4. Несмелов Сергей. Выступление Андрей Курпатов в Давосе на бизнес-завтраке Сбербанка // Видеохостинг «YouTube». URL: //https: youtube.com (дата обращения: 23.11.2019).

5. Рудычева Н. Цифровизацию транспорта тормозит отсутствие стандартов и экономической целесообразности // Интернет-портал о высоких технологиях Cnews.ru. URL: https://www.cnews.ru/reviews/it_v_transportnoj_otrasli_2019/articles/tsifrovizatsiyu_transporta_tormozit_otsutstvie_standartov_i_ekonomicheskoj (дата обращения: 16.10.2019).

6. Никитин В. В. Проблемы выбора методологии при научном анализе труда // Актуальные проблемы теории и истории права и государства на современном этапе : сб. тр. V11 Междунар. науч.-практ. конф. Кострома : КГУ, 2010. С. 62–66.

7. Передельский Денис. Стивен Хокинг рассказал о страшном сценарии будущего // Российская газета. 21.10.2016.

8. Правовое регулирование экономических отношений в современных условиях развития цифровой экономики. М. : Юстицинформ, 2019, 376 с.

9. Северин В. А. Принципы регулирования информационных отношений в инновационной экономике // Коммерческое право. 2017. № 2(25). С. 9.

10. Стрельцов А. А. Содержание информационных отношений // Теоретические проблемы информационного права / Институт государства и права российской академии наук. М., 2006. С. 28–37.

УДК 33

Рубцова Майя Викторовна,
научно-исследовательский институт
Университета прокуратуры Российской Федерации,
г. Москва, Российская Федерация
majya-rubcova@yandex.ru

Цифровые технологии в транспортной сфере: проблемы, перспективы

Статья посвящена вопросам использования современных цифровых технологий в транспортной сфере, правовым отношениям, связанным с транспортным комплексом, единой системы контроля в Российской Федерации, государственным автоматизированным информационным системам, проблемам и перспективам в данной сфере.

Ключевые слова: *цифровые технологии, транспортная сфера, система контроля, правовые отношения, национальный проект, авиакомпании, законодательство, проблема* кибератак в транспортной сфере, транспортная безопасность.

Rubtsova Maya Viktorovna,
Research Institute of the University of the Prosecutor's office
of the Russian Federation,
Moscow, Russian Federation

Digital technologies in the transport sector: problems, prospects

The article is devoted to the use of modern digital technologies in the transport sector, legal relations related to the transport complex, the unified control system in the Russian Federation, state automated information systems, problems and prospects in this area.

Keywords: *digital technologies, transport sphere, control system, legal relations, national project, airlines, legislation, the problem of cyberattacks in the transport sphere, transport security.*

На сегодняшний день рынок транспортных услуг один из самых динамично развивающихся в мире. От эффективности функционирования транспортных сетей зависит продуктивность работы других отраслей промышленности, следовательно, и экономического благосостояния страны.

Одним из самых перспективных направлений развития цифровых сервисов для транспортной отрасли являются геоинформационные технологии. Это не только мониторинг движения транспорта, но и оснащение контейнеров и прицепов датчиками, которые измеряют параметры внешней среды и груза, считывают информацию с окружающих объектов и передают ее в единый центр для онлайн-анализа и контроля процесса доставки. Объем рынка геосервисов в России, по оценкам экспертов, составляет около 6 млрд долл. [1].

Транспорт нуждается в самых современных цифровых технологиях, чтобы оставаться конкурентоспособным на мировом рынке, обеспечивать потребность в перевозках возрастающих объемов пассажиров и грузов, обеспечивать доступность и качество оказываемых услуг. Первоочередные задачи, обозначенные в послании Президента России, в майском указе, расшифрованные в комплексном плане магистральной инфраструктуры, требуют широкого применения цифровых технологий. Такие технологии будут на новом уровне обеспечивать проектирование, строительство и эксплуатацию объектов инфраструктуры, а также процессы мониторинга и управления проектной деятельностью. В транспортном комплексе реализуется целый ряд масштабных проектов по созданию информационных систем нового поколения. Создана и функционирует государственная автоматизированная информационная система «ЭРА-ГЛОНАСС», внедрена и эффективно используется система «Платон». На их основе развиваются необходимые транспортному комплексу сервисы, которые не связаны на-

прямую с взиманием платы с большегрузных автомобилей. Эти системы позволяют собирать и сохранять большие данные. Для формирования доверенного пространства взаимодействия всех участников отрасли предстоит сформировать цифровую платформу транспортного комплекса, которая объединит все перечисленные сервисы и массивы данных и станет своего рода экосистемой для всех участников транспортного процесса. Фактически на основе отечественного программного обеспечения будет создано «единое окно» государства и бизнеса при выполнении всех перевозок. Эта платформа установит единые стандарты, правила и регламенты информационного обмена, в том числе юридически значимые данные о транспортной инфраструктуре и транспортных средствах. Платформа выступит в качестве агрегатора данных о транспорте, который исключает приватизацию этих данных и гарантирует недискриминационный доступ к ним всех заинтересованных участников транспортной отрасли. Наконец, эта платформа позволит сохранить национальный суверенитет над информационными потоками в транспортном комплексе страны. Все перечисленные направления нашли отражение в ведомственном проекте «Цифровой транспорт и логистика». Имеющийся фундамент, заложенный ФГУП «ЗащитаИнфоТранс» в части учета и регистрации беспилотные авиационные системы (БАС), уже позволил начать создание единой системы контроля в Российской Федерации. Единая система контроля БАС должна включать в себя весь сквозной процесс, начиная от учета, регистрации и переходя к обучению и созданию клиентоориентированных интерфейсов, наблюдению, планированию, обеспечению безопасности транспортной и критической инфраструктуры в связи с деятельностью БАС, а также взаимодействию с заинтересованными ведомствами по транспортной, информационной и кибербезопасности, в том числе с использованием единой государственной информационной системы объектов транспортной безопасности. На текущий момент Российская Федерация в лице предприятий и специализированных организаций в полной мере располагает техническими возможностями для построения единого процесса наблюдения за БАС. С опорой на собственные ресурсы создан серьезный задел, технологический и интеллектуальный, что позволяет уже в ближайшее время добиться значительного прогресса в вопросе контроля. Госкорпорация по ОрВД является национальным провайдером аэронавигационного обслуживания в Российской Федерации и осознает необходимость решения в данном контексте целого ряда задач технического характера. При этом располагает для этого интеллектуальными и финансовыми возможностями. Наличие у предприятия собственного учебного заведения позволяет обеспечивать должный уровень подготовки всех категорий персонала, что является одним из необходимых условий для безопасной эксплуатации. Таким образом, предлагается создание единой системы контроля за БАС, беспилотными воздушными судами (БВС) путем формирования единого опера-

тора на основе государственно-частного партнерства за счет собственных средств госкорпорации и за счет привлечения инвестиций и инфраструктурных инвесторов [2].

На сегодняшний день уровень развития цифровых технологий в Аэрофлоте остается одним из самых высоких в мировой транспортной отрасли. Авиакомпания в течение нескольких лет сохраняет 4-е место в мире среди авиакомпаний по цифровизации в рейтинге консалтинговой компании Bain & Co. На практике – это более десятка реализованных бизнес-кейсов на базе современных цифровых технологий. Программа «Интернет на борту», которая реализована на широкофюзеляжных воздушных судах и сейчас распространяется на узкофюзеляжный флот. Система Монитор руководителя, предоставляющая менеджерам Аэрофлота онлайн-доступ к более чем 500 показателям деятельности компании. Оснащение бортпроводников и пилотов планшетами, которые позволяют полностью и детально видеть свое поле работы. Впервые осуществленный в России цифровой проект «Витрина данных налогового мониторинга», не уступающий лучшим западным образцам. Система управления ресурсами, которая сократила среднее время обслуживания самолета между прилетом и вылетом. Система интеллектуальной поддержки эксплуатации воздушных судов, позволившая повысить среднесуточный налет лайнеров «Аэрофлота». Автоматизация основных бизнес-процессов – от офисной работы до обслуживания пассажиров и самолетов уже достигла в компании 100%. В планах дальнейшие разработки в области искусственного интеллекта, которые включены в обновленную стратегию развития Группы «Аэрофлот» до 2023 года [3].

Для транспорта актуальна проблема кибербезопасности. Как известно, в законодательстве отсутствует понятие «кибербезопасность», однако киберпространство – реальность, затрагивающая все сферы деятельности человека, в том числе транспортную. В Федеральном законе от 09.02.2007№ 16-ФЗ «О транспортной безопасности» употребляется только термин «кибербезопасность» без его раскрытия по содержанию. В настоящее время вопросы кибербезопасности становятся одними из основных в общей структуре безопасности транспортного сектора. Широкое внедрение компьютерных технологий для автоматизированного и автоматического управления техническими объектами и технологическими процессами, а также глубокая интегрированность программно-аппаратных комплексов в информационно-коммуникационные сети передачи данных дают возможность злоумышленникам обнаруживать их слабые стороны и активно пользоваться ими. Одним из основных требований к транспортной инфраструктуре любого государства является способность противостоять любым видам преступных посягательств. В случае России это приобретает особое значение, учитывая протяженность ее территории и транспортных коммуникаций (так протяженность железнодорожных путей в России составляет око-

ло 85 тыс. км. – второе место после США). Сегодня вопрос кибербезопасности транспортного сектора – это вопрос национальной *безопасности страны.*

Следует отметить, что бурное развитие транспортного комплекса России ставит новые задачи, связанные с обеспечением транспортной безопасности. Постоянно растет уровень внутренних перевозок на всех видах транспорта. Кроме того, появляются задачи глобального масштаба, продиктованные ростом роли России как транспортного коридора между Европой и Азией, это касается в первую очередь железнодорожных путей и Северного морского пути. В этих условиях повышение значимости информационных технологий в процессах управления неизбежно и продиктовано необходимостью решать новые задачи эффективно, оперативно и с минимальными затратами. Однако стоит отметить, что протяженность территории России это не только преимущество. Этот фактор делает транспорт одним из самых уязвимых точек в системе глобальной безопасности государства и требует создания сложных систем управления инфраструктурой. И с развитием и внедрением новейших информационных систем, с созданием в российских городах интеллектуальных систем управления транспортными потоками уровень опасности возрастает многократно. Объектами кибератак в транспортной сфере могут стать бортовые программно-аппаратные системы управления, системы управления полетами или движением поездов, системы навигации, системы железнодорожной автоматики, телемеханики и электроснабжения, объекты инфраструктуры вокзалов, портов и аэропортов. Целью кибератак может являться кибершпионаж (несанкционированная передача данных, программ или географических координат объектов транспорта и инфраструктуры посредством скрытых каналов связи) или кибераудит (поиск киберуязвимостей в системах управления, разработка сценариев кибератак). Гораздо большую опасность представляет киберсаботаж (снижение пропускной способности железнодорожных участков и аэропортов, вплоть до полной остановки движения) и кибердиверсии (физическое уничтожение аппаратуры, перехват управления транспортным средством, создание опасных маршрутов движения, нарушение технологий транспортировки и скоростного режима, в первую очередь при перевозке особо опасных и социально значимых грузов и пассажиров). Угроза может исходить как от анонимных злоумышленников (хакеров), так и от организованных преступных и экстремистских группировки, а также спецслужб других государств. Следует отметить, что стопроцентной защиты от киберугроз не существует. Сегодня возникает потребность в создании архитектуры безопасности не только объектов, но и целых городов и регионов, неотъемлемой частью которой является транспорт. Для достижения этой цели необходимо создание комплексных систем обеспечения безопасности (КСОБ). Прежде всего, была разработана общая модель угроз и частные модели угроз для каждого объекта, которые позволяли определить актуальные угрозы для каждого объ-

екта, а также мотивировали необходимость применение тех или иных средств мониторинга и защиты транспортной инфраструктуры и транспортных средств. КСОБ была реализована как сигнальная система на основе созданных объектовых технических систем и совокупности аналитических моделей, автоматизирующих процессы выявления событий безопасности. Система также осуществляла обработку информации персонального характера о сотрудниках транспортной инфраструктуры, сотрудниках подрядчиков и потребителях ее услуг. Наконец, КСОБ обеспечивала собственную безопасность в части информационно-телекоммуникационной среды и системы управления этой средой. В целом – это был первый в России уникальный опыт, и уверен, он будет обязательно востребован в будущем в любых уголках нашей страны [4].

Библиографический список

1. Струкалев М. Ю. Цифровизация транспортной отрасли // Офиц. сайт ИД «Коммерсантъ». URL: https://www.kommersant.ru/conference/377 (дата обращения: 16.10.2019).

2. Медведев Д. А. О цифровой трансформации транспортного комплекса // Офиц. сайт Правительства РФ. URL: http://government.ru/news/34821 (дата обращения: 16.10.2019).

3. Семенов А. К. Аэрофлот стал членом ассоциации «Цифровой транспорт и логистика» // Офиц. сайт ИД «Коммерсантъ». URL: https://www.kommersant.ru/doc/4061406 (дата обращения: 16.10.2019).

4. Родионов Д. Н. Киберугрозы и прочие современные вызов // Офиц. сайт Фонда транспортной безопасности. URL: https://tb-inform.ru/kiberugrozy-i-prochie-sovremennye-vyzovy/ (дата обращения: 16.10.2019).