Е.С. Сазонова

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ЦИФРОВОЙ СРЕДЫ В СФЕРЕ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Москва
Институт экономики РАН
2024

Рецензенты:
к.э.н., доцент И.А. Колпакова,
к.э.н., доцент Р.Э. Абдулов

Сазонова Е.С. Проблемы безопасности цифровой среды в сфере государственного управления: Доклад. – М.: Институт экономики РАН, 2024. – 45 с.

ISBN 978-5-9940-0781-5

В докладе рассмотрены складывающиеся контуры государственного регулирования процессов цифровой трансформации государственного управления и обеспечения в этой связи безопасности цифрового пространства на современном этапе технологического развития. Основное внимание уделяется выявлению, рассмотрению и анализу ключевых проблем обеспечения безопасности цифровой среды и возникающих в контексте перехода к цифровому государственному управлению рисков. Отдельно исследованы вопросы реализации экспериментальных режимов в сфере развития цифровых технологий, включая технологии искусственного интеллекта, а также оценены перспективы применения в России институтов цифрового социального мониторинга.

Ключевые слова: безопасность, государственное управление, цифровая трансформация, цифровая среда, инновации, искусственный интеллект, экспериментальные правовые режимы, персональные данные, цифровое профилирование, социальный мониторинг.

Классификация JEL: H10, H56, O33, O38, G38.

Sazonova E.S. Problems of security of the digital environment in the field of public administration: Scientific report. – M.: Institute of Economics of the RAS, 2024 – 45 p.

The report examines the forming contours of public administration, regulating the processes of digital transformations of public administration and providing, in this regard, the security of digital environment at the present stage of technological development. The main focus is on identifying, reviewing and analyzing key issues in providing the security of the digital environment and risks arising in the context of the transition to digital government management. The issues of implementing experimental regimes in the field of development of digital technologies, including artificial intelligence, were separately studied, and the prospects for the use of digital social monitoring institutions in Russia were assessed.

Keywords: security, public administration, digital transformation, digital environment, innovation, artificial intelligence, experimental legal regimes, personal data, digital profiling, social monitoring.

JEL Classification: H10, H56, O33, O38, G38.

Оглавление

Введение

В последние годы цифровая трансформация государственного управления находилась в фокусе пристального внимания руководства страны, и поддержка данного процесса осуществлялась как на политическом уровне, так и на уровне нормативном. Цифровизация, цифровая трансформация вошли в число национальных целей страны и интенсивно развиваются во многих отраслях и сферах в качестве стратегических направлений развития, в том числе и в области государственного управления, цифровые технологии внедряются на всех этапах выполнения государством своих полномочий и функций. Создаваемая в ходе реализации данного процесса цифровая среда подразумевает выход на новый технологический уровень, предусматривающий полноценное электронное взаимодействие государства с гражданами и организациями, организацию работы государственных органов не с оцифрованными, а с цифровыми документами и данными, появление у граждан ранее неизвестных электронных прав.

Процессы цифровой трансформации, затрагивающие многие аспекты государственного строительства, с неизбежностью потребуют новых подходов к реализации задач органов власти и государственному управлению в целом, особенно в контексте перехода к цифровому государственному управлению и переводу традиционных его институтов в цифровой формат. Нельзя не отметить, что данные процессы также создают новые вызовы для экономической безопасности России, поскольку одним из направлений государственной политики в сфере ее обеспечения является «развитие системы государственного управления, прогнозирования и стратегического планирования в сфере экономики»[1]. И в настоящее время страна вошла в новый цикл развития, национальные

1. Пп. 1 п. 15 Стратегии экономической безопасности на период до 2030 года, утв. Указом Президента РФ от 13 мая 2017 г. № 208 // СПС «Гарант».

стратегические приоритеты и задачи которого определены на предстоящие 12 лет как часть предмета деятельности системы обеспечения экономической безопасности [*Городецкий*, 2024. С. 1331].

В этой связи впечатляющие результаты применения цифровых технологий в государственном управлении и выгоды от их стремительного внедрения необходимо соотносить с одновременно возникающими последствиями – проблемами безопасности цифровой среды, которые нуждаются в обозначении и анализе в связи с отсутствием широкой общественной и научной дискуссии по данному вопросу. Последнее и является *объектом настоящего исследования*.

Цель настоящего исследования – проведение институционального анализа происходящих процессов цифровой трансформации государственного управления в современных условиях и систематизация возникающих при этом проблем безопасности цифровой среды, формирование которой обусловлено переводом в цифровую форму совершения всех операций и коммуникаций в государственной управлении.

Задачами исследования являются:

- проведение анализа задач перехода к комплексному и масштабному цифровому государственному управлению и выявление эволюции регулирования этого процесса в современных условиях;
- определение, систематизация и описание проблем безопасности цифровой среды, возникающих в ходе цифровой трансформации государственного управления, и ведущейся в связи с их появлением дискуссии в общественной и научной среде;
- рассмотрение опыта реализации экспериментальных правовых режимов для внедрения цифровых инноваций (и особенно технологий искусственного интеллекта) и возникающих в этом контексте рисков для безопасности цифровой среды;
- определение предпосылок и перспектив формирования в России институтов цифрового социального мониторинга.

I

Задачи перехода к цифровому государственному управлению и институциональные основы регулирования этого процесса в современных условиях

В 2022 г. Россия вошла в число государств–лидеров в области цифровой трансформации государственного управления и цифровизации государственного сектора услуг (по данным Всемирного банка). Речь идет о международном рейтинге «GovTech Maturity Index» (GTMI), в рамках которого оценивается уровень развития цифровых технологий в государственном секторе стран мира (в 2022 г. в рейтинг вошло 198 государств)[2]. Индекс зрелости GovTech (GTMI) формируется по результатам оценки четырех приоритетных областей внедрения цифровых технологий: «Основные государственные системы», «Предоставление государственных услуг», «Цифровая вовлеченность населения» и «Институциональное обеспечение», которые, в свою очередь, рассчитываются на основе показателей, отражающих степени внедрения цифровых технологий в различных сферах государственного управления, доступности цифровых платформ и сервисов для граждан, открытости данных, применения платформ для участия населения в принятии решений, а также показатели по принятию стратегий цифровой трансформации и программ по развитию цифровых технологий, наличию нормативной базы и т.д. Россия, по данным рейтинга, вошла в число лидеров GovTech (категория «А»), что означает, что она демонстрирует современные и новаторские решения, передовой опыт во всех четырех приоритетных областях. Предыдущий отчет Всемирного банка, содержащий данные за 2020 г., относил Россию к категории «В» – т.е. к странам, где цифровым технологиям уделяется значительное внимание[3].

В последние годы внимание к цифровой трансформа-

2. Индекс зрелости государственных технологий: тренды в публичном секторе цифровой трансформации // Отчет Всемирного банка, 2022. – URL: https://www.worldbank.org/en/programs/govtech/gtmi (дата обращения: 12.11.2024).

3. Там же.

ции усиливается на уровнях власти, не исключая руководство страны. Цифровизация, цифровая трансформация вошли в число национальных целей страны и стали определяться и интенсивно развиваться по различным отраслям и сферам как стратегические направления их развития, в том числе в государственном управлении.

Так, в последнем, принятом в 2024 г., майском указе Президента РФ, актуализировавшем национальные цели на период до 2036 г., в качестве одной из них определена «цифровая трансформация государственного и муниципального управления, экономики и социальной сферы» (п. «ж» п. 1), и Правительству РФ для ее реализации поручено принять новый национальный проект «Экономика данных и цифровая трансформация государства» (пп. «а» п. 9)[4]. Ранее, в предыдущем указе, определявшем национальные цели на период до 2030 г., одной из них также была названа цифровая трансформация (пп. «д» п.1), достижение которой характеризовала «"цифровая зрелость" ключевых отраслей экономики и социальной сферы, а также государственного управления» (пп. «д» п. 2)[5]. А в соответствии с еще более ранним «майским указом» 2018 г.[6] к национальной цели было отнесено «обеспечение ускоренного внедрения цифровых технологий в экономике и социальной сфере» (п. «ж» п. 1), а в качестве национальной программы была названа «цифровая экономика» (п. «б» п. 2), которая впоследствии, после ее утверждения, включила в свое содержание федеральный проект «Цифровое государственное управление»[7].

Также Правительством РФ отдельно определено стратегическое направление цифровой трансформации в области госу-

4. Указ Президента РФ от 7 мая 2024 г. № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» // СПС «Гарант».

5. Указ Президента РФ от 21 июля 2020 г. № 474 «О национальных целях развития Российской Федерации на период до 2030 года» // СПС «Гарант».

6. Указ Президента РФ от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» // СПС «Гарант».

7. Паспорт национальной программы «Цифровая экономика Российской Федерации», утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам 24 декабря 2018 г. № 16; Паспорт федерального проекта «Цифровое государственное управление, утв. президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности, протокол от 28.05.2019 № 9) // СПС «Гарант».

дарственного управления – сначала в 2018 г., а затем в 2024 г.[8], в задачи которого входит формирование единого информационного пространства в области внутриведомственного и межведомственного электронного документооборота, формирование модели бесперебойного функционирования государственных информационных систем с использованием государственной единой облачной платформы, повышение качества и удобства предоставляемых онлайн государственных услуг, а также расширение их количества, обеспечение внедрения искусственного интеллекта в государственном управлении и др.

На сегодняшний день создаваемая в ходе реализации вышеуказанных документов цифровая среда уже характеризуется масштабным развитием инфраструктуры электронного правительства, подразумевающей переход к предоставлению государственных услуг в электронном виде, появление у граждан ранее неизвестных электронных прав (например, права «на забвение», права на ограничение обработки данных и др.), а также институтов электронной демократии [*Головин, Большакова, Наумова*, 2020. С. 4].

Процессы цифровизации нашли свое отражение даже на уровне Конституции РФ по результатам конституционной реформы 2020 г. – в новой редакции появились и были отнесены к исключительному ведению РФ «информационные технологии» и «обеспечение безопасности личности, общества и государства при применении информационных технологий, обороте цифровых данных» (пп. «и», «м» ст. 71)[9]. Введение государством данных вопросов в предмет исключительного ведения свидетельствует о значении, придаваемом государством вопросам реализации цифровых трансформационных процессов, их институциональному обеспечению и безопасности.

8. Распоряжение Правительства РФ от 22 октября 2021 г. № 2998-р «Об утверждении стратегического направления в области цифровой трансформации государственного управления»; Распоряжение Правительства Российской Федерации от 16 марта 2024 г. № 637-р «Об утверждении стратегического направления в области цифровой трансформации государственного управления» // СПС «Гарант».

9. Конституция РФ, принятая всенародным голосованием 12 декабря 1993 г. (редакция в соответствии с Законом РФ о поправке к Конституции РФ от 14 марта 2020 г. № 1-ФКЗ «О совершенствовании регулирования отдельных вопросов организации и функционирования публичной власти») // СПС «Гарант».

Недавно, в послании Президента РФ от 29 февраля 2024 г., а затем в п. 8 Перечня поручений по его реализации Правительству РФ поставлена новая задача по подготовке национального проекта – «Экономика данных и цифровая трансформация государства». На его реализацию планируется направить в предстоящие шесть лет не менее 700 млрд руб., результатом чего должно стать формирование к 2030 г. цифровых платформ во всех ключевых отраслях экономики и социальной сферы, а также в сфере государственного управления[10]. Проект должен прийти на смену национальной программе «Цифровая экономика РФ» и включить в свой состав федеральный проект «Цифровое государственное управление», паспорт национального проекта был презентован 4 сентября 2024 г. на Восточном экономическом форуме (но к настоящему моменту еще не утвержден)[11].

Отметим, что *применение информационно-коммуникационных технологий* (далее – ИКТ) в целях развития системы государственного управления началось достаточно давно. Первая программа «Электронная Россия» появилась еще в 2002 г.[12] и была направлена на повышение эффективности государственного управления путем использования ИКТ, оперативности предоставления государственных и муниципальных услуг и полноты контроля за деятельностью государственных органов. Задачи программы концентрировались на развитии инфраструктуры электронного правительства и переходе к предоставлению государственных услуг и исполнению государственных функций в электронном виде, что привело к созданию Единого портала государственных услуг в 2009 г.

Затем начался этап, направленный на формирование электронного правительства в рамках государственной программы

10. Перечень поручений по реализации Послания Президента РФ Федеральному Собранию РФ, утв. Президентом РФ 30 марта 2024 г. № Пр-616) // СПС «Гарант».

11. На ВЭФ представили нацпроект «Экономика данных и цифровая трансформация государства» / Ежедневное онлайн-издание D-russia.ru. 04.09.2024 / URL: https://d-russia.ru/na-vjef-predstavili-nacproekt-jekonomika-dannyh-i-cifrovaja-transformacija-gosudarstva.html https://tass.ru/ekonomika/11562013 (дата обращения: 12.11.2024).

12. Постановление Правительства РФ от 28 января 2002 г. № 65 «О федеральной целевой программе «Электронная Россия (2002–2010 годы)» // СПС «Гарант».

«Информационное общество (2011–2020 годы)»[13] и предполагающий *цифровизацию* государственного управления. Это подразумевало обеспечение полного перехода на предоставление государственных и муниципальных услуг в электронном виде, развитие системы «одного окна», создание Единой системы межведомственного электронного взаимодействия (СМЭВ) и системы электронного документооборота в государственных органах, а также обеспечение открытого доступа к информации об их деятельности (*Конкуренция в цифровую эпоху...*, 2018. С. 59–60). В результате, как констатируется в Стратегии развития информационного общества в Российской Федерации на 2017–2030 гг. (п. 11): «информационные и коммуникационные технологии стали частью современных управленческих систем во всех отраслях экономики, сферах государственного управления, обороны страны, безопасности государства и обеспечения правопорядка»[14].

Процесс распространения ИКТ в системе государственного управления становится все более масштабным, затрагивающим все уровни власти, практически все их задачи и функции, и переходит в современных условиях от цифровизации государственных органов, внедрения электронного документооборота и предоставления государственных услуг на основе реестровой модели учета (т.е. от «электронного правительства») уже к цифровому государственному управлению, основанному на применении «сквозных» цифровых технологий. К последним относят: большие данные, нейротехнологии и искусственный интеллект, системы распределенного реестра (блокчейн), квантовые технологии, промышленный интернет, новые производственные технологии; компоненты робототехники и сенсорики, технологии беспроводной связи; технологии виртуальной и дополненной реальностей[15].

13. Постановление Правительства РФ от 15 апреля 2014 г. № 313 «Об утверждении государственной программы Российской Федерации «Информационное общество (2011–2020 годы)» // СПС «Гарант».

14. Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 гг.» // СПС «Гарант».

15. Постановление Правительства РФ от 3 мая 2019 г. № 551 «О государственной поддержке программ деятельности лидирующих исследовательских центров, реализуемых российскими организациями в целях обеспечения разработки и реализации дорожных карт развития перспективных «сквозных» цифровых технологий»; Паспорт федерального проекта «Цифровые технологии», утв. президиумом Правительственной комиссии по цифровому развитию, использованию информаци-

Такой переход осуществляется посредством реализации комплексной *цифровой трансформации* государственного управления, которая подразумевает полноценное электронное взаимодействие государства с гражданами и организациями, организацию работы государственных органов не с оцифрованными, а с цифровыми документами и данными. Это стало возможным с применением вышеуказанных «сквозных» цифровых технологий, потенциал которых позволяет обеспечить модернизацию значительной части процессов государственного управления, включая выработку государственной политики и управленческих решений в различных сферах, нормотворчества, прогнозирования и т.д.

Формируемая в результате цифровой трансформации цифровая среда обусловлена, таким образом, информационным сетевым обменом, подразумевающим перевод в цифровую форму совершения всех коммуникаций и операций (*Право цифровой среды*, 2022. С. 37). В частности, согласно принятой Концепции трансформации услуг в формат 24/7 абсолютное большинство государственных и муниципальных услуг до конца 2023 г. должно быть переведено публичными органами власти и внебюджетными фондами в электронный вид для их предоставления без необходимости личного присутствия граждан. Реализация указанной Концепции осуществляется путем разработки и внедрения цифровых административных регламентов при методической поддержке Минэкономразвития России[16].

Исследователи отмечают, что процессы цифровой трансформации, затрагивающие многие аспекты государственного строительства, с неизбежностью повлекут за собой пересмотр роли государства и формирования нового общественного порядка, основанного на свободном информационном обмене, потребуют новых подходов к реализации задач органов власти и государственному управлению в целом [*Цифровая трансформация и государственное управление*, 2022. С. XIV–XVI].

онных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (протокол от 28 мая 2019 г. № 9)) // СПС «Гарант».

16. Распоряжение Правительства РФ от 11 апреля 2022 г. № 837-р «Об утверждении Концепции перехода к предоставлению 24 часа в сутки 7 дней в неделю абсолютного большинства государственных и муниципальных услуг без необходимости личного присутствия граждан» // СПС «Гарант».

Процессы внедрения возможностей цифровизации в государственное управление подразумевают развитие механизмов т.н. «гибкого управления», способных адаптироваться к изменениям условий, а также восприимчивых к обратной связи от граждан и организаций. В этой связи следует упомянуть о рассмотрении в исследованиях Института экономики РАН перспектив перехода к новой парадигме государственного управления, которая как раз предполагает активное участие общества в разработке и выполнении социально-экономических задач, в принятии государством управленческих решений [*Смотрицкая, Черных, Сазонова*, 2022] и для которой реализуемая цифровизация государственного управления создает необходимые условия.

Однако полученные впечатляющие результаты применения цифровых технологий в государственном управлении, экономические, социальные и политические выгоды от стремительного их использования необходимо обязательно соотносить с сопутствующими цифровой трансформации рисками и возникающими в этой связи проблемами обеспечения безопасности цифровой среды. Речь идет как о безопасности оборота цифровой информации, содержащейся прежде всего в государственных информационных системах, так и обеспечении безопасности личности и общества, учете их интересов и обеспечении прав в ходе цифровой трансформации.

II

Безопасность цифровой среды и проблемы ее обеспечения в рамках цифровой трансформации государственного управления

Потенциал освоения и применения цифровых технологий в государственном управлении чрезвычайно высок, однако нельзя не принимать во внимание негативные стороны цифровой трансформации, на который указывают противники ее стремительного развития, отмечая потенциальные и реальные угрозы [*Кузякин Ю.П., Кузякин С.В.*, 2023. С. 55].

Несмотря на множественность изданных нормативных актов, обеспечивающих процессы цифровой трансформации государственного управления, вопрос о сопровождающих их проблемах обеспечения безопасности цифровой среды, как правило, не поднимается или декларируется только на уровне принципов (недопустимости нанесения вреда интересам личности, общества и государства и обеспечение защиты прав и свобод граждан—потребителей цифровых технологий, неприемлемости распространения информации ограниченного доступа и др.). И если в концептуальных документах и обозначаются отдельно риски и угрозы, то они касаются возможного негативного влияния на реализацию самих цифровых инициатив. Таков, например, раздел «Риски стратегического направления» в «Стратегическом направлении в области цифровой трансформации государственного управления», в котором указывается на отсутствие технологий, необходимых для развития новой модели государственного управления, недостаточность спроса на получение государственных услуг в электронном виде из-за недоверия граждан, сложности в интеграции информационных систем и координации мероприятий, необходимость дополнительного финансирования.

Указание на проблемы цифровой трансформации часто встречается среди правоведов, но ими же констатируется, что правовое регулирование, как и правовая наука, оказались не готовы к столь масштабной цифровизации и ее теоретического осмысления

пока не произошло. Длительное время, например, не разрабатывались теоретические аспекты цифровой трансформации, не проводился анализ принимаемых нормативно-правовых установлений и адаптации иностранной терминологии, не был поставлен вопрос и концептуально осмыслена необходимость принятия специализированного нормативного акта, регулирующего различные аспекты правоотношений с использованием цифровых технологий. В итоге сложившемуся правовому регулированию свойственно отсутствие единства, внутренняя противоречивость и мозаичность [*Цифровая трансформация и государственное управление*, 2022. С. 222].

При этом Стратегия национальной безопасности РФ[17] выделяет информационную безопасность в качестве стратегического национального приоритета, а в качестве национального интереса – развитие безопасного информационного пространства.

В 2021 г. Президент РФ по итогам заседания Совета при Президенте РФ по развитию гражданского общества и правам человека (СПЧ), во многом посвященного переходу к новому измерению и форматам взаимодействия государства и общества в условиях пандемии и обсуждению в т.ч. преимуществ и рисков цифровизации, поручил Правительству РФ и СПЧ разработать концепцию обеспечения защиты прав и свобод человека и гражданина в цифровом пространстве и план мероприятий («дорожную карту») по ее реализации, включающих меры по обучению навыкам информационной безопасности и цифровой гигиены (пп. «г» п. 3 Перечня поручений Президента РФ от 28 января 2021 г. № Пр-133).

СПЧ разработал проект такой концепции и представил ее в Правительство РФ вместе с аналитическим докладом «Цифровая трансформация и защита прав граждан в цифровом пространстве» [*Цифровая трансформация и защита прав граждан...*, 2021], в котором рассмотрел и оценил проблемы и риски форсированной цифровой трансформации. Данный доклад можно рассматривать как наиболее полное исследование проблем внедрения современных цифровых технологий с точки зрения обеспечения безопасности и учета интересов личности и общества.

17. Утверждена Указом Президента РФ от 2 июля 2021 г. № 400 // СПС «Гарант».

Концепция СПЧ по обеспечению защиты прав и свобод человека и гражданина в цифровом пространстве, однако, не была учтена и одобрена, вероятно, потому что предусматривала запрет собирать обширные базы данных о гражданах как компаниям, так и государственным органам, а также формировать интегральные базы данных (путем объединения имеющихся баз), что шло вразрез с концепцией развития платного доступа частных компаний к государственным информационным системам [*Королев, Лебедева, Старикова*, 2021], а также тенденцией по развитию обмена данными между государственными информационными системами (ГИС), переходу к созданию «гососзера» данных – единой государственной информационной системы (ГИС), объединяющей потоки обезличенных данных государственных органов (подробнее об этом см. ниже).

В своем докладе СПЧ указывает на неконтролируемое и сверхбыстрое развитие цифровой среды и выделяет в качестве основного недостатка отечественной цифровизации отсутствие должного внимания к «защите ключевых конституционных прав граждан, без прогнозирования возможных социальных рисков и без сценарного моделирования последствий цифровизации для будущего людей» [Там же. С. 4, 9].

СПЧ также определяет особые факторы риска для развития цифровой среды, которые заключаются в:

- сверхбыстром, экспоненциальном развитии цифровой среды, увеличивающем ее непредсказуемость;
- постоянно возрастающей сложности цифровой среды [Там же. С. 19–20].

Развитие применения в государственном управлении интеллектуальных систем поддержки решений представляет собой одну из значимых проблем в области развития цифровой среды. Речь идет о внедрении технологий искусственного интеллекта (ИИ), которые постепенно перестают рассматриваться в качестве вспомогательного инструмента поддержки в процессах выработки и принятия управленческих решений и приобретают автономность и самостоятельное значение.

Среди цифровых инноваций именно ИИ является наиболее дискутируемой технологией, обремененной серьезными риска-

ми применения, но при этом активно развивающейся и внедряемой в сфере государственного управления [*Талапина Э.В.*, 2024. С. 145].

Так, технологии ИИ активно применяются при оказании государственных услуг. Минцифры России анонсировал введение в текущем году на Едином портале государственных и муниципальных услуг технологии генерации ответа (чат-бота на основе технологии GPT) по аналогии с GigaChat Сбербанка России и YandexGPT. Электронный помощник предназначен упростить ориентирование пользователей в имеющихся электронных сервисах и будет осуществлять коммуникацию с помощью коротких и понятных ответов, «сокращая путь пользователя», а также генерировать ответ из базы знаний портала под конкретную жизненную ситуацию. Возможности чат-бота включают самостоятельное заполнение заявлений на получение документов, справок и выписок с дальнейшим подтверждением их правильности пользователем[18].

Настораживает в этом предложении то, что Минцифры России в качестве направления дальнейшего развития применения ИИ констатирует не просто постепенный переход к проактивной системе оказания услуг, которые будут оказываться автоматически, но их реализацию даже без обращения пользователя и фактически в отсутствие его спроса на нее[19].

Следует отметить, что элементы такой системы в настоящее время уже внедрены. Так, с 1 января 2022 г. выплаты по временной нетрудоспособности либо по беременности и родам граждане получают автоматически на основании электронного больничного листа, который все медицинские организации размещают в федеральной ГИС «Соцстрах»[20]. В 2020 г. выдача сертификата на материнский (семейный) капитал начала оформляться Пенсионным фондом в проактивном режиме. Для получения новой

18. *Гурьянов С.* Одному боту известно: технологии GPT внедрят в работу «Госуслуг» / Газета «Известия». 06.02.2024 / URL: https://iz.ru/1645325/sergei-gurianov/odnomu-botu-izvestno-tekhnologii-gpt-vnedriat-v-rabotu-gosuslug (дата обращения: 12.11.2024).

19. Там же.

20. Постановление Правительства РФ от 23 ноября 2021 г. № 2010 «Об утверждении Правил получения Фондом социального страхования Российской Федерации сведений и документов, необходимых для назначения и выплаты пособий по временной нетрудоспособности, по беременности и родам, единовременного пособия при рождении ребенка, ежемесячного пособия по уходу за ребенком» // СПС «Гарант».

выплаты семьям, имеющим детей школьного возраста[21], подходящие по критериям пользователи Единого портала государственных и муниципальных услуг автоматически получили уже заполненное заявление, которое им оставалось только проверить и дополнить реквизитами своего счета.

В последнем Послании Президента РФ Федеральному Собранию РФ указывается на необходимость дальнейшего развития государственных услуг в электронном виде и их предоставление «гражданам, бизнесу проактивно, в удобном формате с максимально быстрым получением результата»[22].

Безусловно, проактивный принцип (когда государство на основе имеющейся у него информации анализирует, кому может быть предоставлена та или иная услуга) существенно упрощает процессы предоставления и получения услуг, но одновременно он предполагает агрегирование данных о гражданине в единый источник с последующим отслеживанием происходящих в его жизни событий без какого-либо его уведомления и согласия, что нарушает право на неприкосновенность частной жизни и потенциально может привести к необоснованному вмешательству в личную жизнь.

С развитием применения технологий ИИ происходит не только адаптация государственных услуг под запросы населения, но также иных полномочий и функций государства – в судопроизводстве и в правотворчестве [*Залоило*, 2021]. В отношении правотворчества исследователями прогнозируется появление индивидуальных правовых установлений (набора прав, обязанностей и ответственности), выработанных автономными алгоритмами под конкретного человека и адаптированных под него, на основе доступных данных о гражданах и установленных ИИ различий между конкретными людьми, с возможным переходом в будущем даже к персонализированному праву [*Харитонова, Ци Сунь*, 2023].

В отношении применения ИИ в судопроизводстве в научной дискуссии все же указывается на неприемлемость его полноценного использования для отправления правосудия в связи с алгоритмической непрозрачностью выводов, сделанных интеллектуаль-

21. Указ Президента РФ от 2 июля 2021 г. № 396 «О единовременной выплате семьям, имеющим детей» // СПС «Гарант».

22. Послание Президента РФ Федеральному Собранию РФ от 29 февраля 2024 г. // СПС «Гарант».

ной системой [*Евсиков К.С.*, 2022. С. 125]. Эффект «черного ящика» создает сложности для оспаривания таких решений гражданами и организациями, в отношении которых они были приняты, в т.ч. учитывая машинное обучение нейросетей, а значит, невозможность проконтролировать возникающие у ИИ причинно-следственные связи. С одной стороны, с применением ИИ снижается влияние на принятие решений «человеческого фактора», но с другой — вместо закона начинают действовать правила заложенного алгоритма, что является абсолютно неприемлемым, открывает возможности для различного рода манипуляций и дискриминации в случае ошибочных обучающих данных, а также при внешнем вмешательстве, которое тоже нельзя исключать — применение скрытых «закладок», искажений, модификаций и подмен.

В качестве актуального примера можно привести постановку данной проблемы в вышеуказанном докладе СПЧ применительно к отказам в банковских кредитах в случаях, когда кредитоспособность заемщика анализируется системами ИИ. В докладе указывается, что такой отказ «происходит мгновенно, без объяснений, притом с занесением этого факта в системы кредитной истории», и оспорить это решение и исправить запись обычно возможности не имеется [*Цифровая трансформация и защита прав граждан...*, 2021. С. 48–49]. Замена же человеческого усмотрения машинными алгоритмами при принятии решений в системе государственного управления повлечет гораздо более серьезные последствия для граждан и организаций.

Также следует отметить, что в настоящее время вопросы применения искусственного интеллекта в различных сферах во многом остаются неурегулированными и специфика его использования в законодательстве, как правило, не учитывается. Данной технологии уделяется много внимания в документах стратегического планирования[23], однако концептуального уровня

23. См. Национальную стратегию развития технологий искусственного интеллекта на период до 2030 г. (утв. Указом Президента РФ от 10 октября 2019 г. № 490), Концепцию развития регулирования отношений в сфере технологий искусственного интеллекта и робототехнике до 2024 г. (утв. Распоряжением Правительства РФ от 19 августа 2020 г. № 2129-р), положения Стратегии научно-технологического развития РФ (утв. Указом Президента РФ от 28 февраля 2024 г. № 145), Стратегию развития информационного общества в РФ на 2017–2030 гг. (утв. Указом Президента РФ от 9 мая 2017 г. № 203) и др. // СПС «Гарант.

проработки с учетом интенсификации использования ИИ явно недостаточно.

В этой связи важно отметить, что еще не сложилось единого подхода к правовому статусу ИИ, как и понимания пределов использования системы искусственного интеллекта. Эти вопросы вызывают многочисленные споры среди исследователей. Наибольший интерес, на наш взгляд, представляет обсуждение возможности признания искусственного интеллекта субъектом права с отнесением его в правовом смысле к личности (т.н. «электронной личности») и наделением соответствующими правами и обязанностями, возможностью привлечения к ответственности (например, с рассмотрением робота, наделенного ИИ, в качестве работника) [*Власова В.Ю., Ястребова А.И.,* 2024. С. 65–66; *Юэ Цян, Кичик К.В.*, 2023. С. 20].

Такая позиция основана в том числе на определении ИИ в Национальной стратегии развития технологий ИИ, указывающем, что ИИ позволяет «имитировать когнитивные функции человека» и «получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их» (пп. «а» п. 5).

Все большее распространение такой позиции вызвало крайне отрицательную реакцию у Председателя Конституционного Суда РФ В.Д. Зорькина, опубликовавшего по данному вопросу специальную статью. Он предостерегает от стирания грани между искусственным и человеческим интеллектом, отмечая, что такая постановка вопроса является вторжением «в самое сокровенное человеческой идентичности», а ИИ не является носителем критически важных составляющих личности, в т.ч. ценностей и личных интересов, и его мыслительный процесс никогда не будет подобен человеческому. Также он отметил, что законодательное регулирование обязано возвести «глубоко эшелонированную оборону от тех немалых рисков, которыми чревато использование искусственного интеллекта», который «можно с уверенностью отнести к деятельности, связанной с источниками повышенной опасности», что требует повышенного публичного контроля, включая введение обязательной сертификации для применения ИИ в разных сферах [*Зорькин В.Д.*, 2024].

Укажем, что, по мнению технических специалистов, ИИ не обладает смысловым восприятием и способностью генерировать

и накапливать высокие абстракции. ИИ вычисляет, но самостоятельного понимания и целеполагания не имеет, оставаясь вычислительной мощностью со всеми вытекающими из этого ограничениями [*Чувильдеев В.Н.*, 2019]. А значит, о его субъектности говорить пока преждевременно.

В Национальной стратегии развития ИИ указывается, что отсутствие понимания того, как искусственный интеллект достигает результатов, является одной из причин низкого уровня доверия к технологиям ИИ (п. 8).

Согласно опросу ВЦИОМ 2022 г., жителям России в целом свойственно доверие к технологиям ИИ, однако почти треть (32%) им не доверяют, что связывается ими с возможностью сбоев в работе ИИ, угрозами утечки собранных данных, их использованием в корыстных целях и риском отсутствия ответственности за принятые с помощью ИИ решений[24]. Всероссийский опрос НАФИ 2023 г. показал, что большинство респондентов считают, что технологии ИИ приносят людям пользу (78%), при этом 54% опрошенных согласны с тем, что риски неправомерного использования технологий ИИ будут возрастать, и только 42% полагают, что защита данных будет осуществляться надежно и риски утечки будут снижаться[25].

Результаты международного опроса, проведенного в конце 2023 г. Ассоциацией независимых исследовательских агентств Gallup International, показал, что в России респонденты настроены скептично по отношению к использованию ИИ. 34% участников опроса уверены, что ИИ несет больше проблем, чем возможностей (в обратном уверены 19%). Почти половина (47%) опрошенных сочли себя недостаточно осведомленными в данном вопросе или затруднились с ответом[26].

24. «Россияне назвали свои главные страхи перед искусственным интеллектом» / РБК. 28.12.2022 / URL: https://www.rbc.ru/society/28/12/2022/63ab45de9a7947664c3ef893 (дата обращения: 12.11.2024).

25. Результаты всероссийского онлайн-опроса «Отношение к технологиям искусственного интеллекта» / НАФИ. 2023 / URL: https://ai.gov.ru/knowledgebase/infrastruktura-ii/2023_rezulytaty_oprosa_otnoshenie_k_tehnologiyam_iskusstvennogo_intellekta_nafi_nacionalynye_prioritety/ (дата обращения: 12.11.2024).

26. «Искусственный интеллект: угроза или возможности – мнения разделились» / Портал «Ромир». 06.05.2024 / URL: https://romir.ru/studies/iskusstvennyy-intellekt-ugroza-ili-vozmojnosti--mneniya-razdelilis (дата обращения: 12.11.2024).

Опрос, проведенный ВЦИОМ в 2023 г., также показал скептичное отношение населения к повсеместному использованию технологий ИИ: только 18% опрошенных выступают за полномасштабное их внедрение, а большинство (67%) считают, что ИИ возможно использовать только в некоторых сферах (67%), а 11% не видят необходимости в применении ИИ. При этом 79% полагают необходимым проведение с участием человека оценки этичности продуктов и решений, созданных с помощью технологий ИИ, а 69% и вовсе выступают за обязательность маркировки созданных с применением ИИ цифрового контента и продуктов. Примечательно, что для каждого четвертого опрошенного сферой, где возникают этические вопросы применения ИИ, является государственное управление (25%), лидируют по данному вопросу сферы здравоохранения и образования (34% и 30%, соответственно)[27].

Еще одной значимой проблемой является применение в государственном управлении цифрового профилирования, которое рассматривается в качестве значимого компонента цифровой среды и под которым понимается систематический и целенаправленный процесс сбора, фиксации и классификации данных в информационных системах органов публичной власти, относящихся к отдельным лицам или социальным группам с использованием алгоритмических механизмов в целях их предоставления с согласия соответствующих граждан или юридических лиц субъектам, запросившим доступ к этим сведениям [*Цифровая трансформация и защита прав граждан...*, 2021. С. 24; *Степанов, Басангов*, 2024. С. 59-60; *Виноградова Е.В., Полякова Т.А., Минбалеев А.В.* , 2021. С. 8.].

Национальная программа «Цифровая экономика Российской Федерации» предусматривает создание платформы идентификации, включающей в т.ч. цифровые профили гражданина и юридического лица[28] (п. 1.10). Основой для организации такого профилирования служит Единый портал государственных и муниципальных услуг совместно с Единой системой идентификации и аутентифи-

27. Этика в эпоху роботизации: результаты опроса / ВЦИОМ. 12.09.2023 / URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/ehtika-v-ehpokhu-robotizacii-ishchem-balans (дата обращения: 12.11.2024).

28. Паспорт Программы утвержден президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам (протокол от 4 июня 2019 г. № 7).

кации (ЕСИА), обеспечивающей вход на портал. Использование цифрового профиля связано с предоставлением доступа третьим лицам (вне контура государственного управления) к сведениям, содержащимся в ЕСИА и иных государственных информационных системах. Минцифры России в этой связи разработаны сценарии взаимодействия с цифровым профилем и правила получения из него данных[29].

В рамках цифрового профилирования сегодня происходит централизация находящихся в распоряжении государственных органов данных в единой инфраструктуре с созданием национальной системы управления данными[30]. Благодаря цифровому профилированию пользователям предлагается все более широкий перечень услуг, уже не только государственных: предоставление кредита, получение банковской карты, оформление страховки и т.д. При этом постепенно увеличивается круг субъектов, получающих доступ к их персональным сведениям.

В настоящее время возможность получить доступ к данным ЕСИА с согласия граждан имеют кредитные, страховые и микрофинансовые организации, операторы связи и др., а также некоторые маркет-плейсы (ООО «Вайлдберриз», ООО «Интернет Решения» (Ozon)), владельцы информационных ресурсов поиска сотрудников и работы (ООО «Яндекс», ООО «ВКонтакте», ООО «КЕХ еКоммерц», (Авито.ру), ООО «Хэдхантер») и др.

29. Сценарии использования инфраструктуры Цифрового профиля Минцифры России. Верс. 1.37. URL: https://digital.gov.ru/ru/documents/7554/ дата обращения: 12.11.2024).

30. Постановление Правительства РФ от 14 мая 2021 г. № 733 «Об утверждении Положения о федеральной государственной информационной системе «Единая информационная платформа национальной системы управления данными» и о внесении изменений в некоторые акты Правительства Российской Федерации» // СПС «Гарант»; Постановление Правительства РФ от 27 марта 2021 г. №453 «О проведении эксперимента по осуществлению идентификации и аутентификации с использованием федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» пользователей социальных сетей, потребителей (заказчиков) и продавцов (исполнителей), иных сторон договоров при использовании ими информационных ресурсов в информационно-телекоммуникационной сети «Интернет», предоставляющих возможность ознакомиться с предложением о заключении договора купли-продажи товара (выполнения работ, оказания услуг), заключить такой договор, в том числе агрегаторов информации о товарах (услугах), а также пользователей информационных ресурсов поиска сотрудников и работы» // СПС «Гарант».

Московская ГИС (портал mos.ru) является еще более актуальным примером реализации цифрового профилирования, поскольку уже сейчас содержит обширную персонализированную базу данных о практически каждом москвиче[31]. Ее отличительная особенность состоит в обширном перечне предлагаемых системой различных услуг (как городских, так и сторонних), для получения которых пользователям самостоятельно предлагается ввести свои данные: о фактическом месте жительства, месте работы, водительском удостоверении, карте «Тройка», номере своего читательского билета в городскую библиотеку, данные о питомцах и т.д. Возможен вход на портал через другие учетные записи (Госуслуги, Sber ID, Tinkoff ID), и в этом случае данные этой учетной записи добавляются в московскую ГИС автоматически [*Современные институты государственного управления...*, 2024. С. 154].

Явно обозначившаяся тенденция к концентрации персональных данных в единых государственных системах, а также развитие межведомственного обмена данными и расширение доступа к персонализированным данным все более широкого круга лиц вызывает обоснованные опасения в утрате контроля за их распространением.

И в этой связи актуальной представляется задача по ограничению возможностей использования данных, получаемых из цифровых профилей, в целях, не связанных с изначальной целью получения доступа к этим данным, в том числе в коммерческих целях [*Мочалов А.Н.,* 2021. С. 99].

Одной из актуальных проблем обеспечения цифровой безопасности является защищенность данных в ГИС, особенно с учетом того что процессы цифровой трансформации подразумевают объединение самих ГИС, развитие между ними обмена информацией, что подразумевает увеличение объема обрабатываемых в них данных.

Необходимость безопасности таких данных предполагает высокий уровень их защищенности, поскольку, к сожалению, обеспечение абсолютной защищенности обрабатываемой в ГИС информации не соответствует возможностям современных инфор-

31. Постановление Правительства Москвы от 9 февраля 2021 г. № 102-ПП «О государственной информационной системе «Система централизованного ведения профиля заявителя» // СПС «Гарант».

мационных систем [*Головин, Большакова, Наумова*, 2020. С. 5] с учетом широкого спектра потенциальных угроз:

● различного рода внешних посягательств (несанкционированного доступа, искажения, копирования, повреждения, уничтожения и хищения данных как в самих ГИС, так и в виде перехвата информации в сетях передачи данных). Хищение данных в дальнейшем приводит к совершению мошеннических операций, вымогательству и иному неправомерному их использованию. Искажение, повреждение или уничтожение данных способно нанести пользователям прямой экономический ущерб;

● искажения или потери данных в случае программных или аппаратных сбоев, что также является чувствительным для пользователей, поскольку даже незначительный сбой способен привести к искажению информации. А с учетом перехода к электронному документообороту отсутствие аналогичных данных в бумажном виде может привести и к невозможности восстановления информации в исходном виде.

В отчете ВЭФ о глобальных рисках[32] (The Global Risks Report, 2023) отмечается широкое распространение киберпреступности и отсутствие кибербезопасности (в т.ч. нарушение конфиденциальности, мошенничество или кража данных, кибершпионаж). Среди общемировых угроз она занимает 8 место по степени значимости как в краткосрочной, так и в долгосрочной перспективе. Также ВЭФ прогнозируется, что эта угроза будет оставаться постоянной проблемой.

В России постепенно ужесточается ответственность за совершение правонарушений в сфере обработки информации, в т.ч. увеличиваются штрафы для организаций, допускающих утечку персональных данных. Кроме того, с 2017 г. в России развивается законодательство о безопасности критической информационной инфраструктуры[33], направленное на обеспечение защищенности и устойчивое функционирование значимых информационных систем (в т.ч. ГИС) в опорных для экономики и безопасности предприя-

32. Аналитический доклад о глобальных рисках за 2023 г. – URL: https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf (дата обращения: 12.11.2024).

33. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // СПС «Гарант».

тиях и организациях, а также в государственных органах. Данный механизм достаточно сложен и ориентирован на прохождение сложных процедур закупок программного обеспечения по согласованию с уполномоченным органом, проведение аттестации оборудования и т.п.

Тем не менее, несмотря на попытки законодателя обеспечить защищенность данных, по информации Роскомнадзора (РКН), утечки данных увеличиваются из года в год, фиксируется рост теневого спроса на различные группы данных граждан. В 2023 г. РКН зафиксировано 168 утечек данных с попаданием более 300 млн записей о гражданах в открытый доступ. В судах при этом рассмотрено только 87 протоколов о нарушениях с назначением административных штрафов в размере более 4,6 млн руб. В 2022 г. – 140 утечек и 66 протоколов на сумму более 2,4 млн руб.[34]. В сентябре 2023 г. в социальных сетях обсуждалась масштабная утечка персональных данных, в том числе, судя по ее характеру, из баз государственных ресурсов (в Telegram были обнаружены чат-боты, через которых можно было получить досье практически на любого гражданина, включая телефоны, медицинские данные и т.п.). В феврале 2024 г., по данным Роскомнадзора, произошла самая масштабная единовременная утечка данных – около 500 млн записей[35].

Однако установить, имеют ли отношение обнародованные утечки к ГИС, как правило, можно только по косвенным признакам, поскольку РКН не всегда раскрывает операторов таких данных, особенно если ими, предположительно, являются государственные органы. Вероятно, это обусловлено позицией ведомства по недопустимости нарушения уровня доверия пользователей к таким системам.

Как приведенные выше результаты административного судопроизводства, статистика уголовного судопроизводства также демонстрирует, что действующее регулирование в части установления и привлечения к ответственности виновных в произошед-

34. «Роскомнадзор зафиксировал 168 утечек данных в 2023 году» / Портал «Право.ru». 12.11.2024 / URL: https://pravo.ru/news/250809/ (дата обращения: 09.06.2024).

35. «Роскомнадзор сообщил об утечке 500 млн данных о россиянах за один раз» / РБК. 23.02.2024 / URL: https://www.rbc.ru/rbcfreenews/65d7ef3d9a7947d8608dbbb3 (дата обращения: 12.11.2024).

ших утечках непропорциональна серьезности и масштабам данной проблемы.

Так, к уголовной ответственности за утечку и кражу персональных данных в последние два года привлечены:

- по ст. 137 УК РФ («Нарушение неприкосновенности частной жизни») в 2021 г. – 235 человек, в 2022 г. – 265 человек, в 2023 г. – 240 человек (из них по составу, предусматривающему использование служебного положения в 2021–2023 гг. – 17, 13 и 16 человек, соответственно);
- по ст. 272 УК РФ («Неправомерный доступ к компьютерной информации») в 2021 г. – 133 человека, в 2022 г. – 179 человек, в 2023 г. – 221 человек;
- по ст. 274 УК РФ («Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей») в 2021 г. – 0 человек, в 2022 и 2023 гг. – по 1 человеку (статья применяется в отношении кражи и утечки данных, т.к. для наступления ответственности необходимо, чтобы нарушение правил эксплуатации повлекло за собой уничтожение, блокирование, модификацию либо копирование компьютерной информации)[36].

Данную статистику интересно соотнести с данными МВД России, которые показывают рост числа преступлений, совершенных с использованием ИКТ или в сфере компьютерной информации. В 2020 г. МВД России впервые зафиксирован взрывной рост числа таких преступлений – на 73,4%, что связывалось с наступлением пандемии короновируса и развитием дистанционных методов ведения деятельности[37]. В дальнейшем наблюдалось сохранение данной тенденции, и в 2023 г. количество противоправных деяний в сфере ИКТ увеличилось на 28,7% (данные за 8 месяцев). Их удельный вес в числе всех преступных посягательств возрос и составил до 32,9%, а по тяжким и особо тяжким – до 56,4%[38]. По итогам

36. Судебная статистика РФ: уголовное судопроизводство. Данные о назначенном наказании по статьям УК / URL: https://sudstat.ru/stats/ug/t/14/s/17 (дата обращения: 12.11.2024).

37. «Интернет-преступность выросла на 91% в 2020 году» / Портал «Право.ру». 20.01.2021 / URL: https://pravo.ru/news/228987/ дата обращения: 12.11.2024).

38. Краткая характеристика состояния преступности в Российской Федерации за январь–август 2023 г. / Портал МВД России. 22.09.2023 / URL: https://мвд.рф/reports/item/41741442/ (дата обращения: 12.11.2024).

2023 г. МВД выявило 677 тыс. IT-преступлений с нанесенным ущербом в размере 156 млрд руб. За семь месяцев 2024 г. зарегистрировано 577 тыс. таких преступлений, из них 437 тыс. мошенничества и хищений, общий размер ущерба составил 99 млрд руб. [39].

По данным экспертно-аналитического центра группы компаний InfoWatch, возглавляемой Н.И. Касперской, в России на 10,1% выросло количество утечек данных в первом полугодии 2024 г. по сравнению с аналогичным периодом 2023 г., скомпрометировано почти 1 млрд единиц персональных данных (986 млн записей). В 2023 г. объем утечек составил 1,12 млрд записей, что почти на 60% выше уровня предыдущего года (в 2022 г. было скомпрометировано 702 млн записей). При этом более 99% утечек в России не случайны и связаны с умышленным воздействием. В качестве основной причины роста утечек называются массированные атаки на российские компании и госсектор, связанные с напряженной геополитической обстановкой и стремлением скомпрометировать как можно больше данных по политическим мотивам (в связи с проведением СВО). Также InfoWatch отмечается, что реальный объем наносимого ущерба существенно недооценен, поскольку более чем в 35% случаях утечек остается неизвестным объем похищенных данных. При этом компания указывает на рост в 2023 г. объема утечек данных из государственных органов до 19,2% в общей структуре утечек, что на 5,3% больше по сравнению с 2022 г. [40]

Приведенная статистика свидетельствует о том, что, несмотря на быстрый рост количества утечек, имеющих характер умышленных противоправных посягательств, ответственность за них наступает, согласно судебной статистике, достаточно редко. На этот факт указывает также президент группы компаний InfoWatch Н.И. Касперская. По ее мнению, это связано с затруднительностью

39. «МВД за семь месяцев зарегистрировало 577 тыс. IT-преступлений» / Газета «Коммерсант». 04.09.2024 / URL: https://www.kommersant.ru/ (дата обращения: 12.11.2024).

40. «В России в первом полугодии утекло почти 1 млрд персональных данных». Портал InfoWatch. 05.09.2024 / URL: https://www.infowatch.ru/company/presscenter/news/v-rossii-v-pervom-polugodii-uteklo-pochti-odin-milliard-personalnykh-dannykh (дата обращения: 12.11.2024); «Аналитики оценили рост утечек персональных данных в России» / РБК. 11.03.2024 / URL: https://www.rbc.ru/society/11/03/2024/65ec41e89a7947dc41bd43f9?from=from_main_8 (дата обращения: 12.11.2024).

выявления источников утечки, а также сложностью обеспечения и высокой стоимостью системной защиты баз данных [*Касперская*, 2023; *Грамматчиков*, 2021].

III

Безопасность цифровой среды и реализация экспериментальных правовых режимов для внедрения цифровых инноваций и технологий искусственного интеллекта (опыт Москвы)

Вопросы обеспечения безопасности цифровой среды интересно рассмотреть в контексте становления и применения в государственном управлении экспериментальных правовых режимов (далее – ЭПР), предназначенных для снятия правовых ограничений в целях ускоренного применения цифровых технологий.

Данная практика получила распространение в связи утверждением в 2018 г. национальной программы «Цифровая экономика Российской Федерации»[41], предусмотревшей в рамках федерального проекта «Нормативное регулирование цифровой среды» (п. 1.18) принятие отдельного федерального закона, регулирующего вопросы создания и функционирования особых правовых режимов в условиях цифровой экономики («регуляторных песочниц»). Паспорт данного федерального проекта[42], в свою очередь, также закрепляет необходимость обеспечения законодательного регулирования вопросов создания и функционирования особых правовых режимов, которое позволит снять первоочередные регуляторные барьеры, препятствующие развитию и функционированию цифровой экономики (п. 1.16).

Реализация данной задачи получила свое воплощение в разработке Минэкономразвития России и последующем принятии Федерального закона от 31 июля 2020 г. №258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» (далее – Закон №258-ФЗ), установившего правовые рамки введения и осуществления всех ЭПР в сфе-

41. Паспорт национальной программы «Цифровая экономика Российской Федерации» утв. президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам 24 декабря 2018 г. № 16 // СПС «Гарант».

42. Утвержден президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (протокол от 28 мая 2019 г. № 9) // СПС «Гарант».

ре цифровых инноваций. Закон № 258-ФЗ установил направления разработки, апробации и внедрения цифровых инноваций в рамках ЭПР (ч. 2 ст. 1), отнеся к ним и сферу государственного управления (одним из направлений является осуществление полномочий и функций государственными органами и органами местного самоуправления), а также, например, медицинскую деятельность, в т.ч. с применением телемедицинских технологий и технологий сбора и обработки сведений о состоянии здоровья и диагнозах граждан, промышленное производство, проектирование, производство и эксплуатацию транспортных средств, в том числе высокоавтоматизированных транспортных средств и беспилотных воздушных судов, и др. В число целей ЭПР входит повышение эффективности государственного или муниципального управления и создание благоприятных условий для разработки и внедрения цифровых инноваций (ст. 3). Перечень технологий, применяемых в рамках ЭПР, также утвержден[43]. Срок действия ЭПР составляет до 3 лет с возможностью продления.

За рубежом применение ЭПР практикуется во многих зарубежных странах, начиная с 2015 г. При этом они преимущественно вводятся именно в области цифровых инноваций и для сферы финансов, однако направления их применения постепенно расширяются [*Ефремов, Добролюбова, Талапина, Южаков*, 2020. С. 15–23].

По информации Минэкономразвития России, в настоящее время реализуются 16 ЭПР, их участниками стали более 190 организаций и один орган власти (Министерство природных ресурсов и экологии Новосибирской области), также в министерстве прорабатывается восемь заявок на ЭПР, шесть из которых планируется ввести до конца 2024 г. Наиболее популярным направлением уже внедренных ЭПР является тестирование беспилотных авиационных систем в различных отраслях (9 ЭПР), также в рамках ЭПР выполняется апробация систем наземного беспилотного транспорта на территории 38 субъектов РФ (4 ЭПР), технологии медицинской деятельности, включающей телемедицину и дистанционную передачу информации о самочувствии медицинским по-

43. См. Постановление Правительства РФ от 28 октября 2020 г. № 1750 // СПС «Гарант».

мощникам (2 ЭПР), предоставление электронных разрешений в сфере государственного управления (1 ЭПР)[44].

Предполагается, что реализация Закона №258-ФЗ позволит создать условия для ускоренного появления и тестирования новых продуктов и услуг в сферах применения цифровых инноваций и приведет к совершенствованию регулирования в этой сфере – как минимум, к выявлению и снятию регуляторных барьеров, препятствующих развитию данных технологий.

Важно, что в отношении видов деятельности, связанных с «высоким риском нанесения ущерба жизненно важным интересам личности, общества и государства, в том числе при защите государственной тайны, обеспечении безопасности критической информационной инфраструктуры РФ, а также в связи с возможным введением в оборот товаров, работ и услуг, оборот которых ограничен или запрещен» установлен запрет на применение ЭПР[45].

Однако говорить о результатах ЭПР пока преждевременно, поскольку согласно реестру все ЭПР вводятся с 2022–2023 г. на 2–3 года и к настоящему моменту срок действия ни одного из них еще не истек.

Тем не менее, наиболее ярким и показательным в рамках цифровой трансформации государственного управления является отдельный блок экспериментального регулирования – ЭПР по внедрению систем искусственного интеллекта, реализуемый в г. Москве.

В Москве многие годы последовательно реализуется масштабная и комплексная система развития инновационных технологий и новаторских решений, выстраивается инновационная экосистема. С момента начала расчета индекса цифровизации город-

44. Реестр ЭПР в сфере цифровых инноваций // Официальный сайт Минэкономразвития России / URL: https://www.economy.gov.ru/material/directions/gosudarstvennoe_upravlenie/normativnoe_regulirovanie_cifrovoy_sredy/eksperimentalnye_pravovye_rezhimy/reestr_eksperimentalnyh_pravovyh_rezhimov/ (дата обращения: 12.11.2024); «Минэкономразвития России: до конца года планируется установить не менее шести экспериментальных правовых режимов» // Официальный сайт Минэкономразвития России. 3 сентября 2024 г. / URL: https://www.economy.gov.ru/material/news/minekonomrazvitiya_do_konca_goda_planiruetsya_ustanovit_ne_menee_shesti_eksperimentalnyh_pravovyh_rezhimov.html (дата обращения: 12.11.2024).

45. Ст. 11 Федерального закона от 2 июля 2021 г. № 331-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «“Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации”».

ского хозяйства «IQ городов»[46], определяющего базовый уровень цифровизации городского хозяйства и эффективность цифровых решений, которые внедряют города и регионы, Москва занимает по нему первое место вот уже пять лет подряд.

Одной из целей реализуемой в Москве с 2011 г. государственной программы «Умный город»[47] (с 2020 г. – переименована, новое название – «Развитие цифровой среды и инноваций») является «централизованное, сквозное и прозрачное управление городом Москвой на основе больших данных и с использованием технологий искусственного интеллекта» с переходом к новому формату городского управления.

В настоящее время городская среда Москвы выступает и активно используется как экспериментальная площадка по тестированию и развитию технологий искусственного интеллекта (далее – ИИ), что стало возможным с принятием вышеуказанного Закона №258-ФЗ и специального Федерального закона от 24 апреля 2020 г. №123-ФЗ[48] (далее – Закон №123-ФЗ), который предусматривает проведение в Москве эксперимента в виде установления на 5 лет с 1 июля 2020 г. ЭПР в целях создания условий для разработки и внедрения технологий ИИ, а также последующего использования результатов его применения. При этом Закон №123-ФЗ не устанавливает областей применения технологий ИИ для проведения эксперимента, и на практике они вводятся по широкому спектру направлений. В рамках ЭПР для субъектов, осуществляющих в Москве разработку технологий ИИ, их внедрение и использование, применяются специальные правовые нормы,

46. Индекс цифровизации городского хозяйства «IQ городов» разработан Минстроем России совместно с МГУ им. М.В. Ломоносова в рамках ведомственного проекта «Умный город», который реализуется в рамках двух национальных проектов – «Жилье и городская среда» и «Цифровая экономика» / URL: https://russiasmartcity.ru/iq https://www.mos.ru/city/projects/national/cifra/ (дата обращения: 12.11.2024); https://www.tadviser.ru/index.php/Статья:Рейтинг_умных_городов_в_России (дата обращения: 12.11.2024).

47. Утверждена постановлением Правительства Москвы от 9 августа 2011 г. №349-ПП // СПС «Гарант».

48. Федеральный закон от 24 апреля 2020 г. №123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных».

в том числе предусматривающие возможность обработки личных данных физических и юридических лиц.

По данным Департамента информационных технологий Москвы, в 2023 г. в столице выполнялась реализация более 90 цифровых проектов с применением ИИ, и некоторые из них отмечены как наиболее эффективные в стране. При этом в Москве осуществляется системная работа по поиску новых направлений и способов применения ИИ для повышения эффективности управления и предоставления максимально качественного сервиса для жителей и предпринимателей (развития «умной городской среды»)[49]. Также московские компании являются активными участниками ЭПР, устанавливаемых в рамках реализации Закона № 258-ФЗ.

И здесь следует согласиться с позицией, обозначающей важность роли потребителей новых технологий и настаивающей на получении от них обратной связи при проведении апробаций в рамках ЭПР, поскольку последующая востребованность цифровых инноваций будет зависеть именно от них. Однако использования защитных мер по отношению к потребителям, в т.ч. в части защиты их прав (поскольку апробация инноваций осуществляется с использованием их данных), законодательство в области ЭПР практически не предусматривает, за исключением возможности страхования ответственности за причинения вреда участников ЭПР [*Громова Е.А.*, 2021. С. 37].

Также следует учитывать, что механизмам предотвращения возникающих рисков безопасности цифровой среды в рамках ЭПР уделяется неоправданно мало внимания. Хотя ЭПР устанавливается для апробации нового регулирования, именно потому что уверенности в должной эффективности снятия правовых ограничений для участников эксперимента не имеется, в том числе в части соблюдения баланса интересов государства, компаний-разработчиков и граждан. В правовых актах из раза в раз указывается на необходимость обеспечения конфиденциальности и безопасности хранения данных, минимизации рисков причинения вреда, недопустимости разработки технологий в целях умышленного причи-

49. «Проекты Москвы вошли в число наиболее эффективных российских практик применения искусственного интеллекта в умных городах» / Портал Mos.ru. 02.10.2023 / URL: https://www.mos.ru/news/item/130409073/ (дата обращения: 12.11.2024).

нения вреда и т.п. как своего рода мантры. Однако соразмерного регулирования данных вопросов не предлагается, что вызывает сомнения в должном обеспечении провозглашаемых принципов обеспечения цифровой безопасности.

Прозрачность схем проведения экспериментов также является сомнительной, особенно в части обеспечения предварительного обезличивания данных при доступе к ним участников ЭПР и возникающих в этой связи рисков неправомерного использования личной информации граждан и хозяйствующих субъектов [*Экономическая безопасность России в новой реальности...*, 2021. С. 201] (подробнее об обезличивании данных см. ниже).

Проблемным вопросом является также преимущественное участие в разработке и тестировании технологий частных компаний, которые склонны рассматривать свои технологии и основанные на них программы как коммерческую тайну и стремятся максимизировать прибыль от их разработки. Поэтому в большинстве случаев они отказываются раскрывать подробности работы своих программ, основанных на таких технологиях. И это только усиливает общую проблему непрозрачности заложенных в технологиях ИИ алгоритмов [*Блажеев В.В., Егорова М.А., Барабашев А.Г. и др.*, 2020].

IV

Институты цифрового социального мониторинга: регулирование и опыт использования

В контексте рассмотренной выше проблемы применении в России цифрового профилирования у государства возникают возможности по использованию получаемой информации для формирования институтов цифрового мониторинга социального поведения. Как уже было указано, круг субъектов, получающих доступ к персональным сведениям граждан, постепенно увеличивается. Однако наблюдаются и иные сходные и чреватые проблемами процессы – появилась возможность идентификации (прохождения регистрации) граждан в финансовых организациях, социальных сетях, на маркетплейсах при помощи ЕСИА.

Опасность здесь состоит в том, что использование сведений из ЕСИА оставляет за собой «цифровой след», который потенциально позволяет государственным органам его отследить и затем провести анализ полученных сведений [*Сиземова, Бурова*, 2023. С. 145]. В свою очередь, это создает условия для проведения мониторинга и оценки поведения граждан, а также прогнозирования их действий.

И хотя такая перспектива кажется не особенно очевидной, существуют тенденции, которые позволяют предположить возможность реализации такого сценария. Так, Минцифры России был разработан законопроект об обороте данных, который предусматривает создание единой ГИС, в которую операторы (государственный орган, муниципальный орган, юридическое или физическое лицо) обязаны будут направлять обрабатываемые ими персональные данные по запросу министерства[50]. Несмотря на то что законопроект вызвал общественный резонанс и был отрицательно оценен, в том числе крупными российскими компаниями, министерство

50. Проект федерального закона № 992331-7 «О внесении изменений в Федеральный закон «О персональных данных» (в части уточнения порядка обработки персональных данных) / URL: https://sozd.duma.gov.ru/bill/992331-7 (дата обращения: 12.11.2024).

отстаивало необходимость его принятия для дальнейшего развития цифровых технологий. В результате в августе 2024 г. законопроект был принят, он вступит в силу с 1 января 2025 г.[51]

Согласно его положениям в запросах министерства, адресованных операторам, будет указываться перечень данных, которые необходимо передать, а также сроки их предоставления. Перед передачей необходимо будет обезличить их по правилам, установленным Правительством РФ совместно с ФСБ России. Полученные обезличенные данные Минцифры России будет группировать и формировать из них агрегированные составы данных, к которым будет осуществляться доступ пользователей ГИС (к которым отнесены государственные и муниципальные органы, подведомственные им организации, органы государственных внебюджетных фондов, а также граждане РФ и российские юридические лица). Запроса у граждан согласия граждан на передачу их персональных данных во вновь создаваемую ГИС не предполагается в силу проведения их обезличивания. Однако необратимость проведения операторами обезличивания вызывает сомнения. Специалистами отмечается, что, несмотря на то что обезличивание является одним из способов защиты персональных данных, данная функция на практике не может быть выполнена, поскольку деобезличены могут быть практически любые данные, особенно государственными органами – посредством соотнесения обезличенных данных с имеющейся у них информацией о гражданах. При этом чем выше степень обезличивания, тем меньшую ценность представляют такие данные для обучения ИИ, поскольку чем содержательнее сведения о субъектах, тем больше выводов с их помощью можно сделать. Поэтому пользователи ГИС (к которым относятся и государственные органы) заинтересованы именно в низкой степени обезличивания данных. Применение же сверхпрочных методов защиты данных в процессе обезличивания требует значительных ресурсов – временных, финансовых, кадровых [*Лескина Э.И.*, 2024. С. 130–131; *Сафьянников А.В.*,

51. Федеральный закон от 8 августа 2024 г. №233-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» и Федеральный закон «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» // СПС «Гарант».

2022. С. 57–58, 64]. Поэтому, вероятно, в высокой степени обезличивания не будут заинтересованы и операторы. Остается добавить, что согласно отчету РКН за 2023 г. в Реестре операторов, осуществляющих обработку персональных данных, зарегистрировано 944 тыс. юридических и физических лиц[52], т.е. основа для формирования новой ГИС действительно колоссальна.

С высокой степенью вероятности все это означает, что появление ГИС с централизованной и обширной информацией о гражданах повлечет риски утраты конфиденциальности персональных данных, которые обрабатывают различные операторы. Речь может идти в том числе об информации ограниченного доступа – в частности о банковской тайне [*Рожков*, 2024].

В свою очередь, риски деобезличивания персональных данных влекут за собой возникновение возможностей для пользователей новой ГИС, получивших к ним доступ (особенно для крупных компаний, уже обладающих собственными базами данных клиентов), для проведения цифрового мониторинга и анализа поведения граждан.

Наиболее полно использование в государственном управлении систем мониторинга осуществляется в КНР (т.н. система «социального рейтинга», реализуемая 2014 г.), отдельные ее элементы применяются также в европейских странах. Мониторинг заключается в определении государством уровня «социальной репутации» (благонадежности) граждан на основе обработки информации об их поведении с присвоением индивидуального рейтинга. Предоставление некоторых льгот, субсидий зависит от уровня такого рейтинга, а внесение в «черный список» подразумевает введение в отношении гражданина различных ограничений – на выбор вида трудовой деятельности, получение кредитов, выбор мест обучения детей, пользование некоторыми видами транспорта и др. [*Цифровая трансформация в государственном управлении*, 2023. С. 109–112]. Средством реализации такой системы является использование цифрового удостоверения личности, а также и массового наблюдения, позволяющего государству отслеживать взаимодействия граждан, их покупки, поощряемое или неподобающее поведение и т.д. [*Харитонова Ю.С., Ци Сунь,* 2023. С. 15].

52. Отчет о выполнении плана и показателей деятельности Роскомнадзора в 2023 г. / Официальный сайт РКН. С. 116 / URL: https://rkn.gov.ru/docs/doc_3894.pdf (дата обращения: 12.11.2024).

В России граждане получили опыт мониторинга государством их действий в период пандемии. Например, в Москве пациенты с диагнозом коронавирус COVID-19, проходящие лечение на дому, были обязаны применять технологии электронного мониторинга своего местоположения в определенной геолокации, с использованием мобильного приложения «Социальный мониторинг»[53], позволяющего отслеживать их местонахождение и сигнализировать о нарушении режима самоизоляции, которое влекло за собой уплату штрафа.

Также присвоение гражданам определенного рейтинга в настоящее время практикуется коммерческими компаниями с предоставлением возможностей и преимуществ на основе мониторинга их действий или решений, их участия в определенной деятельности. К ним относятся рейтинги таксистов и пассажиров в сервисе «Яндекс. Go», кредитные рейтинги, рейтинги для расчетов страховых тарифов. Данная практика начала применяться и в государственном управлении – например в виде московского проекта «Активный гражданин».

Однако согласно опросам отношение населения к перспективам введения в России таких институтов отрицательное. Например, опрос Института государственного и муниципального управления НИУ ВШЭ 2021 г., проведенный для изучения отношения граждан к публичному раскрытию личных сведений, показал, что каждый второй респондент не готов делиться своими персональными данными, даже если это будет использовано для обеспечения в районе проживания собственной безопасности [Там же. С. 115–116].

Опрос ВЦИОМ 2021 г., касающийся сохранности персональных данных, констатировал, что ровно половина опрошенных (50%) считает злоупотребление полученными данными стороной, которая имеет к ним доступ, основной причиной их утечек[54]. Это подразумевает в том числе недоверие к государству в отношении

53. Указ мэра Москвы от 5 марта 2020 года № 12-УМ «О введении режима повышенной готовности» // СПС «Гарант».

54. Сохранность персональных данных: результаты опроса / ВЦИОМ. 07.09.2021 / URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/sokhrannost-personalnykh-dannykh (дата обращения: 12.11.2024).

как защищенности личных данных в ГИС, так и в части возможности их несанкционированного использования государственными органами (а такое недоверие, в свою очередь, делает маловероятным положительное отношение граждан к осуществлению государством цифрового социального мониторинга).

Недавний опрос ВЦИОМ 2024 г. по информационной безопасности показателен в отношении развития цифрового профилирования: среди опрошенных отсутствует единое мнение по оценке влияния новых технологий на безопасность персональных данных: треть опрошенных (33%) уверена, что новые технологии скорее не повлияют на сохранность личной информации и персональных данных, другая треть (32%) считает, что новые технологии скорее понизят сохранность личной информации и персональных данных[55].

В целом же можно констатировать, что предпосылки для формирования институтов цифрового мониторинга социального поведения в России складываются, однако в ближайшее время они вряд ли получат полноценное воплощение. Однако с учетом формирования Минцифры России единой ГИС возникают условия для развития теневого контроля за поведением граждан.

55. Цифровая самооборона: результаты опроса / ВЦИОМ. 12.03.2024 / URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/cifrovaja-samooborona (дата обращения: 12.11.2024).

Заключение

Подводя итоги текущего исследования, следует указать, что масштабно проводимая цифровая трансформация государственного управления, огромное количество изданных документов, регламентирующих данный процесс, проводимые эксперименты по внедрению цифровых технологий при одновременном отсутствии концептуального подхода и надлежащего обеспечения безопасности цифровой среды порождает многочисленные и весьма серьезные риски. При этом широкой общественной и научной дискуссии по данной проблематике еще не возникло.

На сегодняшний день в качестве наиболее значимых проблем безопасности цифровой среды предлагается рассматривать:

- развитие применения в государственном управлении интеллектуальных систем поддержки принятия решений (ориентированных на все большее внедрение технологий искусственного интеллекта) при непрозрачности алгоритмов, заложенных в них;
- все большее внедрение в практику государственного управления цифрового профилирования и открывающиеся возможности для применения государством на его основе механизмов социального мониторинга;
- предоставление доступа к данным в ГИС все более широкому кругу лиц вне контура государственного управления, что расширяет возможности реализации мошеннических схем;
- недостаточная защищенность персональных данных пользователей ГИС от неправомерных посягательств, а также потерь или искажений информации.

В дальнейших исследованиях по данной проблематике планируется дальнейшая систематизация и актуализация, постановка новых проблемных вопросов (например, возникающих при использовании цифровых сервисов для обеспечения общественного участия в процедурах разработки и принятия управленческих решений), сопоставление личных, общественных и государственных интересов при обеспечении безопасности цифровой среды и анализ

возможностей достижения их баланса, а также выработка конкретных рекомендаций по решению проблем безопасности цифровой среды в рамках цифровой трансформации государственного управления.

Литература

Блажеев В.В., Егорова М.А., Барабашев А.Г., Засемкова О.Ф., Кашкин С.Ю., Минбалеев А.В., Пономарева Д.В., Шахназаров Б.А. (2020) Правовое регулирование искусственного интеллекта в условиях пандемии и инфодемии (под общ. ред. проф. В.В. Блажеева, проф. М.А. Егоровой). Университет имени О.Е. Кутафина (МГЮА). М., «Проспект». 294 с.

Виноградова Е.В., Полякова Т.А., Минбалеев А.В. (2021). Цифровой профиль: понятие, механизмы регулирования и проблемы реализации // Правоприменение. Т. 5. №4. С. 5–19.

Власова В.Ю., Ястребова А.И. (2024). Особенности конституционно-правового регулирования применения технологий искусственного интеллекта в России // Современное право. №4. С. 63–68.

Головин Е.Г., Большакова В.М., Наумова Л.Ю. (2020). Обеспечение прав и свобод граждан и риски цифровизации // Вопросы российского и международного права. Т. 10. №2А. С. 3–10. DOI: 10.34670/AR.2020.93.2.001/ URL: http://www.publishing-vak.ru/file/archive-law-2020-2/1-golovin-bolshakova-naumova.pdf (дата обращения: 12.11.2024).

Грамматчиков А. (2021). Поспешная цифровизация — гигантский риск. Интервью с Н.Касперской // Монокль. 1 ноября / URL: https://monocle.ru/expert/2021/45/pospeshnaya-tsifrovizatsiya-gigantskiy-risk/ (дата обращения: 12.11.2024).

Городецкий А.Е. Экономическая безопасность России: актуальные риски и долгосрочные приоритеты социально-экономического развития (Резолюция по итогам Всероссийской научно-практической конференции VIII Сенчаговские чтения) (2024) / А.Е. Городецкий, И.В. Караваева, М.Ю. Лев // Экономическая безопасность. Т. 7, №6. С. 1327–1338.

Громова Е.А. (2021). О роли специальных и экспериментальных режимов в развитии конкурентоспособных цифровых технологий // Юрист. № 11. С. 34-38.

Евсиков К.С. (2022). Цифровая трансформация альтернативного разрешения споров // Журнал «Lex Russica». №11. С. 120–130.

Ефремов А.А., Добролюбова Е.И., Талапина Э.В., Южаков В.Н. (2020). Экспериментальные правовые режимы: зарубежный опыт и российский старт. М., Издательский дом «Дело» РАНХиГС. 126 с.

Залоило М.В. (2021). Искусственный интеллект в праве: научно-практическое пособие (под ред. Д.А. Пашенцева). М.: Инфотропик Медиа. 132 с.

Зорькин В.Д. (2024). Право и вызовы искусственного интеллекта // Российская газета. 27 июня. / URL: https://rg.ru/2024/06/27/pravo-i-vyzovy-iskusstvennogo-intellekta.html (дата обращения: 12.11.2024).

Касперская Н. (2023). О рисках, угрозах и отсутствии системности в цифровизации / портал Infowatch. 12 августа / URL: https://www.infowatch.ru/resursy/blog/blog-natali-kasperskoy/o-riskakh-ugrozakh-i-otsutstvii-sistemnosti-v-tsifrovizatsii (дата обращения: 12.11.2024).

Конкуренция в цифровую эпоху: стратегические вызовы для Российской Федерации (2018). Доклад Всемирного банка. – 144 с. / URL: https://www.vsemirnyjbank.org/ru/country/russia/publication/competing-in-digital-age (дата обращения: 12.11.2024).

Королев Н., Лебедева В., Старикова М. (2021). Широка цифра моя родная // Коммерсант. 21 декабря / URL: https://www.kommersant.ru/doc/5140980 (дата обращения: 12.11.2024).

Кузякин Ю.П., Кузякин С.В. (2023). Правовое регулирование цифровых технологий в государственном управлении // Административное право и процесс. №3. С. 55–58.

Лескина Э.И. (2024). Доктринальные аспекты правовых режимов данных в условиях развития технологий больших данных // Журнал российского права. №7. С. 122–136.

Мочалов А.Н. (2021) Цифровой профиль: основные риски для конституционных прав человека в условиях правовой неопределенности // Lex Russica. №9. С. 88–101.

Право цифровой среды (2022). Монография / Коллектив авторов; под ред. Т.П. Подшивалова, Е.В. Титовой, Е.А. Громовой. М.: Проспект, 2022. 896 с. // СПС «Гарант».

Рожков Р. (2024). Бизнес просит власти отказаться от законопроекта об обороте данных / Forbes. 10 июня / URL: https://www.forbes.ru/tekhnologii/514438-biznes-prosit-vlasti-otkazat-sa-ot-zakonoproekta-ob-oborote-dannyh (дата обращения: 12.11.2024).

Сафьянников А.В. (2022) Обезличенные данные: есть ли будущее в России? // Вестник экономического правосудия Российской Федерации. №9. С. 55–74.

Сиземова О.Б., Бурова А.Ю. (2023). О принципах построения правового механизма цифрового профилирования граждан // Вестник Университета имени О.Е. Кутафина (МГЮА). №1. С. 139–150 / URL: https://vestnik.msal.ru/jour/article/view/1959/1982 (дата обращения: 12.11.2024).

Смотрицкая И.И., Черных С.И., Сазонова Е.С. (2022). Концепция публичного управления в контексте долгосрочных целей новой экономической политики // Вестник Института экономики Российской академии наук». №4. С. 60–76.

Современные институты государственного управления: вызовы, адаптация, развитие (2024). Монография / Под общ. ред. И.И. Смотрицкой, С.И. Черных. М.: ИЭ РАН. 373 с.

Степанов О.А., Басангов Д.А. (2024). О правовых особенностях и рисках реализации цифрового профилирования // Российская юстиция. №1. С. 59–69.

Талапина Э.В. (2024). Права человека в цифровом государственном управлении // Журнал российского права. №9. С. 137–149.

Харитонова Ю.С., Ци Сунь (2023). Верховенство закона и алгоритмизация принятия решений в России, Китае, Европе: перспективы персонализации правового регулирования // Право и бизнес. №2. С. 11–17.

Цифровая трансформация в государственном управлении (2023). Коллективная монография / Н.Е. Дмитриева, А.Г. Санина, Е.М Стырин и др.; под ред. Е.М. Стырина, Н.Е. Дмитриевой. М.: Изд. дом Высшей школы экономики. 208 с.

Цифровая трансформация и государственное управление (2022). Научно-практическое пособие / А.С. Емельянов, А.А. Ефремов, А.В. Калмыкова и др.; ред. кол.: Л.К. Терещенко, А.С. Емельянов, Н.А. Поветкина. М.: Инфотропик Медиа. 224 с.

Цифровая трансформация и защита прав граждан в цифровом пространстве (2021). Доклад Совета при Президенте Российской Федерации по развитию гражданского общества и правам человека. 124 с. / URL: https://ifap.ru/pr/2021/n211213a.pdf (дата обращения: 12.11.2024).

Чувильдеев В.Н. (2019). Искусственный интеллект понимать не может // Эксперт. № 45–46 (1141) / URL: https://monocle.ru/expert/2019/45/iskusstvennyij-intellekt-ponimat-ne-mozhet/ (дата обращения: 12.11.2024).

Экономическая безопасность России в новой реальности (2021). Коллективная монография / Под общ. ред. А.Е. Городецкого, И.В. Караваевой, М.Ю. Льва. М.: ИЭ РАН. 325 с.

Юэ Цян, Кичик К.В. Исследование российской стратегии развития искусственного интеллекта через призму концепции верховенства права // Право и цифровая экономика. 2023. № 2. С. 14–24.

Институт экономики
Российской академии наук

Редакционно-издательский отдел:
Тел.: +7 (499) 129 0472
e-mail: print@inecon.ru
Сайт: www.inecon.ru

Научный доклад

Сазонова Е.С.

Проблемы безопасности цифровой среды в сфере государственного управления

Оригинал-макет *Валериус В.Е.*
Редактор *Полякова А.В.*
Компьютерная верстка *Борщёва И.В.*

Подписано в печать 27.12.2024 г. Заказ № 27
Тираж 300 экз. Объем 2,3 уч.-изд. л.
Отпечатано в ИЭ РАН

ISBN 978-5-9940-0781-5