Министерство науки и высшего образования Российской Федерации

Национальный исследовательский
Нижегородский государственный университет им. Н.И. Лобачевского

А.В. Мартынов, М.В. Бундин, Е.В. Ширеева, Е.Н. Смирнова,
М.Д. Прилуков, А.Э. Логинова

КОНЦЕПЦИЯ ПРАВОВОГО РЕГУЛИРОВАНИЯ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В СФЕРЕ ГОСУДАРСТВЕННОГО КОНТРОЛЯ И НАДЗОРА В УСЛОВИЯХ «ЦИФРОВОЙ ЭКОНОМИКИ»: РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Монография

Под научной редакцией д.ю.н., профессора А.В. Мартынова

Исследование выполнено при финансовой поддержке РФФИ
в рамках научного проекта № 20-011-00584
«Концепция правового регулирования использования информационных технологий в сфере государственного контроля и надзора
в условиях «цифровой экономики»»

Нижний Новгород
Издательство Нижегородского госуниверситета
2021

УДК 342.95
ББК 67.401
К64

Мартынов А.В. – § 1, § 2 гл. 1, § 4 гл. 2; *Бундин М.В.* – § 4 гл. 2; *Ширеева Е.В.* – § 1 гл. 2; *Смирнова Е.Н* – § 3 гл. 2; *Прилуков М.Д., Логинова А.Э.* – § 2 гл. 2.

Рецензенты:
Старилов Ю.Н. – доктор юрид. наук, профессор, заслуженный деятель науки РФ, декан юридического факультета, заведующий кафедрой административного и административного процессуального права ФГБОУ ВО «Воронежский государственный университет»;
Терещенко Л.К. – доктор юрид. наук, доцент, заслуженный юрист РФ, заместитель заведующего отделом административного законодательства и процесса ФГНИУ «Институт законодательства и сравнительного правоведения при Правительстве РФ»

К64 **Концепция правового регулирования использования информационных технологий в сфере государственного контроля и надзора в условиях «цифровой экономики»: результаты исследования**: монография / А.В. Мартынов, М.В. Бундин, Е.В. Ширеева; Е.Н. Смирнова, М.Д. Прилуков, А.Э. Логинова; под науч. ред. А.В. Мартынова – Н. Новгород: Изд-во Нижегородского госуниверситета им. Н.И. Лобачевского, 2021. – 251 с.

ISBN 978-5-91326-706-1

Данное монографическое исследование посвящено новой концепции правового регулирования использования современных информационных технологий в сфере государственного контроля и надзора в условиях «цифровой экономики». Уделяется внимание особенностям модернизации и трансформации системы контроля и надзора в условиях цифровизации государственного управления в сфере обеспечение правопорядка и общественной безопасности, медицины и фармакологии, промышленности и информации.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-011-00584 «Концепция правового регулирования использования информационных технологий в сфере государственного контроля и надзора в условиях «цифровой экономики»».

ISBN 978-5-91326-706-1

УДК 342.95
ББК 67.401

Lobachevsky State University of Nizhny Novgorod

A.V. Martynov, M.V. Bundin, E.V. Shireeva, E.N. Smirnova,
M.D. Prilukov, A.E. Loginova

THE CONCEPT OF LEGAL REGULATION OF THE USE OF INFORMATION TECHNOLOGIES FOR STATE CONTROL AND SUPERVISION IN THE «DIGITAL ECONOMY'S" ENVIRONMENT: FINAL RESULTS

Monography

Scientific consultant A.V. Martynov

The reported study was funded by RFBR according to the research project
№ 20-011-00584 «The concept of legal regulation of the use
of information technologies for state control and supervision
in the «digital economy's» environment»

Nizhny Novgorod
Lobachevsky State University of Nizhny Novgorod publishing house
2021

Martynov A.V. – § 1, § 2 Ch. 1, § 4 Ch. 2; *Bundin M.V.* – § 4 Ch. 2; *Shireeva E.V.* – § 1 Ch. 2; *Smirnova E.N.* – § 3 Ch. 2; *Prilukov M.D., Loginova A.E.* – § 2 Ch. 2.

Reviewers:

Starilov Yu.N. – doctor of law, professor, Honored worker of science of Russian Federation, dean of the Faculty of Law, head of the Department of Administrative Law and Procedure, Voronezh State University;

Tereshenko L.K. – doctor of law, professor, Honored lawyer of Russian Federation, vice-head of the Department of Administrative law and procedure, the Institute of Legislation and Comparative Law under the Government of the Russian Federation

The concept of legal regulation of the use of information technologies for state control and supervision in the «digital economy's» environment: final results: monography / A.V. Martynov, M.V. Bundin, E.V. Shireeva, E.N. Smirnova, M.D. Prilukov, A.E. Loginova. – N. Novgorod: Lobachevsky State University of Nizhny Novgorod publishing house, 2021. – 251 p.

ISBN 978-5-91326-706-1

This monographic study is devoted to a new concept of legal regulation of the use of modern information technologies in the field of state control and supervision in the «digital economy's» environment. Attention is paid to the peculiarities of modernization and transformation of the state control and supervision system in the context of digitalization of public administration in the field of law enforcement and public security, medicine and pharmacology, industry and information.

The reported study was funded by RFBR according to the research project № 20-011-00584 «The concept of legal regulation of the use of information technologies for state control and supervision in the «digital economy's» environment».

СОДЕРЖАНИЕ

TABLE OF CONTENTS

ВВЕДЕНИЕ

Данная монография направлена на исследование проблематики правового регулирования вопросов внедрения в контрольно-надзорную деятельность новых информационных технологий и выработку системы принципов правового регулирования контрольно-надзорной деятельности (концепции правового регулирования), отвечающей потребностям «цифровой экономики».

Общепризнанная концепция-идея «электронного государства», подразумевающая широкое использование новых информационных технологий в осуществлении государственной деятельности затрагивает множество направлений – это и электронное правительство, и парламент, и правосудие. Очевидно, что современному обществу – обществу информационному с развитой «цифровой экономикой» – очень необходима соответствующая система государственного управления, которая будет построена на широком применении различных технологических решений, основанных на технологиях больших данных, искусственного интеллекта, робототехники, распределенного реестра (блокчейн) и др. Совершенно логично, что в этих условиях должна эволюционировать и существующая система государственного контроля и надзора, которая будет претерпевать дальнейшие серьезные изменения как в части методов, так и в части форм, а также будет немыслима без использования современных и актуальных технологий обработки данных и информации.

Вслед за разработкой нормативных положений, регулирующих те или иные аспекты «цифровой экономики», потребуется создание новых эффективных механизмов контроля и надзора за их реализацией и соблюдением, а равно адаптация уже существующих.

Основной фундаментальной научной задачей настоящего исследования является критический анализ существующего нормативного регулирования и практики государственной контрольно-надзорной деятельности в целом и ее отраслях в отдельности (правопорядок и общественная безопасность, фармакология и медицина, промышленность, информационная сфера), а также формируемых представлений о разрабатываемых законодательных и нормативных решениях по правовому регулированию «цифровой экономики».

Основной целью исследования является разработка и обоснование научной концепции, адаптация существующей системы государственного контроля и надзора к формируемым условиям «цифровой эконо-

мики». Данная концепция предполагает разработку и обоснование системы принципов правового регулирования и осуществления контрольно-надзорной деятельности.

Основные задачи исследования заключаются в:

– анализе существующих научных представлений о тенденциях развития информационного обществ и «цифровой экономики» через призму обеспечения интересов государственного управления и контрольно-надзорной деятельности;

– формирование краткосрочного и долгосрочного прогноза развития правового регулирования контрольно-надзорной деятельности и практики с учетом формирующихся институтов информационного общества и «цифровой экономики»;

– разработка целостной концепции правового регулирования контрольно-надзорной деятельности в условиях «цифровой экономики» и в условиях активного внедрения в сферу государственного управления новых информационных технологий обработки данных и информации.

Научная новизна исследования состоит в разработке нового теоретического подхода к правовому регулированию государственного контроля и надзора посредством использования информационных технологий в условиях «цифровой экономики». Должны быть по-новому определены предмет и объект государственного контроля (надзора), формы и методы государственного контроля (надзора), субъекты и участники контрольно-надзорных отношений, функции и полномочия органов и должностных лиц, осуществляющих государственный контроль и надзор.

Также важным является формирование теоретико-правового обоснования использования при осуществлении государственного контроля и надзора современных информационных технологий, проведения контрольно-надзорных мероприятий без участия человека (электронный инспектор, робот-инспектор и т.п.), а также использования технологий искусственного интеллекта для прогнозирования угроз, которые должны предотвращаться посредством контрольно-надзорных мероприятий и практических действий по осуществлению контрольно-надзорных мероприятий в отношении сложных производственных объектов и технологических процессов.

Основным результатом научной работы представляется разработка и научное обоснование единой концепции правового регулирования внедрения новых информационных технологий (большие данные, искусственный интеллект, робототехника, распределенный реестр, облач-

ные вычисления и др.) в сферу осуществления государственного контроля и надзора в условиях «цифровой экономики».

Данная концепция должна представлять собой систему теоретических принципов – единых руководящих начал для создания и разработки актуального законодательства и нормотворчества. Концепция также будет включать необходимый понятийный аппарат и инструментарий. Кроме того, также обосновывается принятие, в том числе необходимых решений по модернизации действующего законодательства и подзаконных нормативно-правовых актов и иных нормативных документов, регулирующих контрольно-надзорную деятельность.

Определенную практическую значимость имеют практические рекомендации по совершенствованию практики контрольно-надзорной деятельности, повышения ее оснащенности новыми технологическими решениями и в конечном итоге повышения ее эффективности. Данные рекомендации разработаны в том числе на основе проведенного опроса должностных лиц контрольно-надзорных органов.

Авторы научного исследования полагают, что внедрение предложенных принципов будет способствовать, с одной стороны, повышению эффективности и прозрачности контрольно-надзорной деятельности в условиях развивающейся «цифровой экономики», с другой стороны, поможет снизить административные барьеры для граждан и бизнеса.

Глава 1
Основные положения концепции правового регулирования использования информационных технологий в сфере государственного контроля и надзора в условиях «цифровой экономики»

§ 1. Перспективы цифровизации государственного контроля и надзора в условиях «цифровой экономики»

В России во втором десятилетии XXI современные цифровые технологии стали стратегическим направлением для реформирования и модернизации системы государственного управления. Можно констатировать, что в той или иной мере фактически во всех отраслях и сферах государственной деятельности используются современные цифровые технологии, которые стали неотъемлемой частью деятельности органов публичного управления. При этом процесс внедрения цифровых технологий в деятельность государственных органов носит системный и планомерный характер, обуславливается необходимостью на новом качественном уровне осуществлять государственные функции и полномочия.

Более того, внедрение цифровых технологий является не только прерогативой органов публичного управления, но и связано с тем, что в само по себе общество подвержено цифровизации, и каждый человек уже не представляет свою жизнь без новых цифровых технологий. Так, в Российской Федерации наблюдается высокий уровень применения цифровых технологий в повседневной жизни: практически у всех граждан имеются цифровые средства связи (телефоны, смартфоны, планшеты), имеется доступ к сети «Интернет» и беспроводной локальной сети (Wi-Fi), широко используются бытовая умная техника (компьютеры, домашние роботизированные устройства), применяются на постоянной основе цифровые способы финансово-денежных расчетов и операций, и т.д. Бизнес структуры повсеместно осуществляют свою деятельность используя современные цифровые технологии. У некоторых из них предпринимательская деятельность основывается целиком и полностью на современных цифровых технологиях (доставка еды, сервисы такси,

высокоавтоматизированные транспортные средства, цифровые платформы и цифровые сервисы по покупке и продаже товаров и услуг, видеохостингов, социальных сетей и многого другого). С учетом этих процессов государство не может не учитывать, складывающиеся в обществе потребности и запросы, изменившиеся средства коммуникации между людьми, желание активно пользоваться современными цифровыми технологиями. Именно поэтому российское государство не остается в стороне от процессов цифровизации и становится активным участников данных процессов, так как граждане, использующие цифровые технологии, и есть те самые государственные и муниципальные служащие, которые осуществляют публично-управленческую деятельность, а следовательно, государство должно предоставить эффективно реализовывать свои полномочия в изменившихся условиях. С другой стороны, взаимодействие государства с общество и отдельными его гражданами должно быть оптимальным, соответствующим условиям времени и развития технологического прогресса, что требует создание каналов прямой и обратной связи, основанных на современных цифровых технологиях.

Нельзя не отметить, что сложившиеся условия в нашей стране по широкой цифровизации общества и государства стали благоприятной средой для развития «цифровой экономики», то есть осуществление хозяйственной деятельности, в которой ключевым фактором производства являются данные в цифровом виде, обработка больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг[1].

Очевидно, что активное внедрение цифровых технологий в деятельность органов публичного управления не является достаточным условием для успешного развития цифровой экономики в нашей стране. По нашему мнению, главным и определяющим для цифровой экономики является высокотехнологичное государственное (публичное) управление, основанное на иных принципах и подходах при взаимодействии государства и общества, органов государственной власти и граждан, контролирующих органов и предпринимательских структур, правоохранительных органов и общественных объединений и граждан. Вы-

[1] Подпункт «р» пункта 4 Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы, утвержденной Указом Президента РФ от 9 мая 2017 г. № 203 // СЗ РФ. 2017. № 20. Ст. 2901.

сокотехнологичное государственное управление – это фактически новая модель управления, предполагающая более высокий уровень открытости и прозрачности деятельности органов государственной власти, широкий и практически не ограниченный доступ к информации, которой располагают органы публичной власти и публичные организации, взаимодействие, не предполагающее личного общения с должностными лицами органов публичной власти, высокий уровень автоматизации повторяющихся и однотипных процессов и административных процедур, возможность аутсорсинга отдельных властных полномочий искусственному интеллекту или принятие публично-властных и юридически значимых решений без участия человека с использованием искусственного интеллекта, разработка правовых актов искусственным интеллектом, управление, основанное на цифровых сервисах и платформах. Конечно же, все вышеперечисленное можно дополнить и другими важными факторами и условиями применения цифровых технологий (нейросети, квантовые технологии, большие данные, блокчейн, промышленный интернет, роботы-помощники и т.п.) в публичном управлении. Высокотехнологичность публичного управления и не только и не столько реальное наличие у государственных органов современных цифровых технологий, а прежде всего, активное применение указанных цифровых технологий в повседневной деятельности и что значительно повышают эффективность и результативность деятельности должностных лиц органов публичного управления по сравнению с традиционными формами и методами работы.

Следует отметить, что в настоящее время существует неоднородность процессов внедрения современных цифровых технологий в деятельность государственных органов. Это связано с несколькими как объективными, так и субъективными факторами. К объективным факторам можно отнести невозможность внедрения цифровых технологий по причине закрытости деятельности органа государственной власти, выполняющего функции по обеспечению национальной или государственной безопасности. Следовательно, внедрение цифровых технологий, которые разработаны или контролируемы иностранными государствами, не может осуществляться в таких условиях. При этом могут отсутствовать отечественные разработки в сфере определенных цифровых технологий, что естественным образом тормозит процесс цифровизации деятельности определенных органов государственной власти (это прежде всего касается органов безопасности и правоохранительных органов). К субъективным факторам может отнесено, как отсутствие

поддержки со стороны руководства страны для цифровизации деятельности отдельных государственных органов (так как, например, это не считается для страны приоритетным направлением), так и архаичность деятельности органа или слабая инициативность руководства этого органа. К сожалению, фактор личности руководителя того или иного государственного органа имеет огромное значение в нашей стране. Например, деятельность на посту руководителя Федеральной налоговой службы М.В. Мишустина позволила значительно продвинутся в цифровизации функций налогового администрирования и налогового контроля. Налоговые органы фактически стали передовыми по использованию современных цифровых технологий. Этот фактор стал во многом решающим при назначении М.В. Мишустина председателем Правительства РФ 16 января 2020 года.

Немаловажным фактором является процесс глобализации использования цифровых технологий. Применение цифровых технологий уже давно не ограничивается национальной юрисдикцией и правовыми механизмами, установленными в государствах. Глобальный характер применения цифровых технологий связан прежде всего с доступностью этих технологий для обычных пользователей, а также глобальным распространением своей цифровой продукции крупными IT-гигантами (Apple, Microsoft, Samsung, Xiaomi, Huawei, и т.д.). При этом современные цифровые технологии используются не только обычными гражданами и организациями, но и государственными структурами, которые вынуждены закупать оборудование, программное обеспечение, цифровые продукты у крупных IT-гигантов, так как обеспечить выполнение высокотехнологичных операций или цифрового взаимодействия без данных цифровых технологий не представляется возможным.

В России складывается достаточно сложная ситуация в сфере использования современных цифровых технологий государственными структурами. С одной стороны, Российская Федерация позиционирует себя как один из мировых лидеров (наравне с США, Китаем, Японией, Германий, Францией, Южной Кореей) по внедрению цифровых технологий в различные сферы экономики. Приняты на государственном уровне стратегические документы краткосрочного и долгосрочного внедрения современных цифровых технологий в различные сферы и области жизнедеятельности обществ и государства. Активно используются экспериментальные правовые режимы для применения передовых цифровых технологий в отдельных сферах экономической деятельности. Государство выделяет серьезные бюджетные субсидии и гранты на

развитие различных проектов по внедрению передовых цифровых технологий в различные сферы и области экономических и общественных отношений. Не остается без внимания и сфера деятельности органов государственной власти, в которой происходит цифровизация государственного управления и цифровая трансформация деятельности органов государственной власти.

С другой стороны, начиная с 2014 года Российская Федерация находится под санкциями, введенными ведущими мировыми державами (США. Япония, Германия, Франция, Канада, Австралия, и др.), которыми ограничиваются в нашу страну высокотехнологичного оборудования, комплектующих для создания передовых цифровых технологий, современного программного обеспечения, ограничиваются доступ к цифровым платформам и цифровым сервисам, и многое другое. Все это приводит к торможению процессов цифровизации различных сфер экономики и государственного управления. Угроза постоянного введения или усиления санкций не позволяет широко использовать и применять современные цифровые технологии, зарубежного производства. В государственном секторе из-за этого делается акцент на отечественных цифровых технологиях и программном обеспечении. Установление запретов на цифровое сотрудничество и взаимодействие обуславливается национальной безопасностью и стабильностью государственного управления. Между тем, в условиях глобализации невозможно добываться новых открытий и передовых цифровых технологий без сотрудничества и взаимодействия с международными партнерами. Как показал опыт пандемии COVID-19, что несмотря на отечественные разработки вакцины, для победы над грозным вирусом необходимо сотрудничество и взаимодействие с международными партнерами, которые также имеют подобные разработки. В качестве примера может быть приведено сотрудничество между разработчиками российской вакцины «Спутник-V» и компанией «Pfizer» по изучению возможности усовершенствования собственных разработок на основе сотрудничества.

Безусловно лидерами цифровой индустрии в России являются частные компании или компании с государственным участием, такие как Яндекс, Лаборатория Карсперского, Сбербанк, Ростелеком, Вконтакте и др. Но эти компании крайне зависимы от зарубежных цифровых технологий и в случае блокирования зарубежными производителями элементарных цифровых гаджетов (телефонов, смартфонов, компьютеров) и программного обеспечения, то весь процесс цифровизации экономической деятельности будет приостановлен или полностью прекращен.

В этом плане совершенно верным представляется стратегический курс государства на приоритет в деятельности государственных органов и крупных государственных компаний отечественных цифровых технологий и ограничение использования цифровых технологий и программного обеспечения, созданных зарубежными производителями.

К глубочайшему сожалению, следует констатировать, что Россия вряд ли в ближайшие несколько десятилетий вряд ли сможет преодолеть отставание в разработке передовых цифровых технологий и даже в случае отмены санкций не сможет быстро перейти к производству высокотехнологичного оборудования и разработке передовых цифровых технологий. Это объективные процессы, связанные и с отсутствием промышленных предприятий и компаний, опыта производительной деятельности в этой сфере, но и прежде всего, постоянным оттоком высококвалифицированных специалистов и ученых из страны в зарубежные компании и научно-исследовательские институты. Развитие цифровых компаний препятствует также отсутствие стабильной экономической ситуации в стране, чрезмерное давление со стороны правоохранительных органов, отсутствие значимых мер со стороны государства для ученых и специалистов в IT-сферы.

При таких обстоятельствах, единственным выходом из такой достаточно сложной ситуации является создание экспериментальных полигонов для применения современных цифровых технологий. Здесь имеется в виду, то что в России должны активно использоваться современные цифровые сферы (без каких-либо ограничений), если это не затрагивается сферу национальной или общественной безопасности. При этом должен делаться акцент именно на передовых цифровых технологиях вне зависимости их производителя или страны производства. В некоторых случаях, иностранные производители будут заинтересованы в таких условиях применения их новых цифровых технологий. К примеру, мы имеем колоссальное технологическое отставание в сфере добычи угля. Взрыв на шахте «Листвяжная» 25 ноября 2021 года, в Кемеровской области, в результате которого погибло 51 человек (шахтеров и горноспасателей), в очередной раз доказывает, что работа в этой сфере является одной из самых опасных в мире. Очевидно, что переход к добыче угля с использованием высокотехнологичного оборудования, в том числе роботов, а также осуществление высокоцифровизированного государственного надзора в этой области, является крайне необходимо для нашего государства. Поэтому государство могло допустить к разработке месторождений угля именно высокотехнологичные компа-

нии, в том числе зарубежные, которые будут внедрять новые цифровые технологии для добычи угля без непосредственного участия человека. То есть это будет рассматриваться такими компаниями как полигон по внедрению современных цифровых технологий, и возможность получения прибыли от этой деятельности. Альтернативы этому не существует, так как российский опыт показывает, что собственники таких компаний, которые практически не несут никой ответственности за причиненный ущерб людям и окружающей среде, не желают вкладывать какие-либо ресурсы в повышения безопасности и высокотехнологичности своего производства. При этом получаемые прибыли они переводят за рубеж, вкладывая опять же в иностранные компании, зарубежную экономику и недвижимость в странах, которые проводят недружественную политику против России.

Исходя из этого, по нашему мнению, высокая цифровизация государственного контроля и надзора возможна только в тех сферах и отраслях, в которых имеется прогресс в использовании передовых цифровых технологий. Не имеет практического смысла использовать современные цифровые технологии при осуществлении государственного контроля и надзора, если на контролируемом объекте не применяются какие-либо цифровые технологии, например, уголь добывается по технологиям XVIII – XX веков, а собственники предприятия делают все возможное, чтобы такие технологии не внедрялись, избегая излишних затрат на производство, но подвергая опасности жизнь и здоровье людей. На самом деле, таких сфер очень много в современной России, и в которых вполне могли быть созданы полигоны по внедрению передовых цифровых технологий, например, металлургическая промышленность, нефтедобывающая и нефтеперерабатывающая промышленность, газовая промышленность, жилищно-коммунальная сфера, деятельность при экстремальных температурах и агрессивной среды, и т.д.

Рассматривая вопрос о цифровизации деятельности органов исполнительной власти по осуществлению функций государственного контроля и надзора, то мы убеждены, что данная сфера как никогда нуждается во внедрении современных цифровых технологий.

Системные преобразования в сфере государственного контроля и надзора направлены прежде всего на повышение деятельности органов исполнительной власти и их должностных лиц. При реформировании системы государственного контроля и надзора государству требуется решить сразу несколько сложнейших задач. Во-первых, сократить избыточное давление на бизнес, исключить необоснованные и незаконные

проверки граждан и организаций, стимулировать путем послаблений в сфере государственного контроля и надзора субъектов экономической деятельности. Во-вторых, повысить эффективность и результативность контрольно-надзорной деятельность. Главными критериями эффективности и результативности должны статьи предотвращенные случаи причинения вреда жизни и здоровья граждан, окружающей среде, имуществу государства и частных лиц. Приоритетным направлением государственного контроля и надзора должна оставаться безопасность в различных сферах жизнедеятельности человека, а соответственно, проведение профилактических мероприятий становится ключевым направлением осуществления государственного контроля и надзора. В-третьих, повышение прозрачности и открытости деятельности органов государственного контроля и надзора, создание эффективной системы профилактики коррупционных правонарушений среди должностных лиц контрольно-надзорных органов. Актуализация обязательных требований, отмена устаревших и избыточных требований, являющихся предметом проверки при осуществлении государственного контроля и надзора. Размещение в открытом доступе обязательных требований, подлежащих проверке, по видам государственного контроля и надзора, и размещение в открытом доступе проверочных листов, на основании которых проводятся контрольно-надзорные мероприятия. В-четверых, улучшение кадрового и материально-технического обеспечения контрольно-надзорных органов. Применение современных форм и методов осуществления контрольно-надзорных мероприятий. Проведение контрольно-надзорных мероприятий, основанных на дистанционном взаимодействии должностных лиц контрольно-надзорных органов и контролируемых лиц. В-пятых, установление эффективных механизмов защиты прав и законных интересов граждан и организаций при осуществлении государственного контроля и надзора. Введение новых процедур досудебного обжалования действий и решений контрольно-надзорных органов и их должностных лиц, и т.д.

Проведение вышеперечисленных и других преобразований невозможно без активного внедрения в деятельность контрольно-надзорных органов современных цифровых технологий. Данные технологии не только позволяют провести преобразования в контрольно-надзорной деятельности органов исполнительной власти, но и значительно улучшить взаимодействие проверяющих и контролируемых лиц. Не стоит забывать, что контрольно-надзорная деятельность всегда требовала использование самых современных технологий. Например, проверка объ-

ектов нефтехимии и нефтепереработки, трубопроводов и газопроводов, металлургической промышленности, гидротехнических сооружений, атомной промышленности, производства по добыче угля, взрывоопасных и пожароопасных объектов и промышленных производств, и т.д., начиная с середины XX века в России осуществляется с использованием современных технологий: газовых анализаторов, детекторов, иных измерительных приборов, специальных устройств для проведения исследований в труднодоступных местах, различных видов специализированной техники и т.п. Кроме этого, сотрудниками контрольно-надзорных органов становятся как правило лица, имеющие техническое либо инженерное образование, опыт работы на промышленных производствах и предприятиях. Все дает нам основание считать сферу контрольно-надзорной деятельности наиболее благоприятной для внедрения передовых цифровых технологий.

Подтверждение нашему выводу являются результаты проведенного нами опроса должностных лиц контрольно-надзорных органов, которые отметили в целом, что современные информационные технологии способствуют повышению эффективности осуществления ими контрольно-надзорной деятельности (42%), и всего лишь 9% – указали, что информационные технологии никак не способствуют улучшению исполнения ими полномочий по осуществлению по государственному контролю и надзору (см. Приложение).

Тем самым государство делается серьезный акцент при реформировании системы государственного контроля и надзора на нескольких направлениях, связанных с внедрением в деятельность контрольно-надзорных органов современных информационных (цифровых) технологий.

Первым важным шагом становится принятие программы по автоматизации контрольно-надзорной деятельности. 21 декабря 2016 года Президиумом Совета при Президенте РФ по стратегическому развитию и приоритетным проектам был утвержден Паспорт приоритетной программы «Реформа контрольной и надзорной деятельности»[2]. В рамках данного проекта предусматривалось разработка и принятие единых комплексных требований к информационным системам, обеспечиваю-

[2] Паспорт приоритетной программы «Реформа контрольной и надзорной деятельности» (приложение к протоколу президиума Совета при Президенте РФ по стратегическому развитию и приоритетным проектам от 21.12.2016 № 12) (ред. от 30.05.2017) // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

щим выполнение контрольно-надзорных функций (Стандарт информатизации КНД). Иными словами, впервые предполагалось внедрение в деятельность контрольно-надзорных органов определенного стандарта по информатизации (требования к информационным системам). Это означает, что информационные системы должны стать неотъемлемой частью деятельности контрольно-надзорных органов, что является серьезным шагом по направлению к цифровизации государственного контроля и надзора.

27 января 2017 г. был утвержден Паспорт приоритетного проекта Автоматизация контрольно-надзорной деятельности[3]. Целью данного проекта стало снижение административной нагрузки на граждан и организации, осуществляющих предпринимательскую и иные виды деятельности путем снижения транзакционных издержек при взаимодействии контрольно-надзорных органов, являющихся участниками реализации приоритетной программы, и проверяемых субъектов, за счет интерактивного взаимодействия через сеть Интернет с использованием электронных сервисов «Личного кабинета». Период действия приоритетного проекта с 2017 года по 2025 год. Основным результатом реализации приоритетного проекта должно стать рост качества администрирования контрольно-надзорных функций за счет использования информационных систем, соответствующих принятому Стандарту информатизации контрольно-надзорной деятельности.

14 июня 2017 г. были утверждены Комплексные требования к информационным системам, обеспечивающим выполнение контрольно-надзорных функций органами исполнительной власти (Стандарт информатизации контрольно-надзорной деятельности)[4]. Ключевым моментом стало указание в Стандарте информации контрольно-надзорной деятельности на то, что комплексные требования применятся к порядку проектирования и разработки информационных систем, автоматизирующих выполнение контрольно-надзорными органами своих функций.

---

[3] Паспорт приоритетного проекта Автоматизация контрольно-надзорной деятельности, утвержден протоколом заседания проектного комитета от 27.01.2017 № 5 // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

[4] Комплексные требования к информационным системам, обеспечивающим выполнение контрольно-надзорных функций органами исполнительной власти (Стандарт информатизации контрольно-надзорной деятельности), утверждены протоколом заседания проектного комитета от 14.06.2017 № 40(6)) // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

То есть информационные системы должны обеспечивать ни какие-то второстепенные или вспомогательные функции, выполняемые органами государственного контроля и надзора, а прежде всего, непосредственные функции по контролю и надзору.

Стандарт информатизации контрольно-надзорной деятельности преследовал следующие цели:

1) обеспечить возможность информационного взаимодействие органов и организаций, принимающих участие в контрольно-надзорной деятельности, включая проверяемых лиц, в рамках Единой информационной среды контрольно-надзорной деятельности;

2) упростить для органов и организаций, принимающих участие в контрольно-надзорной деятельности, включая проверяемых лиц, практическое применение требований и поручений, содержащихся в правовых актах, программах и дорожных картах, связанных с реформой контрольно-надзорной деятельностью;

3) представить единую методологию автоматизации типовых функций ведомственных информационных систем контрольно-надзорных органов.

Под ведомственной информационной системой автоматизации контрольно-надзорной деятельности контрольно-надзорного органа понимается система электронного документооборота, кадрового учета и иные информационные системы, с помощью которых автоматизируются какие-либо процессы в рамках контрольно-надзорной деятельности (например, внутриведомственное согласование документов в СЭДО (система электронного документооборота), внесение показателей результативности деятельности должностного лица в систему кадрового учета).

При этом значимым результатом информатизации контрольно-надзорной деятельности должно стать создание единой информационной среды контрольно-надзорной деятельности (ЕИС КНД). Под единой информационной средой контрольно-надзорной деятельности понимается совокупность информационных систем (включая ведомственные информационные системы контрольно-надзорных органов), обеспечивающих исполнение обязанностей, реализацию прав и взаимодействие в электронной форме участников контрольно-надзорной деятельности, а также иных заинтересованных лиц на базе инфраструктуры электронного правительства[5].

[5] Пункт 3.1 Комплексных требований к информационным системам, обеспечивающим выполнение контрольно-надзорных функций органами исполнительной власти (Стандарт информатизации контрольно-надзорной деятельно-

В соответствии со Стандартом информатизации контрольно-надзорной деятельности ведомственная информационная система (либо совокупность ведомственных информационных систем) автоматизации контрольно-надзорной деятельности контрольно-надзорного органа предназначена для обеспечения исполнения обязанностей, реализации прав и взаимодействия в электронной форме в ходе и в связи с контрольно-надзорной деятельностью следующих лиц:

а) контрольные (надзорные) органы;

б) проверяемые лица;

в) независимые поставщики сведений для контрольно-надзорной деятельности;

д) заинтересованные граждане и организации.

При этом ведомственная информационная система (либо совокупность ведомственных информационных систем) автоматизации контрольно-надзорной деятельности контрольно-надзорного органа должна автоматизировать следующие процессы в ходе и в связи с контрольно-надзорной деятельностью:

1) внедрение системы управления рисками при осуществлении контрольно-надзорной деятельности;

2) внедрение системы оценки результативности и эффективности контрольно-надзорной деятельности;

3) систематизация и учет обязательных требований к проверяемым лицам, объектам, видам деятельности;

4) автоматизация проведения профилактической работы;

5) автоматизация внедрения современных кадровых технологий;

6) автоматизация проведения антикоррупционных мероприятий;

7) автоматизация информационного взаимодействия между контрольно-надзорными органами и проверяемыми лицами;

8) автоматизация информационного взаимодействия между контрольно-надзорными органами и органами прокуратуры;

9) автоматизация информационного взаимодействия между контрольно-надзорными органами и иными государственными органами;

10) автоматизация информационного взаимодействия между контрольно-надзорными органами и заинтересованными гражданами и организациями;

11) автоматизация проведения контрольно-надзорных мероприятий;

сти), утверждены протоколом заседания проектного комитета от 14.06.2017 № 40(6)) // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

12) ведение информационных ресурсов ведомственных информационных систем контрольно-надзорных органов.

Таким образом, Стандарт информатизации контрольно-надзорной деятельности предполагает, что со временем будут автоматизированы большинство направлений контрольно-надзорной деятельности.

Более того, Стандарт информатизации контрольно-надзорной деятельности предусматривает три уровня функциональных и технологических характеристик ведомственной информационной системы (либо совокупность ведомственных информационных систем) автоматизации контрольно-надзорной деятельности контрольно-надзорного органа: *базовый, средний, высокий* (уровни соответствия, уровни Стандарта). Порядок реализации контрольно-надзорными органами требований, согласно уровням Стандарта, определяется действующим регулированием, утвержденными планами деятельности, поручениями и иными организационно-распорядительными документами, принимаемыми в том числе в рамках реализации приоритетного проекта «Реформа контрольной и надзорной деятельности».

При этом независимо от уровня Стандарта, ведомственная информационная система контрольно-надзорного органа должна обеспечивать единый интерфейс для осуществления должностным лицом всех регламентных действий в рамках контрольно-надзорной деятельности, на которые оно уполномочено - личный кабинет должностного лица контрольно-надзорного органа. Использование множественных интерфейсов не допускается.

Также Стандартом информатизации контрольно-надзорной деятельности определяются критерии для каждого уровня автоматизации.

На базовом уровне Стандарта допускается низкая автоматизация процессов контрольно-надзорной деятельности, а также хранение сведений в произвольных форматах (без использования НСИ). На этом уровне должны быть частично автоматизированы процессы применения системы управления рисками, а также организации сбора и обработки значений показателей результативности и эффективности контрольно-надзорной деятельности, индикативных показателей. Кроме того, должно быть обеспечено информационное взаимодействие с ФГИС ЕРП (при передаче планов контрольно-надзорных мероприятий), а также с иными государственными органами (при получении сведений о проверяемых лицах).

На среднем уровне Стандарта должны быть полностью автоматизированы процессы применения системы управления рисками, плани-

рования контрольно-надзорных мероприятий, сбора и обработки значений показателей контрольно-надзорной деятельности. Этот уровень также предполагает развитие единых личных кабинетов проверяемого и должностного лиц. Кроме того, ведомственная информационная система (либо совокупность ведомственных информационных систем) автоматизации контрольно-надзорной деятельности контрольно-надзорного органа должна обеспечивать решение отдельных задач при систематизации обязательных требований, предполагается также частичная автоматизация процессов проведения профилактической работы и контрольно-надзорных мероприятий.

На высоком уровне Стандарта предполагается полная автоматизация всех процессов контрольно-надзорной деятельности. Должно быть обеспечено применение проверочных листов, актов о проведении контрольно-надзорных мероприятий и иных документов исключительно в электронной форме. Описание обязательных требований должно быть представлено в машиночитаемой форме. Должно быть обеспечено информационное взаимодействие с иными государственными органами в рамках совместного администрирования контрольно-надзорной деятельности. Кроме того, предполагается широкое применение «больших данных» и «интернета вещей»[6].

Необходимо отметить, что 20 декабря 2017 г. проектным комитетом был утвержден новый Паспорт приоритетного проекта «Автоматизация контрольно-надзорной деятельности»[7]. Его отличительной особенностью от предыдущего Паспорта приоритетного проекта с аналогичным названием стало уточнение основных мероприятий по автоматизации контрольно-надзорной деятельности, утвержденных ранее, а также были конкретизированы мероприятия по каждому контрольно-надзорному органу, которые касаются создания «личных кабинетов», предоставляющих возможность досудебного обжалования в электронном виде; возможности передачи в Единый реестр проверок данных для электронных паспортов проверок; актуализации перечня обязательных требований,

[6] Пункт 4.2 Комплексных требований к информационным системам, обеспечивающим выполнение контрольно-надзорных функций органами исполнительной власти (Стандарт информатизации контрольно-надзорной деятельности), утверждены протоколом заседания проектного комитета от 14.06.2017 № 40(6)) // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

[7] Паспорт приоритетного проекта «Автоматизация контрольно-надзорной деятельности», утв. протоколом заседания проектного комитета от 20.12.2017 № 78(14) // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

подлежащие размещению в сети интернет; в «личном кабинете» реализация функционала ведения электронных паспортов проверки, проверочных листов на базе систематизированных обязательных требований; реализация и использование механизма планирования и учета профилактических мероприятий, направленных на соблюдение проверяемыми лицами обязательных требований по отдельным видам контроля (надзора); внедрена система регуляторной переоценки рисков в зависимости от фактического распределения ущерба по категориям риска по отдельным видам контроля (надзора); и др. (должны быть реализованы в течение 2018 года).

Важным этапом по автоматизации контрольно-надзорной деятельности стало принятие Положения о государственной информационной системе «Типовое облачное решение по автоматизации контрольной (надзорной) деятельности», утвержденное постановлением Правительства РФ от 21 апреля 2018 г. № 482[8].

Стоит отметить, что облачные технологии напрямую связаны с использованием интернета, как средства получения, распространения и хранения информации.

Облачные технологии – это модель предоставления повсеместного и удобного сетевого доступа к общему пулу конфигурируемых вычислительных ресурсов (например, серверы, приложения, сети, системы хранения и сервисы), которые могут быть быстро предоставлены и освобождены с минимальными усилиями по управлению и необходимости взаимодействия с провайдером[9].

С прикладной точки зрения речь идет о возможности хранить и обрабатывать информацию в виртуальной среде, которая создается при помощи аппаратных средств, программного обеспечения и каналов связи на стороне провайдера. Данными, хранящимися в «облаке», можно пользоваться в любой точке мира и с помощью любого гаджета. Единственное условие — доступ в интернет. «Облака» легко настраиваются: всего за несколько минут можно масштабировать дисковое пространство, вычислительные мощности или функционал программного обеспечения[10].

[8] СЗ РФ. 2018. № 18. Ст. 2633.

[9] URL: https://kontur.ru/articles/225 (дата обращения: 01.11.2021).

[10] URL: https://aif.ru/boostbook/oblachnye-tekhnologii-i-reshenija.html (дата обращения: 01.11.2021).

Существует три модели обслуживания облачных вычислений:

1) Программное обеспечение как услуга (SaaS, Software as a Servise). Потребителю предоставляются программные средства – приложения провайдера, выполняемые на облачной инфраструктуре.

2) Платформа как услуга (PaaS, Platform as a Service). Потребителю предоставляются средства для развертывания на облачной инфраструктуре создаваемых потребителем или приобретаемых приложений, разрабатываемых с использованием поддерживаемых провайдером инструментов и языков программирования.

3) Инфраструктура как услуга (IaaS, Infrastructure as a Service). Потребителю предоставляются средства обработки данных, хранения, сетей и других базовых вычислительных ресурсов, на которых потребитель может развертывать и выполнять произвольное программное обеспечение, включая операционные системы и приложения[11].

Например, компания IBM предоставляет потребителям услуги по всем трем видам облачных технологий[12].

Создание и использование облачных решений является общемировой тенденцией и дает множество преимуществ. Никто уже не задается вопросом, стоит ли использовать облака, речь идет о том, где и как из лучше использовать. ИТ-системы в облаке предоставляют уникальную возможность переосмыслить многие процессы и перестроить их оптимальным образом. Облачное решение минимизирует или полностью исключает ИТ-затраты на администрирование серверов, организацию хранилищ, устранение неполадок и пр. К компании появляется возможность задействовать освободившиеся ресурсы на других важных задачах[13].

Типовое облачное решение представляет собой автоматизированную систему сопровождения деятельности инспекторского состава контрольно-надзорных органов, содержащую полное и актуальное описание административных процедур, шаблоны и формы документов, модели принятия решения, что позволит устранить излишнюю степень усмотрения и напрямую повлияет на рост индекса качества администрирования контрольно-надзорных функций.

---

[11] URL: https://kontur.ru/articles/225 (дата обращения: 01.11.2021).

[12] URL: https://www.ibm.com/ru-ru/cloud/learn/iaas-paas-saas (дата обращения: 01.11.2021).

[13] URL: https://pmforesight.ru/argumenty/oblachnoe-reshenie/ (дата обращения: 01.11.2021).

Использование типового облачного решения в региональных КНО будет осуществляться по их выбору и позволит обеспечить эффективное исполнение требований законодательства в части использования риск-ориентированного подхода, межведомственного взаимодействия в электронном виде при осуществлении контрольно-надзорных полномочий, снизить административную нагрузку на граждан и организации по осуществляемым субъектами Российской Федерации видам государственного контроля (надзора). В случае использования региональными контрольно-надзорными органами собственных информационных систем, будет обеспечена их информационная совместимость (интеграция) с федеральными информационными ресурсами.

На первом этапе реформы (2017 год) предусматривалось разработка и ввод в опытную эксплуатацию типового облачного решения, обеспечивающего автоматизацию основных процессов при реализации контрольно-надзорных функций (с *Базовым уровнем* соответствия Стандарту информатизации контрольно-надзорной деятельности (КНД)).

На втором этапе данной реформы (2018 год) предусматривалось модернизация и ввод в эксплуатацию типового облачного решения, обеспечивающего автоматизацию основных процессов при реализации контрольно-надзорных функций, соответствующего *Среднему уровню* Стандарта информатизации КНД.

В соответствии со Стандартом информатизации контрольно-надзорной деятельности, утвержденные протоколом заседания проектного комитета от 14 июня 2017 г. № 40 (6) *личный кабинет* должностного лица контрольно-надзорного органа в ведомственной информационной системе или *в типовом облачном решении*, являющийся ключевым инструментом при организации и осуществлении контрольно-надзорной деятельности, а также единой точкой взаимодействия контрольно-надзорного органа с проверяемыми лицами.

Распоряжением Правительства РФ от 26 сентября 2017 г. № 2049-р[14] был утвержден план мероприятий («дорожная карта») по созданию, развитию и вводу в эксплуатацию информационной системы «Типовое облачное решение по автоматизации контрольной (надзорной) деятельности» на 2017–2019 годы.

Реализация плана мероприятий («дорожной карты») по созданию, развитию и вводу в эксплуатацию информационной системы «Типовое облачное решение по автоматизации контрольной (надзорной) деятельности» на 2017–2019 годы направлена на повышение результативности

[14] СЗ РФ. 2017. № 41. Ст. 5993.

и эффективности контрольной (надзорной) деятельности, в том числе посредством внедрения в деятельность контрольных (надзорных) органов автоматизированных систем при организации и осуществлении ими своей деятельности.

В «дорожной карте» отмечается, что осуществление контрольными (надзорными) органами с определенной периодичностью проверки подконтрольных субъектов зачастую требует повышения эффективности расходования задействованных ресурсов. Одновременно складывается ситуация, при которой количество подконтрольных субъектов превышает потенциальные возможности контрольного (надзорного) органа по их проверке. Это приводит к отсутствию возможности обеспечить безопасность обработки и хранения информации о результатах проверки деятельности подконтрольных субъектов.

Согласно Положению о ГИС ТОР КНД государственная информационная система создается в целях реализации полномочий федеральных органов исполнительной власти, государственных корпораций, публично-правовых компаний, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и подведомственных им организаций, осуществляющих государственный контроль (надзор) и муниципальный контроль, в целях досудебного обжалования решений контрольного (надзорного) органа, действий (бездействия) его должностных лиц при осуществлении государственного контроля (надзора), муниципального контроля, а также в целях осуществления разрешительной деятельности[15].

При этом *задачами создания ГИС ТОР КНД* являются автоматизация процессов:

а) управление рисками причинения вреда (ущерба) охраняемым законом ценностям, вызванного нарушениями обязательных требований, в том числе сбор, обработка, анализ и учет сведений, используемых для оценки и управления рисками причинения вреда (ущерба), с использованием подсистемы координации контрольной (надзорной) деятельности;

б) оценка результативности и эффективности деятельности контрольных (надзорных) органов;

в) учет сведений о соблюдении обязательных требований, в том числе наблюдение за соблюдением обязательных требований (мониторинг

[15] Пункт 2 Положения о государственной информационной системе «Типовое облачное решение по автоматизации контрольной (надзорной) деятельности», утвержденное постановлением Правительства РФ от 21 апреля 2018 г. № 482 // СЗ РФ. 2018. № 18. Ст. 2633.

безопасности) с использованием подсистемы сбора данных государственной информационной системы и данных, получаемых с государственных космических аппаратов дистанционного зондирования Земли, а также продуктов, создаваемых на их основе;

г) межведомственное информационное взаимодействие с гражданами и организациями, контрольными (надзорными) органами, иными государственными органами, органами местного самоуправления и подведомственными им организациями;

д) проведение профилактических и контрольных (надзорных) мероприятий, специальных режимов государственного контроля (надзора), в том числе с использованием мобильного приложения государственной информационной системы;

е) досудебное обжалование решений контрольных (надзорных) органов, действий (бездействия) их должностных лиц;

ж) ведение дел об административных правонарушениях, включая ведение реестра административного делопроизводства;

з) ведение реестров разрешительной деятельности;

и) обеспечение лицензирования заготовки, хранения, переработки и реализации лома черных металлов, цветных металлов[16].

Важно отметить, что *пользователями государственной информационной системы являются:*

1) федеральный орган исполнительной власти, осуществляющий функции по выработке государственной политики и нормативно-правовому регулированию в области государственного контроля (надзора) и муниципального контроля;

2) федеральные органы исполнительной власти, осуществляющие нормативно-правовое регулирование в отношении отдельных видов регионального государственного контроля (надзора), муниципального контроля;

3) исполнительные органы государственной власти субъектов Российской Федерации, уполномоченные в сфере цифровизации государственного управления, а также в случаях, установленных указанными органами, подведомственные им государственные учреждения, обеспечивающие выполнение указанных полномочий;

[16] Пункт 3 Положения о государственной информационной системе «Типовое облачное решение по автоматизации контрольной (надзорной) деятельности», утвержденное постановлением Правительства РФ от 21 апреля 2018 г. № 482 // СЗ РФ. 2018. № 18. Ст. 2633.

4) органы государственной власти субъектов Российской Федерации, уполномоченные на формирование и проведение на территории соответствующего субъекта Российской Федерации единой государственной политики в сфере государственного контроля (надзора), в том числе в области обеспечения прав граждан, организаций при осуществлении регионального государственного контроля (надзора);

5) контрольные (надзорные) органы[17].

Важно отметить, что ТОР КНД будет применяться не для всех видов государственного контроля и надзора. 24 апреля 2018 года проектным комитетом был утвержден Перечень видов государственного контроля (надзора), в отношении которых будут реализованы мероприятия приоритетной программы «Реформа контрольно-надзорной деятельности». Всего было определено более 80 видов государственного контроля и надзора на федеральном уровне. Также на сайте digital.gov.ru размещен Перечень приоритетных видов регионального государственного контроля (надзора) для автоматизации в целях внедрения риск-ориентированного подхода[18].

8 мая 2019 г. приказом Министерства цифрового развития, связи и массовых коммуникаций № 185 была введена в эксплуатацию ГИС ТОР КНД[19]. Она представляет собой цифровую платформу, имеющее название «ПорталКНД» (контрольно-надзорная деятельность)[20]. Он включает в себя три основных раздела:

1) Типовое облачное решение по автоматизации контрольной (надзорной) деятельности (предоставляющий доступ в эту систему);

2) Реестр обязательных требований;

3) Единый реестр видов контроля.

Необходимо отметить, что внедрение ТОР КНД осуществляется в соответствии с цифровыми стандартами, разработанными для каждого

---

[17] Пункт 7 Положения о государственной информационной системе «Типовое облачное решение по автоматизации контрольной (надзорной) деятельности», утвержденное постановлением Правительства РФ от 21 апреля 2018 г. № 482 // СЗ РФ. 2018. № 18. Ст.2633.

[18] URL: https://digital.gov.ru/uploaded/files/perechen-prioritetnyih-vidov-regionalnogo-gosudarstvennogo-kontrolya_Z08smwG.pdf (дата обращения: 01.11.2021).

[19] 3 июня 2019 г. Приказом Министерства цифрового развития, связи и массовых коммуникаций РФ были утверждены Единые функционально-технические требования по автоматизации приоритетных видов регионального государственного контроля (надзора) в целях внедрения риск-ориентированного подхода.

[20] URL: https://knd.gov.ru/main (дата обращения: 01.11.2021).

вида государственного контроля и надзора[21], а доступ в систему осуществляется с помощью Единую систему идентификации и аутентификации (ЕСИА) портала Госуслуг.

Следует отметить, что информационная система ТОР КНД стала универсальной платформенной основой для осуществления контрольно-надзорной деятельности большинство органов исполнительной власти, исполняющих государственные функции по контролю и надзору. При этом как показывает исследование данная система постоянно развивается и совершенствуется, происходят постоянные преобразования цифровых сервисов, направленных как взаимодействие между государственными органами, так и между контрольно-надзорными органами и гражданами и организациями.

Проведенные нами опросы показывают, что среди опрошенных должностных лиц 73% используют в своей работе единые государственные автоматизированные системы, к числу которых и относится ТОР КНД, и всего лишь 4% – не используют никаких информационных систем в своей работе. При этом непосредственно ТОР КНД называют всего лишь 7% опрошенных должностных лиц, что само по себе свидетельствует о слабой осведомленности проверяющих о качественных и технических характеристиках современных цифровых технологий.

Другими немаловажным фактором стало проведение процесса цифровой трансформации. Указом Президента РФ от 21 июля 2020 г. № 474 «О национальных целях развития Российской Федерации на период до 2030 года»[22] к числу национальных целей развития Российской Федерации на период до 2030 года отнесена цифровая трансформация.

Под ***цифровой трансформацией*** понимается совокупность действий, осуществляемых государственным органов, направленных на изменение (трансформации) государственного управления и деятельности государственного органа по предоставлению им государственных услуг и исполнению государственных функций за счет использования данных в электронном виде и внедрения информационных технологий в свою деятельность в целях цифровой трансформации[23].

---

[21] URL: https://knd.gov.ru/document/introduction (дата обращения: 01.11.2021).

[22] СЗ РФ. 2020. № 30. Ст. 4884.

[23] Пункт 2 Положения о ведомственных программах цифровой трансформации, утвержденное постановлением Правительства РФ от 10 октября 2020 г. № 1646 // СЗ РФ. 2020. № 42 (часть 3). Ст. 6612.

Целями цифровой трансформации являются:

а) повышение удовлетворенности граждан государственными услугами, в том числе цифровыми, и снижение издержек бизнеса при взаимодействии с государством;

б) снижение издержек государственного управления, отраслей экономики и социальной сферы;

в) создание условий для повышения собираемости доходов и сокращения теневой экономики за счет цифровой трансформации;

г) повышение уровня надежности и безопасности информационных систем, технологической независимости информационно-технологической инфраструктуры от оборудования и программного обеспечения, происходящих из иностранных государств;

д) обеспечение уровня надежности и безопасности информационных систем, информационно-телекоммуникационной инфраструктуры;

е) устранение избыточной административной нагрузки на субъекты предпринимательской деятельности в рамках контрольно-надзорной деятельности.

Цифровая трансформация также представляет собой процесс интеграции информационных технологий по все аспекты деятельности органа исполнительной власти или внебюджетных фондов, сопровождающийся качественным изменением принципов и процессов оказания государственных услуг, предоставляемых органами исполнительной власти, а также подведомственными организациями в электронном виде, и исполнения государственных функций в целях повышения удовлетворенности граждан государственными услугами, снижения издержек бизнеса при взаимодействии с государством, а также издержек непосредственно государственного управления за счет использования данных, создания условий для повышения собираемости доходов и сокращения теневой экономики за счет цифровой трансформации; повышения уровня надежности и безопасности информационных систем, технологической независимости информационно-технологической инфраструктуры от оборудования и программного обеспечения, происходящих из иностранных государств; обеспечения уровня надежности и безопасности информационных систем, информационно-телекоммуникационной инфраструктуры; устранения избыточной административной нагрузки на субъекты предпринимательской деятельности в рамках контрольно-надзорной деятельности[24].

[24] Пункт 4 Положения о департаменте информационных технологий Министерства труда и социальной защиты Российской Федерации, утвержденного

В практическом плане цифровая трансформация представляет собой разработку и реализацию ведомственной программы цифровой трансформации, в раках которой проводятся мероприятия по информатизации, направленные на выполнение задач по оптимизации административных процессов предоставления государственных услуг и (или) исполнения государственных функций, созданию, развитию, вводу в эксплуатацию, эксплуатации или выводу из эксплуатации информационных систем или компонентов информационно-коммуникационных технологий, нормативно-правовому обеспечению указанных процессов или иных задач, решаемых в рамках цифровой трансформации.

Таким образом, можно констатировать, что непосредственными драйверами для цифровизации контрольно-надзорной деятельности стали мероприятиями, направленные на автоматизацию контрольно-надзорной деятельности, и цифровую трансформацию органов государственного контроля (надзора).

Данные преобразования осуществляются в рамках еще более широкомасштабных российских национальных проектов, таких как «Цифровая экономика Российской Федерации»[25] и «Цифровое государственное управление»[26].

Очевидно, что деятельность российского государства, направленная на цифровизацию государственного управления, приносит свои позитивные результаты, которые воплощаются в серьезных преобразованиях в деятельности органов исполнительной власти, осуществляющих различные государственные функции. Деятельность государственных органов соответствует запросам общества, развитию технологического прогресса и условиям «цифровой экономики».

приказом Министерства труда и социальной защиты РФ от 18 марта 2021 г. № 127 // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

[25] Распоряжение Правительства РФ от 28 июля 2017 г. № 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации» (утратило силу) // СЗ РФ. 2017. № 32. Ст. 5138; Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации», утвержден президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 4 июня 2019 г. № 7 // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

[26] Паспорт федерального проекта «Цифровое государственное управление», 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 // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

Предпринятые государством меры позволили модернизировать деятельность контрольно-надзорных органов, поставив ее на рельсы автоматизации и цифровой трансформации. Тем самым сделан существенный задел по развитию таких цифровых сервисов, используемых контрольно-надзорными органами, как «личный кабинет» должностного лица (инспектора) контрольно-надзорного органа, формирование Единого реестра проверок в электронном виде, включение Единого портала государственных услуг в единую среду информационную среду контрольно-надзорной деятельности, повсеместное и широко применяемое государственных информационных систем, таких ГИС «Управление», ведомственных информационных систем, использование онлайн-сервисов для самопроверки контролируемыми лицами, рассмотрение электронных обращений (жалоб) в электронной форме, и др.

Внедрение современных цифровых технологий в контрольно-надзорную деятельность способствуют появлению новых характеристик этой деятельности:

1) *анализ и обработка большого массива полученной информации о контролируемом объекте в автоматическом режиме.* Основой контрольно-надзорной деятельности является получение информации о проверяемом объекте, которая сопоставляется с обязательными требованиями. В результате этого сопоставления должностными лицами контрольно-надзорных органов делаются выводы о соблюдении либо не соблюдении обязательных требований подконтрольным (поднадзорным) лицом. Применение современных цифровых технологий, позволяющих в автоматическом режиме и без участия человека, определить на основе полученной информации соблюдаются ли проверяемым лицом обязательные требования или нет, значительно ускоряет процесс проверки, делает его более прозрачным и независимым.

2) *использование в контрольно-надзорной деятельности риск-ориентированного подхода при проведении контрольно-надзорных мероприятий может основываться на современных цифровых технологиях.* Расчет риска может происходить в автоматическом режиме посредством применения суперкомпьютерных вычислений и искусственного интеллекта. В этом плане риск-ориентированный подход становится может рассматриваться как часть автоматизированной деятельности контрольно-надзорных органов.

3) *современные цифровые технологии позволяют исключить непосредственное взаимодействие (контакт) между контрольно-надзорным органов и проверяемым лицом.* С одной стороны, это позволяет

минимизировать вмешательство в деятельность проверяемого лица, а это снижает издержки от контрольно-надзорных мероприятий, с другой стороны, обеспечивается более высокая беспристрастность и независимость проверочных мероприятий, исключаются коррупционные риски.

4) *посредством цифровых технологий может обеспечиваться на более высоком уровне взаимодействие между контрольно-надзорными органами и проверяемыми лицами.* Цифровое взаимодействие может происходить посредством цифровых платформ (цифровых суперсервисов). Например, Единый портал государственных и муниципальных услуг (функций)» (Госуслуги) позволяет в качестве эксперимента подать административную жалобу на действия должностных лиц контрольно-надзорных органов или обжаловать результаты контрольно-надзорных мероприятий (пока в качестве эксперимента).

5) *с помощью современных технологий обеспечивается транспарентность контрольно-надзорной деятельности.* Размещение открытых данных о контрольно-надзорной деятельности в сети Интернет, взаимодействие между органами государственного контроля (надзора) и контролируемыми лицами в электронной форме без непосредственного взаимодействия, электронные платформы и сервисы проверок и самопроверок, позволяет исключить злоупотребление правами должностных лиц контрольно-надзорных органов и исключить коррупционные риски, то есть обеспечивается необходимая открытость и прозрачность контрольно-надзорной деятельности[27].

Необходимую правовую основу для внедрения в деятельность контрольно-надзорных органов также заложил Федеральный закон от 31 июля 2020 г. № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации»[28]. В новый закон была включена Глава 4, посвященная информационному обеспечению государственного контроля (надзора), муниципального контроля, кото-

[27] Мартынов А.В. Влияние цифровой трансформации на контрольно-надзорную деятельность органов исполнительной власти // Публичная власть в современной России: проблемы и перспективы: сборник научных трудов по материалам международной научно-практической конференции памяти доктора юридических наук, профессора, заслуженного деятеля науки РСФСР Василия Михайловича Манохина (VII Саратовские административно-правовые чтения) (8 июня 2021 г., Саратов) / под общ. ред. А.Ю. Соколова; редкол. А.Ю. Соколов и др.; Саратовская государственная юридическая академия; Саратовский филиал ФГБУН «Институт государства и права РАН». Саратов: Изд-во Саратовской государственной юридической академии, 2021. С. 32–56.

[28] СЗ РФ. 2020. № 31 (часть 1). Ст. 5007.

рая входит в Раздел II «Организация государственного контроля (надзора), муниципального контроля».

В статье 17 Федерального закона от 31 июля 2020 г. № 248-ФЗ устанавливается, что в целях информационного обеспечения государственного контроля (надзора), муниципального контроля создаются:

1) единый реестр видов федерального государственного контроля (надзора), регионального государственного контроля (надзора), муниципального контроля;

2) единый реестр контрольных (надзорных) мероприятий;

3) информационная система (подсистема государственной информационной системы) досудебного обжалования;

4) реестр заключений о подтверждении соблюдения обязательных требований;

5) информационные системы контрольных (надзорных) органов.

Указанным базовым федеральным законом предусматриваются и другие направления внедрения современных цифровых технологий в контрольно-надзорную деятельность органов исполнительной власти. Таким образом, можно констатировать, что в настоящее время создана серьезная правовая основа для внедрения и апробации современных цифровых технологий в контрольно-надзорную деятельность органов публичного управления.

Следует особо отметить, что российское государство не собирается останавливаться на достигнутом уровне автоматизации контрольно-надзорной деятельности.

Так, распоряжением Правительства РФ от 22 октября 2021 г. № 2998-р было утверждено Стратегическое направление в области цифровой трансформации государственного управления[29].

В документе устанавливается, что в ходе реализации стратегического направления будут внедрены следующие технологии:

1) искусственный интеллект;

2) большие данные;

3) интернет вещей.

Стратегическое направление утверждается до 2030 года, актуализация стратегического направления возможна ежегодно, но не более одного раза в год. Реализация стратегического направления предусматривает достижение следующих показателей национальных целей развития

[29] Распоряжение Правительства РФ от 22 октября 2021 г. № 2998-р «Об утверждении стратегического направления в области цифровой трансформации государственного управления» // СЗ РФ. 2021. № 44 (часть III). Ст. 7467.

Российской Федерации, определенных Указом Президента РФ от 21 июля 2020 г. №474 «О национальных целях развития Российской Федерации на период до 2030 года»:

1) достижение «цифровой зрелости» ключевых отраслей экономики, социальной сферы, в том числе здравоохранения и образования, а также государственного управления;

2) доля массовых социально значимых услуг, доступных в электронном виде;

3) увеличение вложений в отечественные решения в сфере информационных технологий в 4 раза по сравнению с показателем 2019 года.

Задачами цифровой трансформации государственного управления являются повышение качества и системности исполнения следующих государственных функций:

а) государственное регулирование и выработка государственной политики в отраслях экономики и социальной сфере;

б) предоставление государственных и муниципальных услуг;

в) осуществление контрольной и надзорной деятельности;

г) управление государственным имуществом;

д) обеспечение безопасности государства в целом и граждан в частности[30].

Иными словами, на следующем этапе государством планируется сделать акцент именно на «сквозных цифровых технологиях»: искусственный интеллект, большие данные, интернет вещей.

В действующем законодательстве Российской Федерации закреплено понятие «искусственного интеллекта», под которым понимается комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе, в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений. Технологии искусственного интеллекта представляют собой технологии, основанные на использовании искусствен-

[30] Раздел II Стратегического направления в области цифровой трансформации государственного управления, утвержденного распоряжением Правительства РФ от 22 октября 2021 г. № 2998-р // СЗ РФ. 2021. № 44 (часть III). Ст. 7467.

ного интеллекта, включая компьютерное зрение, обработку естественного языка, распознавание и синтез речи, интеллектуальную поддержку принятия решений и перспективные методы искусственного интеллекта[31].

По нашему мнению, применение искусственного интеллекта при осуществлении контрольно-надзорной деятельности должно основываться на следующих принципах: законность, целесообразность, безопасность, прозрачность (открытость), подконтрольность, стабильность, моделирование, экспертная оценка[32].

Термин «большие данные» официально не закреплен в российском законодательстве, хотя и употребляется в различных нормативных правовых актах. Между тем, в Стандарте информатизации контрольно-надзорной деятельности указывается, что «большие данные» – это совокупности структурированных и неструктурированных данных значительных объемов, подлежащих обработке с использованием методов статистического анализа с целью категоризации, визуализации, получения прогнозных показателей. Обработка «больших данных» требует использования существенных вычислительных мощностей.

В Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы[33] отмечается, что *обработка больших объемов данных* представляет собой совокупность подходов, инструментов и методов автоматической обработки структурированной и неструктурированной информации, поступающей из большого количества различных, в том числе разрозненных или слабосвязанных, источников информации, в объемах, которые невозможно обработать вручную за разумное время.

Следовательно, большие данные должны аккумулироваться в различных информационных системах, используемых государственными органами, после чего, они должны использоваться для компьютерных вычислений, аналитической работы, принятии управленческих решений, в том числе с применением искусственного интеллекта.

---

[31] Подпункты «а» и «б» пункта 5 Национальной стратегии развития искусственного интеллекта на период до 2030 года, утвержденная Указом Президента РФ от 10 октября 2019 г. № 490 // СЗ РФ. 2019. № 41. Ст. 5700.

[32] Мартынов А.В., Бундин М.В. О правовых принципах применения искусственного интеллекта при осуществлении органами исполнительной власти контрольно-надзорной деятельности // Журнал российского права. 2020. № 10. С. 59–75.

[33] Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // СЗ РФ. 2017. № 20. Ст. 2901.

Интернет вещей представляет собой концепцию вычислительной сети, соединяющей вещи (физические предметы), оснащенные встроенными информационными технологиями для взаимодействия друг с другом или с внешней средой без участия человека[34]. Интернет вещей также определяется как совокупность сетей межмашинных коммуникаций и систем хранения (обработки) больших данных, в которых за счет подключения датчиков и актуаторов (исполнительных механизмов) к сети реализуется цифровизация различных процессов и объектов (Internet of Things, IoT)[35].

В Стандарте информатизации контрольно-надзорной деятельности данный термин используется для обозначения следующих сущностей:

а) средства измерения, обеспечивающие преобразование сведений о внешней среде в машиночитаемые данные (датчики, например, температуры, давления, освещенности, приборы учета потребления, иные измерительные системы), установленные на проверяемых объектах;

б) средства передачи данных от средств измерений в информационные системы проверяемых лиц, внешних поставщиков сведений для контрольно-надзорной деятельности, в ведомственные информационные системы контрольно-надзорных органов (в зависимости от используемой организационной и технологической схемы);

в) средства обработки данных в информационных системах проверяемых лиц, внешних поставщиков сведений для контрольно-надзорной деятельности в ведомственные информационные системы контрольно-надзорных органов (в зависимости от используемой организационной и технологической схемы).

Как отмечается в Стандарте информатизации контрольно-надзорной деятельности «большие данные» и «интернет вещей» должны применяться на высоком уровне Стандарта информатизации контрольно-надзорной деятельности. Предполагается, что динамическое управление категориями риска, классами опасности должно осуществляться в автоматическом режиме на основании оперативно поступающих сведений, в том числе данных датчиков, установленных на проверяемых объектах

[34] Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // СЗ РФ. 2017. № 20. Ст. 2901.

[35] Концепция обеспечения безопасности дорожного движения с участием беспилотных транспортных средств на автомобильных дорогах общего пользования, утвержденная распоряжением Правительства РФ от 25 марта 2020 г. № 724-р // СЗ РФ. 2020. № 13. Ст. 1995.

(«интернет вещей»). В тех случаях, когда для оценки соответствия проверяемого лица обязательным требованиям достаточно сведений от датчиков, установленных на проверяемых объектах («интернет вещей»), для проведения самооценки проверяемым лицом не требуется формирование листа самооценки и его заполнение проверяемым лицом. Ведомственная информационная система контрольно-надзорного органа должна обеспечивать автоматическую фото- и видеофиксацию ключевых фактов контрольно-надзорных мероприятий (например, фактов досмотра товаров), либо сохранение иных полученных с использованием датчиков («интернет вещей») сведений о ключевых фактах контрольно-надзорных мероприятий (например, результатов замера температуры или влажности) без возможности редактирования или удаления каких-либо данных должностным лицом контрольно-надзорного органа, осуществляющим проведение контрольно-надзорных мероприятий[36].

Таким образом, предполагается, что все три «сквозные» цифровые технологии (искусственный интеллект, большие данные, интернет вещей) будут основой для новой цифровой платформы, которая будет обеспечивать все ключевые процессы контрольно-надзорной деятельности. Данная цифровая платформа объединит такие государственные информационные системы как ИС «Реестр обязательных требований», ГИС ТОР КНД, ФГИС «Единый реестр проверок». При этом «сквозные» цифровые технологии должны обеспечивать взаимосвязь, обмен информацией, подготовку управленческих решений для должностных лиц контрольно-надзорных органов, и т.п.[37].

Кроме этого, на региональном уровне происходит автоматизация деятельности органов регионального государственного контроля и надзора. Так, в 2020 году в г. Москве создана цифровая платформа взаимодействия бизнеса контрольно-надзорных органов «Открытый контроль»[38].

---

[36] Комплексные требования к информационным системам, обеспечивающим выполнение контрольно-надзорных функций органами исполнительной власти (Стандарт информатизации контрольно-надзорной деятельности), утверждены протоколом заседания проектного комитета от 14.06.2017 № 40(6)) // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

[37] URL: https://digital.gov.ru/uploaded/files/tsifrovaya-platforma-kontrolnoj-i-nadzornoj-deyatelnosti.pdf (дата обращения: 01.11.2021).

[38] URL: https://knd.ac.gov.ru/wp-content/uploads/2020/12/Otkrytyi-_kontrol_GKU.pdf (дата обращения: 01.11.2021).

Если говорить о дальнейших перспективах внедрения современных цифровых технологий в деятельность органов государственного контроля и надзора, то следует отметить несколько ключевых моментов.

Во-первых, в ближайшие несколько лет планируется создание цифровой платформы мониторинга контроля и надзора в России. Основные задачи проекта – объединить все информационные системы государственных структур, участвующих в контрольно-надзорной деятельности, обеспечив аналитическую обработку этой информации в режиме реального времени на территории всей страны. В рамках этого проекта должны объединиться все созданные в контрольно-надзорной деятельности информационные системы, в том числе уже объединяющиеся сейчас в рамках нового закона о государственном контроле. По нему созданы и запущены в 2020-2021 годах в промышленную эксплуатацию три государственных информационных системы: единый реестр контрольных (надзорных) мероприятий (он приходит на смену Единому реестру проверок, существовавшему в том числе для их согласования с прокуратурой), единый реестр видов контроля и информационная система досудебного обжалования. Таким образом, единая цифровая платформа должна сильно расширить возможности Правительства РФ в контрольно-надзорной деятельности. Это должно произойти за счет доступа к аналитике по всем видам государственного контроля и надзора в режиме реального времени, сопоставления ее с данными ГАС «Управление» и другими государственными информационными системами, в том числе бюджетными, в результате чего станут возможными детальные и достоверные оценки деятельности контрольно-надзорных органов, результативности контрольно-надзорной деятельности, а также связи особенностей ее устройства в конкретном органе с показателями. Но главными идеями единой цифровой платформы считаются настраиваемая и масштабируемая система, позволяющая продолжить реформу контрольно-надзорной деятельности во внепроектном режиме, и возможная постоянная динамическая адаптация контрольно-надзорной деятельности к нуждам экономики[39].

По нашему мнению, создание такой «объединенной» цифровой платформы имеет хорошую перспективу. Безусловно, данная цифровая платформа должна интегрирована другой базовой цифровой платформой – Типовое облачное решение контрольно-надзорной деятельности

[39] Бутрин Д. Наблюдение за наблюдающими // Газета Коммерсантъ. 2021. 19 июля. № 124 (7086) [Электронный ресурс]. URL: https://www.kommersant.ru/doc/4908320 (дата обращения: 01.11.2021).

(ТОР КНД), которая также должна развиваться и совершенствоваться. Амбициозной задачей будет считаться интеграция в единую цифровую платформу и региональных и муниципальных цифровых платформ.

Вместе с тем, как показывает опыт, существуют серьезная опасность повторения судьбы цифровой платформы – Открытое правительство РФ. Это была одна из самых динамично развивающихся цифровых платформ, объединяющая и интегрирующая различные информационные ресурсы других государственных органов. Кроме этого, цифровая платформа Открытого правительства обеспечивала на самом высоком уровне взаимодействие между органами государственной власти, экспертным сообществом, гражданами и организациями. Данный проект планировалось интегрировать с системами открытого правительства зарубежных стран. Однако указанный проект прекратил существование по ряду причин, одной из которых стало широкий доступ граждан к информации о деятельности государственных органов и возможность влиять на принятие ими управленческих решений[40].

Во-вторых, важным направлением цифровизации контрольно-надзорной деятельности должна стать активное внедрение цифровых технологий в осуществление контрольно-надзорных мероприятий. Так, при осуществлении отдельных видов государственного контроля и надзора начинают внедряться системы дистанционного контроля. 1 февраля 2021 года был запущен эксперимент по внедрению дистанционного контроля промышленной безопасности[41]. Полученные при дистанционном контроле показатели о состоянии промышленной безопасности опасных производственных объектов учитываются Ростехнадзором при осуществлении федерального государственного надзора в области промышленной безопасности.

В соответствии со ст.96 Федерального закона от 31 июля 2020 г. №248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации»[42] под мониторингом понимается режим дистанционного государственного контроля (надзора), заключающийся в целенаправленном, постоянном (систематическом, регуляр-

[40] См., подробнее: Мартынов А.В. Туманные перспективы системы «Открытое правительство» в эпоху цифровой экономики России // Законы России: опыт, анализ, практика. 2018. № 11. С. 10–23.

[41] См.: Постановление Правительства РФ от 31 декабря 2020 г. № 2415 «О проведении эксперимента по внедрению системы дистанционного контроля промышленной безопасности» // СЗ РФ. 2021. № 3. Ст. 557.

[42] СЗ РФ. 2020. № 31 (часть 1). Ст. 5007.

ном, непрерывном), опосредованном получении и анализе информации о деятельности граждан и организаций, об объектах контроля с использованием систем (методов) дистанционного контроля, в том числе с применением специальных технических средств, имеющих функции фотосъемки, аудио- и видеозаписи, измерения, должностными лицами контрольного (надзорного) органа в целях предотвращения причинения вреда (ущерба) охраняемым законом ценностям.

Опрошенные нами должностные лица контрольно-надзорных органов исполнительной власти наиболее перспективными информационными технологиями для осуществления контрольно-надзорной деятельности считают именно системы дистанционного контроля и электронные сервисы проверок (26% респондентов). При этом на втором и третьем местах находятся ответы – технологии искусственного интеллекта (10%), облачные технологии и синхронизированные государственные информационные системы – по 8%.

Безусловно, дальнейшая автоматизация контрольно-надзорных мероприятий, осуществляемых органами государственного контроля и надзора, должна преобладать в большинстве видов контрольно-надзорной деятельности, а более высоким уровнем автоматизации должна стать роботизация контрольно-надзорных действий.

В-третьих, важным условием дальнейшей цифровизации контрольно-надзорной деятельности должно быть внедрение «сквозных» цифровых технологий. Несмотря на наличие стратегического направления в области цифровой трансформации государственного управления[43], предполагающего активное внедрение в сферу осуществления контрольно-надзорной деятельности такие «сквозных» цифровых технологий как искусственный интеллект, большие данные, интернет вещей, не должны оставаться без развития и другие «сквозные» цифровые технологии: цифровые двойники, мобильные сети связи пятого поколения (цифровые сервисы), новые коммуникационные интернет-технологии, технологии виртуальной и дополненной реальности, технологии распределенных реестров, квантовые коммуникации, квантовые сенсоры, квантовые вычисления, и др.

При этом должна рассматриваться возможность появления ранее неизвестных новых цифровых технологий, которые при широком рас-

[43] Распоряжение Правительства РФ от 22 октября 2021 г. № 2998-р «Об утверждении стратегического направления в области цифровой трансформации государственного управления» // СЗ РФ. 2021. № 44 (часть III). Ст. 7467.

пространении могут также внедряться в контрольно-надзорную деятельность.

При внедрении «сквозных» цифровых технологий необходимо детально изучать опыт зарубежных стран (США, Китай, Япония, Южная Корея, Германия, Великобритания, и т.д.), которые являются лидерами по внедрению современных «сквозных» цифровых технологий в различные сферы государственного управления, а поэтому могут иметь как положительный, так и негативный опыт по применению таких цифровых технологий.

Нельзя отказываться от взаимодействия с частными компаниями, которые активно внедряют «сквозные» цифровые технологии в свою деятельности. По мотивам обеспечения национальной безопасности приоритет при таком взаимодействии должен отдаваться отечественным частным компаниям.

Безусловно, необходимо учитывать, что сами по себе «сквозные» цифровые технологии требуют колоссальных затрат со стороны государства, а поэтому при внедрении подобных в контрольно-надзорную деятельность должно детально просчитываться финансовая составляющая, то есть внедрение «сквозных» технологий должно обосновываться высокой эффективность и результативностью государственного контроля и надзора, возможностью за счет этих цифровых технологий предотвратить угрозы жизни и здоровью большого числа граждан, либо предотвратить значительный материальный ущерб окружающей среди или имуществу граждан и организаций.

В-четвертых, цифровизация государственного контроля и надзора должна быть интегрирована с другими сферами государственного управления, в которых активно применяются современные цифровые технологии. Цифровые технологии, применяемые в контрольно-надзорной деятельности, должны предоставлять возможность интеграции с другими информационно-коммуникационными системами, прежде всего, такими как «Умный город», «Безопасный город», «Интеллектуальные транспортные системы», «Умное производство», «Умная ферма», «Цифровая медицина», высокоавтоматизированные информационные системы налогообложения и таможенного декларирования, и т.д.

Необходима интеграция и распространение цифровых (мобильных) приложений для смартфонов и планшетов, пользователями которых будут являться должностные лица контрольно-надзорных органов и контролируемые лица.

Важный акцент должен быть сделан на цифровых платформах, которые будут интегрированы в цифровую платформу контрольно-

надзорной деятельности, позволяющие осуществлять общественный контроль и общественное взаимодействие органов государственного контроля и надзора, и контролируемых лиц.

В-пятых, необходимо дальнейшее расширение сферы действия Федерального закона от 31 июля 2020 г. № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации», осуществляющего правовое регулирование вопросов информационного обеспечения государственного контроля (надзора), муниципального контроля. Положения указанного Федерального закона должны совершенствоваться по мере внедрения в деятельность контрольно-надзорных органов современных цифровых технологий.

Следует также признать успешным опыт введения экспериментальных правовых режимов по применению современных цифровых технологий при осуществлении отдельных видов государственного контроля и надзора.

Все вышеперечисленные направления внедрения передовых цифровых технологий в контрольно-надзорную деятельность способствуют формированию новой правовой концепции современной системы государственного контроля и надзора, а также муниципального контроля.

§ 2. Основные положения концепции правового регулирования государственного контроля и надзора в условиях «цифровой экономики»

С начала XXI века в России ведутся поиски новой наиболее оптимальной теоретической концепции государственного контроля и надзора. Как в теории административного права, так и в действующем законодательстве Российской Федерации, преобладала концепция, разработанная видными советскими учеными в 70-80 годы XX века. В основе этой концепции лежал системный подход, то есть контроль и надзор рассматривались как часть системы управления, и выступали как общая и специальная функции управленческой деятельности. Согласно данной концепции, государственный контроль и государственный (административный) надзор рассматривались также в качестве способов обеспечения законности и дисциплины в государственном управлении, наряду с прокурорским надзором, судебным контролем и общественным контролем. При этом на теоретическом уровне учеными разграничивались эти виды управленческой деятельности: деятельность по осу-

ществлению государственного контроля и деятельность по осуществлению административного надзора.

1. Одним из основоположников советской концепции государственного контроля и административного надзора является профессор Марина Семеновна Студеникина. Она, раскрывая сущность государственного контроля, указывала, что «*контроль как функция управления* присуща та специфическая черта, что эта функция *проводится всеми государственными органами независимо от их основных задач и вида деятельности, которые они осуществляют*. Однако, поскольку контроль не выступает в изолированном виде, а реализуется применительно к конкретному предметному содержанию, объем контрольной деятельности, формы и методы ее проявления дифференцируются в зависимости от сферы или отрасли управления, а также от места органа, осуществляющего контрольные полномочия, в общей системе государственного механизма»[44]. С ее точки зрения, «*властность контроля проявляется в наличии у контрольных органов ряда полномочий, связанных с возможностью*: а) давать подконтрольным объектам обязательные для исполнения указания об устранении вскрытых недостатков; б) ставить перед компетентными инстанциями вопрос о привлечении к ответственности виновных в обнаруженных нарушениях лиц; в) непосредственно применять в ряде случаев меры государственного принуждения»[45].

Важное значение имеют также и выводы, сделанные М.С. Студеникиной, относительно разграничения государственного контроля и административного надзора: «*различие между административным надзором и контролем в широте, охватываемой обследованием сферы деятельности, а также в специфике методов и правовых форм воздействия.* Для контроля характерна та особенность, что он не ограничивается кругом вопросов, связанных с соблюдением обязательных предписаний – законов и других нормативных актов. Органы контроля интересуются не только тем, не нарушил ли субъект управления действующее законодательство, но и тем, насколько правильно, целесообразно и эффективно он использовал все представленные ему полномочия. *Специфика административного надзора* проявляется в ограничении пределов его компетенции проверкой только законности действий конкретного

[44] Студеникина М.С. Государственный контроль в сфере управления. М.: Юридическая литература, 1974. С. 9.

[45] Там же. С. 11.

объекта. *Надзор – своего рода суженный контроль, но суженный только в отношении сферы своего приложения*»[46].

Большой вклад в развитие теории государственного контроля внесла также *Е.В. Шорина. В ее фундаментальной работе «Контроль за деятельностью органов управления в СССР»*[47] (1981 год) проводится детальный анализ института контроля в сфере государственного управления. Так, Е.В. Шориной, в частности, отмечается, что «Содержание контроля производно от содержания управленческой деятельности, поскольку она распространяется на все органы, весь управленческий персонал. Но, как бы ни был разнообразен контроль, велико число занимающихся им органов и лиц, проверить управленческую деятельность в полном объеме ввиду ее масштабности, оперативности, сложности, разнохарактерности практически немыслимо. Возможен контроль только за основными, важнейшими сторонами управления, обеспечивающими эффективность работы того или иного органа, лица, аппарата советского государственного управления в целом. Основные направления контроля включают множество других, более частных направлений, зависящих от уровня, назначения, характера работы проверяемого органа управления»[48].

По ее мнению, *к основным направлениям контроля за деятельностью органов государственного управления* относятся:

1) контроль за соблюдением государственной дисциплины, своевременным и доброкачественным выполнением обязанностей по управлению;

2) контроль за рациональным распределением и использованием материальных, финансовых, трудовых и иных ресурсов, бережным отношением к социалистической собственности, соблюдением режима экономии;

3) контроль за научной организацией управленческого труда, внедрением в управление и производство новейших достижений науки и техники, их использованием в интересах повышения эффективности производства с учетом необходимости безопасности производимых работ, охраны здоровья населения, предупреждения загрязнения окружающей среды и иных возможных вредных последствий;

---

[46] Там же. С. 18; Студеникина М.С. Государственные инспекции в СССР. М.: Юридическая литература, 1987. С. 13.

[47] См.: Шорина Е.В. Контроль за деятельностью органов государственного управления в СССР. М.: Издательство «Наука», 1981. 302 с.

[48] Шорина Е.В. Указ. Соч. С. 47.

4) контроль за законностью и целесообразностью принимаемых управленческих решений, издаваемых правовых актов;

5) контроль за соблюдением прав и свобод, охраняемых законом интересов граждан;

6) контроль за подбором, расстановкой, повышением идейного и теоретического уровня, деловой квалификации управленческих кадров;

7) контроль за формами и методами осуществления управленческой деятельности[49].

Значительный интерес представляют также виды контроля, выделяемые Е.В. Шориной. Так, ею отмечается, что «по своему содержанию контроль может быть общим и специальным. Общий контроль распространяется на все стороны деятельности контролируемых объектов и лиц, а специальный – только на какую-либо одну из сторон (достоверность отчетных данных, соблюдение трудовых прав граждан и т.п.). Специальный контроль проводится, как правило, только предназначенными для этого органами и по определенному кругу вопросов»[50].

В.М. Горшенев и И.Б. Шахов рассматривали контроль как правовую форму деятельности[51]. С их точки зрения, контроль, как функция социального управления, направляет процесс управления по установленным идеальным моделям, корректируя поведение подконтрольного объекта. Сущность контроля состоит в том, что субъект управления осуществляет учет и проверку того, как управляемый объект выполняет его предписания. Основной целью данной функции является блокирование отклонений деятельности субъекта управления от заданной управленческой программы, а при обнаружении аномалий – приведение управляемой системы в устойчивое положение при помощи всех социальных регуляторов[52].

Интересным образом данные ученые описывают процесс контроля: «в процессе контроля выявляются: качество самого управленческого решения; эффективность тех организационных мер, которые были приняты для его исполнения; соответствие организации объекта целям успешного выполнения предписаний, содержащихся в управленческом

---

[49] Шорина Е.В. Указ. соч. С. 47-48.

[50] Там же. С. 97.

[51] См.: Горшенев В.М., Шахов И.Б. Контроль как правовая форма деятельности. М.: Юридическая литература, 1987. 176 с.

[52] Там же. С. 23.

решении, а также качество подбора, расстановки и воспитания кадров, исполняющих решение»[53].

Особо следует отметит, что именно В.М. Горшеневым и И.Б. Шаховым делается акцент на информационную и коррекционную составляющие контроля. Они отмечают: *«Контроль является универсальным средством получения информации по каналу обратной связи.* Без механизма обратной связи между субъектом и объектом процесс социального управления потерял бы четкость и целенаправленность. Для того, чтобы успешно управлять, тот, кто управляет, должен знать результаты своего управленческого воздействия на объекты управления. Контроль позволяет получить оперативную информацию, объективно отражающую положение дел на подконтрольных объектах, соответствие их деятельности намеченной программе, выявить недостатки в содержании принимаемых решений, организации их исполнения, способах и средствах их реализации, изучить деловые качества работников»[54].

Учеными также выделяются функции контрольной деятельности: функция корректировки, функция социальной превенции и функция правоохраны[55]. Они обращают внимание на то, что «профилактика является наиболее перспективным видом контрольной деятельности, основное назначение которой предупредить возможные правонарушения, определить меры по устранению условий, способствующих совершению правонарушений, а в случае обнаружения неправомерного поведения привести в действие соответствующие правоохранительные средства»[56].

Как и другие ученые, В.М. Горшенев и И.Б. Шахов не разграничивают контрольную и надзорную деятельность. Они используют термин «контрольно-надзорная деятельность», под которой они понимают, с одной стороны, специфическую правовую форму управленческой деятельности органов Советского государства, а с другой – как организационно-юридическое средство обеспечения законности в управленческой деятельности[57].

Таким образом, подводя итог рассмотрению теоретических взглядов на государственный контроль и административный надзор Советского периода времени, следует констатировать, что *теорией Советского*

---

[53] Горшенев В.М., Шахов И.Б. Указ. соч. С. 24.
[54] Там же.
[55] Там же. С. 31-35.
[56] Горшенев В.М., Шахов И.Б. Указ. соч. С. 33.
[57] Там же. С. 29.

административного права был сформирован ряд концептуальных положений, раскрывающих сущность, содержание и отличительные особенности государственного контроля и административного надзора. Резюмируя вышеизложенные позиции ученых в области административного права, приведем ключевые признаки данных категорий:

Во-первых, государственный контроль и административный надзор входили в единую систему механизма управления различными отраслями и сферами государственного управления. Данные институты рассматривались в качестве неотъемлемой части государственного управления народным хозяйством, предприятиями, учреждениями, организациями, относящимися к государственному сектору экономики. Некоторыми учеными по сути дела не разграничивались данные понятия, *административный надзор же, рассматривался в качестве специального или специализированного надведомственного контроля*[58]. Однако все же большинство советских ученых в области административного права пытались проводить разграничение между данными понятиями. Об этом явно свидетельствуют классические учебники по Советскому административному праву того периода времени.

Во-вторых, если государственный контроль признавался *составной частью государственного управления, одной из его общих функций, методом реализации управленческой компетенции,* то административный надзор соответственно рассматривался как разновидность надведомственного (специального) контроля, являющегося также составной частью государственного управления, но *представляющего собой специальную подфункцию государственного управления и особый метод управленческой компетенции.*

В-третьих, государственный контроль и административный надзор рассматриваются как смежные понятия. Они были включены в единый административно-правовой институт способов обеспечения законности и дисциплины в советском государственном управлении. При этом рядом ученых при характеристике государственного контроля и административного надзора стал использоваться термин «контрольно-надзорная деятельность»[59].

В-четвертых, при осуществлении государственного контроля осуществляется проверка в отношении организационно подчиненных

[58] Шорина Е.В. Указ. соч. С. 98–100.

[59] Советское административное право: учебник / под ред. заслуженного деятеля науки УССР, доктора юридических наук, профессора Р.С. Павловского. Киев: «Вища школа», 1986. С. 241.

субъектов (государственных органов, предприятий, учреждений, организаций), то при административном надзоре происходит напротив проверка деятельности организационно неподчиненных субъектов, в том числе и граждан. Тем самым обуславливается и подчеркивается *надведомственный характер административного надзора.*

В-пятых, отличается также предмет государственного контроля и административного надзора. При государственном контроле осуществляется *проверка всей деятельности подконтрольного субъекта*, а при административном надзоре только *проверка исполнения (соблюдения) специальных правил и норм, установленных уполномоченными на то органами.* Административный надзор ограничен проверкой только законности действия конкретного объекта, когда как при государственном контроле действия объекта оцениваются еще и с точки зрения правильности, целесообразности и эффективности.

В-шестых, особенностью государственного контроля и административного надзора являлось установление органами государственного управления, осуществляющими функции по контролю и надзору, нормативных требованиях, являющихся предметом проверки со стороны органов и должностных лиц государственного контроля и административного надзора.

В-седьмых, общей характеристикой государственного контроля и надзора является возможность *по результатам проверки подконтрольных и поднадзорных субъектов применения мер административного принуждения*. Однако характер этих различен. Если при государственном контроле применяются *меры дисциплинарного воздействия,* то при административном надзоре напротив *меры административного воздействия* (например, штраф).

В-восьмых, устанавливалось различие в видах и компетенции государственных органов, осуществляющих государственный контроль и административный надзор. *Государственный контроль осуществляется государственными органами общей компетенции.* Если говорить о подвидах государственного контроля: надведомственный и внутриведомственный контроль, то он *может осуществляться государственными органами межотраслевой или отраслевой компетенции.* Для административного надзора характерно его *осуществление исключительно государственными органами, наделенными специальной компетенцией.* В связи с этим, выделяются специальные государственные органы административного надзора – *государственные комитеты, государственные инспекции и надзоры* (например, Госгортехнадзор). При этом

правомочиями по осуществлению административного надзора наделялись также и государственные учреждения.

В-девятых, имелись отличия в нормативно-правовом регулировании полномочий органов государственного контроля и административного надзора. Так, особенностью нормативно-правового регулирования полномочий органов административного надзора являлось в принятии высшими органами исполнительной власти (Советом Министров СССР или Советами Министров союзных республик СССР) *специальных положений* о порядке осуществления административного надзора. Нормативно-правовое регулирование государственного контроля имело значительное разнообразие, в том числе применялось внутриведомственное правовое регулирование.

Однако несмотря на достаточно четкие критерии разграничения государственного контроля и административного надзора, выработанные советским административным правом, в законодательстве того времени не закреплялось отдельных понятий государственного контроля и административного надзора, а их разграничение происходило исключительно на теоретическом уровне.

2. В начале 90-х после распада СССР и образования нового государства – Российской Федерации, основой для формирования нового законодательства и новых теоретических концепций в различных отраслях права становится Конституция РФ. Формируются принципиально новые подходы, в основе которых лежат принципы демократического правового государства, формируются новые отрасли права, внутри них новые правовые институты и правовые механизмы.

В теории государственного контроля и административного надзора с годами стало прослеживаться несколько ключевых тенденций.

Тенденция № 1: стали появляться новые теоретические разработки государственного контроля и административного надзора, которые преимущественно носят отраслевой характер. Так, теоретические концепции стали формироваться в рамках конституционного права, административного права, финансового права, налогового права, гражданского права, уголовно-исполнительного права. Стали проводиться теоретико-правовые исследования государственного контроля и надзора. В результате в российской юридической науке были сформированы внутриотраслевые самостоятельные правовые концепции понимания государственного контроля и государственного надзора. Единственным общим моментом стало принципиальное разграничение контроля и надзора как различных видов государственной деятельности, но в каж-

дом конкретном случае определяемые внутриотраслевыми подходами к их пониманию.

Тенденция № 2: наиболее разносторонние исследования современного понимания государственного контроля и надзора проводились учеными в области административно-правовой науки. Учеными было предложено несколько кардинально отличающихся друг от друга концептуальных подходов к пониманию сущности и отличительных особенностей данных видов государственно-управленческой деятельности.

Тенденция № 3: на протяжении всего времени законодатель не желает нормативно разграничивать государственный контроль и государственный надзор. В российском законодательстве встречаются разнообразные термины: «государственный контроль», «государственный надзор», «государственный контроль (надзор)», «государственный надзор (контроль)», «государственный контроль и надзор», «контрольно-надзорная деятельность», «надзорно-контрольная деятельность» не имеющие единой трактовки и конкретного содержания. Тем самым российские законодатели не захотели или не смогли поставить окончательной точки в данном вопросе, не закрепив ни в одном нормативном правовом акте понятия государственного контроля и надзора как различных (разноплановых) юридических терминов. При этом попытки такого законодательного разграничения происходили на всех этапах подготовки и принятия «базовых» или «основных» федеральных законов о государственном контроле и надзоре, муниципальном контроле[60].

Тенденция № 4: несмотря на проводимые административные реформы системы государственного контроля и надзора по многим параметрам они остались не завершенными. Одна из первых попыток легального разграничения терминов «контроль» и «надзор» была осуществлена в *Концепции административной реформы в Российской Федерации на 2006-2010 годы, одобренной Распоряжением Правительства от 25 октября 2005 г. № 1789-р*[61].

---

[60] См., подробнее: Мартынов А.В. Попытки законодательного разграничения государственного контроля и административного надзора в условиях современной административной реформы в России // Актуальные вопросы контроля и надзора в социально значимых сферах деятельности общества и государства: материалы V Всероссийской научно-практической конференции (Россия, г. Нижний Новгород, 7-8 июня 2019 г.) / Отв. ред. доктор юридических наук, профессор А.В. Мартынов. Н. Новгород: Изд-во Нижегородского госуниверситета им. Н.И. Лобачевского, 2019. С. 27–59.

[61] СЗ РФ. 2005. № 46. Ст. 4720.

Направление № 5 Концепции, обозначенное как «оптимизация функций органов исполнительной власти и противодействие коррупции» предполагало модернизацию и совершенствование институтов контрольной и надзорной деятельности органов исполнительной власти. В данном разделе Концепции устанавливалось, что важной составляющей деятельности по оптимизации функций органов исполнительной власти является совершенствование действующей системы контроля и надзора, направленное на дальнейшее сокращение административных ограничений предпринимательской деятельности.

В Концепции отмечается, что действующие в настоящее время *методы государственного контроля и надзора* в неполной мере соответствуют задачам обеспечения безопасности продукции, процессов производства, эксплуатации, хранения, перевозки, реализации, утилизации и обременительны для бизнеса. Система требований избыточна, не прозрачна и противоречива – *контрольные полномочия* (исследования, обследования, экспертиза, анализ первичной информации) *соединены с надзорными полномочиями* (проведение проверок, наложение взысканий, выдача разрешений, приостановление деятельности).

Также в Концепции указывается, что для объектов и предметов контроля и надзора, подпадающих под действие федерального закона «О техническом регулировании», необходимость, периодичность, виды и формы проведения контроля должны определяться соответствующими регламентами. До их принятия надзорные органы вправе проводить проверки действующих обязательных требований только в части безопасности, что необходимо закрепить в соответствующих нормативных правовых актах. Все действующие обязательные требования следует опубликовать в информационных системах общего пользования, их получение должно быть бесплатным.

Самое важное, что Концепцией были предусмотрены важнейшие законодательные изменения, направленные на разграничение государственного контроля и государственного (административного) надзора. Так, предусматривалось, что *необходимо разграничить функции по контролю и надзору и унифицировать в этой части терминологию законодательных и других нормативных актов, что позволит надзор сосредоточить в государственных органах, а контроль рассматривать в качестве функции по проведению испытаний, измерений, экспертиз, осуществляемых субъектами рынка, аккредитованными в органах исполнительной власти в установленном порядке. Для этого после принятия соответствующих нормативных правовых актов пред-*

стоит выделить из действующих надзорных органов лаборатории, исследовательские и испытательные центры, сократить численность государственных служащих.[62]

Очень многое из мероприятий, запланированных данной административной реформой, так и не было реализовано.

Тенденция № 5: большое число исключений при установлении правовых основ государственного контроля и административного надзора. Деятельность по осуществлению государственного контроля и надзора имеет крайне неоднородный характер. Исключение из «общего» правового регулирования «базовыми» федеральными законами отдельных видов государственного контроля и государственного надзора, на наш взгляд, с желанием государства повысить эффективность и придать особую значимость определенным видам контрольной и надзорной деятельности.

Так, исходя из отраслевых особенностях правового регулирования государственного контроля и надзора, из сферы регулирования федерального закона от 8 августа 2001 г. № 134-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при проведении государственного контроля (надзора)»[63], федерального закона от 26 декабря 2008 г. № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля»[64]; федерального закона от 31 июля 2020 г. № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации»[65] последовательно и целенаправленно исключались такие виды государственного контроля и надзора как налоговый контроль, валютный контроль, бюджетный контроль, банковский надзор, страховой надзор, таможенный контроль, контроль за обеспечением защиты государственный тайны, контроль безопасности при использовании атомной энергии и др.

Например, *из сферы действия федерального закона от 26 декабря 2008 г. № 294-ФЗ были исключены как минимум 80 видов государственного контроля и надзора*. По оценкам специалистов на начало 2019 года насчитывалось 221 вид государственного контроля и надзора, не считая

---

[62] См.: Концепция административной реформы в Российской Федерации на 2006–2010 годы, одобренная Распоряжением Правительства от 25 октября 2005 г. № 1789-р // СЗ РФ. 2005. № 46. Ст. 4720.

[63] СЗ РФ. 2001. № 33 (часть 1). Ст. 3436.

[64] СЗ РФ. 2008. № 52 (часть 1). Ст. 6249.

[65] СЗ РФ. 2020. № 31 (часть 1). Ст. 5007.

еще более 50 различных видов лицензионного контроля[66]. Из чего следует, *что данный федеральный закон распространяется чуть больше на половину – 141 вид государственного контроля и надзора*, что вызывает обоснованную озабоченность как теоретиков, так и практических работников[67].

Важное значение имеют и теоретические подходы к формированию концептуальных основ современной системы государственного контроля и административного надзора, которые кратко будут нами проанализированы.

Согласно первому научному направлению, назовем его ***«консервативный» подход***, в основу современного понимания государственного контроля и надзора положены теоретические основы государственного контроля и административного надзора, разработанные в советском административном праве.

По сути дела, в современных учебных и научных изданиях приводятся аналогичные признаки государственного контроля и административного надзора, и критерии разграничения данных административно-правовых категорий, что и в советский период времени. Несомненно, что такой консерватизм еще и связан с тем, что большинство известных ученых в области советского административного права являются авторами учебников по российскому административному праву, а соответственно, отказ от сформированных ими научных и теоретических взглядов на определенные институты административного права вряд ли мог претерпеть фундаментальные изменения.

Мы же можем отметить, что сохранение преемственности в трактовке важнейших институтов административного права, сформулированных в Советский период времени ведущими учеными, является скорее положительным моментом в науке современного административного права.

Так, *Ю.М. Козлов* в авторском учебнике по административному праву указывает, что «контроль по своей сути представляет *наблюдение за правомерностью деятельности,* проверку фактического соответствия тех или иных действий требованиям закона, то есть исполнения. Осуществляется он по отношению к подконтрольным органам (должност-

[66] См.: Контрольно-надзорная и разрешительная деятельность в Российской Федерации. Аналитический доклад. 2018 г. / Кол. авт. Плаксин С.М., Абузярова И.А., Кнутов А.В. и др. М.: Национальный исследовательский университет «Высшая школа экономики», 2019. С. 15–16.

[67] Мартынов А.В. Указ соч. С. 27–59.

ным лицам). Для системы исполнительной власти характерно то, что отношения между контролером и контролируемым, как правило, *строятся на началах организационной или ведомственной соподчиненности* (вышестоящий орган контролирует работу нижестоящего и т.п.).

Надзор есть специфическая разновидность контрольной деятельности. Это означает, что имеется в виду также наблюдение за правомерностью деятельности, но таких объектов, которые *не связаны с надзирающим органом отношениями соподчиненности.* Кроме того, *надзор осуществляется за соблюдением специальных правил* (например, противопожарных, санитарных и т.п.).

Однако различия между контролем и надзором в действующих нормах права четко не проводятся»[68].

Вместе с тем, Ю.М. Козлов в обоснование своей позиции о разграничении государственного контроля и административного надзора приводит следующие аргументы: «По результатам контроля возможно применение к должностным лицам подконтрольных исполнительных органов, предприятий и учреждений, виновных в совершении неправомерных действий, *мер дисциплинарной ответственности. Именно она полностью соответствует отношениям организационной соподчиненности*. Очевидно, что контрольные действия не распространяются на граждан, общественные объединения, иные организации негосударственного характера, на объекты государственной собственности и иного ведомственного подчинения. Вместе с тем контроль может привести к отмене правовых актов подведомственных органов (должностных лиц).

Юридические результаты надзора иные. Они могут найти свое выражение в применении к поднадзорным объектам исключительно *мер административного принуждения* (предупредительных, пресекательных и наказательных). И это соответствует предмету административного надзора, каковыми являются действия по исполнению общеобязательных правил, установленных государством. Эти правила имеют специальный характер и соответствующее ему целевое назначение. Например, противопожарные правила. Осуществляя надзор за их соблюдением, полномочные органы контролируют не все стороны деятельности поднадзорного объекта, что свойственно ведомственному контролю, а лишь состояние его противопожарной безопасности»[69].

---

[68] Козлов Ю.М. Административное право: учебник. М.: Юристъ, 2007. С. 537.

[69] Козлов Ю.М. Указ. соч. С. 544.

Д.М. Овсянко отмечает, что административный надзор представляет собой деятельность специально уполномоченных органов исполнительной власти и их должностных лиц, осуществляемую в отношении организационно не подчиненных органов, предприятий, учреждений, организаций, а также граждан по поводу исполнения ими общеобязательных норм, правил, требований, стандартов с целью предупреждения и пресечения правонарушений и привлечения виновных к административной ответственности.

С его точки зрения, в отличие от государственного контроля в системе исполнительной власти, для административного надзора характерны следующие признаки:

1) отсутствие организационной подчиненности субъектов надзора и поднадзорных объектов;

2) возможность оценки деятельности поднадзорных объектов только с точки зрения законности и по достаточно узкому кругу специальных вопросов;

3) невозможность вмешательства в оперативно-хозяйственную деятельность объекта надзора;

4) наличие специального объекта надзорной деятельности – норм, правил, требований, стандартов, содержащихся в нормативных актах, и их исполнение физическими и юридическими лицами;

5) наличие у субъекта надзора юрисдикционных полномочий – возможности самостоятельного рассмотрения определенных дел и применения мер административного принуждения в случаях обнаружения правонарушений или возникновения угроз безопасности различным объектам;

6) основным методом административного надзора является непосредственно постоянное наблюдение за соответствующими объектами, проверка по заявлениям и жалобам, а также по собственной инициативе уполномоченного органа.[70]

Авторы другого классического учебника по административному праву под редакцией *Л.Л. Попова и М.С. Студеникиной*, проводят еще более детальный анализ всех элементов и признаков государственного контроля и административного надзора. По их мнению, «*контроль – это система наблюдения и проверки функционирования объекта в целях устранения отклонений от заданных параметров.* Сущность контроля за деятельностью органов исполнительной власти заключается в

[70] См.: Овсянко Д.М. Административное право: учебное пособие. Изд. 3-е, перераб. и доп. М.: Юристъ, 2002. С. 203–204.

том, что уполномоченные на то государственные органы (законодательной, исполнительной, судебной власти) и общественные организации, используя организационно-правовые способы и средства, выясняют, не допущены ли в деятельности подконтрольных органов исполнительной власти и их должностных лиц какие-либо нарушения законности, то своевременно их устраняют, восстанавливают нарушенные при этом права, привлекают виновных к ответственности, применяют меры по предотвращению нарушений законности и дисциплины»[71].

Контроль, по мнению данной группы ученых, как способ обеспечения законности, *характеризуется следующими признаками:*

1) между контролирующим органом (должностным лицом) и подконтрольным объектом в большинстве случаев существуют отношения подчиненности или подведомственности;

2) объектом контроля является как законность, так и целесообразность деятельность контролируемого, когда контролирующий вправе вмешиваться в текущую административно-хозяйственную деятельность контролируемого;

3) контролирующий часто наделяется правом отменять или приостанавливать решения контролируемого;

4) в соответствующих случаях контролирующий вправе применять меры дисциплинарного воздействия к контролируемому за допущенные нарушения.

Формы контрольной деятельности, как указывают ученые, разнообразны: заслушивание отчетов, информаций и сообщений, проверки, экспертизы, наблюдение за действиями контролируемого (например, по вопросам государственной регистрации, лицензирования, сертификации), изучение деловых и личных качеств кандидатов на замещение должностей, координация деятельности контрольных органов, рассмотрение жалоб и т.д. Особо значимы проверки, которые заключаются в установлении фактических данных и сборе информации о выполнении нормативных правовых актов по проверяемым вопросам.[72]

По мнению указанных авторов, «надзор как способ обеспечения законности в деятельности органов исполнительной власти отличается от контроля. Надзор заключается в постоянном, систематическом наблюдении специальных государственных органов за деятельностью не под-

[71] Административное право: учебник / под ред. Л.Л. Попова, М.С. Студеникиной. М.: Норма, 2008. С. 388–389.

[72] Административное право: учебник / под ред. Л.Л. Попова, М.С. Студеникиной. М.: Норма, 2008. С. 389.

чиненных им органов или лиц с целью выявления нарушений законности. При этом оценка деятельности поднадзорного объекта дается только с точки зрения законности, но не целесообразности. Поэтому при надзоре, в отличие от контроля, вмешательство в текущую административно-хозяйственную деятельность поднадзорного исполнительного органа (должностного лица) не допускается. Различаются два вида надзора: прокурорский и административный[73].

Также *учеными выделяются ряд существенных признаков административного надзора*, отличающих его от государственного контроля:

1) отсутствие организационной подчиненности субъектов надзора и поднадзорных объектов;

2) возможность оценки деятельности поднадзорных объектов только с точки зрения законности и по достаточно узкому кругу специальных вопросов;

3) невозможность вмешательства в оперативно-хозяйственную деятельность объекта надзора;

4) наличие специального объекта надзорной деятельности – норм, правил, требований, стандартов, содержащихся в нормативных актах, и их исполнение физическими и юридическими лицами;

5) возможность самостоятельного применения мер административного принуждения в случаях обнаружения правонарушений или возникновения угрозы безопасности различных объектов;

6) строгое ограничение данных мер принуждения правовыми рамками;

7) наличие юрисдикционных полномочий[74].

Другие ученые *(Б.В. Россинский и Ю.Н. Старилов),* не отклоняясь от консервативной модели государственного контроля и административного надзора, относят их к методам управленческой деятельности.[75] Они также придерживаются научной концепции, рассматривающей *надзор как специфическую разновидность контроля. Контроль, по мнению указанных ученых, необходим государственным органам как канал обратной связи, по которому им поступает информация о поведении объектов управления.* Информация, собираемая в результате контроля, в большинстве случаев не нацелена на выявление нарушений закона, в

---

[73] Административное право: учебник / под ред. Л.Л. Попова, М.С. Студеникиной. М.: Норма, 2008. С. 390.

[74] Там же. С. 410–411.

[75] См.: Административное право: учебник / Б.В. Россинский, Ю.Н. Старилов. 4-е изд., пересмотр. и доп. М.: Норма, 2009. С. 497–548.

частности административных правонарушений. Контроль нужен для обнаружения и пресечения иных нежелательных проявлений в деятельности проверяемых объектов, например, неэффективного использования предоставленных ему полномочий, отклонения от существующих программ и планов работы, совершения дисциплинарных проступков и др. Контроль нередко нужен, чтобы увидеть нарушения не буквы закона, а духа закона[76].

Исходя из данного подхода, учеными также делаются важные выводы о том, что «поскольку информация, получаемая в процессе осуществления надзора, сводится лишь к сведениям о нарушениях законодательства, естественно, что ее спектр уже, чем объем информации, получаемой при контроле. В связи с этим понятно, почему надзор называют суженным контролем.

Надзор в отличие от контроля не является функцией государственного управления. Его информационная природа иная, чем у контроля. Во многом это объясняется тем, что государственные органы, наделенные надзорными полномочиями, в ряде случаев в зависимости от результатов надзора осуществляют юрисдикционную деятельность»[77].

Другой известный ученых *Ю.А. Тихомиров* также придерживается консервативной модели государственного контроля и административного надзора. *Контроль*, с его точки зрения, *есть проверка соблюдения и выполнения нормативно установленных задач, планов и решений, то есть начало цикла, посвященного оценке фактически осуществленного процесса.* Контрольная деятельность, подчеркивается ученым, присуща всем субъектам управления. Каждый из них контролирует выполнение решений, осуществление плановых заданий, соблюдение законности как применительно к своей внутренней системе (в рамках министерства, предприятия и т.п.), так и вовне ее (в пределах большой системы, например, контроль вышестоящих органов за деятельностью нижестоящих, в пределах других «внешних» систем, например, контроль областных органов за работой федерального значения)[78].

Ю.А. Тихомиров рассматривает административный надзор в качестве разновидности государственного контроля. С его точки зрения, *административный надзор можно определить, как специализированное*

---

[76] Административное право: учебник / Б.В. Россинский, Ю.Н. Старилов. 4-е изд., пересмотр. и доп. – М.: Норма, 2009. С. 527.

[77] Там же. С. 528.

[78] См.: Административное право и процесс: полный курс. 2-е изд., доп. и перераб. М.: Изд. Тихомирова М.Ю., 2008. С. 457–458.

наблюдение и проверку соблюдения строго определенных правил в деятельности юридических и физических лиц. Ему присущи следующие свойства: а) осуществление главным образом уполномоченным органом, иногда и органами отраслевой компетенции; б) заранее установленный и фиксированный круг, перечень норм и правил, подлежащих проверке; в) неограниченный круг лиц и организаций, подлежащих проверке в связи с применением вышеназванных правил; г) принятие предупредительных мер воздействия; д) наложение санкций на юридических и физических лиц, виновных в нарушениях правил; е) юрисдикционные процедуры, когда субъекты административного надзора совершают определенные процедурные действия (сбор информации и доказательств, их оценка, фиксирование правонарушений, разбор дел, принятие административных решений, передача дел органам управления и прокуратуры); ж) непрерывное осуществление функций административного надзора ввиду необходимости обеспечить постоянное действие норм и функционирование объектов жизнеобеспечения[79].

Д.Н. Бахрах отмечал *особую роль административного надзора среди методов деятельности государственной администрации.* По его мнению, административный надзор имеет следующие отличительные особенности. Во-первых, лидирующими субъектами надзорной деятельности являются структурные подразделения государственной администрации, субъекты исполнительной власти. Во-вторых, *основная цель административного надзора состоит в обеспечении безопасности граждан, общества, государства.* Надзор за соблюдением правил государственная администрация осуществляет для предупреждения вредных для общества действий, событий, проявлений стихийных сил (эпидемий, пожаров, взрывов и т.д.), уменьшения тяжести их последствий. В-третьих, *административный надзор всегда специализирован*, направлен на соблюдение специальных правил (санитарных, ветеринарных, таможенных, рыбной ловли, торговли и др.), а не на соблюдение законности в целом. В-четвертых, *административный надзор за конкретными объектами производится систематически.* Он носит инициативный характер, проводится главным образом не в связи с поступлением сигналов, жалоб, а по инициативе самих субъектов власти. В-пятых, *административный надзор осуществляется, как правило, субъектами функциональной власти, наделенными надведомственными полномочиями.* Индивидуальные и коллективные субъекты, за которыми производится надзор, организационно не подчинены субъектам власти, которые

[79] Там же. С. 474–475.

их проверяют. В-шестых, *административный надзор связан с широким применением административного принуждения.* Надзорные структуры наделены большими юрисдикционными полномочиями, правом применять меры административного пресечения и административные взыскания. Таким образом, *административный надзор* – надведомственный, специализированный, систематический контроль государственной администрации за соблюдением гражданами и организациями правовых и технико-правовых норм. С одной стороны, он средство административного воздействия, вид исполнительно-распорядительной деятельности, а с другой – часть государственного надзора, средство обеспечения режима законности[80].

Еще одними представителями консервативной модели считаются *А.П. Алехин и А.А. Кармолицкий.* По их мнению, контроль органов исполнительной власти призван обеспечивать законность и дисциплину на порученных им участках работ по руководству хозяйственным, социально-культурным и административно-политическим строительством в системе подведомственных им органов, предприятий, учреждений и организаций. Они выделяют три вида контроля: а) общий; б) ведомственный; в) надведомственный.

С их точки зрения, *общий контроль* предполагает обследование целого комплекса вопросов деятельности подконтрольных объектов. Его осуществление связано с деятельностью органов исполнительной власти общей компетенции: Правительства РФ, правительств республик, высших исполнительных органов государственной власти субъектов РФ. *Ведомственный контроль*, по его мнению, осуществляется федеральными министерствами, не имеющими подведомственных им федеральных служб и федеральных агентств. Он состоит в проверке этими органами в пределах своей компетенции соблюдения и исполнения законов и подзаконных актов, а также своих решений подведомственными им органами, а также предприятиями, учреждениями, организациями. В субъектах РФ ведомственный контроль осуществляется соответствующими министерствами, ведомствами, управлениями и другими органами отраслевой компетенции. *Надведомственный* контроль осуществляется в основном органами межотраслевой компетенции. В отдельных случаях его проводят отраслевые органы, наделенные государственно-властными полномочиями надведомственного характера. Фе-

[80] См.: Бахрах Д.Н. Административное право России: учебник для вузов. М.: Издательство Норма, 2001. С. 395–396.

деральные министерства контролируют деятельность подведомственных им федеральных служб и федеральных агентств.[81]

Относительно административного надзора А.П. Алехиным и А.А. Кармолицким указывается следующее. *Особенности административного надзора состоят в том*, что, во-первых, *между субъектами и объектами надзора отсутствует организационная соподчиненность,* то есть деятельность органов надзора распространяется, как правило, на поднадзорные объекты, независимо от из ведомственной подчиненности и форм собственности. Следовательно, административный надзор по своему характеру является надведомственным. Во-вторых, *субъекты надзора вправе, при соответствующих обстоятельствах, применять к объектам надзора меры административного принуждения.*

Основной задачей, как отмечается учеными, органов административного надзора, вытекающей из характера содержания их деятельности, является обеспечение четкого, единообразного исполнения специальных норм и общеобязательных правил, то есть обеспечение законности в управлении. Решение данной задачи осуществляется путем предупреждения, пресечения правонарушений, привлечения к ответственности виновных лиц. Для выполнения стоящей перед ними задачи и возложенных функций *органы административного надзора наделены полномочиями, имеющими надведомственный характер,* которые позволяют им не только осуществлять надзор, но и воздействовать в пределах своей компетенции на деятельность поднадзорных объектов. Действующие нормативные акты закрепляют несколько групп полномочий органов, осуществляющих административный надзор: 1) полномочия по предупреждению правонарушений; 2) полномочия по пресечению правонарушений; 3) полномочия по привлечению к ответственности виновных лиц; 4) полномочия по нормотворчеству[82].

Приведенная нами позиции известных ученых в области административного права, изложенными в классических современных учебниках по административному праву России, позволяют нам констатировать, что консервативная модель государственного контроля и административного надзора базируется в основном на тех же научных концепциях, сформировавшихся в советский период времени, и по большей части, прошли незначительную трансформацию применительно к новым реалиям современного Российского государства.

---

[81] См.: Алехин А.П., Кармолицкий А.А. Административное право России: учебник. М.: Изд-во «Зерцало», 2007. С. 411–412.

[82] Там же. С. 412–413.

Следующим направлением развития современных представлений о государственном контроле и государственном надзоре может быть признан ***«рациональный» подход***. Данное направление связано с тем, что ни в советском, ни в российском законодательстве, так и не были выработаны и закреплены единые подходы к легальному понимаю контроля и надзора, то есть в законодательстве происходит подмена понятий, их смешение и отсутствует их разграничение. Следовательно, по мнению этих ученых, было бы рациональным следовать тенденциям развития законодательства, а все теоретические разработки по этой причине не имеют практического значения и не имеют дальнейшей перспективы для обсуждения или дискуссии.

Так, по мнению *В.И. Рохлина* «органы контроля и надзора по их сущности – это разноплановые по своему характеру и содержанию, своим целям и задачам и направленности деятельности. Именно поэтому мы полагаем, что органом надзора являются (кроме Президента и Конституционного Суда, в определенной степени Верховного Суда РФ и Высшего Арбитражного Суда РФ) органы прокурорского надзора, а все остальные, именуемые «надзором», более правильно органами контроля, или, может быть, – органами государственного контроля»[83].

С точки зрения *В.Г. Бессарабова*, «органов «чистого» административного надзора не существует, ибо в практической деятельности всегда наблюдается сочетание элементов внешнего контроля и административного надзора и пытаться в любом конкретном случае отграничить, где именно кончается надзор и начинается контроль, весьма трудно»[84].

Аналогичной точки зрения придерживается *Н.В. Субанова*, которой приводятся следующие аргументы в обоснование своей позиции: «сегодня можно с уверенностью говорить о том, что *фактически практика правового регулирования и правоприменения отражает существование смешанных форм контроля и надзора (с приоритетом той или иной формы)*. Поэтому разграничение их в законе будет не только теоретически сложным, но и потребует последующей кардинальной трансформации всей контрольно-надзорной системы, предполагая внесение масштабных изменений в законодательство. Практически же польза от та-

---

[83] См.: Рохлин В.И. Прокурорский надзор и государственный контроль: история, развитие, понятие, соотношение. СПб.: Издательство «Юридический центр Пресс», 2003. С. 189.

[84] См.: Бессарабов В.Г. Прокуратура в системе государственного контроля Российской Федерации: Дис. … д-ра юрид. наук. М., 2001. С. 64–65.

кого рода изменений (насколько это кощунственно ни прозвучит) для субъектов предпринимательства пока выглядит сомнительной.

Признаки сугубо надзорной деятельности, как представляется, сейчас показывает лишь прокурорский надзор, отличие которого от различных форм социального контроля, осуществляемых иными государственными органами, определяется целевым назначением и правовыми средствами выявления и устранения нарушений законов прокурором. Если для органов государственного контроля (надзора) контроль за исполнением законов является лишь одной из форм деятельности по решению многочисленных задач, то для прокуратуры надзор за исполнением законов – основное содержание деятельности»[85].

Следует отметит, что данная позиция высказывается в основном представителями науки прокурорского надзора, которые также занимаются вопросам административного права. Они пытаются отпачковаться от смежного института административного надзора, относящегося к отрасли административного права. Безусловно, это упрощает их дальнейшие научные исследования, связанные с изучением прокурорского надзора, так как его выраженная уникальность позволит сохранить устоявшиеся признаки института прокурорского надзора, сформированные также Советским учеными в этот период времени. Но вряд ли данный подход соответствует современным тенденциям действующего законодательства, которое к числу основных государственных функций органов исполнительной власти относит функции по государственному контролю и функцию по государственному надзору.

Еще одним подходом может считаться **«интегративный» подход** к пониманию государственного контроля и административного надзора. Он был сформулирован представителями Саратовской школы административного права. *В.М. Манохин и А.С. Адушкин* предлагают использовать термин «контрольно-надзорная деятельность», который «соединяет черты государственного контроля и государственного надзора»[86]. По их

[85] См.: Субанова Н.В. К вопросу о концепции Федерального закона об основах государственного контроля и надзора в Российской Федерации // Актуальные вопросы контроля и надзора в социально значимых сферах деятельности общества и государства: материалы I Всероссийской научно-практической конференции (Нижний Новгород, 4–5 июня 2015 г.) / Отв. ред. докт. юрид. наук, доцент А.В. Мартынов. Н. Новгород: Изд-во Нижегородского госуниверситета им. Н.И. Лобачевского, 2015. С. 90.

[86] См.: Манохин В.М., Адушкин Ю.С. Российское административное право: учебник. 2-е изд., испр. и доп. Саратов: Изд-во ГОУ ВПО «Саратовская государственная юридическая академия права», 2003. С. 243.

мнению, «из содержания надзора в контрольно-надзорную деятельность входит такой элемент, как проверка только с точки зрения законности. Из содержания же контроля заимствован третий его признак – принятие различных мер в ходе или по результатам надзора.

В итоге контрольно-надзорная деятельность заключается по своему содержанию в проведении проверки надзорного характера с последующим принятием мер, но не поощрительных и не дисциплинарных, а мер административного принуждения – предупредительно-пресекательного характера и административных наказаний»[87].

Следует отметить, что предложенная В.М. Манохиным и А.С. Адушкиным формула оказалась крайне востребована в современном российском законодательстве, не разграничивающим контрольную и надзорную деятельность. Однако данная интеграция государственного контроля и надзора вряд ли имеет долгосрочную перспективу и со временем, в законодательстве Российской Федерации государственный контроль и государственный надзор получат четкое разграничение, а их соединение будет рассматриваться как модель из прошлого, в котором только происходило формирование новой модели контрольной и надзорной деятельности. По факту уже сейчас мы можем встретить значительное число нормативных правовых актов различной юридической силы, в которых четко определяются, что осуществляется либо государственный контроль, либо государственный надзор. Так, например, из смысла формулировок, закрепленных в основополагающем Указе Президента РФ от 9 марта 2004 г. № 314 «О системе и структуре федеральных органов исполнительной власти», следует, что выделяются как минимум 3 вида федеральных служб: федеральная служба по контролю, федеральная служба по надзору и федеральная служба по контролю и надзору (совмещающая исполнение нескольких функций)[88].

И наконец, следует обозначить и новые или ***«альтернативные» подходы*** к формирования современной системы государственного контроля и надзора.

Не отказываясь от качественных характеристик государственного контроля и административного надзора, сформулированных представи-

---

[87] См.: Манохин В.М., Адушкин Ю.С. Российское административное право: учебник. 2-е изд., испр. и доп. Саратов: Изд-во ГОУ ВПО «Саратовская государственная юридическая академия права», 2003. С. 243.

[88] Пункт 4 Указа Президента РФ от 9 марта 2004 г. № 314 «О системе и структуре федеральных органов исполнительной власти» // СЗ РФ. 2004. № 11. Ст. 945.

телями «консервативного подхода», профессор *С.М. Зырянов* указывает на отличительные особенности этих видов деятельности. По его мнению, «контрольные полномочия спряжены с правом утверждать планы работы, давать поручения, отменять решения, назначать на должности и освобождать от должностей, применять меры поощрения и дисциплинарной ответственности. Надзорные полномочия, в свою очередь, обеспечиваются возможностью применения мер административного принуждения, включая административную ответственность»[89].

С его точки зрения, отличия государственного контроля и государственного надзора состоят и в субъектах, осуществляющих эти виды деятельности: при надзоре – полномочия реализуются должностными лицами, замещающими, как правило, должности государственных инспекторов и обладающих специальным статусом с элементами, свойственными статусу государственного служащего правоохранительной службы; при контроле – контрольные полномочия в обязательном порядке присутствуют в компетенции всех должностных лиц, замещающих должности руководителей либо имеющих в постоянном или временном подчинении других работников. Существует отличие, по мнению ученого, и в правовых основах данных видов деятельности: при надзоре – правовые режимы надзора и административный надзор вводятся федеральными законами. На законодательном уровне определяются также субъекты административного надзора и меры административного принуждения, которые могут ими применяться; при контроле – контрольная функция регламентируется различными нормативными правовыми актами, чаще всего ведомственного характера.[90] Профессором С.М. Зыряновым указываются и другие отличительные особенности государственного контроля и административного надзора, однако главный смысл заключается в том, что административный надзор представляет собой метод управленческой деятельности и носит сугубо правоохранительный характер. Так, он вполне обоснованно отмечает, что «административный надзор – в чистом виде правоохранительная деятельность, нацеленная на обеспечение безопасности в различных обла-

[89] См.: Зырянов С.М. Соотношение контрольной и надзорной функций органов исполнительной власти (глава 1 §3) // В книге: Правовое регулирование государственного контроля: монография / отв. ред. д-р юрид. наук, проф., заслуженный деятель науки РФ А.Ф. Ноздрачев. М.: Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации; Анкил, 2012. С. 67–68.

[90] Там же. С. 68–69.

стях человеческой деятельности посредством поддержания объекта управления в заданном (безопасном) состоянии, своевременного выявления отклонений от нормы, и их пресечения, предотвращения наступления вредных последствий правонарушений»[91].

Профессором *А.М. Тарасовым рассматривается государственный контроль в призме государственного административного контроля и государственного финансового контроля* (две основные его разновидности). Государственный административный контроль, с его точки зрения, осуществляется всеми государственными органами, их подразделениями, а также должностными лицами. Объектом данного контроля является управленческая (административная) деятельность подконтрольных органов, должностных лиц, общественных организаций, коммерческих структур по своевременному и в полном объеме выполнению ими требований соответствующих нормативных правовых актов и принятых управленческих решений государственными органами. Цель административного контроля, пишет ученый, выявить отклонения в управленческой, исполнительной деятельности подконтрольных органов, их должностных лиц, а цель финансового контроля – в их финансовой деятельности. При этом, в чистом виде финансового и административного контроля не существует, в практической контрольной работе они постоянно переплетаются, проникают друг в друга[92].

По мнению А.М. Тарасова, «*контроль в форме (в виде) надзора* ведется специальными государственными органами, в чью компетенцию входит осуществление надзора (надзор – одна из форм деятельности госорганов по обеспечению законности). Надзор как способ обеспечения законности в деятельности органов исполнительной власти отличается от других форм контроля, например, проверки, инспектирования. Надзор заключается в постоянном, систематическом наблюдении специальных государственных органов за деятельностью не подчиненных им органов или лиц с целью выявления нарушений действующих норм права. При этом оценка деятельности поднадзорного объекта определяется с точки зрения законности, а не целесообразности или рациональности. При осуществлении надзора вмешательство в текущую хозяйственную деятельность поднадзорного органа исполнительной власти

[91] См.: Зырянов С.М. Административный надзор. М.: ИД «Юриспруденция», 2010. С. 20–21.

[92] См.: Тарасов А.М. Государственный контроль в России: монография. М.: ЗАО «Издательство «Континент», 2008. С. 28–29.

(должностного лица), как правило не допускается. Различаются два вида надзора: прокурорский и административный»[93].

Важно отметить, что А.М. Тарасов, *использовал именно альтернативный подход при разграничении государственного контроля и административного надзора***,** что может рассматривается в качестве новой идеи, основанной на существующих научных концепциях. В частности, он указывает, что «понятие «контроль» является родовым или общим по отношению к таким его формам реализации (составным частям), как проверка, ревизия, аудит, инспектирование, а также по отношению к такой специальной форме, каковой является надзор. Такое понимание контроля, считаем, позволяет сформировать целостную упорядоченную внутреннюю структуру данного понятия, поэтому оно, на наш взгляд, обоснованно и достаточно логично. Итак, понятие *«контроль» включает в себя, по нашему мнению, следующие основные формы его реализации: проверка, ревизия, инспектирование, надзор и аудит (как специальные формы)»*[94].

Очевидно, что такой подход заслуживает внимания поскольку основан на теории «расщепления» управленческих функций, когда общая функция расщепляется на более мелкие, так называемые подфункции, реализуемые в определенных формах.

Ю.А. Андреева предлагает разграничить понятия «контроль» и «надзор» с точки зрения их субъектного обеспечения, а именно отказаться от сопоставления этих терминов как общего и частного в функциональном аспекте. Можно утверждать, что контрольная функция нуждается в правовой легализации в не меньшей степени, чем надзорная. С учетом этого, она полагает, что контроль следует рассматривать в качестве одного из функциональных направлений деятельности органов исполнительной власти, в то время как надзор – в качестве основной профилирующей субъектно-определенной функции органов, специализированных в области надзора.[95]

С ее точки зрения, под контролем следует понимать «систему действий по наблюдению, проверке процессов, протекающих в коллективах людей, в обществе, в государстве, по выявлению фактического положения дел, сравнению полученных результатов с предварительно определенными целями, установленными нормами, стандартами и так

---

[93] Тарасов А.М. Указ. соч. С. 104.

[94] Там же. С. 104–105.

[95] См.: Андреева Ю.А. К вопросу о соотношении понятий «контроль» и «надзор» // Административное право и процесс. 2009. № 2. С. 6–9.

далее, устранению выявленных недостатков и оценке эффективности управляющего воздействия. Таким образом, контроль способствует защите конкретных ценностей и общественных отношений; обеспечивает их сохранение и прогрессивное изменение, утверждение и развитие достигнутых положительных результатов, преодоление отрицательных отклонений от требуемого поведения и деятельности, соблюдение законности и дисциплины; оказывает положительное влияние на деятельность как объекта контроля, так и субъекта управления. Что же касается надзора, то, на наш взгляд, это есть система установленных законами и иными нормативными правовыми актами действий и мероприятий, осуществляемых специально уполномоченными органами исполнительной власти и их должностными лицами, направленных на обеспечение соблюдения законов и законности государственными органами и учреждениями, органами местного самоуправления, физическими и юридическими лицами»[96].

Профессор *С.М. Зубарев* рассматривает контроль и надзор как специфические формы государственной деятельности, которые обладают едиными функциями: корректирование, социальная превенция (предупреждение), правоохрана. Именно соотношение объема этих функций, по его мнению, является критерием разграничения контроля и надзора в административном процессе.[97] С точки зрения С.М. Зубарева «в отличие от контроля административно-надзорная деятельность в большей степени обладает юрисдикционным, правоохранительным характером. Управленческую функцию здесь реализуют специально уполномоченные органы исполнительной власти и их должностные лица в отношении организационно неподчиненных объектов. Одновременно надзорные полномочия непосредственно связаны с административным принуждением и направлены на обеспечение строгого и точного исполнения государственными органами, органами местного самоуправления, коммерческими и некоммерческими организациями, а также гражданами общеобязательных правил, обеспечивающих жизнедеятельность и безопасность гражданина, общества и государства. Поэтому надзорная деятельность включает комплекс управленческих процедур (например, планирование, организация проверок, наблюдение), а также административно-юрисдикционных производств по предупреждению, выявлению и пресечению правонарушений, восстановлению установленного

[96] См.: Андреева Ю.А. Там же.

[97] См.: Зубарев С.М. Система контроля в сфере государственного управления: монография. М.: Норма: ИНФРА-М, 2019. С. 30.

правопорядка и привлечению виновных к административной ответственности»[98].

Следует особо отметить, что в последние годы стало появляться большое количество научных работ, посвященных различным вопросам государственного контроля и надзора, во многих диссертационных исследованиях также значительное внимание уделяется вопросам понимания и разграничения контроля и надзора, а также детально рассматриваются вопросы различных видов государственного контроля и надзора, осуществляемых в каких-либо сферах государственного управления.

Очевидно, что вышеприведенные научные взгляды на современное понимание государственного контроля и административного надзора способствуют развитию и совершенствованию общей научной концепции контрольной и надзорной деятельности органов публичного управления.

По нашему мнению, необходимо сконцентрировать внимание на следующих важных ***особенностях содержания современного государственного контроля и административного надзора***.

Во-первых, важнейшим нововведением федерального закона от 31 июля 2020 г. № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации»[99] стала норма о том, что порядок организации и осуществления государственного контроля (надзора), муниципального контроля устанавливается соответствующим положением о виде федерального или регионального государственного контроля и надзора (часть 2 ст. 3). Тем самым правовое содержание контрольной или надзорной деятельности должно быть подробно закреплено в соответствующем положении о виде государственного контроля или надзора, в котором в обязательном порядке указываются: 1) контрольные (надзорные) органы, уполномоченные на осуществление вида контроля; 2) критерии отнесения объектов контроля к категориям риска причинения вреда (ущерба) в рамках осуществления вида контроля; 3) перечень профилактических мероприятий в рамках осуществления вида контроля; 4) виды контрольных (надзорных) мероприятий, проведение которых возможно в рамках осуществления вида контроля, и перечень допустимых контрольных (надзорных) действий в составе каждого контрольного (надзорного) мероприятия; 5) виды и периодичность проведения плановых контрольных (надзор-

[98] См.: Зубарев С.М. Там же. С. 32–33.

[99] СЗ РФ. 2020. № 31 (часть 1). Ст. 5007.

ных) мероприятий для каждой категории риска, за исключением категории низкого риска; 6) особенности оценки соблюдения лицензионных требований контролируемыми лицами, имеющими лицензию; 7) иные вопросы, регулирование которых в соответствии с настоящим федеральным законом, а в случаях, установленных настоящим федеральным законом, в соответствии с федеральными законами о видах контроля осуществляется положением о виде контроля (часть 5 ст. 3).

Еще до вступления в силу федерального закона от 31 июля 2020 г. № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» (1 июля 2021 г.), так и после этой даты, Правительством Российской Федерации принимаются десятки положений о различных видах государственного контроля (надзора)[100].

Изучение принятых положений о видах государственного контроля (надзора) показывает о трёх видах нормативных правовых актов, принятых Правительством РФ:

1) положение о федеральном государственном контроле (надзоре);

2) положение о федеральном государственном надзоре;

3) положение о федеральном государственном контроле.

Очевидно, что если бы «соединительное» понятие «государственный контроль (надзор)» или контрольно-надзорная деятельность, используемые как базовые в федеральном законе от 31 июля 2020 г. № 248-ФЗ, имело бы значение, то не имело бы смысла принимать положения с различными наименованиями, которыми разделяются государственный контроль и государственный надзор.

При этом необходимо непосредственным образом обратиться к ***положениям о государственном надзоре***. Такими положениями являются: Положение о федеральном государственном энергетическом надзоре[101], Положение о федеральном государственном горном надзоре[102], Положение о федеральном государственном надзоре в области защиты

[100] На 1 декабря 2021 года было принято более 70 положений о видах государственного контроля и надзора.

[101] Постановление Правительства РФ от 30 июня 2021 г. № 1085 «О федеральном государственном энергетическом надзоре» // СЗ РФ. 2021. № 28 (часть 1). Ст. 5515.

[102] Постановление Правительства РФ от 30 июня 2021 г. № 1074 «О федеральном государственном горном надзоре» // СЗ РФ. 2021. № 27 (часть 3). Ст. 5450.

населения и территорий от чрезвычайных ситуаций[103], Положение о федеральном государственном надзоре в области промышленной безопасности[104], Положение о федеральном государственном надзоре в области гражданской обороны[105], Положение о федеральном государственном пробирном надзоре[106] и др.

Все положения о видах государственного надзора имеют несколько общих норм, которыми устанавливаются предмет и объект государственного надзора, а именно для всех видов государственного надзора ***общим критерием*** является следующее:

1) ***предметом*** федерального государственного надзора является соблюдение ***организациями (юридическими лицами), индивидуальными предпринимателями и гражданами*** установленных федеральными законами и другими нормативными правовыми актами обязательных требований, которые подлежат проверке органами исполнительной власти;

2) ***объектом*** федерального государственного надзора являются деятельность, действия (бездействия) ***организаций (юридических лиц), индивидуальных предпринимателей и граждан***.

Таким образом, нормативно устанавливается, что государственный надзор может осуществляться в отношении организационно неподчиненных субъектов (организаций, индивидуальных предпринимателей, граждан). ***При этом ключевым моментом является конечно же возможность осуществления государственного надзора в отношении организационно неподчиненных организаций и граждан.***

Кроме этого, в положениях, обозначенных о видах государственного контроля (надзора), также фактически регламентируется надзорная деятельность. Так, в Положении о федеральном государственном геологи-

---

[103] Постановление Правительства РФ от 25 июня 2021 г. № 1013 «О федеральном государственном надзоре в области защиты населения и территорий от чрезвычайных ситуаций» // СЗ РФ. 2021. № 27 (часть 2). Ст. 5400.

[104] Постановление Правительства РФ от 30 июня 2021 г. № 1082 «О федеральном государственном надзоре в области промышленной безопасности» // СЗ РФ. 2021. № 28 (часть 1). Ст. 5512.

[105] Постановление Правительства РФ от 25 июня 2021 г. № 1007 «О федеральном государственном надзоре в области гражданской обороны» // СЗ РФ. 2021. № 27 (часть 2). Ст. 5394.

[106] Постановление Правительства РФ от 25 июня 2021 г. № 1015 «О федеральном государственном пробирном надзоре» // СЗ РФ. 2021. № 27 (часть 3). Ст. 5402.

ческом контроле (надзоре)[107] речь идет о предмете, направленности и объектах именно геологического надзора за соблюдением гражданами и организациями обязательных требований. Аналогичным образом делается акцент именно на государственном надзоре в Положении о федеральном государственном контроле (надзоре) в сфере рекламы[108], Положении о федеральном государственном контроле (надзоре) за безопасностью людей на водных объектах[109] и др.

Вместе с тем, некоторые принятые положения о видах государственного контроля (надзора) не разграничивают контрольную и надзорную деятельность, используя единую формулу «государственный контроль (надзор)»: Положение о федеральном государственном контроле (надзоре) в области защиты прав потребителей[110], Положение о федеральном государственном (надзоре) за соблюдением трудового законодательства и иных нормативных правовых актов, содержащих нормы трудового права[111], Положение о федеральном государственном контроле (надзоре) за состоянием, содержанием, сохранением, использованием, популяризацией и государственной охраной объектов культурного наследия[112], Положение о федеральном государственном контроле (надзоре) в области безопасности дорожного движения[113], и др.

---

[107] Постановление Правительства РФ от 30 июня 2021 г. № 1095 «Об утверждении Положения о федеральном государственном геологическом контроле (надзоре)» // СЗ РФ. 2021. № 28 (часть 1). Ст. 5525.

[108] Постановление Правительства РФ от 30 июня 2021 г. № 1073 «О федеральном государственном контроле (надзоре) в сфере рекламы» // СЗ РФ. 2021. № 27 (часть 3). Ст. 5449.

[109] Постановление Правительства РФ от 25 июня 2021 г. № 1014 «Об утверждении Положения о федеральном государственном контроле (надзоре) за безопасностью людей на водных объектах» // СЗ РФ. 2021. № 27 (часть 2). Ст. 5401.

[110] Постановление Правительства РФ от 25 июня 2021 г. № 1005 «Об утверждении Положения о федеральном государственном контроле (надзоре) в области защиты прав потребителей» // СЗ РФ. 2021. № 27 (часть 2). Ст. 5392.

[111] Постановление Правительства РФ от 21 июля 2021 г. № 1230 «Об утверждении Положения о федеральном государственном контроле (надзоре) за соблюдением трудового законодательства и иных нормативных правовых актов, содержащих нормы трудового права» // СЗ РФ. 2021. № 30. Ст. 5804.

[112] Постановление Правительства РФ от 30 июня 2021 г. № 1093 «О федеральном государственном контроле (надзоре) за состоянием, содержанием, сохранением, использованием, популяризацией и государственной охраной объектов культурного наследия» // СЗ РФ. 2021. № 28 (часть1). Ст. 5523.

[113] Постановление Правительства РФ от 30 июня 2021 г. № 1101 «Об утверждении Положения о федеральном государственном контроле (надзоре) в обла-

При этом фактически регламентируется данными положениями именно ***надзорная деятельность*** (непосредственно указывается только государственный надзор).

В некоторых случаях, фактически надзорная деятельность обозначается в качестве государственного контроля: Положение о федеральном государственном карантинном фитосанитарном контроле (надзоре)[114], Положение о федеральном государственном контроле (надзоре) в области семеноводства в отношении семян сельскохозяйственных растений[115], Положение о федеральном государственном экологическом контроле (надзоре)[116], и др.

По нашему мнению, в случае осуществления контрольно-надзорных мероприятий в отношении организационно неподчиненных организаций и граждан по соблюдению ими обязательных требований (за исключением лицензионного контроля), то в этом случае осуществляется именно государственный надзор, вне зависимости от того, как он именуется в соответствующем положении о виде государственного контроля (надзора), и других подзаконных нормативных правовых актах.

Во-вторых, другой важной особенностью современной системы государственного контроля и надзора является применением риск-ориентированного подхода при организации и осуществлении этих видов деятельности.

Понятие «риск-ориентированного подхода» впервые было раскрыто в ст. 8.1 федерального закона от 26 декабря 2008 г. № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального

сти безопасности дорожного движения и признании утратившими силу некоторых актов Правительства Российской Федерации и отдельных положений некоторых актов Правительства Российской Федерации» // СЗ РФ. 2021. № 28 (часть 2). Ст. 5531.

[114] Постановление Правительства РФ от 25 июня 2021 г. № 995 «Об утверждении Положения о федеральном государственном карантинном фитосанитарном контроле (надзоре)» // СЗ РФ. 2021. № 27 (часть 2). Ст. 5383.

[115] Постановление Правительства РФ от 25 июня 2021 г. № 994 «Об утверждении Положения о федеральном государственном контроле (надзоре) в области семеноводства в отношении семян сельскохозяйственных растений» // СЗ РФ. 2021. № 27 (часть 2). Ст. 5382.

[116] Постановление Правительства РФ от 30 июня 2021 г. № 1096 «О федеральном государственном экологическом контроле (надзоре)» // СЗ РФ. 2021. № 28 (часть 1). Ст. 5526.

контроля»[117]. В части второй статьи 8.1 указанного закона определялось, что ***риск-ориентированный подход*** представляет собой метод организации и осуществления государственного контроля (надзора), при котором в предусмотренных настоящим федеральным законом случаях выбор интенсивности (формы, продолжительности, периодичности) проведения мероприятий по контролю, мероприятий по профилактике нарушения обязательных требований определяется отнесением деятельности юридического лица, индивидуального предпринимателя и (или) используемых ими при осуществлении такой деятельности производственных объектов к определенной категории риска либо определенному классу (категории) опасности.

Постановлением Правительства РФ от 17 августа 2016 г. № 806 был определен перечень видов федерального государственного контроля (надзора), в отношении которых применяется риск-ориентированный подход, и перечень видов регионального государственного контроля (надзора), при организации которых риск-ориентированный подход применяется в обязательном порядке[118].

Новый федеральный закон от 31 июля 2020 г. № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» также отдает приоритет при осуществлении государственного контроля и надзора риск-ориентированному подходу. В этом закон включена отдельная Глава 5 «Управление рисками причинения вреда (ущерба) охраняемым законом ценностям при осуществлении государственного контроля (надзора), муниципального контроля». В части 1 ст. 22 указанного федерального закона устанавливается, что государственный контроль (надзор), муниципальный контроль осуществляются на основе управления рисками причинения вреда (ущерба), определяющего выбор профилактических мероприятий и контрольных (надзорных) мероприятий, их содержание (в том числе объем проверяемых обязательных требований), интенсивность и результаты.

Также рассматриваемым федеральным законом определяется, что под риском причинения вреда (ущерба) понимается вероятность наступления событий, следствием которых может стать причинение вреда (ущерба) различного масштаба и тяжести охраняемым законом

---

[117] СЗ РФ. 2008. № 52 (часть 1). Ст. 6249.

[118] Постановление Правительства РФ от 17 августа 2016 г. № 806 «О применении риск-ориентированного подхода при организации отдельных видов государственного контроля (надзора) и внесении изменений в некоторые акты Правительства Российской Федерации» // СЗ РФ. 2016. № 35. Ст. 5326.

ценностям (часть 2 ст. 22). Под оценкой риска причинения вреда (ущерба) понимается деятельность контрольного (надзорного) органа по определению вероятности возникновения риска и масштаба вреда (ущерба) для охраняемых законом ценностей (часть 3 ст. 22). Под управлением риском причинения вреда (ущерба) понимается осуществление на основе оценки рисков причинения вреда (ущерба) профилактических мероприятий и контрольных (надзорных) мероприятий в целях обеспечения допустимого уровня риска причинения вреда (ущерба) в соответствующей сфере деятельности. Допустимый уровень риска причинения вреда (ущерба) в рамках вида государственного контроля (надзора) должен закрепляться в ключевых показателях вида контроля (часть 4 ст. 22).

Важно отметить, что положением о виде муниципального контроля может быть установлено, что система оценки и управления рисками при осуществлении соответствующего вида муниципального контроля не применяется, если иное не установлено федеральным законом о виде контроля, общими требованиями к организации и осуществлению данного вида муниципального контроля, утвержденными Правительством Российской Федерации. В этом случае плановые контрольные (надзорные) мероприятия и внеплановые контрольные (надзорные) мероприятия проводятся с учетом особенностей, установленных статьями 61 и 66 федерального закона от 31 июля 2020 г. № 248-ФЗ. Федеральным законом о виде контроля могут быть установлены особенности применения системы оценки и управления рисками при проведении плановых контрольных (надзорных) мероприятий, а также дополнительные формы независимой оценки соблюдения обязательных требований. В этом случае плановые контрольные (надзорные) мероприятия проводятся с учетом особенностей, установленных федеральным законом о виде контроля (ч.ч. 7,8 ст. 22).

Таким образом, риск-ориентированный подход может быть использован как при осуществлении государственного контроля, так и государственного надзора. Важное отличие заключается в том, что исходя из целей, которые преследует данный метод (прекращение избыточного влияния контрольных и надзорных органов на бизнес[119]), он наиболее предпочтителен для осуществления именно государственного надзора в отношении организаций и граждан, нежели при государственный кон-

[119] См.: Мартынов А.В. Применение риск-ориентированного подхода при осуществлении государственного контроля и надзора как необходимое условие снижение давления на бизнес // Юрист. 2016. № 18. С. 22–27.

троле, которые осуществляется в отношении организационно подчиненных лиц, например, подведомственных организаций. Тем самым в положениях о видах государственного надзора риск-ориентированный подход закрепляется в качестве обязательного метода управленческой деятельности.

В-третьих, содержание государственного контроля и надзора постоянно расширяется. Если первоначально государственный контроль и надзор рассматривались как деятельность по проведению проверки выполнения юридическим лицом или индивидуальным предпринимателем при осуществлении их деятельности обязательных требований к товарам (работам, услугам)[120], то в дальнейшем в содержание этой деятельности было дополнительно включено проведение мероприятий по профилактике нарушений обязательных требований, мероприятий по контролю, осуществляемых без взаимодействия с юридическими лицами, принятие предусмотренных законодательство Российской Федерации мер по пресечению и устранению последствий выявленных нарушений, а также деятельность по систематическому наблюдению за исполнением обязательных требований, анализу и прогнозированию состояния исполнения обязательных требований при осуществлении деятельности юридическими лицами и индивидуальными предпринимателями[121].

В настоящее время, федеральный закон от 31 июля 2020 г. № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации»[122] включает в содержание государственного контроля и надзора следующие виды деятельности:

1) профилактика нарушений обязательных требований;

2) оценка соблюдения гражданами и организациями обязательных требований;

3) выявление нарушений обязательных требований;

4) принятие предусмотренных законодательством Российской Федерации мер по пресечению выявленных нарушений обязательных требо-

---

[120] Статья 2 Федерального закона от 8 августа 2001 г. № 134-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при проведении государственного контроля (надзора)» // СЗ РФ. 2001. № 33 (часть 1). Ст. 3436.

[121] Статья 2 Федерального закона от 26 декабря 2008 г. № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» // СЗ РФ. 2008. № 52 (часть 10). Ст. 6249.

[122] СЗ РФ. 2020. № 31 (часть 1). Ст. 5007.

ваний, устранению их последствий и (или) восстановлению правового положения, существовавшего до возникновения таких нарушений[123].

Анализ принятых положений о различных видах государственного надзора показывает, что к надзорной деятельности относится:

а) профилактика нарушений обязательных требований;

б) организация и проведение контрольных (надзорных) мероприятий;

в) принятие предусмотренных законодательством Российской Федерации мер по пресечению, предупреждению и (или) устранению последствий выявленных нарушений обязательных требований[124].

Следовательно, содержание деятельности по осуществлению государственного надзора строго регламентируется федеральными законами, когда как при приведении мероприятий государственного контроля могут осуществляться и иные виды деятельности, предусмотренные ведомственными нормативными актами, включаемые в содержание государственного контроля. Например, Приказом Министерства науки и высшего образования от 7 октября 2020 г. № 1277 утверждены Правила осуществления контроля за выполнением государственного задания на оказание государственных услуг (выполнения работ) федеральными государственными учреждениями, находящимися в ведении Министерства науки и высшего образования РФ[125], согласно которым контроль за выполнением учреждением государственного задания осуществляется на основании документов (отчетов, аналитических отчетов), и актов, составленных по результатам плановой и внеплановой проверок, которые могут быть выездными или документарными.

Еще одним примером может Приказ Министерства науки и высшего образования РФ от 14 июля 2021 г. № 621 «Об организации и проведении проверок деятельности организаций, подведомственных Министер-

---

[123] Часть 1 статьи 1 Федеральный закон от 31 июля 2020 г. № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» // СЗ РФ. 2020. № 31 (часть 1). Ст. 5007.

[124] См., например: Постановление Правительства РФ от 30 июня 2021 г. № 1074 «О федеральном государственном горном надзоре» // СЗ РФ. 2021. № 27 (часть 3). Ст. 5450; Постановление Правительства РФ от 30 июня 2021 г. № 1085 «О федеральном государственном энергетическом надзоре» // СЗ РФ. 2021. № 28 (часть 1). Ст. 5515; Постановление Правительства РФ от 30 июня 2021 г. № 1082 «О федеральном государственном надзоре в области промышленной безопасности» // СЗ РФ. 2021. № 28 (часть 1). Ст. 5512; и др.

[125] Официальный интернет-портал правовой информации [Электронный ресурс] // URL: http://pravo.gov.ru (дата обращения: 19.12.2021).

ству науки и высшего образования Российской Федерации»[126], которым утвержден Регламент организации и проведения проверок деятельности организаций, подведомственных Министерству науки и высшего образования РФ. Согласно данному документу, под проверкой понимается совершение контрольных действий по документальному и фактическому изучению законности и эффективности осуществления финансовых и хозяйственных операций, иной деятельности объекта проверки, достоверности бюджетного (бухгалтерского) учета и бюджетной (бухгалтерской) отчетности в отношении деятельности объекта проверки за определенный период (пункт 4 Регламента).

Таким образом, в настоящее время существуют различия в правовом регулировании государственного контроля и административного надзора, и они связаны с либо со строгой фиксацией в законодательстве РФ всех форм и методов деятельности (при государственном надзоре), либо с разнообразием таких форм и методов, которые могут устанавливаться не только законами, но и ведомственными (подзаконными) нормативными правовыми актами, то есть не ограничены только на уровне федеральных законов.

В-четвертых, важным аспектом государственного контроля и административного надзора становится деятельность по установлению обязательных требований.

В соответствии с ч. 1 ст. 2 федерального закона от 31 июля 2020 г. № 247-ФЗ «Об обязательных требованиях в Российской Федерации»[127] *обязательные требования* устанавливаются федеральными законами, Договором о Евразийском экономическом союзе от 29 мая 2014 года, актами, составляющими право Евразийского экономического союза, положениями международных договоров Российской Федерации, не требующими издания внутригосударственных актов для их применения и действующими в Российской Федерации, нормативными правовыми актами субъектов Российской Федерации, муниципальными нормативными правовыми актами.

В случаях и пределах, которые установлены федеральными законами, обязательные требования могут быть установлены указами Президента Российской Федерации, а в случаях и пределах, которые установлены федеральными законами, указами Президента Российской Федерации, обязательные требования могут быть установлены нормативными правовыми актами Правительства Российской Федерации, феде-

[126] Документ опубликован не был. Доступ из СПС «КонсультантПлюс».
[127] СЗ РФ. 2020. № 31 (часть 1). Ст. 5007.

ральных органов исполнительной власти (ч.ч. 2 и 3 ст. 2 федерального закона от 31 июля 2020 г. № 247-ФЗ).

Согласно ч. 1 ст. 10 федерального закона от 31 июля 2020 г. № 247-ФЗ, при установлении обязательных требований нормативными правовыми актами Правительства Российской Федерации, федерального органа исполнительной власти или уполномоченной организации должны быть соблюдены принципы, установленные настоящим федеральным законом, и определены:

1) содержание обязательных требований (условия, ограничения, запреты, обязанности);

2) лица, обязанные соблюдать обязательные требования;

3) в зависимости от объекта установления обязательных требований:

а) осуществляемая деятельность, совершаемые действия, в отношении которых устанавливаются обязательные требования;

б) лица и используемые объекты, к которым предъявляются обязательные требования при осуществлении деятельности, совершении действий;

в) результаты осуществления деятельности, совершения действий, в отношении которых устанавливаются обязательные требования;

4) формы оценки соблюдения обязательных требований (государственный контроль (надзор), привлечение к административной ответственности, предоставление лицензий и иных разрешений, аккредитация, оценка соответствия продукции и иные формы оценки и экспертизы);

5) федеральные органы исполнительной власти и уполномоченные организации, осуществляющие оценку соблюдения обязательных требований.

Так, например, Ростехнадзором устанавливаются десятки федеральных норм и правил в области промышленной безопасности и в области использования атомной энергии (обязательные требования). Другие федеральные службы также участвуют в разработке и установлении обязательных требований (Роскомнадзор, Росприроднадзор, Роспотребнадзор и др.).

Принципиальное значение имеет, что устанавливаемые федеральными органами исполнительной власти, осуществляющими государственные функции по контролю и надзору, обязательные требования, подлежащие проверки при осуществлении государственного контроля и надзора, распространяются на неподчиненных граждан и организации (юридические лица). При государственном контроле установленные обязательные требования распространяются только на подведомственные организации и подчиненных должностных лиц.

В-пятых, существует тесная взаимосвязь деятельности по осуществлению государственного контроля и надзора, и производством по делам об административных правонарушениях (административно-юрисдикционной деятельностью по привлечению к административной ответственности).

В положениях КоАП РФ имеются прямые отсылки к контрольно-надзорной деятельности, результаты которой стали основанием для привлечения к административной ответственности: часть 1 ст. 4.1.1, пункт 7 части 1 ст. 4.2, часть 6.1 ст. 4.5, пункт 5.1 части 1 ст. 24.5, часть 3 ст. 26.2 КоАП РФ.

В-шестых, при осуществлении государственного контроля и административного надзора могут устанавливаться специальные административно-правовые режимы.

Федеральным законом от 18 июля 2011 г. № 242-ФЗ в федеральный закон от 26 декабря 2008 г. № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» была включена статья 13.1 «Режим постоянного государственного контроля (надзора)». В соответствии с данной статьей в отношении юридических лиц, индивидуальных предпринимателей, *эксплуатирующих объекты повышенной опасности* и осуществляющих на этих объектах технологические процессы, представляющие опасность причинения вреда жизни или здоровью людей, окружающей среде, безопасности государства, имуществу физических или юридических лиц, государственному или муниципальному имуществу, возникновения чрезвычайных ситуаций природного и техногенного характера, устанавливается режим постоянного государственного контроля (надзора), предусматривающий *возможность постоянного пребывания уполномоченных должностных лиц органов государственного контроля (надзора) на объектах повышенной опасности и проведение указанными лицами мероприятий по контролю за состоянием безопасности и выполнением мероприятий по обеспечению безопасности на таких объектах*. Режим постоянного государственного надзора устанавливается также в отношении специализированных организаций, которые включены в перечень, утвержденный Правительством РФ.

При этом к объектам повышенной опасности были отнесены: 1) опасные производственные объекты I класса опасности; 2) гидротехнические сооружения I класса (в соответствии с перечнем классов, установленных Правительство РФ); 3) отдельные объекты использования атомной энергии (часть 1.1 ст. 13.1).

Порядок осуществления постоянного государственного контроля (надзора) устанавливается Правительством РФ[128].

В федеральный закон от 31 июля 2020 г. № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» включена отдельная глава 18, посвященная специальным режимам государственного контроля (надзора). К числу таких специальных режимов отнесены: мониторинг (ст. 96), постоянный государственный контроль (надзор) (ст. 97), постоянный рейд (ст. 97.1).

Важным положением является указание на то, что постоянный государственный контроль (надзор) может вводиться при осуществлении федерального государственного надзора в области промышленной безопасности, федерального государственного надзора в области безопасности гидротехнических сооружений, федерального государственного пробирного надзора (часть 2 ст. 97).

Исходя из положений федерального закона от 31 июля 2020 г. № 248-ФЗ *специальный режим постоянного государственного контроля (надзора) может осуществляться только при осуществлении административного надзора, когда как мониторинг и постоянный рейд могут применяться как при государственном контроле, так и при административном надзоре*.

В-седьмых, оценка контрольно-надзорной деятельности осуществляется на основе критериев оценки результативности и эффективности государственного контроля и надзора. Так, под результативностью государственного контроля (надзора) и муниципального контроля понимается степень достижения общественно значимых результатов государственного контроля (надзора) и муниципального контроля, выражающихся в минимизации причинения вреда (ущерба) охраняемым законом ценностям в соответствующей сфере деятельности.[129]

Эффективность государственного контроля (надзора) и муниципального контроля представляет собой степень устранения риска причинения вреда (ущерба) охраняемым законом ценностям с учетом ис-

---

[128] См., например: Положение о режиме постоянного государственного надзора на объектах использования атомной энергии, утвержденное постановлением Правительства РФ от 23 апреля 2012 г. № 373 // СЗ РФ. 2012. № 18. Ст. 2233.

[129] Основные направления разработки и внедрения системы оценки результативности и эффективности контрольно-надзорной деятельности, утверждены распоряжением Правительства РФ от 17 мая 2016 г. № 934-р // СЗ РФ. 2016. № 21. Ст. 3075.

пользуемого объема трудовых, материальных и финансовых ресурсов, а также уровня вмешательства в деятельность граждан и организаций[130].

Именно последний критерий «уровень вмешательства в деятельность граждан и организаций» является характерным для оценки надзорной деятельности, а не государственного контроля.

В соответствии со ст. 30 федерального закона от 31 июля 2020 г. № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» оценка результативности и эффективности деятельности контрольных (надзорных) органов осуществляется по каждому виду контроля на основе системы показателей результативности и эффективности государственного контроля (надзора), муниципального контроля.

В систему показателей результативности и эффективности деятельности контрольных (надзорных) органов входят:

1) ключевые показатели видов контроля, отражающие уровень минимизации вреда (ущерба) охраняемым законом ценностям, уровень устранения риска причинения вреда (ущерба) в соответствующей сфере деятельности, по которым устанавливаются целевые (плановые) значения и достижение которых должен обеспечить соответствующий контрольный (надзорный) орган;

2) индикативные показатели видов контроля, применяемые для мониторинга контрольной (надзорной) деятельности, ее анализа, выявления проблем, возникающих при ее осуществлении, и определения причин их возникновения, характеризующих соотношение между степенью устранения риска причинения вреда (ущерба) и объемом трудовых, материальных и финансовых ресурсов, а также уровень вмешательства в деятельность контролируемых лиц.

Ключевые показатели вида контроля и их целевые значения для видов федерального государственного контроля (надзора) утверждаются положением о виде контроля, индикативные показатели для видов федерального государственного контроля (надзора) утверждаются федеральными органами исполнительной власти, осуществляющими нормативно-правовое регулирование в соответствующей сфере деятельности.

В настоящее время утверждены перечни индикативных показателей федерального государственного контроля (надзора) по видам федераль-

[130] Основные направления разработки и внедрения системы оценки результативности и эффективности контрольно-надзорной деятельности, утверждены распоряжением Правительства РФ от 17 мая 2016 г. № 934-р // СЗ РФ. 2016. № 21. Ст. 3075.

ного государственного контроля (надзора), отнесенным к компетенции Министерства культуры РФ[131]; индикативные показатели для федерального государственного надзора в области защиты населения и территорий от чрезвычайных ситуаций[132]; индикативные показатели для федерального государственного надзора в области гражданской обороны[133] и др.

Таким образом, нами были проанализированы наиболее существенные характеристики современного государственного контроля и административного надзора, которые в том числе позволяют в некоторых случаях разграничивать эти виду государственно-управленческой деятельности. Однако вышеперечисленные изменения не является единственными, а наибольшее влияние на трансформацию систему государственного контроля и административного надзора повлияли современные информационные (цифровые) технологии (речь о которых пойдет дальше).

3. Учитывая вышеприведенные новые качества государственного контроля и надзора, которые характеризуют данные виды деятельности в современных условиях, необходимо отдельно остановиться еще на одном качественном изменении, серьезным образом трансформирующим контрольно-надзорную деятельность. Это качественное изменение связано с внедрением в контрольно-надзорную деятельность современных (передовых) информационных (цифровых) технологий.

Еще более 10 лет назад мы отмечали, что государственный контроль и надзор – это крайне динамические правовые явления, которые могут трансформироваться в зависимости от сложившихся условий в совре-

---

[131] Приказ Минкультуры России от 1 декабря 2021 г. № 1998 «Об утверждении перечней индикативных показателей федерального государственного контроля (надзора) по видам федерального государственного контроля (надзора), отнесенным к компетенции Министерства культуры Российской Федерации» // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

[132] Приказ МЧС России от 16 сентября 2021 г. № 613 «Об утверждении индикативных показателей для федерального государственного надзора в области защиты населения и территорий от чрезвычайных ситуаций» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://pravo.gov.ru (дата обращения: 22.10.2021).

[133] Приказ МЧС России от 16 сентября 2021 г. № 614 «Об утверждении индикативных показателей для федерального государственного надзора в области гражданской обороны» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://pravo.gov.ru (дата обращения: 22.10.2021).

менном правовом государстве[134]. Поэтому воздействие на контрольно-надзорную деятельность внешних и внутренних факторов должно изменять качественные и содержательные характеристики государственного контроля и административного надзора.

Экспертами указывается, что «информационные технологии становятся неотъемлемым элементом практически всех сфер государственного управления. Это неизбежно по двум причинам. Во-первых, цифровые инструменты позволяют многократно повысить объем собираемой информации, ее достоверность и оперативность, что облегчает и ускоряет принятие качественных и взвешенных управленческих решений. Во-вторых, все большая часть общественной жизни перемещается в виртуальную сферу: там предприятия накапливают, хранят и обрабатывают информацию, там они находят своих клиентов и контрагентов, заключают сделки и т.д. Сфера контрольно-надзорной деятельности не является исключением из общей тенденции»[135].

Следует также отметить о существенной роли информационной составляющей контрольно-надзорной деятельности. Так, например, профессор Б.В. Россинский отмечает, что «у контроля и надзора разная информационная природа. При их реализации используются разные каналы обратной связи. При контроле – достаточно простые каналы, такие как прямая или непрямая связь. В процессе осуществления надзорных полномочий используется куда более сложные информационные каналы обратной связи, например, обратной параллельной соединительной связи или обратной параллельной распределительной связи. Это объясняется тем, что в процессе осуществления административного надзора субъекту надзорной деятельности нередко приходится анализировать и обобщать информацию, поступающую по каналам обратной связи не только от поднадзорных объектов, но и от потребителей их услуг, различных организаций, проводящих необходимые экспертные оценки и исследования, иных независимых от субъектов надзорной деятельности структур»[136].

---

[134] См.: Мартынов А.В. Административный надзор в России: теоретические основы построения: монография / под ред. Ю.Н. Старилова. М.: ЮНИТИ-ДАНА: Закон и право, 2010. С. 17.

[135] Контрольно-надзорная и разрешительная деятельность в Российской Федерации. Аналитический доклад – 2020–2021 / С.М. Плаксин (рук. авт. кол.), И.А. Абузярова и др.; Российский союз промышленников и предпринимателей; Нац. исслед. ун-т «Высшая школа экономики». М.: НИУ ВШЭ, 2021. С. 113.

[136] Россинский Б.В. Информационные подходы к разграничению контроля и надзора в деятельности государственных органов // Актуальные вопросы кон-

Содержательная основа контрольно-надзорной деятельности, имеющая глубокую информационную основу, предполагает и способствует внедрению различных цифровых технологий в эту сферу. Широкая информатизация контрольно-надзорной деятельности является благоприятным фактором для повышения ее эффективности и результативности, она будет способствовать более правильному и своевременному исполнению поставленных государством целей и задач перед контрольно-надзорными органами исполнительной власти.

Различными учеными обращается внимание на значимость использования современных цифровых технологий в контрольно-надзорной деятельности. Некоторыми из них указывается на то, что «повышение эффективности информационного обеспечения государственного контроля и надзора должно обеспечиваться путем создания единых федеральных баз данных об организациях, подлежащих государственном контролю и надзору, установления порядка получения субъектами государственного контроля и надзора сведений из названных информационных источников»[137].

По мнению профессора С.М. Зубарева, «с развитием новых информационных технологий в работе контролирующих органов расширились возможности оперативного использования разнообразия методов контроля и получения результатов, что, несомненно, окажет влияние на качество самого контроля, устранит поверхностный характер его проведения и будет способствовать улучшению деятельности государственных служащих и органов исполнительной власти»[138].

П.П. Кабытов и О.Е. Стародубова отмечают, что «органы исполнительной власти уже достаточно длительный период времени используют широкий спектр цифровых инструментов и технологий при осуществлении контрольно-надзорной деятельности. В целях повышения эффективности контрольно-надзорной деятельности цифровые техно-

---

троля и надзора в социально значимых сферах деятельности общества и государства: материалы V Всероссийской научно-практической конференции (Россия, г. Нижний Новгород, 7–8 июня 2019 г.) / Отв. ред. доктор юридических наук, профессор А.В. Мартынов. Н. Новгород: Изд-во Нижегородского госуниверситета им. Н.И. Лобачевского, 2019. С. 22–23.

[137] Правовое регулирование государственного контроля: монография / отв. ред. д-р юрид. наук, проф., заслуженный деятель науки РФ А.Ф. Ноздрачев. М.: Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации; Анкил, 2012. С. 84.

[138] Зубарев С.М. Система контроля в сфере государственного управления: монография. М.: Норма: ИНФРА-М, 2019. С. 73.

логии применяются при планировании, проведении и оформлении результатов контрольных мероприятий»[139].

Таким образом, учеными отмечается позитивная роль цифровых технологий и динамическое влияние на развитие содержательных сторон контрольно-надзорной деятельности органов исполнительной власти.

Более того, проведенное нами изучение нормативной основы для внедрения цифровых технологий и фактических процессов автоматизации контрольно-надзорных органов подтверждают нашу гипотезу, что *все без исключения направления (виды) контрольно-надзорной деятельности подвержены глубокой цифровизации*.

Данный вывод подтверждается также выводами экспертов, отмечающих что цифровизация общей организации контрольно-надзорной деятельности включает в себя 3 элемента:

а) единый реестр видов федерального государственного контроля (надзора), регионального государственного контроля (надзора), муниципального контроля;

б) межведомственное информационное взаимодействие;

в) ГАС «Управление»: агрегация статистических и аналитических данных[140].

При этом цифровизация активно осуществляется и по отдельным направлениям контрольно-надзорной деятельности. Так, при организации и проведении профилактических мероприятий цифровизация включает три элемента:

а) обязательное размещение информации в сети Интернет;

б) дистанционное консультирование и профилактический визит;

в) самообследование[141].

По направлению планирование, подготовка и проведение контрольных (надзорных) мероприятий цифровизация включает 5 основных элементов:

а) единый реестр контрольных (надзорных) мероприятий;

б) обмен исключительно электронными документами;

---

[139] Кабытов П.П., Стародубова О.Е. Влияние цифровизации на реализацию полномочий органов исполнительной власти // Журнал российского права. 2020. № 11. С. 113–126.

[140] Контрольно-надзорная и разрешительная деятельность в Российской Федерации. Аналитический доклад – 2020–2021 / С.М. Плаксин (рук. авт. кол.), И.А. Абузярова и др.; Российский союз промышленников и предпринимателей; Нац. исслед. ун-т «Высшая школа экономики». М.: НИУ ВШЭ, 2021. С. 114–116.

[141] Там же. С. 116–117.

в) Ведомственные информационные системы контрольных органов;

г) очно-дистанционные контрольные мероприятия;

д) полностью дистанционные контрольные мероприятия[142].

И, наконец, еще одним направлением цифровизации контрольно-надзорной деятельности органов исполнительной власти, как отмечается экспертами, является досудебное обжалование в электронной форме[143].

В целом соглашаясь с выводами экспертов Института государственного и муниципального управления НИУ «Высшая школа экономики», следует отметить, что экспертами сделан акцент на текущем положении дел в области цифровизации контрольно-надзорной деятельности. Однако не исследованы проблемные вопросы внедрения новых цифровых технологий и проблемы применения имеющихся в распоряжении контрольно-надзорных органов информационных технологий. Не затрагиваются и перспективные направления внедрения в деятельность контрольно-надзорных органов «сквозных» и опережающих цифровых технологий. Все эти вопросы подробно нами исследованы в настоящей работе, а выводы основаны на проведенных опросах должностных лиц контрольно-надзорных органов исполнительной власти, приведенные в приложении к данной монографии и подробно проанализированные в научных статьях[144].

С учетом всестороннего исследования различных вопросов внедрения современных цифровых технологий в деятельность контрольно-надзор-

---

[142] Контрольно-надзорная и разрешительная деятельность в Российской Федерации. Аналитический доклад – 2020–2021 / С.М. Плаксин (рук. авт. кол.), И.А. Абузярова и др.; Российский союз промышленников и предпринимателей; Нац. исслед. ун-т «Высшая школа экономики». М.: НИУ ВШЭ, 2021. С. 117–128.

[143] Там же. С. 128–130.

[144] См.: Мартынов А.В., Ширеева Е.В., Логинова А.В. Проблемы использования цифровых технологий в деятельности органов государственного контроля и надзора в условиях цифровой экономики (исследование проведенное на основе опроса должностных лиц органов государственного контроля и надзора) // Вестник Нижегородского университета им. Н.И. Лобачевского. 2021. № 5. С. 119–135; Мартынов А.В. Развитие новых форм и методов государственного контроля и надзора в условиях цифровой экономики // Законы России: опыт, анализ, практика. 2021. № 11. С. 10-27; Ширеева Е.В. Правовые формы и методы государственного контроля и надзора в сфере обеспечения правопорядка и общественной безопасности в условиях цифровой трансформации органов исполнительной власти // Вестник Воронежского государственного университета. Серия: Право. 2021. № 4.

ных органов, мы приходим к обоснованному выводу о том, что широкомасштабное и повсеместное использование современных цифровых технологий ***трансформирует (изменяет) основную цель государственного контроля и надзора***, которая изначально была связана с обеспечением законности в деятельности контролируемых лиц, предупреждением и профилактикой нарушений обязательных требований, недопущением нарушений требований нормативных правовых актов, и минимизацией ущерба в случаях нарушений законности, то в настоящее время, к этому всему добавляется еще управляемое воздействие, основанное на современных цифровых технологиях, позволяющих минимизировать участие человека при принятии управленческих решений в контрольно-надзорной деятельности и тем самым исключить необоснованное вмешательство в деятельность хозяйствующих субъектов и граждан.

Исходя из определяемых приоритетов внедрения цифровых технологий и автоматизации контрольно-надзорной деятельности, установленных государством для контрольно-надзорных органов, трансформируются и задачи государственного контроля и административного надзора. По нашему мнению, к таким ***новым задачам государственного контроля и административного надзора*** следует отнести:

1) минимизация административного воздействия на хозяйствующих субъектов и граждан, не препятствующее и не создающее помехи их нормальной деятельности, при проверке соблюдениями ими обязательных требований;

2) приоритет использования «бесконтактного» государственного контроля и надзора, то есть приоритет при осуществлении контрольно-надзорной деятельности контрольно-надзорным мероприятиям без взаимодействия с контролируемым лицом;

3) оценка эффективности и результативности контрольно-надзорной деятельности с точки зрения оказания позитивного влияния на развитие цифровой экономики Российской Федерации;

4) возможность взаимодействия контрольно-надзорных органов с контролируемыми лицами по вопросам внедрения в контрольно-надзорную практику передовых («сквозных») цифровых технологий и стимулирование для проверяемых лиц (например, путем установления лояльных или мягких режимов осуществления контрольно-надзорных мероприятий);

5) проведение контрольно-надзорных мероприятий на основе больших данных и другой информации, получаемой в ходе использования современных цифровых дистанционных технологий;

6) роботизация контрольно-надзорных мероприятий, требующих проведение проверки в условиях, представляющих реальную опасность для проверяющих лиц;

7) моделирование различных ситуаций (поведенческих, производственных, технологических и т.д.) посредством использования современных цифровых технологий (искусственного интеллекта, квантовых вычислений, виртуальной и дополненной реальности, цифровых двойников), позволяющее на основе данных вычислений проводить более эффективные контрольно-надзорные мероприятия;

8) учет объектов государственного контроля и надзора должен осуществляться с использованием современных цифровых технологий.

Необходимо обратить внимание и на изменение принципов государственного контроля и надзора. Так, к общим принципам государственного контроля и надзора, закрепленным в главе 2 федеральным законом от 31 июля 2020 г. № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации»[145] добавляются еще и специальные принципы, которые определяют порядок использования современных цифровых технологий при осуществлении государственного контроля и надзора (например, принципы применения искусственного интеллекта при осуществлении государственного контроля и надзора; принципы использования больших данных в контрольно-надзорной деятельности; принципы интернета вещей в контрольно-надзорной деятельности; и т.д.).

Цифровизация контрольно-надзорной деятельности оказывает существенное влияние и на трансформацию форм и методов государственного контроля и административного надзора.

Системный анализ законодательства РФ показывает, что ***формы государственного контроля и надзора*** характеризуют саму деятельность органов исполнительной власти и их должностных лиц при осуществлении государственных функций по контролю и надзору, включающую в себя контрольно-надзорные мероприятия (контрольная закупка; мониторинговая закупка; выборочный контроль; инспекционный визит; рейдовый осмотр; документарная проверка; выездная проверка). Когда как ***методы государственного контроля и надзора*** отражают именно характер оказываемого управленческого воздействия (способы административного воздействия, подходы при осуществлении административного воздействия и контрольно-надзорные действия).

[145] СЗ РФ. 2020. № 31 (часть 1). Ст. 5007.

По нашему мнению, *систему методов государственного контроля и надзора можно представить следующим образом:*

1) ***общие методы государственного контроля и надзора:***

а) предъявление обязательных для исполнения требований (по даче объяснений, по предоставлению или истребованию документов, по допуску на проверяемый объект и т.д.);

б) установление ограничений и запретов (например, на совершение финансовых операций при проведении проверки; запрет и ограничение на эксплуатацию опасного производственного объекта при проведении проверки, запрет на внесение изменений в документацию и технологическое оборудование при проведении проверки и т.п.);

в) анализ полученных результатов в ходе мониторинга;

г) процессуальное (процедурное) документирование контрольно-надзорных мероприятий и контрольно-надзорных действий (составление акта проверки);

д) выдача предписаний по результатам государственного контроля (надзора);

е) проведение профилактических мероприятий.

2) ***специальные методы государственного контроля и надзора:***

а) риск-ориентированный подход (метод);

б) дистанционный контроль (мониторинг);

в) постоянный государственный контроль (надзор);

г) постоянный рейд;

д) контрольно-надзорные действия (осмотр; досмотр; опрос; получение письменных объяснений; истребование документов; отбор проб (образцов); инструментальное обследование; испытание; экспертиза; эксперимент).

Следует отметить, что этот список общих и специальных методов государственного контроля и надзора не является окончательным, он может изменяться и дополняться как федеральным законом от 31 июля 2020 г. № 248-ФЗ, так и другими федеральными законами, регламентирующими иные виды государственного контроля и надзора, не подпадающие под действие основного закона о государственном контроле (надзоре) и муниципальном контроле.

Вместе с тем, следует констатировать, что в настоящее время значительное влияние на развитие и трансформацию форм и методов государственного контроля (надзора) и муниципального контроля оказывают именно ***цифровые технологии***. Эта трансформация связана с несколькими ключевыми параметрами, которые

обеспечивают качественное изменение контрольно-надзорной деятельности:

1) применение цифровых технологий при реализации форм и методов государственного контроля и надзора является важным условием развития цифровой экономики. Цифровизация контрольно-надзорной деятельности органов исполнительной власти в целом оказывает позитивное влияние на развитие форм и методов государственного контроля и надзора. С помощью цифровых технологий обеспечивается прозрачная и оперативная связь между хозяйствующими субъектами и органами публичного управления, что способствует более эффективному разрешения противоречий и конфликтных ситуаций между ними.

2) применение цифровых технологий при осуществлении форм и методов государственного контроля и надзора направлены в целом на автоматизацию контрольно-надзорной деятельности органов исполнительной власти. При этом главная цель такой автоматизации связана с тем, что исключается прямое взаимодействие (прямой контакт) между органами государственного контроля (надзора) и контролируемыми лицами при осуществлении контрольно-надзорных мероприятий и действий.

3) современные цифровые технологии определяют динамику (поступательное развитие) форм и методов государственного контроля и надзора. Они способствуют появлению новых форм и методов государственного контроля и надзора, а равно и муниципального контроля. Уже сейчас можно назвать несколько новых форм и методов, которые основаны на современных цифровых технологиях: учет сведений о соблюдении обязательных требований с использованием ТОР КНД; автоматический контроль в сфере окружающей среды; виртуальный дистанционный контроль (цифровой двойник); дистанционный контроль на основе (с применением) искусственного интеллекта, и др.

4) при осуществлении контрольно-надзорной деятельности происходит получение и обмен информацией в электронной форме, что способствует ускорению процессуальных (процедурных) действий и обеспечению более полной и достоверной информацией всех участников контрольно-надзорных правоотношений.

5) внедрение новых форм и методов государственного контроля (надзора), основанных на «прорывных» и «технологиях ближайшего будущего», должно происходить с осторожностью и поэтапно. В некоторых случаях целесообразно использовать экспериментальные правовые режимы для получения информации об эффективности и результа-

тивности внедрения новых форм и методов государственного контроля и надзора, основанных на современных цифровых технологиях[146].

В современной концепции государственного контроля и административного надзора появляется такой новый элемент, ранее не обозначаемый в качестве основного элемента содержания государственного контроля и государственного надзора, как ***технологии контрольно-надзорной деятельности***.

Следует отметить, что первые шаги по обозначению цифровых технологий контроля в государственном управлении были сделаны С.М. Зубаревым и А.В. Сладковой, которые определили их как «информационно-технологические процессы, охватывающие контрольную деятельность уполномоченных государственных органов, институтов гражданского общества и граждан, направленную на обеспечение эффективности, законности и целесообразности функционирования субъектов исполнительной власти»[147]. При этом они сделали вывод о том, что «цифровые технологии следует относить к обеспечивающим технологиям, то есть технологиям обработки информации, которые используются как средство, инструмент для решения задач контрольной деятельности, не изменяя сам механизм контроля в сфере государственного управления»[148].

Мы уже писали в первой части нашего исследования о своем принципиальном несогласии с вышеуказанным утверждением уважаемых коллег[149]. Однако в настоящее время наши выводы еще более подкреплены проведенными опросами должностных лиц контрольно-надзорных органов, которые показали, что лишь 4 % респондентов не используют современные информационные технологии при реализации контрольно-надзорных полномочий, а 42 % опрошенных лиц отметили, что приме-

---

[146] См.: Мартынов А.В. Развитие новых форм и методов государственного контроля и надзора в условиях цифровой экономики // Законы России: опыт, анализ, практика. 2021. № 11. С. 10–27.

[147] См.: Зубарев С.М., Сладкова А.В. О понятии и сущности цифровых технологий контроля в сфере государственного управления // Административное право и процесс. 2019. № 9. С. 53–59.

[148] Там же.

[149] Перспективные направления правового регулирования использования современных информационных технологий в контрольно-надзорной деятельности органов исполнительной власти: библиотека лучших российских и зарубежных практик: монография / А.В. Мартынов, М.В. Бундин, М.Д. Прилуков, Е.Н. Смирнова, Е.В. Ширеева; под науч. ред. А.В. Мартынова. Н. Новгород: Изд-во Нижегородского госуниверситета им. Н.И. Лобачевского, 2020. С. 17.

нение современных информационных технологии способствуют повышению эффективности осуществления ими контрольно-надзорной деятельности (*см. Приложение*).

Тем самым предложенный С.М. Зубаревым и А.В. Сладковой «узкий» подход при оценке значимости цифровых технологий в контрольно-надзорной деятельности не соответствует фактическому положению дел в этой сфере государственного управления.

Между тем, в настоящее время и в будущем происходят качественные изменения содержания контрольно-надзорной деятельности, которые связаны с внедрением в эту деятельность современных цифровых технологий.

Так, 24 сентября 2021 г. в рамках IX Всероссийского форума региональной информатизации «ПРОФ-IT.2021» выступил с докладом директор Департамента развития инфраструктуры электронного правительства Минцифры России Сергей Цветков, который отметил, что «с 2023 года госконтроль должен стать **полностью безбумажным**, а приоритетом должны стать использование **дистанционных методов контроля**, средств измерения и мониторинга. Для бизнеса будут запущены сервисы для **самопроверки** и **декларирования**»[150].

С учетом современных тенденций цифровизации контрольно-надзорной деятельности, некоторыми учеными предлагаются новые концептуальные определения цифрового государственного контроля (надзора). Так, например, М.М. Прошунин рассматривает государственный цифровой контроль «как деятельность уполномоченных органов государственной власти, а также уполномоченных организаций, в том числе посредством использования технологий SupTech по обеспечению законности и целесообразности проведения операций и сделок с цифровыми правами, включая цифровые финансовые активы, и цифровыми валютами, внедрения и использования финансовых технологий (регуляторные площадки), функционирования финансовых платформ (маркетплейсов) и инвестиционных платформ (краудфайндинг)»[151].

Следовательно, именно цифровые технологии существенным образом изменяют содержательную сторону контрольно-надзорной деятельности.

Вместе с тем, при осуществлении государственного контроля и надзора могут использоваться различные технологии. Так, например,

---

[150] URL: https://knd.gov.ru/news?id=68188 (дата обращения: 01.12.2021).

[151] См.: Прошунин М.М. Государственный цифровой финансовый контроль: правовая сущность // Финансовое право. 2021. № 5. С. 3–7.

при осуществлении мониторинга, который представляется собой специальный режим государственного контроля (надзора) (ст. 96 федерального закона от 31 июля 2020 г. № 248-ФЗ), могут применяться специальные технические средства, имеющие функции фотосъемки, аудио- и видеозаписи, измерения.

При осуществлении государственного контроля (надзора) должна создаваться инфраструктура, обеспечивающая информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме (ч. 4 ст. 21 федерального закона от 31 июля 2020 г. № 248-ФЗ).

Федеральный закон от 31 июля 2020 г. № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» не содержит понятия информационных или цифровых технологий, используемых при осуществлении государственного контроля (надзора).

В соответствии со ст. 2 федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[152] под *информационными технологиями* понимаются процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Понятие цифровых технологий содержится в Разъяснениях (методических рекомендациях) по разработке региональных проектов в рамках федеральных Национальной программы «Цифровая экономика Российской Федерации», утвержденные приказом Министерством цифрового развития, связи и массовых коммуникаций РФ от 1 августа 2019 г. № 428. Согласно данным Методическим рекомендациям, цифровые технологии – это понятие, которое может использоваться в трех основных категориях:

1) постепенно внедряемые (цифровое образование, цифровые платформы, маркетинговая интеграция, умные помощники (чат-боты), мобильные платежи);

2) прорывные (интернет вещей, искусственный интеллект, виртуальная реальность, беспроводная связь, дополненная реальность);

[152] СЗ РФ. 2006. № 31 (часть 1). Ст. 3448.

3) технологии ближайшего будущего (офисные роботы, квантовые вычисления, директивная аналитика, криптовалюта)[153].

«Сквозные» цифровые технологии представляют собой ключевые научно-технические направления, которые оказывают наиболее существенное влияние на развитие рынков. К «сквозным» относятся те технологии, которые одновременно охватывают несколько трендов или отраслей[154].

Информационные и цифровые технологии прежде всего позволяют автоматизировать контрольно-надзорную деятельность. В нашем исследовании мы делаем акцент именно на цифровых технологиях, которые обеспечивают развитие «цифровой экономики». Исходя из этого, применение современных цифровых технологий способствует ***автоматизации контрольно-надзорной деятельности,*** которая происходит по нескольким направлениям:

1) широкое распространение в деятельности контрольно-надзорных органов государственных информационных систем, в том числе ведомственных информационных систем;

2) внедрение в контрольно-надзорную деятельность «сквозных» цифровых технологий (искусственный интеллект, большие данные, интернет вещей);

3) создание единой информационной системы контрольно-надзорной деятельности;

4) использование облачных технологий в контрольно-надзорной деятельности, таким как Типовое облачное решение по автоматизации контрольно-надзорной деятельности (ГИС ТОР КНД);

5) применение цифровых платформ для взаимодействия государственных органов между собой и контролируемыми лицами (гражданами и организациями);

6) внедрение новых форм и методов цифрового государственного контроля и надзора;

---

[153] Пункт 29 Раздела 1 Разъяснений (методических рекомендаций) по разработке региональных проектов в рамках федеральных проектов Национальной программы «Цифровая экономика Российской Федерации», утвержденные Приказом Минкомсвязи России от 1 августа 2018 г. № 428 // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

[154] Пункт 28 Раздела 1 Разъяснений (методических рекомендаций) по разработке региональных проектов в рамках федеральных проектов Национальной программы «Цифровая экономика Российской Федерации», утвержденные Приказом Минкомсвязи России от 1 августа 2018 г. № 428 // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

7) внедрение совместно с контролируемыми лицами «сквозных» технологий ближайшего будущего (цифровой двойник, высокоавтоматизированные транспортные средства, квантовые вычисления, роботы и т.п.);

8) проведения контрольно-надзорных мероприятий, основанных на широком применении цифровых технологий, и исключающее непосредственное взаимодействие контрольно-надзорного органа и контролируемых лиц (граждан и организаций).

9) внедрение мобильных приложений для должностных лиц контрольно-надзорных органов и контролируемых лиц (граждан и организаций), позволяющих обеспечивать проведение контрольно-надзорных мероприятий в электронном виде, и осуществлять взаимодействие по различным вопросам контрольно-надзорной деятельности с контролируемыми лицами;

10) перевод обязательных требований в машиночитаемый вид (формат), позволяющий в автоматическом режиме модернизировать (совершенствовать) эти требования и осуществлять их проверку соблюдения.

Изменение качественных характеристик государственного контроля и надзора должны учитывать необходимые ***условия применения цифровых технологий в контрольно-надзорной деятельности***.

Во-первых, расширение видов государственного контроля и административного надзора, которые осуществляются с применением различных цифровых технологий в приоритетном порядке. Соответственно, должны быть определены виды государственного контроля и надзора, при осуществлении которых недопустимо применение определенных цифровых технологий (например, виды государственного контроля и надзора в области обеспечения национальной безопасности), и виды контрольно-надзорной деятельности, в которой в обязательном порядке должны использоваться современные цифровые технологии (например, государственный надзор в сфере Интернета).

Во-вторых, приоритет должен отдаваться цифровым технологиям, разработчиками которых являются отечественные производители. В первую очередь, должно внедрять в деятельность контрольно-надзорных органов российское программное обеспечение. В некоторых случаях, оно может проигрывать в конкуренции зарубежным производителям. Однако вопросы обеспечения безопасности и бесперебойной работы государственных органов должны иметь приоритетное значение. Кроме того, использование отечественных цифровых технологий позволит выявить их недостатки и слабые стороны, что в дальнейшем

позволит усовершенствовать информационные технологии и будет происходить поступательное движение вперед к передовым («сквозным») цифровым технологиям мирового уровня.

В-третьих, существуют различия применения современных цифровых технологий при осуществлении государственного контроля и административного надзора. По общему правилу при административном надзоре применение цифровых технологий осуществляется с согласия проверяемого лица, либо с уведомлением о применении цифровых технологий (примером могут быть правила установления дорожных знаков о применении фото- и видеосъемки камерами, работающими в автоматическом режиме). Для установки каких-либо датчиков, камер и т.п. на объекте или направление информации в контрольно-надзорный орган в постоянном режиме для этого требуется согласие от организации или гражданина. Так, например, эксперимент по внедрению системы дистанционного контроля промышленной безопасности проводится на основании соглашения, заключаемого между организацией или индивидуальным предпринимателем, эксплуатирующей опасных производственных объект, и Федеральной службой по экологическому, технологическому и атомному надзору (Ростехнадзором России)[155]. При осуществлении государственного контроля в отношении подчиненных должностных лиц или подведомственных организаций такого согласия, как правило, не требуется.

В-четвертых, на законодательном уровне должны быть разграничены государственный контроль и административный (государственный) надзор. Это является необходимым условием для успешного использования цифровых технологий, так каждый вид управленческой деятельности имеет свои особенности административно-правового воздействия на контролируемых лиц, что предполагает установление различных административно-правовых режимов применения современных цифровых технологий. Так, применения цифровых технологий в отношении неподчиненных граждан и организаций при осуществлении административного надзора имеет свои специфические особенности, связанные с дополнительными гарантиями соблюдения их прав, свобод и законных интересов.

---

[155] Пункт 5 Положения о проведении эксперимента по внедрению системы дистанционного контроля промышленной безопасности, утвержденного постановлением Правительства РФ от 31 декабря 2020 г. № 2415 // СЗ РФ. 2021. № 3. Ст. 557.

В-пятых, необходимо строго обеспечивать баланс интересов граждан и организаций, и органов государственного контроля и надзора. Этот баланс связан с тем, что не всегда применение цифровых технологий могут совпадать с интересами общества и государства. Зачастую происходят ситуации, когда государство считает необходимым использовать какие-то цифровых технологии, однако общество (граждане и организации) рассматривают такое административное воздействие в качестве чрезмерного и нецелесообразного вмешательства в их личную жизнь или предпринимательскую деятельность. В некоторых случаях, применение цифровых технологий может препятствовать нормальной жизни людей или деятельности граждан и организаций. Показательным примером может быть не всегда удачные способы использования цифрового контроля в отношении граждан в период пандемии. Иногда государство просто не в состоянии обеспечить сохранность полученной информации (персональных данных, сведений о деятельности организаций), что впоследствии причиняет еще более значительный вред граждан или организациям, чем предотвращенный ущерб от контрольно-надзорных мероприятий при осуществлении государственного контроля и надзора. А в некоторых случаях, участие в человека в контрольно-надзорной деятельности невозможно заменить цифровыми технологиями (например, государственный контроль (надзор) в сфере сохранности объектов культурного наследия). При отдельных видах государственного контроля и надзора требуется именно взаимодействие людей, а не машин (механическая или автоматизированная проверка).

В-шестых, цифровые технологии должны использоваться только при условии их контроля со стороны человека и возможности их перепроверки со стороны контролируемых лиц (граждан и представителей организаций). Отсутствие открытости, прозрачности, понятности и перепроверки принимаемых решений органов государственного контроля и надзора посредством современных цифровых технологий не будут основаниям для недоверия со стороны граждан и общества ко всей контрольно-надзорной деятельности государства. Как показало наше исследование, даже сами должностные лица контрольно-надзорных органов исполнительной власти не всегда доверяют современным информационным технологиям по причине отсутствия необходимых знаний об их работе, а также опасением некорректной работы или функционирования цифровых технологий и информационных систем. Таким образом, должны быть обеспечены правовые и организационные механизмы независимой проверки (перепроверки) принимаемых решений контрольно-надзорных органов посредством цифровых технологий.

В-седьмых, следует обеспечивать необходимый уровень материально-технического обеспечения и профессиональной подготовки должностных лиц контрольно-надзорных органов. Исследование показало, что во многих органах исполнительной власти отсутствуют возможности для внедрения современных цифровых технологий. Так, среди проблем в этой области должностными лицами контрольно-надзорных органов называлось устаревшие компьютеры и программное обеспечение, отсутствие в штате государственного органа технических специалистов, оказывающих помощь в работе с информационными системами и цифровыми технологиями. Исходя из этого, требуется серьезное обновление материально-технической базы большинства органов исполнительной власти, осуществляющих государственные функции по контролю и надзору, и в которых планируется внедрение современных цифровых технологий.

Таким образом, современная концепция государственного контроля и административного надзора основывается на следующих ***элементах, образующих его целостную организационно-правовую систему***.

Первый элемент: Понятие и сущность государственного контроля и административного надзора.

Под **государственным контролем** понимается деятельность органов публичной власти, направленная на предупреждение, выявление и пресечение нарушений обязательных требований и иных требований законности, осуществляемая в рамках общей функции управления, в отношении подчиненных органов публичной власти и их должностных лиц, а также подведомственных организаций, посредством использования информационных технологий и проведения профилактических мероприятий нарушений обязательных требований и иных требований, установленных ведомственными нормативными актами, оценки соблюдения контролируемыми лицами указанных требований, пресечения нарушений обязательных и иных требований, с целью обеспечения законности и целесообразности деятельности контролируемых лиц, и принятия мер дисциплинарного и иного организационно-правового характера в отношении контролируемых лиц.

Под **административным (государственным) надзором** понимается деятельность органов государственного надзора, направленная на предупреждение, выявление и пресечение обязательных требований, осуществляемая в отношении граждан, организационно неподчиненных должностных лиц, организаций и учреждений, с использованием информационных и цифровых технологий для автоматизации деятельно-

сти, посредством профилактики нарушений обязательных требований, оценки соблюдения организационно неподчиненными гражданами, должностными лицами, организациями и учреждениями обязательных требований, выявления их нарушений, принятие предусмотренных законодательством Российской Федерации по пресечению выявленных нарушений обязательных требований, устранению их последствий и (или) восстановлению правового положения, существовавшего до возникновения таких нарушений, и наделенных полномочиями по возбуждению дел об административных правонарушениях и (или) привлечению виновных лиц к административной ответственности.

Сущность государственного контроля состоит в том, что это является универсальной формой деятельности органов публичной власти, в том числе контрольными полномочиями наделены и органы государственного надзора (например, при осуществлении лицензионного контроля, контроля за переданными надзорными полномочиями другим органам публичной власти). Он осуществляется всеми без исключения органами публичной власти, а поэтому рассматривается в качестве общей функции управления. При этом органами государственной власти могут применяться различные формы и методы государственного контроля, которые могут закрепляться как в законах, так и подзаконных нормативных правовых актах, так и в ведомственных нормативных правовых актах. Целью государственного контроля является обеспечение законности и дисциплины в деятельности подчиненных и подведомственных органов, организаций и учреждений, а также должностных лиц, которые оцениваются не только с точки зрения соблюдения обязательных требований, но и их иных требований, а также дается оценка целесообразности и эффективности деятельности контролируемых лиц. Меры административного воздействия включают дисциплинарную ответственность, организационные и материально-технические мероприятия. Цифровые средства государственного контроля и автоматизация контрольной деятельности прежде всего направлена на своевременное и полное получение необходимой информации о деятельности контролируемого лица. При этом согласия на применение информационных или цифровых технологий от контролируемого лица не требуется.

Сущность административного надзора заключается в административно-правовом воздействии на граждан, организационно неподчиненных должностных лиц, организаций и учреждений, деятельность которых оценивается исключительно с точки зрения законности. Способы государственного надзора разнообразны, но ограничены на уровне

законов (то есть формы и методы государственного надзора должны быть закреплены законом, а не другим каким-то нормативным актом). Большинство органов государственного надзора используют в своей деятельности риск-ориентированный подход (метод). Административный надзор осуществляется уполномоченными органами государственного надзора и специальными должностными лицами – инспекторами. При административном надзоре происходит влияние и ограниченное вмешательство в деятельность поднадзорных лиц, которое должно быть снижено за счет автоматизации надзорной деятельности и применения современных информационных и цифровых технологий, и не приносить непоправимого ущерба экономическим отношениям. Цифровизация государственного надзора позволяет надзорным органам осуществлять эффективное взаимодействие с гражданами, организационно неподчиненными должностными лицами, организациями и учреждениями, проводить надзорные мероприятия без личного взаимодействия с поднадзорными лицами, что снижает коррупционные риски и благоприятно влияет на развитие «Цифровой экономики». Государственный надзор может реализовываться посредством профилактики соблюдения обязательных требований, подготовки, планирования и проведения надзорных мероприятий, применения специальных административно-правовых режимов (режим постоянного государственного надзора), применения по пресечению выявленных нарушений обязательных требований, устранению их последствий и (или) восстановлению правового положения, существовавшего до возникновения таких нарушений, а также что очень важно путем возбуждения дел об административных правонарушения и (или) привлечения виновных лиц к административной ответственности. Органы государственного надзора могут устанавливать обязательные требования для граждан, организационно неподчиненных должностных лиц, организаций и учреждений.

Для государственного контроля и административного надзора должны устанавливаться различные критерии оценки результативности и эффективности контрольной и надзорной деятельности.

Второй элемент: современные цели и задачи государственного контроля и административного надзора (определены в данном параграфе).

Третий элемент: общие и специальные принципы государственного контроля и административного надзора (рассмотрены как в данном параграфе, так и в отдельных статьях[156]).

[156] Мартынов А.В., Бундин М.В. О правовых принципах применения искусственного интеллекта при осуществлении органами исполнительной власти

Четвертый элемент: правовые основы государственного контроля и административного надзора (рассмотрены в данном параграфе).

Пятый элемент: основные направления контрольно-надзорной деятельности (профилактическая деятельность; планирование, подготовка и проведение контрольных (надзорных) мероприятий; применение специальных административно-правовых режимов государственного контроля и надзора; интеграционная деятельность по привлечению к административной ответственности по результатам проведения контрольно-надзорных мероприятий; досудебное обжалование решений контрольно-надзорных органов и их должностных лиц; и другое).

Шестой элемент: современные формы и методы государственного контроля и административного надзора, в том числе основанные на современных цифровых технологиях (рассмотрены как в данном параграфе, так и в отдельных статьях[157]).

Седьмой элемент: автоматизация контрольно-надзорной деятельности (рассмотрена как в данном параграфе, так и в отдельных статьях[158]).

контрольно-надзорной деятельности // Журнал российского права. 2020. № 10. С. 59–75.

[157] Мартынов А.В. Использование современных цифровых технологий при осуществлении профилактической деятельности контрольно-надзорных органов исполнительной власти // Юрист. 2020. № 10. С. 48-56; Мартынов А.В. Развитие новых форм и методов государственного контроля и надзора в условиях цифровой экономики // Законы России: опыт, анализ, практика. № 11. 2021. С. 10-27; Ширеева Е.В. Правовые формы и методы государственного контроля и надзора в сфере обеспечения правопорядка и общественной безопасности в условиях цифровой трансформации органов исполнительной власти // Вестник Воронежского государственного университета. Серия: Право. 2021. № 4.

[158] Мартынов А.В. Влияние цифровой трансформации на контрольно-надзорную деятельность органов исполнительной власти // Публичная власть в современной России: проблемы и перспективы: сборник научных трудов по материалам международной научно-практической конференции памяти доктора юридических наук, профессора, заслуженного деятеля науки РСФСР Василия Михайловича Манохина (VII Саратовские административно-правовые чтения) (8 июня 2021 г., Саратов) / под общ. ред. А.Ю. Соколова; редкол. А.Ю. Соколов и др.; Саратовская государственная юридическая академия; Саратовский филиал ФГБУН «Институт государства и права РАН». Саратов: Изд-во Саратовской государственной юридической академии, 2021. С. 32-56; Логинова А.Э. Современные информационные технологии при осуществлении контроля и надзора в сфере обращения лекарственных средств // Вестник Нижегородского университета им. Н.И. Лобачевского. 2020. № 3. С. 126-131; Логинова А.Э. Цифровиза-

Восьмой элемент: технологии контрольно-надзорной деятельности. Условия применения цифровых технологий в контрольно-надзорной деятельности (определены в данном параграфе).

Девятый элемент: контрольно-надзорные мероприятия и контрольно-надзорные действия, в том числе осуществляемые с использованием цифровых технологий (рассмотрены как различных параграфах монографии, так и в отдельных статьях[159]).

Десятый элемент: Взаимодействие органов государственного контроля (надзора) и контролируемых лиц, в том числе информационное взаимодействие (рассмотрены в отдельных статьях[160]).

Одиннадцатый элемент: Исполнение принятых решений при осуществлении государственного контроля и административного надзора, в том числе с использованием цифровых технологий (рассмотрены в отдельных статьях[161]).

Двенадцатый элемент: пересмотр решений, принятых по результатам проведения контрольно-надзорных мероприятий, досудебное обжалование решений контрольно-надзорных органов и их должностных лиц в электронной форме (рассмотрены в отдельных статьях).

ция государственного контроля качества лекарственных средств в России // Вестник Нижегородского университета им. Н.И. Лобачевского. 2021. № 4. С. 152–158; Смирнова Е.Н. Обеспечение соблюдения прав и свобод личности при осуществлении органами исполнительной власти цифрового контроля // NB: Административное право и практика администрирования. 2021. № 3. С. 37–45; Смирнова Е.Н. Об актуальных вопросах использования информационных технологий в профилактическом направлении контрольно-надзорной деятельности органов исполнительной власти // NB: Административное право и практика администрирования. 2020. № 2. С. 27–37; Ширеева Е.В. Правовые основы применения и практики внедрения искусственного интеллекта при осуществлении судебного контроля // Вестник Воронежского государственного университета. Серия: Право. 2020. № 3 (42). С. 30–39.

[159] Логинова А.Э. Цифровизация государственного контроля качества лекарственных средств в России // Вестник Нижегородского университета им. Н.И. Лобачевского. 2021. № 4. С. 152–158.

[160] Смирнова Е.Н. Обеспечение соблюдения прав и свобод личности при осуществлении органами исполнительной власти цифрового контроля // NB: Административное право и практика администрирования. 2021. № 3. С. 37–45.

[161] Мартынов А.В. Использование современных цифровых технологий при осуществлении профилактической деятельности контрольно-надзорных органов исполнительной власти // Юрист. 2020. № 10. С. 48–56.

Глава 2
Особенности реализации концепции в отдельных направлениях контрольно-надзорной деятельности

§ 1. Контроль и надзор за обеспечением правопорядка и общественной безопасности

В административно-правовой науке юридическое содержание контроля и надзора включает в себя цели, задачи, функции, субъекты, объекты, формы и методы. Учеными-административистами, занимающимися проблематикой контрольно-надзорной деятельности органов исполнительной власти, на сегодняшний день сформированы традиционные представления об указанных элементах[1]. Однако в современный период времени в Российской Федерации активно формируется и используется законодательное регулирование отношений, возникающих в связи с развитием цифровой экономики.

Ведущими российскими учеными отмечается, что в сфере правового регулирования появились отношения, субъектами которых стали «цифровые личности»; отношения, связанные с юридически значимой идентификацией личности в виртуальном пространстве; отношения, возникающие в связи с реализацией прав человека в «цифровом пространстве»; отношения, связанные с применением робототехники; отношения, связанные с использованием информационных баз данных; отношения, сопряженные с реализацией государственных функций в вирту-

[1] См., например: Студеникина М.С. Государственный контроль в сфере управления. Проблемы надведомственного контроля. М.: Юридическая литература, 1974. 160 с.; Зарубицкая Т.К., Скляров И.А. Правовое положение органов, обеспечивающих законность в государственном управлении. Н. Новгород: НА МВД РФ, 1993 / Скляров Иван Александрович. Избранные труды. Н. Новгород: Изд-во Нижегородского госуниверситета им. Н.И. Лобачевского, 2018. С. 140–206; Мартынов А.В. Проблемы правового регулирования административного надзора в России. Административно-процессуальное исследование. М.: NOTA BENE, 2010. 548 с.; Зырянов С.М. Административный надзор. М.: ИД «Юриспруденция», 2010. 208 с. и др.

альном пространстве и их переводом в цифровую форму и другое[2]. В связи с чем закономерным представляется и трансформация в условиях цифровой экономики основных элементов государственного контроля и надзора. Это также напрямую обуславливается внедряемыми современными информационными технологиями в контрольную и надзорную деятельность органов исполнительной власти.

Бесспорно, что одним из ключевых направлений государственной политики в Российской Федерации является обеспечение правопорядка и общественной безопасности, о чем свидетельствуют Стратегия национальной безопасности Российской Федерации[3] (далее – Стратегия) и Концепция общественной безопасности в Российской Федерации[4] (далее – Концепция). Из множества задач, поставленных в Стратегии и Концепции для достижения цели обеспечения государственной и общественной безопасности и имеющих возможность реализации в рамках административно-правовых отношениях, необходимо отметить:

– выявление и пресечение преступлений, связанных с незаконным оборотом оружия, боеприпасов, взрывчатых веществ, а также наркотических средств, психотропных веществ и их прекурсоров;

– повышение безопасности дорожного движения;

– повышение эффективности мер по предупреждению и ликвидации чрезвычайных ситуаций природного и техногенного характера.

Указанные задачи могут реализовываться в рамках административно-правовых отношений, в том числе, посредством осуществления государственного контроля и надзора соответствующими органами исполнительной власти. К таким важнейшим видам контрольной и надзорной деятельности следует отнести:

---

[2] Хабриева Т.Я., Черногор Н.Н. Право в условиях цифровой реальности // Журнал российского права. 2018. № 1. С. 94–96.

[3] Указ Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001202107030001?index=18&rangeSize=1 (дата обращения: 01.09.2021).

[4] Концепция общественной безопасности в Российской Федерации (утв. Президентом РФ 14.11.2013 № Пр-2685) // СПС «КонсультантПлюс» [Электронный ресурс]. URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=154602&dst=1000000001%2C0#U9RXtkSbOlD7FS05 (дата обращения: 01.09.2021).

– государственный надзор за соблюдением участниками дорожного движения требований законодательства Российской Федерации в области безопасности дорожного движения сотрудниками органов внутренних дел РФ;

– государственный надзор и муниципальный контроль за обеспечением сохранности автомобильных дорог;

– государственный контроль (надзор) в сфере деятельности, связанной с оборотом прекурсоров наркотических средств и психотропных веществ;

– контроль за оборотом гражданского, служебного и наградного оружия, боеприпасов, патронов к оружию, сохранностью и техническим состоянием боевого ручного стрелкового и служебного оружия, находящегося во временном пользовании у граждан и организаций, а также за соблюдением гражданами и организациями законодательства Российской Федерации в области оборота оружия;

– государственный пожарный надзор.

Исходя из чего следует, что основными ***субъектами*** государственного контроля и надзора в сфере обеспечения правопорядка и общественной безопасности являются Госавтоинспекция, иные территориальные органы МВД России, Ространснадзор, Росгвардия, территориальные органы МЧС России, а также их должностные лица.

В связи с попытками внедрения технологий искусственного интеллекта некоторыми учеными активно высказывается позиция о возможности его рассмотрения в качестве самостоятельного субъекта права. А.В. Незнамов, В.Б. Наумов в разработанной ими Модельной конвенции о робототехнике и искусственном интеллекте отмечают, что роботы в гражданском обороте могут выступать в качестве самостоятельных лиц[5]. П.М. Морхат вводит понятие специфической правосубъектности «электронного лица»[6]. Рядом ученых сформулированы признаки искусственного интеллекта, которые в некоторым смысле могут его характеризовать как самостоятельный субъект права, – это умение анализировать данные; способность адаптации своего поведения; автономия; воз-

[5] Модельная конвенция о робототехнике и искусственном интеллекте // Проект «Робоправо» [Электронный ресурс]. URL: https://robopravo.ru/matierialy_dlia_skachivaniia (дата обращения: 28.11.2021).

[6] Морхат П.М. К вопросу о правосубъектности «электронного лица» // Юридические исследования. 2018. № 4 [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/k-voprosu-o-pravosubektnosti-elektronnogo-litsa/viewer (дата обращения: 27.11.2021).

можность самообучения и т.д.[7] Также высказывается позиция об определении искусственного интеллекта через термин «квази-субъект права»[8]. Однако возникают закономерные вопросы, насколько правильно позиционировать искусственный интеллект как самостоятельный субъект, в том числе в рамках осуществления государственного контроля и надзора в рассматриваемой сфере, и возможно ли это в условиях существующей правовой действительности?

Большинство ученых достаточно негативно высказываются о наделении искусственного интеллекта статусом субъекта права и полагают, что его необходимо позиционировать как объект права[9]. В свою очередь хочется отметить, что на законодательном уровне в Российской Федерации вопросы развития искусственного интеллекта, его основные принципы и направления развития и использования, а также цели и задачи использования изложены в Национальной стратегии развития искусственного интеллекта на период до 2030 года[10]. Но среди приоритетных направлений использования технологий искусственного интеллекта в социальной сфере указано лишь повышение качества предоставления государственных и муниципальных услуг, а также снижение затрат на их предоставление. Возможность применения робототехники и искусственного интеллекта при осуществлении государственного контроля и надзора не рассматривается.

На международном уровне с 2018 года действует Европейская этическая хартия об использовании искусственного интеллекта в судебных системах и смежных областях. Данная Хартия закрепляет пять важных принципов использования искусственного интеллекта:

«1) принцип уважения основополагающих прав: обеспечить разработку и внедрение инструментов и услуг, основанных на искусственном интеллекте, соответствующих основным правам;

---

[7] Шестак В.А., Волеводс А.Г. Современные потребности правового обеспечения искусственного интеллекта: взгляд из России // Всероссийский криминологический журнал. 2019. Т. 13. № 2. С. 197–206.

[8] Голубцов В.Г. Российская Федерация как субъект гражданского права. М.: Статут, 2019. 272 с.

[9] См. подробнее мнения ученых в статье: Филипова И.А. Искусственный интеллект и нейротехнологии: потребности в конституционно-правовом регулировании // Lex russica. 2021. № 9 (178). С. 119-130.

[10] Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») // СПС «КонсультантПлюс» [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_335184/ (дата обращения: 30.10.2021).

2) принцип недискриминации: определенным образом препятствовать развитию или усилению любой дискриминации между отдельными лицами или группами лиц;

3) принцип качества и безопасности: при обработке судебных решений и данных, необходимо использовать сертифицированные источники и нематериальные данные с применением моделей, разработанных на междисциплинарной основе, в безопасной технологической среде;

4) принцип прозрачности, беспристрастности и достоверности: сделать методы обработки данных доступными и понятными, разрешить проведение внешнего аудита;

5) принцип контроля пользователем: избежать предписывающего подхода и позволить пользователю выступать в роли информированного лица, ответственного за свой выбор»[11].

Указанные принципы фактически исключают основные правовые риски нарушения прав и законных интересов человека и гражданина при его применении и фактически в публично-правовой сфере не позволяют использовать искусственный интеллект в качестве самостоятельного субъекта, который может принимать автономные решения.

Применяемые в зарубежных странах и Российской Федерации программы основываются на технологии «слабого» искусственного интеллекта, что, безусловно, является правильным решением, так как «сильный» искусственный интеллект, способный к самообучению и развитию, в такой важной сфере может представлять какую-либо опасность причинения вреда человеку. «Слабый» искусственный интеллект не способен выносить обоснованные и справедливые решения по существу правового вопроса.

Контроль и надзор в сфере обеспечения правопорядка и общественной безопасности представляет собой деятельность уполномоченных субъектов и преследует такие ***задачи***, как обеспечение законности и дисциплины в деятельности граждан и организаций, поддержание общественного правопорядка и безопасности, выявление и пресечение противоправных действий, привлечение виновных к административной ответственности. Более того, контроль и надзор являются одними из функций исполнительной власти, что также не позволяет применять

[11] Европейская этическая хартия об использовании искусственного интеллекта в судебных системах и окружающих их реалиях, принята на 31-м пленарном заседании ЕКЭП (Страсбург, 3-4 декабря 2018 года) // URL: https: //rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c (дата обращения: 30.10.2021).

искусственный интеллект как самостоятельный субъект в рамках административно-правовых отношений.

Кроме того, в рамках проведенного опроса должностных лиц органов исполнительной власти (см. Приложение) было установлено, что лишь 1% должностных лиц в рамках контрольно-надзорной деятельности применяет роботов помощников / интеллектуальных помощников и лишь 10% должностных лиц в качестве перспективной в контрольно-надзорной деятельности видят применение технологии искусственного интеллекта. Это еще раз подтверждает мысль, что в условиях российской правовой действительности возможность использования искусственного интеллекта в качестве самостоятельного субъекта контрольно-надзорной деятельности исключена. *Но не исключена возможность применения технологий искусственного интеллекта в рамках форм и методов государственного контроля и надзора, которые существенным образом влияют на их трансформацию в условиях «цифровой экономики»*.

Объектами контроля и надзора в сфере обеспечения общественной безопасности и правопорядка являются физические и юридические лица, которые обязаны соблюдать установленные законодательством правила поведения. Трансформация объекта в условиях цифровизации наблюдается в государственном надзоре за соблюдением участниками дорожного движения требований законодательства Российской Федерации в области безопасности дорожного движения сотрудниками органов внутренних дел России. Это обусловлено появлением на дорогах беспилотных транспортных средств. В своем большинстве водитель находится в салоне автомобиля для того, чтобы среагировать в экстренных ситуациях. Но, например, в США в пригороде Феникса уже запущено дочерней компанией Google – Waymo беспилотное такси, в котором водитель отсутствует вообще[12]. Похожая практика в ближайшее время также может быть внедрена и в России. Крупные российские автомобильные компании уже проводят соответствующие разработки в данном направлении. Однако, как отмечается учеными, российское законодательство в настоящее время не совсем готово к появлению беспилотных транспортных средств на дорогах[13]. В связи с чем требуется

[12] URL: https://tass.ru/ekonomika/10733185 (дата обращения: 12.11.2021).

[13] См. подробнее: Bunbin M., Martynov A., Rumyantsev F. Legal framework for self-driving cars: the case of Russia // ACM International Conference Proceeding Series. 13, Digital Governance in the Era of Disruptive Technologies and Globalisa-

внесение изменений в законодательство Российской Федерации, в частности создание технических регламентов, в которых будет предусмотрена возможность эксплуатации такого рода транспортных средств, разработка норм, которые регулировали бы вопросы ответственности участников дорожного движения.

В условиях переосмысления субъектов и объектов государственного контроля и надзора в сфере обеспечения правопорядка и общественной безопасности первоочередным является трансформация правовых форм и методов государственного контроля, так как эффективность выполнения органами исполнительной власти контрольных и надзорных функций в сфере обеспечения правопорядка и общественной безопасности в значительной степени зависит от правильности выбора данных форм и методов.

Серьезную проблему их применения составляет отсутствие в административно-правовой науке единого подхода к определению понятий «форма государственного контроля и надзора» и «метод государственного контроля и надзора», а также к критериям их разграничения. В связи с чем из положений ныне действующего ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации»[14] достаточно сложно правоприменителям установить правовую природу указанных в нем контрольных (надзорных) мероприятий и действий.

В рамках данного научного исследования поддерживается позиция профессора Мартынова А.В., согласно которой под формами государственного контроля и надзора понимается сама деятельность органов исполнительной власти и их должностных лиц при осуществлении государственных функций по контролю и надзору, включающую в себя контрольно-надзорные мероприятия, а под методами государственного контроля и надзора – характер оказываемого управленческого воздействия[15].

---

tion. Сер. «Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance, ICEGOV 2020» 2020. P. 206-213.

[14] Федеральный закон от 31.07.2020 № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» // СЗ РФ. 2020. № 31 (часть I). Ст. 5007.

[15] Прим.: указанное понимание форм и методов государственного контроля и надзора разработано д.ю.н., профессором А.В. Мартыновым в рамках реализации научного проекта РФФИ № 20-011-00584 «Концепция правового регулирования использования информационных технологий в сфере государственного контроля и надзора в условиях «цифровой экономики»; см. подробнее: Марты-

Исходя из анализа зарубежной практики и опыта Российской Федерации, нами было установлено, что наиболее востребованными в настоящий период в рассматриваемой сфере являются передовые информационные системы, беспилотные летательные аппараты и технологии искусственного интеллекта[16].

Так, среди передовых информационных систем следует выделить геоинформационные системы и межведомственные информационные системы, позволяющие обрабатывать большое количество информации в базах данных. Такого рода системы могут быть применимы в любом из выше указанных видов контрольно-надзорной деятельности органов исполнительной власти в сфере обеспечения правопорядка и общественной безопасности.

В Российской Федерации имеется положительный опыт их внедрения и использования. Так, в практической деятельности успешно применяются:

– геоинформационная система МВД России – позволяет создать единое информационное пространство и обеспечить информационный обмен между органами государственной власти;

– геоинформационная система «Экстремум» МЧС России – позволяет спрогнозировать вероятность возникновения чрезвычайных ситуаций, по возможности, предотвратить их, а также спланировать работы по ликвидации последствий чрезвычайных ситуаций с расчетом сведения к минимуму причиненного ущерба;

– федеральная государственная информационная система «Система обеспечения предоставления информации МВД России в рамках межведомственного электронного взаимодействия МВД России (ВИС-СМЭВ)» – позволяет осуществлять межведомственное служебное электронное взаимодействие, а также получать информацию из общих баз данных.

нов А.В. Развитие новых форм и методов государственного контроля и надзора в условиях цифровой экономики // Законы России: опыт, анализ, практика. 2021. № 11. С. 10–27.

[16] См. подробнее: Перспективные направления правового регулирования использования современных информационных технологий в контрольно-надзорной деятельности органов исполнительной власти: библиотека лучших российских и зарубежных практик: монография / А.В. Мартынов, М.В. Бундин, М.Д. Прилуков, Е.Н. Смирнова, Е.В. Ширеева. Н. Новгород: Изд-во Нижегородского госуниверситета им. Н.И. Лобачевского, 2020. 227 с.

Кроме того, ведется активная разработка, не имеющей аналогов в мире, электронной системы Росгвардии для осуществления контроля за оборотом оружия. Предполагается, что посредством данной системы автоматически будет отслеживаться путь каждой единицы выпускаемого в стране оружия от завода до конечного пользователя, в том числе патронов к оружию.

Исходя из возможностей отмеченных геоинформационных систем и межведомственных информационных систем, они являются и могут стать одним из важных инструментов при реализации такой формы государственного контроля и надзора как *документарная проверка*. Среди общих методов государственного контроля и надзора они могут быть применимы для *проведения профилактических мероприятий* в виде *информирования*. А электронная система Росгвардии для осуществления контроля за оборотом оружия позволит более эффективно применять такой специальный метод как *дистанционный государственный контроль (мониторинг)*.

Нововведением в осуществлении государственного контроля и надзора является применение беспилотных летательных аппаратов. Правовое регулирование их применения в государственном секторе фактически только начинает формироваться. Однако некоторая практика их использования в Российской Федерации все же имеется. Беспилотные летательные аппараты в качестве эксперимента использовались при обеспечении правопорядка и общественной безопасности в государственном надзоре за соблюдением участниками дорожного движения требований законодательства Российской Федерации в области безопасности дорожного движения сотрудниками органов внутренних дел РФ; государственном надзоре и муниципальном контроле за обеспечением сохранности автомобильных дорог; государственном пожарном надзоре.

Контроль и надзор за обеспечением безопасности автомобильных дорог с использованием беспилотных летательных аппаратов имеет перспективы развития в следующих направлениях:

– контроль за состоянием дорог – использование БПЛА помогает решить такие задачи, позволяющие принять верные управленческие решения, как мониторинг улично-дорожной сети города; аэрофотосъемка автомобильных и железных дорог, придорожной обстановки; учет и мониторинг дорог, объектов придорожной инфраструктуры; оценка состояния дорог; создание цифровой картографической основы дорожно-транспортной инфраструктуры; создание аэрофотоснимков при проектировании, эксплуатации и строительстве дорог;

– оперативный мониторинг – использование БПЛА позволит в кратчайшие сроки при возникновении чрезвычайных ситуаций обнаружить угрозы безопасности граждан.

В связи с этим новую интерпретацию в указанной сфере могут получить такие специальные методы государственного контроля и надзора как *дистанционный контроль (мониторинг)*, а также *контрольно-надзорные действия в форме осмотра.*

При осуществлении государственного надзора за соблюдением участниками дорожного движения требований законодательства РФ в области безопасности дорожного движения возможность использования беспилотных летательных аппаратов для выявления нарушений правил дорожного движения закреплена в Приказе МВД России от 23.08.2017 № 664 «Об утверждении Административного регламента исполнения Министерством внутренних дел Российской Федерации государственной функции по осуществлению федерального государственного надзора за соблюдением участниками дорожного движения требований законодательства Российской Федерации в области безопасности дорожного движения»[17]. Однако детальной регламентации порядка и правил их использования не имеется. Хотя к беспилотным летательным аппаратам фактически могут быть прикреплены специальные технические приборы, которые позволят фиксировать скорость движения транспортных средств, соблюдение дорожной разметки, дорожно-транспортные происшествия и т.д. То есть в данном случае использование беспилотных летательных аппаратов позволит модернизировать такой специальный метод государственного контроля и надзора как *инструментальное обследование*.

При осуществлении государственного пожарного надзора беспилотные летательные аппараты в своем большинстве на постоянной основе применяются:

– для проведения воздушной разведки кромки действующего крупного пожара;

– в качестве географически привязанного воздушного пункта наблюдения («летающей вышки») для обнаружения пожаров в районах

[17] Приказ МВД России от 23.08.2017 № 664 «Об утверждении Административного регламента исполнения Министерством внутренних дел Российской Федерации государственной функции по осуществлению федерального государственного надзора за соблюдением участниками дорожного движения требований законодательства Российской Федерации в области безопасности дорожного движения» // Российская газета. 2017. № 232.

возникновения высокой (чрезвычайной) пожарной опасности лесов, прежде всего в целях защиты населенных пунктов;

– для осмотра действующих пожаров в чрезвычайные периоды, когда применение классической авиации невозможно из-за задымленности района;

– для мониторинга состояния торфяных пожаров;

– для отслеживания продвижения лесных пожаров и прогнозирования их развития с учетом метеорологических условий и пирогенных факторов;

– для патрулирования лесов с целью контроля соблюдения правил рубок компаниями-лесозаготовителями[18].

В связи с чем представляется возможным их использование при применении такой формы государственного контроля и надзора как *наблюдение за соблюдением обязательных требований,* а также специальных методов – реализация *контрольных и надзорных действий в виде осмотра* и *инструментального обследования*.

Правовое регулирование применения технологий искусственного интеллекта в контрольной и надзорной деятельности органов исполнительной власти в сфере обеспечения общественной безопасности и правопорядка находится на стадии становления. Национальная стратегия развития искусственного интеллекта на период до 2030 года[19] предусматривает возможность их применения лишь для повышения качества предоставления государственных и муниципальных услуг, а также снижения затрат на их предоставление. В связи с чем в Российской Федерации успешной практики их реализации в контрольной и надзорной деятельности не имеется, за исключением практики внедрения технологии распознавания лиц.

Исходя из анализа «лучших зарубежных практик», наиболее перспективными, и которые могут повлиять на расширение возможностей применения форм и методов государственного контроля и надзора в рассматриваемой сфере, видятся технология распознавания лиц, интеллектуальная транспортная система и программные роботы-помощники.

---

[18] URL: https://rusdrone.ru/otrasli/primeneniya-bespilotnikov-dlya-monitoringa-lesov/ (дата обращения: 10.01.2021).

[19] Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») // СПС «КонсультантПлюс» [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_335184/ (дата обращения: 10.09.2021).

Технология распознавания лиц представляет собой систему с искусственным интеллектом, который способен к машинному обучению, самостоятельному сбору и анализу больших объемов данных. Такая технология может эффективно способствовать осуществлению в Российской Федерации государственного надзора за соблюдением участниками дорожного движения требований законодательства Российской Федерации в области безопасности дорожного движения; государственного контроля (надзора) в сфере деятельности, связанной с оборотом прекурсоров наркотических средств и психотропных веществ; контроля за оборотом гражданского, служебного и наградного оружия, боеприпасов, патронов к оружию, сохранностью и техническим состоянием боевого ручного стрелкового и служебного оружия, находящегося во временном пользовании у граждан и организаций, а также за соблюдением гражданами и организациями законодательства Российской Федерации в области оборота оружия; государственного пожарного надзора, например, путем определения лиц, совершивших административное правонарушение, либо наблюдения за субъектами, принимающими участие в осуществлении оборота прекурсоров наркотических средств, психотропных веществ, оружия и т.п.

Таким образом, технология распознавания лиц может получить свое распространение при применении такого общего метода контроля и надзора, как *анализ полученных результатов мониторинга,* а также специального метода – это *дистанционный контроль (мониторинг).*

Интеллектуальная транспортная система – это система, интегрирующая современные информационные, коммуникационные и телематические технологии, технологии управления и предназначенная для автоматизированного поиска и принятия к реализации максимально эффективных сценариев управления транспортной системой региона, конкретным транспортным средством или группой транспортных средств, с целью обеспечения заданной мобильности населения; максимизации показателей использования дорожной сети; повышения безопасности эффективности транспортного процесса; комфортности для водителей и пользователей транспорта[20].

В Российской Федерации основополагающим документом, регламентирующим внедрение интеллектуальных транспортных систем, является национальный проект «Безопасные и качественные автомобиль-

[20] URL: http://www.dorros.ru/wp-content/uploads/2019/12/prezits.pdf (дата обращения: 15.09.2021).

ные дороги»[21] и федеральный проект «Общесистемные меры развития дорожного хозяйства». Предполагается, что интеллектуальная транспортная система будет обладать функциями видеонаблюдения, мониторинга параметров транспортных потоков, метеомониторинга, светофорного управления, информирования участников дорожного движения с помощью динамических информационных табло и знаков переменной информации, мониторинга экологических параметров, весогабаритного контроля транспортных средств, контроля соблюдения ПДД и контроля общественного транспорта. В настоящий момент указанная технология внедряется в 22 субъектах Российской Федерации, которые стали пилотными площадками на конкурсной основе.

Учитывая многофункциональность интеллектуальных транспортных систем, следует отметить, что они могут получить широкую реализацию в методах осуществления государственного контроля и надзора. Во-первых, в осуществлении *дистанционного контроля (мониторинга)* и последующем *анализе полученных результатов мониторинга*, во-вторых, в *контрольно-надзорных действиях в виде инструментального обследования*.

Программные роботы-помощники в мировой практике используются в целях облегчения принятия и вынесения решения по делу. В своем большинстве на современном этапе развития информационных технологий они применяются в судебной деятельности. Однако учитывая специфику контрольной и надзорной деятельности органов исполнительной власти в Российской Федерации, которая включает в себя полномочия органов исполнительной власти по вынесению решения по делу и назначению наказания за административное правонарушение, указанные технологии искусственного интеллекта могут использоваться при осуществлении государственного надзора за соблюдением участниками дорожного движения требований законодательства Российской Федерации в области безопасности дорожного движения.

Они могут применяться в порядке упрощенного производства, когда административное наказание назначается сотрудниками ГИБДД без составления протокола об административном правонарушении в случа-

[21] Паспорт национального проекта «Безопасные и качественные автомобильные дороги» (утв. президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам, протокол № 15 от 24.12.2018) // официальный сайт «Росавтодор» [Электронный ресурс]. URL: http://static.government.ru/media/files/rBdyoIr3S9IDP8Q87lXXYaktpKWGc0NY.pdf (дата обращения: 15.09.2021).

ях, предусмотренных ст. 28.6 Кодекса Российской Федерации об административных правонарушениях[22]. Фактически такие роботы-помощники способны в автоматизированном режиме обрабатывать информацию, полученную с устройств фото- и видео фиксации, и на ее основе формировать постановления о привлечении к административной ответственности за нарушение ПДД. Причем мера административного наказания (размер штрафа) также будет формироваться системой в автоматизированном режиме посредством анализа существующей практики применения, что будет обеспечивать объективность и беспристрастность решения по конкретному делу.

Аналогичные возможности роботов-помощников также могут быть применимы при реализации таких общих методов контроля и надзора как *процессуальное (процедурное) документирование контрольных и надзорных мероприятий и контрольных и надзорных действий*, в частности при составлении актов проверки, а также *анализе полученных результатов в ходе мониторинга.*

Кроме того, следует предположить, что они могут способствовать объективной выборке объектов контроля и надзора при применении такого специального метода как *риск-ориентированный подход*. Фактически роботы-помощники также позволят с большей точностью проведение в некоторых случаях *контрольных и надзорных действий в виде эксперимента* в виртуальном пространстве.

Таким образом, подводя итог к данному параграфу, необходимо отметить следующее:

во-первых, в условиях цифровизации происходит трансформация основных элементов государственного контроля и надзора за обеспечением правопорядка и общественной безопасности;

во-вторых, возможность использования искусственного интеллекта как самостоятельного субъекта контрольно-надзорной деятельности в условиях российской правовой действительной исключена. Однако данные технологии могут эффективно применяться в правовых формах и методах государственного контроля и надзора за обеспечением правопорядка и общественной безопасности;

в-третьих, происходит усложнение объекта контроля и надзора за обеспечением правопорядка и общественной безопасности в связи с внедрением современных информационных технологий в социальную сферу, что обуславливает необходимость цифровой трансформации

[22] Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ // СЗ РФ. 2002. № 1 (ч. 1). Ст. 1.

правовых форм и методов рассматриваемого вида государственного контроля и надзора;

во-четвертых, в сфере контроля и надзора за обеспечением общественной безопасности и правопорядка прорывные информационные технологии находят отражение в такой форме государственного контроля и надзора как документарная проверка и наблюдение за соблюдением обязательных требований;

в-пятых, в сфере контроля и надзора за обеспечением общественной безопасности и правопорядка прорывные информационные технологии используются при применении такого общего метода государственного контроля и надзора как проведение профилактических мероприятий, а также таких специальных методов как дистанционный государственный контроль (мониторинг) и контрольно-надзорные действия в форме осмотра и инструментального обследования;

в-шестых, в сфере контроля и надзора за обеспечением общественной безопасности и правопорядка технологии ближайшего будущего могут применяться для реализации таких общих методов государственного контроля и надзора как анализ полученных результатов в ходе мониторинга и процессуальное (процедурное) документирование контрольно-надзорных мероприятий и контрольно-надзорных действий (составление акта проверки), а также такие специальные методы как дистанционный государственный контроль (мониторинг), риск-ориентированный подход, контрольно-надзорные действия в виде инструментального обследования и эксперимента.

§ 2. Контроль и надзор в сфере фармакологии и медицины

Проводимая реформа контрольно-надзорной деятельности в Российской Федерации охватывает важнейшие сферы и направления деятельности государства, механизмы которых заставляют по-новому функционировать систему органов исполнительной власти для достижения максимальной эффективности в реализации своих полномочий, обеспечения безопасности общества и защиты прав и свобод граждан и организаций. В основе модернизации лежат разные инструменты, однако, акцент сделан на внедрение новых цифровых технологий и поиск оптимальных форм и методов при осуществлении отдельных видов государственного контроля и надзора. По словам заместителя Председателя Правительства – Руководителя Аппарата Правительства Григоренко

Дмитрия Юрьевича, «…по результатам пятилетней работы подготовлены и приняты закон о госконтроле, фундаментальный по своей сути, и его закон-спутник. Не погрешу против истины, если скажу, что за два последних десятилетия мы впервые приводим в порядок все правовые акты, регулирующие государственный и муниципальный контроль. Это имеет огромное значение для всей законодательной системы России. В законе о госконтроле предусмотрено смещение акцента с проверок, затратных как для бизнеса, так и для контрольных органов, на профилактику и предупреждение нарушений. «Спутник» вносит изменения в 132 отраслевых закона, которые регулируют 96 видов федерального контроля, 30 видов регионального контроля и 7 видов муниципального контроля. В продолжение реформы мы работаем над порядком 500 нормативными правовыми актами, направленными на исполнение закона о госконтроле и закона-спутника. Значительная часть правительственных актов, необходимых для этого, уже принята. Возвращаясь к закону о госконтроле, хочу отметить, что при его подготовке мы исходили из необходимости цифровизации контрольно-надзорной деятельности, снижения интенсивности контактов, проверяющих с проверяемыми. Для этого предусмотрено использование ряда информационных систем, в их числе – единый реестр контрольных мероприятий, единый реестр видов контроля, информационная система досудебного обжалования»[23].

Поскольку охрана здоровья граждан и обеспечение безопасной деятельности организаций при оказании медицинской помощи является стратегически важной сферой функционирования государства, то это направление имеет важное значение при реализации вышеуказанной реформы. Все изменения, проводимые в рамках реформы контроля и надзора в сфере здравоохранения, достаточно обширны и в значительной мере связаны с цифровизацией в самой системе здравоохранения. Как отмечает председатель комитета Госдумы по охране здоровья Д.А. Морозов, «телемедицинские технологии и совершенствование Геоинформационной системы, всей единой государственной информационной системы здравоохранения – определяющие в доступности и качестве медицины будущего. Россией накоплен серьезный опыт, и в том числе на пике эпидемии COVID-19, по взаимодействию «врач-врач», «врач-пациент», работе консультативных центров, мониторинге

[23] Проверки меняют акцент // Российская газета [Электронный ресурс]. URL: https://rg.ru/2021/07/12/dmitrij-grigorenko-vsiu-kontrolno-nadzornuiu-sistemu-nuzhno-delat-bolee-sovremennoj.html (дата обращения: 07.12.2021).

здоровья. Следует закрепить в законе новые возможности телемедицины, искусственного интеллекта и систем поддержки врачебных решений. Следует быстрее перейти на полный электронный документооборот, в том числе в системе взаимодействия с контролирующими органами, Следственным комитетом и прокуратурой. В продолжение принятого закона о дистанционной продаже лекарств необходимы подзаконные акты, гарантирующие качество доставки, работу фармацевтов и курьеров, информационных систем и отсутствие фальсификата. Развитие этого направления – на парламентском контроле»[24]. В развитие этого направления Правительством РФ был утвержден план создания целого ряда электронных медицинских сервисов: предложения по принятию нормативных правовых актов в целях внедрения в субъектах Российской Федерации электронных рецептов; предложения по внесению изменений в нормативные правовые акты в целях развития продажи лекарств дистанционным способом; предложения по выделению в структуре тарифа медицинской услуги расходов на информационные технологии и др.[25]

Всё это требует определенной модернизации и контрольно-надзорной деятельности в сфере здравоохранения, поэтому рассмотрим, на наш взгляд, основные аспекты в этом ключе.

Так, Постановлением Правительства Российской Федерации от 29.06.2021 г. № 1048 утверждено «Положение о федеральном государственном контроле (надзоре) качества и безопасности медицинской деятельности»[26] (далее – Положение о контроле (надзоре) качества и безопасности медицинской деятельности), которое устанавливает порядок организации и осуществления федерального государственного контроля (надзора) качества и безопасности медицинской деятельности, а также

[24] Законодательное регулирование здравоохранения Российской Федерации: итоги работы Комитета Государственной Думы по охране здоровья в период 2016-2021 годов // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

[25] План мероприятий («дорожная карта») «Создание дополнительных условий для развития отрасли информационных технологий», утв. Правительством РФ 09.09.2021 // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

[26] Постановление Правительства РФ от 29.06.2021 № 1048 «Об утверждении Положения о федеральном государственном контроле (надзоре) качества и безопасности медицинской деятельности» // СЗ РФ. 2021. № 27 (часть III). Ст. 5426.

закрепляет предмет государственного контроля (надзора), которым является:

1. Соблюдение медицинскими организациями (в том числе медицинскими работниками), фармацевтическими организациями (в том числе фармацевтическими работниками), Федеральным фондом обязательного медицинского страхования и территориальными фондами обязательного медицинского образования, индивидуальными предпринимателями, осуществляющими медицинскую деятельность, и индивидуальными предпринимателями, осуществляющими фармацевтическую деятельность, обязательных требований в сфере охраны здоровья, требований к объектам, используемым при осуществлении деятельности в сфере охраны здоровья в том числе:

1.1. прав граждан в сфере охраны здоровья;

1.2. порядка оказания медицинской помощи, положений об организации оказания медицинской помощи по видам медицинской помощи, правил проведения лабораторных, инструментальных, патологоанатомических и иных видов диагностических исследований, порядка проведения медицинских экспертиз, диспансеризации, диспансерного наблюдения, медицинских осмотров и медицинских освидетельствований;

1.3. стандартов медицинской помощи;

1.4. порядка и условий предоставления платных медицинских услуг, за исключением обязательных требований, отнесенных к предмету федерального государственного надзора в области защиты прав потребителей;

1.5. ограничений, налагаемых на медицинских работников, руководителей медицинских организаций, фармацевтических работников и руководителей аптечных организаций, при осуществлении ими профессиональной деятельности;

1.6. требований к организации и проведению внутреннего контроля качества и безопасности медицинской деятельности;

1.7. требований к обеспечению доступности для инвалидов объектов инфраструктуры и предоставляемых услуг в сфере охраны здоровья.

2. Соответствия оказываемой медицинскими работниками медицинской помощи критериям оценки качества медицинской помощи.

3. Соблюдение лицензионных требований при осуществлении медицинской деятельности.

Кроме этого, в данном нормативном акте не конкретизируются формы и методы осуществления государственного контроля и надзора. В рамках данного научного исследования поддерживается позиция

профессора Мартынова А.В., что «положения, устанавливающие особенности осуществления отдельных видов государственного контроля и надзора, регламентируют проведение контрольных (надзорных) мероприятий, и также не используют термины «формы» и «методы» государственного контроля (надзора). С нашей точки зрения, если следовать логике законодателя, то к формам государственного контроля и надзора следует отнести контрольно-надзорные мероприятия, а к методам государственного контроля и надзора контрольно-надзорные действия».

В соответствии с п. 42 Положения о контроле (надзоре) качества и безопасности медицинской деятельности при осуществлении государственного контроля (надзора) проводятся следующие виды контрольных (надзорных) мероприятий: а) документарная проверка; б) выездная проверка; в) контрольная закупка; г) инспекционный визит. Таким образом, данные виды мероприятий можно отнести к формам, осуществляемые в сфере контроля (надзора) качества и безопасности медицинской деятельности. К методам можно отнести установленные в п. 44 контрольные (надзорные) действия, которые могут совершаться в ходе документарной проверки: а) получение объяснений в письменной форме; б) истребование документов; в) экспертиза. В п. 51 закрепляется, что в ходе выездной проверки могут совершаться следующие контрольные (надзорные) действия: а) осмотр; б) опрос; в) получение письменных объяснений; г) истребование документов; д) экспертиза. В п. 54 утверждается, что в ходе контрольной закупки может совершаться контрольное (надзорное) действие - осмотр. В п. 59 указываются, что в ходе инспекционного визита могут совершаться следующие контрольные (надзорные) действия: а) осмотр; б) опрос; в) получение письменных объяснений. Однако важно отметить, что при осуществлении контрольных (надзорных) действий для фиксации инспектором и лицами, привлекаемыми к совершению контрольных (надзорных) действий, доказательств нарушений обязательных требований могут использоваться фотосъемка, аудио- и видеозапись (п.39). Само по себе использование фотосъемки, аудио- и видеозаписи как один из способов получения доказательств не является новым и, на наш взгляд, не может свидетельствовать о применении цифровых технологий, однако в положении есть метод контроля (надзора), который вполне можно соотнести с цифровыми технологиями. Он закреплен в п. 53, где указывается, что контрольная закупка может проводиться с использованием почтовой связи, сетей электросвязи, в том числе сети «Интернет», а также сетей связи для трансляции телеканалов и (или) радиоканалов (далее – ди-

станционная контрольная закупка). Законодатель установил понятие дистанционной контрольной закупки, однако порядок использования данного метода в положении не раскрыт, что, по нашему мнению, приводит к тому, что данный метод использовать нельзя, поскольку отсутствует регламентация порядка использования данного метода при осуществлении контроля (надзора) качества и безопасности медицинской деятельности.

Кроме этого, еще одним новшеством, которое было установлено в Положении о контроле (надзоре) качества и безопасности медицинской деятельности, является внедрение досудебного порядка подачи жалобы (Раздел V) контролируемым лицом в Федеральную службу по надзору в сфере здравоохранения в электронном виде с использованием единого портала государственных и муниципальных услуг и (или) регионального портала государственных и муниципальных услуг. Интересным моментом является то, что данное новшество получило определенную апробацию перед внедрением. Заместитель Председателя Правительства – Руководитель Аппарата Правительства Григоренко Дмитрий Юрьевич следующим образом ответил на вопрос о том, зачем система обязательного досудебного обжалования действий и решений контрольно-надзорных органов, вводимая законом с 2023 года, в пилотном формате была запущена ещё в августе 2020 года: «Мы хотели обкатать систему, посмотреть, где могут возникнуть проблемные моменты, чтобы устранить их до полноформатного запуска системы. В эксперименте участвовали 19 министерств и ведомств, чья деятельность охватывает около 90% всего существующего контроля. В их числе ФНС России, МЧС России, Ростехнадзор, Ростуризм, Роструд, Роспотребнадзор, Росздравнадзор, Росалкогольрегулирование, Минпромторг. В ходе эксперимента удалось создать инструмент прямого дистанционного общения заявителя и контрольного органа. Появилась понятная среда для разрешения споров, процессы которой на всех этапах, начиная от подачи жалобы до её разрешения, являются максимально прозрачными. Работает это следующим образом. На портале госуслуг запущен специальный сервис, который позволяет подать жалобу в контрольный орган в электронном виде, а также отслеживать все этапы её рассмотрения и взаимодействовать с должностными лицами без личного посещения ведомства. Процедура рассмотрения жалоб четко регламентирована: на ответ заявителю даётся 20 рабочих дней. Работа сервиса построена на основе наиболее распространённых жизненных ситуаций, с которыми сталкиваются предприниматели и граждане в процессе общения с кон-

трольными органами. В числе таких ситуаций, например, нарушение процедуры проведения проверки, несогласие с назначенным по итогам проверки предписанием. Процедура максимально проста и удобна как для заявителей, так и для контролёров. Единой точкой входа для подачи жалоб стал новый сервис на портале госуслуг. Он позволяет не только буквально в «три клика» подать жалобу, но и максимально упрощает при этом процедуру взаимодействия контрольного органа и лица, подавшего жалобу. Процесс рассмотрения жалобы может контролироваться заявителем в режиме онлайн, в том числе со своего смартфона. Для контрольных органов также была создана своя информационная среда. Она учитывает специфику каждого контрольного органа и позволяет обеспечить единый подход к рассмотрению жалоб в различных контрольных органах. На сегодняшний день к информационной системе досудебного обжалования подключён 31 контрольный орган в 85 субъектах Российской Федерации. Мы также получили инструмент для анализа наиболее частых оснований жалоб в конкретных сферах и корректировки законодательства по итогам такого анализа. Кстати, досудебное обжалование как процедура, так и сам сервис по реализации этой процедуры построены по принципу, исключающему истории, когда контролёр, например, кого-то проверил, потом на него же жалуются, и он же рассматривает, насколько качественно он проводил проверку»[27].

Однако, при всех положительных моментах, на наш взгляд, есть и определённый недостаток, который касается порядка подачи жалобы. При подаче жалобы гражданином она должна быть подписана простой электронной подписью либо усиленной квалифицированной электронной подписью. При подаче жалобы организацией жалоба должна быть подписана усиленной квалифицированной электронной подписью. Возникает ряд закономерных вопросов. Во-первых, что делать, если электронная подпись отсутствует у гражданина и у организации? Процесс получения электронной подписи требует определённых временных затрат и действий. Во-вторых, что делать, если по техническим и иным причинам портал государственных и муниципальных услуг и (или) региональный портал государственных и муниципальных услуг не работает или «подвисает»? Таким образом, при определенных обстоятельствах возникают барьеры и данный механизм может и не сработать. На

[27] Проверки меняют акцент // Российская газета [Электронный ресурс]. URL: https://rg.ru/2021/07/12/dmitrij-grigorenko-vsiu-kontrolno-nadzornuiu-sistemu-nuzhno-delat-bolee-sovremennoj.html (дата обращения: 07.12.2021).

наш взгляд, должен быть сформирован альтернативный путь подачи жалобы, например, подача жалобы, через многофункциональные центры по оказанию государственных и муниципальных услуг, где бы гражданин или представитель от организации не имея цифровой, в том числе квалифицированной подписи, могли подать жалобу.

Как указывает д.ю.н, профессор А.В. Мартынов, что 21 декабря 2016 г. был утвержден Паспорт приоритетной программы «Реформа контрольной и надзорной деятельности»[28], в рамках которого было предусмотрено внедрение в контрольно-надзорную деятельность современных цифровых технологий, таких как: технологии работы с массивами больших данных (Big Data); расчет показателей результативности и эффективности деятельности контрольно-надзорных органов в автоматическом режиме; создание электронных личных кабинетов поднадзорных субъектов; внедрение электронного декларирования «Электронный инспектор»; использование «интернета вещей» в целях совершенствования контрольно-надзорной деятельности; и др.

Таким образом, при реформировании системы государственного контроля и надзора государством был задан вектор на активное внедрение современных цифровых технологий в деятельность органов государственного контроля и надзора. Необходимо отметить, что на сегодняшний день такой платформой выступает государственная информационная система «Типовое облачное решение по автоматизации контрольной (надзорной) деятельности»[29] (далее – ТОР КНД). Данная государственная информационная система создается в целях реализации полномочий федеральных органов исполнительной власти, государственных корпораций, публично-правовых компаний, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и подведомственных им организаций, осуществляющих государственный контроль (надзор) и муниципальный контроль, а также в целях досудебного обжалования решений контрольного (надзорного) органа, действий (бездействия) его должност-

[28] Паспорт приоритетной программы «Реформа контрольной и надзорной деятельности», утвержден решением президиума Совета при Президенте РФ по стратегическому развитию и приоритетным проектам 21 декабря 2016 г. (приложение к протоколу № 12) (в ред. от 30.05.2017 г.) // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

[29] Постановление Правительства РФ от 21.04.2018 № 482 «О государственной информационной системе «Типовое облачное решение по автоматизации контрольной (надзорной) деятельности» // СЗ РФ. 2018. № 18. Ст. 2633.

ных лиц при осуществлении государственного контроля (надзора), муниципального контроля. ТОР КНД предназначена для автоматизации решения следующих задач: а) управление рисками причинения вреда (ущерба) охраняемым законом ценностям, вызванного нарушениями обязательных требований; б) оценка результативности и эффективности деятельности контрольных (надзорных) органов; в) учет сведений о соблюдении обязательных требований; г) межведомственное информационное взаимодействие с гражданами и организациями (далее - контролируемые лица), контрольными (надзорными) органами, иными государственными органами, органами местного самоуправления и подведомственными им организациями; д) проведение профилактических и контрольных (надзорных) мероприятий, специальных режимов государственного контроля (надзора), в том числе с использованием мобильного приложения государственной информационной системы; е) досудебное обжалование решений контрольных (надзорных) органов, действий (бездействия) их должностных лиц; ж) ведение дел об административных правонарушениях.

Таким образом, модернизация контрольно-надзорной деятельности в сере здравоохранения обеспечивается единой государственной информационной системой «Типовое облачное решение по автоматизации контрольной (надзорной) деятельности».

Одно из важнейших мест в системе охраны здоровья граждан занимает сфера обращения лекарственных средств. Она объединяет собой целый ряд этапов так называемого «жизненного цикла» лекарства: разработку, доклинические исследования, клинические исследования, экспертизу, государственную регистрацию, стандартизацию и контроль качества, производство, изготовление, хранение, перевозку, ввоз в Российскую Федерацию, вывоз из Российской Федерации, рекламу, отпуск, реализацию, передачу, применение, уничтожение лекарственных средств, - что, безусловно, имеет свое правовое закрепление в Федеральном законе «Об обращении лекарственных средств»[30] (далее по тексту – Закон об обращении лекарственных средств).

Основным контрольно-надзорным органом в этой сфере, как и в целом в системе охраны здоровья, является Федеральная служба по надзору в сфере здравоохранения (далее по тексту – Росздравнадзор). Одной из ее приоритетных задач в рамках реформы контрольно-надзорной деятельности выступает «создание и внедрение комплексной

[30] Федеральный закон от 12.04.2010 № 61-ФЗ «Об обращении лекарственных средств» // Российская газета. 2010. № 78; 2021. № 133.

модели информационного обеспечения и системы автоматизации контроля (надзора) в сфере здравоохранения»[31], что, несомненно, распространяется и на обращение лекарственных средств.

Как отмечается в литературе, «цифровизация контрольно-надзорной деятельности рассматривается в качестве одного из действенных инструментов достижения целей текущего этапа реформы»[32], к которым относятся «повышение уровня безопасности, устранение избыточной административной нагрузки на субъекты предпринимательской деятельности»[33]. Конечно, Росздравнадзор и иные контрольно-надзорные органы, реализующие свои полномочия в сфере обращения лекарств, имеют тот или иной опыт применения информационных технологий в своей деятельности, что уже помогло достичь определенных результатов на пути реформирования данной сферы реализации исполнительной власти.

Для подтверждения данного суждения стоит обратиться к Стандарту информатизации контрольно-надзорной деятельности (далее по тексту – Стандарт), в котором выделяются три уровня функциональных возможностей ведомственных информационных систем контрольно-надзорных органов: базовый, средний и высокий, а также критерии их определения[34]. Относительно Росздравнадзора можно констатировать, что его деятельность соответствует среднему уровню Стандарта, так как:

1) должностные лица Росздравнадзора осуществляют все свои функции от планирования контрольных мероприятий с применением риск-ориентированного подхода до учета начисленных штрафов и исполнения предписаний в электронном виде[35];

---

[31] Реформа контрольно-надзорной деятельности // Федеральная служба по надзору в сфере здравоохранения [Электронный ресурс]. URL: https://roszdravnadzor.gov.ru/reform (дата обращения: 15.10.2021).

[32] Кабытов П.П., Стародубова О.Е. Влияние цифровизации на реализацию полномочий органов исполнительной власти // Журнал российского права. 2020. № 11. С. 117.

[33] Там же.

[34] Комплексные требования к информационным системам, обеспечивающим выполнение контрольно-надзорных функций органами исполнительной власти (Стандарт информатизации контрольно-надзорной деятельности) (утв. протоколом заседания проектного комитета от 14 июня 2017 г. № 40 (6)) // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

[35] Публичный отчет Федеральной службы по надзору в сфере здравоохранения по итогам работы в 2019 году // Федеральная служба по надзору в сфере

2) используются личные кабинеты в автоматизированной информационной системе (далее по тексту – АИС) Росздравнадзора[36];

3) ведомственная информационная система разрешает отдельные задачи в рамках систематизации обязательных требований (на сайте Росздравнадзора представлен развернутый перечень нормативно-правовых актов, содержащих обязательные требования, с необходимой дополнительной информацией[37]);

4) реализован механизм направления уведомлений в подконтрольные организации о проведении контрольных мероприятий в электронном виде из информационной системы Росздравнадзора[38];

5) ведется работа по созданию интерактивных сервисов для добровольного подтверждения подконтрольным субъектом соблюдения обязательных требований в электронном виде[39].

Об этом же свидетельствует «Паспорт реализации проекта «Совершенствование функции государственного надзора в сфере здравоохранения в рамках реализации приоритетной программы Реформа контрольной и надзорной деятельности»[40]. Согласно его содержанию, одним из направлений реализации данного проекта является автоматиза-

---

здравоохранения [Электронный ресурс]. URL: https://roszdravnadzor.gov.ru/about/declaration (дата обращения: 03.11.2021).

[36] АИС Росздравнадзора [Электронный ресурс] // URL: http://external.roszdravnadzor.ru/?type=logon (дата обращения: 03.11.2021).

[37] Перечень нормативных правовых актов (их отдельных положений), содержащих обязательные требования, оценка соблюдения которых осуществляется в рамках государственного контроля (надзора), привлечения к административной ответственности в соответствии с постановлением Правительства Российской Федерации от 22.10.2020 № 1722 по состоянию на 10.11.2021 // Федеральная служба по надзору в сфере здравоохранения [Электронный ресурс]. URL: https://roszdravnadzor.gov.ru/services/prevention (дата обращения: 03.11.2021)

[38] Публичный отчет Федеральной службы по надзору в сфере здравоохранения по итогам работы в 2019 году // Федеральная служба по надзору в сфере здравоохранения [Электронный ресурс]. URL: https://roszdravnadzor.gov.ru/about/declaration (дата обращения: 03.11.2021).

[39] Приказ Росздравнадзора от 04.05.2021 № 3881 «Об утверждении Ведомственной программы профилактики нарушений обязательных требований при осуществлении государственного контроля качества и безопасности медицинской деятельности, федерального государственного надзора в сфере обращения лекарственных средств и государственного контроля за обращением медицинских изделий» // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

[40] Утв. протоколом заседания проектного комитета от 13.02.2018 № 1 // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

ция контрольно-надзорной деятельности, в рамках которой была завершена разработка по приведению ведомственной информационной системы до соответствия среднему уровню стандарта информатизации контрольно-надзорной деятельности.

Вместе с тем важно, чтобы такой опыт по использованию цифровых технологий в контрольно-надзорной деятельности органов государственной власти стал систематизированным, оформленным в стройную концепцию. Понятно, что для этого необходим целый комплекс мер различного характера (в том числе правового, технического, организационного). Росздравнадзором уже многое запланировано в этом русле. Например, принята ведомственная программа цифровой трансформации данного органа[41], которая предусматривает, помимо прочего, в рамках федерального государственного надзора в сфере обращения лекарственных средств достижение к 2023 году 100% выполнения таких показателей, как:

– доля проверок, проведенных дистанционно с использованием чек-листов в электронном виде от общего объема проверок;

– доля проведенных проверок, по которым результаты сформированы в автоматизированном режиме на основе заполненных в электронном виде чек-листов от общего объема проведенных проверок.

Кроме того, Сводным Планом реализации Федеральной службой по надзору в сфере здравоохранения паспорта приоритетного проекта «Совершенствование контрольной и надзорной деятельности в сфере здравоохранения»[42] предусматривался целый ряд мероприятий (к настоящему времени уже завершенных), направленных на расширение использования цифровых технологий в деятельности данного органа:

1) создание и использование личного кабинета должностного лица для планирования и исполнения контрольно-надзорных мероприятий с использованием исчерпывающих реестров проверяемых объектов

[41] Приказ Росздравнадзора от 30.12.2020 № 12641 «О внесении изменений в приказ Федеральной службы по надзору в сфере здравоохранения от 15 декабря 2020 г. № 11931 «Об утверждении ведомственной программы цифровой трансформации Федеральной службы по надзору в сфере здравоохранения на 2021–2023 годы»» // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

[42] Комплексная модель информационного обеспечения и системы автоматизации контроля (надзора) // Федеральная служба по надзору в сфере здравоохранения [Электронный ресурс]. URL: https://roszdravnadzor.gov.ru/reform/automation (дата обращения: 05.11.2021).

2) предоставление в электронном виде в единый реестр проверок соответствующих учетных данных;

3) внедрение возможности досудебного обжалования подконтрольными субъектами в электронном виде и др.

Более того, Росздравнадзор намерен использовать в своей деятельности и сквозные цифровые технологии. К примеру, планируется применять технологии искусственного интеллекта для обработки поступающих в орган обращений граждан, количество которых стабильно растет от года к году. Так, в 2020 году этот показатель увеличился на 39%, причем более 60% обращений посвящено вопросам лекарственного обеспечения[43].

Важным моментом является тот факт, что цифровую трансформацию в сфере обращения лекарств ускорила пандемия новой коронавирусной инфекции COVID-19. Например, принят закон, разрешающий дистанционную торговлю лекарственными средствами, хотя законотворческий процесс по данному акту не имел никакого движения с 2017 года после его принятия Государственной Думой РФ в первом чтении[44]. Это, соответственно, сказалось и на особенностях осуществления государственного контроля и надзора в этой области: стало возможным проведение дистанционных контрольных закупок.

Далеко не последнее место в деле информатизации контрольно-надзорной деятельности в сфере обращения лекарств занимает юридический аспект, призванный упорядочить механизм применения информационных технологий, уточнить правовой статус участников таких отношений, обеспечить информационную безопасность правовыми средствами.

Нынешнее законодательство об обращении лекарственных средств включает в себя целый ряд нормативно-правовых актов, в большей или меньшей степени касающихся вопросов урегулирования использования информационных технологий в государственной контрольно-надзорной деятельности. Примечательно, что основной нормативно-правовой акт - Закон об обращении лекарственных средств – не освещает данный во-

[43] Росздравнадзор призовет искусственный интеллект для обработки обращений граждан // Фармацевтический вестник [Электронный ресурс]. URL: https://pharmvestnik.ru/content/news/Roszdravnadzor-prizovet-iskusstvennyi-intellekt-dlya-obrabotki-obrashenii-grajdan.html (дата обращения: 06.11.2021).

[44] Законопроект № 285949-7 // Система обеспечения законодательной деятельности [Электронный ресурс]. URL: http:// http://sozd.duma.gov.ru/bill/285949-7 (дата обращения: 06.11.2021).

прос в принципе. Содержащаяся в нем глава 4, посвященная почти полностью государственному контролю (надзору) в сфере обращения лекарственных средств, не упоминает даже об отдельных аспектах использования информационных технологий в процессе осуществления исследуемой государственной деятельности. Лишь несколько статей из иных глав закона в небольшой степени затрагивают данный вопрос, но только применительно к фармаконадзору (мониторингу эффективности и безопасности лекарственных средств) и системе мониторинга движения лекарственных препаратов. Так, п. 1.4 ст. 30 и ст. 66 Закона об обращении лекарственных средств устанавливают обязанность Росздравнадзора размещать на своем официальном сайте информацию о выявленных в результате фармаконадзора (и, в отдельных случаях, в результате проверок соответствия требованиям к качеству) нежелательных реакциях и побочных действиях лекарств, а также о принятых в связи с этим решениях (о внесении изменений в инструкцию по применению, приостановлении применения, изъятии из обращения или возобновлении применения лекарственного препарата). Что касается федеральной государственной информационной системы мониторинга движения лекарственных препаратов, то в рассматриваемом законе она лишь очерчивается статьей 67, и ее использование в государственной контрольно-надзорной деятельности не раскрывается.

В подзаконных актах правовому регулированию исследуемого вопроса уделено заметно больше внимания. Так, в Постановлении Правительства РФ «О федеральном государственном контроле (надзоре) в сфере обращения лекарственных средств»[45] отмечается уже несколько случаев, когда Росздравнадзор обязан размещать на своем официальном сайте информацию, связанную с осуществлением контрольно-надзорной деятельности. К такой информации относятся:

1) ежегодная программа профилактики рисков причинения вреда (ущерба) охраняемым законом ценностям (п. 18);

2) доклад о правоприменительной практике при осуществлении федерального государственного контроля (надзора) в сфере обращения лекарственных средств (п. 23);

3) информационные письма о результатах контрольно-надзорных мероприятий (п. 75);

[45] Постановление Правительства РФ от 29.06.2021 № 1049 «О федеральном государственном контроле (надзоре) в сфере обращения лекарственных средств» // СЗ РФ. 2021. № 27 (часть III). Ст. 5427.

4) письменные разъяснения по однотипным обращениям контролируемых лиц (п. 34).

Отметим, что в настоящее время все эти пункты в большей степени реализуются. Так, в связи с тем, что первая ежегодная программа профилактики будет применяться лишь в 2022 году, на официальном сайте Росздравнадзора размещен ее проект с информацией о возможности направления предложений в рамках общественного обсуждения данного документа[46]. Что касается докладов о правоприменительной практике, то они уже не первый год размещаются на официальном сайте Росздравнадзора, при чем вместе со специальными сервисами для сбора отзывов и обращений[47]. Информационные письма Росздравнадзора также находятся в открытом доступе на сайте данного органа, их можно найти с использованием электронного сервиса «Поиск писем по контролю качества лекарственных средств» (несколько подробнее данный сервис будет рассмотрен далее). Предоставляется возможность ознакомления и с письменными разъяснениями по однотипным обращениям на официальном сайте Росздравнадзора в разделе «Ответы на часто задаваемые вопросы»[48]. При этом стоит обратить внимание, что данная информация размещается не обособленно в рамках обращения лекарственных средств, а в отношении всей контрольно-надзорной деятельности в сфере здравоохранения.

Однако упомянутое постановление Правительства РФ «О федеральном государственном контроле (надзоре) в сфере обращения лекарственных средств» в рамках регулирования использования информационных технологий ограничивается лишь указанными выше пунктами. Ряд дополнений содержит в себе административный регламент Росздравнадзора, посвященный федеральному государственному надзору в

---

[46] Проект Программы профилактики рисков причинения вреда (ущерба) охраняемым законом ценностям при осуществлении федерального государственного контроля (надзора) качества и безопасности медицинской деятельности в 2022 году // Федеральная служба по надзору в сфере здравоохранения [Электронный ресурс]. URL: https://roszdravnadzor.gov.ru/pages/reform/prevention/program/doc1 (дата обращения: 08.11.2021).

[47] Общественное обсуждение // Федеральная служба по надзору в сфере здравоохранения [Электронный ресурс]. URL: https://roszdravnadzor.gov.ru/discussion/control1/documents/b3751 (дата обращения: 08.11.2021).

[48] О службе // Федеральная служба по надзору в сфере здравоохранения [Электронный ресурс]. URL: https://roszdravnadzor.gov.ru/about/faq (дата обращения: 08.11.2021).

сфере обращения лекарственных средств[49]. В нем увеличивается количество цифровых средств информирования об осуществлении государственного контроля (надзора): это не только официальный сайт Росздравнадзора, но и федеральные государственные информационные системы «Единый портал государственных и муниципальных услуг (функций)» и «Федеральный реестр государственных услуг (функций)», а также единый реестр проверок. Помимо этого, данный регламент закрепляет нетрадиционную форму проведения одного из контрольно-надзорных мероприятий – дистанционную контрольную закупку, которая исключает непосредственный контакт при совершении сделки должностным лицом, так как она осуществляется с использованием сети Интернет.

Вместе с тем в настоящее время в контрольно-надзорной деятельности в сфере обращения лекарственных средств довольно широко применяются различные специализированные государственные информационные системы, которые не только не обозначены в вышеназванных правовых актах, но и в принципе не имеют системного правового регулирования как такового. К примеру, информационная система «Фармаконадзор», функционирующая для сбора сведений о побочных действиях и нежелательных реакциях лекарств, лишь упоминается в приказе Росздравнадзора, утверждающем порядок осуществления фармаконадзора[50], как способ направления сообщений с такой информацией. Иные сведения о данной системе фрагментарно представлены в различных методических рекомендациях и письмах Росздравнадзора[51].

---

[49] Приказ Росздравнадзора от 28.07.2020 № 6720 «Об утверждении Административного регламента Федеральной службы по надзору в сфере здравоохранения по осуществлению федерального государственного надзора в сфере обращения лекарственных средств» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://www.pravo.gov.ru (дата обращения: 20.10.2021).

[50] Приказ Росздравнадзора от 15.02.2017 № 1071 «Об утверждении Порядка осуществления фармаконадзора» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://www.pravo.gov.ru (дата обращения: 22.10.2021).

[51] См., например: Письмо Росздравнадзора от 29.03.2019 № 01и-841/19 «О регистрации пользователей в обновленной базе данных «Фармаконадзор» АИС Росздравнадзора» // Документ опубликован не был. Доступ из СПС «КонсультантПлюс»; Методические рекомендации «Алгоритм взаимодействия участников системы фармаконадзора по выявлению и работе со спонтанными

Другая информационная система – «Мониторинг качества лекарственных средств», предназначенная для сбора и анализа сведений о выявлении несоответствия качества лекарств, – упоминается только в одном письме Росздравнадзора, уведомляющем о порядке получения персонифицированного доступа к ней[52]. При этом в данном письме она именуется подсистемой АИС Росздравнадзора, а на официальном сайте Росздравнадзора – автоматизированной системой внесения сведений[53].

Автоматизированная система внесения сведений «Выборочный контроль» (как она именуется на сайте Росздравнадзора[54]) единожды упоминается в одном из приказов Росздравнадзора, но именно как подсистема АИС Росздравнадзора, доступ к которой предоставляется производителям и импортерам лекарственных средств «для сбора и обработки сведений в электронном виде о сериях, партиях лекарственных средств, поступающих в гражданский оборот в Российской Федерации»[55]. Стоит отметить, что Росздравнадзор всё же предоставляет более подробную информацию о ней, но опять же лишь в одном из своих писем, именуя ее вновь автоматизированной системой, а не подсистемой[56].

Помимо этого, с осуществлением государственной контрольно-надзорной деятельности тесно связаны три поисковых сервиса Росздравнадзора. Первый из них – «Сведения о лекарственных средствах,

---

сообщениями» (утв. Росздравнадзором 22.10.2009) // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

[52] Письмо Росздравнадзора от 18.07.2013 № 16И-779/13 «О предоставлении сведений о качестве лекарственных средств» // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

[53] Автоматизированная система внесения сведений «Мониторинг качества лекарственных средств» // Федеральная служба по надзору в сфере здравоохранения [Электронный ресурс]. URL: https://roszdravnadzor.gov.ru/services/mkls_ais (дата обращения: 22.10.2021).

[54] Автоматизированная система внесения сведений «Выборочный контроль» // Федеральная служба по надзору в сфере здравоохранения [Электронный ресурс]. URL: https://roszdravnadzor.gov.ru/services/vk_ais (дата обращения: 24.10.2021).

[55] Приказ Росздравнадзора от 07.08.2015 № 5539 «Об утверждении Порядка осуществления выборочного контроля качества лекарственных средств для медицинского применения» // Бюллетень нормативных актов федеральных органов исполнительной власти. 2015. № 48.

[56] Письмо Росздравнадзора от 28.11.2019 № 01И-2906/19 «О вводе в гражданский оборот» // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

вводимых в гражданский оборот в Российской Федерации»[57]. Получение контролирующим органом таких сведений является основанием для проведения выборочного контроля качества, и в соответствии с постановлением Правительства РФ[58] и приказом Росздравнадзора[59] они подлежат размещению на официальном сайте данного органа. Более подробного регулирования данного вопроса в действующих нормативно-правовых актах не наблюдается. Второй сервис – «Поиск изъятых из обращения лекарственных средств»[60] – предоставляет информацию об одном из негативных последствий контроля качества, эффективности, безопасности лекарств и законности их оборота при выявлении соответствующих нарушений. Данный сервис упоминается в кратком письме Росздравнадзора и называется в нем поисковым разделом[61]. При этом в одном из приказов Росздравнадзора[62] лаконично закрепляется, какая информация подлежит размещению в данном электронном сервисе (он называется в документе именно так), а также в ещё одном, треть-

[57] Сведения о лекарственных средствах, вводимых в гражданский оборот в Российской Федерации // Федеральная служба по надзору в сфере здравоохранения [Электронный ресурс]. URL: https://roszdravnadzor.gov.ru/services/turnover (дата обращения: 24.10.2021).

[58] Постановление Правительства РФ от 26.11.2019 № 1510 «О порядке ввода в гражданский оборот лекарственных препаратов для медицинского применения» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://www.pravo.gov.ru (дата обращения: 24.10.2021).

[59] Приказ Росздравнадзора от 07.08.2015 № 5539 «Об утверждении Порядка осуществления выборочного контроля качества лекарственных средств для медицинского применения» // Бюллетень нормативных актов федеральных органов исполнительной власти. 2015. № 48.

[60] Поиск изъятых из обращения лекарственных средств // Федеральная служба по надзору в сфере здравоохранения [Электронный ресурс]. URL: https://roszdravnadzor.gov.ru/services/lssearch (дата обращения: 25.10.2021).

[61] Письмо Росздравнадзора от 25.07.2014 № 01И-1085/14 «О поисковом разделе сайта Росздравнадзора» // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

[62] Приказ Росздравнадзора от 04.05.2021 № 3881 «Об утверждении Ведомственной программы профилактики нарушений обязательных требований при осуществлении государственного контроля качества и безопасности медицинской деятельности, федерального государственного надзора в сфере обращения лекарственных средств и государственного контроля за обращением медицинских изделий» // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

ем, – «Поиск писем по контролю качества лекарственных средств»[63]. Он позволяет находить письма Росздравнадзора, связанные с осуществлением им контроля качества лекарств, по различным параметрам, и кроме вышеуказанного не имеет дополнительной регламентации в официальных документах органов власти.

Безусловно, функционируют и некоторые иные информационные системы Росздравнадзора, но они не столь выраженно связаны с контрольно-надзорной деятельностью в сфере обращения лекарственных средств. Вместе с тем нельзя обойти стороной уже упоминаемую нами систему мониторинга движения лекарственных препаратов (далее по тексту – ФГИС МДЛП), которая занимает важнейшее место в ходе осуществления государственного контроля и надзора, хотя и используется не только с этой целью.

ФГИС МДЛП позволяет проследить весь путь лекарств от производителей до потребителя благодаря нанесению специальных идентифицирующих средств, т. е. маркировке. Например, для потребителя это означает, что, «покупая маркированную упаковку таблеток, каждый может быть уверен в ее подлинности, проверив ее через приложение “Честный знак”»[64]. С 1 июля 2020 года внесение сведений о лекарственных средствах во ФГИС МДЛП стало обязательным, однако широкомасштабное использование системы породило немало проблем на фармацевтическом рынке: «Производители после запуска системы вынуждены были в авральном режиме искать способы, как обеспечить непрерывность собственного производства и поставок, так как сбои, ошибки и потеря данных в системе не позволяли им успешно и в привычные сроки проводить все операции, необходимые для передачи товаров дистрибьюторам. В результате где-то увеличились сроки поставок, в других случаях лекарства оказались просто заблокированными на складах»[65]. В настоящее время, «когда вопросы работоспособности системы более или менее урегулированы, а участники рынка - от производителей до аптек и больниц - наработали опыт работы в ней, отрасль

[63] Поиск писем по контролю качества лекарственных средств // Федеральная служба по надзору в сфере здравоохранения [Электронный ресурс]. URL: https://roszdravnadzor.gov.ru/services/qclssearch (дата обращения: 25.10.2021).

[64] Слабое звено // Российская газета [Электронный ресурс]. URL: https://rg.ru/2020/11/29/sistema-markirovki-lekarstv-ne-spravilas-s-nagruzkoj-v-pandemiiu.html (дата обращения: 10.11.2021).

[65] Там же.

вернулась к проработке решений по использованию данных о движении лекарств, которые содержатся в МДЛП»[66].

В концепции создания ФГИС МДЛП закрепляется ее цель – «обеспечение гарантированных поставок потребителям качественных, эффективных и безопасных лекарственных препаратов путем защиты легального оборота от фальсифицированных, контрафактных и недоброкачественных лекарственных препаратов»[67]. При этом в соответствующем поручении Президента РФ отмечается, что разработка и внедрение такой системы необходимы «в целях обеспечения эффективного контроля качества лекарственных препаратов, находящихся в обращении, и борьбы с их фальсификацией»[68]. Помимо этого, данная система позволяет эффективнее применять риск-ориентированный подход в контрольно-надзорной деятельности, так как в ней аккумулируется «информация о нарушениях качества лекарственных препаратов, допущенных поднадзорными Росздравнадзору субъектами обращения лекарственных средств. Таким образом, включение этих сведений в риск-ориентированную модель определенным образом повлияет на рейтинг организаций, участвующих в обороте лекарственных препаратов при проведении контрольно-надзорных мероприятий»[69].

Правовое регулирование относительно ФГИС МДЛП осуществляется на основании Закона об обращении лекарственных средств и нескольких постановлений Правительства РФ[70], в которых подробно ре-

---

[66] Мониторинг движения лекарств в действии // Российская газета [Электронный ресурс]. URL: https://rg.ru/2021/10/14/farmotrasl-zanialas-prorabotkoj-reshenij-monitoringa-dvizheniia-lekarstv.html (дата обращения: 11.11.2021)

[67] Приказ Минздрава России от 30.11.2015 № 866 «Об утверждении Концепции создания Федеральной государственной информационной системы мониторинга движения лекарственных препаратов от производителя до конечного потребителя с использованием маркировки» // Документ опубликован не был. Доступ из СПС «КонсультантПлюс»

[68] Перечень поручений по итогам совещания с членами Правительства // официальный сайт Президента РФ [Электронный ресурс]. URL: http://www.kremlin.ru/acts/assignments/orders/47725 (дата обращения: 26.10.2021).

[69] Поспелов К.Г. Создание и внедрение комплексной модели информационного обеспечения и системы автоматизации контроля (надзора) в сфере здравоохранения // Вестник Росздравнадзора. 2017. № 3. С. 35.

[70] Постановление Правительства РФ от 14.12.2018 № 1556 «Об утверждении Положения о системе мониторинга движения лекарственных препаратов для медицинского применения» // СЗ РФ. 2018. № 53 (часть I). Ст. 8641; № 27 (часть III). Ст. 5445; Постановление Правительства РФ от 14.12.2018 № 1557 «Об осо-

гламентируется порядок ее создания, внедрения, использования и функционирования. Отметим, что упоминается данная система и во многих иных нормативно-правовых актах различного уровня.

Изложенное выше позволяет заключить, что современное правовое регулирование использования цифровых технологий в контрольно-надзорной деятельности, осуществляемой в сфере обращения лекарственных средств, не является системным и носит фрагментарный характер. Об этом свидетельствуют такие факты, как:

1) отсутствие основополагающих правовых норм, посвященных данному вопросу, в базовом Законе об обращении лекарственных средств;

2) обрывочное правовое регулирование использования информационных технологий в подзаконных актах о контрольно-надзорной деятельности в сфере обращения лекарственных средств;

3) правовая неопределенность в функционировании многих государственных информационных систем, применяемых в контрольно-надзорной деятельности Росздравнадзора

В связи с этим представляется необходимым внесение изменений в действующее законодательство в сфере обращения лекарственных средств, а также практику его применения в направлении реализации целостной концепции правового регулирования информатизации контрольно-надзорной деятельности.

Во-первых, это касается содержания Закона об обращении лекарственных средств. В нем, как в базовом правовом акте данной сферы, важно закрепить основы информационного обеспечения контрольно-надзорной деятельности за обращением лекарств путем введения дополнительных норм в главу 4, закрепляющих перечень используемых государственных информационных систем, содержащиеся в них сведения, функциональную направленность таких систем, основы их взаимодействия между собой.

Во-вторых, цифровые технологии оказывают заметное влияние на изменение форм и методов государственного контроля и надзора, которые включают в себя, помимо прочего, и контрольно-надзорные мero-

---

бенностях внедрения системы мониторинга движения лекарственных препаратов для медицинского применения» // СЗ РФ. 2018. № 53 (часть I). Ст. 8642; Постановление Правительства РФ от 14.12.2018 № 1558 «Об утверждении Правил размещения общедоступной информации, содержащейся в системе мониторинга движения лекарственных препаратов для медицинского применения, в информационно-телекоммуникационной сети «Интернет» (в том числе в форме открытых данных)» // СЗ РФ. 2018. № 53 (часть I). Ст. 8643.

приятия. Такие изменения должны быть отражены в законодательстве, и в первую очередь – в Законе об обращении лекарственных средств. Например, появилась дистанционная контрольная закупка лекарственных средств, позволяющая выявить нарушения обязательных требований при реализации лекарств дистанционным способом (в подавляющем большинстве она осуществляется посредством сети Интернет). Такую форму проведения контрольно-надзорной деятельности необходимо закрепить Законом об обращении лекарственных средств (а не только административным регламентом) в соответствующем перечне контрольно-надзорных мероприятий, ведь процедура ее проведения значительно отличается от стандартной контрольной закупки. Более того, согласно сведениям, представленным в Едином реестре проверок, за почти полуторагодовалый срок существования дистанционной реализации лекарственных средств не было произведено ни одной дистанционной контрольной закупки лекарств[71]. Необходимо, чтобы такая форма проведения контрольно-надзорного мероприятия не игнорировалась и применялась уполномоченными должностными лицами (безусловно, при наличии на то правовых оснований) для качественной проверки соблюдения обязательных требований к осуществлению торговли лекарствами дистанционно. Особенно это актуально в период пандемии, когда такой способ приобретения медикаментов пользуется большой популярностью у потребителей.

В-третьих, разрозненные отдельные положения подзаконных актов по поводу использования информационных технологий в контрольно-надзорной деятельности важно дополнить, систематизировать, привести к единому знаменателю. Представляется недостаточным лишь указание в них на обязанность размещения той или информации на официальном сайте Росздравнадзора или в ином электронном источнике. Подзаконные акты о проведении государственного контроля (надзора) в сфере обращения лекарственных средств должны содержать исчерпывающие перечни используемых цифровых технологий и правила их функционирования. Представляется целесообразным отразить данные сведения в Постановлении Правительства РФ «О федеральном государственном контроле (надзоре) в сфере обращения лекарственных средств», а также в Административном регламенте Росздравнадзора по осуществлению федерального государственного надзора в сфере обращения лекарственных средств. При этом ныне существующие информационные

[71] Поиск проверок // ФГИС «Единый реестр проверок» [Электронный ресурс]. URL: https://proverki.gov.ru/portal/public-search (дата обращения: 13.11.2021).

письма и методические рекомендации, не имеющие статуса нормативно-правового акта, не должны подменять собой полноценное правовое регулирование в данной сфере.

Кроме того, проблемным является вопрос о правовой базе используемых в контрольно-надзорной деятельности информационных систем. О большинстве из них только вскользь упоминается в отдельных подзаконных актах, а некоторым в большей или меньшей степени посвящены лишь письма Росздравнадзора. Полноценное правовое регулирование свойственно лишь ФГИС МДЛП. По этой причине целесообразным является разработка и принятие единого правового акта в форме приказа Росздравнадзора, утверждающего положение об АИС Росздравнадзора (как это реализовано в некоторых иных сферах контрольно-надзорной деятельности[72]).

Вместе с этим, как показал анализ правовых документов и иной официальной информации открытого доступа, сложности возникают и в разграничении ряда понятий, используемых относительно цифровизации Росздравнадзора, так как одна и та же информационная система в разных источниках может иметь статус самостоятельной автоматизированной системы, подсистемы иной системы, сервиса или раздела сайта. Для его разрешения необходимо закрепить в положении об АИС Росздравнадзора определения ключевых понятий: автоматизированная информационная система, подсистема автоматизированной информационной системы, электронный сервис. С целью поддержания единообразия в правовом регулировании мы обратились к нормативно-правовым актам, раскрывающим подобные этим понятия, но распространяющим свое действие на иные сферы общественной жизни[73], что позволило нам

---

[72] См., например: Приказ ФНС России от 14.03.2016 № ММВ-7-12/134@ «Об утверждении Положения об автоматизированной информационной системе Федеральной налоговой службы (АИС «Налог-3»)» // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

[73] См.: Постановление Правительства РФ от 01.10.2020 № 1586 «Об утверждении Правил перевозок пассажиров и багажа автомобильным транспортом и городским наземным электрическим транспортом» // СЗ РФ. 2020. № 41. Ст. 6428; Приказ ФНС России от 14.03.2016 № ММВ-7-12/134@ «Об утверждении Положения об автоматизированной информационной системе Федеральной налоговой службы (АИС «Налог-3»)» // Документ опубликован не был. Доступ из СПС «КонсультантПлюс»; Приказ Росстандарта от 08.11.2019 № 1273-ст «Об утверждении национального стандарта Российской Федерации» // Документ опубликован не был. Доступ из СПС «КонсультантПлюс»; Распоряжение Минэкономразвития России от 04.12.2019 № 36Р-Д09 «Об утверждении мето-

сформулировать следующие возможные варианты легальных определений обозначенных понятий:

1. *автоматизированная информационная система (АИС) Росздравнадзора* – совокупность программно-аппаратных средств, образующих единую информационную систему Росздравнадзора, обеспечивающую автоматизацию деятельности Росздравнадзора по всем выполняемым им функциям;

2. *подсистема АИС Росздравнадзора* – составная часть АИС Росздравнадзора, позволяющая автоматизировать отдельные функции Росздравнадзора;

3. *электронный сервис Росздравнадзора* – функциональное решение, размещенное на официальном сайте Росздравнадзора или Едином портале государственных услуг, позволяющее получить государственную услугу, информацию из АИС Росздравнадзора или подать обращение в Росздравнадзор.

Такое разграничение понятий позволяет сделать вывод, что из рассмотренных нами систем к подсистемам АИС Росздравнадзора относятся «Фармаконадзор», «Мониторинг качества лекарственных средств» и «Выборочный контроль», а к электронным сервисам – «Сведения о лекарственных средствах, вводимых в гражданский оборот в Российской Федерации», «Поиск изъятых из обращения лекарственных средств», «Поиск писем по контролю качества лекарственных средств». Причем называть данные подсистемы и электронные сервисы самостоятельными автоматизированными системами представляется некорректным.

Таким образом, правовое регулирование применения цифровых технологий в государственном контроле и надзоре за обращением лекарственных средств должно получить свое выражение в иерархической системе правовых актов. При этом важно, чтобы оно шло в ногу со временем, не оставляя в дальнейшем без регламентации новые проявления цифровизации в данной государственной деятельности.

дики мониторинга качества перевода государственных и муниципальных услуг в электронную форму» // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

§ 3. Контроль и надзор в информационной сфере

В современном мире медиапространство все больше переходит из сферы традиционных для XX века способов коммуникаций и распространения массовой информации, таких как печатные издания, телевидение, радио, к совершенно новому миру – пространству Интернета, то есть полностью цифровому пространству что является крайне серьезным вызовом для государства.

Активное продвижение и распространение Интернета поставило множество вопросов о возможности государства в определенной степени осуществлять контроль над этим информационным пространством, ответ на которые порой не столь и однозначен[74].

В цифровом пространстве осуществляются практически все виды общественных отношений, регулируемые различными отраслями права, что подтверждает необходимость правовой регламентации наиболее значимых из них. Среди прочих, наиболее важных общественных отношений особняком стоят правоотношения, возникающие между государственными органами и гражданами, и в особенности правоотношения, возникающие между органами исполнительной власти и гражданами при осуществлении контрольно-надзорной деятельности[75].

Кроме этого, нельзя оставлять без внимания тот факт, что согласно прогнозам аналитиков, к 2024 году взаимодействие с государством будет осуществляться уже не так, как на современном этапе. Планируется, что к 2024 году все данные о человеке уже будут храниться в специальном реестре, поэтому граждане будут иметь возможность не посещать те или иные организации для оформления услуг, а смогут все делать удаленно. Любую государственную услугу граждане смогут получить в цифровом виде.[76] Активное внедрение современных информационных

---

[74] Перспективные направления правового регулирования использования современных информационных технологий в контрольно-надзорной деятельности органов исполнительной власти: библиотека лучших российских и зарубежных практик: монография / А.В. Мартынов, М.В. Бундин, М.Д. Прилуков, Е.Н. Смирнова, Е.В. Ширеева. – Нижний Новгород: Издательство Нижегородского госуниверситета, 2020. 227 с.

[75] Смирнова Е.Н. Обеспечение соблюдения прав и свобод личности при осуществлении органами исполнительной власти цифрового контроля // NB: Административное право и практика администрирования. 2021. № 3. С. 37–45.

[76] Григорьева Н.С., Гладкова К.С. Государственное управление на пути цифровой трансформации // Вестник Белгородского университета кооперации, экономики и права. 2021. № 1 (86). С. 88–100.

технологий в контрольно-надзорную деятельность предполагает разработку серьезной теоретическо-правовой основы для их применения в государственно-управленческой деятельности[77]. Следует признать правоту ученых, указывающих, что «цифровизация – это здесь и сейчас, и для того, чтобы не оказаться в аутсайдерах, нужны кардинальные перемены сразу в нескольких областях общественного развития: технологиях, методах управления, менталитете»

Справедливо замечание, высказанное в Докладе Уполномоченного по правам человека в Российской Федерации за 2020 г.[78] о том, что важнейшей задачей является достижение баланса интересов личности, общества и государства. Главным образом – баланса между соблюдением права на свободу слова в Интернете и права на доступ к современным информационным технологиям, с одной стороны, и обеспечением безопасности всех и каждого члена общества, защитой их от кибератак, манипуляций общественным сознанием, массового подстрекательства к совершению преступлений – с другой. Необходимо построение новой архитектуры кибербезопасности личности, в том числе защиты домашних сетей и цифрового оборудования, облачного хранения частной информации, поскольку с помощью цифровых технологий возможно масштабное нанесение вреда не только здоровью и финансовому состоянию граждан, но и самой жизни.

Об актуальности расширения механизмов защиты прав граждан в условиях развития информационных технологий свидетельствуют и обращения граждан к Уполномоченному. В 2020 году к Уполномоченному поступило 269 обращений по указанным вопросам, 35 из которых было посвящено вопросам обеспечения безопасности в сети интернет и защите персональных данных[79].

Информационная сфера, является, пожалуй, одной из самых быстроменяющихся подконтрольных сфер, рассматриваемых в настоящей главе, однако важно отметить, что кроме динамичности подконтроль-

[77] Мартынов А.В., Бундин М.В. О правовых принципах применения искусственного интеллекта при осуществлении органами исполнительной власти контрольно-надзорной деятельности // Журнал российского права. 2020. № 10. С. 59–75.

[78] Официальный доклад о деятельности Уполномоченного по правам человека в Российской Федерации за 2020 г. // Официальный сайт Уполномоченного по правам человека в Российской Федерации [Электронный ресурс]. URL: https://ombudsmanrf.org/upload/files/docs/lib/Doc4.pdf (дата обращения: 05.12.2021).

[79] Там же.

ной среды необходимо отметить и динамичность государственного контроля. Справедливо замечание С.М. Зубарева, о том, что «с развитием новых информационных технологий в работе контролирующих органов расширились возможности оперативного использования разнообразия методов контроля и получения результатов, что, несомненно, окажет влияние на качество самого контроля, устранит поверхностный характер его проведения и будет способствовать улучшению деятельности государственных служащих и органов исполнительной власти»[80].

Формы и методы управления воплощают ключевые признаки, характеризующие особенности осуществления любого вида государственно-управленческой деятельности. Не является исключением в этом смысле и деятельность по осуществлению государственного контроля и надзора. И если форма управления определяет внешнее юридическое содержание контрольно-надзорной деятельности – форму контроля, то методы управления характеризуют сущность и содержание способа административно-правового воздействия, которое осуществляется в результате контрольно-надзорной деятельности – методы государственного контроля и надзора[81].

Ключевым органом в системе органов исполнительной власти, выполняющим функцию государственного контроля (надзора) в информационной сфере в РФ выступает Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее-Роскомнадзор), согласно Постановлению Правительства РФ от 16.03.2009 № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций»[82] Роскомнадзор является федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, в том числе электронных, и массовых коммуникаций, информационных технологий и связи, функции по контролю и надзору за соответствием обработки персональных данных требованиям законо-

[80] Зубарев С.М. Система контроля в сфере государственного управления: монография. М.: Норма, 2019. С. 73.

[81] Мартынов А.В. Развитие новых форм и методов государственного контроля и надзора в условиях цифровой экономики // Законы России: опыт, анализ, практика. 2021. № 11. С. 10–27.

[82] Постановление Правительства РФ от 16.03.2009 № 228 (ред. от 17.08.2021) «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» // СЗ РФ. 2009. № 12. Ст. 1431.

дательства Российской Федерации в области персональных данных, а также функции по организации деятельности радиочастотной службы.

Рассматривая непосредственного вопрос о реализации концепции правового регулирования использования цифровых технологий в сфере государственного контроля (надзора) в сфере защиты персональных данных необходимо обратиться к Положению о федеральном государственном контроле (надзоре) за обработкой персональных данных[83], которое в качестве форм осуществления контрольно-надзорной деятельности выделяет: профилактические и контрольные мероприятия.

В соответствии с п.13 Положением о федеральном государственном контроле (надзоре) за обработкой персональных данных профилактические мероприятия проводятся в форме информирования; обобщения правоприменительной практики; объявления предостережения; консультирования; профилактического визита.

При проведении любой из форм профилактического мероприятия возможно использование цифровых технологий, обратим внимание на каждый из видов профилактического мероприятия поподробнее и проанализируем каким образом возможно использование цифровых технологий.

Информирование. Донесение информации Роскомнадзором для поднадзорных субъектов возможно различными способами, такими как публикации руководств, проведения семинаров, толкования спорных вопросов в СМИ и пр.

Руководства по соблюдению действующих обязательных требований могут быть представлены в виде брошюр, схем, инфографического материала в доступной форме и опубликованы на официальном сайте контрольно-надзорного органа или его территориального органа в сети «Интернет»;

Еще одним способом информирования является организация консультаций с подконтрольными субъектами по вопросам обязательных требований. Консультирование индивидуальных предпринимателей и юридических лиц возможно в форме семинаров, инструктажей, тематических конференций, заседаний рабочих групп, «горячих линий» с подконтрольными субъектами как в режиме реального времени, так и онлайн-режиме;

---

[83] Постановление Правительства РФ от 29.06.2021 № 1046 «О федеральном государственном контроле (надзоре) за обработкой персональных данных» (вместе с «Положением о федеральном государственном контроле (надзоре) за обработкой персональных данных») // СЗ РФ. 2021. № 27 (часть III). Ст. 5424.

Третьей формой информирования выступает информирование посредством печатных изданий, телевидения, радио, социальных сетей, направленное на охват широкого круга подконтрольных субъектов с целью формирования заинтересованности юридических лиц и индивидуальных предпринимателей в соблюдении обязательных требований.

Роскомнадзор выступает активным пользователем социальны сетей, имеет свои официальные страницы в социальной сети Вконтакте[84] и телеграмме[85], где помимо размещения новостных событий ведомства также оказывает консультационную помощь поднадзорным субъектам.

Но отдельно стоит отметить, что для информирования поднадзорных субъектов было логичным использовать возможности искусственного интеллекта. Главным преимуществом использования современных цифровых технологии, в том числе искусственного интеллекта, как отмечает Минбалеев А.В., можно обозначить возможность оперативно информировать о необходимости подготовки той или иной информации для размещения на сайте. Используя решения на базе искусственного интеллекта, веб-сайт можно еще лучше адаптировать под потребности каждого отдельного посетителя. Такие технологии позволяют обеспечить и информационную открытость[86].

К сожалению, на сегодняшний день Роскомнадзор не использует возможности искусственного интеллекта при информировании поднадзорных субъектов, используя традиционные формы взаимодействия, лишь в небольшой степени использования возможности цифровых технологий.

Следующей формой осуществления профилактических мероприятий является *обобщение правоприменительной практики.* Обобщение правоприменительной практики контрольно-надзорным органом должно проводиться не реже одного раза в год. По результатам обобщений проводятся публичные слушания для подконтрольных субъектов с обсуждением полученных результатов.

При проведении указанного профилактического мероприятия контрольно-надзорный орган должен учитывать положения, содержащиеся

---

[84] Официальная страница в социальной сети «Вконтакте» [Электронный ресурс] // URL: https://vk.com/rkn (дата обращения: 05.12.2021).

[85] Официальный канал в «Телеграм» [Электронный ресурс] // URL: https://t.me/rkn_tg (дата обращения: 05.12.2021).

[86] Минбалеев А.В. Проблемы правового регулирования использования цифровых технологий в деятельности саморегулируемых организаций // Гражданское право. 2020. № 4. С. 31–34.

в «Методических рекомендациях по организации и проведению публичных обсуждений результатов правоприменительной практики, руководств по соблюдению обязательных требований органа государственного контроля (надзора)»[87].

Однако, стоит отметить, что общей тенденцией в работе контрольно-надзорных органов является отсутствие обратной связь с подконтрольными субъектами несмотря на то, что курс на выстраивание диалога обозначен в посланиях Президента и обозначен в паспорте «Реформы контрольно-надзорной деятельности», на необходимость получения обратной связи указывают и Методические рекомендации, в пункте 17, указанных Методических рекомендаций закреплено положение, что в целях подведения итогов проведения публичных обсуждений, определения их эффективности и полезности на официальном сайте органа государственного контроля (надзора) создается сервис для сбора обратной связи посредством размещения специальной анкеты либо обеспечивается заполнение участниками публичных обсуждений специальных анкет в бумажном виде непосредственно после завершения мероприятия.

Обобщенные итоги рассмотрения специальных анкет размещаются на официальном сайте органа государственного контроля (надзора) в течение двух недель после завершения публичных обсуждений.

Однако, на официальном сайте Роскомнадзора размещена только информация о том, что в случае наличия предложений возможно обращение через специальную форму, размещенную по адресу: https: //rkn.gov.ru/treatments/ask-question/, иной анализ анкет отсутствует.

При этом, стоит отметить, что использование технологии «блокчеин» при анализе анкет могло бы способствовать решению ряда государственных функций.

Автоматизация процесса сбора и анализа статистической информации, в том числе социальной, проявляется в связи с внедрением технологий обработки «больших данных», получения информации из социальных сетей, обмена данными между государственными органами в автоматическом

[87] Методические рекомендации по организации и проведению публичных обсуждений результатов правоприменительной практики, руководств по соблюдению обязательных требований органа государственного контроля (надзора) (приложение к протоколу заседания проектного комитета по основному направлению стратегического развития «Реформа контрольной и надзорной деятельности» от 21.02.2017 № 13(2)) // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

порядке, использования технологий предиктивной аналитики, которые позволят уже на этапе сбора информации предсказывать возможные варианты организации государственного управления. Таким образом, происходит взаимосвязанная трансформация такой функции государственного управления, как прогнозирование, ее автоматизация[88].

Следующей формой реализации профилактического направления деятельности Роскомнадзора является *объявление предостережения.* Предостережение – акт реагирования органов публичной власти, осуществляющих правообеспечительные функции, прежде всего, контрольно-надзорные, направляемый при наличии специальных юридико-фактических оснований[89].

Предостережение – это ненормативный правовой акт государственного органа, адресованный должностному лицу хозяйствующего субъекта (или органа государственной власти в соответствующих случаях), содержащий информацию о недопустимости совершения действий, которые могут привести к нарушению законодательства[90].

Правовую основу указанного профилактического мероприятия составляет Постановление Правительства РФ от 10 февраля 2017 г. № 166 «Об утверждении Правил составления и направления предостережения о недопустимости нарушения обязательных требований, подачи юридическим лицом, индивидуальным предпринимателем возражений на такое предостережение и их рассмотрения, уведомления об исполнении такого предостережения»[91].

Для вынесения предостережения необходимо соблюдение ряда условий, а именно:

1. Подконтрольный субъект ранее не привлекался к ответственности за нарушение соответствующих обязательных требований.

---

[88] Юридическая концепция роботизации: монография / Н.В. Антонова, С.Б. Бальхаева, Ж.А. Гаунова и др.; отв. ред. Ю.А. Тихомиров, С.Б. Нанба. М.: Проспект, 2019. 240 с.

[89] Панченко В.Ю., Макарчук И.Ю. Предостережение как правовое средство // Законность. 2013. № 6 (944).

[90] Хохлов Е.С. Меры предупредительного воздействия на хозяйствующих субъектов, занимающих доминирующее положение // Закон. 2017. № 4. С. 132–140.

[91] Постановление Правительства РФ от 10 февраля 2017 г. № 166 (ред. от 29.03.2019) «Об утверждении Правил составления и направления предостережения о недопустимости нарушения обязательных требований, подачи юридическим лицом, индивидуальным предпринимателем возражений на такое предостережение и их рассмотрения, уведомления об исполнении такого предостережения» // СЗ РФ. 2017. № 8. Ст. 1239.

2. Орган государственного контроля (надзора) располагает сведениями о том, что обязательные требования могут быть нарушены или уже нарушены.

3. Нарушение обязательных требований не причинило вред жизни, здоровью граждан, вред животным, растениям, окружающей среде, объектам культурного наследия, безопасности государства и не создало угрозу такого вреда, а также не привело к чрезвычайной ситуации и угрозе возникновения чрезвычайной ситуации;

Предельный срок для составления и направления предостережения составляет 30 дней с момента поступления в контрольно-надзорный орган информации о потенциальном или уже случившемся факте нарушения обязательных требований.

После вынесения предостережение подконтрольный субъект имеет право направить возражения в орган, вынесший предостережение. В течение 20 рабочих дней контрольно-надзорный орган должен предоставить ответ на возражения[92].

Если в отношении составленного предостережения у подконтрольного субъекта не возникает возражений, то в течение 60 дней он обязан уведомить контрольно-надзорный орган об исполнении предостережения.

На сегодняшний день предостережения выносятся как в простой письменной форме, так и по средствам направления с помощью электронных ресурсов.

Следующим профилактическим мероприятием, которое также было закреплено в Стандарте комплексной профилактики нарушений обязательных требований и в Стандарте комплексной профилактики рисков причинения вреда охраняемым законом ценностям выступает – *консультирование,* закрепленное в ст.50 Федеральный закон от 31.07.2020 № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации».

Консультирование является схожим профилактическим мероприятием с другим видом профилактического мероприятия – информированием, также носит разъяснительный и справочный характер, но в отличие от него осуществляется в результате обращения контролируемого лица. При этом, важно отметить, что законом предусмотрены различные каналы для проведения консультирования, такие как телефон, видео-конференц-связь, на личном или даже в ходе проведения иного профилактического мероприятия, или контрольного (надзорного) мероприятия.

[92] Там же.

Для проведения данного профилактического мероприятия необходимо активное волеизъявление от контролируемого лица, при этом закон обязывает предоставлять информацию заявителю в письменной форме только в случае, если такая обязанность предусмотрена положением о виде контроля.

Однако законодатель не решает возможности хозяйствующие субъекты обратиться с запросом в контрольно-надзорный орган с запросом о предоставлении письменного ответа, в этом случае ответ должен быть подготовлен в соответствии с требованиями, в сроки, установленные Федеральным законом от 2 мая 2006 года № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации».

Контрольно-надзорный орган ведет учет поступивших к нему обращений, также законом предусмотрена возможность опубликования ответов по однотипным обращениям посредством размещения на официальном сайте контрольного (надзорного) органа в сети «Интернет».

При проведении консультирования поднадзорных субъектов, так же как и при информировании было бы полезно использование технологий искусственного интеллекта.

Следующим профилактическим мероприятием является *профилактический визит.* Профилактический визит осуществляется посредством проведения профилактической беседы с помощью использования видео-конференц-связи. В ходе проведения профилактического визита контролируемое лицо информируется об обязательных требованиях, предъявляемых к его деятельности либо к принадлежащим ему объектам контроля, их соответствии критериям риска, основаниях и о рекомендуемых способах снижения категории риска, а также о видах, содержании и об интенсивности контрольных (надзорных) мероприятий, проводимых в отношении объекта контроля исходя из его отнесения к соответствующей категории риска.

Использование видео-конференцсвязи выступает ярким примером использования цифровых технологий. Профилактический визит является, пожалуй, одним из самых прогрессивных профилактических мероприятий в части использования современных технологий.

Контрольные (надзорные) мероприятия согласно Положению о федеральном государственном контроле (надзоре) за обработкой персональных данных проводятся в форме инспекционного визита, документарной проверки и выездной проверки. Указанные мероприятия в отличии от профилактических не могут похвастаться высоким уровнем цифровизации.

Рассматривая вопрос контроля и надзора в информационной сфере, отдельно хотелось бы обратить внимание на электронные сервисы, внедряемые Роскомнадзором за последние годы.

Так, в конце декабря 2017 г. Роскомнадзор запустил Портал операторов связи. Сервис позволил значительно упростить процедуры подачи заявочных материалов и получения результатов оказания услуг, появилась возможность подавать одно заявление на получение нескольких видов услуг, направлять документы в электронном виде и отслеживать этапы их прохождения в онлайн-режиме[93].

7 августа 2018 года Роскомнадзор открыл сервис для самопроверки операторами связи исполнения лицензионных и обязательных требований.

В рамках профилактической работы Роскомнадзор открыл сервис для самопроверки исполнения лицензионных и обязательных требований в сфере связи. Сервис доступен на портале ведомства в личном кабинете оператора связи (https://service.rkn.gov.ru/)[94].

Основная задача сервиса – помочь оператору самостоятельно определить, нарушены ли им нормы и требования законодательства с тем, чтобы устранить нарушения до проведения проверки надзорным органом. Самопроверка проводится путем заполнения проверочных листов, которые содержат перечень вопросов, касающихся выполнения конкретных норм и обязательных требований.

По итогам самопроверки сервис информирует оператора, является ли он законопослушным или же в случае проверки Роскомнадзором ему будет выдано предписание и составлен протокол об административном правонарушении.

По желанию оператора информация о проведении добровольной самопроверки может быть доведена до Роскомнадзора. Данный факт может быть учтен при планировании проверок на следующий год.

Согласно информации с официального сайта Роскомнадзора[95] с 1 июля 2021 года Роскомнадзор запустил *сервис* для операторов пер-

---

[93] Савченко Е.А. Некоторые аспекты соблюдения законности субъектами разрешительной и контрольно-надзорной деятельности в условиях модернизации социально-экономического развития // Журнал российского права. 2019. № 7. С. 104–114.

[94] Официальный сайт федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций [Электронный ресурс] // URL: https://rkn.gov.ru/news/rsoc/news60240.htm (дата обращения: 05.12.2021).

[95] Официальный сайт федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций [Электронный ресурс] // URL: https://rkn.gov.ru/news/rsoc/news73724.htm (дата обращения: 05.12.2021).

сональных данных, который позволил им сформировать шаблон формы согласия на обработку персональных данных, разрешенных субъектом для распространения.

Необходимость создания такого сервиса обусловлена тем, что с 1 сентября 2021 года для операторов вступают в силу обязательные требования к форме согласия на обработку персональных данных, разрешенных для распространения. Разработанный Роскомнадзором сервис позволит операторам сформировать шаблон согласия, который будет соответствовать требованиям, а также учитывать специфику деятельности конкретного оператора.

Созданию такого сервиса предшествовал анализ правоприменительной практики и обращений операторов по оформлению согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

В сентябре 2021 года Роскомнадзор открыл Центр правовой помощи гражданам в цифровой среде[96]. Специалисты названного центра должны оказывать консультационную помощь по вопросам защиты персональных данных, а в случае выявления нарушений в ходе рассмотрения заявлений будут оказывать юридическое консультирование, готовить документы в государственные органы, формировать исковое заявления, представлять интересы потерпевшего в судах.

Однако в цифровой сфере, кроме защиты персональных данных, существует еще один немаловажный вопрос, который также «курирует» Роскомнадзор, это вопрос контроля деятельности средств массовой информации.

В своей деятельности, осуществляя функцию по государственному контролю (надзору) за СМИ, Роскомнадзор обязан руководствоваться Положением о федеральном государственном контроле (надзоре) за соблюдением законодательства Российской Федерации о средствах массовой информации, утвержденном Правительством РФ[97].

Формы профилактической деятельности совпадают с формами, представленными в Положении о защите персональных данных и выражаются в информировании; обобщении правоприменительной прак-

[96] РИА Новости [Электронный ресурс] // URL: https://ria.ru/20210913/tsentr-1749824185.html (дата обращения: 05.12.2021).

[97] Постановление Правительства РФ от 25.06.2021 № 1020 «Об утверждении Положения о федеральном государственном контроле (надзоре) за соблюдением законодательства Российской Федерации о средствах массовой информации» // СЗ РФ. 2021. № 28 (часть I). Ст. 5503.

тики; объявлении предостережения; консультировании, профилактическом визите, так как данные формы были описаны ранее не будем останавливаться на них подробно.

Контрольно-надзорные мероприятия согласно Положению о федеральном государственном контроле (надзоре) за соблюдением законодательства Российской Федерации о средствах массовой информации, утвержденном Правительством РФ, проводятся в форме документарной проверки и выездной проверки.

Однако, стоит отметить, что целесообразным было бы внести изменения в Положение о федеральном государственном контроле (надзоре) за соблюдением законодательства Российской Федерации о средствах массовой информации[98], добавив такую форму контрольно-надзорного мероприятия как мониторинг цифрового пространства. Данная форма контрольно-надзорной деятельности способствовала бы защите прав граждан в цифровом пространстве. Как уже было сказано ранее, одной из угроз, связанной с активным использованием цифрового пространства является возможность быстрого распространения недостоверной информации. Так, можно обратиться к международным данным и обнаружить следующее.

Согласно последнему опросу «Евробарометра» (~26 тыс. респондентов), общество чувствует, что в ЕС циркулирует много ложной информации, что, по мнению 83% участников, представляет серьезную опасность для демократии. Опрос также подчеркивает важность обеспечения «качества» средств массовой информации: участники считают, что наиболее надежным источником информации являются традиционные средства массовой информации (радио – 70%, телевидение – 66%, печатные средства массовой информации – 63%). Онлайн-новостным сервисам и социальным сетям доверяют лишь соответственно 26% и 27% участников[99].

В США наблюдается скорее обратная ситуация. В ходе исследований выяснено, что достаточно большой процент американцев узнают новости из онлайн-ресурсов (~ 93%), при этом 36% назвали источником веб-сайт; 35% – социальные сети (что обычно означает сообщение от новостной организации, но может быть комментарием друга); 20% вспомнили поисковую систему; 15% – электронную почту, текст или

[98] Там же.

[99] Fake News and Disinformation Online 2018 // European Comission [Электронный ресурс]. URL: https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/fflas/surveyky/2183 (дата обращения: 05.12.2021).

предупреждение новостной организации; 9% – другой источник; 7% назвали электронную почту или текст, полученный от члена семьи.[100]

Как отмечается учеными[101], вопрос о распространении информации становится «глобальным трендом». В странах Запада активно выделяют деньги и создают целые правительственные организации по борьбе с «фейками». Сообщения, которые пользователи социальной сети сочтут «фейками», будут не только проходить автоматизированную проверку, но и проверяться независимыми фактчекерами[102].

В Российской Федерации учеными также отмечается существенное увеличение «фейковых новостей» Н.Р. Красовская, А.А. Гуляев и Г.Н. Юлина, например, отмечают, что за последние 10 лет фейковые новости, как пожар, охватили различные интернет-ресурсы, в частности социальные сети. В результате интернет-пользователи тысячами ставят лайки лживым сообщениям и постам. На смену простому «зомбоящику» пришел более сложный и изощренный «зомбоэкран» с клавиатурой.

По их мнению, все фейковые новости по степени недостоверности информации могут быть разделены на три группы. В первую группу входят новости, ложные от начала и до конца. Во вторую группу фейковых новостей входят новости, являющиеся частично ложными. На фоне достоверных событий, представленных выборочно, появляется откровенный фейк. В третью группу фейковых новостей входят новости, искажающие суть реального события. Это могут быть фразы, цитаты, выдернутые из контекста или изложенные не целиком, а выборочно[103].

Внедрение такой формы осуществления контрольно-надзорной деятельности как мониторинг (наблюдение за соблюдением обязательных требований) цифрового пространства поможет повысить эффективность контрольно-надзорной деятельности, а также будет действенным механизмом по реализации защиты прав граждан.

---

[100] West D.M. How to combat fake news and disinformation // Brookings. 18 December 2017 [Электронный ресурс]. URL: https://www.brookings.edu/research/how-to-combat-fake-news-and-disinformation/ (дата обращения: 05.12.2021).

[101] Дорофеева В.В. Фейковые новости в современном медиапространстве // Вопросы теории и практики журналистики. 2019. Т. 8. № 4. С. 774-786.

[102] Dwoskin E. Twitter is looking for ways to let users flag fake news, offensive content // The Washington Post. 2017. 29 June.

[103] Красовская Н.Р., Гуляев А.А., Юлина Г.Н. Фейковые новости как феномен современности // Власть. 2019. № 4. С. 79-82.

Согласно ч. 1 ст. 74 Федерального закона от 31.07.2020 № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации»[104] под наблюдением за соблюдением обязательных требований (мониторингом безопасности) понимается сбор, анализ данных об объектах контроля, имеющихся у контрольного (надзорного) органа, в том числе данных, которые поступают в ходе межведомственного информационного взаимодействия, предоставляются контролируемыми лицами в рамках исполнения обязательных требований, а также данных, содержащихся в государственных и муниципальных информационных системах, данных из сети «Интернет», иных общедоступных данных, а также данных полученных с использованием работающих в автоматическом режиме технических средств фиксации правонарушений, имеющих функции фото – и киносъемки, видеозаписи.

Мониторинг имеет множество значений в зависимости от конкретного вида деятельности. Согласно Толковому словарю Л.П. Крысина мониторинг (от англ. monitor – контролировать, проверять) – это: 1) наблюдение, оценка и прогноз состояния окружающей среды в связи с хозяйственной деятельностью человека; 2) систематическое наблюдение за каким-нибудь процессом с целью фиксировать соответствие (или несоответствие) результатов этого процесса первоначальным предположениям[105].

Постоянный цифровой мониторинг способен выявлять совершение нежелательных действий в цифровом пространстве поднадзорными субъектами (такие, как например, размещение недостоверной информации) и обеспечивать своевременную реакцию со стороны контрольно-надзорного органа. Стоит отметить, что данный механизм не является новым и широко используется в ряде стран, приведем некоторые примеры.

Одним из удачных примеров можно назвать деятельность – Национальной комиссии по информатике и гражданским свободам. Национальная комиссия по информатике и свободам (далее – Комиссия) – это Французский контрольно-надзорный орган, один из самых авторитетных европейских органов по защите прав субъектов персональных данных.

---

[104] Федеральный закон от 31.07.2020 № 248-ФЗ (ред. от 06.12.2021) «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» // Российская газета. 2020. № 171.

[105] Крысин Л.П. Толковый словарь иноязычных слов. М.: Эксмо, 2006. С. 500.

Согласно статье 11 Закона об информатике и свободах Комиссия осуществляет 4 основных группы полномочий.

1. Информирование физических лиц и операторов персональных данных об их правах и обязанностях.

2. Осуществлять контроль за соблюдением положений Закона об информатике и свободах при обработке персональных данных (выдача разрешений на обработку отдельных категорий персональных данных (биометрических, с использованием государственных идентификаторов и т.д.)); издание нормативных актов; рассмотрение претензий, обращений, жалоб на обработку персональных данных; выдача заключений по запросам государственных органов, судов; информирование прокурора Республики о выявленных нарушениях с целью уголовного преследования.

3. Выдача по запросам профессиональных объединений и ассоциаций юридических лиц заключений о соответствии их процедур, правил, кодексов поведения положениям Закона об информатике и свободам.

4. Информирует общественные и государственные институты о появлении новых информационных технологий обработки данных и производит оценку их внедрения с точки зрения опасности правам и свободам личности (Комиссия дает рекомендательные заключения по проектам законов и актов, регулирующих вопросы обработки данных, предлагает принятие законодательных и нормативных актов; по указанию Премьер-министра представляет страну в международных организациях и участвует в выработке решений на международном уровне, по вопросам защиты персональных данных; проводит изучение этических и социальных аспектов эволюции информационных технологий; изучает и дает рекомендации по вопросам использования и применения технологий защиты информации при обработке персональных данных)[106].

Комиссия на постоянной основе осуществляет наблюдение за соблюдением требований законодательства о персональных данных в различных отраслях экономики (здравоохранение, банковская деятельность и т.д.), используя для этого различные цифровые технологии, такие как искусственный интеллект, блок-чейн технологии.

---

[106] Бундин М.В. Национальная комиссия по информатике и свободам как орган по защите прав субъектов персональных данных во Франции // Актуальные вопросы контроля и надзора в социально значимых сферах деятельности общества и государства: материалы IV Всероссийской научно-практической конференции. Нижний Новгород: Изд-во Нижегородского госуниверситета, 2018. С. 279–286.

Комиссия ежегодно публикует доклады о своей деятельности, и как отмечается экспертами за последние несколько лет количественные показатели деятельности Комиссии достаточно резко возросли, причем в большей степени в части деятельности по информированию, разъяснению и пропаганде знаний в области персональных данных, а также мониторингу[107].

Еще одним удачным примером постоянного цифрового мониторинга с помощью технологий искусственного интеллекта является опыт Китая. В КНР с 2003 г. претворяется в жизнь крупномасштабный проект под названием «Золотой щит» (The Golden Shield Project) означающий целую систему фильтрации содержимого китайского Интернета. Проект представляет собой систему серверов на интернет-канале между провайдерами и международными сетями передачи информации, которая фильтрует информацию по определенным ключевым словам.

Файрволы применяются провайдерами для защиты от вирусов и хакеров, но используются и для блокирования доступа к определенным сайтам. В их основу лег созданный еще в 1994 г. Министерством общественной безопасности КНР Государственный информационный центр по преступлениям. Специалисты, отвечающие за работу «Золотого щита», при помощи искусственного интеллекта осуществляют непрерывный мониторинг деятельности интернет-пользователей и пресекают распространение незаконной информации в китайском сегменте Интернета[108].

Подводя итоги, стоит сказать, что внедрение цифровых технологий в контрольно-надзорную деятельность позволяет развивать такие формы контрольно-надзорной деятельности как регулярное и систематическое наблюдение - мониторинг и анализ состояния подконтрольной сферы и ее объектов без непосредственного взаимодействия с объектами контроля. Предупреждение должно быть главной целью контрольно-надзорной деятельности, карательная же функция контрольно- надзорной деятельности должна служить крайней мерой, используемой только в отношении злостных нарушителей, не желающих выстраивать диалог с государством, выгодный для обеих сторон. Внедрение цифровых тех-

---

[107] CNIL Rapport d'activité 2017 [Электронный ресурс] // URL: https://www.cnil.fr/sites/default/files/atoms/files/cnil-38e_rapport_annuel_2017.pdf (дата обращения: 02.12.2021).

[108] Трощинский П.В. Цифровой Китай до и в период коронавируса: особенности нормативно-правового регулирования // Право и цифровая экономика. 2021. № 1. С. 44–58.

нологий в контрольно-надзорную деятельность будет способствовать исчезновению архаичных принципов работы государственных органов, которые формировали настороженное отношение подконтрольных субъектов и мешали организации новой модели взаимодействия.

Цифровизация контрольно-надзорной деятельности безусловно приведет к сокращению числа государственных служащих контрольно-надзорных органов исполнительной власти, осуществляющих контрольно-надзорные функции в информационной сфере. С одной стороны, сокращение числа государственных служащих можно назвать недостатком цифровизации, так как это способствует возникновению социальной напряженности и увеличению уровню безработицы. Факт сокращения числа чиновников в результате цифровизации государственного управления известен и очевиден уже давно, например, в 2017 году А.Л. Кудрин на форуме Calvert forum Siberia предупредил, что автоматизация в ближайшие пять лет сократит количество чиновников на треть: «Цифровизация и переход на другие модели управления, профилактику любых нарушений существенно сократят потребность в чиновниках, и решения будут приниматься автоматически»[109]. Но с точки зрения нагрузки на финансирование контрольно-надзорной деятельности, в долгосрочной перспективе, цифровизация обеспечит значительную экономию бюджетных средств. Высвободившиеся средства могут быть потрачены либо на дальнейшую модернизацию государственного управления, либо смогут быть потрачены на иные статьи расходов государства, но в любом случае сокращение численности государственных служащих контрольно-надзорных органов на треть приведет к колоссальной экономии.

Кроме того, активное использование цифровых технологий в контрольно-надзорной деятельности способствует упрощению взаимодействия между органами федеральной исполнительной власти, осуществляющими контрольно-надзорную деятельность в информационной сфере, а также в перспективе могут быть использованы и для международного сотрудничества в указанной сфере.

Внедрение цифровых технологий в контрольно-надзорную деятельность позволяет создать условия не только для оперативного выявления нарушений, но и для развития такой формы контроля, как регулярное и систематическое наблюдение – мониторинг и анализ состояния подкон-

[109] Кудрин помечтал о роботахналоговиках // Новостной сайт «Lenta.ru» [Электронный ресурс]. URL: https://lenta.ru/news/ 2017/11/10/kudrin (дата обращения: 25.09.2021).

трольной сферы и ее объектов без непосредственного взаимодействия с объектами контроля. То есть контрольно-надзорные органы могут предугадывать и ликвидировать непосредственно возникающие угрозы и риски, предупреждая возникновение правонарушений и дальнейшего ущерба для подконтрольной среды, что выступает несомненным плюсом для всех участников контрольно-надзорной деятельности в информационной сфере, как для подконтрольных субъектов, так и для контроллеров.

§ 4. Контроль и надзор в сфере промышленности

Цифровизация контрольно-надзорной деятельности коснулась многих отраслей и сфер контроля и надзора в том числе и в области промышленной безопасности. При этом сфера промышленности в определённой степени подвергается серьезным и качественным изменениям и в том числе под воздействием новых информационных технологий «интернет вещей», сенсорика, искусственный интеллект, 3D-моделирование, нейросети, облачные и туманные вычисления, виртуальную и дополненную реальность, машинное обучение, компьютерную имитацию на основе цифровых двойников, интеллектуальные датчики, роботизацию производства, аддитивные технологии.

Причем сфера промышленности, имеющая ориентир на адаптацию новых и передовых/прорывных технологических решений, в первую очередь подвержена кардинальным преобразованиям для сохранения технологического превосходства и лидирующих позиций на рынке, в противном случае такие проекты обречены изначально на неудачу в условиях глобального рынка и конкуренции. Сейчас часто такие вызовы для современной промышленности принято обозначать общим термином индустрия 4.0[110] как обозначение четвертого этапа промышленной революции.

В таких условиях у предприятий у современных промышленных предприятий кардинально усложнились условия ведения хозяйственно-экономической деятельности. Индустрия 4.0 постепенно захватывает весь мир – США создали некоммерческий консорциум Industrial Internet

[110] Юдина М.А. Индустрия 4.0: конкуренция за актуальность // Государственное управление. Электронный вестник. 2020. № 80 [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/industriya-4-0-konkurentsiya-za-aktualnost (дата обращения: 20.12.2021).

в 2014 году, которым руководят лидеры промышленности General Electric, AT&T, IBM и Intel[111]. Реалии современного рынка вынуждают компании чтобы оставаться конкурентоспособным применять в деятельности предприятия технологии, повышающие эффективность производства. Современные данные свидетельствуют, что информационные технологии значительно повышают авторитет компании и ее успешность на рынке[112].

В настоящий момент принято говорить о распространении технологических решений, объединенных общей формулой PLM (product lifecycle management), как правило – это целые информационные комплексы, которые позволяют эффективно управлять и контролировать сложные производственные процессы на всех стадиях. В такие системы часто интегрированы самые передовые цифровые технологические решения: искусственный интеллект, интернет вещей, анализ больших данных, 3-D моделирование, виртуальная и дополненная реальность и др. В перспективе создается модель или цифровое описание реальных технологических процессов[113].

В таких условиях требуется существенным образом переосмыслить традиционную практику контрольно-надзорной деятельности в сфере промышленности и обеспечить ее соответствующую оснащенность и эффективность. Современные технологии продемонстрировали свою эффективность в контроле и мониторинге сложных технологических процессов и управлении крупными промышленными объектами и даже целыми городами.

Среди множества технологических решений, используемых для контрольно-надзорной деятельности за промышленными объектами, уже ранее рассмотренными авторами в рамках настоящего исследования (системы автоматического контроля на основе информации, собираемой с помощью сенсоров и датчиков, интернета вещей, дистанционного

---

[111] AT&T, Cisco, GE, IBM и Intel образуют промышленный интернет-консорциум для улучшения интеграции физического и цифрового миров [Электронный ресурс] // URL: https://about.att.com/story/att_cisco_ge_ibm_intel_industrial_internet_consortium.html (дата обращения: 20.12.2021).

[112] Козлова Г.Г., Арбузова Т.А. Влияние индустрии 4.0 на промышленные предприятия // Международный журнал гуманитарных и естественных наук. 2021. № 4-3 [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/vliyanie-industrii-4-0-na-promyshlennye-predpriyatiya (дата обращения: 20.12.2021).

[113] What is a digital twin? // IBM [Электронный ресурс]. URL: https://www.ibm.com/topics/what-is-a-digital-twin (дата обращения: 20.12.2021).

контроля)[114] следует выделить наиболее перспективную и высоко технологичную – это технология «цифровых двойников», потенциал которой может быть в полной мере раскрыт именно с точки зрения промышленного контроля и надзора и реализации сформированной Концепции правового регулирования применения новых информационных технологий в сфере государственного контроля и надзора.

Технология «цифровой двойник» относится к передовым цифровым технологиям, которые составляют основу для цифровой экономики и цифровой трансформации деятельности органов государственной власти и местного самоуправления, осуществляющих публичное управление.

Среди множества передовых технологий, технология цифровой двойник (Digital Twin) является технологией-интегратором практически всех сквозных цифровых технологий и субтехнологий, выступает технологией-драйвером, обеспечивает технологические прорывы и позволяет высокотехнологичным компаниям переходить на новый уровень технологического и устойчивого развития на пути к промышленному лидерству на глобальных рынках[115].

В действующем законодательстве РФ встречаются различные трактовки цифровой технологии «цифровой двойник» (цифровые двойники). В соответствии с Приказом Федеральной службы государственной статистики от 30 июля 2020 г. № 424 «Об утверждении форм федерального статистического наблюдения для организации федерального статистического наблюдения за деятельностью в сфере образования, науки, инноваций и информационных технологий» под цифровым двойником предлагается понимать цифровую модель продукта или процесса, которая включает в себя требования к конструкции и технические модели, описывающие ее геометрию, материалы, компоненты, сборку и поведение; технические и эксплуатационные данные, уникальные для каждого конкретного физического актива.

Согласно Комплексному плану модернизации и расширения магистральной инфраструктуры на период до 2024 года, утвержденного Рас-

---

[114] Перспективные направления правового регулирования использования современных информационных технологий в контрольно-надзорной деятельности органов исполнительной власти: библиотека лучших российских и зарубежных практик: монография / А.В. Мартынов, М.В. Бундин, М.Д. Прилуков, Е.Н. Смирнова, Е.В. Ширеева; под науч. ред. А.В. Мартынова. Н. Новгород: Изд-во Нижегородского госуниверситета им. Н.И. Лобачевского, 2020. 227 с.

[115] URL: https://www.cnews.ru/news/top/2019-10-13_rossii_nuzhny_145_milliardov (дата обращения: 20.12.2021).

поряжением Правительства РФ от 30 сентября 2018 г. № 2101-р, под цифровыми двойниками предлагается понимать виртуальные образы транспортных средств и объектов транспортной инфраструктуры, в том числе для управления их жизненным циклом.

Как следует из Концепции проекта цифровизации городского хозяйства «Умный город», утвержденного приказом Министерства строительства и жилищно-коммунального хозяйства РФ от 25 декабря 2020 г. № 866/пр, «цифровой двойник» определяется как виртуальный прототип реального городского объекта или процесса, суть которого заключается в непрерывном сборе данных, стандартизации данных и отношений элементов, их визуализации и комплексном анализе.

Можно констатировать, что в настоящее время отсутствует в законодательстве РФ единое понимание цифровой технологии «цифровой двойник». Вместе с тем, необходимо учитывать, что Постановлением Правительства РФ от 10 октября 2020 года № 1646 «О мерах по обеспечению эффективности мероприятий использованию информационно-коммуникационных технологий в деятельности федеральных органов исполнительной власти и органов управления государственными внебюджетными фондами» утверждено Положение о ведомственных программах цифровой трансформации. Согласно данному документу, под «цифровой трансформацией» понимается совокупность действий, осуществляемых государственным органом, направленных на изменение (трансформацию) государственного управления и деятельности государственного органа по предоставлению им государственных услуг и исполнению государственных функций за счет использования данных в электронном виде и внедрения информационных технологий в свою деятельность в целях: а) повышение удовлетворенности граждан государственными услугами, в том числе цифровыми, и снижение издержек бизнеса при взаимодействии с государством; б) снижение издержек государственного управления, отраслей экономики и социальной сферы; в) создание условий для повышения собираемости доходов и сокращения теневой экономики за счет цифровой трансформации; г) повышение уровня надежности и безопасности информационных систем, технологической независимости информационно-технологической инфраструктуры от оборудования и программного обеспечения, происходящих из иностранных государств; д) обеспечение уровня надежности и безопасности информационных систем, информационно-телекоммуникационной инфраструктуры; е) устранение избыточной административной нагрузки на субъекты предпринимательской деятельности в рамках

контрольно-надзорной деятельности. Безусловно, внедрение в различные сферы деятельности государственных органов и граждан технологии «цифровой двойник» отвечает потребностям и целям цифровой трансформации публичного управления.

В соответствии с Энергетической стратегией Российской Федерации на период до 2035 года, утвержденной Распоряжением Правительства РФ от 9 июня 2020 г. № 1523-р, указывается, что быстрыми темпами разрабатываются и внедряются в том числе в отраслях топливно-энергетического комплекса цифровые технологии, в состав которых включают интернет вещей, 3D-моделирование, моделирование и прогнозирование на основе анализа «больших данных» (Big Data), нейросети, облачные и туманные вычисления, виртуальную и дополненную реальность, машинное обучение, компьютерную имитацию на основе цифровых двойников, интеллектуальные датчики, роботизацию производства, аддитивные технологии. Оборудование и технологии цифровых двойников, включая средства проведения комплексных цифровых испытаний оборудования и технологий и подтверждения параметров надежности отнесено данной Стратегией к перечню технологического оборудования, востребованного организациями топливно-энергетического комплекса Российской Федерации (в сфере электроэнергетики), создание или локализация производства которого необходимы на территории Российской Федерации до 2035 года.

Основой для создания технологических решений «цифровых двойников» является технология интернета вещей, т.е. автоматического сбора данных о состоянии реальных объектов и мониторинга технологических и иных процессов. В этом вопросе Россия последнее время предпринимает самые активные шаги. В конце 2020 года Минцифры анонсировала введение в эксплуатацию Государственной платформы сбора данных, анонсированной еще в конце 2020 года. Фактически данная платформа была создана в рамках федерального проекта «Цифровое государственное управление» национального проекта «Цифровая экономика» и интегрирована с «Типовым облачным решением по автоматизации контрольно-надзорной деятельности», куда передаются данные, которые в последствии становятся доступны для контрольно-надзорных органов. По заявлению Министерства цифрового развития, связи и коммуникации: «Создание ГПСД – наглядный пример цифровой трансформации социально значимого сектора с применением новых технологий. Во второй очереди проекта будет создана система экологического надзора в области охраны водных ресурсов, а также решение

для обнаружения фактов незаконного строительства и нарушения параметров строительства»[116]. В основе платформы используется технология интернета вещей – отечественная разработка от компании продукт Mail.ru IoT Platform. Сейчас платформ проходит апробацию в нескольких регионах России и позволяет отслеживает температуру, влажность воздуха, уровень задымления, протечки и появление трещин на фасадах зданий (Челябинская и Вологодская области). В Калужской области платформа помогает выявлять незаконные вырубки леса.

Важным шагом на пути к использованию современных методов контроля и надзора в сферу промышленности стало проведение эксперимента по внедрению системы дистанционного контроля промышленной безопасности[117] фактически с 1 февраля по 31 декабря 2022 г.

Целями эксперимента являются:

а) апробация динамической модели риск-ориентированного подхода в области промышленной безопасности с использованием системы дистанционного контроля промышленной безопасности;

б) определение эффективности и удобства применения для организаций и индивидуальных предпринимателей технологий сбора, аналитической обработки информации о состоянии промышленной безопасности и технологических процессах на эксплуатируемых ими опасных производственных объектах, расчета показателей состояния промышленной безопасности, оперативной оценки рисков возникновения аварий и передачи информации в Федеральную службу по экологическому, технологическому и атомному надзору (Ростехнадзор);

в) оценка параметров применения системы дистанционного контроля промышленной безопасности на опасных производственных объектах;

г) формирование методических, организационных и технологических условий для обеспечения возможности функционирования и применения системы дистанционного контроля промышленной безопасности;

---

[116] В России начали дистанционно контролировать охраняемые законом объекты // Министерство цифровой трансформации, связи и коммуникации [Электронный ресурс]. URL: https://digital.gov.ru/ru/events/40206/ (дата обращения: 20.12.2021).

[117] Постановление Правительства Российской Федерации от 31 декабря 2020 г. № 2415 «О проведении эксперимента по внедрению системы дистанционного контроля промышленной безопасности» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001202101090045 (дата обращения: 20.12.2021).

д) апробация новых подходов к обеспечению федеральных органов исполнительной власти автоматизированным инструментарием оценки рисков возникновения аварий на опасных производственных объектах с использованием систем оперативного мониторинга технологических процессов и расчета показателей состояния промышленной безопасности;

е) формирование модели бесперебойного функционирования системы дистанционного контроля промышленной безопасности;

ж) оценка достоверности сведений, вносимых в систему дистанционного контроля, по итогам проведения эксперимента.

Участниками являются Ростехнадзор и организации или индивидуальные предприниматели, которые эксплуатируют опасные производственные объекты и имеющие соответствующее оснащение для участия в эксперименте. Информация с производственных объектов и систем мониторинга/контроля поступает непосредственно в контролирующий орган, однако при этом не оценивается общее состояния зданий, сооружений, территории, цехов, участков, площадок, технических устройств, средств и оборудования; работоспособность приборов и систем контроля безопасности на объекте повышенной опасности; пригодность к использованию систем наблюдения, оповещения, связи и поддержки действий в случае аварии.

Организация или индивидуальный предприниматель, желающие принять участие в эксперименте, вправе направить соответствующую заявку в Ростехнадзор, подлежащую рассмотрению в течении 30-и дней и в случае положительного решения участие в эксперименте оформляется соглашением, в котором указывается:

а) порядок участия организации или индивидуального предпринимателя, эксплуатирующих опасные производственные объекты, предоставляющих ресурсы и сервисы для организации инфраструктуры системы дистанционного контроля промышленной безопасности;

б) требования к обеспечению информационной безопасности и защиты информации, используемой в рамках функционирования системы дистанционного контроля промышленной безопасности, в том числе от несанкционированного ее копирования, распространения, уничтожения и модификации, блокирования доступа к ней, а также от иных неправомерных действий, согласованные с федеральным органом исполнительной власти в области обеспечения безопасности и с федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации;

в) правила и порядок идентификации, аутентификации и авторизации с использованием системы дистанционного контроля промышлен-

ной безопасности участников информационного взаимодействия, осуществляющих в ней формирование, размещение, изменение и удаление информации;

г) порядок приема и хранения информации, поступившей с использованием системы дистанционного контроля промышленной безопасности, а также учета действий пользователей по ее изменению и удалению;

д) перечень, состав и формат информации, передаваемой посредством системы дистанционного контроля промышленной безопасности;

е) порядок и основания расторжения соглашения;

ж) иные положения, определяющие порядок взаимодействия сторон соглашения.

Участие лица в эксперименте означает согласие на беспрерывную передачу информации со средства дистанционного контроля в органы Ростехнадзора.

По заверению ведомства суть эксперимента заключается в том, чтобы всю обязательную документацию, которая ведётся организацией, перевести из бумажного в электронный вид и заполнять её непосредственно в личном кабинете в новой системе. Программа в автоматическом режиме будет анализировать поступающую информацию и предупредит об ошибках. Таким образом, у организации появится возможность самостоятельно себя проверить и исправить нарушения, не дожидаясь прихода инспектора. Кроме того, новая система будет в онлайн-режиме обрабатывать и передавать в контролирующие органы информацию о технологических процессах, состоянии противоаварийных систем и возможных рисках возникновения опасных ситуаций. Это поможет прогнозировать и предотвращать аварии, а также позволит отменить плановые проверки на производстве, снизив административную нагрузку на организации. Внедрение новой системы не потребует покупки дорогостоящего оборудования. По сути, это программно-аппаратный комплекс, который подключается к уже действующим на производстве автоматизированным системам[118].

Реализация этого эксперимента происходит параллельно с введением в эксплуатацию «АИС Ростехнадзора», появление которой было обозначено еще в конце 2020 года[119]. По сути эта система и будет получателем передаваемых в рамках эксперимента данных.

---

[118] Состоялось расширенное заседание секции № 1 НТС Ростехнадзора // Ростехнадзор [Электронный ресурс]. URL: https://www.gosnadzor.ru/news/64/3795/?sphrase_id=2228166 (дата обращения: 20.12.2021).

[119] Цифровая трансформация Ростехнадзора за 500 миллионов рублей // Охрана труда в России [Электронный ресурс]. URL: https://ohranatruda.ru/news/899/589135/ (дата обращения: 20.12.2021).

Оценка текущих условий и методические рекомендации

Для понимания текущих перспектив, связанных с реализацией положений предлагаемой концепции правового регулирования использования информационных технологий в сфере государственного контроля и надзора в условиях «цифровой экономики», важно отчётливо понимать текущие угрозы, которые могут оказать негативное влияние на ее реализацию, а также имеющиеся благоприятные условия и факторы, которые, наоборот, станут основой для будущих позитивных трансформаций.

1. Основные угрозы и негативные факторы. Действующие в настоящий момент программные и стратегические документы достаточно часто содержат упоминание угроз, в том числе, в связи с цифровизацией. В данном случае следует дать определенные пояснения по поводу того, что может трактоваться как угроза в контексте современных представлений.

В частности, Стратегия национальной безопасности определяет угрозы национальной безопасности как «совокупность условий и факторов, создающих прямую или косвенную возможность причинения ущерба национальным интересам Российской Федерации»[120]. В документе говорится об информационной безопасности, как одном из направлений обеспечения информационной безопасности, а также о том, что «быстрое развитие информационно-коммуникационных технологий сопровождается повышением вероятности возникновения угроз безопасности граждан, общества и государства»[121].

В принятой в 2016 году Доктрине информационной безопасности есть определение угрозы информационной безопасности (информационной угрозы) как «совокупности действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере»[122]. В разделе документа дается общее представление о те-

[120] Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // Официальный интернет портал правовой информации [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001202107030001 (дата обращения: 12.12.2021).

[121] Там же. П. 48.

[122] Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Официальный интернет портал правовой информации [Электронный ресурс].

кущих угрозах информационной безопасности России, к которым относится целый ряд факторов от возросшего информационного противостояния государств, возрастания масштабов использования информационно-психологического воздействия на личность до признания технологической зависимости отечественной промышленности от зарубежных информационных технологий.

В Прогнозе научно-технологического развития Российской Федерации до 2030 года[123] также указывается на ряд существенных угроз, связанных со сферой информационно-коммуникационных технологий: ускоренное формирование единого глобального информационного пространства; обострение «цифрового неравенства»; неготовность к широкомасштабному предоставлению гражданам медицинских и иных социальных услуг с использованием ИКТ; возможность использования потенциала ИКТ в целях подрыва национальной безопасности, нарушения государственного и общественного порядка; необходимость обеспечения эффективного (защищенного) документооборота; неготовность к массовому применению технологий виртуальной реальности; растущая незащищенность личной жизни и личного жизненного пространства.

Безусловно, многие из этих угроз имеют достаточно универсальный характер и могут быть вполне справедливо экстраполированы на более конкретные сферы и отрасли экономики и социальной жизни. Аналогичным образом можно вести речь и об их влиянии на сферу государственного контроля и надзора. С учетом этих факторов следует провести более подробный анализ степени их влияния на обозначенную сферу, а также иных факторов, не обозначенных в выше указанных документах, которые потенциально стоит рассматривать как угрозы в таком случае.

С определенной долей условности эти факторы можно классифицировать на внешние и внутренние факторы. Внешними в нашем случае будут факторы, которые будут характерны для российского общества и государства на пути к цифровизации в текущей перспективе. Внутренние будут связаны со сложившимися условиями функционирования органов контроля и надзора и системы государственного (муниципального) контроля и надзора в целом.

URL: http://publication.pravo.gov.ru/Document/View/0001201612060002 (дата обращения: 12.12.2021).

[123] Прогноз научно-технологического развития Российской Федерации до 2030 года // Официальный сайт Правительства Российской Федерации [Электронный ресурс]. URL: http://static.government.ru/media/files/41d4b737638b91da2184.pdf (дата обращения: 12.12.2021).

Внешние угрозы.

1) Высокий уровень зависимости отечественной промышленности от зарубежных информационных технологий в части, касающейся электронной компонентной базы, программного обеспечения, вычислительной техники и средств связи. Данная угроза сохраняет свою актуальность и применительно к сфере контроля и надзора. Эксперты Высшей школы экономики в своем аналитическом докладе назвали Россию «опаздывающим производителем» в сфере развития передовых технологий. Россия по-прежнему не рассматривается как крупный игрок на мировом рынке передовых технологий, и рискует навсегда отстать от крупных IT-лидеров. К таким сферам можно отнести электронику, оптоэлектронику, информационно-коммуникационные технологии, биотехнологии, робототехнику и другие[124].

Наиболее активными участниками рынка были признаны такие страны как Германия, Нидерланды, Швейцария, Бельгия, Чехия, Венгрия и Вьетнам. «Окружение лидеров» – Великобритания, Франция, Канада, Австрия, Дания. «Двигающие мировую технологическую границу» или лидеры по патентам в области производственных технологии – Корея, Япония, Швеция, Израиль и Финляндия. «Догоняющие производители» или интенсивно использующие производственные технологии для собственных нужд – Польша, Румыния, Словакия, Таиланд, Филиппины, Мексика, ОАЭ и Китай. К «опаздывающим производителям» исследователи отнесли 35 стран, в том числе, Россию, Бразилию, Индию, Казахстан и другие. В настоящий момент у России есть два пути – это либо навсегда застрять среди «отстающих» или попасть в группу «догоняющих».

Такие нелицеприятные оценки не всегда далеки от истины, несмотря на определенные успехи в сфере использования ИТ-технологий применительно к сфере государственного управления и контрольной и надзорной деятельности, в части развития цифровых сервисов.

Уже сейчас можно говорить о достаточно неплохих темпах цифровизации контрольной т надзорной деятельности и определенных фактах использования технологий облачных вычислений в части создания Типового облачного решения для контрольно-надзорной деятельности, применения дронов для контроля и надзора за состоянием окружающей

[124] Бунина В. Навсегда застрять среди отстающих: что ждет Россию на рынке технологий // Газета.ru. 13 апреля 2021 года [Электронный ресурс]. URL: https://www.gazeta.ru/tech/2021/04/13/13556486/lag_behind.shtml (дата обращения: 12.12.2021).

среды и противопожарного режима в лесной местности, технологий цифровых двойников и сенсорики в обеспечении промышленной безопасности. В тоже время стоит отметить сохранение серьезного отставания России в развитии элементной базы, технологий телекоммуникаций, создании продуктов и технологий в области искусственного интеллекта и др. Значительная часть применяемых решений основана на иностранных разработках и технологиях, что является потенциально серьезной угрозой для их применения в сфере публичного управления и контрольно-надзорной деятельности. Достаточно типичным примером является политика санкций, которые в том числе и проявляются через госсектор. С 2014 года для российских госструктур был закрыт доступ к приобретению оборудования и технологий видеоконференцсвязи, где лидирующие позиции занимали американские компании Cisco и Polycom, а также норвежская Tandberg. Отголоски этого решения в той или иной мере сказываются до сих пор и не всегда получается найти им полноценную замену, хотя определенные успехи в этом уже есть[125]. С началом пандемии COVID-19 в 2020 году как минимум два крупных программных разработчика, доминирующих на международном рынке в своих сегментах, отказались поставлять свои продукты для использования в госсекторе. В декабре 2020 года компания Microsoft отказалась участвовать в тендерах на поставку программного обеспечения в МГТУ им. Н.Э. Баумана, отнеся вуз к числу «конечных военных пользователей» с учетом большого количества оборонных разработок в нем[126]. Весной 2021 года компания Zoom Video Communications (владелец сервиса веб-конференций) анонсировала уже более «системный» запрет на поставку своих продуктов, в том числе, и своими авторизованными партнерами всем учреждениям и организациям госсектора. С учетом большой доли рынка в России и условий пандемии это стало достаточно ощутимым «ударом» для работы органов власти и госучреждений, которые вынуждены были искать альтернативные решения[127]. Еще хуже

[125] Импортозамещение ВКС в госструктурах // Российская газета. 22 декабря 2020 года [Электронный ресурс]. URL: https://rg.ru/2020/12/22/importozameshchenie-vks-v-gosstrukturah.html (дата обращения: 12.12.2021).

[126] Кинякина Е., Исакова Т. Microsoft отказался продавать софт Бауманке // Ведомости. 8 декабря 2020 года [Электронный ресурс]. URL: https://www.vedomosti.ru/technology/articles/2020/12/08/850139-microsoft-otkazalsya (дата обращения: 12.12.2021).

[127] Котляр М. Zoom запретила российскому госсектору пользоваться своей видеосвязью // РБК 6 апреля 2021 года [Электронный ресурс]. URL: https:

обстоят дела с элементной базой. Например, такой важный элемент любой вычислительной системы как процессор в России практически не производится. Пока в той или иной степени можно говорить о двух отечественных разработках – это процессоры Эльбрус (АО «МЦСТ») и Baikal (АО «Байкал Электроникс»). Процессоры Эльбрус в основном используются достаточно узконаправленно для военных и оборонных нужд и не могут конкурировать с иностранными производителями в потребительском сегменте[128]. «Байкал Электроникс» пока только апробирует возможности для производства своих процессоров в России на базе Калининградской компании GS Nanotech[129]. Безусловно, это шаги вперед, но в целом эти шаги явно недостаточны для покрытия потребностей российского рынка.

Высокие темпы цифровизации также стоит рассматривать не только с положительной стороны. Фактически уже сейчас можно встретить массу исследований, которые отмечают высокие риски динамичной цифровизации. Во многом эта угроза объясняется отставанием «классического» законодательства и права от текущей практики отношений по внедрению цифровых технологий в самые различные сферы жизни общества и государства. Часто технологические решения появляются с такой быстротой, что государство и общество не успевают в полной мере оценить все потенциальные риски, вызванные ими, и разработать соответствующее правовое регулирование. За последнее время часто ведется речь о необходимости поиска альтернативных решений путем использования правового эксперимента (регуляторных песочниц)[130],

---

//www.rbc.ru/technology_and_media/06/04/2021/606cbbde9a79476bb34333ed (дата обращения: 12.12.2021).

[128] Российский процессор вышел на мировой уровень // Яндекс. 2 марта 2021 года [Электронный ресурс]. URL: https://zen.yandex.ru/media/sdelanounas.ru/rossiiskii-processor-vyshel-na-mirovoi-uroven-603e54f1063b6456b1edcd5c (дата обращения: 12.12.2021).

[129] Процессоры Байкал-М начнут собирать в России на заводе GS Nanotech // Яндекс. 2 декабря 2021 [Электронный ресурс]. URL: https://zen.yandex.ru/media/id/5f20a49cf01f506fcb80c60b/processory-baikalm-nachnut-sobirat-v-rossii-na-zavode-gs-nanotech-61a73a440a881b67adbc8079 (дата обращения: 12.12.2021).

[130] См.: Наумов В.Б., Бутримович Я.В., Котов А.А. Обеспечение качества правового регулирования экспериментальных правовых режимов // Российское право: образование, практика, наука. 2020. № 3 [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/obespechenie-kachestva-pravovogo-regulirovaniya-eksperimentalnyh-pravovyh-rezhimov (дата обращения: 12.12.2021).

опережающего правотворчества[131], применения мягкого права[132] и инструментов саморегулирования[133]. Каждое из перечисленных решений может иметь свои достоинства и недостатки, но при этом угроза попрежнему остается актуальной[134]. Например, паспорт федерального проекта «Нормативное регулирование цифровой среды» предусматривает разработку в течении 2019–2024 годов более 350 нормативно-правовых актов в сфере правового регулирования цифровой экономики, порядка 250 из них должны быть приняты в 2021-2024 году, что свидетельствует скорее о начале планомерной работы в этом направлении нежели о ее завершении, если конечно последнее вообще применимо в таком случае.

2) Низкий уровень доверия к цифровым технологиям также можно рассматривать и как негативный фактор, который может создать препятствие к дальнейшему внедрению цифровых технологий в сферу контроля и надзора. Данный вид угрозы часто связан с эффектом так называемого «черного ящика»[135], когда люди не в полной мере понимают, как работают и используются те или иные цифровые технологии, и не могут оценить потенциальные риски и преимущества от их использова-

---

[131] См.: Баранова М.В. О специфике новелл опережающего правотворчества современно России (доктрина, практика, техника) // Юридическая техника. 2021. № 15 [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/o-spetsifike-novell-operezhayuschego-pravotvorchestva-sovremennoy-rossii-doktrina-praktika-tehnika (дата обращения: 12.12.2021).

[132] См.: Константин В.Н. Применение концепции «мягкой силы» в налогообложении криптовалют // Экономика. Налоги. Право. 2020. № 6 [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/primenenie-kontseptsii-myagkoy-sily-v-nalogooblozhenii-kriptovalyut (дата обращения: 12.12.2021).

[133] См.: Минбалеев А. В. Место и роль саморегулирования в развитии цифровых технологий // Образование и право. 2019. № 1 [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/mesto-i-rol-samoregulirovaniya-v-razvitii-tsifrovyh-tehnologiy (дата обращения: 20.11.2021).

[134] Бессонов Н.К. Правовые барьеры развития цифровизации в субъектах Российской Федерации // Образование и право. 2021. № 8 [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/pravovye-bariery-razvitiya-tsifrovizatsii-v-subektah-rossiyskoy-federatsii (дата обращения: 13.12.2021).

[135] Yu, R., & Alì, G. What's Inside the Black Box? AI Challenges for Lawyers and Researchers // Legal Information Management. 2019. № 19(1). Pp. 2–13. DOI:10.1017/S1472669619000021.

ния[136]. Часть таких опасений вызвана тем, что многие современные ИТ-компании предпочитают скрывать реальное предназначение тех или иных технологий и алгоритмы их работы[137]. Аналогичная ситуация может быть актуальна и в отношении случаев использования цифровых технологий в сфере государственного управления. Например, в России более половины граждан по результатам соцопросов в 2020 году не поддержали введение биометрической идентификации и создание Единой биометрической системы[138]. В настоящий момент система наиболее активно применяется в банковском секторе[139], но вот в остальных случаях ее применение часто сталкивается с недоверием пользователей[140]. В 2022 году в этом отношении планируются серьезные нововведения, в частности на Федеральном портале проектов нормативных актов размещен проект постановления Правительства РФ, которым предусматривается создание «Единой информационной системы персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица»[141], что подразумевает создание факти-

[136] Sutherland S.A. Some Thoughts on Black Box AI and Law // Slaw. Canada Online legal magazine. 18.08.2021 [Электронный ресурс]. URL: http://www.slaw.ca/2021/08/18/some-thoughts-on-black-box-ai-and-law/ (дата обращения: 21.10.2021).

[137] Kramer A. 6 successful tech companies that are surprisingly secretive about their internal workings // Insider. 25.09.2019 [Электронный ресурс]. URL: https://www.businessinsider.com/secretive-tech-companies-apple-google-palantir-2019-9 (дата обращения 21.10.2021).

[138] Скобелев В., Чернышева Е. Половина россиян не поддержали создание властями биометрической системы // РБК. 28 декабря 2020 года [Электронный ресурс]. URL: https://www.rbc.ru/technology_and_media/28/12/2020/5fe5cee59a7947dfd4362d12 (дата обращения: 12.12.2021).

[139] Орехин П. Безопасность во главе угла // Российская газета. 8 октября 2019 года [Электронный ресурс]. URL: https://rg.ru/2019/10/08/ispolzovanie-biometricheskoj-sistemy-pravo-grazhdan-a-ne-obiazannost.html (дата обращения: 12.12.2021).

[140] Ногаева К. Применение биометрии развивается на фоне недоверия россиян // Деловой Петербург. 7 декабря 2021 [Электронный ресурс]. URL: https://www.dp.ru/a/2021/12/06/Otdam_v_horoshie_ruki (дата обращения: 12.12.2021).

[141] Проект Постановления Правительства РФ «О внесении изменений в постановление Правительства Российской Федерации «Об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в

чески единой системы биометрической идентификации в том числе и для госсектора. Данная система должна стать частью единой инфраструктуры, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме[142]. Очевидно, что она будет использована в будущем и для осуществления контрольной и надзорной функций. Тем не менее степень доверия к таким решениям часто «расшатывается», в том числе, и ввиду появления фактов «ошибок», которые допускают системы распознавания лиц с искусственным интеллектом. В качестве примера можно назвать случай в США, где в 2020 году полиция штата Детройт задержала мужчину по подозрению в преступлении и продержала его 30 часов в камере, пока выяснялись все обстоятельства[143]. Аналогичный случай произошел и в Москве, когда гражданин был задержан сотрудниками охраны супермаркета на два часа и после был передан в полицию, где, по его словам, ему угрожали тюремным заключением[144]. Еще большую озабоченность вызывают случаи, когда цифровые технологии неправомерно используются представителями органов власти, как это произошло в ситуации с группой сотрудников полиции в Москве, которые «продавали» данные граждан, собираемые с использованием городских камер видеонаблюдения и

электронной форме» // Федеральный портал проектов нормативных актов [Электронный ресурс]. URL: https://regulation.gov.ru/projects/List/AdvancedSearch#departments=122&npa=122184 (дата обращения: 12.12.2021).

[142] Постановление Правительства РФ от 08.06.2011 № 451 «Об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001202103310017 (дата обращения: 12.12.2021).

[143] Hill K. Wrongfully Accused by an Algorithm // New York Times. 24.06.2020 [Электронный ресурс]. URL: https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html (дата обращения: 12.12.2021).

[144] Касми Э. Россиянина едва не посадили на 8 лет из-за ошибки искусственного интеллекта // CNews. 20.11.2020 [Электронный ресурс]. URL: https://www.cnews.ru/news/top/2020-11-12_rossiyanina_edva_ne_posadili (дата обращения: 12.12.2021).

технологии распознавания лиц[145]. Такие случаи в совокупности усиливают уровень недоверия граждан к цифровым технологиям в значительной степени от непонимания того, как они работают и сомнений в том, насколько эти алгоритмы безопасны и не нарушают их законные права и интересы[146]. В то же время процессы внедрения цифровых технологий носят часто необратимый характер, и в условиях их повсеместного распространения в различных сферах экономики было бы не логично отказываться от их внедрения в сферу публичного управления, а также в сферу контроля и надзора.

3) Возросшие масштабы информационно-технического воздействия на объекты государственной информационной инфраструктуры со стороны иностранных спецслужб[147]*, а также возросшие масштабы компьютерной преступности* в России и мире. Данные факторы представляют серьезную угрозу для обеспечения безопасного использования цифровых технологий в публичном секторе. По некоторым данным 68% кибератак (атаки типа advanced persistent threat, APT-атаки) на объекты информационной инфраструктуры приходится на госсектор, государственные учреждения и органы власти. При этом 2/3 таких преступных сообществ (APT-групп) ориентированы именно на совершение кибератак в отношении государственных информационных систем, где, как правило, обрабатываются критически важные конфиденциальные и/или секретные данные[148]. Так в 2018 году в период избирательной кампании на выборах Президента РФ были совершены масштабные

[145] Александров А., Королев Н. Система распознавания дала правоохранительный сбой // Коммерсантъ. 24 сентября 2020 года [Электронный ресурс]. URL: https://www.kommersant.ru/doc/4503252 (дата обращения: 12.12.2021).

[146] Кочетова К. На темной стороне силы: чем грозят технологии распознавания лиц // KasperskyDaily. 22 августа 2016 года [Электронный ресурс]. URL: https://www.kaspersky.ru/blog/bad-facial-recognition/12823/ (дата обращения: 12.12.2021).

[147] Апулеев И. Миллионы кибератак: Патрушев о происках иностранных спецслужб // ГазетаRU. 25 октября 2019 года [Электронный ресурс]. URL: https://www.gazeta.ru/tech/2019/10/25_a_12776498.shtml?updated (дата обращения: 12.12.2021).

[148] APT-атаки на госучреждения в России: обзор тактик и техник 2019 // Positive Technologies. 5 декабря 2019 года [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/apt-attacks-government-2019/ (дата обращения: 12.12.2021).

кибератаки на ГАС «Выборы»[149]. В 2019 году были озвучены, в том числе и на официальном уровне, серьезные претензии к американским спецслужбам, которые подозревались в организации масштабных кибератак на российский энергетический сектор[150]. В 2018 году Приказом Федеральной службы безопасности от 24.07.2018 г. № 366 «О национальном координационном центре по компьютерным инцидентам» создан одноименный центр в целях обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты[151]. Сегодня Центром регистрируется еженедельно сотни инцидентов информационной безопасности и кибератак на объекты критической информационной инфраструктуры[152]. Масштабы компьютерной преступности также вызывают все больше опасений. По некоторым данным ее объемы выросли в 25 раз за последние 5 лет[153]. Причем пандемия COVID-19 вызвала резкую вспышку Интернет-преступности, и в 2020 году в сравнении с 2019 ее показатели составили целых 91%[154]. Общее количество инцидентов в I квартале 2021 года в сравнении с аналогичным периодом 2020 года увеличилось на 17%, а относительно IV квартала 2020 прирост составил 1,2%[155]. Все эти фак-

[149] МВД: на ГАС «Выборы» были совершены хакерские атаки // ТАСС. 18 марта 2018 года [Электронный ресурс]. URL: https://tass.ru/politika/5042534 (дата обращения: 12.12.2021).

[150] Сухоруков А. Источник подтвердил, что США атакуют российскую энергосистему // РИА Новости. 17 июня 2019 года [Электронный ресурс]. URL: https://ria.ru/20190617/1555640687.html (дата обращения: 12.12.2021).

[151] Приказ Федеральной службы безопасности Российской Федерации от 24.07.2018 № 366 «О Национальном координационном центре по компьютерным инцидентам» // Официальный интернет-портал правовой инфорации [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001201809100001 (дата обращения: 12.12.2021).

[152] Основные результаты деятельности НКЦКИ // НКЦКИ [Электронный ресурс]. URL: https://safe-surf.ru/search/?tags=статистика%20НКЦКИ (дата обращения: 12.12.2021).

[153] Число киберпреступлений в России выросло в 25 раз за пять лет // ПравоRU. 17 июля 2020 года [Электронный ресурс]. URL: https://pravo.ru/news/223988/ (дата обращения: 12.12.2021).

[154] Число преступлений с использованием интернета выросло на 51% // ПравоRU. 19 апреля 2021 [Электронный ресурс]. URL: https://pravo.ru/news/231041/ (дата обращения: 12.12.2021).

[155] Актуальные киберугрозы: I квартал 2021 года // Positive Technologies. 11 июня 2021 года [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-

торы и подтвержденные случаи взлома государственных информационных систем иностранными группами хакеров[156], безусловно, вызывают обеспокоенность за безопасность цифровых технологий, применяемых, в том числе и для осуществления государственного контроля и надзора. Более того большинство информационных систем и соответственно объектов инфраструктуры, используемых для предоставления цифровых сервисов в области контроля и надзора объективно относятся к критической информационной инфраструктуре[157], а значит, требуют пристального внимания с точки зрения обеспечения информационной безопасности.

4) Состояние научных исследований в области информационных технологий и информационной безопасности. Данный фактор также в совокупности может представлять серьезную угрозу эффективному применению информационных технологий, в том числе в сфере государственного контроля и надзора. Аналитические данные скорее свидетельствуют об относительно низком в сравнении с зарубежными странами объеме исследований, связанных с цифровыми технологиями. В докладе НИУ ВШЭ указывается, что удельный вес России в общемировом объеме научных публикаций по цифровым технологиям не превышает 5%. С 2018 года наша страна стабильно находится только в 20–30-ке стран по уровню научных исследований в этом направлении. Относительно сильные позиции Россия занимает в области исследований квантовых технологий и блокчейна. Однако мировую повестку дня по-прежнему формируют пять стран: Китай, США, Япония, Германия, Великобритания[158]. При этом в последние годы динамика публикационной активности российских авторов положительна и опережает сред-

---

ru/research/analytics/cybersecurity-threatscape-2021-q1/ (дата обращения: 12.12.2021).

[156] Коварные заграничные хакеры годами взламывали сети органов власти России и оставались незамеченными // CNews. 20 мая 2021 года [Электронный ресурс]. URL: https://www.cnews.ru/news/top/2021-05-20_kovarnye_inostrannye_hakery (дата обращения: 12.12.2021).

[157] Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001201707260023 (дата обращения: 12.12.2021).

[158] Цифровые технологии в российской экономике / К.О. Вишневский, Л.М. Гохберг, В.В. Дементьев и др.; под ред. Л.М. Гохберга; Нац. исслед. ун-т «Высшая школа экономики». М.: НИУ ВШЭ, 2021. 116 с.

немировую. В тоже время критически важным является междисциплинарность в осмыслении и оценке новых цифровых технологий[159]. Необходимость проведения междисциплинарных исследований, в том числе и в сфере информационно-коммуникационных технологий, подчеркивалась ещё в Программе фундаментальных научных исследований в Российской Федерации на долгосрочный период (2013–2020 годы)[160]. Однако важны не только сами исследования цифровых технологий, но и научное осмысление их влияния на конкретные сферы экономики и социальной жизни. Например, применительно к сфере контроля и надзора в Научной электронной библиотеке «E-library» в поиске по ключевым словам «контроль и надзор» и «цифровые технологии» отображаются в не более чем 75 публикациях, что, пожалуй, говорит о недостаточности исследований в этой области на данный момент[161]. К сожалению, фундаментальные научные исследования часто проводятся и финансируются в общей массе. Пожалуй, одним из немногих тематических конкурсов научных исследований в сфере юриспруденции можно назвать конкурс РФФИ по теме «Трансформация права в условиях развития цифровых технологий»[162], который проводился в 2018 году и был скорее исключением из общего правила. Все это в совокупности заставляет задумываться о необходимости разработки мер дальнейшей поддержки междисциплинарных научных исследований и разработок в сфере цифровизации контроля и надзора в свете текущих существенных законодательных изменений в сфере государственного управления в связи с принятием изменений в Конституцию РФ[163], разработкой

[159] Касавина Н.А. Цифровизация как предмет междисциплинарный исследований // Эпистемология и философия науки. 2019. Т. 56. № 4. С. 251-259.

[160] Распоряжение Правительства РФ от 27 декабря 2012 г. № 2538-р «О Программе фундаментальных научных исследований в РФ на долгосрочный период (2013-2020 гг.)» // Правительство Российской Федерации [Электронный ресурс]. URL: http://government.ru/docs/20270/ (дата обращения: 12.12.2021).

[161] Научная электронная библиотека e-Library [Электронный ресурс] // URL: https://elibrary.ru/query_results.asp (дата обращения: 12.12.2021).

[162] Конкурс на лучшие научные проекты междисциплинарных фундаментальных исследований по теме «Трансформация права в условиях развития цифровых технологий» // РФФИ [Электронный ресурс]. URL: https://www.rfbr.ru/rffi/ru/contest/n_812/o_2058677 (дата обращения: 12.12.2021).

[163] Закон РФ о поправке к Конституции РФ от 14.03.2020 № 1-ФКЗ «О совершенствовании регулирования отдельных вопросов организации и функционирования публичной власти» // Официальный интернет-портал правовой ин-

закона о публичной власти[164] и вступления в силу закона о контроле и надзоре[165].

К числу ***внутренних угроз***, связанных с особенностями внутренней организации и функционирования органов контроля и надзора, можно отнести ряд факторов, которые существенным образом влияют на эффективность контрольно-надзорной деятельности.

1) Недостаточное кадровое и организационное обеспечение цифровой трансформации государственного управления. В настоящий момент уже очевидно, что цифровизация государственного управления совершенно невозможна без системного подхода к организации и кадровому обеспечению этих процессов. Требуется глубокий системный подход к созданию соответствующей структуры внутри органов власти и управления, которая бы управляла этими процессами, а также координационных центров по межведомственному взаимодействию. Более того все эти структуры требуют кадрового обеспечения, при чем не только внутри, и должны содействовать формированию соответствующего вектора к изменению и обновлению компетенций государственных служащих этих органов власти. До недавнего времени в России ситуация в этой части была достаточно критической, причем кадровый «голод» на госслужбе сформировался еще до пандемии COVID-19, которая его только обострила. Согласно исследованию, проведенному Центром подготовки руководителей цифровой трансформации ВШГУ РАНХиГС, затруднения в организационно-кадровом обеспечении государственной службы можно разделить на три группы:

– кадровые сложности (дефицит кадров на рынке труда, отсутствие мотивации к развитию цифровых компетенций у госслужащих, нехватка ИТ-специалистов в штате и системного подхода к обучению новым цифровым технологиям, методам управления);

формации [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001202003140001 (дата обращения: 12.12.2021).

[164] Законопроект № 1256381-7 «Об общих принципах организации публичной власти в субъектах Российской Федерации» // Система обеспечения законодательной деятельности (СОЗД) [Электронный ресурс]. URL: https://sozd.duma.gov.ru/bill/1256381-7 (дата обращения: 12.12.2021).

[165] Федеральный закон «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» от 31.07.2020 № 248-ФЗ // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001202007310018 (дата обращения: 12.12.2021).

– нормативные и финансовые ограничения (штатное расписание не соответствует потребностям органа власти в ИТ-поддержке, низкий уровень оплаты труда, отсутствие компетентных сотрудников для разработки технических документов для госструктур);

– проблемы, связанные с бессистемным подходом к управлению цифровыми проектами (сотрудники участвуют в 5−10 проектах параллельно, ресурсы ИТ-подразделения тратятся на решение задач отраслевых ведомств, конфликт интересов, отсутствие автоматизации и др.)[166].

В то же время по поводу дефицита кадров ИТ-специалистов имеются и альтернативные мнения. В частности, в исследовании, проведенном экспертами НИУ ВШЭ, наоборот отмечается достаточность или даже насыщенность рынка специалистами в области цифровых технологий, в особенности с учетом количества выпускаемых специалистов по направлениям «Компьютерные и информационные науки», «Информатика и вычислительная техника», «Информационная безопасность», совокупная доля в бакалавриате которых составляет уже 11% от всех бюджетных мест[167]. В таких условиях нехватка указанных специалистов в госсекторе скорее вызвана отсутствием необходимой мотивации и низкой стоимостью услуг (заработной платы) в государственных органах[168]. С другой стороны, сами участники рынка, представители органов власти, отвечающие за вопросы информационной безопасности, часто говорят о готовности взять специалиста сразу на выпуске из вуза, используя формулу, что проще вырастить редкого эксперта, чем найти[169]. При этом молодой выпускник может получить серьезный опыт

[166] Организационные структуры и команды цифровой трансформации в системе государственного управления / авт.-сост. Н.С. Гаркуша, А.С. Шубин; под ред. М.С. Шклярук. М.: РАНХиГС, 2020. 165 с.

[167] Цифровая трансформация государственного управления: мифы и реальность: докл. к XX Апр. междунар. науч. конф. По проблемам развития экономики и общества, Москва, 9-12 апр. 2019 г. / Д.Ю. Двинских, Н.Е. Дмитриева, А.Б. Жулин и др.; под общ. ред. Н.Е. Дмитриевой; Нац. исслед. ун-т «Высшая школа экономики». М.: Изд. дом Высшей школы экономики, 2019. 43, [1] с.

[168] Почему ИТ-шники идут в госсектор, где зарплаты до 30% ниже рынка. Дискуссия на конференции TAdviser // TAdviser. 18 марта 2020 года [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/Статья:Почему_ИТ-шники_идут_в_госсектор,_где_зарплаты_до_30%25_ниже_рынка._Дискуссия_на_конференции_TAdviser (дата обращения: 12.12.2021).

[169] Информационная безопасность в госсекторе (Материалы заочного круглого стола) // Системный администратор. 2021. № 5(222) [Электронный ресурс]. URL: http://samag.ru/archive/article/4382 (дата обращения: 12.12.2021).

и существенно улучшить свои позиции в дальнейшем на рынке труда. В данном случае, отмечается и тот факт, что ситуация на рынке кадров и текущая ситуация с развитием цифровых технологий часто приводит к тому, что содержание образовательных программ бакалавриата и специалитета банально не успевает за текущими реалиями. В конечном итоге это приводит к необходимости более гибко и системно подходить к формированию и распространению дополнительных профессиональных программам развития цифровых компетенций у государственных служащих. Как бы то ни было, и принимая во внимание различные мнения о причинах и следствиях кадрового «голода» ИТ-специалистов на госслужбе следует признать, что проблема существует и требует решения. Определенные активные шаги в этом направлении уже принимаются. В частности, уже сейчас в России активно распространяется практика назначения в органах власти ответственных за цифровизацию в ранге заместителей ведомств[170], а в Аппарате Правительства было назначено 5 заместителей, отвечающих за различные направления цифровизации[171].

2. Благоприятные условия и факторы. Реальное внедрение современных информационных технологий в контрольно-надзорную деятельность органов исполнительной власти, а также развитие правового регулирования в указанной сфере возможно лишь при наличии позитивных условий и факторов.

Условие – это «обстоятельство, от которого что-нибудь зависит; обстановка, в которой происходит, осуществляется что-нибудь»[172]. Следовательно, ключевым условием внедрения информационных технологий в контрольно-надзорную деятельность органов исполнительной власти является степень разработанности и развития в целом правового регулирования, затрагивающего вопросы применения современных информационных технологий. Основы правового регулирования применения ин-

[170] ИТ в федеральных ведомствах России // TAdviser. 26 ноября 2021 года [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/Статья:ИТ_в_федеральных_ведомствах_России# (дата обращения: 12.12.2021).

[171] За цифровизацию России взялись пять замов главы Аппарата Правительства // Cnews. 6 марта 2020 года [Электронный ресурс]. URL: https://www.cnews.ru/news/top/2020-03-06_tsifrovizatsiej_rossii_zajmutsya (дата обращения: 12.12.2021).

[172] Ожегов С.И. Словарь русского языка [Электронный ресурс] // URL: https://slovarozhegova.ru/word.php?wordid=33352 (дата обращения: 20.07.2021).

формационных технологий в контрольно-надзорной деятельности органов исполнительной власти на современном этапе представлены рядом нормативных актов программного характера. Данные акты достаточно подробно рассмотрены в § 1 главы 1 настоящей монографии.

Рассмотренные программные документы в целом являются правовой основой применения современных информационных технологий в государственном управлении. В них отмечаются основные направления развития, а также возможные для применения информационные технологии в российской правовой действительности. Однако указанные базовые документы являются лишь некоторыми ориентирами развития правового регулирования применения современных информационных технологий в государственном секторе. В связи с чем они должны находить свое закономерное развитие в нормативно-правовых актах специального характера, затрагивающих конкретные вопросы внедрения современных информационных технологий в контрольно-надзорную деятельность органов исполнительной власти. К сожалению, на современном этапе данное правовое регулирование видится фрагментарным либо отсутствует.

Но несмотря на это, все же следует констатировать, что в правовой действительности Российской Федерации на настоящий момент в целом сформировались необходимые базовые условия, которые позволяют внедрять современные информационные технологии в контрольную и надзорную деятельность органов исполнительной власти, а также способствуют цифровой трансформации и модернизации форм и методов государственного контроля и надзора. Данные выводы также подтверждаются полученными результатами проведенного опроса должностных лиц контрольно-надзорных органов, которые оценивают уровень правового регулирования информационных технологий как средний (52 % респондентов).

Фактор – это «момент, существенное обстоятельство в каком-нибудь процессе, явлении»[173]. Факторы представляют собой движущую причину внедрения информационных технологий. В теории права выделяют следующие основные группы факторов: политические, экономические, социальные, технические и юридические. Среди ключевых положительных факторов, относящихся к перечисленным группам и стимулирующих к внедрению информационных технологий в контрольную и надзорную деятельность органов исполнительной власти в сфере обес-

[173] Ожегов С.И. Словарь русского языка [Электронный ресурс] // URL: https://slovarozhegova.ru/word.php?wordid=33656 (дата обращения: 20.07.2021).

печения общественной безопасности и правопорядка, на наш взгляд, следует отнести:

– технологический прорыв (технические факторы);

– формирование нового мировоззрения о цифровизации общества (социальные факторы);

– появление новых «цифровых» отношений, которые ранее не требовали своего урегулирования (юридические факторы);

– постоянный рост объемов информации, который диктует необходимость долгосрочного сетевого хранения (технические факторы);

– курс государства на активное развитие и внедрение информационных технологий во все сферы жизнедеятельности (политические факторы).

3. Методические рекомендации. С учетом изложенных факторов авторы могли бы предложить определенный алгоритм внедрения цифровых технологий в сферу контроля и надзора. Данный алгоритм сопряжен с описанием конкретных предложений для органов контроля и надзора и основывается на необходимости разрешения определенных вопросов для практического внедрения цифровых технологи.

Определение сфер применения цифровых технологий. На данном этапе речь идет о выборе непосредственных сфер и областей применения тех или иных технологий. В целом тут можно вести речь о необходимости оценки рисков, связанных с цифровизацией той или иной сферы государственного контроля и надзора. Безусловно, в первую очередь стоит вести речь о том, как внедрение цифровых технологий скажется на эффективности его осуществления. Однако при определении таких сфер немаловажным будет также понять и оценить негативные последствия для проверяемых лиц и общества в целом. В частности, насколько осуществление контроля и надзора будет являться более удобным, комфортным и понятным для участников отношений, не станет ли это критичным для изменения уровня доверия граждан к контрольно-надзорным действиям и мероприятиям, а также оценить потенциальный уровень опасности для участников отношений. Более того, стоит рассматривать цифровые технологии с точки зрения допустимости или недопустимости внедрения некоторых из них. В данном случае речь идет о тех технологиях, в отношении которых в обществе может сложиться противоречивая оценка их эффективности, безопасности, или их могут рассматривать как ущемление прав и свобод личности, законных интересов юридических лиц и т.д. Примером таких технологий могут служить технологии распознавания лица, биометрической идентифика-

ции и аутентификации, искусственного интеллекта и др. В конечном итоге в данном случае видится целесообразным выделять следующие сферы применения цифровых технологий:

1) сферы, где применение этих цифровых технологий является необходимым условием для эффективного осуществления контроля и надзора, в противном случае его осуществление было бы невозможным или затруднительным. К таким сферам можно отнести саму сферу информационных технологий, где органы контроля и надзора также должны идти «в ногу со временем» и использовать новейшие цифровые технологии для достижения необходимого результата. Кроме этого, сложные производственные и технические сферы, современная промышленность, транспорт, медицина, которые тоже часто требуют соответствующей оснащенности органов контроля и надзора.

2) сферы, где применение цифровых технологий будет являться допустимым и/или желательным. В таких сферах эти технологии могли бы стать эффективным инструментом, часто с сохранением возможности осуществления действий и мероприятий без их использования. В этом случае информационные технологии могут предоставлять альтернативные варианты для проведения мероприятий по контролю и надзору, как это происходит при использовании дистанционных способов взаимодействия участников контрольно-надзорной деятельности. В данном случае ситуация с пандемией ясно продемонстрировала широкие возможности для таких форм взаимодействия.

3) сферы, где применение цифровых технологий нежелательно/ограниченно и/или невозможно. Конечно, в данном случае речь идет возможности использования тех или иных технологий, а не всей их совокупности. В то же время практика, бывает, показывает, с одной стороны, неготовность соответствующей среды для использования цифровых технологий, а с другой стороны, высокие риски или их низкую/неопределённую надежность. Следует признать, что таких сфер становится все меньше, однако в современном обществе в отношении некоторых технологий существует сформировавшееся «недоверие» или «озабоченность», в связи с чем вполне возможен отказ от их использования там, где получаемый эффект несравним с высокими рисками социальных последствий, и в особенности, если результат может быть достижим «обычными» средствами.

Выбор цифровой технологии. Данный этап или шаг следует связать с формированием необходимых требований и оценкой ожиданий от внедрения цифровой технологии, а также анализом существующего

рынка цифровых продуктов и сервисов. Логически и практически этот этап можно подразделить на ряд направлений, которые могут реализовываться системно и в параллели:

1) Анализ существующего рынка продуктов в области цифровых технологий, определения их возможностей и преимуществ в сравнении с используемыми в настоящий момент решениями и сервисами. Выявление необходимых потребностей в их замене или модернизации. Поиск оптимальных решений с точки зрения стоимости, эффективности и совместимости с имеющимися и используемыми решениями. По-видимому, в помощь органам власти было бы логичным создавать своего рода каталоги с описанием функциональных возможностей существующих на рынке решений, которые могут быть оптимальными с точки зрения потребностей и нужд органов власти и отвечающими базовым требованиям безопасности, информационной безопасности, стоимости, надежности и эксплуатационных качеств. Более того в определенном смысле гармонизация приобретаемых продуктов дала бы массу таких преимуществ, как:

– унификация правил эксплуатации и использования (руководств пользователя, внутренних правил, регулирующих порядок использования цифровых продуктов или решений);

– снижение стоимости обслуживания/эксплуатации однотипных устройств и технологических решений;

– унификация обучения и подготовки специалистов, ответственных за эксплуатацию цифровых продуктов;

– упрощение межведомственного взаимодействия.

2) Формирования требований к цифровым технологическим решениям и продуктам. Данный аспект часто связан с необходимостью соотнесения тех или иных продуктов и/или решений с существующими стандартами в области информационных технологий, используемых на международном уровне (ИСО/МЭК) или их национальных аналогов при наличии (ГОСТ). В настоящий момент разработаны сотни стандартов в области информационных технологий и цифровых продуктов в том числе в области искусственного интеллекта, робототехники, сенсорики, беспроводных сетей связи и др. Наиболее остро сейчас стоит вопрос, в частности, о разработке стандартов в области искусственного интеллекта, активную работу над ними ведется как на международном уровне[174], так и в Рос-

[174] ИСО/МЭК разработает международные стандарты в области искусственного интеллекта // Технолект. 1 ноября 2018 года [Электронный ресурс]. URL: https://tehnolet.cntd.ru/news/read/isomk-razrabotaet-mejdunarodnye-standarty-v-

сии[175]. При этом скорее всего данные стандарты могут быть скорее ориентиром для формирования необходимых ведомственных и/или межведомственных требований к цифровым продуктам и технологиям, при выборе которых требуется делать поправку на специфику той или иной сферы контроля и надзора. В некоторых случаях, как, например, в борьбе с фейковыми новостями, это может стать принципиально новым и потенциально высоко эффективным решением.[176]

3) Приоритет отечественным разработкам и продуктам. Данный параметр является крайне важным в выборе и формировании требований к разработчикам и поставщикам цифровых продуктов для госсектора. В совокупности это объясняется как достаточно банальными соображениями информационной безопасности, так и необходимостью поддержки и сохранения притока инвестиций в российскую цифровую экономику. С учетом общих потребностей российского государственного сектора данный вклад вполне можно рассматривать как ощутимый. Надо сказать, что российское государство все чаще прибегает к ограничительным мерам в допуске иностранных цифровых продуктов на рынок государственных закупок. В отношении программного обеспечения с 2015 года последовательно вводятся жесткие ограничительные меры. Первоначально был запрещен допуск программного обеспечения, происходящего из иностранных государств[177], а далее был сформирован

---

oblasti-iskusstvennogo-intellekta/novosti-cifrovoj-ehkonomiki (дата обращения: 12.12.2021).

[175] Развитию искусственного интеллекта в здравоохранении будут способствовать новые // Росстандарт. 6 декабря 2021 года [Электронный ресурс]. URL: https://www.rst.gov.ru/portal/gost/home/presscenter/news/newsRST/redirect/news/1/5241?portal:componentId=88beae40-0e16-414c-b176-d0ab5de82e16&navigationalstate=JBPNS_rO0ABXczAAZhY3Rpb24AAAABAA5zaW5nbGVOZXdzVmlldwACaWQAAAABAAQ4NDM3AAdfX0VPRl9f (дата обращения: 12.12.2021).

[176] Сахмеев В. Физтех за 14 млн создаст Роскомнадзору программу по поиску экстремизма и видео для взрослых в Сети // Собеседник. 11 октября 2021 года [Электронный ресурс]. URL: https://sobesednik.ru/obshchestvo/20211011-fiztex-za-14-mln-sozdast-roskomnadzoru-p (дата обращения: 12.12.2021).

[177] Постановление Правительства РФ от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102382688 (дата обращения: 12.12.2021).

реестр отечественного программного обеспечения[178] и план перехода органов власти на его использование[179], и в некоторых случаях на переход к единым закупкам (офисное ПО)[180]. С другой стороны, выбор в пользу российского продукта возможен при наличии эффективного отечественного решения, что не всегда возможно, несмотря на наличие по состоянию на ноябрь 2021 года в базе отечественного ПО более 12 000 программных разработок[181]. В данном случае стоит вести речь о необходимости принятия мер по стимулированию отечественных разработок, ориентированных на использовании для нужд государственного управления в целом и контроля и надзора в частности. При этом может потребоваться доработка и адаптация таких решений к нуждам контрольно-надзорной деятельности. Скорее всего и здесь стоит вести речь о системном подходе, в том числе и в плане формирования общей государственной политики в области государственных закупок цифровых продуктов и решений для органов контроля и надзора.

Организационно-кадровое обеспечение цифровизации. Как уже отмечалось неоднократно авторами, вне всякого сомнения требуется си-

---

[178] Единый реестр российских программ для электронных вычислительных машин и баз данных (создан на основании ст. 12.1 Федерального закона «Об информации, информационных технологиях и о защите информации») [Электронный ресурс] // URL: https://reestr.digital.gov.ru/.

[179] Приказ Минкомсвязи России от 04.07.2018 № 335 «Об утверждении методических рекомендаций по переходу органов исполнительной власти субъектов Российской Федерации и органов местного самоуправления муниципальных образований Российской Федерации на использование отечественного офисного программного обеспечения, в том числе ранее закупленного офисного программного обеспечения» // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации [Электронный ресурс]. URL: https://digital.gov.ru/ru/documents/6142/#:~:text=Приказ.%2004.07.2018%20№335.%20Москва.%20Об,ранее%20закупленного%20офисного%20программного%20обеспечения (дата обращения: 12.12.2021).

[180] Постановление Правительства Российской Федерации от 08.06.2018 г. № 658 «О централизованных закупках офисного программного обеспечения, программного обеспечения для ведения бюджетного учета, а также программного обеспечения в сфере информационной безопасности» // Официальный сайт Правительства Российской Федерации [Электронный ресурс]. URL: http://government.ru/docs/all/116897/ (дата обращения: 12.12.2021).

[181] Единый реестр российских программ для электронных вычислительных машин и баз данных (создан на основании ст. 12.1 Федерального закона «Об информации, информационных технологиях и о защите информации») [Электронный ресурс] // URL: https://reestr.digital.gov.ru/

стемность в организации внедрения цифровых продуктов и технологий в сферу контроля и надзора. В *организационном плане* уже давно предпринимаются определённые шаги. Сейчас вопрос о цифровизации вынесен на самый высокий управленческий уровень органов власти и управления. С 2020 года фактически рекомендовано иметь не только управленческую структуру, ответственную за информатизацию, но также назначение ответственного за цифровизацию в ранге заместителя руководителя органа власти. Более того эти процессы предполагают серьезную проработку и планирование. В 2020 году специальным постановлением Правительства РФ[182] вводятся типовые программы цифровой трансформации, которые необходимо согласовывать с Минцифрой. Руководители органов теперь будут нести персональную ответственность за их реализацию и достижение программных показателей. Таким образом, вводится программно-целевой принцип с трехлетним горизонтом планирования и ежеквартальной отчетностью. Ответственным за цифровизацию (Chief Digital Transformation Officer, CDTO) будет переданы широкие полномочия для изменения рабочих процессов внутри органов власти. Типизации в таком случае подлежат: типовой должностной регламент заместителя руководителя государственного органа, ответственного за цифровую трансформацию; типовое положение о самостоятельном структурном подразделении государственного органа, ответственного за цифровую трансформацию; типовая форму программы; типовое положение об управлении проектами цифровой трансформации; единая техническая политику реализации программы; методические документы, необходимые для обеспечения функционирования системы управления процессами разработки и реализации программ; правила проверки сведений о мероприятиях по информатизации; порядок формирования кода мероприятия программы и др. В то же время, несмотря на такие серьезные организационные изменения в системе исполнительной власти, по-прежнему важным вопросом остается гармонизация процессов цифровой трансформации не только на федеральном, но и региональном, а также местном уровне. Это происходит

[182] Постановление от 10 октября 2020 года № 1646 «О мерах по обеспечению эффективности мероприятий по использованию информационно-коммуникационных технологий в деятельности федеральных органов исполнительной власти и органов управления государственными внебюджетными фондами» // Официальный сайт Правительства Российской Федерации [Электронный ресурс]. URL: http://government.ru/docs/all/116897/ (дата обращения: 12.12.2021).

со своей спецификой с учетом разного экономического и кадрового потенциала регионов и скорее всего потребует организационных изменений и на этих уровнях власти и управления. Причем с учетом стоимости таких преобразований важное и принципиальное значение может иметь их интеграция с существующей практикой на федеральном уровне.

Несмотря на существенные сдвиги в области организационного обеспечения, *кадровое обеспечение* контрольно-надзорной деятельности по-прежнему испытывает определённые затруднения. В настоящий момент уже разработаны программы для развития цифровых компетенций государственных служащих. Создан Центр подготовки руководителей цифровой трансформации на базе Высшей школы государственного управления РАНХиГС и до 2024 года планируется подготовка порядка 174 тысяч госслужащих по программе «цифрового спецназа»[183]. Тем не менее нехватка кадров в связи с дальнейшей акселерацией процессов цифровой трансформации может только усилиться. По всей видимости здесь нужно принято во внимание сразу несколько факторов и прежде всего повышение интереса для ИТ-специалистов к участию в проектах цифровизации госсектора. Очевидно, что в уровне оплаты труда российский государственный сектор еще долго будет проигрывать коммерческим бизнес-проектам. В таких условиях планы и программы цифровизации непременно должны дополнятся мерами стимулирования к привлечению молодых специалистов к государственному ИТ-сектору, принципиальными акцентами здесь может стать фактор стабильности и возможности приобретения уникального профессионального опыта. В противном случае вряд ли получиться закрыть текущие потребности только за счет программ повышения квалификации и профессиональной переподготовки. Увеличение бюджетных расходов, выраженное в постоянном увеличении количества «бюджетных» мест на ключевых ИТ-направлениях, должно сопровождаться эффективными мерами по повышению привлекательности трудоустройства на критически важных направлениях развития государственного сектора, включая дальнейшее реформирование контрольно-надзорной деятельности.

Преодоление текущих вызовов цифровизации. Данный этап предполагает в некоторой степени проработки ответа на текущие вызовы цифровизации, к наиболее острыми из которых применительно к сфере

[183] ИТ в федеральных ведомствах России // TAdviser. 26 ноября 2021 года [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/Статья:ИТ_в_федеральных_ведомствах_России# (дата обращения: 12.12.2021).

контроля и надзора можно отнести: информационную безопасность, обеспечение прав личности и преодоление социального недоверия. *Обеспечение информационной безопасности цифровизации* является важнейшим аспектом, который необходимо учитывать при разработке планов и программ внедрения цифровых технологий в контрольно-надзорную деятельность. С учетом общей специфики, как уже было отмечено ранее, информационные системы, используемые органами контроля и надзора, в полной мере следует отнести к числу объектов критической информационной инфраструктуры, что в свою очередь требует принятия необходимых правовых, организационных и технических мер по защите информации. Однако не только эти вопросы следует рассматривать в качестве первостепенных. Государственные органы испытывают серьезную нехватку специалистов в области информационной безопасности, что важно учитывать при разработке планов и программ цифровизации и рассматривать в числе прочих мер, с одной стороны, по привлечению соответствующих специалистов, а с другой стороны, компенсирующих мер по повышению эффективности применяемых технических решений и цифровых сервисов. Помимо этого, важным аспектом в обеспечении информационной безопасности является разработка и реализация мер по мониторингу и контролю за тем, как используются информационные технологии сотрудниками органов власти. Часто отсутствие эффективных мер по контролю за действиями сотрудников и реализации мер ответственности существенным образом не только снижает общий уровень информационной безопасности, но и серьезным образом подрывает доверие общества как к самим органам власти, так и применимым цифровым сервисам и решениям. Еще одной необходимой составляющей в обеспечении цифровых сервисов является разрешение вопрос исключительных прав на разрабатываемые программные продукты по заказу и/или в интересах органов контроля и надзора. При заказе и выборе программных продуктов и цифровых сервисов продуктов необходимым является передача всех необходимых прав на полученные разработки, включая исходные программные коды и алгоритмы.

Другой существенной угрозой для цифровизации контроля и надзора может стать *недоверие общества к новым цифровым технологиям* и решениям на их основе. Часто они воспринимаются как попытка *ущемления прав граждан*, вторжения в частную и личную жизнь или нарушение прав предпринимателей. В большинстве случаев срабатывает фактор неизвестности и непонятности того, как они работают и какие

реально опасности они несут. Все это в совокупности потенциально приводит к социальной напряженности, попытке определенных политических сил манипулировать и спекулировать на этих страхах и ожиданиях. Для их преодоления потребуется создание новых в том числе и правовых механизмов по раскрытию достоверной и объективной информации об алгоритмах работы, рисках, последствиях и преимуществах от внедрения новых технологий. Крайне интересной тут является практика во Франции по раскрытию содержания исходного кода, который лежит в основе цифровых государственных сервисов и доступен для изучения и анализа всем желающим. В таком случае исходный программный код рассматривается как «официальный документ», с которым в том числе в какой-то степени регулируется осуществление прав и свобод граждан и законных интересов юридических лиц и как следствие подлежит обязательному опубликованию. Безусловно, тут есть и свои опасности в плане обеспечения информационной безопасности, и не для всех случаев такое решение проблемы было бы приемлемым. С другой стороны, отсутствие информации и часто голословные заверения официальных лиц вряд ли воспринимаются обществом как раскрытие реального положения дел. Еще одним важным шагом является стимулирование и поддержка актуальных научных исследований связанных с оценкой потенциальных рисков цифровизации для общества, государства и личности. В таком случае это усилило бы аргументацию необходимых социальных цифровых трансформаций и позволило бы органам власти корректировать текущую практику внедрения цифровых сервисов и технологий опираясь на мнение научного и экспертного сообщества и фактически путем непосредственного взаимодействия с ним.

По всей видимости программные проекты цифровизации и текущая практика должны быть в равной степени ориентированы не только на создание самих цифровых сервисов и продуктов или внедрение технических решений на основе новых технологий, но также на создание эффективной системы гарантий для контролируемых лиц как граждан, так и организаций. Например, при применении исключительно автоматизированной обработки данных и принятии решений исключительно на их основе, а также в области технологий искусственного интеллекта достаточно давно обсуждается необходимость закрепления «права на человеческое участие», на основании которого можно инициировать принятие или пересмотре человеком решения, принятого ИИ или с его участием. Видится необходимым и в сфере и контроля и надзора рассмот-

реть необходимость/обязательность человеческого участия, создание механизмов и правил критической оценки результата, полученного с использованием цифровых технологий (ИИ) и его учета в системе принятия решений. Достаточно интересной в этом плане практикой является появление нового вида обращений «Я-двойник» Федеральной службы судебных приставов в ответ на участившиеся случаи ошибочного исполнения судебных решений в отношении граждан, имеющих полное совпадение в имени, фамилии и отчестве[184]. Такие случаи стали резонансными и явились причиной серьезной критики в адрес государственных информационных систем и их надежности. В данном случае это стоит рассматривать как пример адресной работы с обращениями граждан и инструмент по снижению социальной напряженности от негативных эффектов цифровизации.

Данные рекомендации и предложения являются своего рода попыткой заострить внимание на важных аспектах, которые стоит учесть как при реализации предлагаемой авторами Концепции внедрения цифровых технологий в сферу контроля и надзора, так и при использовании их в разработке текущих документов, планов и программ цифровизации контрольно-надзорных органов, а также скоординировать текущую практику.

[184] В Интернет-приемной ФССП России создан новый вид обращений для граждан-двойников // Федеральная служба судебных приставов. 22 декабря 2021 года [Электронный ресурс]. URL: https://fssp.gov.ru/pressreleases/document30105677/ (дата обращения: 12.12.2021).

ЗАКЛЮЧЕНИЕ

Таким образом, можно констатировать, что сфера контроля и надзора так же подвержена трансформациям, как в целом и многие другие социальные институты в условиях взрывной цифровизации, охватившей современное общество. Можно с уверенностью сказать, что внедрение современных цифровых технологий в контрольно-надзорную деятельность способствуют появлению новых характеристик этой деятельности, в частности:

1) *анализ и обработка большого массива полученной информации о контролируемом объекте в автоматическом режиме.* Основой контрольно-надзорной деятельности является получение информации о проверяемом объекте, которая сопоставляется с обязательными требованиями. В результате этого сопоставления должностными лицами контрольно-надзорных органов делаются выводы о соблюдении либо не соблюдении обязательных требований подконтрольным (поднадзорным) лицом. Применение современных цифровых технологий, позволяющих в автоматическом режиме и без участия человека, определить на основе полученной информации соблюдаются ли проверяемым лицом обязательные требования или нет, значительно ускоряет процесс проверки, делает его более прозрачным и независимым.

2) *использование в контрольно-надзорной деятельности риск-ориентированного подхода при проведении контрольно-надзорных мероприятий может основываться на современных цифровых технологиях.* Расчет риска может происходить в автоматическом режиме посредством применения суперкомпьютерных вычислений и искусственного интеллекта. В этом плане риск-ориентированный подход становится может рассматриваться как часть автоматизированной деятельности контрольно-надзорных органов.

3) *современные цифровые технологии позволяют исключить непосредственное взаимодействие (контакт) между контрольно-надзорным органов и проверяемым лицом.* С одной стороны, это позволяет минимизировать вмешательство в деятельность проверяемого лица, а это снижает издержки от контрольно-надзорных мероприятий, с другой стороны, обеспечивается более высокая беспристрастность и независимость проверочных мероприятий, исключаются коррупционные риски.

4) *посредством цифровых технологий может обеспечиваться на более высоком уровне взаимодействие между контрольно-надзорными*

органами и проверяемыми лицами. Цифровое взаимодействие может происходить посредством цифровых платформ (цифровых суперсервисов). Например, Единый портал государственных и муниципальных услуг (функций)» (Госуслуги) позволяет в качестве эксперимента подать административную жалобу на действия должностных лиц контрольно-надзорных органов или обжаловать результаты контрольно-надзорных мероприятий (пока в качестве эксперимента).

5) *с помощью современных технологий обеспечивается транспарентность контрольно-надзорной деятельности.* Размещение открытых данных о контрольно-надзорной деятельности в сети Интернет, взаимодействие между органами государственного контроля (надзора) и контролируемыми лицами в электронной форме без непосредственного взаимодействия, электронные платформы и сервисы проверок и самопроверок, позволяет исключить злоупотребление правами должностных лиц контрольно-надзорных органов и исключить коррупционные риски, то есть обеспечивается необходимая открытость и прозрачность контрольно-надзорной деятельности.

Если говорить о дальнейших перспективах внедрения современных цифровых технологий в деятельность органов государственного контроля и надзора, то следует отметить несколько ключевых моментов.

Во-первых, в ближайшие несколько лет планируется создание цифровой платформы мониторинга контроля и надзора в России. Основные задачи проекта – объединить все информационные системы государственных структур, участвующих в контрольно-надзорной деятельности, обеспечив аналитическую обработку этой информации в режиме реального времени на территории всей страны. В рамках этого проекта должны объединиться все созданные в контрольно-надзорной деятельности информационные системы, в том числе уже объединяющиеся сейчас в рамках нового закона о государственном контроле. По нему созданы и запущены в 2020-2021 годах в промышленную эксплуатацию три государственных информационных системы: единый реестр контрольных (надзорных) мероприятий (он приходит на смену Единому реестру проверок, существовавшему в том числе для их согласования с прокуратурой), единый реестр видов контроля и информационная система досудебного обжалования. Таким образом, единая цифровая платформа должна сильно расширить возможности Правительства РФ в контрольно-надзорной деятельности. Это должно произойти за счет доступа к аналитике по всем видам государственного контроля и надзора в режиме реального времени, сопоставления ее с данными ГАС

«Управление» и другими государственными информационными системами, в том числе бюджетными, в результате чего станут возможными детальные и достоверные оценки деятельности контрольно-надзорных органов, результативности контрольно-надзорной деятельности, а также связи особенностей ее устройства в конкретном органе с показателями.

По нашему мнению, создание такой «объединенной» цифровой платформы имеет хорошую перспективу. Безусловно, данная цифровая платформа должна интегрирована другой базовой цифровой платформой – Типовое облачное решение контрольно-надзорной деятельности (ТОР КНД), которая также должна развиваться и совершенствоваться. Амбициозной задачей будет считаться интеграция в единую цифровую платформу и региональных и муниципальных цифровых платформ.

Вместе с тем, как показывает опыт, существуют серьезная опасность повторения судьбы цифровой платформы – Открытое правительство РФ. Это была одна из самых динамично развивающихся цифровых платформ, объединяющая и интегрирующая различные информационные ресурсы других государственных органов. Кроме этого, цифровая платформа Открытого правительства обеспечивала на самом высоком уровне взаимодействие между органами государственной власти, экспертным сообществом, гражданами и организациями. Данный проект планировалось интегрировать с системами открытого правительства зарубежных стран. Однако указанный проект прекратил существование по ряду причин, одной из которых стало широкий доступ граждан к информации о деятельности государственных органов и возможность влиять на принятие ими управленческих решений.

Во-вторых, важным направлением цифровизации контрольно-надзорной деятельности должна стать активное внедрение цифровых технологий в осуществление контрольно-надзорных мероприятий. Так, при осуществлении отдельных видов государственного контроля и надзора начинают внедряться системы дистанционного контроля. 1 февраля 2021 года был запущен эксперимент по внедрению дистанционного контроля промышленной безопасности. Полученные при дистанционном контроле показатели о состоянии промышленной безопасности опасных производственных объектов учитываются Ростехнадзором при осуществлении федерального государственного надзора в области промышленной безопасности.

В соответствии со ст. 96 Федерального закона от 31 июля 2020 г. № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» под мониторингом понимается ре-

жим дистанционного государственного контроля (надзора), заключающийся в целенаправленном, постоянном (систематическом, регулярном, непрерывном), опосредованном получении и анализе информации о деятельности граждан и организаций, об объектах контроля с использованием систем (методов) дистанционного контроля, в том числе с применением специальных технических средств, имеющих функции фотосъемки, аудио- и видеозаписи, измерения, должностными лицами контрольного (надзорного) органа в целях предотвращения причинения вреда (ущерба) охраняемым законом ценностям.

Опрошенные нами должностные лица контрольно-надзорных органов исполнительной власти наиболее перспективными информационными технологиями для осуществления контрольно-надзорной деятельности считают именно системы дистанционного контроля и электронные сервисы проверок (26% респондентов). При этом на втором и третьем местах находятся ответы – технологии искусственного интеллекта (10%), облачные технологии и синхронизированные государственные информационные системы – по 8%.

Безусловно, дальнейшая автоматизация контрольно-надзорных мероприятий, осуществляемых органами государственного контроля и надзора, должна преобладать в большинстве видов контрольно-надзорной деятельности, а более высоким уровнем автоматизации должна стать роботизация контрольно-надзорных действий.

В-третьих, важным условием дальнейшей цифровизации контрольно-надзорной деятельности должно быть внедрение «сквозных» цифровых технологий. Несмотря на наличие стратегического направления в области цифровой трансформации государственного управления, предполагающего активное внедрение в сферу осуществления контрольно-надзорной деятельности такие «сквозных» цифровых технологий как искусственный интеллект, большие данные, интернет вещей, не должны оставаться без развития и другие «сквозные» цифровые технологии: цифровые двойники, мобильные сети связи пятого поколения (цифровые сервисы), новые коммуникационные интернет-технологии, технологии виртуальной и дополненной реальности, технологии распределенных реестров, квантовые коммуникации, квантовые сенсоры, квантовые вычисления, и др.

При этом должна рассматриваться возможность появления ранее неизвестных новых цифровых технологий, которые при широком распространении могут также внедряться в контрольно-надзорную деятельность.

При внедрении «сквозных» цифровых технологий необходимо детально изучать опыт зарубежных стран (США, Китай, Япония, Южная Корея, Германия, Великобритания, и т.д.), которые являются лидерами по внедрению современных «сквозных» цифровых технологий в различные сферы государственного управления, а поэтому могут иметь как положительный, так и негативный опыт по применению таких цифровых технологий.

Нельзя отказываться от взаимодействия с частными компаниями, которые активно внедряют «сквозные» цифровые технологии в свою деятельности. По мотивам обеспечения национальной безопасности приоритет при таком взаимодействии должен отдаваться отечественным частным компаниям.

Безусловно, необходимо учитывать, что сами по себе «сквозные» цифровые технологии требуют колоссальных затрат со стороны государства, а поэтому при внедрении подобных в контрольно-надзорную деятельность должно детально просчитываться финансовая составляющая, то есть внедрение «сквозных» технологий должно обосновываться высокой эффективность и результативностью государственного контроля и надзора, возможностью за счет этих цифровых технологий предотвратить угрозы жизни и здоровью большого числа граждан, либо предотвратить значительный материальный ущерб окружающей среди или имуществу граждан и организаций.

В-четвертых, цифровизация государственного контроля и надзора должна быть интегрирована с другими сферами государственного управления, в которых активно применяются современные цифровые технологии. Цифровые технологии, применяемые в контрольно-надзорной деятельности, должны предоставлять возможность интеграции с другими информационно-коммуникационными системами, прежде всего, такими как «Умный город», «Безопасный город», «Интеллектуальные транспортные системы», «Умное производство», «Умная ферма», «Цифровая медицина», высокоавтоматизированные информационные системы налогообложения и таможенного декларирования, и т.д.

Необходима интеграция и распространение цифровых (мобильных) приложений для смартфонов и планшетов, пользователями которых будут являться должностные лица контрольно-надзорных органов и контролируемые лица.

Важный акцент должен быть сделан на цифровых платформах, которые будут интегрированы в цифровую платформу контрольно-над-

зорной деятельности, позволяющие осуществлять общественный контроль и общественное взаимодействие органов государственного контроля и надзора, и контролируемых лиц.

В-пятых, необходимо дальнейшее расширение сферы действия Федерального закона от 31 июля 2020 г. №248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации», осуществляющего правовое регулирование вопросов информационного обеспечения государственного контроля (надзора), муниципального контроля. Положения указанного Федерального закона должны совершенствоваться по мере внедрения в деятельность контрольно-надзорных органов современных цифровых технологий.

Следует также признать успешным опыт введения экспериментальных правовых режимов по применению современных цифровых технологий при осуществлении отдельных видов государственного контроля и надзора.

Все вышеперечисленные направления внедрения передовых цифровых технологий в контрольно-надзорную деятельность способствуют формированию новой правовой концепции современной системы государственного контроля и надзора, а также муниципального контроля.

Более того, проведенное нами изучение нормативной основы для внедрения цифровых технологий и фактических процессов автоматизации контрольно-надзорных органов *подтверждают нашу гипотезу, что все без исключения направления (виды) контрольно-надзорной деятельности подвержены в настоящий момент подвержены глубокой цифровизации*, что в свою очередь **трансформирует (изменяет) основную цель государственного контроля и надзора**, которая изначально была связана с обеспечением законности в деятельности контролируемых лиц, предупреждением и профилактикой нарушений обязательных требований, недопущением нарушений требований нормативных правовых актов, и минимизацией ущерба в случаях нарушений законности, то в настоящее время, к этому всему добавляется еще управляемое воздействие, основанное на современных цифровых технологиях, позволяющих минимизировать участие человека при принятии управленческих решений в контрольно-надзорной деятельности и тем самым исключить необоснованное вмешательство в деятельность хозяйствующих субъектов и граждан.

Исходя из определяемых приоритетов внедрения цифровых технологий и автоматизации контрольно-надзорной деятельности, установленных государством для контрольно-надзорных органов, **трансфор-**

мируются и задачи государственного контроля и административного надзора. По нашему мнению, к таким новым задачам государственного контроля и административного надзора следует отнести:

1) минимизация административного воздействия на хозяйствующих субъектов и граждан, не препятствующее и не создающее помехи их нормальной деятельности, при проверке соблюдениями ими обязательных требований;

2) приоритет использования «бесконтактного» государственного контроля и надзора, то есть приоритет при осуществлении контрольно-надзорной деятельности контрольно-надзорным мероприятиям без взаимодействия с контролируемым лицом;

3) оценка эффективности и результативности контрольно-надзорной деятельности с точки зрения оказания позитивного влияния на развитие цифровой экономики Российской Федерации;

4) возможность взаимодействия контрольно-надзорных органов с контролируемыми лицами по вопросам внедрения в контрольно-надзорную практику передовых («сквозных») цифровых технологий и стимулирование для проверяемых лиц (например, путем установления лояльных или мягких режимов осуществления контрольно-надзорных мероприятий);

5) проведение контрольно-надзорных мероприятий на основе больших данных и другой информации, получаемой в ходе использования современных цифровых дистанционных технологий;

6) роботизация контрольно-надзорных мероприятий, требующих проведение проверки в условиях, представляющих реальную опасность для проверяющих лиц;

7) моделирование различных ситуаций (поведенческих, производственных, технологических и т.д.) посредством использования современных цифровых технологий (искусственного интеллекта, квантовых вычислений, виртуальной и дополненной реальности, цифровых двойников), позволяющее на основе данных вычислений проводить более эффективные контрольно-надзорные мероприятия;

8) учет объектов государственного контроля и надзора должен осуществляться с использованием современных цифровых технологий.

Необходимо обратить внимание и на **изменение принципов государственного контроля и надзора**. Так, к общим принципам государственного контроля и надзора, закрепленным в главе 2 федеральным законом от 31 июля 2020 г. № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» добав-

ляются еще и специальные принципы, которые определяют порядок использования современных цифровых технологий при осуществлении государственного контроля и надзора (например, принципы применения искусственного интеллекта при осуществлении государственного контроля и надзора; принципы использования больших данных в контрольно-надзорной деятельности; принципы интернета вещей в контрольно-надзорной деятельности; и т.д.).

Системный анализ законодательства РФ показывает, что *формы государственного контроля и надзора* характеризуют саму деятельность органов исполнительной власти и их должностных лиц при осуществлении государственных функций по контролю и надзору, включающую в себя контрольно-надзорные мероприятия (контрольная закупка; мониторинговая закупка; выборочный контроль; инспекционный визит; рейдовый осмотр; документарная проверка; выездная проверка). Когда как *методы государственного контроля и надзора* отражают именно характер оказываемого управленческого воздействия (способы административного воздействия, подходы при осуществлении административного воздействия и контрольно-надзорные действия).

По нашему мнению, **систему методов государственного контроля и надзора можно представить следующим образом**:

1) общие методы государственного контроля и надзора:

а) предъявление обязательных для исполнения требований (по даче объяснений, по предоставлению или истребованию документов, по допуску на проверяемый объект и т.д.);

б) установление ограничений и запретов (например, на совершение финансовых операций при проведении проверки; запрет и ограничение на эксплуатацию опасного производственного объекта при проведении проверки, запрет на внесение изменений в документацию и технологическое оборудование при проведении проверки и т.п.);

в) анализ полученных результатов в ходе мониторинга;

г) процессуальное (процедурное) документирование контрольно-надзорных мероприятий и контрольно-надзорных действий (составление акта проверки);

д) выдача предписаний по результатам государственного контроля (надзора);

е) проведение профилактических мероприятий.

2) специальные методы государственного контроля и надзора:

а) риск-ориентированный подход (метод);

б) дистанционный контроль (мониторинг);

в) постоянный государственный контроль (надзор);

г) постоянный рейд;

д) контрольно-надзорные действия (осмотр; досмотр; опрос; получение письменных объяснений; истребование документов; отбор проб (образцов); инструментальное обследование; испытание; экспертиза; эксперимент).

В современной концепции государственного контроля и административного надзора появляется такой новый элемент, ранее не обозначаемый в качестве основного элемента содержания государственного контроля и государственного надзора, как *технологии контрольно-надзорной деятельности*.

С учетом сказанного можно обозначить **ключевые элементы разработанной авторами и предлагаемой к внедрению Концепции правового регулирования использования информационных технологий в сферу контроля и надзора в условиях цифровых трансформаций (цифровой экономики).**

Первый элемент: Понятие и сущность государственного контроля и административного надзора. **Под государственным контролем** понимается деятельность органов публичной власти, направленная на предупреждение, выявление и пресечение нарушений обязательных требований и иных требований законности, осуществляемая в рамках общей функции управления, в отношении подчиненных органов публичной власти и их должностных лиц, а также подведомственных организаций, посредством использования информационных технологий и проведения профилактических мероприятий нарушений обязательных требований и иных требований, установленных ведомственными нормативными актами, оценки соблюдения контролируемыми лицами указанных требований, пресечения нарушений обязательных и иных требований, с целью обеспечения законности и целесообразности деятельности контролируемых лиц, и принятия мер дисциплинарного и иного организационно-правового характера в отношении контролируемых лиц.

Под административным (государственным) надзором понимается деятельность органов государственного надзора, направленная на предупреждение, выявление и пресечение обязательных требований, осуществляемая в отношении граждан, организационно неподчиненных должностных лиц, организаций и учреждений, с использованием информационных и цифровых технологий для автоматизации деятельности, посредством профилактики нарушений обязательных требований, оценки соблюдения организационно неподчиненными гражданами,

должностными лицами, организациями и учреждениями обязательных требований, выявления их нарушений, принятие предусмотренных законодательством Российской Федерации по пресечению выявленных нарушений обязательных требований, устранению их последствий и (или) восстановлению правового положения, существовавшего до возникновения таких нарушений, и наделенных полномочиями по возбуждению дел об административных правонарушениях и (или) привлечению виновных лиц к административной ответственности.

Сущность государственного контроля состоит в том, что это является универсальной формой деятельности органов публичной власти, в том числе контрольными полномочиями наделены и органы государственного надзора (например, при осуществлении лицензионного контроля, контроля за переданными надзорными полномочиями другим органам публичной власти). Он осуществляется всеми без исключения органами публичной власти, а поэтому рассматривается в качестве общей функции управления. При этом органами государственной власти могут применяться различные формы и методы государственного контроля, которые могут закрепляться как в законах, так и подзаконных нормативных правовых актах, так и в ведомственных нормативных правовых актах. Целью государственного контроля является обеспечение законности и дисциплины в деятельности подчиненных и подведомственных органов, организаций и учреждений, а также должностных лиц, которые оцениваются не только с точки зрения соблюдения обязательных требований, но и их иных требований, а также дается оценка целесообразности и эффективности деятельности контролируемых лиц. Меры административного воздействия включают дисциплинарную ответственность, организационные и материально-технические мероприятия. Цифровые средства государственного контроля и автоматизация контрольной деятельности прежде всего направлена на своевременное и полное получение необходимой информации о деятельности контролируемого лица. При этом согласия на применение информационных или цифровых технологий от контролируемого лица не требуется.

Сущность административного надзора заключается в административно-правовом воздействии на граждан, организационно неподчиненных должностных лиц, организаций и учреждений, деятельность которых оценивается исключительно с точки зрения законности. Способы государственного надзора разнообразны, но ограничены на уровне законов (то есть формы и методы государственного надзора должны

быть закреплены законом, а не другим каким-то нормативным актом). Большинство органов государственного надзора используют в своей деятельности риск-ориентированный подход (метод). Административный надзор осуществляется уполномоченными органами государственного надзора и специальными должностными лицами – инспекторами. При административном надзоре происходит влияние и ограниченное вмешательство в деятельность поднадзорных лиц, которое должно быть снижено за счет автоматизации надзорной деятельности и применения современных информационных и цифровых технологий, и не приносить непоправимого ущерба экономическим отношениям. Цифровизация государственного надзора позволяет надзорным органам осуществлять эффективное взаимодействие с гражданами, организационно неподчиненными должностными лицами, организациями и учреждениями, проводить надзорные мероприятия без личного взаимодействия с поднадзорными лицами, что снижает коррупционные риски и благоприятно влияет на развитие «Цифровой экономики». Государственный надзор может реализовываться посредством профилактики соблюдения обязательных требований, подготовки, планирования и проведения надзорных мероприятий, применения специальных административно-правовых режимов (режим постоянного государственного надзора), применения по пресечению выявленных нарушений обязательных требований, устранению их последствий и (или) восстановлению правового положения, существовавшего до возникновения таких нарушений, а также что очень важно путем возбуждения дел об административных правонарушения и (или) привлечения виновных лиц к административной ответственности. Органы государственного надзора могут устанавливать обязательные требования для граждан, организационно неподчиненных должностных лиц, организаций и учреждений.

Второй элемент: современные цели и задачи государственного контроля и административного надзора.

Третий элемент: общие и специальные принципы государственного контроля и административного надзора.

Четвертый элемент: правовые основы государственного контроля и административного надзора.

Пятый элемент: основные направления контрольно-надзорной деятельности (профилактическая деятельность; планирование, подготовка и проведение контрольных (надзорных) мероприятий; применение специальных административно-правовых режимов государственного контроля и надзора; интеграционная деятельность по привлечению к адми-

нистративной ответственности по результатам проведения контрольно-надзорных мероприятий; досудебное обжалование решений контрольно-надзорных органов и их должностных лиц; и другое).

Шестой элемент: современные формы и методы государственного контроля и административного надзора, в том числе основанные на современных цифровых технологиях.

Седьмой элемент: автоматизация контрольно-надзорной деятельности.

Восьмой элемент: технологии контрольно-надзорной деятельности. Условия применения цифровых технологий в контрольно-надзорной деятельности.

Девятый элемент: контрольно-надзорные мероприятия и контрольно-надзорные действия, в том числе осуществляемые с использованием цифровых технологий.

Десятый элемент: Взаимодействие органов государственного контроля (надзора) и контролируемых лиц, в том числе информационное взаимодействие.

Одиннадцатый элемент: Исполнение принятых решений при осуществлении государственного контроля и административного надзора, в том числе с использованием цифровых технологий.

Двенадцатый элемент: пересмотр решений, принятых по результатам проведения контрольно-надзорных мероприятий, досудебное обжалование решений контрольно-надзорных органов и их должностных лиц в электронной форме.

Более подробное описание каждого из указанных элементов нашло отражение в данной монографии и других публикациях участников научного коллектива исследования. Вместе с тем, стоит отметить, что помимо общих теоретических выводов членами научного коллектива с учетом научной специализации были предложены и отраслевые вывод и предложения по отдельным направления контрольно-надзорной деятельности, которые раскрывают, органично дополняют, а также обосновывают необходимость дальнейшего практического внедрения разработанной Концепции.

В части *контроля и надзора за обеспечением правопорядка и общественной безопасности* необходимо отметить следующее:

во-первых, в условиях цифровизации происходит трансформация основных элементов государственного контроля и надзора за обеспечением правопорядка и общественной безопасности;

во-вторых, возможность использования искусственного интеллекта как самостоятельного субъекта контрольно-надзорной деятельности в

условиях российской правовой действительной исключена. Однако данные технологии могут эффективно применяться в правовых формах и методах государственного контроля и надзора за обеспечением правопорядка и общественной безопасности;

в-третьих, происходит усложнение объекта контроля и надзора за обеспечением правопорядка и общественной безопасности в связи с внедрением современных информационных технологий в социальную сферу, что обуславливает необходимость цифровой трансформации правовых форм и методов рассматриваемого вида государственного контроля и надзора;

в-четвертых, в сфере контроля и надзора за обеспечением общественной безопасности и правопорядка прорывные информационные технологии находят отражение в такой форме государственного контроля и надзора как документарная проверка и наблюдение за соблюдением обязательных требований;

в-пятых, в сфере контроля и надзора за обеспечением общественной безопасности и правопорядка прорывные информационные технологии используются при применении такого общего метода государственного контроля и надзора как проведение профилактических мероприятий, а также таких специальных методов как дистанционный государственный контроль (мониторинг) и контрольно-надзорные действия в форме осмотра и инструментального обследования;

в-шестых, в сфере контроля и надзора за обеспечением общественной безопасности и правопорядка технологии ближайшего будущего могут применяться для реализации таких общих методов государственного контроля и надзора как анализ полученных результатов в ходе мониторинга и процессуальное (процедурное) документирование контрольно-надзорных мероприятий и контрольно-надзорных действий (составление акта проверки), а также такие специальные методы как дистанционный государственный контроль (мониторинг), риск-ориентированный подход, контрольно-надзорные действия в виде инструментального обследования и эксперимента.

В области контроля и надзора в сфере фармакологии и медицины представляется необходимым внесение изменений в действующее законодательство в сфере обращения лекарственных средств, а также практику его применения в направлении реализации целостной концепции правового регулирования информатизации контрольно-надзорной деятельности.

Во-первых, это касается содержания Закона об обращении лекарственных средств. В нем, как в базовом правовом акте данной сферы,

важно закрепить основы информационного обеспечения контрольно-надзорной деятельности за обращением лекарств путем введения дополнительных норм в главу 4, закрепляющих перечень используемых государственных информационных систем, содержащиеся в них сведения, функциональную направленность таких систем, основы их взаимодействия между собой.

Во-вторых, цифровые технологии оказывают заметное влияние на изменение форм и методов государственного контроля и надзора, которые включают в себя, помимо прочего, и контрольно-надзорные мероприятия. Такие изменения должны быть отражены в законодательстве, и в первую очередь – в Законе об обращении лекарственных средств. Например, появилась дистанционная контрольная закупка лекарственных средств, позволяющая выявить нарушения обязательных требований при реализации лекарств дистанционным способом (в подавляющем большинстве она осуществляется посредством сети Интернет). Такую форму проведения контрольно-надзорной деятельности необходимо закрепить Законом об обращении лекарственных средств (а не только административным регламентом) в соответствующем перечне контрольно-надзорных мероприятий, ведь процедура ее проведения значительно отличается от стандартной контрольной закупки. Более того, согласно сведениям, представленным в Едином реестре проверок, за почти полуторагодовалый срок существования дистанционной реализации лекарственных средств не было произведено ни одной дистанционной контрольной закупки лекарств. Необходимо, чтобы такая форма проведения контрольно-надзорного мероприятия не игнорировалась и применялась уполномоченными должностными лицами (безусловно, при наличии на то правовых оснований) для качественной проверки соблюдения обязательных требований к осуществлению торговли лекарствами дистанционно. Особенно это актуально в период пандемии, когда такой способ приобретения медикаментов пользуется большой популярностью у потребителей.

В-третьих, разрозненные отдельные положения подзаконных актов по поводу использования информационных технологий в контрольно-надзорной деятельности важно дополнить, систематизировать, привести к единому знаменателю. Представляется недостаточным лишь указание в них на обязанность размещения той или информации на официальном сайте Росздравнадзора или в ином электронном источнике. Подзаконные акты о проведении государственного контроля (надзора) в сфере обращения лекарственных средств должны содержать исчерпывающие

перечни используемых цифровых технологий и правила их функционирования. Представляется целесообразным отразить данные сведения в постановлении Правительства РФ «О федеральном государственном контроле (надзоре) в сфере обращения лекарственных средств», а также в Административном регламенте Росздравнадзора по осуществлению федерального государственного надзора в сфере обращения лекарственных средств. При этом ныне существующие информационные письма и методические рекомендации, не имеющие статуса нормативно-правового акта, не должны подменять собой полноценное правовое регулирование в данной сфере.

Кроме того, проблемным является вопрос о правовой базе используемых в контрольно-надзорной деятельности информационных систем. О большинстве из них только вскользь упоминается в отдельных подзаконных актах, а некоторым в большей или меньшей степени посвящены лишь письма Росздравнадзора. Полноценное правовое регулирование свойственно лишь ФГИС МДЛП. По этой причине целесообразным является разработка и принятие единого правового акта в форме приказа Росздравнадзора, утверждающего положение об АИС Росздравнадзора (как это реализовано в некоторых иных сферах контрольно-надзорной деятельности).

Вместе с этим, как показал анализ правовых документов и иной официальной информации открытого доступа, сложности возникают и в разграничении ряда понятий, используемых относительно цифровизации Росздравнадзора, так как одна и та же информационная система в разных источниках может иметь статус самостоятельной автоматизированной системы, подсистемы иной системы, сервиса или раздела сайта. Для его разрешения необходимо закрепить в положении об АИС Росздравнадзора определения ключевых понятий: автоматизированная информационная система, подсистема автоматизированной информационной системы, электронный сервис. С целью поддержания единообразия в правовом регулировании мы обратились к нормативно-правовым актам, раскрывающим подобные этим понятия, но распространяющим свое действие на иные сферы общественной жизни, что позволило нам сформулировать следующие возможные варианты легальных определений обозначенных понятий:

1. *автоматизированная информационная система (АИС) Росздравнадзора* – совокупность программно-аппаратных средств, образующих единую информационную систему Росздравнадзора, обеспечивающую автоматизацию деятельности Росздравнадзора по всем выполняемым им функциям;

2. *подсистема АИС Росздравнадзора* – составная часть АИС Росздравнадзора, позволяющая автоматизировать отдельные функции Росздравнадзора;

3. *электронный сервис Росздравнадзора* – функциональное решение, размещенное на официальном сайте Росздравнадзора или Едином портале государственных услуг, позволяющее получить государственную услугу, информацию из АИС Росздравнадзора или подать обращение в Росздравнадзор.

Такое разграничение понятий позволяет сделать вывод, что из рассмотренных нами систем к подсистемам АИС Росздравнадзора относятся «Фармаконадзор», «Мониторинг качества лекарственных средств» и «Выборочный контроль», а к электронным сервисам – «Сведения о лекарственных средствах, вводимых в гражданский оборот в Российской Федерации», «Поиск изъятых из обращения лекарственных средств», «Поиск писем по контролю качества лекарственных средств». Причем называть данные подсистемы и электронные сервисы самостоятельными автоматизированными системами представляется некорректным.

Таким образом, правовое регулирование применения цифровых технологий в государственном контроле и надзоре за обращением лекарственных средств должно получить свое выражение в иерархической системе правовых актов. При этом важно, чтобы оно шло в ногу со временем, не оставляя в дальнейшем без регламентации новые проявления цифровизации в данной государственной деятельности.

Применительно к *контролю и надзору в информационной сфере* было отмечено, что внедрение цифровых технологий в контрольно-надзорную деятельность позволяет развивать такие формы контрольно-надзорной деятельности как регулярное и систематическое наблюдение - мониторинг и анализ состояния подконтрольной сферы и ее объектов без непосредственного взаимодействия с объектами контроля. Предупреждение должно быть главной целью контрольно-надзорной деятельности, карательная же функция контрольно- надзорной деятельности должна служить крайней мерой, используемой только в отношении злостных нарушителей, не желающих выстраивать диалог с государством, выгодный для обеих сторон. Внедрение цифровых технологий в контрольно-надзорную деятельность будет способствовать исчезновению архаичных принципов работы государственных органов, которые формировали настороженное отношение подконтрольных субъектов и мешали организации новой модели взаимодействия.

Цифровизация контрольно-надзорной деятельности безусловно приведет к сокращению числа государственных служащих контрольно-надзорных органов исполнительной власти, осуществляющих кон-

трольно-надзорные функции в информационной сфере. С одной стороны, сокращение числа государственных служащих можно назвать недостатком цифровизации, так как это способствует возникновению социальной напряженности и увеличению уровню безработицы. Факт сокращения числа чиновников в результате цифровизации государственного управления известен и очевиден уже давно. Но с точки зрения нагрузки на финансирование контрольно-надзорной деятельности, в долгосрочной перспективе, цифровизация обеспечит значительную экономию бюджетных средств. Высвободившиеся средства могут быть потрачены либо на дальнейшую модернизацию государственного управления, либо смогут быть потрачены на иные статьи расходов государства, но в любом случае сокращение численности государственных служащих контрольно-надзорных органов на треть приведет к колоссальной экономии.

Кроме того, активное использование цифровых технологий в контрольно-надзорной деятельности способствует упрощению взаимодействия между органами федеральной исполнительной власти, осуществляющими контрольно-надзорную деятельность в информационной сфере, а также в перспективе могут быть использованы и для международного сотрудничества в указанной сфере.

Внедрение цифровых технологий в контрольно-надзорную деятельность позволяет создать условия не только для оперативного выявления нарушений, но и для развития такой формы контроля, как регулярное и систематическое наблюдение - мониторинг и анализ состояния подконтрольной сферы и ее объектов без непосредственного взаимодействия с объектами контроля. То есть контрольно-надзорные органы могут предугадывать и ликвидировать непосредственно возникающие угрозы и риски, предупреждая возникновение правонарушений и дальнейшего ущерба для подконтрольной среды, что выступает несомненным плюсом для всех участников контрольно-надзорной деятельности в информационной сфере, как для подконтрольных субъектов, так и для контроллеров.

Сфера *промышленного контроля и надзора* также становится объектом последовательного внедрения цифовых технологий. Можно отметить следующие тенденции в развитии форм и методов государственного контроля (надзора) в сфере промышленности:

Во-первых, имеется выраженная тенденция к дальнейшей цифровизации контроля и надзора в сфере промышленной безопасности в части разработки и создания единых информационных систем, интегрированных как с другими смежными ведомствами, так и в отдельных случаях с

информационными системами контролируемых лиц для мониторинга безопасности;

Во-вторых, в настоящий момент цифровые технологии активно используются в той или иной степени для осуществления практически всех контрольно-надзорных действий и мероприятий, а также профилактических мероприятий;

В-третьих, существенные перспективы для повышение эффективности деятельности контрольно-надзорных органов открывают технологи промышленного интернета (интернета вещей), интегрированные с технологиями искусственного интеллекта, больших данных и цифровых двойников».

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

I. Международные нормативно-правовые акты

1. Европейская этическая хартия об использовании искусственного интеллекта в судебных системах и окружающих их реалиях, принята на 31-м пленарном заседании ЕКЭП (Страсбург, 3-4 декабря 2018 года) // URL: https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c (дата обращения: 30.10.2021).

II. Нормативно-правовые акты Российской Федерации

2. Закон Российской Федерации о поправке к Конституции РФ от 14 марта 2020 г. № 1-ФКЗ «О совершенствовании регулирования отдельных вопросов организации и функционирования публичной власти» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001202003140001 (дата обращения: 12.12.2021).

3. Федеральный закон от 8 августа 2001 г. № 134-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при проведении государственного контроля (надзора)» // СЗ РФ. – 2001. – № 33 (часть 1). – Ст. 3436.

4. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ // СЗ РФ. – 2002. – № 1 (ч. 1). – Ст. 1.

5. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. – 2006. – № 31 (часть 1). – Ст. 3448.

6. Федеральный закон от 26 декабря 2008 г. № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» // СЗ РФ. – 2008. – № 52 (часть 1). – Ст. 6249.

7. Федеральный закон от 12 апреля 2010 г. № 61-ФЗ «Об обращении лекарственных средств» // Российская газета. – 2010. – № 78; 2021. – № 133.

8. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Официальный интернет-портал правовой информации [Элек-

тронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001201707260023 (дата обращения: 12.12.2021).

9. Федеральный закон от 31 июля 2020 г. № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» // СЗ РФ. – 2020. – № 31 (часть 1). – Ст. 5007.

10. Указ Президента РФ от 9 марта 2004 г. № 314 «О системе и структуре федеральных органов исполнительной власти» // СЗ РФ. – 2004. – № 11. – Ст. 945.

11. Концепция общественной безопасности в Российской Федерации, утверждена Президентом РФ 14 ноября 2013 г. № Пр-2685) // СПС «КонсультантПлюс» [Электронный ресурс]. URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=154602&dst=1000000001%2C0#U9RXtkSbOlD7FS05 (дата обращения: 01.09.2021).

12. Указ Президента Российской Федерации от 5 декабря 2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Официальный интернет портал правовой информации [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001201612060002 (дата обращения: 12.12.2021).

13. Стратегия развития информационного общества в Российской Федерации на 2017 – 2030 годы, утвержденная Указом Президента РФ от 9 мая 2017 г. № 203 // СЗ РФ. – 2017. – № 20. – Ст. 2901.

14. Указ Президента Российской Федерации от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» // официальный сайт Президента РФ [Электронный ресурс]. URL: http://www.kremlin.ru/acts/bank/43027 (дата обращения: 02.08.2021).

15. Национальная стратегия развития искусственного интеллекта на период до 2030 года, утвержденная Указом Президента РФ от 10 октября 2019 г. № 490 // СЗ РФ. – 2019. – № 41. – Ст. 5700.

16. Указ Президента РФ от 21 июля 2020 г. № 474 «О национальных целях развития Российской Федерации на период до 2030 года» // СЗ РФ. – 2020. – № 30. – Ст. 4884.

17. Указ Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001202107030001?index=18&rangeSize=1 (дата обращения: 01.09.2021).

18. Паспорт приоритетной программы «Реформа контрольной и надзорной деятельности» (приложение к протоколу президиума Совета

при Президенте РФ по стратегическому развитию и приоритетным проектам от 21 декабря 2016 № 12) // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

19. Паспорт национального проекта «Безопасные и качественные автомобильные дороги», утвержден президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам, протокол № 15 от 24 декабря 2018 г. // официальный сайт «Росавтодор» [Электронный ресурс]. URL: http://static.government.ru/media/files/rBdyoIr3S9IDP8Q87lXXYaktpKWGc0NY.pdf (дата обращения: 15.09.2021).

20. Паспорт федерального проекта «Цифровое государственное управление», утвержден президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности, протокол № 9 от 28 мая 2019 г. // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

21. Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации», утвержден президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол № 7 от 4 июня 2019 г. // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

22. Паспорт приоритетного проекта «Автоматизация контрольно-надзорной деятельности», утвержден протоколом заседания проектного комитета от 27 января 2017 г. № 5 // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

23. Методические рекомендации по организации и проведению публичных обсуждений результатов правоприменительной практики, руководств по соблюдению обязательных требований органа государственного контроля (надзора) (приложение к протоколу заседания проектного комитета по основному направлению стратегического развития «Реформа контрольной и надзорной деятельности» от 21 февраля 2017 г. № 13(2)) // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

24. Комплексные требования к информационным системам, обеспечивающим выполнение контрольно-надзорных функций органами исполнительной власти (Стандарт информатизации контрольно-надзорной деятельности), утверждены протоколом заседания проектного комитета от 14 июня 2017 г. № 40(6)) // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

25. Паспорт приоритетного проекта «Автоматизация контрольно-надзорной деятельности», утвержден протоколом заседания проектного комитета от 20 декабря 2017 г. № 78(14) // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

26. Паспорт реализации проекта «Совершенствование функции государственного надзора в сфере здравоохранения в рамках реализации приоритетной программы Реформа контрольной и надзорной деятельности», утвержден протоколом заседания проектного комитета от 13 февраля 2018 г. № 1 // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

27. Постановление Правительства РФ от 16 марта 2009 г. № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» // СЗ РФ. – 2009. – № 12. – Ст. 1431.

28. Постановление Правительства РФ от 8 июня 2011 г. № 451 «Об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001202103310017 (дата обращения: 12.12.2021).

29. Положение о режиме постоянного государственного надзора на объектах использования атомной энергии, утвержденное постановлением Правительства РФ от 23 апреля 2012 г. № 373 // СЗ РФ. – 2012. – № 18. – Ст. 2233.

30. Постановление Правительства РФ от 15 апреля 2014 г. № 313 (ред. от 31.03.2021) «Об утверждении государственной программы Российской Федерации “Информационное общество”» // СПС «КонсультантПлюс» [Электронный ресурс]. URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=382395&dst=145502%2C0#2D1qxeScfe4DGXd81 (дата обращения: 02.08.2021).

31. Постановление Правительства РФ от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102382688 (дата обращения: 12.12.2021).

32. Постановление Правительства РФ от 17 августа 2016 г. № 806 «О применении риск-ориентированного подхода при организации отдельных видов государственного контроля (надзора) и внесении изме-

нений в некоторые акты Правительства Российской Федерации» // СЗ РФ. – 2016. – № 35. – Ст. 5326.

33. Постановление Правительства РФ от 10 февраля 2017 г. № 166 «Об утверждении Правил составления и направления предостережения о недопустимости нарушения обязательных требований, подачи юридическим лицом, индивидуальным предпринимателем возражений на такое предостережение и их рассмотрения, уведомления об исполнении такого предостережения» // СЗ РФ. – 2017. – № 8. – Ст. 1239.

34. Положение о государственной информационной системе «Типовое облачное решение по автоматизации контрольной (надзорной) деятельности», утвержденное постановлением Правительства РФ от 21 апреля 2018 г. № 482 // СЗ РФ. – 2018. – № 18. – Ст. 2633.

35. Постановление Правительства Российской Федерации от 8 июня 2018 г. № 658 «О централизованных закупках офисного программного обеспечения, программного обеспечения для ведения бюджетного учета, а также программного обеспечения в сфере информационной безопасности» // Официальный сайт Правительства Российской Федерации [Электронный ресурс]. URL: http://government.ru/docs/all/116897/ (дата обращения: 12.12.2021).

36. Постановление Правительства РФ от 14 декабря 2018 г. № 1556 «Об утверждении Положения о системе мониторинга движения лекарственных препаратов для медицинского применения» // СЗ РФ. – 2018. – № 53 (часть I). – Ст. 8641; № 27 (часть III). – Ст. 5445.

37. Постановление Правительства РФ от 14 декабря 2018 г. № 1557 «Об особенностях внедрения системы мониторинга движения лекарственных препаратов для медицинского применения» // СЗ РФ. – 2018. – № 53 (часть I). – Ст. 8642.

38. Постановление Правительства РФ от 14 декабря 2018 г. № 1558 «Об утверждении Правил размещения общедоступной информации, содержащейся в системе мониторинга движения лекарственных препаратов для медицинского применения, в информационно-телекоммуникационной сети «Интернет» (в том числе в форме открытых данных)» // СЗ РФ. – 2018. – № 53 (часть I). – Ст. 8643.

39. Постановление Правительства РФ от 26 ноября 2019 г. № 1510 «О порядке ввода в гражданский оборот лекарственных препаратов для медицинского применения» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://www.pravo.gov.ru (дата обращения: 24.10.2021).

40. Постановление Правительства РФ от 1 октября 2020 г. № 1586 «Об утверждении Правил перевозок пассажиров и багажа автомобиль-

ным транспортом и городским наземным электрическим транспортом» // СЗ РФ. – 2020. – № 41. – Ст. 6428.

41. Постановление Правительства РФ от 10 октября 2020 года № 1646 «О мерах по обеспечению эффективности мероприятий по использованию информационно-коммуникационных технологий в деятельности федеральных органов исполнительной власти и органов управления государственными внебюджетными фондами» // Официальный сайт Правительства Российской Федерации [Электронный ресурс]. URL: http://government.ru/docs/all/116897/ (дата обращения: 12.12.2021).

42. Постановление Правительства РФ от 31 декабря 2020 г. № 2415 «О проведении эксперимента по внедрению системы дистанционного контроля промышленной безопасности» // СЗ РФ. – 2021. – № 3. – Ст. 557.

43. Постановление Правительства РФ от 25 июня 2021 г. № 994 «Об утверждении Положения о федеральном государственном контроле (надзоре) в области семеноводства в отношении семян сельскохозяйственных растений» // СЗ РФ. – 2021. – № 27 (часть 2). – Ст. 5382.

44. Постановление Правительства РФ от 25 июня 2021 г. № 995 «Об утверждении Положения о федеральном государственном карантинном фитосанитарном контроле (надзоре)» // СЗ РФ. – 2021. – № 27 (часть 2). – Ст. 5383.

45. Постановление Правительства РФ от 25 июня 2021 г. № 1005 «Об утверждении Положения о федеральном государственном контроле (надзоре) в области защиты прав потребителей» // СЗ РФ. – 2021. – № 27 (часть 2). – Ст. 5392.

46. Постановление Правительства РФ от 25 июня 2021 г. № 1007 «О федеральном государственном надзоре в области гражданской обороны» // СЗ РФ. – 2021. – № 27 (часть 2). – Ст. 5394.

47. Постановление Правительства РФ от 25 июня 2021 г. № 1013 «О федеральном государственном надзоре в области защиты населения и территорий от чрезвычайных ситуаций» // СЗ РФ. – 2021. – № 27 (часть 2). – Ст. 5400.

48. Постановление Правительства РФ от 25 июня 2021 г. № 1014 «Об утверждении Положения о федеральном государственном контроле (надзоре) за безопасностью людей на водных объектах» // СЗ РФ. – 2021. – № 27 (часть 2). – Ст. 5401.

49. Постановление Правительства РФ от 25 июня 2021 г. № 1015 «О федеральном государственном пробирном надзоре» // СЗ РФ. – 2021. – № 27 (часть 3). – Ст. 5402.

50. Постановление Правительства РФ от 25 июня 2021 г. № 1020 «Об утверждении Положения о федеральном государственном контроле (надзоре) за соблюдением законодательства Российской Федерации о средствах массовой информации» // СЗ РФ. – 2021. – № 28. – (Часть I). – Ст. 5503.

51. Постановление Правительства РФ от 29 июня 2021 г. № 1046 «О федеральном государственном контроле (надзоре) за обработкой персональных данных» (вместе с «Положением о федеральном государственном контроле (надзоре) за обработкой персональных данных») // СЗ РФ. – 2021. – № 27. – (Часть III). – Ст. 5424.

52. Постановление Правительства РФ от 29 июня 2021 г. № 1048 «Об утверждении Положения о федеральном государственном контроле (надзоре) качества и безопасности медицинской деятельности» // СЗ РФ. – 2021. – № 27 (часть III). – Ст. 5426.

53. Постановление Правительства РФ от 29 июня 2021 г. № 1049 «О федеральном государственном контроле (надзоре) в сфере обращения лекарственных средств» // СЗ РФ. – 2021. – № 27 (часть III). – Ст. 5427.

54. Постановление Правительства РФ от 30 июня 2021 г. № 1073 «О федеральном государственном контроле (надзоре) в сфере рекламы» // СЗ РФ. – 2021. – № 27 (часть 3). – Ст. 5449.

55. Постановление Правительства РФ от 30 июня 2021 г. № 1074 «О федеральном государственном горном надзоре» // СЗ РФ. – 2021. – № 27 (часть 3). – Ст. 5450.

56. Постановление Правительства РФ от 30 июня 2021 г. № 1082 «О федеральном государственном надзоре в области промышленной безопасности» // СЗ РФ. – 2021. – № 28 (часть 1). – Ст. 5512.

57. Постановление Правительства РФ от 30 июня 2021 г. № 1085 «О федеральном государственном энергетическом надзоре» // СЗ РФ. – 2021. – № 28 (часть 1). – Ст. 5515.

58. Постановление Правительства РФ от 30 июня 2021 г. № 1093 «О федеральном государственном контроле (надзоре) за состоянием, содержанием, сохранением, использованием, популяризацией и государственной охраной объектов культурного наследия» // СЗ РФ. – 2021. – № 28 (часть1). – Ст. 5523.

59. Постановление Правительства РФ от 30 июня 2021 г. № 1095 «Об утверждении Положения о федеральном государственном геологическом контроле (надзоре)» // СЗ РФ. – 2021. – № 28 (часть 1). – Ст. 5525.

60. Постановление Правительства РФ от 30 июня 2021 г. № 1096 «О федеральном государственном экологическом контроле (надзоре)» // СЗ РФ. – 2021. – № 28 (часть 1). – Ст. 5526.

61. Постановление Правительства РФ от 30 июня 2021 г. № 1101 «Об утверждении Положения о федеральном государственном контроле (надзоре) в области безопасности дорожного движения и признании утратившими силу некоторых актов Правительства Российской Федерации и отдельных положений некоторых актов Правительства Российской Федерации» // СЗ РФ. – 2021. – № 28 (часть 2). – Ст. 5531.

62. Постановление Правительства РФ от 21 июля 2021 г. № 1230 «Об утверждении Положения о федеральном государственном контроле (надзоре) за соблюдением трудового законодательства и иных нормативных правовых актов, содержащих нормы трудового права» // СЗ РФ. – 2021. – № 30. – Ст. 5804.

63. Концепция административной реформы в Российской Федерации на 2006–2010 годы, одобренная распоряжением Правительства от 25 октября 2005 г. № 1789-р // СЗ РФ. – 2005. – № 46. – Ст. 4720.

64. Распоряжение Правительства РФ от 27 декабря 2012 г. № 2538-р «О Программе фундаментальных научных исследований в РФ на долгосрочный период (2013–2020 гг.)» // Правительство Российской Федерации [Электронный ресурс]. URL: http://government.ru/docs/20270/ (дата обращения: 12.12.2021).

65. Основные направления разработки и внедрения системы оценки результативности и эффективности контрольно-надзорной деятельности, утверждены распоряжением Правительства РФ от 17 мая 2016 г. № 934-р // СЗ РФ. – 2016. – № 21. – Ст. 3075.

66. Распоряжение Правительства РФ от 28 июля 2017 г. № 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации» (утратило силу) // СЗ РФ. – 2017. – № 32. – Ст. 5138.

67. Распоряжение Правительства РФ от 26 сентября 2017 г. № 2049-р «Об утверждении плана мероприятий («дорожной карты») по созданию, развитию и вводу в эксплуатацию информационной системы «Типовое облачное решение по автоматизации контрольной (надзорной) деятельности» на 2017–2019 годы» // СЗ РФ. – 2017. – № 41. – Ст. 5993.

68. Концепция обеспечения безопасности дорожного движения с участием беспилотных транспортных средств на автомобильных дорогах общего пользования, утвержденная распоряжением Правительства РФ от 25 марта 2020 г. № 724-р // СЗ РФ. – 2020. – № 13. – Ст. 1995.

69. Распоряжение Правительства РФ от 22 октября 2021 г. № 2998-р «Об утверждении стратегического направления в области цифровой трансформации государственного управления» // СЗ РФ. – 2021. – № 44 (часть III). – Ст. 7467.

70. План мероприятий («дорожная карта») «Создание дополнительных условий для развития отрасли информационных технологий», утвержден Правительством РФ 9 сентября 2021 г. // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

71. Методические рекомендации «Алгоритм взаимодействия участников системы фармаконадзора по выявлению и работе со спонтанными сообщениями», утверждены Росздравнадзором 22 октября 2009 г. // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

72. Приказ Росздравнадзора от 7 августа 2015 г. № 5539 «Об утверждении Порядка осуществления выборочного контроля качества лекарственных средств для медицинского применения» // Бюллетень нормативных актов федеральных органов исполнительной власти. – 2015. – № 48.

73. Приказ Минздрава России от 30 ноября 2015 г. № 866 «Об утверждении Концепции создания Федеральной государственной информационной системы мониторинга движения лекарственных препаратов от производителя до конечного потребителя с использованием маркировки» // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

74. Приказ ФНС России от 14 марта 2016 г. № ММВ-7-12/134@ «Об утверждении Положения об автоматизированной информационной системе Федеральной налоговой службы (АИС «Налог-3»)» // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

75. Приказ Росздравнадзора от 15 февраля 2017 г. № 1071 «Об утверждении Порядка осуществления фармаконадзора» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://www.pravo.gov.ru (дата обращения: 22.10.2021).

76. Приказ МВД России от 23 августа 2017 г. № 664 «Об утверждении Административного регламента исполнения Министерством внутренних дел Российской Федерации государственной функции по осуществлению федерального государственного надзора за соблюдением участниками дорожного движения требований законодательства Российской Федерации в области безопасности дорожного движения» // Российская газета. – 2017. – № 232.

77. Приказ Минкомсвязи России от 4 июля 2018 года № 335 «Об утверждении методических рекомендаций по переходу органов исполнительной власти субъектов Российской Федерации и органов местного самоуправления муниципальных образований Российской Федерации на использование отечественного офисного программного обеспечения, в том числе ранее закупленного офисного программного

обеспечения» // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации [Электронный ресурс]. URL: https://digital.gov.ru/ru/documents/6142/#:~:text=Приказ.%2004.07.2018%20№335.%20Москва.%20Об,ранее%20закупленного%20офисного%20программного%20обеспечения (дата обращения: 12.12.2021).

78. Приказ ФСБ России от 24 июля 2018 г. № 366 «О Национальном координационном центре по компьютерным инцидентам» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001201809100001 (дата обращения: 12.12.2021).

79. Разъяснения (методические рекомендации) по разработке региональных проектов в рамках федеральных проектов Национальной программы «Цифровая экономика Российской Федерации», утвержденные приказом Минкомсвязи России от 1 августа 2018 г. № 428 // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

80. Приказ Росстандарта от 8 ноября 2019 г. № 1273-ст «Об утверждении национального стандарта Российской Федерации» // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

81. Распоряжение Минэкономразвития России от 4 декабря 2019 г. № 36Р-Д09 «Об утверждении методики мониторинга качества перевода государственных и муниципальных услуг в электронную форму» // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

82. Приказ Росздравнадзора от 28 июля 2020 г. № 6720 «Об утверждении Административного регламента Федеральной службы по надзору в сфере здравоохранения по осуществлению федерального государственного надзора в сфере обращения лекарственных средств» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://www.pravo.gov.ru (дата обращения: 20.10.2021).

83. Правила осуществления контроля за выполнением государственного задания на оказание государственных услуг (выполнения работ) федеральными государственными учреждениями, находящимися в ведении Министерства науки и высшего образования РФ, утвержденные приказом Министерства науки и высшего образования от 7 октября 2020 г. № 1277 // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://pravo.gov.ru (дата обращения: 19.12.2021).

84. Приказ Росздравнадзора от 30 декабря 2020 г. № 12641 «О внесении изменений в приказ Федеральной службы по надзору в сфере здравоохранения от 15 декабря 2020 г. № 11931 «Об утверждении ведом-

ственной программы цифровой трансформации Федеральной службы по надзору в сфере здравоохранения на 2021–2023 годы»» // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

85. Положение о департаменте информационных технологий Министерства труда и социальной защиты Российской Федерации, утвержденное приказом Министерства труда и социальной защиты РФ от 18 марта 2021 г. № 127 // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

86. Приказ Росздравнадзора от 4 мая 2021 г. № 3881 «Об утверждении Ведомственной программы профилактики нарушений обязательных требований при осуществлении государственного контроля качества и безопасности медицинской деятельности, федерального государственного надзора в сфере обращения лекарственных средств и государственного контроля за обращением медицинских изделий» // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

87. Приказ Министерства науки и высшего образования РФ от 14 июля 2021 г. № 621 «Об организации и проведении проверок деятельности организаций, подведомственных Министерству науки и высшего образования Российской Федерации» // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

88. Приказ МЧС России от 16 сентября 2021 г. № 613 «Об утверждении индикативных показателей для федерального государственного надзора в области защиты населения и территорий от чрезвычайных ситуаций» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://pravo.gov.ru (дата обращения: 22.10.2021).

89. Приказ МЧС России от 16 сентября 2021 г. № 614 «Об утверждении индикативных показателей для федерального государственного надзора в области гражданской обороны» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://pravo.gov.ru (дата обращения: 22.10.2021).

90. Приказ Минкультуры России от 1 декабря 2021 г. № 1998 «Об утверждении перечней индикативных показателей федерального государственного контроля (надзора) по видам федерального государственного контроля (надзора), отнесенным к компетенции Министерства культуры Российской Федерации» // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

91. ГОСТ Р ИСО 14813-1-2011 «Интеллектуальные транспортные системы. Схема построения архитектуры интеллектуальных транспорт-

ных систем. Часть 1. Сервисные домены в области интеллектуальных транспортных систем, сервисные группы и сервисы» // Электронный фонд правовой и нормативно-технической документации «Кодекс» [Электронный ресурс]. URL: http://docs.cntd.ru/document/1200086739 (дата обращения: 21.08.2021).

92. Письмо Росздравнадзора от 18 июля 2013 г. № 16И-779/13 «О предоставлении сведений о качестве лекарственных средств» // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

93. Письмо Росздравнадзора от 25 июля 2014 г. № 01И-1085/14 «О поисковом разделе сайта Росздравнадзора» // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

94. Письмо Росздравнадзора от 29 марта 2019 г. № 01и-841/19 «О регистрации пользователей в обновленной базе данных «Фармаконадзор» АИС Росздравнадзора» // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

95. Письмо Росздравнадзора от 28 ноября 2019 г. № 01И-2906/19 «О вводе в гражданский оборот» // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

96. Законопроект № 1256381-7 Об общих принципах организации публичной власти в субъектах Российской Федерации // Система обеспечения законодательной деятельности (СОЗД) [Электронный ресурс]. URL: https://sozd.duma.gov.ru/bill/1256381-7 (дата обращения: 12.12.2021).

97. Законопроект № 285949-7 // Система обеспечения законодательной деятельности [Электронный ресурс]. URL: http:// http://sozd.duma.gov.ru/bill/285949-7 (дата обращения: 06.11.2021).

98. Проект Постановления Правительства РФ «О внесении изменений в постановление Правительства Российской Федерации «Об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме» // Федеральный портал проектов нормативных актов [Электронный ресурс]. URL: https://regulation.gov.ru/projects/List/AdvancedSearch#departments=122&npa=122184 (дата обращения: 12.12.2021).

III. Научные труды и аналитические доклады

99. Bunbin M., Martynov A., Rumyantsev F. Legal framework for self-driving cars: the case of Russia // ACM International Conference Proceeding

Series. 13, Digital Governance in the Era of Disruptive Technologies and Globalisation. «Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance, ICEGOV 2020», 2020. – P. 206–213.

100. Sutherland S.A. Some Thoughts on Black Box AI and Law // Slaw. Canada Online legal magazine. 18.08.2021. URL: http://www.slaw.ca/2021/08/18/some-thoughts-on-black-box-ai-and-law/ (дата обращения: 21.10.2021).

101. Yu, R., & Alì, G. What's Inside the Black Box? AI Challenges for Lawyers and Researchers // Legal Information Management. – 2019. – № 19 (1). – Pp. 2-13. – DOI: 10.1017/S1472669619000021.

102. Административное право [Текст]: учебник / Б.В. Россинский, Ю.Н. Старилов. – 4-е изд., пересмотр. и доп. – М.: Норма, 2009. – 926 с.

103. Административное право [Текст]: учебник / под ред. Л.Л. Попова, М.С. Студеникиной. М.: Норма, 2008. С. 388-389.

104. Алехин А.П., Кармолицкий А.А. Административное право России [Текст]: учебник / А.П. Алехин, А.А. Кармолицкий. – М.: Изд-во «Зерцало», 2007. – 686 с.

105. Андреева Ю.А. К вопросу о соотношении понятий «контроль» и «надзор» [Текст] / Ю.А. Андреева // Административное право и процесс. – 2009. – № 2. – С. 6-8.

106. Баранова М.В. О специфике новелл опережающего правотворчества современно России (доктрина, практика, техника) / М.В. Баранова // Юридическая техника. – 2021. – № 15 [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/o-spetsifike-novell-operezhayuschego-pravotvorchestva-sovremennoy-rossii-doktrina-praktika-tehnika (дата обращения: 12.12.2021).

107. Бахрах Д.Н. Административное право России [Текст]: учебник для вузов / Д.Н. Бахрах. – М.: Издательство «Норма», 2001. – 640 с.

108. Бессарабов В.Г. Прокуратура в системе государственного контроля Российской Федерации: дис. … докт. юрид. наук: 12.00.02 [Текст] / В.Г. Бессарабов. – М., 2001. – 483 с.

109. Бессонов Н.К. Правовые барьеры развития цифровизации в субъектах Российской Федерации / Н.К. Бессонов // Образование и право. – 2021. – № 8 [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/pravovye-bariery-razvitiya-tsifrovizatsii-v-subektah-rossiyskoy-federatsii (дата обращения: 13.12.2021).

110. Бундин М.В. Национальная комиссия по информатике и свободам как орган по защите прав субъектов персональных данных во Франции [Текст] / М.В. Бундин // Актуальные вопросы контроля и надзора в социально значимых сферах деятельности общества и госу-

дарства: материалы IV Всероссийской научно-практической конференции. – Н. Новгород: Изд-во Нижегородского госуниверситета, 2018. – С. 279–286.

111. Голубцов В.Г. Российская Федерация как субъект гражданского права [Текст] / В.Г. Голубцов. – М.: Статут, 2019. – 272 с.

112. Горшенев В.М., Шахов И.Б. Контроль как правовая форма деятельности [Текст] / В.М. Горшенев, И.Б. Шахов. – М.: Юридическая литература, 1987. – 176 с.

113. Григорьева Н.С., Гладкова К.С. Государственное управление на пути цифровой трансформации [Текст] / Н.С. Григорьева, К.С. Гладкова // Вестник Белгородского университета кооперации, экономики и права. – 2021. – № 1 (86). – С. 88–100.

114. Дорофеева В.В. Фейковые новости в современном медиапространстве [Текст] / В.В. Дорофеева // Вопросы теории и практики журналистики. – 2019. – Т. 8. – № 4. – С. 774–786.

115. Законодательное регулирование здравоохранения Российской Федерации: итоги работы Комитета Государственной Думы по охране здоровья в период 2016–2021 годов // Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

116. Зарубицкая Т.К., Скляров И.А. Правовое положение органов, обеспечивающих законность в государственном управлении. Н. Новгород: НА МВД РФ, 1993 [Текст] / Т.К. Зарубицкая, И.А. Скляров // Скляров Иван Александрович. Избранные труды. – Н. Новгород: Изд-во Нижегородского госуниверситета им. Н.И. Лобачевского, 2018. – С. 140-206.

117. Зубарев С.М. Система контроля в сфере государственного управления [Текст]: монография / С.М. Зубарев. – М.: Норма: ИНФРА-М, 2019. – 152 с.

118. Зубарев С.М., Сладкова А.В. О понятии и сущности цифровых технологий контроля в сфере государственного управления [Текст] / С.М. Зубарев, А.В. Сладкова // Административное право и процесс. – 2019. – № 9. – С. 53–59.

119. Зырянов С.М. Административный надзор [Текст]: монография / С.М. Зырянов. – М.: ИД «Юриспруденция», 2010. – 208 с.

120. Зырянов С.М. Соотношение контрольной и надзорной функций органов исполнительной власти (глава 1 §3) [Текст] / С.М. Зырянов // В книге: Правовое регулирование государственного контроля: монография / отв. ред. д-р юрид. наук, проф., заслуженный деятель науки РФ А.Ф. Ноздрачев. – М.: Институт законодательства и сравнительного

правоведения при Правительстве Российской Федерации; Анкил, 2012. – С. 57–72.

121. Информационная безопасность в госсекторе (Материалы заочного круглого стола) // Системный Администратор. – 2021. – № 5 (222) [Электронный ресурс]. URL: http://samag.ru/archive/article/4382 (дата обращения: 12.12.2021).

122. Кабытов П.П., Стародубова О.Е. Влияние цифровизации на реализацию полномочий органов исполнительной власти [Текст] / П.П. Кабытов, О.Е. Стародубова // Журнал российского права. – 2020. – № 11. – С. 113–126.

123. Касавина Н.А. Цифровизация как предмет междисциплинарный исследований [Текст] / Н.А. Касавина // Эпистемология и философия науки 2019. – Т. 56. – № 4. – С. 251–259.

124. Козлов Ю.М. Административное право [Текст]: учебник / Ю.М. Козлов. – М.: Юристъ, 2007. – 554 с.

125. Козлова Г.Г., Арбузова Т.А. Влияние индустрии 4.0 на промышленные предприятия / Г.Г. Козлова, Т.А. Арбузова // Международный журнал гуманитарных и естественных наук. 2021. № 4-3 [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/vliyanie-industrii-4-0-na-promyshlennye-predpriyatiya (дата обращения: 20.12.2021).

126. Константин В.Н. Применение концепции «мягкой силы» в налогообложении криптовалют / В.Н. Константин // Экономика. Налоги. Право. – 2020. – № 6 [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/primenenie-kontseptsii-myagkoy-sily-v-nalogooblozhenii-kriptovalyut (дата обращения: 12.12.2021).

127. Контрольно-надзорная и разрешительная деятельность в Российской Федерации. Аналитический доклад. 2018 г. [Текст] / Кол. авт. Плаксин С.М., Абузярова И.А., Кнутов А.В. и др. – М.: Национальный исследовательский университет «Высшая школа экономики», 2019. – 146 с.

128. Контрольно-надзорная и разрешительная деятельность в Российской Федерации. Аналитический доклад – 2020-2021 [Текст] / С.М. Плаксин (рук. авт. кол.), И.А. Абузярова и др.; Российский союз промышленников и предпринимателей; Нац. исслед. ун-т «Высшая школа экономики». – М.: НИУ ВШЭ, 2021. – 148 с.

129. Красовская Н.Р., Гуляев А.А., Юлина Г.Н. Фейковые новости как феномен современности [Текст] / Н.Р. Красовская, А.А. Гуляев, Г.Н. Юлина // Власть. – 2019. – № 4. – С. 79–82.

130. Крысин Л.П. Толковый словарь иноязычных слов [Текст] / Л.П. Крысин. – М.: Эксмо, 2006.

131. Логинова А.Э. Современные информационные технологии при осуществлении контроля и надзора в сфере обращения лекарственных средств [Текст] / А.Э. Логинова // Вестник Нижегородского университета им. Н.И. Лобачевского. – 2020. – № 3. – С. 126–131.

132. Логинова А.Э. Цифровизация государственного контроля качества лекарственных средств в России [Текст] / А.Э. Логинова // Вестник Нижегородского университета им. Н.И. Лобачевского. – 2021. – № 4. – С. 152–158.

133. Манохин В.М., Адушкин Ю.С. Российское административное право [Текст]: учебник / В.М. Манохин, Ю.С. Адушкин. – 2-е изд., испр. и доп. – Саратов: Изд-во ГОУ ВПО «Саратовская государственная юридическая академия права», 2003. – 496 с.

134. Мартынов А.В. Административный надзор в России: теоретические основы построения [Текст]: монография / под ред. Ю.Н. Старилова. – М.: ЮНИТИ-ДАНА: Закон и право, 2010. – 183 с.

135. Мартынов А.В. Влияние цифровой трансформации на контрольно-надзорную деятельность органов исполнительной власти [Текст] / А.В. Мартынов // Публичная власть в современной России: проблемы и перспективы: сборник научных трудов по материалам международной научно-практической конференции памяти доктора юридических наук, профессора, заслуженного деятеля науки РСФСР Василия Михайловича Манохина (VII Саратовские административно-правовые чтения) (8 июня 2021 г., Саратов) / под общ. ред. А.Ю. Соколова; редкол. А.Ю. Соколов и др.; Саратовская государственная юридическая академия; Саратовский филиал ФГБУН «Институт государства и права РАН». – Саратов: Изд-во Саратовской государственной юридической академии, 2021. – С. 32–56.

136. Мартынов А.В. Использование современных цифровых технологий при осуществлении профилактической деятельности контрольно-надзорных органов исполнительной власти [Текст] / А.В. Мартынов // Юрист. – 2020. – № 10. – С. 48–56.

137. Мартынов А.В. Попытки законодательного разграничения государственного контроля и административного надзора в условиях современной административной реформы в России [Текст] / А.В. Мартынов // Актуальные вопросы контроля и надзора в социально значимых сферах деятельности общества и государства: материалы V Всероссийской научно-практической конференции (Россия, г. Нижний Новгород, 7-8 июня 2019 г.) / Отв. ред. доктор юридических наук, профессор А.В. Мартынов. – Н. Новгород: Изд-во Нижегородского госуниверситета им. Н.И. Лобачевского, 2019. – С. 27–59.

138. Мартынов А.В. Применение риск-ориентированного подхода при осуществлении государственного контроля и надзора как необходимое условие снижение давления на бизнес // Юрист. – 2016. – № 18. – С. 22–27.

139. Мартынов А.В. Проблемы правового регулирования административного надзора в России. Административно-процессуальное исследование [Текст]: монография / А.В. Мартынов. – М.: NOTA BENE, 2010. – 548 с.

140. Мартынов А.В. Развитие новых форм и методов государственного контроля и надзора в условиях цифровой экономики [Текст] / А.В. Мартынов // Законы России: опыт, анализ, практика. – 2021. – № 11. – С. 10–27.

141. Мартынов А.В. Туманные перспективы системы «Открытое правительство» в эпоху цифровой экономики России [Текст] / А.В. Мартынов // Законы России: опыт, анализ, практика. – 2018. – № 11. – С. 10–23.

142. Мартынов А.В., Бундин М.В. О правовых принципах применения искусственного интеллекта при осуществлении органами исполнительной власти контрольно-надзорной деятельности [Текст] / А.В. Мартынов, М.В. Бундин // Журнал российского права. – 2020. – № 10. – С. 59–75.

143. Мартынов А.В., Ширеева Е.В., Логинова А.В. Проблемы использования цифровых технологий в деятельности органов государственного контроля и надзора в условиях цифровой экономики (исследование проведенное на основе опроса должностных лиц органов государственного контроля и надзора) [Текст] / А.В. Мартынов, Е.В. Ширеева, А.Э. Логинова // Вестник Нижегородского университета им. Н.И. Лобачевского. – 2021. – № 5. – С. 119–135.

144. Минбалеев А.В. Место и роль саморегулирования в развитии цифровых технологий / А.В. Минбалеев // Образование и право. – 2019. – № 1 [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/mesto-i-rol-samoregulirovaniya-v-razvitii-tsifrovyh-tehnologiy (дата обращения: 20.11.2021).

145. Минбалеев А.В. Проблемы правового регулирования использования цифровых технологий в деятельности саморегулируемых организаций [Текст] / А.В. Минбалеев // Гражданское право. – 2020. – № 4. – С. 31–34.

146. Модельная конвенция о робототехнике и искусственном интеллекте // Проект «Робоправо» [Электронный ресурс]. URL: https://robopravo.ru/matierialy_dlia_skachivaniia (дата обращения: 28.11.2021).

147. Морхат П.М. К вопросу о правосубъектности «электронного лица» / П.М. Морхат // Юридические исследования. – 2018. – № 4 [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/k-voprosu-o-pravosubektnosti-elektronnogo-litsa/viewer (дата обращения: 27.11.2021).

148. Наумов В.Б., Бутримович Я.В., Котов А.А. Обеспечение качества правового регулирования экспериментальных правовых режимов / В.Б. Наумов, Я.В. Бутримович, А.А. Котов // Российское право: образование, практика, наука. – 2020. – № 3 [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/obespechenie-kachestva-pravovogo-regulirovaniya-eksperimentalnyh-pravovyh-rezhimov (дата обращения: 12.12.2021).

149. Овсянко Д.М. Административное право [Текст]: учебное пособие / Д.М. Овсянко. – Изд. 3-е, перераб. и доп. – М.: Юристъ, 2002. – 468 с.

150. Ожегов С.И. Словарь русского языка [Электронный ресурс] // URL: https://slovarozhegova.ru (дата обращения: 20.09.2021).

151. Организационные структуры и команды цифровой трансформации в системе государственного управления [Текст] / авт.-сост. Н.С. Гаркуша, А.С. Шубин под ред. М.С. Шклярук. – М.: РАНХиГС, 2020. – 165 с.

152. Официальный доклад о деятельности Уполномоченного по правам человека в Российской Федерации за 2020 г. // Официальный сайт Уполномоченного по правам человека в Российской Федерации [Электронный ресурс]. URL: https://ombudsmanrf.org/upload/files/docs/lib/Doc4.pdf (дата обращения: 05.12.2021).

153. Панченко В.Ю., Макарчук И.Ю. Предостережение как правовое средство [Текст] / В.Ю. Панченко, И.Ю. Макарчук // Законность. – 2013. – № 6 (944). – С. 13–18.

154. Перспективные направления правового регулирования использования современных информационных технологий в контрольно-надзорной деятельности органов исполнительной власти: библиотека лучших российских и зарубежных практик [Текст]: монография / А.В. Мартынов, М.В. Бундин, М.Д. Прилуков, Е.Н. Смирнова, Е.В. Ширеева. – Н. Новгород: Изд-во Нижегородского госуниверситета им. Н.И. Лобачевского, 2020. – 227 с.

155. Погодина И.В., Авдеев Д.А. Возможности применения технологии blockchain в публичном управлении [Текст] / И.В. Погодина, Д.А. Авдеев // Муниципальная служба: правовые вопросы. – 2019. – № 2. – С. 9–12.

156. Поспелов К.Г. Создание и внедрение комплексной модели информационного обеспечения и системы автоматизации контроля (надзора) в сфере здравоохранения [Текст] / К.Г. Поспелов // Вестник Росздравнадзора. – 2017. – № 3. – С. 31–35.

157. Правовое регулирование государственного контроля [Текст]: монография / отв. ред. д-р юрид. наук, проф., заслуженный деятель науки РФ А.Ф. Ноздрачев. – М.: Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации; Анкил, 2012. – 480 с.

158. Прогноз научно-технологического развития Российской Федерации до 2030 года // Официальный сайт Правительства Российской Федерации [Электронный ресурс]. URL: http://static.government.ru/media/files/41d4b737638b91da2184.pdf (дата обращения: 12.12.2021).

159. Прошунин М.М. Государственный цифровой финансовый контроль: правовая сущность [Текст] / М.М. Прошунин // Финансовое право. – 2021. – № 5. – С. 3–7.

160. Россинский Б.В. Информационные подходы к разграничению контроля и надзора в деятельности государственных органов [Текст] / Б.В. Россинский // Актуальные вопросы контроля и надзора в социально значимых сферах деятельности общества и государства: материалы V Всероссийской научно-практической конференции (Россия, г. Нижний Новгород, 7-8 июня 2019 г.) / Отв. ред. доктор юридических наук, профессор А.В. Мартынов. – Н. Новгород: Изд-во Нижегородского госуниверситета им. Н.И. Лобачевского, 2019. – С. 22–26.

161. Рохлин В.И. Прокурорский надзор и государственный контроль: история, развитие, понятие, соотношение [Текст] / В.И. Рохлин. – СПб.: Издательство «Юридический центр Пресс», 2003. – 305 с.

162. Савченко Е.А. Некоторые аспекты соблюдения законности субъектами разрешительной и контрольно-надзорной деятельности в условиях модернизации социально-экономического развития [Текст] / Е.А. Савченко // Журнал российского права. – 2019. – № 7. – С. 104–114.

163. Смирнова Е.Н. Об актуальных вопросах использования информационных технологий в профилактическом направлении контрольно-надзорной деятельности органов исполнительной власти [Текст] / Е.Н. Смирнова // NB: Административное право и практика администрирования. – 2020. – № 2. – С. 27-37.

164. Смирнова Е.Н. Обеспечение соблюдения прав и свобод личности при осуществлении органами исполнительной власти цифрового контроля [Текст] / Е.Н. Смирнова // NB: Административное право и практика администрирования. – 2021. – № 3. – С. 37–45.

165. Советское административное право [Текст]: учебник / под ред. заслуженного деятеля науки УССР, доктора юридических наук, профессора Р.С. Павловского. – Киев: Вища школа, 1986.

166. Студеникина М.С. Государственные инспекции в СССР [Текст] / М.С. Студеникина. – М.: Юридическая литература, 1987. – 112 с.

167. Студеникина М.С. Государственный контроль в сфере управления. Проблемы надведомственного контроля [Текст] / М.С. Студеникина. – М.: Юридическая литература, 1974. – 160 с.

168. Субанова Н.В. К вопросу о концепции Федерального закона об основах государственного контроля и надзора в Российской Федерации [Текст] / Н.В. Субанова // Актуальные вопросы контроля и надзора в социально значимых сферах деятельности общества и государства: материалы I Всероссийской научно-практической конференции (Нижний Новгород, 4-5 июня 2015 г.) / Отв. ред. докт. юрид. наук, доцент А.В. Мартынов. – Н. Новгород: Изд-во Нижегородского госуниверситета им. Н.И. Лобачевского, 2015. – С. 88-95.

169. Тарасов А.М. Государственный контроль в России [Текст]: монография / А.М. Тарасов. – М.: ЗАО «Издательство «Континент», 2008. – 672 с.

170. Тихомиров М.Ю. Административное право и процесс [Текст]: полный курс / М.Ю. Тихомиров. – 2-е изд., доп. и перераб. – М.: Изд. Тихомирова М.Ю., 2008. – 697 с.

171. Трощинский П.В. Цифровой Китай до и в период коронавируса: особенности нормативно-правового регулирования [Текст] / П.В. Трощинский // Право и цифровая экономика. – 2021. – № 1. – С. 44–58.

172. Филипова И.А. Искусственный интеллект и нейротехнологии: потребности в конституционно-правовом регулировании [Текст] / И.А. Филипова // Lex russica. – 2021. – № 9 (178). – С. 119–130.

173. Хабриева Т.Я., Черногор Н.Н. Право в условиях цифровой реальности [Текст] / Т.Я. Хабриева, Н.Н. Черногор // Журнал российского права. – 2018. – № 1. – С. 85–102.

174. Хохлов Е.С. Меры предупредительного воздействия на хозяйствующих субъектов, занимающих доминирующее положение [Текст] / Е.С. Хохлов // Закон. – 2017. – № 4. – С. 132–140.

175. Цифровая трансформация государственного управления: мифы и реальность [Текст]: докл. к XX Апр. междунар. науч. конф. По проблемам развития экономики и общества, Москва, 9–12 апр. 2019 г. / Д.Ю. Двинских, Н.Е. Дмитриева, А.Б. Жулин и др.; под общ. ред. Н.Е. Дмитриевой; Нац. исслед. ун-т «Высшая школа экономики». – М.: Изд. дом Высшей школы экономики, 2019. – 43 с.

176. Цифровые технологии в российской экономике [Текст] / К.О. Вишневский, Л.М. Гохберг, В.В. Дементьев и др.; под ред. Л.М. Гохберга; Нац. исслед. ун-т «Высшая школа экономики». – М.: НИУ ВШЭ, 2021. – 116 с.

177. Шестак В.А., Волеводс А.Г. Современные потребности правового обеспечения искусственного интеллекта: взгляд из России [Текст] / В.А. Шестак, А.Г. Волеводс // Всероссийский криминологический журнал. – 2019. – Т. 13. – № 2. – С. 197–206.

178. Ширеева Е.В. Правовые основы применения и практики внедрения искусственного интеллекта при осуществлении судебного контроля [Текст] / Е.В. Ширеева // Вестник Воронежского государственного университета. Серия: Право. – 2020. – № 3 (42). – С. 30–39.

179. Ширеева Е.В. Правовые формы и методы государственного контроля и надзора в сфере обеспечения правопорядка и общественной безопасности в условиях цифровой трансформации органов исполнительной власти [Текст] / Е.В. Ширеева // Вестник Воронежского государственного университета. Серия: Право. – 2021. – № 4.

180. Шорина Е.В. Контроль за деятельностью органов государственного управления в СССР [Текст] / Е.В. Шорина. – М.: Издательство «Наука», 1981. – 302 с.

181. Юдина М.А. Индустрия 4.0: конкуренция за актуальность / М.А. Юдина // Государственное управление. Электронный вестник. 2020. № 80 [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/industriya-4-0-konkurentsiya-za-aktualnost (дата обращения: 20.12.2021).

182. Юридическая концепция роботизации [Текст]: Монография / Отв. ред. Ю.А. Тихомиров, С.Б. Нанба. – М.: Проспект, 2019. – 240 с.

IV. Интернет-ресурсы

183. AT&T, Cisco, GE, IBM и Intel образуют промышленный интернет-консорциум для улучшения интеграции физического и цифрового миров [Электронный ресурс] // URL: https://about.att.com/story/att_cisco_ge_ibm_intel_industrial_internet_consortium.html (дата обращения: 20.12.2021).

184. CNIL Rapport d'activité 2017 [Электронный ресурс] // URL: https://www.cnil.fr/sites/default/files/atoms/files/cni-l38e_rapport_annuel_2017.pdf (дата обращения: 02.12.2021).

185. Dwoskin E. Twitter is looking for ways to let users flag fake news, offensive content // The Washington Post. 2017. 29 June [Электронный

ресурс]. URL: https://www.washingtonpost.com/news/theswitch/wp/2017/06/29/twitter-is-looking-for-ways-to-let-users-flag-fake-news/ (дата обращения: 05.12.2021).

186. Fake News and Disinformation Online 2018 // European Comission [Электронный ресурс]. URL: https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruinstr/flash/surveyky/2183 (дата обращения: 05.12.2021).

187. Hill K. Wrongfully Accused by an Algorithm // New York Times. 24 июня 2020 года [Электронный ресурс]. URL: https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html (дата обращения: 12.12.2021).

188. Kramer A. 6 successful tech companies that are surprisingly secretive about their internal workings // Insider. 25 сентября 2019 года [Электронный ресурс]. URL: https://www.businessinsider.com/secretive-tech-companies-apple-google-palantir-2019-9 (дата обращения: 21.10.2021).

189. West D.M. How to combat fake news and disinformation // Brookings. 18 December 2017 [Электронный ресурс]. URL: https://www.brookings.edu/research/how-to-combat-fake-news-and-disinformation/ (дата обращения: 05.12.2021).

190. Александров А., Королев Н. Система распознавания дала правоохранительный сбой // Коммерсантъ. 24 сентября 2020 года [Электронный ресурс]. URL: https://www.kommersant.ru/doc/4503252 (дата обращения: 12.12.2021).

191. Апулеев И. Миллионы кибератак: Патрушев о происках иностранных спецслужб // ГазетаRU. 25 октября 2019 года [Электронный ресурс]. URL: https://www.gazeta.ru/tech/2019/10/25_a_12776498.shtml?updated (дата обращения: 12.12.2021).

192. Бунина В. Навсегда застрять среди отстающих: что ждет Россию на рынке технологий // Газета.ru. 13 апреля 2021 года [Электронный ресурс]. URL: https://www.gazeta.ru/tech/2021/04/13/13556486/lag_behind.shtml (дата обращения: 12.12.2021).

193. Бутрин Д. Наблюдение за наблюдающими // Газета Коммерсантъ. 19 июля 2021 года. № 124 (7086) [Электронный ресурс]. URL: https://www.kommersant.ru/doc/4908320 (дата обращения: 01.11.2021).

194. В Интернет-приемной ФССП России создан новый вид обращений для граждан-двойников // Федеральная служба судебных приставов [Электронный ресурс]. URL: https://fssp.gov.ru/pressreleases/document30105677/ (дата обращения: 12.12.2021).

195. Глазунов С. Бизнес в облаках. Чем полезны облачные технологии для предпринимателя // Журнал «Контур». 22 февраля 2013 года

[Электронный ресурс]. URL: https://kontur.ru/articles/225 (дата обращения: 01.11.2021).

196. Заоблачные перспективы облачных технологий. 8 трендовых решений для бизнеса // Аргументы и факты [Электронный ресурс]. URL: https://aif.ru/boostbook/oblachnye-tekhnologii-i-reshenija.html (дата обращения: 01.11.2021).

ИСО/МЭК разработает международные стандарты в области искусственного интеллекта // Техноллект. 1 ноября 2018 года [Электронный ресурс]. URL: https://tehnolet.cntd.ru/news/read/isomk-razrabotaet-mejdunarodnye-standarty-v-oblasti-iskusstvennogo-intellekta/novosti-cifrovoj-ehkonomiki (дата обращения: 12.12.2021).

197. Касми Э. Россиянина едва не посадили на 8 лет из-за ошибки искусственного интеллекта // CNews. 20 ноября 2020 года [Электронный ресурс]. URL: https://www.cnews.ru/news/top/2020-11-12_rossiyanina_edva_ne_posadili (дата обращения: 12.12.2021).

198. Кинякина Е., Исакова Т. Microsoft отказался продавать софт Бауманке // Ведомости. 8 декабря 2020 года [Электронный ресурс]. URL: https://www.vedomosti.ru/technology/articles/2020/12/08/850139-microsoft-otkazalsya (дата обращения: 12.12.2021).

199. Конкурс на лучшие научные проекты междисциплинарных фундаментальных исследований по теме «Трансформация права в условиях развития цифровых технологий» // РФФИ [Электронный ресурс]. URL: https://www.rfbr.ru/rffi/ru/contest/n_812/o_2058677 (дата обращения: 12.12.2021).

200. Котляр М. Zoom запретила российскому госсектору пользоваться своей видеосвязью // РБК. 6 апреля 2021 года [Электронный ресурс]. URL: https://www.rbc.ru/technology_and_media/06/04/2021/606cbbde9a79476bb34333ed (дата обращения: 12.12.2021).

201. Кочетова К. На темной стороне силы: чем грозят технологии распознавания лиц // KasperskyDaily. 22 августа 2016 года [Электронный ресурс]. URL: https://www.kaspersky.ru/blog/bad-facial-recognition/12823/ (дата обращения: 12.12.2021).

202. Кудрин помечтал о роботах-налоговиках // Новостной сайт «Lenta.ru» [Электронный ресурс]. URL: https://lenta.ru/news/ 2017/11/10/kudrin (дата обращения: 05.12.2021).

203. Ногаева К. Применение биометрии развивается на фоне недоверия россиян // Деловой Петербург. 7 декабря 2021 года [Электронный ресурс]. URL: https://www.dp.ru/a/2021/12/06/Otdam_v_horoshie_ruki (дата обращения: 12.12.2021).

204. Облачное решение // ПМ Форсайт [Электронный ресурс]. URL: https://pmforesight.ru/argumenty/oblachnoe-reshenie/ (дата обращения: 01.11.2021).

205. Орехин П. Безопасность во главе угла // Российская газета. 8 октября 2019 года [Электронный ресурс]. URL: https://rg.ru/2019/10/08/ispolzovanie-biometricheskoj-sistemy-pravo-grazhdan-a-ne-obiazannost.html (дата обращения: 12.12.2021).

206. Основные результаты деятельности НКЦКИ // НКЦКИ [Электронный ресурс]. URL: https://safe-surf.ru/search/?tags=статистика%20НКЦКИ (дата обращения: 12.12.2021).

207. Развитию искусственного интеллекта в здравоохранении будут способствовать новые // Росстандарт. 6 декабря 2021 года [Электронный ресурс]. URL: https://www.rst.gov.ru/portal/gost/home/presscenter/news/newsRST/redirect/news/1/5241?portal:componentId=88beae40-0e16-414c-b176-d0ab5de82e16&navigationalstate=JBPNS_rO0ABXczAAZhY3Rpb24AAAABAA5zaW5nbGVOZXdzVmlldwACaWQAAAABAAQ4NDM3AAdfX0VPRl9f (дата обращения: 12.12.2021).

208. Росздравнадзор призовет искусственный интеллект для обработки обращений граждан // Фармацевтический вестник [Электронный ресурс]. URL: https://pharmvestnik.ru/content/news/Roszdravnadzor-prizovet-iskusstvennyi-intellekt-dlya-obrabotki-obrashenii-grajdan.html (дата обращения: 06.11.2021).

209. Сахмеев В. Физтех за 14 млн создаст Роскомнадзору программу по поиску экстремизма и видео для взрослых в Сети // Собеседник. 11 октября 2021 года [Электронный ресурс]. URL: https://sobesednik.ru/obshchestvo/20211011-fiztex-za-14-mln-sozdast-roskomnadzoru-p (дата обращения: 12.12.2021).

210. Скобелев В., Чернышева Е. Половина россиян не поддержали создание властями биометрической системы // РБК. 28 декабря 2020 года [Электронный ресурс]. URL: https://www.rbc.ru/technology_and_media/28/12/2020/5fe5cee59a7947dfd4362d12 (дата обращения: 12.12.2021).

211. Сухоруков А. Источник подтвердил, что США атакуют российскую энергосистему // РИА Новости. 17 июня 2019 года [Электронный ресурс]. URL: https://ria.ru/20190617/1555640687.html (дата обращения: 12.12.2021).

212. Цифровая трансформация Ростехнадзора за 500 миллионов рублей // Охрана труда в России [Электронный ресурс]. URL: https://ohranatruda.ru/news/899/589135/ (дата обращения: 20.12.2021).

213. АИС Росздравнадзора [Электронный ресурс] // URL: http: //external.roszdravnadzor.ru/?type=logon.

214. Национальный координационный центр по компьютерным инцидентам [Электронный ресурс] // URL: https://cert.gov.ru.

215. Официальный сайт «Портал КНД» [Электронный ресурс] // URL: https://knd.gov.ru.

216. ФГИС «Единый реестр проверок» [Электронный ресурс] // URL: https://proverki.gov.ru/portal/public-search.

217. Официальный сайт компании «Съемка с воздуха» [Электронный ресурс] // URL: https://rusdrone.ru.

218. Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации [Электронный ресурс] // URL: https://digital.gov.ru.

219. Официальный сайт Президента Российской Федерации [Электронный ресурс] // URL: http://www.kremlin.ru.

220. Официальный сайт Федеральной службы по надзору в сфере здравоохранения [Электронный ресурс] // URL: https://roszdravnadzor.gov.ru.

221. Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций [Электронный ресурс] // URL: https://rkn.gov.ru.

222. Официальный сайт Федеральной службы по экологическому, технологическому и атомному надзору [Электронный ресурс] // URL: https://www.gosnadzor.ru.

223. Официальный сайт ФКУ «Дороги России» [Электронный ресурс] // URL: http://www.dorros.ru.

224. Cnews [Электронный ресурс] // URL: https://www.cnews.ru.

225. IBM [Электронный ресурс] // URL: https://www.ibm.com.

226. Positive Technologies [Электронный ресурс] // URL: https://www.ptsecurity.com/ru-ru/.

227. TAdviser [Электронный ресурс] // URL: https://www.tadviser.ru.

228. ИТАР-ТАСС [Электронный ресурс] // URL: https://tass.ru.

229. ПравоRU [Электронный ресурс] // URL: https://pravo.ru/news.

230. РИА Новости [Электронный ресурс] // URL: https://ria.ru.

231. Российская газета [Электронный ресурс] // URL: https://rg.ru.

232. Яндекс [Электронный ресурс] // URL: https://zen.yandex.ru.

ПРИЛОЖЕНИЕ

Результаты опроса
должностных лиц органов государственного контроля и надзора

319 должностных лиц

23 федеральных и региональных органов исполнительной власти

Федеральные органы исполнительной власти:

- Волжско-Окское управление Ростехнадзора
- Главное управление МЧС России по г. Москва,
- Главное управление МЧС России по Нижегородской области
- Главное управление ФССП России по Свердловской области
- Госавтоинспекция по Нижегородской области
- Госавтоинспекция по Республике Марий Эл
- Государственная инспекция труда в Нижегородской области
- Межрегиональное управление Росфинмониторинга по Приволжскому федеральному округу
- Северо-Уральское Межрегиональное управление государственного автодорожного надзора Ространснадзора
- Управление Роскомнадзора по Воронежской области
- Управление Роскомнадзора по Приволжскому федеральному округу
- Управление Росреестра по Нижегородской области
- Управление ФАС России по Нижегородской области
- Управление Федерального казначейства по Нижегородской области
- Управление ФССП России по Астраханской области
- Управление ФССП России по Нижегородской области
- Управление ФССП России по Омской области
- Управление ФССП России по Ярославской области
- Центральный аппарат ФССП России

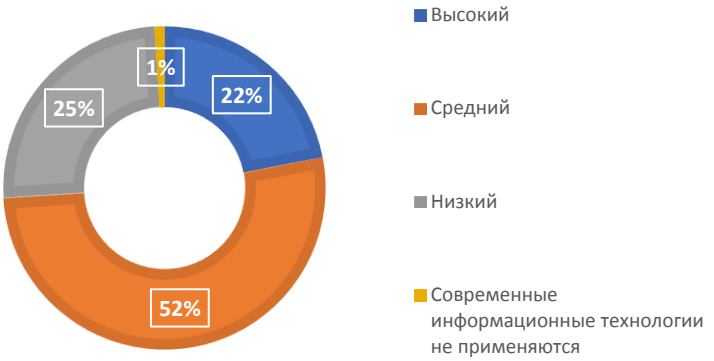
Региональные органы исполнительной власти:

- Инспекция государственного строительного надзора Нижегородской области
- Министерство информационных технологий и связи Нижегородской области
- Министерство образования, науки и молодежной политики Нижегородской области
- Министерство промышленности, торговли и предпринимательства Нижегородской области

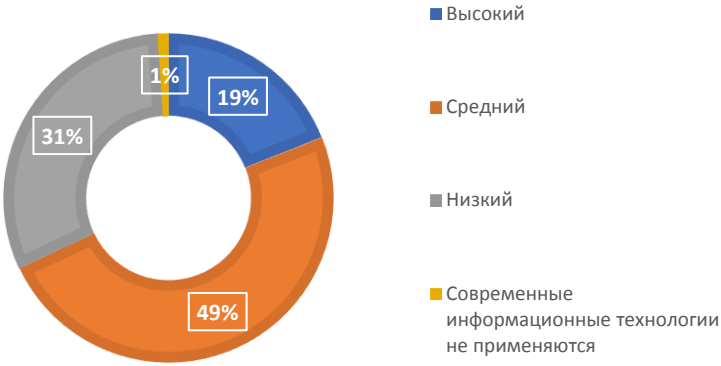
23 субъекта Российской Федерации

- Республика Башкортостан
- Республика Марий Эл
- Республика Мордовия
- Республика Татарстан
- Удмуртская Республика
- Чувашская Республика – Чувашия
- Пермский край
- Астраханская область
- Воронежская область
- Кировская область
- Нижегородская область
- Омская область
- Оренбургская область
- Пензенская область
- Самарская область
- Саратовская область
- Свердловская область
- Тюменская область
- Ульяновская область
- Ярославская область
- город федерального значения Москва
- Ханты-Мансийский автономный округ – Югра
- Ямало-Ненецкий автономный округ

1. КАК ВЫ ОЦЕНИВАЕТЕ УРОВЕНЬ ПРАВОВОГО РЕГУЛИРОВАНИЯ ИСПОЛЬЗОВАНИЯ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В СФЕРЕ ГОСУДАРСТВЕННОГО КОНТРОЛЯ И НАДЗОРА?

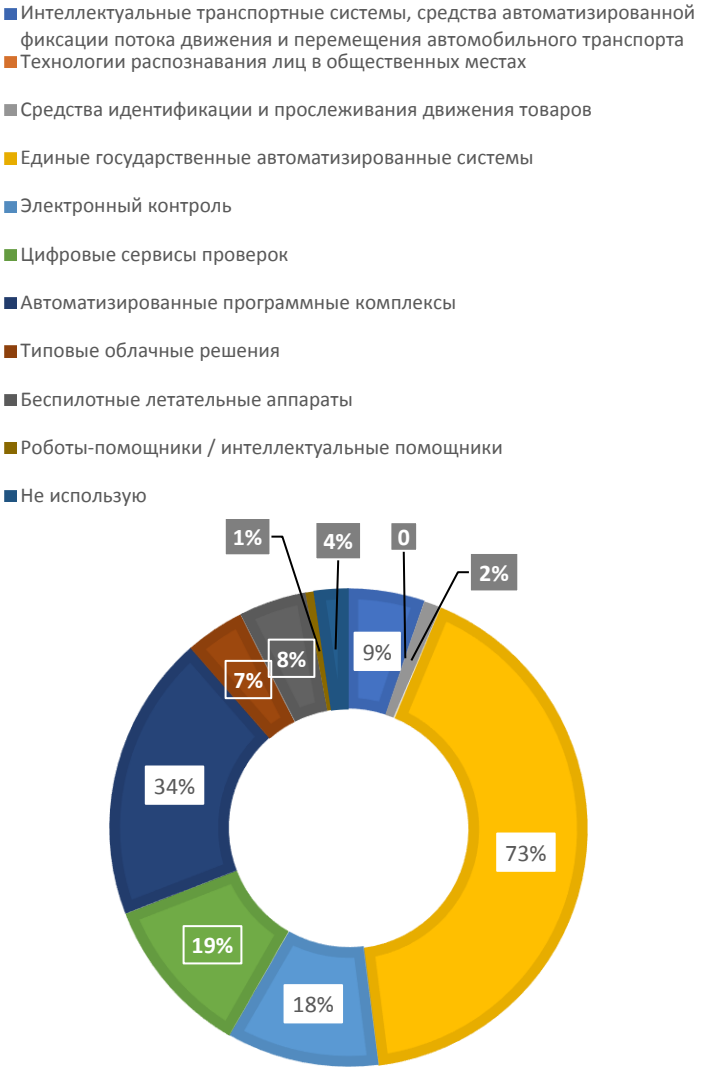


2. КАК ВЫ ОЦЕНИВАЕТЕ УРОВЕНЬ РАЗВИТИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В КОНТРОЛЬНО-НАДЗОРНОЙ ДЕЯТЕЛЬНОСТИ?



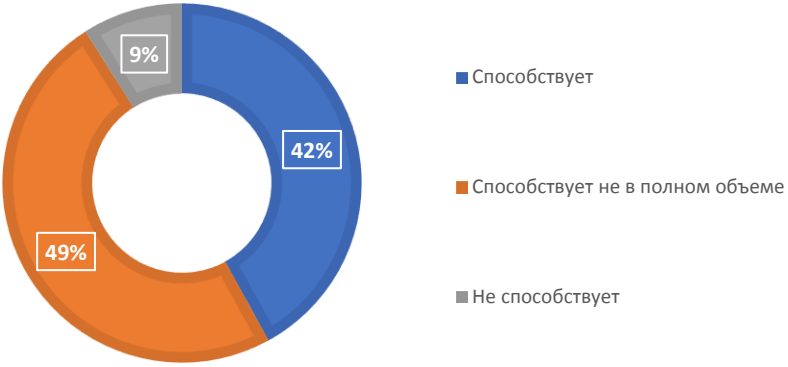
3. КАКИЕ СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ВЫ ИСПОЛЬЗУЕТЕ В КОНТРОЛЬНО-НАДЗОРНОЙ ДЕЯТЕЛЬНОСТИ?

(*респонденты указывали несколько вариантов ответов)



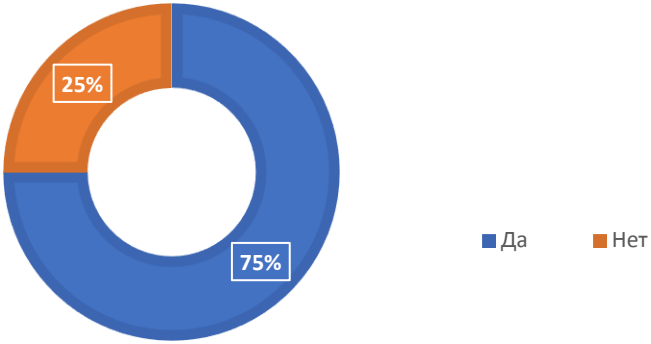
4. КАКИЕ СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ВЫ ИСПОЛЬЗУЕТЕ ДЛЯ ВЗАИМОДЕЙСТВИЯ С ОБЪЕКТАМИ КОНТРОЛЬНО-НАДЗОРНОЙ ДЕЯТЕЛЬНОСТИ (ПРОВЕРЯЕМЫМИ ЛИЦАМИ)?
(*респонденты указывали несколько вариантов ответов)

5. СПОСОБСТВУЕТ ЛИ ПРИМЕНЕНИЕ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПОВЫШЕНИЮ ЭФФЕКТИВНОСТИ ОСУЩЕСТВЛЕНИЯ ВАМИ КОНТРОЛЬНО-НАДЗОРНОЙ ДЕЯТЕЛЬНОСТИ?



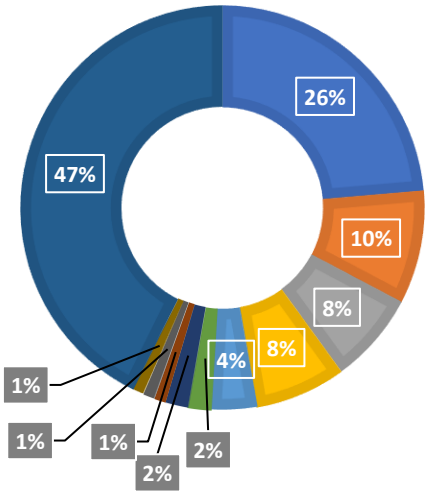
6. КАКИЕ НЕГАТИВНЫЕ ФАКТОРЫ ПРИМЕНЕНИЯ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В КОНТРОЛЬНО-НАДЗОРНОЙ ДЕЯТЕЛЬНОСТИ ВЫ МОЖЕТЕ ОТМЕТИТЬ? (*респонденты указывали несколько вариантов ответов)

7. ДОЛЖНЫ ЛИ СОЗДАВАТЬСЯ СПЕЦИАЛЬНЫЕ ПОДРАЗДЕЛЕНИЯ (ОТДЕЛЫ, УПРАВЛЕНИЯ) В СТРУКТУРЕ ОРГАНОВ ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ ПО РАЗРАБОТКЕ И ВНЕДРЕНИЮ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В СФЕРУ КОНТРОЛЬНО-НАДЗОРНОЙ ДЕЯТЕЛЬНОСТИ?



8. ПРИМЕНЕНИЕ КАКИХ ИНЫХ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ВЫ СЧИТАЕТЕ ПЕРСПЕКТИВНЫМИ В КОНТРОЛЬНО-НАДЗОРНОЙ ДЕЯТЕЛЬНОСТИ? (*респонденты указывали несколько вариантов ответов)

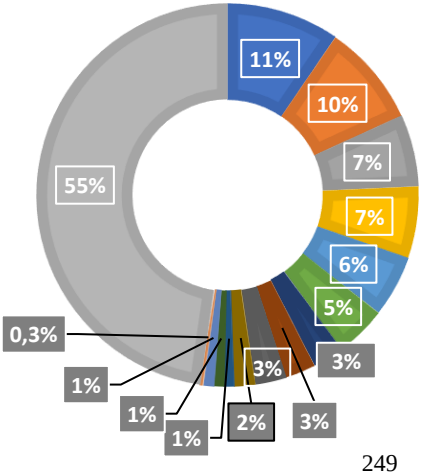
- Система дистанционного контроля, электронные сервисы проверок
- Технологии искусственного интеллекта
- Облачные технологии
- Синхронизированные государственные информационные системы / единые базы данных
- Современные средства мобильной коммуникации
- Интеллектуальный поиск информации с гибкими критериями и параметрами
- Электронный документооборот (в т.ч. подконтрольных субъектов)
- Технология распознавания предметов (в т.ч. с помощью беспилотных летательных аппаратов и спутниковой фото- и видеосъемки)
- Программы безопасности информационных систем
- Единый портал государственных услуг и функций с расширенным функционалом
- Затрудняюсь ответить



9. КАКИМИ ПРАВОВЫМИ И ОРГАНИЗАЦИОННЫМИ СРЕДСТВАМИ ДОЛЖНА ОБЕСПЕЧИВАТЬСЯ БЕЗОПАСНОСТЬ ПРИМЕНЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В КОНТРОЛЬНО-НАДЗОРНОЙ ДЕЯТЕЛЬНОСТИ? (*респонденты указывали несколько вариантов ответов)

10. ВАШИ ПРЕДЛОЖЕНИЯ ПО СОВЕРШЕНСТВОВАНИЮ ПРИМЕНЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В КОНТРОЛЬНО-НАДЗОРНОЙ ДЕЯТЕЛЬНОСТИ? (*респонденты указывали несколько вариантов ответов)

- Оснащение современной компьютерной техникой с необходимым программным обеспечением и скоростным интернетом
- Создание единой информационной системы
- Повышение уровня информатизации и автоматизации, отказ от бумажного документооборота
- Обеспечение квалифицированной технической поддержкой
- Периодическое обучение сотрудников работе с электронными системами
- Качественная подготовка и тестирование программ до введения в эксплуатациюми
- Совершенствование систем защиты информации
- Обеспечение эффективного электронного взаимодействия органов исполнительной власти
- Разработка мобильных приложений
- Внедрение дистанционного электронного контроля, включая электронное взаимодействие с подконтрольными субъектами
- Совершенствование нормативно-правового регулирования
- Создание типового облачного решения по автоматизации контрольно-надзорной деятельности
- Введение цифровых порталов самопроверок
- Ужесточение ответственности за разглашение информации ограниченного доступа
- Затрудняюсь ответить




Степень развития информационных технологий в контрольно-надзорной деятельности в целом недостаточно высока
Однозначно, что применение современных информационных технологий в большей или меньшей степени способствует повышению эффективности осуществления контрольно-надзорной деятельности
Необходимо создать специальные подразделения в структуре органов исполнительной власти по разработке и внедрению информационных технологий
ВЫВОДЫ
Уровень правового регулирования использования информационных технологий в контрольно-надзорной деятельности в целом недостаточно высок
Выявлена необходимость расширения перечня применяемых информационных технологий в контрольно-надзорной деятельности


ПРЕДЛОЖЕНИЯ для минимизации выявленных негативных факторов
Совершенствование синхронизации данных в различных государственных информационных системах
Сведение к минимуму бумажного документооборота
Периодическое обучение сотрудников контрольно-надзорных органов работе с электронными системами, повышение их квалификации в данном направлении
Налаживание электронного взаимодействия с подконтрольными субъектами (применение защищенных каналов связи, расширение использования личных кабинетов)

А.В. Мартынов, М.В. Бундин, Е.В. Ширеева, Е.Н. Смирнова,
М.Д. Прилуков, А.Э. Логинова

КОНЦЕПЦИЯ ПРАВОВОГО РЕГУЛИРОВАНИЯ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В СФЕРЕ ГОСУДАРСТВЕННОГО КОНТРОЛЯ И НАДЗОРА В УСЛОВИЯХ «ЦИФРОВОЙ ЭКОНОМИКИ»: РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Монография

Под научной редакцией д.ю.н., профессора А.В. Мартынова

Подписано в печать 30.12.2021. Формат 60x84/16.
Уч.-изд. л. 15,1. Усл. печ. л. 14,6. Тираж 500 экз. Заказ № 500.

Издательство Нижегородского госуниверситета им. Н.И. Лобачевского
603950, г. Нижний Новгород, пр. Гагарина, 23.

Отпечатано с готового оригинал-макета
в типографии Нижегородского госуниверситета им. Н.И. Лобачевского
603000, г. Нижний Новгород, ул. Б. Покровская, 37
Тел. 433-53-02; 433-83-25