ИНФОРМАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ТРАНСПОРТНОЙ ДЕЯТЕЛЬНОСТИ И ТРАНСПОРТНОЙ БЕЗОПАСНОСТИ

УДК 347.9

Быстрякова Светлана Анатольевна,
Акционерное общество «Нефтетранссервис»

Формирование государственной политики реализации национальных целей развития Российской Федерации в системе транспортной безопасности: публично-правовые вопросы цифрового оборота и защиты персональных данных граждан

Аннотация. Системные проблемы развития правового обеспечения информационной безопасности транспортного комплекса, как показывает исследование, сегодня приобретают приоритетный характер и стратегическое значение в связи с включением в критическую информационную инфраструктуру. Актуальность научных исследований определена в настоящее время и требованиями реализации стратегических целей национального развития, определенных Президентом РФ после вступления в должность 7 мая до 2024 г. Выполнение стратегических задач государственной политики, направленных на обеспечение приоритета прав и свобод человека, справедливости в социальной сфере и обеспечение равенства возможностей граждан, безопасности общества и государства, непосредственно связано с развитием транспорта, его мультипликацией практически со всеми сферами и отраслями, задачами достижения цифровой зрелости экономики России в сложных условиях дальнейшей цифровизации, санкционной агрессии и формирования многополярного мира. Укрепление государственного суверенитета России связано с обеспечением транспортной безопасности во всех его проявлениях для достижения требуемого уровня состояния защищенности. В условиях цифровой трансформации это напрямую связано с обеспечением информационной безопасности, защиты граждан от деструктивного информационного воздействия, формированием защиты цифрового оборота их персональных данных. Автором обоснована актуальность этой темы, учитывая стратегические задачи национального развития, включая связанные с разработкой и принятием обновленного блока национальных проектов в отношении развития инфраструктуры транспортной системы,

туризма, экономики данных и др. В связи с этим необходим научный анализ с позиции информационного права, а также на основе мониторинга правоприменения, состояния правового регулирования и развития процессов формирования межотраслевого института правового регулирования цифрового оборота персональных данных в системе транспортной безопасности.

Ключевые слова: информационная безопасность; транспортная безопасность; защита персональных данных; цифровой оборот персональных данных; трансграничность; идентификация субъектов.

Svetlana An. Bystryakova,
Joint Stock Company “Neftetransservis”

Formation of state policy for the implementation of national goals of the development of the Russian Federation in the transport security system: public and legal issues of digital circulation and protection of personal data of citizens

Abstract. At present systemic problems in the development of legal support for information security of the transport complex, as the current study shows, are of great priority and strategic importance due to their inclusion in the critical information infrastructure. The relevance of the study is currently determined by the requirements for the implementation of the strategic goals of national development, defined by the President of the Russian Federation after Inauguration on May 7, 2024. The implementation of strategic objectives of state policy which is aimed at prioritizing human rights and freedoms, justice in the social sphere and ensuring equality of citizens, society and state security, is directly related to the transport development, its multiplication with almost all spheres and industries, and the tasks of achieving digital maturity of the Russian economy in difficult conditions of further digitalization, sanctions aggression and the formation of a multipolar world. Strengthening the state sovereignty of Russia is associated with enforcing transport security in all its manifestations to achieve the required level of security. In the context of digital transformation, this is directly related to enforcing information security, protecting citizens from destructive information effect, and developing protection for the digital circulation of their personal data. There has been substantiated the relevance of this topic, considering the strategic objectives of national development, including those related to the development and adoption of an updated block of national projects on the development of transport system infrastructure, tourism, data economy, etc. In this regard, a scientific analysis is of great necessity according to information law, as well as

based on law enforcement monitoring, the state of legal regulation and the development of processes for the formation of an intersectoral institution of legal regulation of the digital circulation of personal data in the transport security system.

Keywords: information security; transport security; protection of personal data; digital circulation of personal data; cross-border; identification of subjects.

В условиях изменения мироустройства, усиления санкционной политики недружественных по отношению к России государств и в целях обеспечения устойчивого социального и экономического развития страны особую актуальность приобретают правовые вопросы обеспечения приоритетов национальной безопасности и укрепления национального суверенитета в контексте формирования высокого уровня технологической независимости Российской Федерации во всех областях экономики, развития экономики данных и системы государственного управления. В связи с этим следует особо выделить информационную безопасность как один из системообразующих факторов и стратегических векторов национальной безопасности. Несомненную важность и социальную значимость в настоящее время всеобщей цифровой трансформации приобретает информационное обеспечение транспортной безопасности и выработка системных научно обоснованных межотраслевых подходов в этой области [1].

Развитие национальной транспортной сферы при одновременном обеспечении ее информационной безопасности выступает одним из краеугольных камней достижения национальной безопасности России, поскольку транспортный комплекс — это огромная критическая информационная инфраструктура (далее — КИИ), которая постоянно масштабируется. Также нельзя недооценивать беспрецедентную территорию России и связанные с этим новые задачи в рамках поручения о разработке и утверждении целого блока новых национальных проектов, определенных в Указе Президента РФ от 7 мая 2024 г. № 309. В рамках этих проектов важное значение, кроме прочего, придается формированию единой системы пространственных данных. Следует также отметить, что предусмотрено принятие комплексного плана развития, в котором наряду с иными в центре внимания находится транспортная инфраструктура. Обращает внимание, что во многих действующих актах стратегического планирования в области безопасности, начиная с общих — Стратегии национальной безопасности Российской Федерации, Стратегии научно-технологического развития Российской Федерации, Доктрины информационной безопасности Российской Федерации и до специализированной Морской доктрины Российской Федерации, отмечается стратегическое значение обеспечения транспортной

безопасности, технологического развития отраслей экономики и цифровизации. В связи с этим, безусловно, важны вопросы научно-технологического развития и задачи достижения технологического суверенитета страны в транспортной сфере посредством повышения уровня связанности территории России, создания интеллектуальных транспортных средств, достижения лидерства в мире в отношении транспортно-логистических систем.

Между тем для организационно-правового обеспечения транспортной безопасности, включая защищенность транспортных средств и транспортной инфраструктуры, пассажиров и сотрудников транспортного комплекса согласно Федеральному закону от 9 февраля 2007 г. № 16-ФЗ «О транспортной безопасности» в ходе реализации Комплексной программы обеспечения безопасности населения на транспорте, утвержденной распоряжением Правительства РФ от 30 июля 2010 г. № 1285-р, разработана и используется единая государственная информационная система обеспечения транспортной безопасности (далее — ЕГИС ОТБ).

В 2018 г. традиционное мероприятие Минтранса России — «Транспортная неделя» прошла в ракурсе идей цифровой трансформации и ключевой темой множества докладов и обсуждений явилась цифровизация в транспортной сфере, в основе которой именно формирование ЕГИС ОТБ [URL: https://securityexp.ru/novyi-etap-razvitiia-egis-otb? (дата обращения: 11 мая 2024 г.)]. 1 сентября 2023 г. вступило в силу новое Положение об этой системе, утвержденное постановлением Правительства РФ от 1 августа 2023 г. № 1251.

Ключевой целью разработки и использования ЕГИС ОТБ является информационное обеспечение деятельности федеральных органов исполнительной власти для реализации установленных организационно-правовых, технических, экономических и иных мер в сфере функционирования всех видов транспорта. Это касается нейтрализации и противодействия возрастающим угрозам незаконного вмешательства в работу транспорта на территории России. Рассматриваемая система обеспечивает поддержку цифровыми данными выполнение полномочий Минтранса России, Росавиации, Росавтодора, Росжелдора, Росморречфлота, Ространснадзора и иных уполномоченных организаций. В рамках межведомственного взаимодействия производится информационное обеспечение деятельности субъектов транспортной безопасности, включая ФСБ России и МВД России.

Совокупность цифровых данных, включенных в рассматриваемую систему, согласно действующему законодательству, является государственным информационным ресурсом, а сама система — централизованной, территориально-распределенной государственной системой и объектом КИИ. В цифровые системы персональных данных входят данные о пассажирах, персонале и экипажах средств транспорта,

используемых при решении определяемых государством задач безопасности функционирования транспортного комплекса.

Государственные услуги в области транспортной безопасности в цифровом формате реализуются на основе использования уполномоченными органами инфраструктуры ЕГИС ОТБ в соответствии с правовым регулированием, включающим и вопросы обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе [2]. Переход от так называемой «бумаги» к «цифре» позволил транспортной отрасли и ее составляющей транспортной безопасности сократить не только финансовые, но и временные затраты на совершение юридически значимых действий. Важно отметить, что начиная с 2022 г. сервис для заявителей стал доступен на портале Госуслуг [3].

Разработчиком ЕГИС ОТБ выступило ФГУП «ЗащитаИнфоТранс», подведомственное Минтрансу России, которое осуществляет его эксплуатацию на всех этапах жизненного цикла. Условия и порядок осуществления доступа к цифровым данным системы определяются ст. 11 Федерального закона «О транспортной безопасности» и приказом Минтранса России от 2 мая 2024 г. № 162 «Об утверждении порядка формирования и ведения автоматизированных централизованных баз персональных данных о пассажирах и персонале (экипаже) транспортных средств, а также срока хранения и порядка предоставления содержащихся в них данных». Вместе с тем порядок создания, ведения и доступа заинтересованных лиц к ЕГИС ОТБ регламентируется целой совокупностью нормативных правовых и иных актов, в том числе: Федеральными законами «Об информации, информационных технологиях и о защите информации», «Об обеспечении безопасности критической информационной инфраструктуры Российской Федерации», «О персональных данных» и др.

В Положении о единой государственной информационной системе обеспечения транспортной безопасности определены цель, задачи, принципы функционирования, структура, состав ресурсов и подсистем, а также закреплены полномочия участников информационного взаимодействия, и что важно подчеркнуть, предусмотрены общие требования к защите информации, включая персональные данные.

В рамках данной статьи заслуживает отдельного внимания вопрос об обороте цифровых данных о гражданах и его правовом обеспечении в целях защищенности. Объем персональных данных россиян, передаваемых в ЕГИС ОТБ, возрастает в прогрессии, что требует выработки новых научно обоснованных подходов к актуальным вопросам обеспечения информационной безопасности и цифрового оборота персональных данных граждан России в системе транспортной безопасности [4, стр. 252; 5, стр. 166]. При этом вышеназванная государственная автоматизированная система уже сегодня включает в

себя множество централизованно обрабатываемых баз персональных данных пассажиров и персонала (экипажа) средств различных видов транспорта. Однако наблюдается тенденция увеличения в ближайшие три года объема обрабатываемых данных. Вместо 6 видов данных планируется обрабатывать 22. Наряду с этим виды дополнительных цифровых данных пассажиров, планируемых для передачи и обработки в рассматриваемую информационную систему, Минтрансом России пока не раскрывается. Это закреплено в паспорте ведомственной программы цифровой трансформации на 2024 г. и плановый период 2025-2026 гг. Минтранса России, который размещен в Федеральной государственной информационной системе координации информатизации [URL: https://www.pnp.ru/social/fsb-i-mvd-uznayut-o-passazhirakh-vsyo.html (дата обращения: 12 мая 2024 г.)].

Согласно новому порядку, утвержденному приказом Минтранса России от 2 мая 2024 г. № 162, помимо традиционных данных паспорта и билета пассажиров планируется обязать перевозчиков передавать в единую базу цифровые данные, указанные гражданином при бронировании и покупке билета, включая *PNR* (*Passenger Name Records*) — специальный цифровой код, присутствующий на билете после бронирования (включает номер телефона, адрес электронной почты, сведения о билете), который должен проверить подлинность билета и получить сервисы регистрации и получения посадочного талона, а также возврата или обмена.

Дополнительно предлагается аккумулировать цифровые данные учетной записи пользователя сайта или приложения перевозчика (логин и пароль), IP-адрес и номер порта, с которого передавалась информация. При оплате бронирования или покупке билета банковской картой планируется, что перевозчик должен передать четыре последние цифры карты и данные банка, а также стоимость приобретаемого билета и класс обслуживания, выбранный пассажиром. Ранее они должны были вносить лишь паспортные данные, дату поездки и маршрут. Указанные данные будут храниться семь лет. Одновременно отмечается, что все указанные сведения должны передаваться перевозчиками воздушного, водного и железнодорожного транспорта, а также автотранспорта на междугородном и международном сообщении за некоторыми исключениями. Перечисленные персональные данные в цифровой форме в соответствии с проектом должны поступать в ЕГИС ОТБ.

Необходимо обратить внимание на различные дискуссионные точки зрения о внесении указанных изменений. Так, Ассоциацией эксплуатантов воздушного транспорта (далее — АЭВТ) указывается, что определенная часть дополнительных данных о пассажирах, планируемых к обработке в ЕГИС ОТБ (в частности логин и пароль учетной записи пользователя), являются «сведениями конфиденциального характера, в связи с чем не подлежат раскрытию без согласия субъекта таких данных» [URL: https://www.kommersant.ru/doc/6531303 (дата обращения: 11 мая 2024

г.)]. Кроме того, передача данных цифрового кода *PNR* в течение нескольких минут после завершения регистрируемой операции с проездными билетами «не соответствует установленным стандартам и рекомендациям ИКАО и является труднореализуемой задачей как для российских, так и иностранных перевозчиков, использующих различные системы бронирования». Также АЭВТ отмечает, что обработка таких цифровых данных осуществляется в соответствии с международным стандартом ИКАО (Doc 9944) «Рекомендации в отношении записей регистрации пассажиров (*PNR*)», предписывающей «не требовать от эксплуатанта возлагать на него ответственность за предоставление данных *PNR*» [URL: https://www.kommersant.ru/doc/6531303 (дата обращения: 11 мая 2024 г.)].

Вместе с тем обращено внимание, что действующее законодательство не обязывает перевозчиков или уполномоченных агентов на этапе бронирования получать у пассажира данные документа, удостоверяющего личность, что определяет вопрос о целесообразности указанной обработки в целях защиты прав пассажиров. Увеличение массива обрабатываемых цифровых данных формирует новые информационные угрозы и риски большей уязвимости субъектов персональных данных и информационных систем, а также требует принятия дополнительных средств защиты, увеличивая нагрузку на оператора [6]. Как справедливо отмечают специалисты авиакомпаний, «чем больше информации собирается, тем больше может быть негативных последствий в случае утечки» [URL: https://www.kommersant.ru/doc/6531303 (дата обращения: 11 мая 2024 г.)]. Это влияет на важность обсуждения и научного обоснования вопроса о достаточности либо избыточности информации, планируемой к обработке, информационных рисках в этой области и соотношении принимаемых решений с ценностными ориентирами правовой защиты персональных данных граждан [7; 8].

Заместитель Председателя Комитета Государственной Думы Федерального Собрания РФ по информационной политике, информационным технологиям и связи А. Горелкин в своем аккаунте указал, что не сомневается в уровне защиты ЕГИС ОТБ, что он превышает многие системы бронирования. Однако следует признать избыточным набор персональных данных для предоставления в систему Минтранса России. «Например, пароль для доступа в личный кабинет пользователя. Не понимаю, как его раскрытие поможет обеспечить безопасность пассажиров. Наоборот, это создаст дополнительные риски, ведь перевозчики будут вынуждены прекратить шифровать пользовательские пароли. Хакеры скажут “спасибо”», — констатировал А. Горелкин [URL: https://www.pnp.ru/social/fsb-i-mvd-uznayut-o-passazhirakh-vsyo.html (дата обращения: 12 мая 2024 г.)]. Кроме того, следует отметить, что избыточный сбор данных не соответствует основным принципам законодательства о персональных данных и нарушает права и свободы

граждан [6], а также размывает формирование концептуальных положений правового обеспечения защиты данных цифровых сервисов [9].

Вызывает интерес и вопрос в отношении использования персональных данных при рейсовых автобусных перевозках, при котором через информационно-телекоммуникационную сеть Интернет оформляется около 10—15% проездных документов, что отмечается директором «Объединения автопассажирских перевозчиков» Т. Ракуловой. Верификация банковских карт пассажиров при безналичном расчете за билеты создаст дополнительные сложности для организаций перевозчиков. Она отмечает, цифровизация в этой области и сбор персональных данных пассажиров успешно внедряются в международной практике, однако увеличение круга обрабатываемых данных сегодня «опережает ситуацию на российском рынке перевозок» [URL: https://www.kommersant.ru/doc/6531303 (дата обращения: 11 мая 2024 г.)].

Вместе с тем благодаря предполагаемым нововведениям заинтересованные государственные ведомства имеют возможность получать уведомления о паспорте обеспечения транспортной безопасности транспортного средства в электронном виде, сведения о категорированных объектах транспортной инфраструктуры и транспортных средствах, а также записи о пассажирских перевозках по всем видам транспорта в ЕГИС ОТБ.

Рассмотренное позволяет сделать ряд выводов. Как показывает исследование, вопросам организационно-правового обеспечения информационной безопасности при обороте цифровых персональных данных, особенно в условиях современной трансграничности транспортного комплекса, уделяется специалистами и исследователями значительное внимание. Отмечается тенденция увеличения массива сбора и обработки персональных данных в целях обеспечения транспортной безопасности. Предполагается, что таким образом увеличится вероятность выявления пассажиров, представляющих опасность для транспортного комплекса, в целях противодействия нарушениям на транспорте и повышения антитеррористической защищенности. При этом, по мнению специалистов, обычные граждане не испытают неудобств и не почувствуют разницы, так как все собираемые данные будут также храниться в надежно защищенной системе — ЕГИС ОТБ, которая постоянно совершенствуется.

Для перевозчиков возможны риски наложения на них новых расходов (штрафы за утечку информации, а также необходимость «перестройки» внутренних процессов), обязанностей и ответственности за сбор и передачу дополнительных сведений. При этом вопрос обеспечения безопасной передачи всех необходимых данных граждан в государственную систему без допущения утечек является

первоочередным, требующим дальнейших научных исследований и внимания при формировании государственной политики и правоприменении.

Литература

1. Трансформация информационного права : монография / ответственные редакторы Т. А. Полякова, А. В. Минбалеев, В. Б. Наумов. — Москва : Институт государства и права РАН, 2023.
2. Модели правового регулирования обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе: монография / под общей редакцией Т. А. Поляковой. — Саратов : Амирит, 2020.
3. Чеботарева, А. А. Этапы формирования новой модели управления цифровой трансформации транспортных предприятий / А. А. Чеботарева, Е. И. Данилина // Бизнес. Образование. Право. — 2024. — № 1 (66). — С. 46—52.
4. Бойченко, И. С. Цифровая трансформация и новеллы в правовом регулировании, направленные на защиту персональных данных в Российской Федерации / И. С. Бойченко, С. А. Быстрякова // Новые горизонты развития системы информационного права в условиях цифровой трансформации : монография / ответственные редакторы Т. А. Полякова, А. В. Минбалеев, В. Б. Наумов. — Москва : ИГП РАН, 2022.
5. Быстрякова, С. А. Биометрические персональные данные: правовые проблемы и организационно-правовые риски / С. А. Быстрякова, В. С. Буланова // Шестые Бачиловские чтения: сборник статей участников Международной научно-практической конференции / ответственные редакторы Т. А. Полякова, А. В. Минбалеев, В. Б. Наумов. — Москва, 2023.
6. Правовое регулирование оборота персональных данных в условиях современных вызовов и угроз: монография / под ред. А. М. Минбалеева. — Саратов: ООО «Амирит», 2023. — 138 с.
7. Камалова, Г. Г. Информационно-правовые риски / Г. Г. Камалова // Цифровые технологии и право : сборник научных трудов I Международной научно-практической конференции : в 6 томах / под редакцией И. Р. Бегишева [и др.]. — Казань, 2022.
8. Полякова, Т. А. Ценностные изменения развития информационного права России / Т. А. Полякова, Г. Г. Камалова // Правовое государство: теория и практика. — 2023. — № 2 (72). — С. 53—59.
9. Камалова, Г. Г. Вопросы правого обеспечения информационной безопасности в контексте развития цифровых сервисов / Г. Г. Камалова // Информационное право. — 2022. — № 4 (74). — С. 38—40.

References

1. Transformatsiya informatsionnogo prava : monografiya [Transformation of information law] / otvetstvennyye redaktory T. A. Polyakova, A. V. Minbaleyev, V. B. Naumov. — Moskva : Institut gosudarstva I prava RAN, 2023.
2. Modeli pravovogo regulirovaniya obespecheniya informatsionnoy bezopasnosti v usloviyakh bol’shikh vyzovov v global’nom informatsionnom obshchestve: monografiya [Models of legal regulation of ensuring information security in the face of great challenges in the global information society] / pod obshchey redaktsiyey T. A. Polyakovoy. — Saratov : Amirit, 2020.
3. Chebotareva, A. A. Etapy formirovaniya novoy modeli upravleniya tsifrovoy transformatsii transportnykh predpriyatiy [Stages of formation of a new model for

managing the digital transformation of transport enterprises] / A. A. Chebotareva, Ye. I. Danilina // Biznes. Obrazovaniye. Pravo. — 2024. — № 1 (66). — S. 46—52.
4. Boychenko, I. S. Tsifrovaya transformatsiya I novelly v pravovom regulirovanii, napravlennyye na zashchitu personal'nykh dannykh v Rossiyskoy Federatsii [Digital transformation and innovations in legal regulation aimed at protecting personal data in the Russian Federation] / I. S. Boychenko, S. A. Bystryakova // Novyye gorizonty razvitiya sistemy informatsionnogo prava v usloviyakh tsifrovoy transformatsii : monografiya / otvetstvennyye redaktory T. A. Polyakova, A. V. Minbaleyev, V. B. Naumov. — Moskva : IGP RAN, 2022.
5. Bystryakova, S. A. Biometricheskiye personal'nyye dannyye: pravovyye 73arvo73m I organizatsionno-pravovyye riski [Biometric personal data: legal problems and organizational and legal risks] / S. A. Bystryakova, V. S. Bulanova // Shestyye Bachilovskiye chteniya: sbornik statey uchastnikov Mezhdunarodnoy nauchno-prakticheskoy konferentsii / otvetstvennyye redaktory T. A. Polyakova, A. V. Minbaleyev, V. B. Naumov. — Moskva, 2023.
6. Pravovoye regulirovaniye oborota personal'nykh dannykh v usloviyakh sovremennykh vyzovov I ugroz: monografiya [Legal regulation of the circulation of personal data in the context of modern challenges and threats] / pod red. A. M. Minbaleyeva. — Saratov: OOO «Amirit», 2023. — 138 s.
7. Kamalova, G. G. Informatsionno-pravovyye riski [Information and legal risks] / G. G. Kamalova // Tsifrovyye tekhnologii I 73arvo : sbornik nauchnykh trudov I Mezhdunarodnoy nauchno-prakticheskoy konferentsii : v 6 tomakh / pod redaktsiyey I. R. Begisheva [I dr.]. — Kazan', 2022.
8. Polyakova, T. A. Tsennostnyye izmeneniya razvitiya informatsionnogo prava Rossii [Value changes in the development of information law in Russia] / T. A. Polyakova, G. G. Kamalova // Pravovoye gosudarstvo: teoriya I praktika. — 2023. — № 2 (72). — S. 53—59.
9. Kamalova, G. G. Voprosy pravogo obespecheniya informatsionnoy bezopasnosti v kontekste razvitiya tsifrovykh servisov [Issues of legal support of information security in the context of the development of digital services] / G. G. Kamalova // Informatsionnoye 73arvo. — 2022. — № 4 (74). — S. 38—40.