

Так в 2019 г. было принято Положение Банка России от 17.04.2019 № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента», устанавливающее обязательные для кредитных организаций требования к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента. Данное положение реализуется на сегодняшний день всеми кредитными организациями, что проверяется обязательной проверкой оценки уровня соответствия информационной защиты установленным Постановлением требованиям. В случае невыполнения банками указанных требований, Банк России имеет право в порядке надзора применять к такой кредитной организации меры, установленные Федеральным законом от 02.12.1990 № 395-1 «О Центральном банке Российской Федерации (Банке России)».

На долгосрочную перспективу Правительством РФ, например, вносятся проекты нормативных актов и предложения по совершенствованию системы безопасной цифровизации деятельности финансово-кредитного сектора экономики. Так, в рамках проекта «Стратегии развития финансового рынка Российской Федерации до 2030 года» в качестве одного из долгосрочных приоритетов развития финансового рынка выдвинуто содействие цифровизации платежных сервисов. Для этого предполагается последовательное и подконтрольное внедрение технологий, способствующих повышению эффективности контроля и надзора со стороны регуляторов, а также выполнению регуляторных требований, указанных в Стратегии, участниками рынка.

Также, в 2020 г. на ежегодной встрече Ассоциации банков России с главой Банка России Эльвирой Набиуллиной, было выдвинуто

[1] URL: https://tass.ru/interviews/13246307 (дата обращения 13.01.2022).

предложение создать аутсорсинговую компанию под контролем Банка России, которая будет осуществлять киберзащиту небольших банков. Данное предложение сегодня более, чем актуально, поскольку высокая уязвимость небольших банков — проблема всего финансового сектора, потому что через мелкие банки злоумышленники могут проникнуть в сети крупных участников финансового рынка[1].

Банки, наряду с законодателями, также анализируют недостатки систем киберзащиты и модернизируют их. В частности, создана и функционирует достаточно устойчивая и эффективная система информационной защиты и используются комплексные антифрод-системы (от англ. anti-fraud «борьба с мошенничеством»). Антифрод-системы применяются кредитными организациями для защиты денежных операций, в том числе при оказании услуг в онлайн-формате, и используются также крупными магазинами и платежными системами (*Visa, MasterCard, PayPal*).

Также, в качестве примера некоторых элементов системы киберзащиты внутри конкретного банка рассмотрим ПАО «Сбербанк», поскольку этот банк демонстрирует одну из лучших самостоятельных работ по организации киберзащиты из отечественных банков. Сотрудниками разработана система защиты *CORE*-систем — ключевых, корневых систем, в которых хранится вся информация о счетах и клиентах, методом внедрения самых современных технологий и процессов управления безопасностью. Эффективность центра фрод-мониторинга ПАО «Сбербанк» имеет один из лучших показателей в мире — около 97% мошеннических операций хеджируются и пресекаются. В ПАО «Сбербанк» создан и эффективно функционирует операционный центр кибербезопасности (*Security Operation Center*), который в круглосуточном режиме мониторит все киберугрозы вокруг систем банка. ПАО «Сбербанком» создана дочерняя компании *Bi.Zone*, сотрудничающая с Интерполом, которая образована для создания продуктов в области кибербезопасности, проведения экспертизы и расследования, тестирования систем банка на предмет выявления уязвимостей, разработки рекомендаций по хеджированию кибер-рисков.

Таким образом, банк самостоятельно организовал достаточно эффективную систему киберзащиты, что подтверждается данными об

[1] URL: https://www.kommersant.ru/doc/3888889?tg (дата обращения 19.12.2021).

отраженных атаках, представленными на сайте банка, занимается работой по обучению и повышению квалификации сотрудников и постоянно выпускает продукты, пополняющие элементы системы кибербезопасности.

Анализируя вышеизложенное, можно сделать вывод, что сегодня организация систем киберзащиты банков становится все более актуально. При этом такая защита в финансово-кредитном секторе экономики осуществляется только в виде систем кибербезопасности отдельных банков, которые самостоятельно разрабатывают и обеспечивают их бесперебойную работу. В связи с этим необходимо реализовать комплексные и более единообразные меры по защите от киберугроз во всей финансово-кредитной системе.

Красиков Иван Денисович,
студент Юридического института Российского университета транспорта (МИИТ)

Цифровизация, право и воздушный транспорт

Научный руководитель — кандидат юридических наук, доцент В. И. Ивакин

Аннотация. Освещаются основные направления цифровизации авиационной отрасли, технологии беспилотного контроля транспортного средства, развития электронного документооборота, реализации технологий *Big Data* и искусственного интеллекта.

Ключевые слова: воздушный транспорт; цифровизация; безопасность; искусственный интеллект; машинное обучение.

Krasikov Ivan D.
student of the Law Institute of the Russian University of Transport

Digitalization, law and air transport

Abstract. The main directions of digitalization of the aviation industry, the technology of unmanned vehicle control, the development of electronic document

management, the implementation of Big Data technologies and artificial intelligence are highlighted.

Keywords: air transport; digitalization; security; artificial intelligence; machine learning.

Цифровая эволюция, как отдельное понятие, уже не обладает новизной, но не смотря на это является достаточно актуальной темой на сегодняшний день. Это путь к развитию информационной и организационной группы технологий, начало которого было определено несколько десятков лет назад, продолжая свое становление в настоящее время. Рассматриваемый институт вносит значимые коррективы не только в деятельность бизнес-среды, но и в их культурную составляющую. Не останавливается цифровая информация и в различных отраслях авиации. Регулирование потока пассажиров, бухгалтерский учет, менеджмент, договорооборот, а также работа с персоналом, закупочная деятельность, лизинг и другие процессы. В отмеченном видно, с какими областями (процессами) взаимодействует цифровизация. Различный характер и глобальность проектов на рынке авиации гражданской части представлено доказательством того, что в части данной деятельности активно занимает место система организации цифровизации. Обращая внимание на положительный факт в лице участия отечественных производителей, следует отметить, что они держат планку наравне с иностранными коллегами по качеству и участию в цифровой трансформации.

Одновременно с этим отрасль авиатехнологий занимает место в строке ведущих игроков по производству и накоплению данных цифровой информации. Объем такой информации представляет собой колоссальный массив, содержащий в себе данные по состоянию судов воздушной отрасли, затрат топливной энергии, клиентскую информацию и др. Их потенциальные возможности внушительны в целях оптимизирования технического контроля и поддержания результативности, реализации требуемой эксплуатации топливной энергии, создания индивидуализированных предложений пассажирам и т.д. Раскрытие потенциала в полной мере для данной прогрессирующей направленности еще ожидается.

Виталий Савельев, который является главой Минтранса России, 3 июня 2021 г., участвуя в конференции «Транспортный каркас эконо-

мики», проходящего на площадке Петербургского международного экономического форума (ПМЭФ) отметил стоящую перед ведомством задачу, которая представляет собой не только оцифровку чего-то конкретного внутри ведомства, а необходимую оцифровку полноценного транспортного комплекса. На основе отмеченного следует сделать вывод, что объем задействованных данных вынужден показывать только рост. Данное суждение располагает к согласию с экспертами в частных областях транспорта, которые считают, что главенствующие достижения цифровой эволюции в авиационной отрасли еще ожидаются. Несомненно, немаловажным будет отметить, что это крупная ниша не только для развития новых технологий (технологий будущего), например, искусственного интеллекта, машинного обучения (*ML — machine learning*), но также и для развития классических BI-решений, практика реализации методов и ресурсов бизнес-аналитики.

Цифровизация авиаотрасли тесно связана с производством авиатехники и транспортировками (пассажирскими, грузовыми). Во втором случае персонального внимания требует работа авиационных компаний, аэропортов, взаимодействие с пассажирами, заказчиками грузовой транспортировки (перевозки), применение и действие системы организации воздушного передвижения. В том числе обязательным и одновременно условным требованием является помнить про контролирующие органы и обучение кадров в данной отрасли.

В отношении организации авиационного движения, на наш взгляд, является разработка *ADS-B* (*Automatic Dependent Surveillance Broadcast*) / АЗН-В (автономное зависимое наблюдение-вещание). Разработка, эксплуатируемая на сегодняшний день, не только в России, предоставляет возможность пилотам в кабине самолета, а также авиадиспетчерам на координирующем пункте контролировать передвижение самолетов с лучшей точностью, чем было возможно раньше, и владеть воздушными навигационными и погодными данными. В скором времени разработка будет способна организовывать автоматическое управление воздушным передвижением с минимизацией воздействия человеческого фактора.

Большинство актуальных направлений цифровизации в других ипостасях авиационной отрасли, по нашему мнению, адаптированы больше на связь с клиентурой. В любом случае, данный вариативный

взгляд является фундаментом в главенствующем отраслевом документе — Транспортной стратегии Российской Федерации до 2030 года, с прогнозом на период до 2035 год, утвержденной Правительством РФ, главная идея которой, основываясь на слова первого заместителя Председателя Правительства РФ Андрея Белоусова, заключается в том, чтобы «реконструировать» транспорт в «единую, связанную, клиентоцентричную систему с опорой на новейшие технологии», где определение клиента — «это пассажир и грузоотправитель».

В плановой задаче (стратегии) первостепенной целью стоит предусмотренный «поэтапный цифровой переход» транспортной отрасли, в том числе:

— для организации основы беспилотного контроля транспортного средства;

— организации переводческой деятельности транспортной документации в электронный вид;

— перехода к эффективному моделированию транспортных путей в настоящем времени (реальном времени);

— реализации технологий *Big Data* и искусственного интеллекта, в особенности при условии расширения инфраструктуры в сфере транспорта;

— использования разработки прогнозной (предиктивной) аналитики отказных состояний.

Указанные выше направленности тесно связаны и с авиационной отраслью. К примеру, искусственный интеллект активно задействуется как на борту, так и в обеспечивающих задачах при производстве техники.

Во всех отраслях во все времена «борьба» шла и будет идти либо за снижение издержек (внутренняя оптимизация), либо за повышение доходов (расширение продаж). Следует дополнить, что в авиационной отрасли также важна составляющая безопасности полетов. Цифровизация способствует и первому, и второму, и третьему. Во времена кризисов, в том числе во время пандемии COVID-19, когда авиаотрасль оказалась в группе наиболее пострадавших, борьба только обостряется. В связи с этим внимание к цифровой трансформации в авиаотрасли сегодня как никогда высоко, особенно в контексте повышения комфорта и безопасности услуг авиаперевозчика, аэропортов и снижения цен.

Транспорт остается отраслью, производящей колоссальный объем данных, лишь малая часть которого действительно задействуется. Это огромный потенциал для развития. И его реализация, включая указанное выше, сегодня осуществляется самым активным образом. Важно, что это происходит системно, на основе разных концепций. Например, в соответствии с концепцией перспективной трансформации бизнес-процессов на основе цифровизации *NEXTT* (*New Experience in Travel and Technologies*), разработанной еще в 2017 г. Международной ассоциацией воздушного транспорта (*IATA*) и Международным советом аэропортов (*ACI*).

Инапшба Милана Робертовна,
студент Юридического института Российского университета транспорта (МИИТ)

Сравнительно-правовой анализ транспортного налога в России и зарубежных странах

Аннотация. Налоги играют важную роль в пополнении доходной части бюджетов различных уровней, а также возможности воздействовать на национальную экономику в целом и на отдельные ее части, в частности это относится к транспортному налогу, которому посвящена настоящая статья. В статье проводится сравнительно-правовой анализ транспортного налога в России и зарубежных странах, позволивший выявить основные проблемы транспортного налогообложения в Российской Федерации и сформировать направления их решения.

Ключевые слова: транспортный налог; объект налогообложения; налоговые ставки; зарубежный опыт, концепция реформирования транспортного налогообложения.

Inapshba R. Milana,
student of the Law Institute Russian University of transport

Comparative legal analysis of the transport tax in Russia and foreign countries

Abstract. Taxes play an important role in replenishing the revenue side of budgets of various levels, as well as the ability to influence the national economy as a whole and its individual parts. This article is devoted to the transport tax. In particular, the article provides a comparative legal analysis of the transport tax in Russia and foreign countries. In the course of the study of this topic, the main problems of transport taxation in the Russian Federation have been identified.

Keywords: transport tax; object of taxation; tax rates; foreign experience, the concept of reforming transport taxation.

Транспортный налог в Российской Федерации введен в действие с 31 августа 2002 г. с принятием Федерального закона от 24.07.2002 № 110-ФЗ «О внесении изменений и дополнений в часть вторую Налогового кодекса Российской Федерации и некоторые другие акты законодательства Российской Федерации». На основании данного Закона, гл. 28 Налогового кодекса Российской Федерации (далее — НК РФ) была включена во вторую часть Кодекса. Транспортный налог, введенный в налоговое законодательство РФ, заменил такие раннее действовавшие налоги, как налог с владельцев транспортных средств, налог на имущество физических лиц в части автотранспортных средств, а также налог на пользователей автодорог.

Транспортный налог является региональным, порядок исчисления и взимания устанавливается НК РФ и законами субъектов РФ о налоге. Он обязателен к уплате налогоплательщиками на территории соответствующего субъекта РФ. Плательщиками данного налога являются как организации, так и физические лица, в том числе индивидуальные предприниматели, на которых в соответствии с российским законодательством зарегистрированы транспортные средства.

Объектом налогообложения в соответствии с положениями ст.358 НК РФ признаются автомобили, мотороллеры, мотоциклы, самолеты, вертолеты, а также целый ряд других транспортных средств, зарегистрированных в установленном порядке в соответствии с законодательством РФ.

Налоговые ставки в соответствии со ст. 361 НК РФ устанавливаются законами субъектов РФ. Ставка налога зависит от мощности двигателя, тяги реактивного двигателя или валовой вместимости транспортного средства в расчете на одну лошадиную силу мощности двигателя транспортного средства, один килограмм силы тяги реак-

тивного двигателя, одну регистровую тонну, одну единицу валовой вместимости транспортного средства или одну единицу транспортного средства (п. 1 ст. 361 НК РФ).

Субъекты РФ вправе увеличивать (уменьшать) налоговые ставки, но не более чем в десять раз. Кроме того, закон допускает установление дифференцированных налоговых ставок в отношении каждой категории транспортных средств, а также с учетом количества лет, прошедших с года выпуска транспортных средств, и (или) их экологического класса (п. 3 ст. 361 НК РФ).

Для предприятий отменена сдача декларации по транспортному налогу. С 2020 г. суммы налогов налоговыми органами рассчитываются самостоятельно на основании предыдущих расчетов и оплат [4].

Транспортное налогообложение в зарубежных странах существенно отличается от отечественного налогообложения. Рассмотрим поподробнее особенности применения транспортного налога в некоторых странах.

Во Франции действует двухуровневая система налогообложения. Так, при постановке на учет владелец транспортного средства платит единовременный налог в зависимости от объема и мощности двигателя. Второй уровень — ежегодный налог, который исчисляется в зависимости от объема углекислого газа, выбрасываемого автотранспортом в атмосферу на каждые 100 км пробега. Расчет производится согласно данным производителя. Не облагаются налогом транспортные средства, выделяющие менее 130 г углекислого газа на 1 км. Денежные поступления от данного налога во Франции направляются на финансирование программ по охране окружающей среды. Действующая во Франции двухуровневая система налогообложения является справедливой и эффективной. Так, при расчете налога здесь учитываются объемы выбросов углекислого газа в атмосферу, от чего напрямую зависит размер вреда от автомобиля.

В Японии транспортный налог делится на три вида. Так, при покупке автомобиля необходимо уплатить налог в размере 5% от покупной стоимости автомобиля [2]. Далее, необходимо уплатить налог при постановке автомобиля на учет. Налоговая ставка зависит от массы и объема двигателя автомобиля. Также владельцам автотранспортных средств необходимо уплатить ежегодный транспортный налог. Налоговая ставка зависит от массы и объема двигателя авто-

мобиля. Средства от транспортного налога направляются на развитие автомобильной промышленности. Таким образом, действующая система транспортного налогообложения в Японии является весьма эффективной.

Транспортный налог в Великобритании зависит от следующих показателей: объема двигателя, даты регистрации автомобиля, типа топлива и объема выбросов автомобилем CO2 в атмосферу. Владельцы электромобилей, а также гибридных автомобилей освобождаются от уплаты транспортного налога. Отличительной особенностью уплаты транспортного налога в Великобритании, является возможность вносить ежемесячные платежи. Около 80% средств от данного налога направляются на поддержание дорожной отрасли, оставшиеся средства — на финансирование экологических программ [2]. Данный подход следует считать справедливым, поскольку старые автомобили, автомобили с вредными видами топлива оказывают негативное воздействие на экологию, то и транспортный налог будет уплачиваться в большем размере.

В Израиле сумма транспортного налога зависит от уровня загрязнения окружающей среды. По данному показателю в 2009 г. все автомобили были условно разделены на 15 экологических групп. Так, для владельцев электромобилей установлена минимальная ставка налога — 10% от стоимости транспортного средства. Для автомобилей, сильно загрязняющих окружающую среду, установлена максимальная ставка налога — 92% от стоимости транспортного средства. В среднем же налоговая нагрузка составляет около 70% от стоимости автомобиля. Таким образом, можно сделать вывод о том, что действующая в Израиле система транспортного налогообложения является справедливой, так как данная мера будет мотивировать людей на покупку экологически чистого вида транспорта, что позволит снизить объемы выбросов вредных веществ в атмосферу.

Транспортный налог в Дании является одним из самых высоких в мире. Налог уплачивается при покупке автомобиля, а также в процессе его эксплуатации (т.к. налог включен в стоимость топлива). При регистрации автомобиля налоговая ставка составляет 105% от стоимости автомобиля. Если же стоимость автомобиля более 34 тыс. крон, то налоговая ставка составит 180% от стоимости автомобиля. Налоговая ставка при покупке автомобиля, сильно загрязняющего окру-

жающую среду, может составить до 175% от покупной стоимости автомобиля. Власти Дании, таким образом, стимулируют покупателей на приобретение экологически чистого транспортного средства. Денежные средства от налогов направляются на финансирование социальной сферы — здравоохранения, образования. Таким образом, в Дании действуют самые высокие налоговые ставки на транспортный налог, это обусловлено тем, что в Дании программы сохранения экологии напрямую зависят от транспортного налога.

Транспортный налог в Германии, величина которого в этой стране зависит от объема двигателя автомобиля и от объема выброса CO2 в атмосферу. Так, для автомобилей с бензиновым двигателем налоговая ставка составляет два евро за каждые 100 кум. см, а для автомобилей с дизельным двигателем — девять евро за каждые 100 куб. см. Что касается выбросов CO2 в атмосферу, если автомобиль выделяет больше 120 г CO2 на 1 км пробега, то владельцу необходимо будет уплатить два евро за каждый грамм, превышающий установленную норму [3]. Владельцы электромобилей освобождаются от уплаты транспортного налога в течение десяти лет с момента первой регистрации. Также, за покупку электромобиля правительство Германии выплачивает премии в размере 9000 евро. Действующая система транспортного налогообложения в Германии является весьма эффективной, так как заставляет задумываться граждан о покупке экологичных автомобилей, что в свою очередь оказывает позитивное воздействие на окружающую среду.

Законодательство Испании предусматривает несколько видов налогов для владельцев автомобилей. Так, при покупке нового автомобиля необходимо уплатить налог на добавленную стоимость в размере 21%. Далее закон устанавливает обязанность уплатить регистрационный налог (*Impuesto de Matriculación*), величина которого зависит от уровня выбросов автомобилем CO2 в атмосферу. Если автомобиль выбрасывает в атмосферу менее 120 г углекислого газа на один километр пробега, то собственник данного транспортного средства освобождается от уплаты налога. Максимальная ставка налога для автомобилей, сильно загрязняющих окружающую среду, составляет 14,75% от покупной стоимости [1]. От уплаты данного налога освобождаются физические лица с ограниченными возможностями. Также, государство предоставляет многодетным семьям скидку в размере

50% при уплате регистрационного налога. Помимо вышеназванных налогов, автовладельцы ежегодно уплачивают налог на механические транспортные средства (*Impuesto Sobre Vehículos de Tracción Mecánica*). Данный налог является местным. Размер налога зависит от объемов потребления топлива и экологической безопасности автомобиля. Необходимо отметить, что муниципалитеты самостоятельно устанавливают ставки налогов. Если стоимость автомобиля превышает 700 тыс. евро, то владелец автомобиля уплачивает еще и налог на «роскошь» (*Impuesto sobre el Patrimonio*). Действующая в Испании система транспортного налогообложения имеет преимущества и недостатки. Так, преимуществом является то, что при исчислении транспортного налога учитываются количество объемов выброса CO2 в атмосферу. К недостаткам транспортного налога в Испании относятся существенные различия в ставках.

В Соединенных штатах Америки транспортный налог включен в стоимость топлива (около 15% от цены с галлона бензина). Средняя ставка данного налога, включая федеральные и местные сборы, составляет 45 центов. Данная система построена в пользу экологии — кто больше ездит, тот больше платит. Таким образом, чем чаще эксплуатируется автомобиль, тем больше топлива он расходует, следовательно, больше вредных веществ выбрасывает в атмосферу, тем больше налога заплатит владелец транспортного средства. Данный подход является справедливым, так как активное использование автомобилей оказывает негативное воздействие на состояние окружающей среды.

Таким образом, рассмотрев особенности исчисления транспортного налога в зарубежных странах, можно отметить, что транспортный налог зависит не только от технических характеристик транспортного средства, но и от объемов выбросов автомобилем углекислого газа в атмосферу.

На сегодняшний день транспортный налог является одним из самых обсуждаемых в системе имущественного налогообложения Российской Федерации. Это вызвано, прежде всего, несовершенством законодательства.

Основными проблемами исчисления транспортного налога в Российской Федерации являются:

— во-первых, действующая прогрессивная шкала ставок не является справедливой. Существующая на сегодняшний день градация

ставок нуждается в реформировании, так как из-за разницы мощности двигателя на единицу лошадиной силы (далее — л.с.), налогоплательщик может заплатить в несколько раз больше. В соответствии с положениями ст. 361 НК РФ, автомобиль с мощностью 101 л.с. переходит в категорию «свыше 100 до 150 л.с.». Таким образом, налоговая ставка будет увеличена с 2,5 руб./л.с. на 3,5 руб./л.с.

Субъекты РФ вправе самостоятельно устанавливать налоговые ставки. Если обратиться к Закону города Москвы от 09.07.2008 № 33 «О транспортном налоге», то налоговая ставка для автомобилей с мощностью двигателя до 100 л.с. составит 12 руб./ л.с., а для автомобилей с мощностью двигателя свыше 100 л.с. — 25 руб./л.с. Так, владелец автомобиля с мощностью двигателя 100 л.с. уплатит налог в сумме 1200 руб., а вот владелец автомобиля с мощностью двигателя 101 л.с. заплатит уже в размере 2525 руб.

Следовательно, разница мощности двигатели на одну лошадиную силу приводит к увеличению суммы уплачиваемого налога на 1325 руб. Поэтому необходимо пересмотреть шкалу налоговых ставок;

— во-вторых, экологическая проблема. Ставка транспортного налога зависит от мощности двигателя, которая напрямую не связана с объемами выбросов транспортным средством углекислого газа в атмосферу. Зачастую именно старые автомобили в большей степени загрязняют окружающую среду, так как работают не на экологическом чистом топливе. Как было отмечено ранее, многие зарубежные страны ставят в зависимость величину налога от объема выбросов транспортным средством углекислого газа в атмосферу. Поэтому необходимо учитывать при исчислении транспортного налога также объемы выбросов транспортным средством вредных веществ в атмосферу.

В научной литературе различными авторами предлагаются варианты реформирования транспортного налога. Первым способом реформирования транспортного налога является включение транспортного налога в стоимость топлива. Здесь необходимо выделить преимущества и недостатки данного подхода. Так, к числу преимуществ включения транспортного налога в стоимость топлива следует отнести:

— повышение уровня собираемости налога — транспортный налог оплачивается одновременно со стоимостью топлива, соответственно, невозможно будет заправиться, не уплатив налог;

— социальная справедливость — больше платит тот, кто больше ездит;

— упрощение налогообложения — налоговым органам не нужно будет направлять физическим лицам уведомления для уплаты налогов.

В то же время данное предложение имеет существенные недостатки. К их числу, главным образом, относится увеличение стоимости топлива и сокращение доходов региональных бюджетов. Так как транспортный налог является региональным налогом и устанавливается законами субъектов РФ, а акциз, является федеральным налогом, то рассматриваемое нововведение приведет к уменьшению автономности субъектов РФ, в частности налоговые ставки не будут зависеть от региональной специфики.

Следующим вариантом реформирования транспортного налога является установление налоговых ставок исходя из экологического критерия. На сегодняшний день проблема загрязнения окружающей среды является наиболее актуальной проблемой современности. Как известно, основным источником загрязнения воздуха является автомобильный транспорт, выхлопные газы которого оказывают негативное воздействие на окружающую среду. Сегодня многие зарубежные страны (Испания, Франция, Великобритания) ставят в зависимость величину налога от объема выбросов транспортным средством углекислого газа в атмосферу. Данная мера стимулирует покупателей на приобретение экологичных транспортных средств, что в свою очередь оказывает позитивное воздействие на окружающую среду.

Введение же данной системы налогообложения в Российской Федерации несколько осложняется, так как уровень жизни большинства граждан не позволяет заменить старые транспортные средства на новые.

Зарубежный опыт предусматривает еще один вариант реформирования транспортного налога — исчисление налога исходя из фактического пробега автомобиля.

На сегодняшний день законодательство определяет исчисление налога исходя из фактического наличия транспортного средства. То есть независимо от того использует ли владелец автомобиль ежедневно или раз в год, ему в любом случае необходимо уплатить налог. В данном случае, можно было бы обратиться к опыту Нидер-

ландов, где был разработан проект по оснащению всех автомобилей системой *GPS* (спутниковая система навигации, обеспечивающая измерение расстояния, времени и определяющая местоположение). Сбором информации об эксплуатации транспортного средства занимается центр взимания платы.

Однако, реализовать данный проект в России не представляется возможным. Причин для этого несколько. Во-первых, недостаточная техническая оснащенность. К тому же, территория РФ в несколько раз превышает территорию Нидерландов, соответственно, достаточно проблематично отследить все передвижения транспортных средств. Во-вторых, установка системы *GPS*. Если данная установка будет осуществляться за счет владельцев транспортного средства, то это вызовет негативную реакцию со стороны общества. В то же время осуществить такую установку за счет средств бюджетов будет стоить больших денег, и в таком случае целесообразность ее внедрения ставится под вопрос.

Таким образом, изложенное свидетельствует о том, что действующая система расчета транспортного налога нуждается в совершенствовании. Методика расчета транспортного налога устарела и не соответствует современным условиям.

Рассмотрев особенности исчисления транспортного налога в зарубежных странах необходимо последовать по пути Европейских стран. В частности, при расчете транспортного налога учитывать также объемы выбросов автомобилем CO2 в атмосферу, так как именно от данного показателя зависит размер вреда, причиненного автомобилем. Однако это довольно не простой путь и для его реализации потребуется создание определенной инфраструктуры.

Литература

1. Левшукова, О. А. Транспортный налог: отечественный и зарубежный опыт / О. А. Левшукова, Д. В. Волошко, Д. А. Зацепилина // URL: https://cyberleninka.ru/article/n/transportnyy-nalog-otechestvennyy-i-zarubezhnyy-opyt/viewer
2. Немыкина, О. Е. Зарубежный опыт транспортного налогообложения / О. Е. Немыкина, А. А. Голубева // URL: https://cyberleninka.ru/article/n/zarubezhnyy-opyt-transportnogo nalogooblozheniya-1/viewer;
3. Каширина, М. В. Актуальные проблемы и пути реформирования транспортного налога в России / М. В. Каширина, Г. М. Салихов //

URL: https://cyberleninka.ru/article/n/aktualnye-problemy-i-puti-reformirovaniya-transportnogo-naloga-v-rossii/viewer.
4. Шатская, И. И. Налоговое законодательство в 2020 году: изменения, дополнения // Вестник Юридического института МИИТ. 2020 № 2.

Коцюба Вероника Денисовна,
студент Российского университета транспорта (МИИТ)

Использование смарт-контрактов при оказании финансовых услуг

Аннотация. Автор в своей статье раскрывает насущную тему современного цифрового права — использование смарт-контрактов в юридической деятельности. Технология смарт-контрактов меняет традиционные отраслевые и бизнес-процессы. Будучи встроенными в блокчейны, смарт-контракты позволяют автоматически выполнять договорные условия соглашения без вмешательства доверенной третьей стороны. Автор анализирует возможности его применения в отечественном договорном праве. На примерах показывает внедрение смарт-контрактов, а также проблемы их использования.

Ключевые слова: смарт-контракт; блокчейн; криптовалюта; договорное право; финансы; децентрализация; цифровизация.

Kotsiuba D. Veronika,
student of the Law Institute Russian University of transport

The use of smart contracts in the provision of financial services

Abstract. The author in his article reveals the pressing topic of modern digital law — the use of smart contracts in legal activity. Smart contract technology is changing traditional industry and business processes. Being embedded in the blockchain, smart contracts allow you to automatically fulfill the contractual terms of the agreement without the intervention of a trusted third party. The author analyzes the possibilities of its application in domestic contract law. Examples show the implementation of smart contracts, as well as the problems of their use.

Keywords: smart contract; blockchain; cryptocurrency; contract law; finance; decentralization; digitalization.

Смарт-контракты можно рассматривать как большой прогресс в технологии блокчейн. В 1990-х гг. смарт-контракт был предложен в качестве компьютерного протокола транзакций, который выполняет договорные условия соглашения. Договорные положения, встроенные в смарт-контракты, будут исполняться автоматически при выполнении определенного условия (например, одна сторона, нарушившая контракт, будет автоматически наказана).

Блокчейны позволяют создавать смарт-контракты. Смарт-контракты, по сути, реализуются поверх блокчейнов. Подтвержденные договорные положения преобразуются в исполняемые компьютерные программы. Логические связи между договорными положениями также были сохранены в виде логических потоков в программах. Выполнение каждого заявления о контракте записывается как неизменяемая транзакция, хранящаяся в блокчейне. Смарт-контракты гарантируют надлежащий контроль доступа и соблюдение контрактов. В частности, разработчики могут назначить разрешение на доступ для каждой функции в контракте. Как только какое-либо условие в смарт-контракте будет выполнено, запущенный оператор автоматически выполнит соответствующую функцию предсказуемым образом. Например, поставщик и покупатель договариваются о наказании за нарушение контракта. Если поставщик нарушит контракт, соответствующий штраф (как указано в контракте) будет автоматически выплачен (вычтен) из депозита Поставщика.

В отличие от смарт-контрактов, обычные контракты выполняются доверенной третьей стороной централизованно, что приводит к длительному сроку выполнения и дополнительным затратам. Интеграция технологии блокчейн с смарт-контрактами воплотит мечту о “одноранговом рынке” (peer-to-peer market) в реальность.

Смарт-контракты обладают следующими преимуществами по сравнению с обычными контрактами:

— снижение рисков. Из-за неизменности блокчейнов смарт-контракты не могут быть произвольно изменены после их выпуска. Более того, все транзакции, которые хранятся и дублируются по всей распределенной блокчейн-системе, отслеживаются и проверяются. В результате злонамеренное поведение, такое как финансовые махинации, может быть значительно упразднено;

— покращение административных и сервисных расходов. Смарт-контракты, хранящиеся в блокчейнах, могут автоматически запус-

каться децентрализованным способом. Следовательно, административные расходы и расходы на услуги, связанные с вмешательством третьей стороны, могут быть значительно сэкономлены;

— повышение эффективности бизнес-процессов. Устранение зависимости от посредника может значительно повысить эффективность бизнес-процесса. Финансовый расчет будет автоматически завершен одноранговым способом, как только будет выполнено заранее определенное условие (например, покупатель подтвердит получение товаров). В результате время выполнения работ может быть значительно сокращено.

Что касается недостатков смарт-контрактов, то они порождают его проблемы применения, что ставит под вопрос их дальнейшее развитие на отечественном рынке.

К недостаткам можно отнести:

— недостаточная гибкость функциональности умных контрактов. Если на бумажном договоре всегда есть возможность в любой момент договориться и изменить условия, то в смарт-контракте такие действия во время его исполнения совершить затруднительно. К примеру, если поставленного товара оказалось меньше, чем указано в контракте, то трекеры, отслеживающие соответствующие параметры незамедлительно передадут информацию в смарт-контракт, который в свою очередь произведет расчет с корректирующим коэффициентом;

— отсутствие в мировой законодательной практики правовое закрепление статуса смарт-контракта, что порождает проблему в их регулировании, при возникновении спорных вопросов, возникающих из нарушения контрактных условий;

— некорректность функционирования кода при создании смарт-контракта. Такое может привести к ненадлежащему исполнению условий договора или возможности проведения мошеннических операций;

— трудности описательной части поставляемых товаров или выполняемых услуг (работ);

— недостаточное наличие квалифицированных работников в данной сфере. Грамотное составление смарт-контракта зависит от компетентности специалиста, что в свою очередь требует глубокие познания в программировании и юриспруденции, знания механизма работы

всех этапов исполнения умного договора, владения определенными программами, позволяющими реализовать исполнения смарт-контракта.

Какими бы не были умные контракты надежными, при этом есть серьезные проблемы безопасности их функционирования. В начале 2018 г. был проведен анализ 970 898 смарт-контрактов на платформе *Ethereum*, показавший, что 34 200 контрактов подвержены уязвимостям, которые позволяют злоумышленникам украсть, заморозить или удалить активы, которые зафиксированы в смарт-контрактах.

Сейчас мы рассмотрим использование смарт-контрактов при оказании финансовых услуг, на примере торгового финансирования и договора факторинга.

Для финансовых услуг смарт-контракты дают возможность банкам сократить расходы, в первую очередь за счет автоматизации процесса заключения и исполнения контракта; отслеживания передвижения активов. Благодаря смарт-контракту платежи по договору становятся автоматизированными, что таким образом позволяет снизить кредитные риски и неопределенность. Следовательно, исключение человеческого фактора при документообороте, что влечет сокращение издержек.

Традиционное торговое финансирование состоит из устоявшихся этапов:

1) компания А и Б через посредника заключают контракт торгового финансирования. В качестве посредника выступает банк;

2) открытие аккредитива;

3) компания Б осуществляет поставку товаров компании А на основании заключенного договора с составлением накладной;

4) когда компания А получает товар, она оповещает об этом компанию Б через посредника, после чего совершает оплату товаров.

Как видим, традиционное торговое финансирование носит долгосрочный и затратный характер, поскольку присутствует посредник, заключение контракта проходит на бумажном формате. Также могут присутствовать трудности отслеживания поставляющихся товаров.

Торговое финансирование на основе смарт-контракта будет проходить в системе распределительного реестра — блокчейн, где две компании А и Б, заключают смарт-контракт, прописывая все условия, а также санкции за ненадлежащее исполнение договора. В состав до-

кументов, подтверждающих исполнение условий аккредитива, могут входить электронные документы: сертификат происхождения товара, страховой сертификат, счет, товарно-транспортная накладная. Далее в смарт-контракте компания А подтверждает получение товара и оплачивает его. Транзакция может быть произведена с помощью фиатных денег. Данная операция может занять всего несколько часов.

Использование технологии распределенных реестров и смарт-контрактов для осуществления сделки уменьшает риск мошенничества и существенно снижает временные издержки.

Договор факторинга для отечественного гражданского законодательства является относительно новым соглашением, который позволяет кредитору получить от третьего лица сумму в счет обязательств должника (ст. 824 ГК РФ). Факторинг — комплекс финансовых услуг, оказываемых факторинговой компанией (фактором) своему клиенту в обмен на уступку дебиторской задолженности.

Этапы классического факторинга заключаются в следующем.

1. Поставщик (кредитор) и покупатель (дебитор) заключают договор купли-продажи товара (работ, услуг).

2. Кредитор заключает договор с факторинговой компанией или банком (фактором).

3. Кредитор выполняет работы или предоставляет дебитору товары и услуги с отсрочкой платежа.

4. Кредитор передает фактору документы, подтверждающие факт появления дебиторской задолженности.

5. Фактор покрывает большую часть этой задолженности (75-95%).

6. Дебитор проводит оплату за товар (работы, услуги).

7. Кредитор и фактор проводят между собой окончательные расчеты: фактор получает обратно свои деньги с дополнительной комиссией за оказанные услуги, кредитор получает остаток полагающихся ему денежных средств (5—25%).

Одним из путей автоматизации факторинга стало применение блокчейна: соответствующие технологии в условиях приватного проекта относительно безопасны и прозрачны для всех участников. В каждый момент времени у каждого участника имеется локальная база всех операций: у поставщиков — номенклатура отгрузки, у ретейлера — принятого товара, у банков — сведения о расчетах. При наличии надежного информационного обмена между реестрами всех субъек-

тов факторинга система должна работать без сбоев и утечек. Загружаемые в сеть смарт-контракты получают на входе бухгалтерские документы в виде *Excel*-файлов унифицированной структуры — все участники факторинга применяют единый формат обмена сведениями. По каждой поставке товара на основе ключевых полей с помощью алгоритма SHA-3 (функция для создания цифровых отпечатков выбранной длины из входных данных любого размера) формируется хеш, а в смарт-контракте записывается хеш поставки, а также все суммы в валюте документа для данного хеша и даты проводки, соответствующие суммам. Если участники факторинга с помощью хеш-функции обработали один и тот же документ и при этом хеши совпали, то это служит подтверждением успешной поставки товара. У банка появляется запись о подтверждении факта поставки, и он может уверенно перечислить поставщику необходимую сумму.

Технологии блокчейна позволят в будущем вообще избавиться от недостатков традиционной схемы факторинга. В перспективе всем участникам сети не потребуется создавать или дорабатывать свои корпоративные системы для поддержки обмена данными с ретейлером, а можно будет воспользоваться уже готовыми инструментами для быстрого создания в организации узла-майнера и его подключения к своей информационной системе.

В обозримом будущем смарт-контракты станут довольно удобным инструментом появления, изменения и прекращения определенных прав и обязанностей сторон. Они позволят в течении нескольких часов заключать сделку, обеспечивая ее прозрачность и надежность. Но так ли все хорошо и безопасно? Из применительной практики данного договора следует, что они уязвимы перед компьютерными атаками, что влечет за собой, как минимум, утечку конфиденциальной информации, а как максимум, замораживание активов. Мировое законодательство должно прийти к выводу, что умные контракты — не простое явление, требующее применения «мягкого права» и закрепления в нормативно-правовых актах. Отсутствие судебной практики решения споров, вытекающих из смарт-контрактов, отталкивает контрагентов заключать их, так как при возникновении вопросов применения таких договоров, их некорректном исполнении или ошибок, стороны не смогут подать иск в защиту своих нарушенных прав.

Лопатина Виталия Вадимовна,
студент Юридического института Российского университета транспорта (МИИТ)

Сравнительная характеристика налога на доходы физических лиц в Российской Федерации и в других странах

Аннотация. В статье приводится сравнительная характеристика налога на доходы физических лиц в Российской Федерации и в Республики Беларуси, кроме того рассматриваются некоторые аспекты налогообложения этим налогом в других странах с целью выбора оптимального варианта налогообложения этим налогом. Также, с учетом опыта некоторых стран в статье анализируются различные варианты, применимые к этому налогу: от уменьшения или увеличения ставок НДФЛ, вплоть до отмены этого налога на территории РФ и анализируется целесообразность такого решения.

Ключевые слова: НДФЛ; Российская Федерация; Республика Беларусь; зарубежные страны; подоходный налог; прямой налог.

Lopatina V. Vitalia,
student of the Law Institute Russian University of transport

Comparative characteristics of personal income tax in the Russian Federation and in other countries

Abstract. The article compares the personal income tax of Russia with other countries such as Slovenia, Saudi Arabia, Somalia, including a detailed comparison of the income tax of the Republic of Belarus and the Russian Federation. It tells about countries with the highest personal income tax in the world and about countries where it is completely absent. The author discusses whether it is possible to abolish this tax in Russia and whether it is advisable.

Keywords: Personal income tax; Russian Federation; Republic of Belarus; foreign countries; income tax; direct tax.

Налог на доходы физических лиц (НДФЛ) является одним из самых важных инструментов формирования доходной части бюджетов

для большинства стран мира. Выполняя функцию перераспределения национального дохода, НДФЛ также является центральным инструментом экономической и социальной политики государства. Данный налог обладает большими возможностями воздействия на уровень реальных доходов населения и обеспечивает стабильность поступлений в бюджет за счет роста доходов граждан.

Налог на доходы физических лиц (НДФЛ) — основной вид прямых налогов, который исчисляется в процентах от совокупного дохода физических лиц за вычетом документально подтвержденных расходов, в соответствии с действующим законодательством (гл. 23.НК). Плательщиками налога на доходы физических лиц являются физические лица, для целей налогообложения, подразделяемые на две группы:

— лица, являющиеся налоговыми резидентами Российской Федерации (те, кто живет в России, постоянно и проводит на ее территории не менее 183 дней в течение 12 месяцев, идущих подряд);

— лица, не являющиеся налоговыми резидентами Российской Федерации, в случае получения дохода на территории России (ст. 207 НК) (человек, находящийся на территории РФ менее 183 календарных дней).

Статус налогоплательщика не зависит от гражданства — гражданин РФ может быть нерезидентом РФ, а иностранец — резидентом.

Для нерезидентов определены две ставки —15% (для дивидендов) и 30% (для всех остальных источников). Налогом облагаются доходы нерезидентов, полученные ими от источников в России.

Для резидентов определены следующие налоговые ставки — 9%, 13%,15% 35%. Облагаются как доходы от источников в России, так и от источников за ее пределами. К доходам граждан, которые облагаются налогом на доходы физических лиц: доходы от продажи имущества, находившегося в собственности менее трех лет; доходы от сдачи имущества в аренду; доходы от источников за пределами Российской Федерации; доходы в виде разного рода выигрышей; и иные доходы.

В соответствии со ст. 217 НК РФ к доходам физических лиц, которые не облагаются налогом на доходы физических лиц, относятся: доходы от продажи имущества, находившегося в собственности более трех лет; доходы, полученные в порядке наследования; доходы, полученные по договору дарения от члена семьи и (или) близкого род-

ственника в соответствии с Семейным кодексом Российской Федерации (от супруга, родителей и детей, в том числе усыновителей и усыновленных, дедушки, бабушки и внуков, полнородных и не полнородных (имеющих общих отца или мать) братьев и сестер) и иные доходы.

До 2020 г. включительно доходы физических лиц облагались НДФЛ по ставке 13%. С 2021 г. те, кто зарабатывает больше 5 млн руб. в год, платят при определенных условиях налог на доходы физических лиц по ставке 15%. Минфин уточнил перечень доходов, подпадающих под обложение НДФЛ в 15%, исключив из него разовые или нерегулярные доходы. Основным принципом данного законопроекта стало применение повышенной ставки НДФЛ к периодическим и активным доходам свыше 5 млн руб., связанным непосредственно с трудовой деятельностью граждан. При этом экономический эффект от новых налоговых мер не значительный. Минфин констатировал, что дополнительные доходы бюджета от введения новой ставки НДФЛ составили 60 млрд руб. в 2021 г., а в 2022 г. предполагается, что они составят 64 млрд руб., в 2023 г. — 68,5 млрд руб.

Изменение ставки с 13% до 15% коснулись не значительной части населения, для большинства населения страны ставка налога на доходы физических лиц осталась прежней — 13%. Подоходный налог остается одним из самых низких в Европе.

Налоговая система Российской Федерации постоянно совершенствуется, а вместе с ней совершенствуются механизмы исчисления и взимания налога на доходы физических лиц. Несмотря на то, что налог на доходы физических лиц давно существует и претерпевает большое количество изменений проблем достаточно много, как и дискуссий по увеличению и уменьшению ставок этого налога, поэтому необходимость его реформирования всегда будет выходить на первый план, что может эффективно отразиться на всей системе налогообложения.

В свете разговоров об объединении налоговых систем России и Республики Беларусь и создании единого налогового кодекса этих двух стран проведем подробный анализ и сравнение данного налога в России и Республике Беларусь.

В Республике Беларусь применяются разные ставки подоходного налога, однако они зависят не от величины дохода, а от его источника

и других обстоятельств. Кроме того, по каждому из видов доходов ставки подоходного налога установлены в ст. 214 НК РБ.

По данным сайта Министерства по налогам и сборам в Республике Беларусь с начала 2021 г. действуют ставки подоходного налога:

— 16% подоходного налога начисляется на доходы от основной деятельности индивидуальных предпринимателей, адвокатов и нотариусов, основание — ст. 214 НК РБ;

— 16% взимается от сумм превышения расходов над доходами — ст. 214 НК РБ;

— 16% платят физические лица по доходам от незаконной предпринимательской деятельности — ст. 214 НК РБ;

— 13% — основная ставка на все доходы физических лиц (в том числе наемных работников) — ст. 214 НК РБ.

— увеличен размер подоходного налога с 9% до 13% для доходов, полученных физлицами по трудовым договорам от резидентов ПВТ, резидентов «Великого камня»;

— 6% взимают с дивидендов, если в течение 3-х лет подряд не было распределения прибыли между отечественными получателями — ст. 214 НК РБ;

— 4% назначают на суммы выигрышей полученных от юридических лиц Республики Беларусь (законно работающие казино, букмекерские конторы, лотереи) — ст. 214 НК РБ;

— 0% платят по дивидендам, если прибыль не распределялась в течение 5 лет до этого — ст. 214 НК РБ;

— с 1 до 2 базовых величин вырос сбор за осуществление ремесленной деятельности.

В Беларуси ставка 13% — в отношении доходов, полученных физическими лицами от резидентов парка высоких технологий, а также индивидуальными предпринимателями — резидентами парка высоких технологий.

Ставка 16% — в отношении доходов индивидуальных предпринимателей, а также доходов, исчисленных налоговым органом исходя из сумм превышения расходов над доходами.

Ставка 6% — в отношении доходов в виде дивидендов при условии, если в течение трех предшествующих календарных лет последовательно прибыль не распределялась между участниками (акционерами) белорусской организации — резидентами Республики Беларусь.

Ставка 0% — в отношении доходов в виде дивидендов при условии, если в течение пяти предшествующих календарных лет последовательно прибыль не распределялась между участниками (акционерами) белорусской организации — резидентами Республики Беларусь.

Ставка 4% — в отношении доходов в виде выигрышей (возвращенных несыгравших ставок), полученных от организаторов азартных игр.

Результат сравнения по основной ставке показал, что в России и в Республики Беларусь стандартная ставка — 13%. Однако количество применяемых ставок в Республике Беларусь существенно больше и при этом налоговые ставки НДФЛ двух стран разнятся, и, это помимо основных отличий в налоговом законодательстве стран, что в будущем станет сложностью для создания общей налоговой базы.

Если обратиться к опыту взимания НДФЛ в других странах, то можно также наблюдать различную картину, существенно отличающуюся, как от России, так и от Республики Беларусь.

Так если в России, как и в Беларуси, не самая высокая процентная ставка, т.е. страны, где она достигает колоссальных размеров — 57,19% в Швеции. Как правило, такая высокая ставка в странах с высоким уровнем жизни, а высокие налоги позволяют правительствам в этих странах предоставлять своим гражданам лучшие общественные объекты и инфраструктуру и поддерживать чистоту, которая является отражением эффективного использования налогов.

В некоторых странах подоходный налог платят все физические лица, как граждане страны, так и нерезиденты этой страны, но получающие доход в рамках государства. Особенностью других стран является то, что подоходный налог взимается не только на общегосударственном уровне, но и на местном уровне — устанавливаются отчисления в бюджет префектур и муниципалитетов.

В африканской стране Кот-д'Ивуаре действует так называемый шедулярный подоходный налог, которым облагается не весь доход налогоплательщика, а только какой-нибудь конкретный его вид. Например, налог на доход от предпринимательской деятельности в промышленности, в сельском хозяйстве и торговле — 35%; налог на коммерческие доходы — 35%. Налог на заработную плату, пенсии и другие выплаты, которыми облагается 80% полученной заработной

платы оплачивается по ставке — 1,5%. Кроме того, в Кот-д'Ивуаре имеется общий подоходный налог, взимаемый по прогрессивным ставкам (максимальная — 60%), им также облагается не весь доход налогоплательщика, а его определенные составляющие.

Любое сравнение только дает подтверждение, что в России НДФЛ не высокий. Однако при этом следует разобраться, это преимущество или существуют свои минусы.

Большим плюсом высокого НДФЛ то, что большая его часть идет на развитие одних из самых важных сфер жизни общества — социальной и сферы здравоохранения, однако низкая ставка НДФЛ сильно не ударяет по доходам граждан. При этом следует не забывать, что в мире есть ряд государств, в которых, в принципе, отсутствует подоходный налог, т.е. такие государства, где физические лица не обязаны ничего выплачивать со своей заработной платы в государственный бюджет. Список государств, где жители не платят подоходный налоговый платеж: Андорра, Багамские острова, Бахрейн, Бермуды, Бурунди, Кувейт, Оман, Катар, Сомали, Объединенные Арабские Эмираты, Уругвай, Вануату, Виргинские острова, Острова Кайман, Монако, Саудовская Аравия. Все эти страны являются весьма богатыми и экономически развитыми. Большая часть из них богата природными ресурсами, в частности, нефтью и природным газом. Благодаря добыче полезных ископаемых и весьма развитой экономике эти страны не нуждается во взыскании подоходного налога с граждан.

Дискуссии подвергаются не только ставки НДФЛ, которые имеют существенные различия: от высоких до низких ставок или отсутствие этого налога вообще, также применяемые шкалы налогообложения: плоская шкала и прогрессивная. Так, в Германии, Франции, США, Китае и других странах используют прогрессивную шкалу. При прогрессивной шкале бедные иногда вовсе не платят налог или платят очень мало, а сумма подоходного налога для богатых может превышать половину дохода. В Латвии, Литве, Грузии и других применяется плоская шкала подоходного налога, которая означает одинаковый для всех процент отчислений.

Обсуждение увеличения НДФЛ или введение прогрессивной ставки налога в России идет постоянно. За введение прогрессивной шкалы подоходного активно выступают партии России, например, введение прогрессивной шкалы налогообложения — это одно из главных

требований партии «Справедливая Россия». Законодатели предлагают: ввести пониженную ставку НДФЛ 5% с доходов граждан, составивших за календарный год менее 100 тыс. руб., оставить ставку 13% с доходов от 100 тыс. руб. до 3 млн руб., ввести повышенную ставку 18% с доходов от 3 млн руб. до 10 млн руб. в год, ввести ставку НДФЛ для доходов свыше 10 млн руб. в год

Прогрессивная шкала налогообложения НДФЛ существовала в Российской Федерации до 2001 г. Минимальная ставка налога при этом составляла 12%, максимальная — 35%. При этом по данным Всероссийского центра изучения общественного мнения (ВЦИОМ), граждане с самой высокой оплатой труда, попадающей под повышенную процентную ставку, в основном являлись получателями неофициальных доходов, с которых не удерживался налог.

Переход к прогрессивной шкале налогообложения НДФЛ может привести к уклонению от уплаты налогов и не дополучению в бюджетную систему Российской Федерации соответствующих объемов денежных средств от НДФЛ. В настоящее время в России наблюдается стабильность собираемости данного налога, что является немаловажным аргументом в пользу сохранения действующей шкалы налогообложения НДФЛ.

Вывод: налоговые системы различных государств не похожи друг на друга, ставки и в целом НДФЛ зависит от многих факторов, поэтому сложно сказать, где налог лучше, а где он хуже, везде он свой, так как является составной частью всей финансовой системы государства и в каждой стране удовлетворяет свои потребности.

Мокрицына Анастасия Сергеевна,
студент Юридического института Российского университета транспорта (МИИТ)

Правовое регулирование цифрового формата взаимодействия Федеральной налоговой службы и налогоплательщиков

Аннотация. В статье анализируются программы Федеральной налоговой службы по взаимодействию с налогоплательщиками в цифровом формате, в

частности «Налогоплательщик-ЮЛ», упрощенный налоговый режим АУСН. Кроме того рассматриваются концепция по развитию электронного документооборота и практическая составляющая применения электронной подписи физическими и юридическими лицами. В статье на основании анализа сделан вывод: цифровизация документов и значительный рост их оборота оказывают стимулирующее воздействие на формирование новых цифровых сервисов для бизнеса, а цифровые процессы непосредственно влияют на вовлечение налогоплательщиков во взаимодействие с налоговыми органами в цифровой среде.

Ключевые слова: электронная подпись; налогоплательщик; цифровой формат; программы.

Anastasia S. Mokritsyna,
student of the Law Institute Russian University of Transport

Legal regulation of the digital format of interaction between the Federal Tax Service and taxpayers

Abstract. The article analyzes the programs of the Federal Tax Service for interaction with taxpayers in digital format, in particular «Taxpayer-LE», the simplified tax regime of the AUSN. In addition, the concept for the development of electronic document management and the practical component of the use of electronic signatures by individuals and legal entities are considered. Based on the analysis, the article concludes that the digitalization of documents and a significant increase in their turnover have a stimulating effect on the formation of new digital services for business, and digital processes directly affect the involvement of taxpayers in interaction with tax authorities in the digital environment.

Keywords: electronic signature; taxpayer; digital format; programs.

В современных реалиях приоритетами деятельности налоговых органов являются повышение прозрачности и уровень доверия общества за счет внедрения механизмов автоматического соблюдения налогового законодательства. В настоящий момент примером такого механизма является функционирование приложения для самозанятых граждан, которое позволило максимально упростить уплату налогов для указанной категории лиц. Кроме того введение такого налога способствовало выводу из тени тех, кто получал доход, но не платил

налогов. В ближайшей перспективе такой же алгоритм будет предложен и малому бизнесу. Данные решения помогают обеспечивать прозрачность экономики и усилить контроль за своевременной уплатой налогов.

В Указе Президента РФ от 21.07.2020 № 474 «О национальных целях развития Российской Федерации на период до 2030 года» в качестве национальной цели определена «цифровая трансформация», которая стала флагманом в работе налоговых органов. Цифровые процессы, которые в настоящее время можно наблюдать в налоговом администрировании вносят новые способы реализации в уже существующие функции. Предоставление электронных услуг вошло в повседневные обязанности ФНС России. Культура построения взаимодействия ФНС России и налогоплательщика отражается в развитии процесса предоставления электронных услуг, которая позволила сократить очереди в инспекциях, и время, как правило, уходящее на бумажную переписку и самостоятельный расчет налоговой ставки. В данный период времени в работе ФНС России функционируют 23 онлайн-сервиса, способствующих тому, что налогоплательщик самостоятельно может пройти регистрацию с помощью госуслуг (ЕСИА), с использованием простого и понятного алгоритма, который включает регистрацию: фамилию имя отчества (ФИО), номер пенсионного страхования и номер индивидуального налогоплательщика (ИНН). После прохождения данного этапа пользователю открывается доступ ко всем доступным на портале услугам в соответствии с распорядительными документами. Таким образом, для понимания процесса подачи налоговой отчетности через систему интернет необходимо найти законодательное закрепление таких основополагающих понятий, как электронный документ и его правовой режим.

Под электронным документом понимается документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах. Исходя из этого, можно сделать вывод, что электронный документ — это любой документ, который представлен в электронном виде, в том числе это может быть скан-образ документа, файл, набранный в текстовом редакторе, и т.п. Юридическая значимость

электронного документа закрепляется нормативно-правовыми актами: Гражданский кодекс Российской Федерации, Налоговый кодекс Российской Федерации, Федеральные законы от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений Российской Федерации», от 27.07.2006 № 152-ФЗ «О персональных данных», от 06.04.2011 № 63-ФЗ «Об электронной подписи», от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 06.12.2011 № 402-ФЗ «О бухгалтерском учете».

В качестве одного из примеров развития правового регулирования цифрового формата взаимодействия ФНС России и налогоплательщиков рассмотрим возможность сдачи налоговых деклараций. ФНС России предлагает пользователям «Налогоплательщик-ЮЛ». Это бесплатное программное обеспечение, позволяющее сформировать налоговую декларацию. Функциями данной программы являются: автоматический расчет показателей в соответствии с порядком по заполнению; контроль показателей в соответствии с порядком по заполнению и форматом представления в электронной форме; формирование файла в формате передачи данных в электронной форме; ведение реестра выгруженных файлов; автоматизированное формирование документов путем загрузки данных из файлов установленного формата; ведение списка налогоплательщиков и их объектов; ведение списка сотрудников и контрагентов; ведение архива описаний форм отчетности; формирование файла транспортного контейнера для дальнейшей передачи через интернет-сайт ФНС России налоговой и бухгалтерской отчетности, справок о доходах физических лиц и других документов; сохранение и восстановление информации. При этом данное программное обеспечение ФНС России выполняет множество функций, формируя файлы для передачи данных о налогах, сборах, страховых взносах, пенях, штрафах, процентах для перечисления в бюджетную систему Российской Федерации единого налогового платежа организации, индивидуального предпринимателя в электронной форме в соответствии с приказом ФНС России от 25.02.2022 № ЕД-7-10/162@ «Об утверждении Дорожной карты по сокращению бумажного документооборота в Федеральной налоговой службе до 2025 года».

Однако работа по улучшению взаимодействия с налогоплательщиками со стороны ФНС России продолжается. Следующим этапом та-

кого взаимодействия выступает экспериментальный ввод налогового режима для юридических лиц и индивидуальных предпринимателей с 1 июля 2022 г., который продлиться до 31 декабря 2027 г. в Москве, Московской области, Калужской области и Республики Татарстан. Данный режим будет представлять собой автоматизированную упрощенную систему налогообложения (АУСН) для юридических лиц и индивидуальных предпринимателей численностью до пяти человек. В рамках пилотного проекта предлагается два варианта ставки: доходы 8%, либо доходы-расходы 20%. Предприниматели смогут выбирать из двух вариантов сборов: от доходов либо от доходов минус расходы.

ФНС России предпринимаются попытки к созданию идеальной среды для самостоятельной уплаты налогов гражданами. Исходя из результатов исследований, простота цифрового формата взаимодействия влияет на стремление людей самостоятельно выплачивать основные налоги. В результате формируется система доверия граждан, экономится время за счет автоматизации расчетов налогов.

Курс на сервисные функции уже показывает свои результаты, влияя на качество уплаты налогов налогоплательщиками собственноручно. Опыт налоговой службы подтверждает, что с помощью услуг может обеспечивать уплату большего количества налогов, при этом во многом сокращая издержки. В данном случае под издержками следует понимать в целом издержки не только денежные и временные, но и издержки взаимодействия ФНС России с плательщиком.

Кроме того переход на безбумажные технологии оказал экономический эффект, путем снижения затрат на почтовые услуги, содержание бумажных архивов, а именно экономия на бумаге, аренду помещений для архивов, сокращение персонала.

В 2020 г. при участии бизнес-сообщества и ФНС России были проанализированы проблемы, существующие в практике электронного документооборота. Итогом данного мероприятия стала разработка двух важных документов: Концепции по развитию электронного документооборота в хозяйственной деятельности предприятия и План мероприятий по ее реализации.

Концепция по развитию электронного документооборота в хозяйственной деятельности предприятия направлена на повышение качества и эффективности документооборота, в частности на основе вы-

сокотехнологичных решений, упрощения, облегчения и создания комфортных условий для электронного взаимодействия между государственными органами власти и хозяйствующими субъектами, на повышении доверия к цифровым технологиям и за счет оптимизации нормативного правового регулирования.

В качестве принятых мер по внедрению электронного документооборота разработан сервис «Типовой сценарий перехода на электронный документооборот». В первую очередь данный сервис для тех субъектов, которые хотят перейти на электронный документооборот, но не знают, как это сделать, в частности это касается небольших предприятий. Система шагов, на которой построен сервис, позволяет ознакомиться с документами, которые нужно изучить для перехода на электронный документооборот, а также ознакомится с существующими на рынке решениями и мероприятиями, которые нужно организовать внутри предприятия.

Отрасль цифрового взаимодействия находится в стадии формирования, поэтому стоит отметить проблему, возникающую при реализации информационных технологий — сложности с электронно-цифровыми подписями налогоплательщиков. В ходе изучения поставленного вопроса были проанализированы теоретические и практические аспекты применения электронной подписи.

В Федеральном законе «Об электронной подписи» законодателем разъяснено, что понимается под электронной подписью. Информация в электронной форме, присоединенная к другой информации в электронной форме, используемая в целях определения лица, подписывающего информацию. Для ее создания формируется ключ, сочетающий в себе уникальную последовательность символов. По юридической силе электронная подпись равна традиционной, письменной, подписи, удостоверяющей лицо, ее совершившее.

На данном этапе такая процедура была доступна физическим лицам. Однако большинству предприятий, индивидуальным предпринимателям для предоставления сведений в электронной форме, связанных с осуществляемой ими предпринимательской или профессиональной деятельностью, требуется квалифицированная электронная подпись, которая необходима для направления налоговой отчетности через систему интернет, предоставления государственных и муниципальных услуг в электронном виде и обеспечения межведомственно-

го электронного взаимодействия. Осуществление такого порядка невозможно без законодательного закрепления таких основополагающих понятий, как электронная подпись и ее правовой режим.

Кроме того набирающая ход цифровизация, повлияла на необходимость изменений в законе об электронной подписи, которая была обусловлена проблемами несовершенства механизмов использования электронной подписи. С 1 января 2022 г. на ФНС России возлагаются функции по выпуску квалифицированной электронной подписи юридических лиц (лиц, имеющих право действовать от имени юридического лица), индивидуальных предпринимателей и нотариусов в соответствии с законодательством об электронной подписи. Юридическими лицами в соответствии с законодательством применяется квалифицированная электронная подпись, особенностью которой является применение методов криптографической защиты. В связи с тем, что аккредитованным в настоящее время удостоверяющим центрам необходимо пройти процедуру переаккредитации, при этом срок действия выпущенных ими квалифицированных сертификатов электронной подписи имеет ограничительные сроки, ФНС России совместно с удостоверяющими центрами приступил обеспечивать выпуск квалифицированной электронной подписи для юридических лиц, индивидуальных предпринимателей и нотариусов в целях обеспечения перехода от платной услуги по выпуску электронной подписи к безвозмездной государственной услуге по выпуску электронной подписи.

В результате проведенного анализа были изучены, исследованы и выявлены проблемы реализации использования электронной подписи, рассмотрены области применения электронного документа, отмечены положительные стороны реформирования ФНС. Также было раскрыто значение цифровых процессов для вовлечения налогоплательщиков во взаимодействие с налоговыми органами в цифровой среде. Кроме того проанализированы основные программы ФНС России по взаимодействию с налогоплательщиками в цифровом формате.

Вывод: объем информации увеличивается регулярно, возможности налоговой службы по обработке и хранению информации требуют постоянного развития и совершенствования для комфортного взаимодействия между налогоплательщиками и ФНС России, а ряд выявленных проблем, необходимо решить в ближайшие несколько лет. Кроме того отмечается позитивное направление политики ФНС Рос-

сии в области цифрового взаимодействия с налогоплательщиками, ряд программ ФНС России: «Налогоплательщик-ЮЛ», упрощенный налоговый режим АУСН, концепция по развитию электронного документооборота в хозяйственной деятельности является подтверждением.

Мушегян Карине Арменовна,
студент Юридического института Российского университета транспорта (МИИТ)

Проблемы и пути решения при налогообложении самозанятых граждан в Российской Федерации

Аннотация. В данной статье рассматривается налоговый режим — налог на профессиональный доход и возможность получения физическим лицом статуса самозанятого. Анализируются особенности режима с учетом существующих достоинств и выявленных недостатков. Кроме того исследуются проблемы, позволившие определить противоречивый характер налогового режима для самозанятых и предложить способы мотивации самозанятых лиц самостоятельно вставать на учет в налоговых органах и увеличивать количество добровольных пенсионных взносов.

Ключевые слова: налогообложение; новый налоговый режим; налог для самозанятых; самозанятые; законодательство.

Mushegyan A. Karine,
student of the Law Institute, Russian University of Transport

Problems of taxation of self-employed citizens in Russia and ways to solve them

Abstract. This article discusses a new tax regime — the tax on professional income. The possibility of obtaining self-employed status by an individual is described, its features, including existing advantages and disadvantages. The problems, the contradictory nature of the tax regime for the self — employed and possible ways of motivating self-employed persons to register with the tax authorities

on their own, to increase the number of voluntary pension contributions to the Pension Fund of Russia are investigated.

Keywords: taxation; tax; self-employed; legislation; new tax regime; tax on the self-employed.

В России самозанятые граждане составляют до четверти всех работающих граждан — около 16—17 млн человек. По некоторым оценкам, число самозанятых граждан достигает 25 млн, для 9—10 млн из них самозанятость — единственный источник дохода. При этом по данным налоговых органов, только полмиллиона человек официально зарегистрированы в качестве самозанятых и платят налоги, что отражается на бюджете страны, который теряет несколько десятков миллиардов рублей ежегодно.

Быть неплательщиком налогов сложно, так как отсутствие официального статуса подводит к определенному риску проверок и штрафов при привлечении клиентов через средства массовой информации и рекламу. Также возникают сложности по взятию кредита или ипотеки в банке, где требуется справка о наличии подтвержденных доходов. Кроме того существовала проблема с уплатой налога с доходов от самозанятости, решением которой было: либо заполнять декларацию и платить НДФЛ 13%, либо получать статус индивидуально предпринимателя, что вызывало определенные неудобства, а кроме того было невыгодно, поэтому большинство самозанятых работали нелегально.

С 1 января 2019 г. в России начал функционировать новый налоговый режим — налог на профессиональный доход (НПД). Введение этого налога в 2019 г. способствовало выводу из тени тех, кто получал доход, но не платил налогов. Кроме того у налогоплательщиков этого налога появилась возможность открыто размещать рекламу, расширять клиентскую базу за счет новых клиентов и законно отстаивать свои права в суде. Изначально НПД проводился в городе федерального значения Москве, в Московской и Калужской областях, а также в Республике Татарстан, затем в связи с изменениями в закон, с 1 июля 2020 г. налог на профессиональный доход за счет своей востребованности и действенности распространился на все регионы страны, количество зарегистрированных лиц составило около 1,7 млн человек. Эксперимент продолжится до окончания 2028 г., при этом налоговая ставка останется неизменной.

Налоговая ставка для самозанятых зависит, от кого получен доход — 4% от физических лиц и 6% от индивидуальных предпринимателей или юридических лиц. Налог на профессиональный доход могут платить: физические лица, которые оказывают услуги или продают что-то, сделанное своими руками, при этом перепродавать готовые товары нельзя и индивидуальные предприниматели, которые занимаются бизнесом, но уже не на упрощенной системе налогообложения, а на новом режиме. Если они не откажутся от своего прежнего налогового режима, стать самозанятыми не смогут. Кроме того у них нет наемных работников с трудовыми договорами и они подали заявление на регистрацию как плательщики налога на профессиональный доход — в инспекцию того региона, где работают.

Однако стоит подчеркнуть, что не все могут перейти на новый налоговый режим. Налог на профессиональный доход не могут платить физические лица и индивидуальные предприниматели, которые занимаются следующими видами деятельности: продажа подакцизных товаров и тех, которые нужно обязательно маркировать; перепродажа товаров и имущественных прав; добыча и продажа полезных ископаемых; работа в интересах других лиц по договорам поручения, комиссии или агентским; деятельность курьеров и водителей, которые при доставке принимают деньги у покупателей и потом передают их продавцам.

Налог на профессиональный доход могут применять только те, у кого доход не больше 2,4 млн руб. в год. Это примерно 200 тыс. руб. в месяц, но сумма дохода в месяц не имеет значения — отдельных ограничений именно по ежемесячному доходу нет. Можно в январе получить 20 тыс., в феврале ничего, а в марте — 400 тыс. В том случае, если лимит превышен у физического лица все доходы сверх лимита облагаются налогом НДФЛ по ставке 13%, Индивидуальные предприниматели же должны будут перейти на любой спецрежим или применять общую систему. Переход на спецрежим у них не произойдет автоматически, нужно подать заявление в налоговую. На это есть 20 календарных дней. В следующем году можно будет опять перейти на спецрежим для самозанятых, но необходимо подавать заявление вновь.

Доходы от физических лиц и юридических лиц учитываются отдельно. Все это отражается в мобильном приложении «Мой налог» и личном кабинете самозанятого на сайте ФНС России.

Суть данного эксперимента, заключается в «обелении» или легализации теневой экономики России. Главное, что позволяет данный режим, — это заниматься предпринимательской деятельностью без образования юридического лица (например, ООО или открытия индивидуального предпринимательства), что упрощает налоговую отчетность и применяемую ставку. Кроме того эксперимент помог без особых трудностей легализовать бизнес и подработки, облегчить процесс оформления и сэкономить на налогах.

Вопросы вовлечения в сферу налогообложения самозанятых граждан актуальны на территории РФ. Главной проблема подобной занятости остается то, что большая часть граждан, потенциально относящихся к самозанятым, не платит вовсе никаких налогов и социальных взносов со своего заработка, что в свою очередь ведет к потере значительной части доходов бюджетной системы.

В настоящее время проблема неуплаты налогов самозанятыми актуализируется в связи с расширением спектра видов деятельности, обусловленных развитием информационных технологий, в котором активно задействованы самозанятые граждане. Существенное беспокойство вызывает активное формирование новой категории работников — независимых профессионалов, не входящих в работу организаций, оказывающих услуги различным организациям в режиме удаленного доступа — фрилансеров. Однако решение этой проблемы на данный период времени — это привлечение к налоговой, административной и уголовной ответственности.

Если до налоговой дойдут сведения о неуплате налога, то она может доначислить их за три года и взыскать пени — 1/300 ключевой ставки Банка России за каждый день просрочки.

Штраф за неуплату налогов составляет от 20 до 40% от неуплаченной суммы. Еще есть штраф за не сданные декларации — до 30% от суммы налога за каждый год.

Проблема налогообложения самозанятых связана с частным характером предоставления ряда услуг (репетиторы, услуги по ремонту квартир, художники, кондитеры на дому и др.), которые могут оказываться частным путем, без официального документального оформления трудовых отношений и, как следствие, не облагаться налогами.

Но на сегодняшний день у самозанятых граждан нет полной уверенности в том, что их бизнес-идея принесет положительный результат,

привлечет интерес потенциальных клиентов и тем самым принесет прибыль. В такой ситуации справедливо будет введение дополнительных условий, согласно которым самозанятым будет дан период времени, чтобы адаптироваться к рынку. Продолжительность такого периода должна устанавливаться налоговыми органами и может видоизменяться в зависимости от вида деятельности и сферы ее реализации, но механизм применения и функционирования должен остаться без изменений.

Как ранее уже отмечалось, в новом налоговом режиме нельзя нанимать сотрудников по трудовым договорам. Самозанятые могут работать только сами на себя. Если нужны помощники, придется нанимать людей по гражданско-правовому договору или регистрировать индивидуальное предпринимательство, что значительно усложняет процесс ведения собственного бизнеса. Данную проблему возможно было избежать, если бы государство позволило нанимать хотя бы одного сотрудника по трудовому договору. К примеру, вы кондитер и нуждаетесь в помощи, для того чтобы успевать отдавать заказы в срок. Вам не нужен целый штат сотрудников, достаточно одного помощника. В этом случае вы бы могли привлечь такого сотрудника по трудовому договору.

Важной проблемой режима самозанятости является тот факт, что трудовой стаж не идет в пенсию. То есть если не платить страховые взносы, трудовой стаж не засчитают. Поэтому копить на пенсию придется самостоятельно. Если не набрать нужное количество пенсионных баллов, на пенсию можно будет выйти в 70 лет. При этом пенсия будет минимальной. В будущем будет большое количество пожилого нетрудоспособного населения, оставшиеся без полной финансовой поддержки государства. Но почему самозанятые пока принимают именно такой выбор? Причина, по нашему убеждению, ментальная — пенсия у нас ассоциируется со старостью и потерей трудоспособности. Если поменять восприятие и начать говорить не о пенсии, а о будущей финансовой свободе, у людей появится интерес.

Таким образом, проанализировав содержание Федерального закона от 27.11.2018 № 422-ФЗ «О проведении эксперимента по установлению специального налогового режима “Налог на профессиональный доход”», можно сделать вывод, что необходимо совершенствование налогового законодательства, особенно в процедуре взимания налогов с самозанятых лиц.

Реализация мер, описанных в статье, скорее всего, послужит мотивирующим фактором для самозанятых самостоятельно зарегистрироваться в налоговых органах и своевременно уплатить налог, так же как и повысить статистику перечисления добровольных страховых взносов в Пенсионный фонд РФ.

Орлов Михаил Викторович

Актуальные вопросы обеспечения кибербезопасности систем организации воздушного движения

Аннотация. Статья посвящена анализу современной проблемы обеспечения кибербезопасности в авиационной сфере с учетом возрастающего развития информационных технологий. Автором рассматриваются существующие рекомендации международного уровня по необходимости внедрения комплексного подхода к использованию новейших разработок средств обеспечения кибербезопасности в инфраструктуре информационных и связных технологий гражданской авиации.

Ключевые слова: информационная безопасность; кибербезопасность; системы организации воздушного движения; киберугрозы; кибератаки; стратегия кибербезопасности; средства защиты информации.

Orlov V. Mihail

Current issues of ensuring cybersecurity of air traffic management systems

Abstract. The article is devoted to the analysis of the modern problem of ensuring cybersecurity in the aviation sector, taking into account the increasing development of information technologies. The author examines the existing recommendations of the international level on the need to introduce an integrated approach to the use of the latest developments in cybersecurity in the infrastructure of information and communication technologies of civil aviation.

Keywords: information security; cybersecurity; air traffic management systems; cyber threats; cyber attacks; cybersecurity strategy; information security tools.

Введение

Составной частью национальных программ обеспечения безопасности полетов и авиационной безопасности являются мероприятия по обеспечению кибербезопасности систем информационных и связных технологий гражданской авиации [Руководство по безопасности системы организации воздушного движения 2013 г.].

Международная организация гражданской авиации (ИКАО) рекомендует [Руководство по авиационной безопасности 2014 г.], включать в государственные системы контроля над обеспечением авиационной безопасности и безопасности полетов кибербезопасность, как часть комплексной системы управления факторами риска.

Кибербезопасность — это реализация мер защиты систем, сетей и программных приложений от сетевых атак.

В стандартах и нормативных документах часто встречаются различные термины «информационная безопасность» и «кибербезопасность».

Оба термина являются синонимами друг друга, но разница между ними тонкая. Кибербезопасность — это защита киберпространства от несанкционированного цифрового доступа. Таким образом, все дело в защите данных, которые находятся в электронной форме. Информационная безопасность — это защита информационных активов от несанкционированного доступа.

Угрозы кибербезопасности исходят от потенциальных нарушителей, которыми могут являться:

— хакеры (хакерские группировки);

— киберпреступники;

— кибершпионы.

Регулирование вопросов обеспечения кибербезопасности

Вопросы обеспечения кибербезопасности в различных автоматизированных и информационно-телекоммуникационных системах регулируются уполномоченными органами международного, регионального и национального уровня.

Общие вопросы обеспечения кибербезопасности международного уровня регулируются следующими организациями: Международным союзом электросвязи (МСЭ); Международной организацией по стандартизации (ИСО); Международной электротехнической комиссией (МЭК). Указанные органы, в пределах своей компетенции, разраба-

тывают и издают рекомендации и международные стандарты. Ими создается и организуется работа экспертных групп по различным направлениям обеспечения кибербезопасности.

Вопросы обеспечения кибербезопасности в гражданской авиации на территории государств-участников Соглашения[1] регулируются: Международной организацией гражданской авиации (ИКАО**)**; Межгосударственным авиационным комитетом (МАК). Указанные органы издают руководства (рекомендации) и квалификационные требованиям.

В качестве примера, можно привести Руководство по безопасности системы организации воздушного движения (DOC 9985) — ИКАО, а также квалификационные требования КТ-178 — МАК.

Объекты защиты в системах организации воздушного движения

В соответствии с рекомендациями объектами защиты от киберугроз в системах организации воздушного движения (ОрВД) являются:

— информация/данные;

— киберсистемы информационных технологий;

— киберсистемы связных технологий.

К информации/данным относятся оперативная информация и личные данные сотрудников, которые формируются и обрабатываются в системах ОрВД.

Под оперативной информацией понимается информация, относящаяся к предоставлению обслуживания воздушного движения.

В ее состав также входит информация по обеспечению безопасности, которой органы ОрВД обмениваются с национальными и региональными ведомствами по авиационной безопасности, органами национальной безопасности и обороны, правоохранительными органами. Часть такой информации о безопасности может носить конфиденциальный характер.

Киберсистемы информационных технологий включают в себя программные и аппаратные средства.

Программные средства охватывают операционные системы, прикладные программы и программные средства обработки данных.

[1] Соглашение о гражданской авиации и об использовании воздушного пространства Содружества Независимых Государств 1991 г.

Аппаратные средства включают в себя сервера, терминалы, системы хранения данных и кабельные сети.

Киберсистемы связных технологий — это телекоммуникационые устройства и сети, которые могут носить локальный, региональный и глобальный характер и быть проводными и беспроводными.

Задачами обеспечения кибербезопасности систем ОрВД являются:

1) конфиденциальность — исключение возможности получения информации субъектами, не имеющими на это полномочий. Нарушение конфиденциальности может привести к несанкционированному ознакомлению и раскрытию информации. При необходимости, конфиденциальность обеспечивается путем шифрования передаваемых или хранимых данных;

2) целостность — исключение возможности несанкционированного изменения или уничтожения информации;

3) доступность — обеспечение непрерывности, надежности и доступности данных, своевременное и санкционированное предоставление пользователям ресурсов. Нарушение доступности может привести к сбоям и отказам в работе систем ОрВД.

Угрозы кибербезопасности систем организации воздушного движения

В настоящее время существуют следующие угрозы кибербезопасности систем ОрВД:

— нанесение умышленного вреда;

— влияние человеческого фактора;

— ошибки сторонних кампаний, участвующих в обеспечении работы систем ОрВД;

— системные ошибки в функционирований программных и аппаратных средств, телекоммуникационного оборудования;

— явления природного характера;

Для проведения кибератак на системы ОрВД потенциальные нарушители используются следующие методы:

— внедрение вредоносного программного обеспечения;

— взлом через уязвимости web-приложений;

— отказ сервисов (DoS, DDoS-атаки);

— применение бот-сетей;

— фишинг, фрод и другие виды хакерских атак;

— использование вирусов-вымогателей;

Возможными негативными последствиями кибератак для авиакомпаний/аэропортов являются:

— кража персональных данных пассажиров;
— перебои в работе служб и систем;
— кража данных платежных карт;
— нарушение работы паспортного контроля;
— репутационные риски;
— угрозы жизни и безопасности пассажиров;
— сбои при обработке багажа;
— отказ элементов критической инфраструктуры;
— нарушения графика полетов;
— взлом терминалов CCTV.

Известные случаи кибератак на объекты гражданской авиации:

— 2013 г. — на одной из международных авиаконференций было продемонстрировано, как при помощи оборудования за 2000 долл. в открытой продаже можно создавать ложные метки воздушных судов, которые службы УВД будут воспринимать как реальные. В этом же году один из хакеров, сидя в аэровокзале, вошел в систему развлечения пассажиров на борту летящего самолета;

— 2013 г. — кибератака привела к остановке систем паспортного контроля в аэропортах Стамбула. В том же году — кибератака на 75 аэропортов США;

— 2014 г. — исчезновение рейса MH370 Малазийских авиалиний. Одна из версий — связное оборудование самолета было отключено дистанционно злоумышленниками, которые затем направили самолет в Индийский океан, лишив экипаж какой-либо возможности вернуть себе управление воздушным судном. Поскольку поиски закончились безрезультатно, данная версия не подтверждается, но и не отметается полностью, несмотря на заверения *Boeing* в невозможности таких действий. В том же году хакеры провели скоординированные атаки на компьютерные системы более чем в 16 странах, включая аэропорты и авиакомпании Пакистана, Саудовской Аравии, Южной Кореи и США;

— 2015 г. — сразу несколько чрезвычайных происшествий.

FAA обнаруживает различные формы вредоносного программного обеспечения в персональных учетных записях электронной почты.

Компания *United Airlines* приостановила все свои рейсы над территорией США после того как в компьютерной системе появились ложные планы полета.

Польская авиакомпания *LOT* столкнулась с кибератакой, которая привела к сбоям в наземном обслуживании воздушных судов. Авиакомпании *Ryanair* нанесен финансовый ущерб в размере около 3 млн фунтов в результате кибератаки на ее банковские счета.

В августе 2016 г. из-за сбоя в компьютерной системе *Delta Airlines* в Атланте отключились сервера компьютерной системы авиакомпании. В результате сотни тысяч людей по всему миру столкнулись с непредвиденными сложностями.

В декабре 2016 г. появились официальные сведения о том, что группе компьютерных специалистов, при помощи беспроводного *Wi-Fi* подключения в салоне пассажирского воздушного судна, удалось установить контроль над самолетом. Фактически, экспертам удалось обойти встроенную защиту и заполучить полный доступ над воздушным судном, и этому есть неопровержимые доказательства.

British Airways была оштрафована на 183 млн фунтов стерлингов за утечку данных в 2018 г., когда киберпреступники похитили около 500 тыс. личных данных пассажиров, используя фальшивый вебсайт.

В том же 2018 г. авиакомпания *Cathay Pacific* из Гонконга стала жертвой успешной кибератаки, которая привела к утечке персональных данных до 9,4 млн человек!

Многие киберинциденты не предаются гласности в целях сохранения репутации авиакомпаний и аэропортов.

Согласно информации экспертов по авиационной кибербезопасности:

— в 2021 г. хакеры предпринимали более 1000 кибератак в месяц на объекты авиационного сектора;

— к концу 2021 г. авиакомпании могут потерять от кибератак более 2 трлн долл.

Наблюдается рост инцидентов в области информационной безопасности, включаю как кибератаки, так и нарушения в работе информационных и связных технологий, которым подвержена отрасль гражданской авиации по всему миру в последние годы.

Обеспечение кибербезопасности систем организации воздушного движения

Большинство государств мира принимают меры для обеспечения защиты своих автоматизированных и информационно-телекоммуникационных систем от киберугроз.

В первую очередь это разработка национальной стратегии кибербезопасности — 38% стран опубликовали стратегию кибербезопасности, 12% государств находятся в процессе ее разработки. Вместе с тем, 50% стран до сих пор не имеют стратегии кибербезопасноти, то есть — четкого плана действий по защите от киберугроз, в том числе в гражданской авиации.

Концептуальное видение ИКАО глобальной кибербезопасности [Декларация о кибербезопасности в гражданской авиации (Дубайская декларация) 2017 г., Стратегия в области авиационной кибербезопасности 2019 г., План действий по обеспечению кибербезопасности 2020 г.] состоит в том, что авиационный сектор должен быть устойчив к кибератакам, сохраняя надежность и глобальное доверие к себе, продолжая при этом внедрять инновации и развиваться.

По мнению международных организаций, основными элементами, повышающими уровень кибербезопасности, являются:

— юридическое обеспечение (разработка и реализация правовой основы обеспечения кибербезопасности);

— технический уровень (изучение и применении новейших информационных технологий для защиты от киберугроз);

— организационное обеспечение (создание специализированных подразделений, разработка организационных документов по кибербезопасности);

— наращивание потенциала борьбы с киберпреступностью (изучение кибератак, разработка форм и методов защиты информации);

— международное сотрудничество (обмен информацией по кибератакам, взаимодействие по предупреждению киберпреступности).

Для защиты систем ОрВД рекомендовано использование следующих средств защиты информации:

— программные средства разграничения доступа;

— программные (технические) средства идентификации и аутентификации;

— межсетевые экраны (МЭ);

— средства обнаружения компьютерных атак (СОА);

— средства антивирусной защиты (САВЗ);

— средства криптографической защиты информации (СКЗИ).

В последнее время в составе автоматизированных систем появились комплексы средств мониторинга кибербезопасности (Центры средств мониторинга кибербезопасности (по-английски — *SOC*)).

Для обеспечения кибербезопасности систем ОрВД необходимо осуществить комплекс следующих мероприятий:

— выбор технических и программных средств — применение программно-технических платформ, отвечающих требованиям кибербезопасности (процессор, *BIOS*, *ОС*, приложения и т.п.);

— разработка систем защиты на основе модели угроз и модели нарушителя — определение угроз, нарушителей, которые могут реализовать эти угрозы, на их основе применение средств защиты нейтрализующих угрозы;

— полная и точная реализация мер обеспечения кибербезопасности — при вводе систем ОрВД в эксплуатацию выполнение всех требований по защиты информации;

— ежедневное выполнение комплекса мер обеспечения кибербезопасности — разработка организационных документов, доведение их до персонала, работа администраторов безопасности информации;

— мониторинг угроз кибербезопасности и своевременное реагирование — изучение новых информационных технологий, выявление и изучение новых угроз.

В части средств вычислительной техники (СВТ) и программного обеспечения (ПО) систем ОрВД целесообразно проведение следующих мероприятий:

— поиск уязвимостей в СВТ и ПО;

— контроль выполнения мер защиты информации;

— модернизация программных и технических средств.

Обязательно проведение мероприятий с персоналом систем ОрВД (человеческий фактор):

— обучение выполнению мер защиты информации;

— контроль выполнения требований организационных документов по обеспечению кибербезопасности;

— совершенствование знаний персонала по защите информации (повышение квалификации, занятия, зачеты).

В обеспечении кибербезопасности систем ОрВД существуют следующие проблемы:

1) существенное увеличение количества кибератак на объекты ОрВД — ежемесячно более 1000 атак;

2) отсутствие средств защиты от кибератак линий передачи данных АЗН-К, CPDLC, TIS-B, FIS-B, SWIM, DGNSS, а также для голосовых сообщений;

3) автоматическое зависимое наблюдение вне зависимости от используемого стандарта линии передачи данных на сегодняшний день не обеспечивает целостности данных, необходимой для использования информации наблюдения в целях обслуживания воздушного движения.

4) не обеспечена киберзащита систем ОрВД при переходе от системы аэронавигационной информации к управлению аэронавигационной информации;

5) в системах ОрВД используются технологии, уязвимые для взлома из-за открытой архитектуры и применения незашифрованных сигналов.

С учетом рекомендаций ИКАО предлагаются следующие направления обеспечения кибербезопасности систем ОрВД:

1) разработка и внедрение нормативных документов по кибербезопасности (рекомендации и руководства, международные и национальные стандарты, национальные стратегии и планы);

2) совершенствование технологий систем ОрВД (внедрение новых информационных технологий, с учетом требований по обеспечению кибербезопасности);

3) анализ рисков и мониторинг угроз кибербезопасности (проведение научных исследований по анализу угроз, оценке рисков, мониторинг действующих систем ОрВД);

4) обучение и контроль деятельности персонала (занятия и курсы усовершенствования, периодический и выборочный контроль выполнения мер кибербезопасности);

5) сотрудничество и обобщение опыта обеспечения кибербезопасности (сотрудничество на международном, региональном уровне, обмен информацией о кибератаках и киберинцидентах).

Павлюченкова Светлана Евгеньевна,
студент Юридического института Российского университета транспорта (МИИТ)

Экологическое налогообложение: реалии России и опыт зарубежных стран

Аннотация. В статье проанализированы экологические платежи в Российской Федерации и зарубежных странах, в частности: плата за негативное воздействие на окружающую среду, экологический и утилизационный сбор и сделаны выводы: технический прогресс, задействовавший практически все отрасли производства стран мира вывел проблемы экологии из вторичных в ранг основных, что в свою очередь обусловило необходимость внедрения новых инструментов регулирования данных правоотношений и разработку новых механизмов по совершенствованию экологической политики, в том числе, в сфере налогообложения.

Ключевые слова: экологические налоги; экологические сборы; плата за негативное воздействие на окружающую среду; экологическая политика.

Svetlana E. Pavlyuchenkova
student of the Law Institute Russian University of Transport

Environmental taxation: realities in Russia and the experience of foreign countries

Abstract. The article analyzes environmental payments in the Russian Federation and foreign countries, in particular: payment for the negative impact on the environment, environmental and recycling fees, and draws conclusions: technological progress, involving almost all industries of the world's countries, has brought environmental problems from secondary to the rank of major, which in turn, it necessitated the introduction of new instruments for regulating these legal relations and the development of new mechanisms to improve environmental policy, including in the field of taxation.

Keywords: environmental taxes; environmental fees; payment for negative environmental impact; environmental policy.

На современном этапе вопросы экологии являются особенно актуальными, поскольку они касаются будущего всей нашей планеты.

Воздействие человека на окружающую среду в XXI в. достигло угрожающего уровня. Вырубка лесов, уничтожение биосферы, ассимилирующей солнечную энергию, варварская эксплуатация природных ископаемых, вредные выбросы и сбросы, отходы производства и потребления нарушают экологический и энергетический баланс нашей планеты и ведут к глобальному изменению климата на Земле, которое с каждым годом становится все ощутимее.

В связи с этим представляется необходимым вмешательство государства в эти процессы с целью эффективного регулирования экологических правоотношений и природоохранной деятельности. Одним из инструментов по регулированию данной деятельности является развитая система экологических налогов и сборов.

В России, в отличие от зарубежных стран, налоговое законодательство в области экологии не получило должного развития. В Налоговом кодексе и других федеральных законах не закреплено понятие «экологические налоги», что является следствием отсутствия широкой нормативно-правовой базы.

Статистической службой Европейского Союза разработано понятие, принятое странами Организации экономического сотрудничества и развития, в котором закреплен критерий отнесения того или иного платежа в разряд экологических налогов. Исходя из этого понятия, налоговая база должна иметь «доказанное специфическое влияние на окружающую среду», тогда соответствующие платежи будут считаться экологическими.

В налоговом законодательстве и правовой доктрине Российской Федерации можно встретить термины «природоресурсные налоги», «налоги, связанные с использованием природных ресурсов». Одним из таких налогов является налог на добычу полезных ископаемых, урегулированный гл. 26 НК РФ. Наряду с ним в российском законодательстве установлены другие налоги и сборы, связанные с использованием природных ресурсов — водный налог, земельный налог, сбор за пользование объектами животного мира. Перечисленные налоги и сборы, в первую очередь, несут фискальную и регулирующую функцию, в то время как за рубежом экологическое налогообложение используется в целях компенсации за вредное воздействие на окружающую среду и в качестве стимула для производств организовывать деятельность наиболее экологичным способом.

Федеральным законом от 10.01.2002 № 7-ФЗ «Об охране окружающей среды» (ст. 16), предусмотрено, что негативное воздействие на окружающую среду является платным. В России действует система экологических сборов и платежей. Так, плата за негативное воздействие на окружающую среду предусмотрена Федеральным законом «Об охране окружающей среды». Плату за негативное воздействие на окружающую среду перечисляют юридические лица и индивидуальные предприниматели, деятельность которых связана с выбросами в атмосферу и в водные объекты загрязняющих веществ или с хранением, захоронением отходов производства и потребления. Целью такого сбора является возмещение вреда, принесенного окружающей среде. Ставки сбора зависят от вида наносимого ущерба и от объема выделяемых загрязняющих веществ. При этом используют понижающие и повышающие коэффициенты, которые применяются при соблюдении или несоблюдении нормативов выбросов и лимитов на размещение отходов. Нормативы платы за различные виды негативного воздействия содержатся в постановлении Правительства от 03.03.2017 № 255 «Об исчислении и взимании платы за негативное воздействие на окружающую среду».

Требование утилизировать собственный товар и упаковку после их использования закреплено законодательством в 2015 г., Федеральным законом «Об отходах производства и потребления», в котором закреплено, что предприниматели обязаны собирать свою продукцию после использования и утилизировать собственными силами, а затем отчитываться перед Росприроднадзором. Однако такой вариант поведения не всегда реализуем. Поэтому для производителей и импортеров существует другая разновидность экологической отчетности за отходы от использования товаров — оплата экологического сбора. Экологический сбор закреплен нормами Федерального закона от 24.06.1998 № 89-ФЗ «Об отходах производства и потребления». Экологический сбор ежегодно платят производители и импортеры товаров и упаковки, которые не утилизируют образовавшиеся отходы самостоятельно.

Можно выделить три категории плательщиков экологического сбора:

— производители и импортеры товаров, подлежащих утилизации после утраты ими потребительских свойств;

— производители, использующие упаковку, подлежащую утилизации;

— импортеры, которые ввозят товары и упаковку, подлежащие утилизации.

При этом в случае, если товары и упаковка импортируются для собственных нужд без цели дальнейшей реализации, экологический сбор не уплачивается.

Ставка сбора формируется на основе средних сумм затрат на сбор, транспортировку и утилизацию единицы изделия с расчетом массы и количества утративших потребительские свойства товаров или упаковок. Нормативы утилизации устанавливаются распоряжением Правительства РФ от 31.12.2020 № 3722-р «Об утверждении нормативов утилизации отходов от использования товаров на 2021 м 2023 годы». Экологический сбор призван уменьшить количество отходов, которое поступает на захоронение, стимулируя производителей и импортеров уничтожать непригодные для использования товары и упаковку. Для предпринимателей, которые безответственно относятся к экологической отчетности, существует ряд санкций. Так, неуплата экологического сбора с 2021 г. наказывается административной ответственностью в виде штрафа в силу ст. 8.41.1. КоАП РФ. Сумма штрафа варьируется от 5000 —7000 руб. для должностных лиц, трехкратный размер неуплаченного сбора, но не менее 250 тыс. руб. — для индивидуальных предпринимателей и до трехкратного размера неуплаченного сбора, но не менее 500 тыс. руб. — для юридических лиц. По статистике за 2021 г. за иные правонарушения в области охраны окружающей среды и природопользования, предусмотренные гл. 8 КоАП РФ, рассмотрено 1047 дел и взыскано штрафов на сумму 16 431 руб., что составило 1,4% от общего числа дел касаемо правонарушений в области охраны окружающей среды и природопользования.

Одним из экологических сборов является также утилизационный сбор, взимаемый в России с 2012 г. Он распространяется на лиц, производящих и ввозящих на территорию России транспортные средства. Согласно ст. 24.1 Федерального закона «Об отходах производства и потребления» за каждое колесное транспортное средство, каждую самоходную машину, каждый прицеп к ним, ввозимые в Российскую Федерацию или произведенные, изготовленные в Российской Федерации, за исключением транспортных средств, указанных в п. 6 настоя-

щей статьи, уплачивается утилизационный сбор в целях обеспечения экологической безопасности, в том числе для защиты здоровья человека и окружающей среды от вредного воздействия эксплуатации транспортных средств, с учетом их технических характеристик и износа.

Цель утилизационного сбора — убрать с дороги старый небезопасный автотранспорт и дать стимул к покупке новых и более экологичных авто. За счет утилизационного сбора был налажен механизм утилизации старых автомобилей, модернизировались старые предприятия по переработке. Утилизационный сбор оплачивается единовременно, а его размер зависит от мощности и объема двигателя, грузоподъемности, категории и года выпуска авто.

Покупатели новых автомобилей не платят утилизационный сбор — это обязанность производителей и дилеров транспортных средств. Но все же есть лица, которые признаются плательщиками утилизационного сбора, в случае, если, авто было приобретено у льготной категории граждан или было самостоятельно ввезено на территорию России из-за рубежа.

Также к экологическим сборам можно отнести плату за пользование лесными ресурсами и водным объектом, сбор за участие в конкурсе (аукционе) на пользование недрами, разовые и регулярные платежи за пользование недрами.

На практике можно отметить, что данные экологические сборы слабо выполняют свою главную функцию — компенсацию причиненного вреда окружающей среде. Именно к такому выводу приходит Счетная палата РФ в своем отчете на 2017—2020 г. Фискальная и регулирующая функции экологических сборов имеют явный приоритет над обеспечением экологической безопасности.

Среди аудиторов также бытует мнение, что плата за негативное воздействие на окружающую среду также не компенсирует вреда природе, поскольку понижающие коэффициенты не стимулируют предприятия в должной мере проводить природоохранные мероприятия. Так, к 2021 г. из приблизительно 180 тыс. организаций и индивидуальных предпринимателей только 226 из них (0,13%) смогли воспользоваться нулевым коэффициентом при использовании наилучших доступных технологий.

Одной из проблем, касающейся реализации и эффективного функционирования экологического сбора, является то, что многие пред-

приятия не становятся на учет для его оплаты. Д. Буцаев, генеральный директор «Российского экологического оператора», отмечает, что в 2019 г. с бизнеса было собрано всего 3,7 млрд руб. в виде экологического сбора, тогда как население заплатило за вывоз отходов 193 млрд руб.

Счетная палата обращает внимание на два возможных варианта разрешения ситуации. Первый — усилить компенсационную функцию экологических неналоговых платежей, поскольку она слабо реализована на практике. Второй вариант — пересмотр подходов к установлению экологических неналоговых платежей и последующее включение их в НК РФ. Второй вариант возможен после комплексной реформы системы расширенной ответственности производителей и импортеров за утилизацию товаров и упаковки.

Зарубежные страны также сталкиваются с потребностью поиска таких инструментов, которые позволили бы минимизировать негативное воздействие на окружающую среду с наименьшими экономическими затратами. Наиболее удачным опытом в сфере экологического налогообложения является опыт Великобритании, которая активно разрабатывает национальное законодательство в области охраны окружающей среды, в том числе в части сохранения чистоты атмосферного воздуха и сокращения выбросов парниковых газов.

В настоящее время в Великобритании действуют такие экологические налоги, как налог на захоронение отходов, на изменение климата, на карьерные разработки и некоторые другие. Налог на захоронение отходов был введен в 1996 г. с целью снижения производства промышленных отходов и повышения интереса организаций к их эффективной утилизации. Налогом облагаются отходы, захораниваемые на официальных полигонах. Также для организаций, эксплуатирующих полигоны, предусмотрена система налоговых льгот, в соответствии с которыми они приобретают право на вычеты в случае вложения ими средств в проекты по сохранению окружающей среды.

Налог на изменение климата в Великобритании был введен с целью уменьшения выбросов парниковых газов в атмосферу. Налог взимается на все виды промышленного использования энергии. Нефтепродукты налогом не облагаются, поскольку они уже облагаются акцизом по достаточно высокой ставке. Практика взимания налога на изменение климата показала, что основным недостатком

данной процедуры является то, что налогообложению подлежат энергоносители, а не парниковые газы, тем самым, уровень снижения выбросов недостаточно высок. Подобная проблема была решена в Норвегии путем взимания налога на ископаемое топливо, т.е. государство берет плату за право выброса углекислого газа.

Налог на карьерные разработки взимается в Великобритании с 2002 г. и преследует цель снижения потребления сырья, добываемого карьерным методом, и материалов из него, а также стимулирование к использованию альтернативных материалов.

Отличительной чертой экологических налогов Великобритании является то, что они имеют целевое значение и используются строго на финансирование мероприятий по охране окружающей среды, в отличие от Российской Федерации, где экологические платежи используются по целевому назначению лишь в части. Опыт Великобритании, несмотря на существование недостатков, показывает комплексный и достаточно эффективный подход в вопросе применения финансовых инструментов экологической политики.

Еще одной страной, где введение экологических налогов наиболее актуально, является Китай, бурное и стремительное развитие которого наносит непоправимый ущерб для экологии. Экологическая ситуация в КНР — проблема для всего мира. Поэтому с 1 января 2018 г. на территории страны был введен экологический налог, заменивший сбор за загрязнение окружающей среды 1979 г. Налог ужесточил юридическую ответственность для плательщиков и увеличил число их обязанностей. Также были введены льготы и различные меры поддержки (например, на покупку очистных сооружений), что стимулирует развитие экологической безопасности экономической деятельности. От налога были освобождены владельцы очистных сооружений и предприятия по утилизации твердых отходов. Данные меры позволяют найти компромисс между сохранением темпов экономического развития и снижением негативного воздействия на экологию страны. При введении нового налога в Китае усилилась роль местных правительств, которые сами могут корректировать ставки и льготы исходя из экологической ситуации в регионе.

Проведенная китайскими законодателями реформа позволила повысить определенность правового регулирования и уровень гарантий прав участников налоговых правоотношений. Изучение результатов

введения экологического налога в Китае может быть полезным для российского законодателя.

Фундаментом для экологического законодательства в сфере налогообложения в Германии стали принципы предусмотрительности и «загрязнитель платит». Платежи побуждают предпринимателей к такому поведению, которое предотвращало бы возникновение экологических проблем. Налоговая реформа 1999 г. в Германии урегулировала производственные процесс и спрос на технологические инновации, повысив тем самым энергоэффективность производимых товаров.

Экологические налоги в Германии можно разделить на четыре группы:

— платежи за природопользование;

— финансирующие экологические платежи (финансируют доходную часть бюджета);

— выравнивающие платежи (применяются к лицам, причинившим вред окружающей среде, вместо компенсационных мероприятий);

— управляющие платежи (их цель — сокращение вредного воздействия на экологию, например, налог на минеральные масла).

Экологическая система налогов в Германии не статична, она эволюционирует, постоянно изменяются налоговые ставки, объекты налогообложения и методы взимания налогов, но теоретические основы при этом остаются неизменными. Таким образом, ее можно назвать устоявшейся и соответствующей постоянно изменяющейся реальности в сфере экологии.

Подводя итог, можно сказать о том, что загрязнение окружающей среды является одной из глобальных проблем всего человечества. Индустриальные страны, осознавая опасность, принимают меры по улучшению состояния экологии. Налогообложение играет немаловажную роль в экологической политике.

Современная действующая система экологических налогов и сборов в России является недостаточно эффективной, она не отвечает запрашиваемым условиям для устойчивого развития. Одним из недостатков существующей системы экологических платежей является ее нецелевое расходование. Основной целью экологического налогообложения должно стать формирование фонда для финансирования мероприятий, направленных на сохранение и восстановление окружающей среды. Пока что существующие экологические платежи в России

плохо справляются с функцией возмещения вреда окружающей среде и на практике имеют признаки экологических налогов. В связи с этим представляется возможным усилить компенсационную функцию сборов, либо внести данные платежи в Налоговый кодекс [1] и фактически сделать их налогами. Зарубежный опыт в сфере экологического налогообложения также может послужить подспорьем для отечественного законодателя.