Государственное и муниципальное управление. Ученые записки. 2023. № 2. С. 115–127
State and Municipal Management. Scholar Notes. 2023;(2):115–127

Проблемы экономики

Научная статья
УДК 351.741
doi: 10.22394/2079-1690-2023-1-2-115-127

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ СИСТЕМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Елена Валерьевна Лобкова[1], Алина Александровна Ки-Юан[2]

[1]Сибирский федеральный университет, Красноярск, Россия, elenavalerin@yandex.ru, https://orcid.org/0000-0003-2804-3427

[2]ООО «МФЦ Полюс», Красноярск, Россия, kiyuan@inbox.ru, https://orcid.org/0000-0001-9897-9082

Аннотация. Авторами рассмотрены вопросы и проблемы цифровизации систем обеспечения безопасности в разных сферах: общественной, транспортной, информационной. Проведено исследование проектов цифровой трансформации систем безопасности субъектов Российской Федерации с акцентом на группировке регионов по уровню активности в области разработки и внедрения указанных проектов. Представлен обзор региональных практик систем управления и обеспечения безопасности населения, информационных систем, транспортных систем, городской среды. На примере Красноярского края показаны процессы цифровой трансформации сферы безопасности, ее проблемы и перспективы. Определены факторы, препятствующие достижению целей проектов цифровой трансформации отрасли «Безопасность» субъектов Российской Федерации. Выявлены конкурентные преимущества и социально-экономические эффекты цифровой трансформации сферы обеспечения безопасности.

Ключевые слова: проект цифровой трансформации, система обеспечения, общественная безопасность, информационная безопасность, интеллектуальная среда, органы исполнительной власти, государственные и муниципальные услуги, чрезвычайная ситуация, цифровизация

Финансирование: Исследование выполнено в рамках реализации проекта № 2022030908431 «Разработка методики оценки эффективности реализации стратегических направлений цифровой трансформации ключевых отраслей экономики, социальной сферы и государственного управления субъектов Российской Федерации (на примере Красноярского края)», поддержанного Красноярским краевым фондом поддержки научной и научно-технической деятельности в рамках регионального конкурса «Конкурс проектов прикладных научных исследований и инновационных разработок в интересах развития Красноярского края» по приоритетным темам, представленным органами государственной власти и местного самоуправления Красноярского края.

Для цитирования: Лобкова Е. В., Ки-Юан А. А. Цифровая трансформация систем обеспечения безопасности // Государственное и муниципальное управление. Ученые записки. 2023. № 2. С. 115–127. https://doi.org/10.22394/2079-1690-2023-1-2-115-127

Problems of Economics

Original article

DIGITAL TRANSFORMATION OF SECURITY SYSTEMS

Elena V. Lobkova[1], Alina A. Ki-Yuan[2]

[1]Siberian Federal University, Krasnoyarsk, Russia, elenavalerin@yandex.ru, https://orcid.org/0000-0003-2804-3427

[2] LLC «MFC POLYUS» (Multifunctional Center Polyus Limited Liability Company), Krasnoyarsk, Russia, kiyuan@inbox.ru, https://orcid.org/0000-0001-9897-9082

Abstract. The authors considered the issues and problems of digitalization of security systems in various areas: public, transport, information. Research has been carried out of projects for the digital transformation of the security systems of the constituent entities of the Russian Federation with an emphasis on grouping regions according to the level of activity in the development and implementation of these projects. This report provides an overview of regional practices of management systems

© Лобкова Е. В., Ки-Юан А. А., 2023

and ensuring the safety of the population, information systems, transport systems, and the urban environment. The example of Krasnoyarsk Krai shows the processes of digital transformation of the security sphere, its problems and prospects. The factors that hinder achievement of goals of projects of digital transformation of industry «Security» of subjects of the Russian Federation have been determined. It reveals competitive advantages and socio-economic effects of digital transformation.

Keywords: digital transformation project, support system, public security, information security, intellectual environment, executive authorities, state and municipal services, emergency situation, digitalization

Financial Support: The study was carried out as part of the implementation of the project 2022030908431 «Development of methods of assessment of effectiveness of realization of strategic directions of digital transformation of key sectors of economy, social sphere and state administration of subjects of the Russian Federation (on example of the Krasnoyarsk region)»supported by the Krasnoyarsk Regional Fund for Support of Scientific and Scientific and Technical Activities in the Regional Competition «Projects of Applied Scientific Research and Innovative Development for the Development of the Krasnoyarsk Region» on priority topics, represented by the bodies of state power and local self-government of the Krasnoyarsk Krai.

For citation: Lobkova E. V., Ki-Yuan A. A. Digital transformation of security systems. *State and Municipal Management. Scholar Notes.* 2023;(2):115-127. (In Russ.). https://doi.org/10.22394/2079-1690-2023-1-2-115-127

Актуальность

Среди национальных целей развития Российской Федерации до 2030 г., утвержденных Указом Президента Российской Федерации от 21.07.2020 г. № 474, на особом месте находится цель сохранения здоровья и благополучия населения, обеспечение комфортной и безопасной среды для жизни. Стратегия развития информационного общества в Российской Федерации на 2017–2030 гг. диктует внедрение цифровых технологий и инструментов в управленческие системы всех отраслей экономики, социальной сферы, государственного управления, обороны и безопасности, обеспечения правопорядка.

Требование перевода всех основных и вспомогательных систем обеспечения жизнедеятельности населения, функционирования бизнеса и управления органов власти на цифровые платформы и специализированные цифровые экосистемы продиктовано всеобъемлющей тенденцией цифровой трансформации по пути автоматизации и оптимизации протекающих процессов. Указанные системы и платформы должны характеризоваться высокими показателями оперативности работы, устойчивости функционирования и информационной безопасности. Еще более высокие требования предъявляются к продуктам, внедряемым в сфере обеспечения безопасности жизнедеятельности человека. Последствия от реализации наблюдаемых и контролируемых рисков в этой сфере могут выражаться в прямом экономическом, физическом, психическом, социальном и т.д. ущербе и быть общественно опасными, одномоментными и точечными (однородными) или комплексными, иметь продолжающийся во времени характер. Автоматизация и оптимизация на основе цифровых систем в области обеспечения безопасности ориентированы, прежде всего, на предотвращение в кроткие сроки угроз либо последствий их реализации в результате чрезвычайных ситуаций [1].

Наиболее обстоятельно авторами разработаны правовые аспекты вопроса обеспечения национальной безопасности в условиях всеобщей цифровизации, при этом системы и инструменты решения задач в этой отрасли заметно тяготеют к созданию и развитию систем межведомственного информирования и взаимодействия [2–4]. Проблемы предупреждения чрезвычайных ситуаций исследуются группой авторов, акцентирующих внимание на применении современных информационных технологий [5]. Ряд авторов работают над вопросом обеспечения безопасности с позиций управления рисками в рамках сценарного подхода. Идеи разработаны концептуально, предложены основные направления трансформации общественных отношений и задачи их законодательного регулирования. Акцент в исследовании авторами делается на управлении противодействием коррупционным и экстремистским проявлениям [6–7]. Отдельным аспектом обеспечения безопасности является промышленная безопасность. В этом направлении разработки систем и инструментов идут активно и давно, но успехи очень дифференцированы в зависимости от финансовых возможностей компаний инвестировать в эту сферу охраны труда [8–9].

Международный опыт систем обеспечения безопасности населения включает: развитие механизмов и инструментов предотвращения угроз, нивелирования, минимизации и защиты от последствий реализации рисков с помощью решений Интернета вещей (*IoT*); создание и развитие мобильных пунктов управления ситуациями, в т.ч. чрезвычайными; внедрение датчиков мониторинга состояния объектов повышенной опасности (атомных электростанций, гидросооружений), водных объектов, лесов и т.д.; разработку приложений для населения, немедленно передающих информацию о возникших угрозах (затоплениях, землетрясениях, экстремальных погодных условиях, пожарах, оползнях и т.д.). Примером может служить система защиты персонала экстренных служб с помощью интеллектуальных масок, касок и костюмов, которые контролируют качество воздуха и жизненно важные функции организма, передают информацию лицам, контролирующим процесс [10–12].

Созданная в 1992 г. Российская система предупреждения и действий в чрезвычайных ситуациях и преобразованная в 1995 г. в Единую государственную систему по предупреждению и ликвидации чрезвычайных ситуаций (РСЧС) законодательно основана на Федеральном законе от 21.12.1994 г. № 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера». В 2013 г. внимание на законодательном уровне было уделено системам обнаружения, предупреждения и ликвидации последствий компьютерных атак и атак на ИТ-ресурсы[1].

Концептуальные, нормативные и методические основы обеспечения безопасности в Российской Федерации были заложены «Основными направлениями государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры РФ» (утв. Президентом РФ 03.02.2012 г. № 803), «Концепцией государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ» (№ К 1274 от 12.12.2014 г.), Федеральным законом от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», Методическими рекомендациями по созданию ведомственных и корпоративных центров ГосСОПКА от Центра защиты информации и специальной связи Федеральной службы безопасности, созданным Национальным координационным центром по компьютерным инцидентам и др. [13]

Цифровая трансформация РСЧС, проводимая органами власти в приоритетном порядке, содействует росту уровня контролируемости рисков и угроз для населения и государства в чрезвычайных ситуациях, в области пожарной безопасности, безопасности на водных объектах и т.д. путем развития и повышения эффективности взаимодействия граждан, организаций и органов власти (государственных и муниципальных). Одним из направлений в этой области является развитие аппаратно-программных комплексов и технических средств мониторинга, прогнозирования и поддержки принятия решений.

Как и в других отраслях, цифровизация в сфере безопасности имеет свои особенности в разных регионах. Во многих регионах и крупных городах используются технологии повышения безопасности города, например, системы видеонаблюдения, которые позволяют отслеживать происходящее на улицах и в общественных местах; системы распознавания лиц, которые помогают быстрее находить граждан, совершивших преступление. Важным элементом цифровизации является создание единой базы данных о лицах, нарушивших закон, и их местонахождении; активно внедряются цифровые технологии повышения безопасности дорожного движения – системы, позволяющие быстро обнаруживать нарушения правил дорожного движения и адресовать штрафы; системы дистанционного наблюдения за объектами, которая помогает быстро реагировать на возможные угрозы [14].

В Калининградской области функционирует единая система управления оперативной обстановкой, которая позволяет быстро реагировать на возможные угрозы, координировать действия служб безопасности и своевременно информировать население о происходящем. В Республике Татарстан активно внедряются системы контроля доступа к объектам. Например, в школах и дошкольных учреждениях используются системы биометрического контроля или технологии распознавания лиц в целях контроля посещаемости и оплаты питания учеников и воспитанников. Система распознавания лиц используется в Татарстане правоохранительными органами и местными властями.

[1] Указ Президента РФ от 15.01.2013 г. № 31с (ред. от 22.12.2017).

Примеров региональных систем контроля и управления ситуацией довольно много: часть из них основаны на федеральных проектах, а некоторые субъекты РФ разработали и реализуют собственные проекты и системы.

Материалы и методы

Авторами проведено исследование по материалам текстов стратегий в области цифровой трансформации ключевых отраслей субъектов РФ[1] с целью выявления активности регионов в разработке и внедрении цифровых проектов в области обеспечения безопасности. Акцент сделан на сфере обеспечения общественной безопасности, но также учитывались проекты обеспечения транспортной и информационной безопасности.

Согласно ОКВЭД[2], ключевая отрасль цифровой трансформации «Безопасность» относится к деятельности по обеспечению безопасности в чрезвычайных ситуациях (код классификатора 84.25). Деятельность, относящаяся к сфере обеспечения информационной безопасности, расположена в классификаторе под кодом 74.90.3 «Предоставление консультационных услуг по вопросам безопасности».

Авторами выявлено, что 16 субъектов РФ (19 %) включили в свои стратегии отрасль «Безопасность» («Безопасность жизнедеятельности») в качестве ключевой в области цифровой трансформации. Из них 7 регионов сделали акцент только на проектах, рекомендованных федеральными органами власти (ФОИВ), – «Развитие «Озера данных» регионального уровня в рамках РСЧС» и «Цифровизация процесса оказания финансовой помощи населению, пострадавшему в результате чрезвычайных ситуаций природного и техногенного характера» (Курская область, Тамбовская область, Республика Тыва, Челябинская область и др.). Всего 9 субъектов РФ помимо федеральных реализуют и региональные проекты цифровой трансформации в отрасли «Безопасность»: Мурманская область, Забайкальский край, Сахалинская область, Красноярский край и др. (рис. 1).

Наибольшее количество субъектов РФ вошли в группу регионов, реализующих рекомендованные ФОИВ проекты в иных сферах и отраслях цифровой трансформации (в области обеспечения отдельных аспектов безопасности, например, транспортной, информационной, промышленной безопасности), – всего 43 субъекта РФ или 51 % (Курганская область, Республика Ингушетия, Астраханская область, Приморский край, Республика Калмыкия и др.). К субъектам, реализующим рекомендованные ФОИВ и региональные проекты в иных отраслях цифровой трансформации в области обеспечения отдельных аспектов безопасности, отнесено 19 субъектов РФ или 23 % от общего количества регионов. И еще 6 регионов в текстах своих стратегий цифровой трансформации не уделили пристального внимания вопросам безопасности, в том числе в сфере транспорта (рис. 1).

В число обследованных субъектов РФ не вошла Москва – у города федерального значения отсутствует стратегия цифровой трансформации как документ. В Москве в 2011 г. принята государственная программа «Развитие цифровой среды и инноваций» (постановление Правительства Москвы от 09.08.2011 г. № 349-ПП в ред. от 29.03.2022 г. № 494-ПП)[3], включающая в качестве задач подпрограмм: обеспечение информационной безопасности систем и ресурсов города; обеспечение общественной безопасности в рамках городской системы видеонаблюдения (почти 165 тыс. камер), информация из которой поступает в ГИС «Единый центр хранения и обработки данных» (ЕЦХД, доступ к нему предоставлен сотрудникам правоохранительных органов), и другие направления, сформулированные в «Концепции комплексной безопасности города Москвы»[4].

[1] Сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. Стратегии цифровой трансформации:
https://digital.gov.ru/ru/activity/directions/1064/?utm_referrer=https%3a%2f%2fwww.google.com%2f
[2] Общероссийской классификатор видов экономической деятельности (ред. 2022 г.)
[3] https://www.mos.ru/dit/documents/gosudarstvennaya-programma-goroda-moskvy/view/275384220/
[4] Распоряжение Правительства Москвы от 16.04.2010 г. № 707-рп «Об утверждении концепции комплексной безопасности города Москвы»

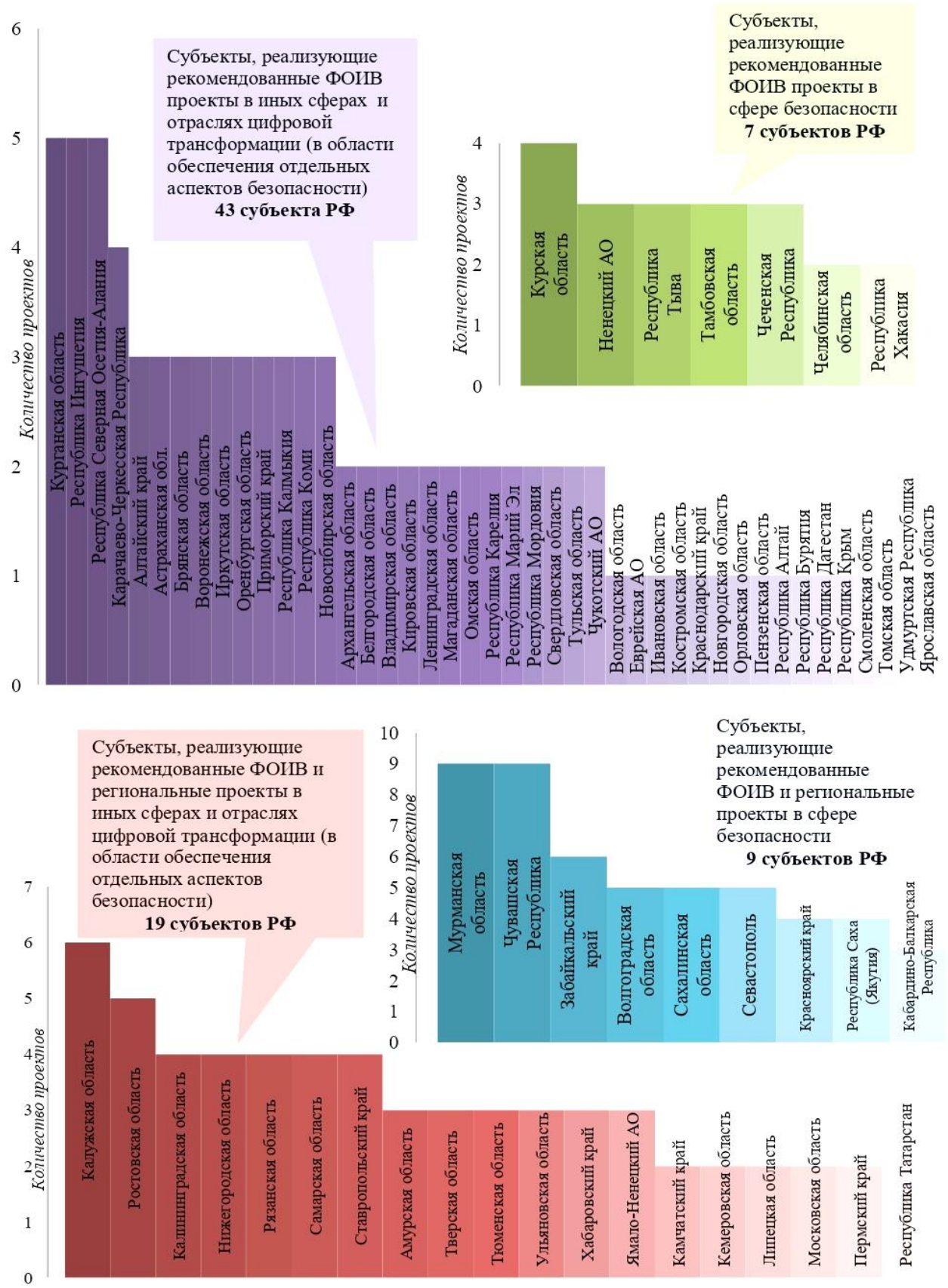


Рис. 1. Распределение субъектов РФ по реализации проектов цифровой трансформации в области безопасности

Fig.1. Distribution of Russian subjects for the implementation of digital transformation projects in the field of security

Источник: разработано авторами

Результаты и обсуждение

Активность субъектов РФ по разработке и внедрению проектов цифровой трансформации в области обеспечения общественной, транспортной, информационной безопасности характеризуется показателем количества проектов в этой области. На рис. 1 показано, что наибольшую активность среди всех регионов проявили Мурманская область и Чувашская Республика (общее количество проектов в области обеспечения безопасности – 9). Большая часть регионов реализуют 3–4 и менее проектов, 6 регионов не включили проекты обеспечения безопасности в текст стратегии цифровой трансформации.

Наиболее часто реализуемыми проектами явились:

– «Цифровое управление транспортным комплексом» и «Цифровизация для транспортной безопасности» (проекты отрасли «Транспорт и логистика»);

– «Развитие «Озера данных» регионального уровня в рамках РСЧС» (проект реализуется субъектами в рамках отраслей «Государственное управление», «Социальная сфера», «Развитие городской среды», «Безопасность»);

– «Цифровизация процесса оказания финансовой помощи населению, пострадавшему в результате чрезвычайных ситуаций природного и техногенного характера» (проект отраслей «Государственное управление», «Социальная сфера», «Безопасность»);

– «Интеллектуальная городская среда» (проект отрасли «Развитие городской среды»).

Частично эти проекты реализуются субъектами РФ в рамках проектов «Умный город» и «Безопасный город» (системы общественной безопасности). Указанные проекты относятся к рекомендованным федеральными органами власти (ФОИВ).

Среди региональных проектов субъектов РФ следует отметить:

– внедрение принципиально новой системы информирования граждан о возникновении чрезвычайных ситуаций (обеспечение своевременного и гарантированного доведения информации и сигналов оповещения до органов управления гражданской обороны и населения (РАСИОН) Волгоградской области);

– интеллектуальные транспортные системы обеспечения транспортной безопасности (Калининградская область, Амурская область, Камчатский край);

– создание и развитие ситуационного центра (Кабардино-Балкарская Республика, Калужская область, Рязанская область, Тульская область, Чувашская Республика);

– «Регистратор» Нижегородской области (получение оперативной информации о технологических нарушениях, об аварийных или чрезвычайных ситуациях, возникших на объектах жизнеобеспечения населения);

– развитие информационно-аналитической системы оперативного мониторинга обстановки при введении режима чрезвычайной ситуации, повышенной готовности на территории Республики Саха (Якутия) (отрасль «Безопасность»);

– автоматизированная информационная система «Единая платформа управления транспортной системой Республики Татарстан» (отрасль «Транспорт и логистика»);

– «Единая государственная информационная система «ГЛОНАСС+112», создание (модернизация) интеллектуальных транспортных систем в Ростовской агломерации (отрасль «Транспорт и логистика»);

– интеграция «Системы-112» Чувашской Республики с мобильным приложением вызова экстренных оперативных служб, реконструкция РАСЦО, формирование единой системы экстренного оповещения населения Чувашской Республики.

Ряд субъектов реализуют проекты построения SOC-центра обеспечения информационной безопасности (Волгоградская область), трансформации ведомственного центра ГосСОПКА в SOC (информационная безопасность Красноярского края), создания платформы автоматизированных систем обеспечения общественной безопасности (отрасль «Безопасность» Красноярского края), создания комплексной системы сбора и обработки данных из различных источников информации, системы мониторинга, камер видеонаблюдения, датчиков состояния окружающей среды и т.д., описывающие критически важные показатели безопасности населения (отрасль «Безопасность» Мурманской области).

Некоторые регионы включают в тексты стратегий проекты в сфере промышленной безопасности – «Цифровая промышленная безопасность в ТЭК» (отрасль «Энергетическая инфраструктура» Брянской области, Мурманской области и др.).

Вопрос выбора отрасли в качестве ключевой для включения проектов в области безопасности у субъектов РФ решен по-разному. Ряд регионов включили проекты по развитию «Озера данных» в отрасль «Государственное управление» (Алтайский край, Забайкальский край, Иркутская область и др.). Проект по цифровизации процесса оказания финансовой помощи населению, пострадавшему в результате ЧС, часто субъектами реализуется в рамках отраслей «Социальная сфера» (Забайкальский край, Иркутская область) или «Государственное управление» (Алтайский край, Амурская область).

Превалирующая часть субъектов РФ акцентирует внимание в своих стратегиях на обеспечении безопасности дорожного движения, развивая проекты «Интеллектуальная транспортная система» (Ивановская область, Иркутская область и др.), «Цифровое управление транспортным комплексом» и «Цифровизация для транспортной безопасности» [15].

К субъектам РФ, не включившим в тексты своих стратегий цифровой трансформации проекты в области обеспечения общественной безопасности (в том числе в сфере транспорта), относятся Псковская область, Республика Адыгея, Республика Башкортостан, Санкт-Петербург, Саратовская область, Ханты-Мансийский АО. В некоторых из них реализуются проекты, подразумевающие внедрение инструментов и технологий обеспечения информационной безопасности (Псковская область, Ханты-Мансийский АО).

Проекты цифровой трансформации отрасли «Безопасность» Красноярского края

В целях обеспечения безопасности по основным направлениям жизнедеятельности населения Красноярского края в рамках государственной программы «Развитие информационного общества», утвержденной Постановлением Правительства Красноярского края от 30.09.2013 г. № 504-п, Министерство цифрового развития Красноярского края и его подведомственное учреждение КГКУ «Центр информационных технологий» осуществляют развитие, содержание и эксплуатацию комплексной автоматизированной системы «Безопасный город», реализуют мероприятия по созданию, развитию и организации автоматизированного обмена информацией в рамках «Озера данных» регионального уровня РСЧС, совершенствование системы «112».

В стратегию цифровой трансформации Красноярского края в 2022 г. в качестве приоритетной (ключевой) была введена отрасль «Безопасность». Помимо рекомендованных федеральными органами власти проектов по развитию «Озера данных» и цифровизации процесса оказания финансовой помощи населению, пострадавшему в результате ЧС, в стратегию включены проекты по трансформации центра ГосСОПКА края в SOC края и по созданию платформы автоматизированных систем обеспечения безопасности – аппаратно-программный комплекс «Безопасный город» (АПК «БГ»).

Реализация проекта «Умный город» в рамках цифровой трансформации отрасли «Безопасность» позволит решить, помимо прочих, задачи формирования оперативной и эффективной системы управления городским хозяйством, создания безопасных и комфортных условий для населения за счет внедрения систем круглосуточного мониторинга и видеонаблюдения.

Цифровая трансформация отрасли «Безопасность» невозможна без качественной информационной инфраструктуры, поэтому цифровизация безопасности в Красноярском крае во многом зависит от реализации регионального проекта «Информационная инфраструктура», который предполагает развитие широкополосного доступа к сети Интернет на территории всего края. Проект создания и развития «Озера данных» нацелен на повышение уровня межведомственного взаимодействия за счет внедрения цифровых решений в работу всех ведомств (перевод 100 % ведомств к 2024 г.). Проект трансформации центра ГосСОПКА в SOC Красноярского края ориентирован на автоматизацию обработки информации (до 85 % информации о событиях безопасности к 2024 г.), что позволит повысить уровень кибербезопасности. Проект создания платформы автоматизированных систем обеспечения общественной безопасности правопорядка и безопасности среды обитания Красноярского края подразумевает подключение всех органов местного самоуправления края к платформе автоматизации безопасности к концу 2024 г.

В Красноярском крае предполагается реализовать следующие решения для развития отрасли «Безопасность»:

– формирование системы управления оперативными данными в цифровом формате, сокращение времени реагирования органов повседневного управления;
– повышение эффективности функционирования РСЧС;
– повышение степени оперативности и эффективности действий реагирующих структур;
– минимизация ущерба в результате реализации рисков, воздействия факторов природного и техногенного характера, возникновения кризисных ситуаций для населения и окружающей среды;
– сокращение среднего срока простоя государственных информационных систем исполнительных органов государственной власти;
– снижение риска простоя после компьютерных атак;
– расширение возможностей обращения в экстренные службы;
– недостаток профессиональных компетенций сотрудников;
– получение дополнительных гарантий безопасности при возникновении аварий;
– совершенствование процесса оказания финансовой помощи населению, пострадавшему в результате ЧС природного и техногенного характера, посредством предоставления государственных услуг, в том числе в электронной форме.

В табл. 1 приведены ожидаемые результаты цифровой трансформации отрасли «Безопасность» Красноярского края.

Таблица 1 – Проекты цифровой трансформации отрасли «Безопасность» Красноярского края

Table 1 – Digital Transformation Projects of the Industry «Security» of the Krasnoyarsk Region

Наименование проекта стратегии цифровой трансформации	
Показатель развития отрасли	*Целевое значение показателя*
Проект «Создание и развитие «Озера данных» регионального уровня в рамках РСЧС» (рекомендовано ФОИВ)	
«перевод в цифровой формат информационного взаимодействия со всеми (100 %) органами повседневного управления территориальной подсистемы РСЧС до 2024 года»	показатель измеряется в процентах, ожидаемые значения: 2022 г. – 0 %, 2023 г. – 100 %, 2024 г. – 100 %.
Проект «Трансформация Ведомственного центра ГосСОПКА Красноярского края в SOC Красноярского края»	
«доля событий безопасности информации, обрабатываемых автоматизировано»	показатель измеряется в процентах, ожидаемые значения: 2022 г. – 20 %, 2023 г. – 80 %, 2024 г. – 85 %.
Проект «Создание платформы автоматизированных систем обеспечения общественной безопасности правопорядка и безопасности среды обитания Красноярского края»	
«доля органов местного самоуправления, подключенных к платформе автоматизации безопасности»	показатель измеряется в процентах, ожидаемые значения: 2022 г. – 0 %, 2023 г. – 16 %, 2024 г. – 100 %.
Проект «Цифровизация процесса оказания финансовой помощи населению, пострадавшему в результате чрезвычайных ситуаций природного и техногенного характера» (рекомендовано ФОИВ)	
«фактический перевод процесса оказания финансовой помощи населению, пострадавшему в результате чрезвычайных ситуаций природного и техногенного характера, на предоставление государственных услуг в I полугодии 2023 года (100 % услуг)»	показатель измеряется в процентах, ожидаемые значения: 2022 г. – 0 %, 2023 г. – 100 %, 2024 г. – 100 %.

Источник: Стратегия в области цифровой трансформации отраслей экономики, социальной сферы и государственного управления Красноярского края[1].

[1] http://digital.krskstate.ru/page11464/page14216

Среди проблем текущего состояния отрасли «Безопасность», решаемых в рамках процесса цифровой трансформации, выделяются следующие:

– низкий уровень межведомственного взаимодействия, обусловленный разрозненностью информационных систем, задействованных в ликвидации ЧС;

– отсутствие интеграции между разными программными продуктами (ведомственными ИС), используемыми при обеспечении безопасности;

– недостаточная отработка механизма возмещения ущерба лицам, пострадавшим в результате ЧС природного и техногенного характера;

– необходимость повышения уровня кибербезопасности.

РСЧС объединяет 15 министерств, 8 федеральных служб, 11 федеральных агентств и 2 госкорпорации. Цифровая трансформация РСЧС путем формирования «Озера данных» в рамках федерального проекта «Искусственный интеллект» включает также внедрение системы космического мониторинга ситуаций, механизмов сокращения времени реагирования на чрезвычайные ситуации и инциденты, а также повышение безопасности населения края. Проект направлен на организацию единого информационного пространства федерального и регионального уровней с целью снижения ущерба от чрезвычайных ситуаций за счет формирования платформы межведомственного обмена информацией и глубокой аналитики на основе больших данных, цифровизацию процессов предупреждения и ликвидации последствий ЧС. Использование «Озера данных» и технологий искусственного интеллекта позволит построить модели развития наиболее вероятных сценариев, способствующих принятию управленческих решений по недопущению и минимизации ущерба. Информационные технологии значительно ускоряют процесс прогнозирования, а также способствуют изменению временных показателей в реагировании на чрезвычайные ситуации и происшествия оперативных служб РСЧС.

В августе 2022 г. в целях повышения качества и оперативности реагирования на инциденты информационной безопасности в органах исполнительной власти, а также в целях снижения риска простоя после компьютерных атак в Красноярском крае был разработан проект «Трансформация Ведомственного центра ГосСОПКА Красноярского края в SOC Красноярского края». Центр ГосСОПКА ориентирован на выявление атак на объекты критической информационной инфраструктуры, проведение мероприятий по ликвидации последствий таких атак и снижение вероятности их повторного возникновения. В развитие этой системы Центр управления инцидентами информационной безопасности (Security Operation Center – SOC) выполняет мониторинг и анализирует вторжения в режиме реального времени, предотвращает кибератаки, действуя на опережение, сканируя сети на уязвимости и анализируя киберинциденты.

За последние три года в Красноярском крае проведена масштабная работа в области информационной безопасности: созданы отдельные подразделения в министерстве цифрового развития и подведомственных учреждениях, организован ведомственный центр ГосСОПКА, получена лицензия на оказание услуг по защите информации, регулярно проводится обучение специалистов. Все эти меры ориентированы на противостояние киберугрозам.

В целях повышения эффективности деятельности экстренных оперативных служб при предупреждении и ликвидации чрезвычайных ситуаций, расширения возможностей обращения в экстренные службы, получения дополнительных гарантий безопасности при возникновении чрезвычайной ситуации, минимизации ущерба для населения и окружающей среды и др. в августе 2022 г. в Красноярском крае был разработан проект «Создание платформы автоматизированных систем обеспечения общественной безопасности, правопорядка и безопасности среды обитания Красноярского края».

Для достижения поставленных целей в Красноярском крае в течение 2022–2023 гг. планируется развернуть аппаратно-программный комплекс «Безопасный город» (далее АПК «БГ») на территории всего края. На первом этапе реализации планируется приобретение специализированного программного обеспечения для создания базовой инфраструктуры в целях дальнейшего ее внедрения на территории всего региона. На втором этапе планируется выполнить проектирование аппаратно-программного комплекса с учетом созданной инфраструктуры и для обеспечения подключения к АПК «БГ» крупных территорий региона. На третьем этапе планируется развернуть АПК «БГ» на территории остальных муниципальных образований Красноярского края и перевести

систему в режим постоянной эксплуатации. АПК «БГ» как комплекс систем всесторонней защиты населения от разного рода внешних угроз (природных, техногенных, экологических и т.д.) включает также правоохранительный блок с камерами наблюдения, фиксирующими нарушения общественного порядка и правил дорожного движения. Суть его работы заключается не только в фиксации фактов происшествий – система настроена на предупреждение чрезвычайных ситуаций, что существенно снижает расходы на их ликвидацию.

К основным направлениям «Безопасного города» следует отнести:

– формирование коммуникационной площадки для органов местного самоуправления с целью устранить риски и обеспечить безопасность населения;

– разработка требований к аппаратным и программным средствам, ориентированным на обеспечение природной и техногенной безопасности на муниципальном уровне;

– обеспечение обмена информацией между участниками всех существующих программ в сфере безопасности через единое информационное пространство на всех уровнях управления;

– проведение ситуационного анализа причин дестабилизации, прогнозирование существующих и потенциальных угроз.

Основным координатором реализации и развития АПК «Безопасный город» в регионах является МЧС России, его соисполнителями мероприятий по строительству и развитию комплекса на федеральном уровне являются около 20 министерств, служб и агентств.

Система «Безопасный город» внедряется в Красноярске с 2010 г. Проводится круглосуточный мониторинг ситуации на городских дорогах, общественных пространствах, просматриваются «тревожные» места с помощью камер и направляются сотрудники правоохранительных структур. По состоянию на начало 2023 г. в Красноярске функционирует 3 565 камер, видеоинформация с которых транслируется в режиме реального времени и в режиме видеоархива на рабочие места сотрудников полиции, силовых структур, администраций, объектов образования, подключенных к комплексной автоматизированной системе «Безопасный город». Проект постепенно расширяет свои границы путем развертывания единой платформы комплекса для всех муниципальных образований края. Перспективными модулями, которые будут включены в АПК «БГ», являются блоки экологического мониторинга и мониторинга промышленных объектов.

Существует ряд причин, которые препятствуют достижению целей проектов цифровой трансформации отрасли «Безопасность» субъектов РФ:

– территориально неравномерное развитие цифровой инфраструктуры;

– недостаточный уровень квалификации кадров для работы с цифровыми решениями;

– низкий уровень цифровой грамотности граждан;

– недостаточное финансирование проектов цифровой трансформации;

– низкий уровень совместного использования имеющихся у органов власти информационных ресурсов и систем, использование в работе министерствами и ведомствами только собственных ресурсов.

Внедрение цифровых технологий в отрасль «Безопасность» ведет к значительному трансформационному эффекту. В первую очередь, это позволяет повысить качество государственных и муниципальных услуг в области безопасности, ускорить реакцию на происшествия и снизить риски. Цифровизация позволяет сократить время ожидания и упростить процедуры получения государственных и муниципальных услуг, снизить затраты на их оказание и сделать услуги более доступными для населения, что ведет к росту качества жизни граждан и повышению уровня безопасности в регионе.

Заключение

На протяжении последних лет цифровая трансформация стала одной из стратегических задач национального развития Российской Федерации. Цифровизация субъектов РФ проводится в рамках региональных стратегий в области цифровой трансформации отраслей экономики, социальной сферы и государственного управления. Большое значение для достижения национальных целей имеет программа «Цифровая экономика Российской Федерации», целями которой являются: повышение цифровой грамотности граждан, обеспечение информационной безопасности, рост качества и доступности государственных услуг. Цифровизация и трансформация территорий проходит неравномерно, отсутствуют универсальные решения по внедрению цифровых сервисов.

Цифровая трансформация является нетривиальной задачей, требующей больших усилий и специфических подходов от органов власти, а также определенного уровня восприятия этого процесса средой внедрения (населением, организациями).

Реализация Стратегии в области цифровой трансформации отраслей экономики, социальной сферы и государственного управления Красноярского края позволяет получить ряд конкурентных преимуществ, повышающих уровень безопасности и эффективности превентивной деятельности в этой сфере:

– внедрение цифровых технологий и систем безопасности увеличивает эффективность работы правоохранительных органов и служб безопасности – возрастает скорость реакции на возможные угрозы, уровень безопасности в регионе повышается;

– цифровая трансформация позволяет создать новые услуги и продукты в сфере безопасности: обеспечена возможность мониторинга общественной безопасности через системы видеонаблюдения; внедрены новые технологии защиты информации, что позволило повысить уровень кибербезопасности;

– цифровые технологии позволяют эффективно управлять финансовыми и человеческими ресурсами, оптимизировать процессы в сфере безопасности.

Цифровая трансформация отрасли «Безопасность» позволяет получить следующие социально-экономические эффекты:

– рост качества услуг в сфере обеспечения безопасности: применение новых технологий и цифровых решений позволяет повысить эффективность работы сотрудников, ускорить реакцию на происшествия и снизить имущественные и личные риски;

– сокращение затрат на обеспечение безопасности: внедрение цифровых технологий позволяет автоматизировать процессы и оптимизировать кадровый состав соответствующих структур;

– развитие новых рынков и возможностей для бизнеса: цифровая трансформация отрасли «Безопасность» позволяет создать новые рынки для различных технологических решений и услуг, стимулируя развитие инновационных компаний и привлечение инвестиций;

– рост качества жизни людей: благодаря повышению уровня безопасности, люди могут чувствовать себя более защищенными и уверенными, что положительно сказывается на их психологическом и физическом здоровье.

Цифровая трансформация сферы оказания государственных и муниципальных услуг обеспечивает:

– рост качества услуг за счет применения цифровых технологий, внедрение которых позволяет повысить эффективность работы сотрудников, занятых оказанием услуг;

– автоматизацию процессов и уменьшение количества необходимых документов и справок, упрощая процедуры получения услуг и сокращая время ожидания;

– оптимизацию процессов, решая кадровые вопросы и задачи минимизации расходов бюджетов;

– рост безопасности получения и доступности услуг для населения, в том числе для проживающего в отдаленных или труднодоступных местностях.

На текущий момент Красноярский край активно развивает цифровые технологии в сфере безопасности. Внедрены цифровые платформы обмена информацией между правоохранительными органами, системы видеонаблюдения и иные технические средства мониторинга ситуации и фиксации фактов и инцидентов. Реализация проектов стратегии: решает проблему межведомственного взаимодействия в регионе; позволяет наладить механизм возмещения ущерба населению, пострадавшему в результате ЧС природного и техногенного характера, и интеграцию между различными программными продуктами, используемыми в работе ведомств; повышает уровень кибербезопасности. В Красноярском крае регулярно проводятся мероприятия по повышению квалификации сотрудников правоохранительных органов в области цифровых технологий. При этом важно продолжать работу по внедрению новых цифровых решений и развитию существующих в целях повышения уровня безопасности и качества услуг для населения.

Список источников

1. Алиева Э. Цифровизация и безопасность // Научные труды Северо-Западного института управления РАНХиГС. 2019. № 10-3 (40). С. 84–87.

2. Корабельников С. М. Цифровизация и национальная безопасность // Вестник Российской правовой академии. 2022. № 1. С. 44–49. doi: 10.33874/2072-9936-2022-0-1-44-49

3. Vedysheva N., Mukhlynina M., Efimova O., Nikiforov A. Digital Technologies in Ensuring the Protection of the Population and Territories of the Russian Federation from Natural and Man-Made Emergencies: Legal Aspect. SHS Web of Conferences. 2021; 93: 02022. doi: 10.1051/shsconf/20219302022

4. Sidorenko E. L., von Arx P. Transformation of Law in the Context of Digitalization: Defining the correct priorities // Digital Law Journal. 2020. № 1(1). С. 24–38. doi: 10.38044/DLJ-2020-1-1-24-38

5. Юркин М. А., Латышенко К. П., Семенов Е. С. Предупреждение чрезвычайных ситуаций с применением современных информационных технологий // Научные и образовательные проблемы гражданской защиты. 2019. № 1 (40). 40–45.

6. Шульц В. Л., Бочкарев С. А., Кульба В. В. и др. Сценарное исследование проблем обеспечения общественной безопасности в условиях цифровизации. М.: Проспект. 2020. 240 с.

7. Шульц В. Л., Кульба В. В., Шелков А. Б., Чернов И. В., Тимошенко А. А. Методы анализа влияния процессов трансформации права на развитие социально-экономической системы в условиях цифровизации: сценарный подход (постановка задачи) // Российский журнал правовых исследований. 2021. № 8-1. С. 19–36. doi: 10.17816/RJLS65146

8. Водянова С., Мальцев С. Цифровизация промышленной безопасности и прогресс в области средств охраны труда // CONNECT. 2020. № 5–6. С. 102–106. https://www.connect-wit.ru/wp-content/uploads/2021/06/BTU_Vodjanova_5_6_20.pdf

9. Киселева О. Н. Инновационная цифровизация в контексте обеспечения управленческой безопасности промышленной безопасности России // Основы экономики, управления и права. 2019. № 1(19). С. 21–25. doi: 10.51608/23058641_2019_1_21

10. Ellebrecht S., Kaufmann S. Digitalization and Its Security Manifestations // European Journal for Security Research. 2020;(5):1–3. doi: 10.1007/s41125-019-00063-8

11. Salminen M., Hossain K. Digitalisation and human security dimensions in cybersecurity: An appraisal for the European High North // Polar Record. 2018. № 54(2). P. 108–118. doi: 10.1017/S0032247418000268

12. OECD Policy Framework on Digital Security: Cybersecurity for Prosperity. OECD Publishing, Paris. 2022. doi: 10.1787/a69df866-en

13. Снастин В. А., Харитонов Т. П., Сорока Г. Ю. Оценка качества обеспечения информационной безопасности России в условиях цифровизации экономики // Международный журнал гуманитарных и естественных наук. 2021. № 8-1(59). С. 105–108. doi: 10.24412/2500-1000-2021-8-1-105-108

14. Морозова Г. А., Лапаев Д. Н. Современная цифровизация и обеспечение безопасности // Развитие и безопасность. 2019. № 1. С. 70–81. doi: 10.46960/74159_2019_1_70

15. Бажина М. А. Правовое регулирование безопасности дорожного движения в эпоху цифровизации // Безопасность дорожного движения. 2021. № 4. С. 4–6.

References

1. Aliyeva E. Digitalization and Security. *Nauchnyye trudy Severo-Zapadnogo instituta upravleniya RANKhiGS = Scientific works of the North-Western Institute of Management of RANEPA*. 2019; 10-3(40): 84-87. (In Russ.)

2. Shipbuilders S. M. Digitalization and national security. *Vestnik Rossiyskoy pravovoy akademii = Bulletin of the Russian Law Academy*. 2022; 1: 44-49. doi: 10.33874/2072-9936-2022-0-1-44-49. (In Russ.)

3. Vedysheva N., Mukhlynina M., Efimova O., Nikiforov A. Digital Technologies in Ensuring the Protection of the Population and Territories of the Russian Federation from Natural and Man-Made Emergencies: Legal Aspect. *SHS Web of Conferences*. 2021; 93: 02022. doi: 10.1051/shsconf/20219302022

4. Sidorenko E. L., von Arx P. Transformation of Law in the Context of Digitalization: Defining the correct priorities. *Digital Law Journal*. 2020; 1(1): 24–38. doi: 10.38044/DLJ-2020-1-1-24-38

5. Yurkin M. A., Latyshenko K. P., Semenov E. S. Prevention of emergency situations using modern information technologies. *Nauchnyye i obrazovatel'nyye problemy grazhdanskoy zashchity = Scientific and educational problems of civil protection*. 2019; 1 (40): 40–45. (In Russ.)

6. Shults V. L., Bochkarev S. A., Kulba V. V. et al. Scenario study of the problems of ensuring public safety in the context of digitalization. Moscow: Prospekt. 2020. 240 p. (In Russ.)

7. Shults V. L., Kulba V. V., Shelkov A. B., Chernov I. V., Timoshenko A. A. Methods for analyzing the impact of law transformation processes on the development of the socio-economic system in the context of digitalization: a scenario approach (problem setting). *Rossiyskiy zhurnal pravovykh issledovaniy = Russian Journal of Legal Research.* 2021; 8 (1): 19–36. doi: 10.17816/RJLS65146. (In Russ.)

8. Vodyanova S., Maltsev S. Digitalization of industrial safety and progress in the field of labor protection. *CONNECT.* 2020; 5–6: 102–106. Available from: https://www.connect-wit.ru/wp-content/uploads/2021/06/BTU_Vodjanova_5_6_20.pdf. (In Russ.)

9. Kiseleva O. N. Innovative digitalization in the context of ensuring the management security of industrial enterprises in Russia. *Osnovy ekonomiki, upravleniya i prava = Fundamentals of Economics, Management and Law*. 2019; 1 (19): 21–25. doi: 10.51608/23058641_2019_1_21. (In Russ.)

10. Ellebrecht S., Kaufmann S. Digitalization and Its Security Manifestations. *European Journal for Security Research*. 2020; 5: 1–3. doi: 10.1007/s41125-019-00063-8

11. Salminen M., Hossain K. Digitalisation and human security dimensions in cybersecurity: An appraisal for the European High North. *Polar Record*. 2018; 54(2): 108–118. doi: 10.1017/S0032247418000268

12. OECD Policy Framework on Digital Security: Cybersecurity for Prosperity. OECD Publishing, Paris. 2022. doi: 10.1787/a69df866-en

13. Snastin V. A., Kharitonov T. P., Soroka G. Yu. Assessment of the quality of information security in Russia in the context of digitalization of the economy. *Mezhdunarodnyy zhurnal gumanitarnykh i yestestvennykh nauk = International Journal of Humanities and Natural Sciences*. 2021; 8-1(59): 105–108. doi: 10.24412/2500-1000-2021-8-1-105-108. (In Russ.)

14. Morozova G. A., Lapaev D. N. Modern digitalization and security. *Razvitiye i bezopasnost' = Development and security*. 2019; 1: 70–81. doi: 10.46960/74159_2019_1_70. (In Russ.)

15. Bazhina M. A. Legal regulation of road safety in the era of digitalization. *Bezopasnost' dorozhnogo dvizheniya = Road safety*. 2021; 4: 4–6. (In Russ.)

Информация об авторах

Е. В. Лобкова – кандидат экономических наук, доцент кафедры социально-экономического планирования Института экономики, государственного управления и финансов Сибирского федерального университета.
А. А. Ки-Юан – эксперт ООО «МФЦ Полюс».

Information about the authors

E. V. Lobkova – Candidate of Economic Sciences, Associate Professor of Department of Socio-economic Planning, Institute of Economics, Public Administration and Finance, Siberian Federal University.
A. A. Ki-Yuan – expert of LLC «MFC POLYUS» (Multifunctional Center Polyus Limited Liability Company).

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.
Contribution of the authors: the authors contributed equally to this article. The authors declare no conflicts of interests.

Статья поступила в редакцию 20.04.2023; одобрена после рецензирования 12.05.2023; принята к публикации 15.05.2023.
The article was submitted 20.04.2023; approved after reviewing 12.05.2023; accepted for publication 15.05.2023.